

แนวปฏิบัติพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคล (ภาคส่วนทั่วไป)

BASIC GUIDELINES FOR PERSONAL DATA PROTECTION (GENERAL SECTOR)



สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
THE OFFICE OF THE PERSONAL DATA PROTECTION COMMITTEE

คำนำ

“แนวปฏิบัติพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคล (ภาคส่วนทั่วไป)” ฉบับนี้ จัดทำขึ้นเพื่อใช้เป็นแนวทางให้กับหน่วยงานและองค์กรต่าง ๆ นำไปประยุกต์ใช้ในการปฏิบัติตาม “แนวทางปฏิบัติและหลักเกณฑ์การประเมินความสอดคล้อง ด้านการคุ้มครองข้อมูลส่วนบุคคลทั้ง 10 ด้าน” ซึ่งเป็นมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับมาตรฐานสากล โดยมีเป้าหมายเพื่อเสริมสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้มีความเหมาะสม และสอดคล้องกับกฎหมาย

เนื้อหาในเอกสารฉบับนี้ ได้มีรายละเอียดเกี่ยวกับการดำเนินการตามมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมทั้ง 4 กลุ่ม 10 ด้าน 337 ข้อ เอกสารหลักฐานสำหรับใช้ประกอบการจัดทำตามมาตรฐาน พร้อมทั้งได้จัดทำตัวอย่างของเอกสารแต่ละประเภท เพื่อให้สามารถนำไปยึดถือปฏิบัติได้สะดวกยิ่งขึ้น

คณะผู้จัดทำหวังเป็นอย่างยิ่งว่า เอกสารฉบับนี้จะเป็นประโยชน์ต่อผู้ที่เกี่ยวข้องทุกภาคส่วนทั้งในเชิงการบริหารจัดการ การกำกับดูแล และการปฏิบัติ เพื่อก่อให้เกิดการดำเนินงานที่มีมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างยั่งยืนต่อไป

คณะผู้จัดทำ

สารบัญ

หน้า

บทที่ 1 สรุปแนวทางและเกณฑ์ตามเอกสารคู่มือการตรวจรับรองความสอดคล้องตามมาตรฐาน การ คุ้มครองข้อมูลส่วนบุคคล	1
บทที่ 2 การจัดทำเอกสารด้านองค์กรและการกำกับดูแล.....	3
บทที่ 3 การจัดทำเอกสารด้านนโยบายและแนวปฏิบัติ	75
บทที่ 4 การจัดทำเอกสารที่เกี่ยวข้องกับการอบรมและการสร้างความตระหนักรู้	149
บทที่ 5 สิทธิของเจ้าของข้อมูลส่วนบุคคล	222
บทที่ 6 การจัดทำเอกสารด้านการแจ้งวัตถุประสงค์และความโปร่งใส	303
บทที่ 7 การจัดทำบันทึกการรายการและฐานทางกฎหมาย	365
บทที่ 8 ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DPA และ DSA)	442
บทที่ 9 ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล.....	539
บทที่ 10 มาตรการรักษาความมั่นคงปลอดภัย (Data Security)	641
บทที่ 11 การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล.....	922
บทที่ 12 การยื่นคำขอ และหลักเกณฑ์การให้คะแนน.....	1049

บทที่ 1

สรุปแนวทางและเกณฑ์ตามเอกสารคู่มือการตรวจรับรองความสอดคล้องตามมาตรฐาน

การคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคลเป็นหนึ่งในประเด็นสำคัญที่ทุกองค์กรต้องให้ความสำคัญอย่างยิ่งในยุคดิจิทัลที่การประมวลผลข้อมูลมีบทบาทเชื่อมโยงกับกิจกรรมทางธุรกิจ การศึกษา และการบริการสาธารณะ โดยเฉพาะในประเทศไทยซึ่งได้ประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เพื่อสร้างมาตรฐานในการรักษาสิทธิและเสรีภาพของเจ้าของข้อมูล และเพื่อสร้างความน่าเชื่อถือให้แก่องค์กรที่ต้องประมวลผลข้อมูลในลักษณะต่าง ๆ หนึ่งในกลไกสำคัญที่จะช่วยยืนยันว่าองค์กรมีการดำเนินการที่เป็นไปตามกฎหมายและมาตรฐานสากล คือการตรวจรับรองความสอดคล้อง หรือที่มักเรียกว่า Trustmark

Trustmark เปรียบเสมือนตรารับรองที่ยืนยันว่าองค์กรมีมาตรการด้านการคุ้มครองข้อมูลที่ครบถ้วน โปร่งใส และสามารถตรวจสอบได้ ไม่เพียงแต่ช่วยสร้างความมั่นใจแก่เจ้าของข้อมูล แต่ยังเพิ่มความน่าเชื่อถือทางธุรกิจและความไว้วางใจในสถาบันการศึกษา หน่วยงานรัฐ หรือองค์กรเอกชนที่ได้รับการรับรองด้วย การได้รับ Trustmark ไม่ใช่เพียงเรื่องของการผ่านเกณฑ์ตรวจสอบ แต่ยังเป็นการแสดงออกถึงความรับผิดชอบ ความโปร่งใส และความมุ่งมั่นในการยกระดับมาตรฐานการจัดการข้อมูลส่วนบุคคลให้เทียบเท่าระดับสากล

กระบวนการตรวจรับรองดังกล่าวได้ถูกกำหนดให้ครอบคลุม 10 ด้านหลัก ที่เป็นหัวใจสำคัญของระบบ การบริหารจัดการข้อมูลส่วนบุคคล ตั้งแต่การกำกับดูแลในระดับนโยบาย การบริหารจัดการความเสี่ยง การคุ้มครองสิทธิของเจ้าของข้อมูล ไปจนถึงการตรวจสอบและประเมินความสอดคล้องอย่างต่อเนื่อง การดำเนินการในทั้ง 10 ด้านนี้ถือเป็นกรอบแนวทางที่ทำให้องค์กรสามารถปฏิบัติได้อย่างถูกต้อง มีประสิทธิภาพ และสามารถรับมือกับเหตุการณ์หรือปัญหาที่อาจเกิดขึ้นได้อย่างเป็นระบบ

ดังนั้น การทำความเข้าใจและปฏิบัติตามเกณฑ์ทั้ง 10 ด้านของ Trustmark จึงเป็นพื้นฐานสำคัญสำหรับองค์กรทุกประเภทที่ต้องการปฏิบัติตาม PDPA อย่างแท้จริง และสร้างความเชื่อมั่นที่ยั่งยืนแก่เจ้าของข้อมูลและผู้มีส่วนได้เสียทุกฝ่าย

การตรวจรับรองความสอดคล้อง (Trustmark) ด้านการคุ้มครองข้อมูลส่วนบุคคล ครอบคลุม 10 ด้านหลัก ดังนี้

1. Governance – การกำกับดูแลและนโยบายด้านข้อมูลส่วนบุคคล
2. Risk Management – การระบุและบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล
3. Data Subject Rights – การคุ้มครองสิทธิของเจ้าของข้อมูล
4. Lawful Basis – การอ้างอิงฐานทางกฎหมายในการประมวลผลข้อมูล
5. Consent Management – การจัดการความยินยอม
6. Data Security – มาตรการด้านความมั่นคงปลอดภัยของข้อมูล

7. Third Party Management – การจัดการผู้ประมวลผลข้อมูลส่วนบุคคลภายนอก (Data Processor / Third Party)

8. Incident Management – การรับมือและจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Data Breach)

9. Training & Awareness – การอบรมและสร้างความตระหนักรู้แก่บุคลากร

10. Monitoring & Audit – การติดตาม ตรวจสอบ และประเมินความสอดคล้อง

ซึ่งเนื้อหาทั้ง 10 ด้านจะทำการตรวจสอบในประเด็น ๆ ที่สำคัญในภาพรวม ๆ ดังนี้

ด้าน	สิ่งที่ตรวจสอบ
1. Governance (การกำกับดูแล)	ตรวจสอบว่ามีการกำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นลายลักษณ์อักษร มีโครงสร้างผู้รับผิดชอบ (เช่น DPO) และมีการกำกับติดตามอย่างต่อเนื่อง
2. Risk Management (การบริหารความเสี่ยง)	ตรวจสอบการประเมินและระบุความเสี่ยงด้านข้อมูลส่วนบุคคล มีทะเบียนความเสี่ยง และมีมาตรการควบคุมหรือลดความเสี่ยง
3. Data Subject Rights (สิทธิของเจ้าของข้อมูล)	ตรวจสอบกระบวนการรับคำขอใช้สิทธิ เช่น การเข้าถึงข้อมูล แก้ไข ลบ ระบุ ใช้สิทธิคัดค้าน และการตอบสนองต่อคำขออย่างเหมาะสม
4. Lawful Basis (ฐานทางกฎหมาย)	ตรวจสอบว่าการเก็บ ใช้ เผยข้อมูลอ้างอิงฐานทางกฎหมายที่ถูกต้อง (เช่น สัญญา กฎหมาย ความยินยอม หรือประโยชน์โดยชอบด้วยกฎหมาย)
5. Consent Management (การจัดการความยินยอม)	ตรวจสอบการขอเก็บและจัดเก็บความยินยอม การเพิกถอนความยินยอม และการเก็บหลักฐานการให้ความยินยอมอย่างโปร่งใส
6. Data Security (ความมั่นคงปลอดภัยของข้อมูล)	ตรวจสอบมาตรการด้านความปลอดภัย เช่น การเข้ารหัส การควบคุม สิทธิผู้ใช้งาน การตรวจสอบการเข้าถึง การสำรองข้อมูล และแผนตอบสนองเหตุการณ์
7. Third Party Management (การจัดการผู้ประมวลผล/ผู้รับจ้าง)	ตรวจสอบสัญญา/ข้อตกลงกับผู้ประมวลผลข้อมูล (Data Processor) และมาตรการกำกับดูแลคู่ค้าหรือผู้ให้บริการภายนอก
8. Incident Management (การจัดการเหตุการณ์)	ตรวจสอบขั้นตอนการรายงาน แจ้งเหตุ และจัดการเหตุละเมิดข้อมูล (Data Breach) รวมถึงการแจ้งเจ้าของข้อมูลและหน่วยงานกำกับตามกฎหมาย
9. Training & Awareness (การอบรมและตระหนักรู้)	ตรวจสอบการจัดอบรมบุคลากร การสื่อสารภายในองค์กร และการสร้างความตระหนักรู้เกี่ยวกับ PDPA อย่างต่อเนื่อง

ด้าน	สิ่งที่ตรวจสอบ
10. Monitoring & Audit (การติดตามและตรวจสอบ)	ตรวจสอบระบบติดตามและการตรวจสอบภายใน มีการทบทวนและประเมินความสอดคล้องกับ PDPA อย่างสม่ำเสมอ

บทที่ 2

การจัดทำเอกสารด้านองค์กรและการกำกับดูแล

การกำกับดูแล (Governance) ถือเป็นรากฐานสำคัญของการจัดการด้านการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร เนื่องจากเป็นกลไกที่สะท้อนถึงความมุ่งมั่น ความรับผิดชอบ และความโปร่งใสในการดำเนินงานให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และมาตรฐานสากล การมีโครงสร้างการกำกับดูแลที่ชัดเจนจะช่วยให้องค์กรสามารถกำหนดนโยบาย วางระเบียบปฏิบัติ กำหนดบทบาทหน้าที่ และกำกับติดตามการปฏิบัติได้อย่างเป็นระบบ ซึ่งเป็นสิ่งที่ผู้ตรวจรับรองให้ความสำคัญเป็นอันดับแรก

ในการตรวจรับรองความสอดคล้อง (Trustmark) ด้าน Governance จะไม่เพียงมุ่งพิจารณาว่าองค์กรมีเอกสารนโยบายหรือระเบียบที่เกี่ยวข้องเท่านั้น แต่ยังให้ความสำคัญต่อการบังคับใช้อย่างเป็นรูปธรรม เช่น การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) การจัดทำแผนปฏิบัติการประจำปี การกำหนดข้อบังคับภายในสำหรับบุคลากร การเผยแพร่นโยบายไปสู่ผู้ที่เกี่ยวข้อง และการจัดทำรายงานความคืบหน้าเพื่อเสนอผู้บริหาร

ดังนั้น เพื่อให้การดำเนินงานด้าน Governance ได้รับคะแนนเต็มในการตรวจรับรอง องค์กรจำเป็นต้องมีเอกสารหลักฐานที่ชัดเจน ครบคลุม และเป็นปัจจุบัน ตลอดจนต้องสามารถพิสูจน์ได้ว่าการนำไปปฏิบัติจริง ไม่ว่าจะเป็นนโยบายคุ้มครองข้อมูลส่วนบุคคล แผนการดำเนินงาน รายงานประชุม หรือคู่มือการปฏิบัติ การมีระบบการกำกับดูแลที่ครบถ้วนดังกล่าวไม่เพียงช่วยให้องค์กรผ่านเกณฑ์การตรวจรับรองเท่านั้น แต่ยังสร้างความเชื่อมั่นแก่เจ้าของข้อมูล บุคลากร และผู้มีส่วนได้ส่วนเสียในระยะยาว

ตารางรายละเอียดสิ่งที่ต้องทำในด้านที่ 1: Governance

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
1.1 นโยบาย คุ้มครอง ข้อมูลส่วน บุคคล	จัดทำนโยบาย PDPA ที่ ครอบคลุมทุกหลักการ และ ประกาศใช้อย่างเป็นทางการ	เอกสาร “Privacy Policy” เผยแพร่ต่อบุคลากรและ ผู้เกี่ยวข้อง	มีนโยบายเป็นลายลักษณ์ อักษร เผยแพร่ทั้งภายใน และภายนอก

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
1.2 โครงสร้าง การกำกับ ดูแล	กำหนดโครงสร้างองค์กร ด้านการคุ้มครองข้อมูล มี DPO/คณะกรรมการ PDPA	ผังองค์กร/คำสั่งแต่งตั้ง คณะกรรมการและ DPO	มีโครงสร้างชัดเจน ระบุ ผู้รับผิดชอบพร้อมหน้าที่
1.3 คำสั่ง แต่งตั้ง DPO	ออกคำสั่งแต่งตั้งเจ้าหน้าที่ คุ้มครองข้อมูล (DPO) อย่าง เป็นทางการ	เอกสารคำสั่งแต่งตั้ง/บันทึก การมอบหมายงาน	มีการแต่งตั้งเป็นลายลักษณ์ อักษร ระบุบทบาทหน้าที่
1.4 ระเบียบ/ ข้อบังคับ ภายใน	กำหนดข้อปฏิบัติ/วินัยใน การจัดการข้อมูลสำหรับ บุคลากร	ระเบียบปฏิบัติ / คู่มือ / Handbook บุคลากร	มีระเบียบข้อบังคับ และใช้ จริงในองค์กร
1.5 แผนการ ดำเนินงาน (Action Plan)	จัดทำแผนงาน/โครงการเพื่อ บังคับใช้นโยบาย PDPA	แผนปฏิบัติการรายปี/ราย ภาคการศึกษา	มีแผนชัดเจน พร้อม timeline และผู้รับผิดชอบ
1.6 การ ติดตามและ รายงานผล	มีระบบติดตามผลและ รายงานความคืบหน้าแก่ ผู้บริหาร	รายงานประชุม/รายงานผล การดำเนินงาน	มีรายงานและหลักฐานว่ามี การประชุม/รายงานต่อเนื่อง
1.7 เอกสาร มอบอำนาจ และ SOP	กำหนดขั้นตอนปฏิบัติ (Standard Operating Procedure) ในงานสำคัญ เช่น การเก็บ/ลบข้อมูล	SOP / คู่มือปฏิบัติ / แบบฟอร์มที่เกี่ยวข้อง	มี SOP ครอบคลุมทุก ขั้นตอนสำคัญ ใช้งานจริง
1.8 การ สื่อสารและ เผยแพร่	มีการแจ้งนโยบายและ แนวทางแก่บุคลากรและ ผู้เกี่ยวข้อง	เอกสารประกาศ แจ้งเวียน อีเมล เว็บไซต์	มีการเผยแพร่หลายช่องทาง ตรวจสอบได้
1.9 การ ตรวจสอบ ภายใน	มีการตรวจสอบภายในด้าน Governance อย่างน้อยปี ละ 1 ครั้ง	รายงาน Audit/Internal Review	มีรายงานตรวจสอบครบถ้วน พร้อมข้อเสนอแนะปรับปรุง

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
1.10 การปรับปรุง อย่าง ต่อเนื่อง	มีการทบทวนและแก้ไข นโยบาย/ระเบียบให้ทันสมัย	เอกสารเวอร์ชันใหม่ + บันทึกการปรับปรุง	มีการอัปเดตตามรอบหรือ เมื่อกฎหมายเปลี่ยน

ตัวอย่างการจัดทำเอกสารแต่ละข้อในรายละเอียด

1.1.1 คณะกรรมการหรือผู้บริหารสูงสุดมีหน้าที่รับผิดชอบโดยรวมในการคุ้มครองข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: คณะกรรมการ ผู้บริหารต้องมีส่วนร่วมในการกำหนดนโยบาย มีการติดตาม

หลักฐาน: 1) นโยบายการที่แสดงให้เห็นถึงการกำกับติดตามการดำเนินงาน
2) รายงานการประชุม กก.บริษัทหรือผู้บริหารองค์กร หรือ กก.กำกับดูแล

สภาพบังคับ: ไม่มีกฎหมายบังคับ

นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Policy)

องค์กรตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลของพนักงาน ลูกค้า คู่ค้า ผู้ใช้บริการ และผู้เกี่ยวข้องทุกฝ่าย โดยถือว่าข้อมูลส่วนบุคคลเป็นทรัพย์สินที่มีคุณค่าและต้องได้รับการปกป้องอย่างเหมาะสมตามหลักการความปลอดภัย ความชอบธรรม และความโปร่งใส ทั้งนี้ เพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรฐานสากลในการบริหารจัดการข้อมูล เพื่อให้เกิดการดำเนินงานอย่างเป็นระบบและมีประสิทธิภาพ คณะกรรมการบริษัทและผู้บริหารระดับสูงมีบทบาทสำคัญในการกำกับดูแล ทบทวน และอนุมัตินโยบายฉบับนี้ โดยมีวัตถุประสงค์เพื่อกำหนดแนวทางในการจัดเก็บ ใช้ เผยแพร่ และคุ้มครองข้อมูลส่วนบุคคล รวมถึงการกำหนดบทบาทหน้าที่ของหน่วยงานและบุคลากรภายในองค์กรที่เกี่ยวข้อง

1. ขอบเขตของนโยบาย

นโยบายนี้ครอบคลุมถึงข้อมูลส่วนบุคคลที่องค์กรเก็บรวบรวมจากเจ้าของข้อมูลทุกประเภท ทั้งที่อยู่ในรูปแบบเอกสารหรืออิเล็กทรอนิกส์ ซึ่งดำเนินการโดยองค์กร หรือโดยบุคคลภายนอกที่ปฏิบัติงานแทนองค์กร

2. บทบาทของคณะกรรมการและผู้บริหาร

คณะกรรมการบริษัทมีหน้าที่กำหนดนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล และทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

ผู้บริหารระดับสูงมีหน้าที่ในการสนับสนุนทรัพยากรและการปฏิบัติให้เป็นไปตามนโยบาย รวมถึงติดตามผลการดำเนินงานจากหน่วยงานที่รับผิดชอบโดยตรง

คณะกรรมการกำกับดูแลความเสี่ยงอาจได้รับมอบหมายให้พิจารณารายงานผลจาก Data Protection Officer (DPO) และให้ข้อเสนอแนะต่อไปยังคณะกรรมการชุดใหญ่

3. บทบาทของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

DPO ทำหน้าที่ให้คำปรึกษา ตรวจสอบ และรายงานผลการดำเนินงานตามนโยบายนี้แก่ผู้บริหารและคณะกรรมการอย่างสม่ำเสมอ รวมถึงประสานงานกับหน่วยงานต่าง ๆ ภายในองค์กรให้ปฏิบัติตามข้อกำหนดของกฎหมาย

4. การประเมินและติดตามผล

องค์กรจะมีการติดตาม ตรวจสอบ และประเมินผลการดำเนินงานตามนโยบายนี้อย่างต่อเนื่อง โดยมีการจัดทำรายงานผลและข้อเสนอแนะเพื่อพัฒนากระบวนการบริหารจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลง

5. การสื่อสารและสร้างการรับรู้

องค์กรจะส่งเสริมความเข้าใจและความตระหนักแก่พนักงานทุกระดับ ผ่านการอบรมภายใน การเผยแพร่คู่มือ และการสื่อสารอื่น ๆ เพื่อสร้างวัฒนธรรมด้านการคุ้มครองข้อมูลส่วนบุคคล

นโยบายฉบับนี้มีผลบังคับใช้ตั้งแต่วันที่ [ระบุวัน] เป็นต้นไป และให้หน่วยงานที่เกี่ยวข้องดำเนินการตามแนวทางที่กำหนดไว้โดยเคร่งครัด

ลงชื่อ

(ผู้บริหารสูงสุด/ประธานคณะกรรมการ)

วันที่

รายงานการประชุมคณะกรรมการบริหารองค์กร

ครั้งที่ 3/2568

วัน/เวลา: วันพุธที่ 15 พฤษภาคม พ.ศ. 2568 เวลา 13.30 - 15.30 น.

สถานที่ประชุม: ห้องประชุมใหญ่ ชั้น 5 อาคารสำนักงานใหญ่

ผู้เข้าร่วมประชุม:

1. นาย A – ประธานกรรมการ
2. นาย B – รองประธานกรรมการ
3. นาย C – กรรมการ
4. นางสาว D – กรรมการ
5. นาย E – กรรมการและผู้จัดการทั่วไป

เลขานุการการประชุม: นางสาว F

วาระการประชุม

วาระที่ 1: รับรองรายงานการประชุมครั้งที่ผ่านมา

ที่ประชุมมีมติเป็นเอกฉันท์ให้รับรองรายงานการประชุมครั้งที่ 2/2568 โดยไม่มีการแก้ไข

วาระที่ 2: เรื่องแจ้งเพื่อทราบ

ประธานแจ้งถึงแนวโน้มนการปรับปรุงกฎหมายด้านความมั่นคงปลอดภัยของข้อมูล ซึ่งอาจมีผลต่อแนวทางปฏิบัติขององค์กรในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

วาระที่ 3: เรื่องเพื่อพิจารณา

3.1 รายงานผลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (ไตรมาส 1/2568)

นางสาว F (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล: DPO) ได้นำเสนอผลการดำเนินงานที่สำคัญ ดังนี้

- มีการจัดอบรมเชิงปฏิบัติการให้แก่พนักงานใหม่ 50 คน เรื่องสิทธิของเจ้าของข้อมูล
- พบเหตุการณ์ Data Breach จำนวน 1 กรณี อยู่ระหว่างกระบวนการสอบสวน
- ได้มีการทบทวนนโยบายจัดเก็บข้อมูล (Data Retention) และเตรียมนำเสนอร่างปรับปรุงฉบับใหม่ในไตรมาสหน้า

ข้อเสนอแนะจากที่ประชุม:

นาย A เสนอให้มีการกำหนด KPI ด้านการคุ้มครองข้อมูล เช่น สัดส่วนการอบรม และระยะเวลาการจัดการเหตุละเมิด

นาย B เห็นว่าควรจัดทำรายงาน Dashboard ความเสี่ยงข้อมูลส่วนบุคคลเพื่อนำเสนอทุกไตรมาส ที่ประชุมเห็นพ้องให้ฝ่าย DPO ร่วมกับฝ่ายไอทีและกฎหมาย ปรับปรุงระบบการจัดการข้อมูลให้เป็นไปตามหลัก Privacy by Design

มติที่ประชุม:

ที่ประชุมมีมติ “รับทราบรายงาน และมอบหมายให้เจ้าหน้าที่ DPO ดำเนินการตามข้อเสนอแนะ พร้อมจัดทำรายงานความคืบหน้าเสนอในที่ประชุมไตรมาสต่อไป”

วาระที่ 4: เรื่องอื่น ๆ

ไม่มีวาระเพิ่มเติม

ปิดประชุมเวลา: 15.30 น.

ลงชื่อ.....

(นาย A)

ประธานการประชุม

ลงชื่อ.....

(นางสาว F)

เลขานุการการประชุม

1.1.2 ผู้บริหารเป็นผู้นำ เป็นแบบอย่าง และส่งเสริมวัฒนธรรมเชิงบวก เชิงรุกในการปฏิบัติตามกฎหมาย

สิ่งที่ต้องทำ: ผู้บริหารเป็นแบบอย่างที่ดีในการรักษาความมั่นคงปลอดภัยฯ และส่งเสริมวัฒนธรรมเชิงบวก

หลักฐาน: 1) รายงานการประชุม กก.บริษัท หรือผู้บริหารองค์กร หรือ กก.กำกับฯ หรืองานงานของ DPO ต่อกรรมการที่แสดงให้เห็นว่าผู้บริหารระดับสูงปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยฯ

2) รายงานการเข้าถึงข้อมูลตามสิทธิที่กำหนด

สภาพบังคับ: ไม่มีกฎหมายบังคับ

1) รายงานการประชุมคณะกรรมการบริหาร (แสดงบทบาทผู้นำของผู้บริหาร)

รายงานการประชุมคณะกรรมการบริหารองค์กร

ครั้งที่ 4/2568

วัน/เวลา: วันพฤหัสบดีที่ 16 พฤษภาคม พ.ศ. 2568 เวลา 13.30 – 15.00 น.

สถานที่ประชุม: ห้องประชุมใหญ่ ชั้น 5 อาคารสำนักงาน

ผู้เข้าร่วมประชุม:

1. นาย A – ประธานกรรมการ
2. นาย B – รองประธานกรรมการ
3. นาย C – กรรมการ
4. นางสาว D – กรรมการ
5. นาย E – กรรมการและผู้จัดการทั่วไป

เลขานุการการประชุม: นางสาว F (เจ้าหน้าที่ DPO)

วาระที่ 3: การเสริมสร้างวัฒนธรรมเชิงรุกในการคุ้มครองข้อมูลส่วนบุคคล

นางสาว F (DPO) รายงานว่า:

ได้จัดกิจกรรม “Privacy Week” ภายในองค์กร โดยมีผู้บริหารเข้าร่วมเป็นวิทยากรเปิดงาน

นาย A ได้ร่วมทำคลิปวิดีโอสั้นรณรงค์เรื่องความปลอดภัยของข้อมูล และส่งถึงพนักงานทุกคน

มีการประกาศภายในองค์กรว่า ผู้บริหารจะเป็นกลุ่มแรกที่เข้ารับการทดสอบความเข้าใจด้าน PDPA ทุกไตรมาส

ความคิดเห็นจากที่ประชุม:

- นาย B กล่าวว่า ผู้บริหารต้องเป็นต้นแบบในเรื่องวินัยข้อมูล (Data Discipline) โดยเฉพาะการไม่ถ่ายภาพเอกสารหรือหน้าจอข้อมูลลูกค้า
- นางสาว D เสนอให้จัดทำประกาศ “ค่านิยมองค์กรด้านข้อมูล” (Data Integrity Values) เพื่อสร้างวัฒนธรรมองค์กร

มติที่ประชุม:

เห็นชอบให้ทุกฝ่ายสนับสนุนการสร้างวัฒนธรรมคุ้มครองข้อมูล โดยผู้บริหารจะเป็นต้นแบบและ
รายงานผลความคืบหน้าในทุกไตรมาส

ปิดประชุมเวลา: 15.00 น.

ลงชื่อ (นาย A)

ประธานการประชุม

ลงชื่อ (นางสาว F)

เลขานุการการประชุม

2) รายงานการเข้าถึงข้อมูลตามสิทธิที่กำหนด (โดยมีผู้บริหารเป็นแบบอย่าง)

รายงานการเข้าถึงข้อมูลส่วนบุคคล (Access Log Report)

ระหว่างวันที่ 1 เม.ย. – 30 เม.ย. 2568

จัดทำโดย: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ส่งถึง: คณะกรรมการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล

1. ภาพรวมการเข้าถึงข้อมูล

- พนักงานทั่วไป 32 คน เข้าถึงข้อมูลตามบทบาทหน้าที่
- มีการตรวจสอบย้อนหลังกรณีการเข้าถึงผิดปกติ 0 ครั้ง

2. ผู้บริหารเข้าถึงข้อมูลตามนโยบาย Role-based Access Control (RBAC)

- นาย A (ประธานกรรมการ): เข้าถึงเฉพาะรายงานสรุปเชิงสถิติที่ไม่สามารถระบุตัวตน
- นาย E (ผู้จัดการทั่วไป): เข้าถึงข้อมูลระดับระบบเพื่อตรวจสอบการปฏิบัติตามนโยบาย โดยมี
เหตุผลตามแบบคำร้อง

ไม่มีผู้บริหารคนใดเข้าถึงข้อมูลส่วนบุคคลในเชิงลึกโดยไม่มีแบบฟอร์มหรือคำสั่ง

3. การทบทวนและรับรองการเข้าถึง

ผู้บริหารทุกคนได้ลงนามรับรองการปฏิบัติตามมาตรการในการประชุมเมื่อวันที่ 16 พฤษภาคม

2568

ไม่มีรายงานการฝ่าฝืนมาตรการเข้าถึง

สรุป: ผู้บริหารมีบทบาทเป็นแบบอย่างโดยจำกัดตนเองให้เข้าถึงข้อมูลเท่าที่จำเป็น มีการรับรองและตรวจสอบอย่างโปร่งใส ช่วยเสริมสร้างวัฒนธรรมเชิงบวกในองค์กร

ลงชื่อ (นางสาว F)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ตัวอย่างการประกาศลำดับสิทธิ

ประกาศลำดับสิทธิการเข้าถึง แก๊ไข ลบ และปรับปรุงข้อมูลส่วนบุคคล

องค์กรตัวอย่าง จำกัด

ประกาศ ณ วันที่ 1 มิถุนายน พ.ศ. 2568

เพื่อให้การบริหารจัดการข้อมูลส่วนบุคคลขององค์กรเป็นไปอย่างมีประสิทธิภาพ และสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล องค์กรได้กำหนดลำดับสิทธิในการ “เข้าถึง แก๊ไข ลบ ปรับปรุง” ข้อมูลส่วนบุคคลของเจ้าของข้อมูล ดังรายละเอียดต่อไปนี้

1. ผู้มีอำนาจสูงสุดในสิทธิการเข้าถึงและจัดการข้อมูล (High-Level Authority)

1.1 ประธานกรรมการบริหาร (CEO/MD/กรรมการผู้จัดการ)

สิทธิ:

- ขั้นสุดท้ายการเข้าถึง แก๊ไข ลบข้อมูลของบุคลากรระดับสูง
- ตรวจสอบกิจกรรมการเข้าถึงของฝ่ายต่าง ๆ

การเข้าถึง: ผ่านแบบฟอร์มคำร้องขอใช้งาน พร้อมเหตุผลและลายเซ็นรับรอง DPO

1.2 รองกรรมการผู้จัดการ/ผู้อำนวยการฝ่าย (ระดับ C-level เช่น CIO, COO)

สิทธิ:

- ขออนุมัติการเข้าถึง/แก๊ไขข้อมูลเฉพาะฝ่ายตนเอง
- ตรวจสอบความถูกต้องของข้อมูลในความรับผิดชอบ

เงื่อนไข: ต้องมีการบันทึกเหตุผล และแจ้งต่อ DPO ภายใน 24 ชั่วโมง

2. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

สิทธิ:

- ตรวจสอบ บันทึก และติดตามการเข้าถึงของทุกระดับ
- ไม่มีสิทธิ “ลบ” ข้อมูล ยกเว้นเพื่อปฏิบัติตามคำสั่งของผู้มีอำนาจสูง
- ทำหน้าที่กลั่นกรองก่อนส่งต่อให้ผู้บริหารอนุมัติ

3. หัวหน้าฝ่าย/หัวหน้างาน

สิทธิ:

- เข้าถึงข้อมูลส่วนบุคคลของลูกค้า/บุคลากรในฝ่ายที่ตนดูแล
- ขอปรับปรุงข้อมูลเพื่อความถูกต้อง เช่น การอัปเดตเบอร์โทรศัพท์/ที่อยู่

เงื่อนไข: ต้องขอผ่านระบบพร้อม Log บันทึกการเปลี่ยนแปลง

4. เจ้าหน้าที่ทั่วไป (ระดับปฏิบัติการ)

สิทธิ:

- เข้าถึงข้อมูลเฉพาะที่ได้รับมอบหมาย เช่น แบบฟอร์มลงทะเบียน
- ไม่มีสิทธิในการ “ลบ” หรือ “แก๊ไข” ข้อมูลโดยตรง

เงื่อนไข: การดำเนินการต้องอยู่ภายใต้คำสั่งหัวหน้างาน และระบบควบคุมการเข้าถึง (RBAC)

5. พนักงานจ้างเหมา / ชั่วคราว / นักศึกษาฝึกงาน

สิทธิ:

- ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ เว้นแต่มีหนังสืออนุญาตเป็นกรณีพิเศษ

เงื่อนไข: ต้องอยู่ภายใต้การกำกับดูแลใกล้ชิดของหัวหน้างาน

แนวปฏิบัติเพิ่มเติม

- การขอเข้าถึงหรือจัดการข้อมูลใด ๆ ต้องดำเนินการผ่านระบบที่องค์กรจัดเตรียมไว้ พร้อมมีการบันทึก Log ทุกครั้ง
- องค์กรจะทำการทบทวนสิทธิเป็นประจำทุก 6 เดือน และปรับปรุงสิทธิการเข้าถึงตามโครงสร้างงานที่เปลี่ยนแปลง

ลงชื่อ.....

(นาย A)

ประธานกรรมการบริหาร

ลงชื่อ.....

(นางสาว F)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

1.1.3 มีสายรายงานหรือบังคับบัญชาและการไหลเวียนของข้อมูลหรือส่วนงาน

1.1.4 มินโยบายที่ชัดเจนในการกำหนดโครงสร้างองค์กรสำหรับการคุ้มครองข้อมูลส่วนบุคคลและกำกับ

ดูแล

สิ่งที่ต้องทำ: มินโยบายที่กำหนดโครงสร้างสำหรับการคุ้มครองข้อมูลส่วนบุคคล

หลักฐาน: 1) รายงานการประชุมของ กก.บริษัทหรือองค์กรหรือผู้บริหารที่ระบุถึงนโยบายในการกำหนดโครงสร้างองค์กรเพื่อคุ้มครองข้อมูลหรือกำกับดูแล

สภาพบังคับ: ไม่มีกฎหมายบังคับ

รายงานการประชุมผู้บริหารองค์กร

ครั้งที่ 3/2567

วันเวลา: วันที่ 15 มีนาคม 2567

สถานที่: ห้องประชุมใหญ่ ชั้น 5 อาคารสำนักงานกลาง

ผู้เข้าร่วมประชุม:

- นาย A ประธานกรรมการบริหาร
- นาย B รองประธานกรรมการ
- นางสาว C ผู้จัดการฝ่ายทรัพยากรบุคคล
- นาย D เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- นาย E หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

วาระการประชุมที่ 2: การกำหนดนโยบายโครงสร้างองค์กรสำหรับการคุ้มครองข้อมูลส่วนบุคคล

นาย A ได้กล่าวเปิดวาระโดยเสนอให้มีการกำหนดนโยบายที่ชัดเจนเกี่ยวกับโครงสร้างองค์กรในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับแนวทางการบริหารจัดการข้อมูลอย่างปลอดภัยและมีประสิทธิภาพ

ที่ประชุมมีมติให้กำหนดโครงสร้างองค์กรสำหรับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้:

1. แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) อย่างเป็นทางการ ซึ่งจะรายงานตรงต่อคณะผู้บริหาร

2. จัดตั้งฝ่ายคุ้มครองข้อมูลส่วนบุคคล ภายใต้การกำกับดูแลของ DPO โดยมีเจ้าหน้าที่สนับสนุนอย่างน้อย 2 คน

3. ให้แต่ละฝ่ายภายในองค์กรมีผู้ประสานงานด้านข้อมูลส่วนบุคคล (Data Liaison) เพื่อประสานงานกับ DPO

4. ให้มีการทบทวนโครงสร้างและนโยบายทุกปี และสามารถปรับปรุงเพิ่มเติมตามความเหมาะสมที่ประชุมรับรองนโยบายดังกล่าว และมอบหมายให้ DPO ดำเนินการตามขั้นตอนต่อไป

ลงชื่อ (นาย A)

ประธานกรรมการบริหาร

วันที่ลงนาม: 15 มีนาคม 2567

1.1.5 JD ระบุความรับผิดชอบและสายรายงานผู้บริหาร

สิ่งที่ต้องทำ: ระบุความรับผิดชอบด้าน PDPA ใน JD และสายการบังคับบัญชา

หลักฐาน: 1) เขียน JD หรือข้อตกลงการปฏิบัติงาน หรือสัญญาจ้าง หรือสภาพการจ้าง โดยต้องมีเนื้อหา “ระบุความรับผิดชอบด้าน PDPA แก่พนักงานทุกคนว่ามีหน้าที่ตามกฎหมาย”

สภาพบังคับ: ไม่มีกฎหมายบังคับ

ตัวอย่าง Job Description (JD) สำหรับพนักงานทุกระดับ (PDPA & Security)

ตำแหน่ง: _____

แผนก: _____

ผู้บังคับบัญชา: _____

วันที่: _____

หน้าที่และความรับผิดชอบหลัก

1. ปฏิบัติงานตามที่ได้รับมอบหมายอย่างเต็มความสามารถและมีคุณภาพรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ได้รับมอบหมายหรือเข้าถึงในระหว่างปฏิบัติงานปฏิบัติตามนโยบาย กฎระเบียบ และมาตรการขององค์กรที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างเคร่งครัด
2. รับผิดชอบในการดูแลและป้องกันข้อมูลส่วนบุคคลไม่ให้รั่วไหล สูญหาย หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
3. รายงานเหตุการณ์หรือปัญหาที่เกี่ยวข้องกับข้อมูลส่วนบุคคลหรือความมั่นคงปลอดภัยของข้อมูลต่อผู้บังคับบัญชาหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยทันที
4. ร่วมมือในการอบรมและพัฒนาความรู้ความเข้าใจเกี่ยวกับ PDPA และการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างต่อเนื่อง

5. ปฏิบัติตามคำแนะนำและคำสั่งจากผู้บริหารหรือเจ้าหน้าที่ที่เกี่ยวข้องในการจัดการข้อมูลส่วนบุคคลและความปลอดภัยของข้อมูล

6. ดำเนินการอื่น ๆ ที่ได้รับมอบหมายซึ่งเกี่ยวข้องกับหน้าที่ดังกล่าว
ความรับผิดชอบเพิ่มเติมเฉพาะ (ถ้ามี)

สายการบังคับบัญชา

รายงานตรงต่อ: _____

ประสานงานกับ: _____

ลงชื่อพนักงาน: _____

วันที่: _____

ลงชื่อผู้บังคับบัญชา: _____

วันที่: _____

1.1.6 JD เป็นปัจจุบัน เหมาะสมกับวัตถุประสงค์ และมีการทบทวนสม่ำเสมอ

สิ่งที่ต้องทำ: ทำ JD เป็นปัจจุบัน เหมาะสมกับวัตถุประสงค์ และมีการทบทวนสม่ำเสมอ

หลักฐาน: 1) อาจกำหนดระยะเวลาทบทวนเพื่อแก้ไขปรับปรุง JD หรือข้อตกลงการปฏิบัติงาน หรือสัญญาจ้าง หรือสภาพการจ้าง โดยต้องมีเนื้อหา “ระบุความรับผิดชอบด้าน PDPA แก่พนักงานทุกคนว่ามีหน้าที่ตามกฎหมาย”

สภาพบังคับ: ไม่มีกฎหมายบังคับ

รายงานการประชุมและคำอธิบายเรื่องการทบทวน JD

รายงานการประชุมฝ่ายทรัพยากรบุคคล

บริษัท ตัวอย่าง จำกัด

วันที่: 15 มิถุนายน 2568

สถานที่: ห้องประชุมฝ่ายทรัพยากรบุคคล ชั้น 3

เรื่อง: การทบทวนและปรับปรุงรายละเอียดงาน (Job Description - JD) ให้ทันสมัยและสอดคล้องกับกฎหมาย PDPA

ผู้เข้าร่วมประชุม:

- นาง C (หัวหน้าฝ่ายทรัพยากรบุคคล)
- นาย E (เจ้าหน้าที่ฝ่ายพัฒนาองค์กร)

- นาง D (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - DPO)

สาระสำคัญการประชุม:

1. ที่ประชุมเห็นชอบให้มีการทบทวนรายละเอียดงาน (JD) ทุกตำแหน่งงาน อย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับวัตถุประสงค์ขององค์กรและกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ที่มีการเปลี่ยนแปลงอยู่เสมอ

2. กำหนดให้ในทุกครั้งของการทบทวน JD ต้องตรวจสอบและปรับปรุงให้ระบุมความรับผิดชอบด้าน PDPA อย่างชัดเจนในทุกตำแหน่งงาน รวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายขององค์กร

3. กำหนดให้ฝ่ายทรัพยากรบุคคลทำหน้าที่รวบรวมข้อมูลและแก้ไข JD พร้อมส่งให้ผู้บริหารพิจารณาอนุมัติ ก่อนนำไปใช้บังคับใช้อย่างเป็นทางการ

รายงานการทบทวน JD จะถูกจัดเก็บเป็นหลักฐานเพื่อแสดงความต่อเนื่องและความรับผิดชอบขององค์กรในด้านการคุ้มครองข้อมูลส่วนบุคคล

มติที่ประชุม: เห็นชอบให้ทบทวน JD ปีละ 1 ครั้ง และจัดทำรายงานการทบทวนเป็นลายลักษณ์อักษรทุกครั้ง

คำอธิบายเรื่องระยะเวลาทบทวน:

บริษัทฯ กำหนดให้มีการทบทวนรายละเอียดงาน (JD) อย่างสม่ำเสมอทุกปี เพื่อให้มั่นใจว่า JD นั้นยังคงเหมาะสมกับวัตถุประสงค์ขององค์กรและสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) การทบทวนนี้ช่วยให้สามารถปรับปรุงหรือแก้ไขหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับ PDPA ได้ทันเวลา และส่งเสริมให้พนักงานตระหนักถึงหน้าที่และความรับผิดชอบในด้านนี้อย่างต่อเนื่อง

ลงชื่อ:

(นาง C)

หัวหน้าฝ่ายทรัพยากรบุคคล

ลงชื่อ:

(นาง D)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

1.1.7 DPO และการกำกับดูแลเข้าใจโครงสร้างองค์กรและความรับผิดชอบของตน

สิ่งที่ต้องทำ: สร้างความเข้าใจให้พนักงานทุกคน เข้าใจเรื่องโครงสร้างองค์กรและสร้างความเข้าใจเกี่ยวกับความรับผิดชอบด้าน PDPA

หลักฐาน: 1) รายงานการประชุมในระดับฝ่ายที่มีเนื้อความแสดงให้เห็นว่าพนักงานเข้าใจให้พนักงานทุกคน เข้าใจเรื่องโครงสร้างองค์กรและสร้างความเข้าใจเกี่ยวกับความรับผิดชอบด้าน PDPA

สภาพบังคับ: ไม่มีกฎหมายบังคับ

รายงานการประชุมฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO)

บริษัท ตัวอย่าง จำกัด

วันที่: 20 มิถุนายน 2568

สถานที่: ห้องประชุมฝ่ายคุ้มครองข้อมูล ชั้น 4

เรื่อง: การสร้างความเข้าใจเกี่ยวกับโครงสร้างองค์กรและความรับผิดชอบด้าน PDPA แก่พนักงานทุกคน

ผู้เข้าร่วมประชุม

- นาง D (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - DPO)
- นาย F (หัวหน้าฝ่ายไอที)
- นาง G (หัวหน้าฝ่ายทรัพยากรบุคคล)
- พนักงานฝ่ายต่าง ๆ รวม 20 คน

สาระสำคัญการประชุม:

1. นาง D ได้ชี้แจงและนำเสนอแผนผังโครงสร้างองค์กร โดยเน้นบทบาทและหน้าที่ความรับผิดชอบของแต่ละฝ่ายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA)
2. อธิบายหน้าที่และบทบาทของ DPO ในการกำกับดูแลและสนับสนุนการปฏิบัติตาม PDPA รวมถึงช่องทางการสื่อสารและการรายงานปัญหา
3. ให้ความรู้และสร้างความเข้าใจเกี่ยวกับหน้าที่ของพนักงานแต่ละระดับในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และการปฏิบัติตามนโยบาย PDPA ขององค์กร
4. เปิดโอกาสให้พนักงานซักถามข้อสงสัยเกี่ยวกับโครงสร้างองค์กรและความรับผิดชอบด้าน PDPA เพื่อให้เกิดความชัดเจนและการมีส่วนร่วม
5. สรุปและเน้นย้ำให้ทุกคนปฏิบัติตามหน้าที่ด้วยความรับผิดชอบและความรอบคอบ

มติที่ประชุม:

- พนักงานทุกคนเข้าใจบทบาทความรับผิดชอบและโครงสร้างองค์กรที่เกี่ยวข้องกับ PDPA อย่างชัดเจน
- กำหนดให้มีการอบรมและทบทวนความรู้เรื่อง PDPA อย่างต่อเนื่องทุก 6 เดือน

ลงชื่อ:

(นาง D)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ลงชื่อ:

(นาย F)

หัวหน้าฝ่ายไอที

1.2.1 DPO มีหน้าที่รับผิดชอบตาม ม. 42

สิ่งที่ต้องทำ: การปฏิบัติงานหรือดำเนินการของ DPO ครบถ้วนตาม ม. 42

หลักฐาน: 1) รายงานการประชุมของผู้บริหาร หรือ กก.กำกับฯ หรือเอกสารการรายงานผลของ DPO
เนื้อหาต้องมีเรื่องการทำหน้าที่
2) เอกสารคำสั่งแต่งตั้ง DPO (ระบุหน้าที่ให้ครบทุกด้านตาม ม. 42)

สภาพบังคับ: มาตรา 42

1. รายงานการประชุมผู้บริหารเกี่ยวกับการรายงานผลการปฏิบัติหน้าที่ของ DPO

บริษัท ตัวอย่าง จำกัด

รายงานการประชุมผู้บริหาร

วันที่: 10 มิถุนายน 2568

สถานที่: ห้องประชุมใหญ่ ชั้น 5

เรื่อง: การรายงานผลการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามมาตรา 42 PDPA

ผู้เข้าร่วมประชุม:

- นาย A (กรรมการผู้จัดการ)
- นาง B (รองกรรมการผู้จัดการ)
- นาย C (หัวหน้าฝ่ายกฎหมาย)
- นาง D (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - DPO)

สาระสำคัญ:

1. นาง D รายงานความคืบหน้าการดำเนินงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตาม PDPA โดยสรุปการปฏิบัติตามมาตรา 42 ครอบคลุมเรื่องการจัดทำทะเบียนข้อมูลส่วนบุคคล การให้ความรู้และอบรมพนักงาน การรับเรื่องร้องเรียน และการประสานงานกับหน่วยงานที่เกี่ยวข้อง
2. แจ้งการติดตามและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยข้อมูล รวมถึงมาตรการที่นำมาใช้เพื่อป้องกันเหตุละเมิดข้อมูล
3. รับทราบปัญหาและอุปสรรค พร้อมเสนอแนะแนวทางแก้ไข

4. กรรมการและผู้บริหารแสดงความเห็นชอบและให้การสนับสนุนการปฏิบัติหน้าที่ของ DPO อย่างเต็มที่

มติที่ประชุม:

- รับทราบรายงานและเห็นชอบแนวทางการดำเนินงานของ DPO
- กำหนดให้มีการรายงานผลการปฏิบัติงานทุกไตรมาส

ลงชื่อ:

(นาย A)

กรรมการผู้จัดการ

ลงชื่อ:

(นาง D)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

1.2.2 DPO มีอำนาจปฏิบัติหน้าที่ การได้รับการสนับสนุน การจัดทรัพยากรอย่างมีประสิทธิภาพ

สิ่งที่ต้องทำ: ให้อำนาจ DPO เข้าถึงข้อมูลองค์กร และจัดสรรทรัพยากรสนับสนุน DPO

หลักฐาน: 1) ภาพถ่ายอุปกรณ์ หรือเครื่องมือที่องค์กรจัดให้ DPO
2) บันทึกเอกสารการให้อำนาจ DPO เข้าถึงฐานข้อมูลองค์กร และบันทึกที่แสดงว่า DPO มีสิทธิเข้าถึงฐานข้อมูลองค์กร

สภาพบังคับ: มาตรา 42

คำสั่งแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

บริษัท ตัวอย่าง จำกัด

คำสั่งแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เลขที่คำสั่ง: 01/2568

วันที่: 1 มิถุนายน 2568

เพื่อให้เป็นไปตามมาตรา 42 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัท ตัวอย่าง จำกัด มีความประสงค์แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO) ดังนี้

แต่งตั้ง: นาง ด.ดวงดี ใจดี ตำแหน่ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

หน้าที่และความรับผิดชอบ:

1. ดำเนินการและกำกับดูแลให้การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)
2. ให้คำแนะนำแก่ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลเกี่ยวกับการปฏิบัติตามกฎหมาย
3. ประสานงานกับหน่วยงานกำกับดูแลและเจ้าหน้าที่อื่น ๆ ในการคุ้มครองข้อมูลส่วนบุคคล
4. จัดทำและดูแลระบบทะเบียนการประมวลผลข้อมูลส่วนบุคคล
5. เป็นจุดติดต่อหลักสำหรับผู้ที่เกี่ยวข้องในการจัดการข้อมูลส่วนบุคคล
6. ดูแลและติดตามการจัดการเรื่องร้องเรียนเกี่ยวกับข้อมูลส่วนบุคคล
7. ให้ความรู้และฝึกอบรมพนักงานเกี่ยวกับการคุ้มครองข้อมูล
8. ตรวจสอบและประเมินความเสี่ยงในการจัดการข้อมูลส่วนบุคคล
9. รายงานผลการดำเนินงานและประเด็นที่เกี่ยวข้องต่อคณะกรรมการหรือผู้บริหารระดับสูงอย่างสม่ำเสมอ

สัปดาห์

ประกาศ ณ วันที่: 1 มิถุนายน 2568

ลงชื่อ:

(นาย A)

กรรมการผู้จัดการ

ตัวอย่าง ภาพถ่ายอุปกรณ์หรือเครื่องมือที่องค์กรจัดให้ DPO

ภาพถ่ายตัวอย่าง (กรุณาแนบภาพจริงที่องค์กรมีให้ DPO)

- คอมพิวเตอร์โน้ตบุ๊กพร้อมซอฟต์แวร์ด้านความปลอดภัยข้อมูล
- โทรศัพท์มือถือสำหรับการปฏิบัติงาน
- บัตรประจำตัวพนักงานที่มีสิทธิ์เข้าถึงข้อมูลในระบบ
- ซอฟต์แวร์ระบบบริหารจัดการข้อมูลส่วนบุคคล (PDPA Management System)
- สิทธิ์การเข้าถึงระบบฐานข้อมูลสำคัญขององค์กร (ผ่าน VPN หรือระบบภายใน)
- ค่าตอบแทนพิเศษสำหรับ DPO
- แผนงานการพัฒนาความรู้ของ DPO ประจำปี

บันทึกเอกสารการให้อำนาจ DPO เข้าถึงฐานข้อมูลองค์กร

บริษัท ตัวอย่าง จำกัด

บันทึกข้อความเลขที่: บค-2025/07

วันที่: 2 กรกฎาคม 2568

เรื่อง: การให้อำนาจเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เข้าถึงฐานข้อมูลขององค์กร

เรียน: ผู้บริหารทุกฝ่าย

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 42 บริษัท ตัวอย่าง จำกัด แต่งตั้ง นาง ด.ดวงดี ใจดี ดำรงตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อปฏิบัติหน้าที่ดูแลคุ้มครองข้อมูลส่วนบุคคลขององค์กร

โดยมอบอำนาจให้ DPO ดังนี้

- มีสิทธิ์เข้าถึงฐานข้อมูลทั้งหมดที่เกี่ยวข้องกับการเก็บรวบรวม ประมวลผล และการรักษา ความปลอดภัยของข้อมูลส่วนบุคคลในองค์กร
- ใช้ทรัพยากรทั้งบุคลากร เครื่องมือ และระบบที่จำเป็นเพื่อปฏิบัติหน้าที่ตามกฎหมายอย่างมีประสิทธิภาพ
- ประสานงานกับฝ่าย IT ฝ่ายรักษาความปลอดภัย และฝ่ายบริหาร เพื่อสนับสนุนการปฏิบัติงานของ DPO

ทั้งนี้ ให้ฝ่ายที่เกี่ยวข้องจัดเตรียมข้อมูลและทรัพยากรที่จำเป็นเพื่อสนับสนุนการปฏิบัติหน้าที่ของ DPO อย่างเต็มที่

ลงชื่อ:

(นาย A)

กรรมการผู้จัดการ

บันทึกสิทธิเข้าถึงฐานข้อมูลของ DPO

บริษัท ตัวอย่าง จำกัด

บันทึกข้อความเลขที่: บค-2025/08

วันที่: 3 กรกฎาคม 2568

เรื่อง: การกำหนดสิทธิการเข้าถึงฐานข้อมูลของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เรียน: ฝ่ายไอทีและฝ่ายที่เกี่ยวข้อง

เพื่อสนับสนุนการปฏิบัติหน้าที่ตามมาตรา 42 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัท ตัวอย่าง จำกัด ได้กำหนดสิทธิการเข้าถึงฐานข้อมูลสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ดังนี้

- สิทธิในการดูข้อมูลและดึงข้อมูลที่เกี่ยวข้องกับการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลในระบบฐานข้อมูลหลักขององค์กร
- สิทธิในการเรียกดู Log การใช้งานฐานข้อมูลและระบบรักษาความปลอดภัย
- สิทธิในการตรวจสอบและประเมินความเสี่ยงของระบบฐานข้อมูลร่วมกับฝ่าย IT
- สิทธิในการประสานงานและขอข้อมูลจากหน่วยงานต่าง ๆ ตามความจำเป็นในการปฏิบัติหน้าที่ฝ่ายไอทีและฝ่ายที่เกี่ยวข้องโปรดจัดให้สิทธิดังกล่าวแก่ DPO ภายในวันที่ 5 กรกฎาคม 2568 และรายงานผลการดำเนินการมายังฝ่ายบริหาร

ลงชื่อ:

(นาย B)

หัวหน้าฝ่ายไอที

1.2.3 DPO มีความรู้ ความเชี่ยวชาญกฎหมาย และแนวปฏิบัติ

สิ่งที่ต้องทำ: DPO มีประกาศนียบัตรตามหลักสูตรที่สอดคล้องกับ สคส กำหนด หรือหลักสูตรสากล หรือมีมาตรฐานสากล

หลักฐาน: 1) หลักฐานการฝึกอบรม หลักสูตรการคุ้มครองข้อมูลส่วนบุคคลของ DPO
2) วุฒิบัตรการฝึกอบรม หรือประกาศนียบัตรหลักสูตรการคุ้มครองข้อมูลส่วนบุคคลของ

DPO

สภาพบังคับ: ไม่มีกฎหมายกำหนด

หลักฐานการฝึกอบรมหลักสูตรการคุ้มครองข้อมูลส่วนบุคคลของ DPO

บริษัท ตัวอย่าง จำกัด

บันทึกข้อความเลขที่: บค-2025/09

วันที่: 10 กรกฎาคม 2568

เรื่อง: รายงานการเข้าร่วมอบรมหลักสูตรการคุ้มครองข้อมูลส่วนบุคคลของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เรียน: ผู้บริหารบริษัท

ตามที่บริษัท ตัวอย่าง จำกัด ได้แต่งตั้ง นาง ด.ดวงดี ใจดี เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) นาง ด.ดวงดี ได้เข้าร่วมอบรมหลักสูตร “การคุ้มครองข้อมูลส่วนบุคคลและแนวทางปฏิบัติสำหรับเจ้าหน้าที่ DPO” ซึ่งจัดโดย สถาบันฝึกอบรมเทคโนโลยีสารสนเทศแห่งชาติ ระหว่างวันที่ 1-3 กรกฎาคม 2568 โดยมีรายละเอียดดังนี้

เนื้อหาหลักสูตร: กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA), แนวทางปฏิบัติ, การบริหารความเสี่ยง, การจัดการเหตุละเมิดข้อมูล

จำนวนชั่วโมงอบรม: 24 ชั่วโมง

ผู้เข้าอบรม: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจากองค์กรภาครัฐและเอกชน

บริษัทฯ ขอรายงานให้ทราบเพื่อประกอบการพิจารณาและการจัดทำหลักฐานในระบบบริหารความปลอดภัยข้อมูล

ลงชื่อ:

(นาย A)

กรรมการผู้จัดการ

ตัวอย่าง วุฒิบัตรการฝึกอบรมหรือประกาศนียบัตรหลักสูตรการคุ้มครองข้อมูลส่วนบุคคลของ DPO

ประกาศนียบัตร

ออกให้แก่ นาง ด.ดวงดี ใจดี

เนื่องด้วยได้ผ่านการอบรมหลักสูตร “การคุ้มครองข้อมูลส่วนบุคคลและแนวทางปฏิบัติสำหรับเจ้าหน้าที่ DPO” ซึ่งจัดโดย สถาบันฝึกอบรมเทคโนโลยีสารสนเทศแห่งชาติ

ระหว่างวันที่ 1-3 กรกฎาคม 2568

ได้รับคะแนนผ่านเกณฑ์มาตรฐานและได้รับประกาศนียบัตรฉบับนี้เพื่อแสดงถึงความรู้ความสามารถในการปฏิบัติหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

วันที่ออกประกาศนียบัตร: 5 กรกฎาคม 2568

(ลายเซ็นผู้รับรอง)

(นาง ส.สมศรี)

ผู้อำนวยการสถาบันฝึกอบรมเทคโนโลยีสารสนเทศแห่งชาติ

1.2.4 หากองค์กรไม่ต้องแต่งตั้ง DPO ต้องบันทึกการตัดสินใจหรือเหตุผลไว้ให้ตรวจสอบ

สิ่งที่ต้องทำ: บันทึกการตัดสินใจหรือเหตุผลว่าทำไมไม่ตั้ง DPO ซึ่งควรเป็นเหตุผลที่เป็นข้อยกเว้นของกฎหมายให้อำนาจ

หลักฐาน: 1) บันทึกการตัดสินใจ (อาจมีกฎหมายประกอบ หรือข้อหารือฝ่ายกฎหมาย)

2) การบันทึกรายการกิจกรรมการประมวลผลฯ หรือ ROPA

สภาพบังคับ: ไม่มีกฎหมายกำหนด

บันทึกการตัดสินใจไม่แต่งตั้ง DPO

บริษัท ตัวอย่าง จำกัด

บันทึกข้อความเลขที่: บค-2025/10

วันที่: 12 กรกฎาคม 2568

เรื่อง: บันทึกการตัดสินใจไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ตามที่บริษัท ตัวอย่าง จำกัด ได้พิจารณาเรื่องการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) เพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และข้อกฎหมายที่เกี่ยวข้อง

โดยจากการพิจารณา พบว่าองค์กรมีลักษณะดังนี้

- ขนาดองค์กรไม่ถึงเกณฑ์ที่กฎหมายกำหนดให้แต่งตั้ง DPO

- ปริมาณและประเภทข้อมูลส่วนบุคคลที่ประมวลผลอยู่ในระดับจำกัด
- มีมาตรการรักษาความปลอดภัยข้อมูลอย่างเหมาะสมและครบถ้วน

ดังนั้น บริษัทฯ จึงมีมติไม่ดำเนินการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ในขณะนี้ โดยจะมีการทบทวนและประเมินสถานการณ์อย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงในอนาคต

การตัดสินใจครั้งนี้ได้รับคำปรึกษาจากฝ่ายกฎหมายและอ้างอิงตามข้อยกเว้นที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

ลงชื่อ:

(นาย A)

กรรมการผู้จัดการ

บันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA)

บริษัท ตัวอย่าง จำกัด

บันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA)

วันที่บันทึก: 12 กรกฎาคม 2568

ลำดับ	ข้อมูลส่วนบุคคลที่เก็บรวบรวม	วัตถุประสงค์ของการเก็บรวบรวมข้อมูล	ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล	ระยะเวลาการเก็บรักษาข้อมูล	สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล และเงื่อนไขการเข้าถึง	การใช้หรือเปิดเผยข้อมูลตามมาตรา 27 วรรคสาม	การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30,31,32,36	คำอธิบายมาตรการรักษาความมั่นคงปลอดภัยข้อมูลตามมาตรา 37
1	ชื่อ, ที่อยู่, เบอร์โทรศัพท์, อีเมล	ให้บริการลูกค้า	บริษัท ตัวอย่าง จำกัด ฝ่ายบริการลูกค้า	5 ปี หลังเลิกใช้บริการ	เจ้าของข้อมูลสามารถขอแก้ไขข้อมูลผ่านฝ่ายบริการลูกค้าได้	ใช้เฉพาะภายในบริษัท เพื่อให้บริการลูกค้า	มีสิทธิยื่นคัดค้านการใช้ข้อมูลตามกฎหมาย	เข้ารหัสข้อมูล จำกัด สิทธิเข้าถึงผ่านระบบล็อกอิน
2	ข้อมูลส่วนตัวพนักงาน, ประวัติการทำงาน	บริหารงานบุคคล	บริษัท ตัวอย่าง จำกัด ฝ่ายทรัพยากรบุคคล	ตลอดเวลาที่ทำงาน	พนักงานสามารถเข้าถึงข้อมูลส่วนตัวได้ตามสิทธิที่กำหนด	ใช้สำหรับบริหารงานบุคคลและสวัสดิการ	มีสิทธิยื่นคำร้องปฏิเสธการใช้ข้อมูลที่ไม่ถูกต้อง	ระบบล็อกอิน 2 ชั้น ตรวจสอบบันทึกการเข้าใช้งาน

บริษัทฯ ได้ดำเนินการบันทึกและตรวจสอบกิจกรรมการประมวลผลข้อมูลส่วนบุคคลอย่างเคร่งครัดและสม่ำเสมอ เพื่อให้มั่นใจว่าการดำเนินงานเป็นไปตามข้อกำหนดของกฎหมายและนโยบายภายใน

ลงชื่อ:

(นาง B)

เจ้าหน้าที่ความปลอดภัยข้อมูล (Data Security Officer)

1.2.5 หากองค์กรไม่ต้องแต่งตั้ง DPO มอบหมายความรับผิดชอบให้บุคคลหนึ่งปฏิบัติหน้าที่แทน และองค์กรมีพนักงานและทรัพยากรเพียงพอที่จะดำเนินการต่าง ๆ ในการคุ้มครองข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: จัดให้มีพนักงานรับผิดชอบด้าน PDPA และสนับสนุนทรัพยากร

หลักฐาน: 1) รายงานการประชุมของ กก.บริษัท หรือผู้บริหารฯ ว่าตั้งบุคคลหนึ่งบุคคลใด หรือ คณะกรรมการ หรือ

2) หลักฐานการแต่งตั้งหรือมอบหมาย

3) ภาพถ่ายอุปกรณ์หรือเครื่องมือที่องค์กรสนับสนุนหรือจัดหาให้

สภาพบังคับ: ไม่มีกฎหมายกำหนด

รายงานการประชุมผู้บริหาร

บริษัท ตัวอย่าง จำกัด

วันที่: 15 กรกฎาคม 2568

เรื่อง: การแต่งตั้งบุคคลรับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) แทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ในการประชุมผู้บริหารครั้งที่ 7/2568 ได้มีการพิจารณาและมีมติเห็นชอบแต่งตั้ง นายสมชาย ใจดี เป็นผู้รับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) แทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยมอบหมายให้ดำเนินการตามข้อกำหนดของ PDPA พร้อมทั้งสนับสนุนทรัพยากรและอุปกรณ์ที่จำเป็นในการปฏิบัติงานอย่างเต็มที่

ผู้บริหารทุกท่านรับทราบและเห็นชอบตามมติที่ประชุมนี้

ลงชื่อ.....

(นายกิตติ พิทักษ์ธรรม)

ประธานกรรมการบริหาร

ตัวอย่าง หนังสือแต่งตั้ง/มอบหมายงาน

บริษัท ตัวอย่าง จำกัด

บันทึกข้อความเลขที่: 0123/2568

วันที่: 15 กรกฎาคม 2568

เรื่อง: การแต่งตั้งผู้รับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) แทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ตามที่บริษัท ตัวอย่าง จำกัด มีความประสงค์ให้บุคคลรับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) บริษัทฯ จึงแต่งตั้ง

นายสมชาย ใจดี

ตำแหน่ง: ผู้จัดการฝ่ายไอที

ให้เป็นผู้รับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) แทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยมีหน้าที่รับผิดชอบตามที่กฎหมายกำหนด พร้อมทั้งสนับสนุนทรัพยากรและอุปกรณ์ที่จำเป็นในการปฏิบัติงาน

จึงเรียนมาเพื่อโปรดทราบและดำเนินการต่อไป

ลงชื่อ.....

(นายกิตติ พิทักษ์ธรรม)

ประธานกรรมการบริหาร

ภาพถ่ายอุปกรณ์และเครื่องมือสนับสนุนสำหรับผู้รับผิดชอบ PDPA

ภาพถ่ายคอมพิวเตอร์สำนักงานที่จัดไว้สำหรับผู้รับผิดชอบด้าน PDPA

ภาพถ่ายโทรศัพท์มือถือที่บริษัทจัดให้ใช้ในการติดต่อประสานงานด้านข้อมูลส่วนบุคคล

ภาพถ่ายซอฟต์แวร์ระบบบริหารจัดการข้อมูล (Data Management System) ที่ได้รับการติดตั้งเพื่อสนับสนุนงาน PDPA

1.3.1 สมาชิกในองค์กรทราบดีว่า DPO คือใคร มีหน้าที่อะไร จะติดต่ออย่างไร

สิ่งที่ต้องทำ: แจกจ่ายรายละเอียดครบถ้วน

- หลักฐาน:
- 1) ทำเอกสารรายละเอียดเกี่ยวกับ DPO ได้แก่ ชื่อ หน้าที่ ความรับผิดชอบ ช่องทางการติดต่อให้ปรากฏอยู่ในเอกสารดังนี้
 - ก) รายงานการประชุมของคณะกรรมการองค์กร หรือผู้บริหาร หรือ กก.กำกับฯ
 - 3) ประกาศ หรือเผยแพร่คำสั่งแต่งตั้ง DPO หรืออาจทำหนังสือเวียน

สภาพบังคับ:

- 1) มาตรา 37(1) และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลฯ ข้อ 4(2)(7)
- 2) มีโทษทางปกครองตามมาตรา 37 โทษปรับทางปกครองไม่เกิน 3 ล้าน

ตัวอย่าง รายงานการประชุมคณะกรรมการองค์กร/ผู้บริหาร

บริษัท ตัวอย่าง จำกัด

วันที่: 20 กรกฎาคม 2568

เรื่อง: แจ้งแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และหน้าที่รับผิดชอบ

ที่ประชุมคณะกรรมการบริษัทได้พิจารณาและมีมติแต่งตั้ง

นางสาวปรียา สมใจ

ตำแหน่ง: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

โดยมีหน้าที่ความรับผิดชอบหลักดังนี้

- ดูแลและควบคุมการปฏิบัติตาม PDPA ภายในองค์กร
- ให้คำปรึกษาและแนะแนวทางการคุ้มครองข้อมูลส่วนบุคคลแก่พนักงานเป็นจุดติดต่อหลักสำหรับเจ้าของข้อมูลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ช่องทางติดต่อ

โทรศัพท์: 0x-xxx-xxxx

อีเมล: DPO@example.com

ผู้บริหารรับทราบและเห็นชอบการแต่งตั้งนี้ เพื่อให้เกิดความชัดเจนและเป็นไปตามข้อกำหนด

ลงชื่อ.....

(นายกิตติ พิทักษ์ธรรม)

ประธานกรรมการบริหาร

ประกาศ

บริษัท ตัวอย่าง จำกัด

บันทึกข้อความเลขที่: 045/2568

วันที่: 20 กรกฎาคม 2568

เรื่อง: แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

ตามที่บริษัท ตัวอย่าง จำกัด มีความมุ่งมั่นในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และเพื่อให้เกิดการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรอย่างเคร่งครัดและมีประสิทธิภาพ บริษัทฯ จึงแต่งตั้ง

นางสาวปรียา สมใจ

ดำรงตำแหน่ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

โดยมีอำนาจหน้าที่ความรับผิดชอบ ดังนี้

1. เป็นผู้ดูแลและควบคุมการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้อง รวมถึงแนวทางปฏิบัติที่สอดคล้องกับมาตรฐานสากล
2. ให้คำปรึกษาและแนะแนวทางการประมวลผลข้อมูลส่วนบุคคลแก่พนักงานและหน่วยงานต่าง ๆ ภายในองค์กร เพื่อให้เป็นไปตามหลักเกณฑ์และมาตรฐานที่กำหนด
3. ตรวจสอบและติดตามกิจกรรมการประมวลผลข้อมูลส่วนบุคคล รวมถึงการจัดทำและบำรุงรักษาบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) ตามมาตรา 39 แห่ง PDPA
4. เป็นจุดติดต่อหลักสำหรับเจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ในการแจ้งคำร้อง การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล และประสานงานในกรณีที่เกี่ยวข้อง
5. ประสานงานกับฝ่ายกฎหมายและฝ่ายความมั่นคงปลอดภัยข้อมูล เพื่อวางแผนและจัดทำมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เหมาะสม
6. จัดฝึกอบรมและเผยแพร่ความรู้เกี่ยวกับ PDPA และการคุ้มครองข้อมูลส่วนบุคคลแก่พนักงานในองค์กร
7. รับผิดชอบในการรายงานผลการดำเนินงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลต่อผู้บริหารหรือคณะกรรมการองค์กรเป็นประจำ
8. มีประกาศนียบัตรหรือวุฒิบัตรที่สอดคล้องกับหลักสูตรที่ สคส. หรือมาตรฐานสากลกำหนด เพื่อยืนยันความรู้และความเชี่ยวชาญในการปฏิบัติงาน

ช่องทางการติดต่อ

โทรศัพท์: 0x-xxx-xxxx

อีเมล: DPO@example.com

ประกาศ ณ วันที่ 20 กรกฎาคม 2568

ลงชื่อ.....

(นายกิตติ พิทักษ์ธรรม)

กรรมการผู้จัดการ

หนังสือเวียนแจ้งให้พนักงานทราบเกี่ยวกับ DPO

บริษัท ตัวอย่าง จำกัด

วันที่: 20 กรกฎาคม 2568

เรื่อง: แจ้งแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และช่องทางการติดต่อ

เรียน พนักงานทุกท่าน

ด้วยบริษัท ตัวอย่าง จำกัด ได้แต่งตั้ง

นางสาวปรียา สมใจ

ดำรงตำแหน่ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) เพื่อดูแลและรับผิดชอบการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

หากพนักงานท่านใดมีข้อสงสัย หรือต้องการคำปรึกษาเกี่ยวกับการปฏิบัติตาม PDPA หรือต้องการแจ้งปัญหาการคุ้มครองข้อมูลส่วนบุคคล สามารถติดต่อ DPO ได้ที่

โทรศัพท์: 0x-xxx-xxxx

อีเมล: DPO@example.com

ขอความร่วมมือพนักงานทุกท่านรับทราบและปฏิบัติตามอย่างเคร่งครัด

ขอขอบคุณครับ/ค่ะ

ลงชื่อ.....

(ฝ่ายบุคคล)

1.3.2 DPO มีส่วนร่วมในการให้ความเห็นทุกประเด็นที่เกี่ยวข้องกับ PDPA ในเวลาที่เหมาะสม

สิ่งที่ต้องทำ: ต้องจัดการให้ DPO ร่วมให้ความเห็นทุกเรื่องที่มีความสำคัญ

หลักฐาน: 1) รายงานการประชุมในระดับฝ่าย หรือ

ก) จัดให้มีระบบหรือและใช้หนังสือ หรืออีเมล หรือ App ตอบโต้ข้อหารือ DPO เป็น

หลักฐาน

สภาพบังคับ: 1) มาตรา 42 วรรคแรก

ตัวอย่างรายงานการประชุมฝ่ายบริหารเรื่อง PDPA

บริษัท ตัวอย่าง จำกัด

รายงานการประชุมฝ่ายบริหารครั้งที่ 5/2568

วันที่ 25 กรกฎาคม 2568

เรื่อง: การพิจารณาและรับฟังความคิดเห็นเกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

ผู้เข้าร่วมประชุม:

- นายกิตติ พิทักษ์ธรรม (กรรมการผู้จัดการ)
- นางสาวปรียา สมใจ (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล – DPO)
- หัวหน้าฝ่ายทรัพยากรบุคคล
- หัวหน้าฝ่ายไอที

เนื้อหาการประชุม:

1. พิจารณานโยบายและมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล
2. รับฟังความคิดเห็นและข้อเสนอแนะจาก DPO เกี่ยวกับแนวทางปฏิบัติในการประมวลผลข้อมูล
3. ทบทวนความคืบหน้าการจัดทำบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA)
- 4.หารือเกี่ยวกับคำร้องขอใช้สิทธิของเจ้าของข้อมูล

สรุปผล:

DPO ได้ให้ความเห็นและข้อเสนอแนะอย่างครบถ้วนในทุกประเด็นที่เกี่ยวข้อง โดยเสนอแนะแนวทางการปรับปรุงมาตรการรักษาความปลอดภัยและการจัดทำเอกสารที่เกี่ยวข้อง เพื่อให้สอดคล้องกับข้อกำหนดใน PDPA

ลงชื่อ.....

(นายกิตติ พิทักษ์ธรรม)

ประธานที่ประชุม

ตัวอย่างระบบการหารือและตอบข้อซักถามผ่านอีเมล

ระบบหารือเรื่อง PDPA ผ่านอีเมล

หัวข้อ: ขอคำแนะนำเรื่องการจัดเก็บข้อมูลส่วนบุคคลของลูกค้าใหม่

ผู้ส่ง: หัวหน้าฝ่ายการตลาด

ผู้รับ: DPO@example.com (นางสาวปรียา สมใจ - DPO)

วันที่: 30 กรกฎาคม 2568

เนื้อหาอีเมล:

เรียน DPO ฝ่ายการตลาดขอคำแนะนำเกี่ยวกับแนวทางการจัดเก็บข้อมูลส่วนบุคคลของลูกค้าใหม่ เพื่อให้เป็นไปตาม PDPA โดยเฉพาะเรื่องระยะเวลาเก็บรักษาข้อมูลและมาตรการความปลอดภัย

ขอขอบคุณล่วงหน้าสำหรับคำแนะนำครับ/ค่ะ

คำตอบจาก DPO:

เรียน หัวหน้าฝ่ายการตลาด, ตามที่สอบถามมา การเก็บข้อมูลลูกค้าใหม่ควรจัดเก็บเฉพาะข้อมูลที่จำเป็น และกำหนดระยะเวลาการเก็บรักษาไม่เกิน 5 ปี นับจากวันสุดท้ายที่มีการติดต่อกับลูกค้า พร้อมทั้งใช้มาตรการรักษาความปลอดภัย เช่น การเข้ารหัสข้อมูลและจำกัดสิทธิ์เข้าถึง เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

หากต้องการรายละเอียดเพิ่มเติมสามารถติดต่อได้ครับ/ค่ะ

ขอแสดงความนับถือ

ลงชื่อ.....

นางสาวปรียา สมใจ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

1.3.3 DPO ปฏิบัติหน้าที่อย่างเป็นอิสระ โดยไม่มีผลประโยชน์ทับซ้อน และมีส่วนร่วมตัดสินใจโดยตรงเกี่ยวกับลักษณะและวัตถุประสงค์ของการประมวลผลในองค์กร

สิ่งที่ต้องทำ: ต้องจัดการให้ DPO ทำงานอย่างอิสระ และไม่มีผลประโยชน์ทับซ้อน

หลักฐาน:

- 1) เอกสารที่แสดงให้เห็นว่า DPO ตัดสินใจได้โดยอิสระ และเอกสารต้องแสดงให้เห็นว่า DPO สามารถแนะนำโดยตรงต่อผู้บริหารระดับสูง และแจ้งข้อกังวลได้ อาจอยู่ในรูปเอกสาร
 - รายงานการประชุมของ กก. บริหารขององค์กร หรือ กก.กำกับฯ หรือ
 - นโยบายที่เขียนชัดว่า DPO มีอิสระโดยไม่มีผลประโยชน์ทับซ้อน หรือ
 - สัญญาระบุชัดว่าให้ DPO เข้ามาทำงานโดยมีอิสระโดยไม่มีผลประโยชน์ทับซ้อน

สภาพบังคับ: 1) มาตรา 42 วรรคแรก

2) โทษทางปกครองมาตรา 82 ปรับไม่เกิน 1 ล้านบาท

ตัวอย่างรายงานการประชุมคณะกรรมการบริหาร (บอร์ด)

บริษัท ตัวอย่าง จำกัด
รายงานการประชุมคณะกรรมการบริหาร
ครั้งที่ 8/2568
วันที่ 5 สิงหาคม 2568

เรื่อง: การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และการกำหนดอำนาจหน้าที่

ผู้เข้าร่วมประชุม:

- นายสมชาย จงรักภักดี (ประธานกรรมการ)
- นางสาวปรีญา สมใจ (เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - DPO)
- กรรมการบริหารท่านอื่น ๆ

เนื้อหาการประชุม:

- รับรองการแต่งตั้ง DPO
- กำหนดบทบาทและอำนาจของ DPO ให้ทำงานอย่างอิสระ ไม่มีผลประโยชน์ทับซ้อน
- กำหนดให้ DPO มีสิทธิ์เข้าถึงข้อมูล และสามารถแนะนำ แจ้งข้อกังวลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยตรงต่อคณะกรรมการบริหาร

มติที่ประชุม:

คณะกรรมการบริหารรับรองให้ DPO ปฏิบัติหน้าที่อย่างเป็นอิสระ และไม่มีผลประโยชน์ทับซ้อน โดย DPO มีอำนาจให้ความเห็นและแจ้งข้อกังวลได้โดยตรงต่อผู้บริหารระดับสูงโดยไม่ถูกแทรกแซง

ลงชื่อ.....

(นายสมชาย จงรักภักดี)

ประธานกรรมการ

ตัวอย่างนโยบายองค์กร (Policy) เรื่องความเป็นอิสระของ DPO

นโยบายความเป็นอิสระและหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

บริษัท ตัวอย่าง จำกัด ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลโดยแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อทำหน้าที่ควบคุมดูแลการปฏิบัติตาม PDPA อย่างเป็นอิสระ

หลักการ:

1. DPO ต้องดำเนินงานโดยไม่มีผลประโยชน์ทับซ้อน และไม่อยู่ภายใต้คำสั่งของฝ่ายใดที่อาจขัดแย้งกับบทบาทของตน
 2. DPO มีสิทธิให้คำแนะนำ แนะนำข้อปฏิบัติ แจ้งเตือนข้อกังวล และรายงานต่อผู้บริหารระดับสูงหรือคณะกรรมการบริหารโดยตรง
- บริษัทฯ สนับสนุนและจัดสรรทรัพยากรที่เหมาะสมให้แก่ DPO ในการปฏิบัติหน้าที่
- นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่ 1 สิงหาคม 2568 เป็นต้นไป

ตัวอย่างข้อความในสัญญาจ้างหรือแต่งตั้ง DPO

สัญญาจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ข้อ 3: ความเป็นอิสระในการปฏิบัติหน้าที่

ผู้ว่าจ้างตกลงและรับรองให้ผู้รับจ้างปฏิบัติหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยมีอิสระเต็มที่ในการปฏิบัติงาน และไม่มีผลประโยชน์ทับซ้อนในการให้คำแนะนำและควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคลผู้รับจ้างมีสิทธิรายงานข้อกังวลและข้อเสนอแนะโดยตรงต่อผู้บริหารระดับสูงและคณะกรรมการบริหารของบริษัทฯ โดยไม่ถูกแทรกแซงหรือขัดขวาง

ลงชื่อ.....

(ผู้ว่าจ้าง)

ลงชื่อ.....

(ผู้รับจ้าง – DPO)

1.3.4 DPO ให้คำแนะนำโดยตรงต่อผู้มีอำนาจตัดสินใจระดับสูงและแจ้งข้อกังวลกับผู้บริหารระดับสูงสุดได้

สิ่งที่ต้องทำ: ต้องมีช่องทาง หรือผังองค์กร หรือสายการบังคับบัญชาให้ DPO ให้คำแนะนำโดยตรงต่อผู้มีอำนาจตัดสินใจระดับสูงและแจ้งข้อกังวลกับผู้บริหารระดับสูงสุดได้

หลักฐาน: เอกสารที่แสดงให้เห็นว่า DPO ตัดสินใจได้โดยอิสระ และเอกสารต้องแสดงให้เห็นว่า DPO สามารถแนะนำโดยตรงต่อผู้บริหารระดับสูง และแจ้งข้อกังวลได้ อาจอยู่ในรูปเอกสาร

- รายงานการประชุมของ กก. บริหารขององค์กร หรือ กก.กำกับฯ หรือ
- นโยบายที่เขียนชัดว่า DPO มีอิสระโดยไม่มีผลประโยชน์ทับซ้อน หรือ
- สัญญาระบุชัดว่าให้ DPO เข้ามาทำงานโดยมีอิสระโดยไม่มีผลประโยชน์ทับซ้อน

สภาพบังคับ: 1) มาตรา 42 วรรคแรก

2) โทษทางปกครองมาตรา 82 ปรับไม่เกิน 1 ล้านบาท

รายงานการประชุมคณะกรรมการบริหาร (บอร์ด)

บริษัท ตัวอย่าง จำกัด

รายงานการประชุมคณะกรรมการบริหาร

ครั้งที่ 10/2568

วันที่ 20 กันยายน 2568

เรื่อง: การกำหนดบทบาทและสิทธิ์ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ในการให้คำแนะนำและ
แจ้งข้อกังวลต่อผู้บริหารระดับสูง

ผู้เข้าร่วมประชุม:

- นายสมชาย จงรักภักดี (ประธานกรรมการ)
- นางสาวปรีญา สมใจ (DPO)
- กรรมการบริหารท่านอื่น ๆ

เนื้อหาการประชุม:

1. กำหนดให้ DPO สามารถให้คำแนะนำโดยตรงต่อผู้บริหารระดับสูงและคณะกรรมการบริหาร
2. อนุมัติผังการบังคับบัญชาที่แสดงให้เห็นว่า DPO รายงานตรงต่อผู้บริหารระดับสูงสุด
3. ยืนยันความเป็นอิสระในการปฏิบัติหน้าที่ของ DPO โดยไม่มีผลประโยชน์ทับซ้อน

มติที่ประชุม:

คณะกรรมการบริหารรับรองบทบาทของ DPO ในการตัดสินใจและรายงานโดยตรงต่อผู้บริหาร
ระดับสูงสุด พร้อมรับรองให้อิสระเต็มที่ในการปฏิบัติหน้าที่

ลงชื่อ.....

(นายสมชาย จงรักภักดี)

ประธานกรรมการ

นโยบายองค์กร (Policy) เรื่องสิทธิและอำนาจของ DPO

นโยบายสิทธิและอำนาจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

บริษัท ตัวอย่าง จำกัด ให้ความสำคัญกับบทบาทของ DPO โดยกำหนดนโยบายดังนี้

1. DPO มีสิทธิและอำนาจในการให้คำแนะนำโดยตรงต่อผู้บริหารระดับสูงและคณะกรรมการบริหารองค์กร
 2. DPO สามารถแจ้งข้อกังวลหรือความเสี่ยงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยตรงแก่ผู้บริหารระดับสูงสุดได้โดยไม่มีข้อจำกัด
 3. บริษัทฯ สนับสนุนและรับรองความเป็นอิสระของ DPO ในการปฏิบัติหน้าที่ตามมาตรา 42 PDPA
- นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่ 1 กันยายน 2568 เป็นต้นไป

ข้อความในสัญญาจ้างหรือแต่งตั้ง DPO

สัญญาจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ข้อ 4: สิทธิและอำนาจในการรายงานและให้คำแนะนำ

ผู้ว่าจ้างตกลงให้ผู้รับจ้างในตำแหน่ง DPO มีสิทธิให้คำแนะนำและรายงานข้อกังวลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลโดยตรงต่อผู้บริหารระดับสูงสุดและคณะกรรมการบริหารขององค์กร โดยไม่มีข้อจำกัดหรือข้อกีดกันใด ๆ และต้องได้รับการสนับสนุนในการปฏิบัติงานอย่างอิสระตามมาตรา 42 ของ PDPA

ลงชื่อ.....

(ผู้ว่าจ้าง)

ลงชื่อ.....

(ผู้รับจ้าง - DPO)

1.3.5 องค์กรปฏิบัติตามคำแนะนำของ DPO ในฐานะผู้เชี่ยวชาญ หากไม่ดำเนินการต้องบันทึกไว้

- สิ่งที่ต้องทำ:
- 1) ต้องปฏิบัติตามคำแนะนำ
 - 2) ถ้าไม่ปฏิบัติตาม ต้องให้เหตุผลประกอบ

- หลักฐาน:
- 1) รายงานการประชุมของหัวหน้าฝ่าย
 - 2) หนังสือตอบโต้ อีเมล หรือ app ข้อหารือของ DPO กับฝ่ายงานในองค์กร

ทั้ง 2 ข้อ ต้องมีข้อความว่า “ได้ปฏิบัติตามคำแนะนำ” ซึ่งอาจมีบันทึกการรายงานผลการปฏิบัติงาน

สภาพบังคับ:

- 1) มาตรา 42 วรรคแรก
- 2) โทษทางปกครองมาตรา 82 ปรับไม่เกิน 1 ล้าน

ตัวอย่างรายงานการประชุมของหัวหน้าฝ่าย

บริษัท ตัวอย่าง จำกัด

รายงานการประชุมหัวหน้าฝ่าย

ครั้งที่ 5/2568

วันที่ 15 พฤษภาคม 2568

เรื่อง: การปฏิบัติตามคำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ผู้เข้าร่วมประชุม:

- นายวิทยา ศรีสุข (หัวหน้าฝ่ายไอที)
- นางสาวอรรทัย ใจดี (หัวหน้าฝ่ายทรัพยากรบุคคล)
- นายสมชาย จงรักภักดี (DPO)
- หัวหน้าฝ่ายอื่น ๆ

เนื้อหาการประชุม:

1. DPO เสนอคำแนะนำเกี่ยวกับการปรับปรุงระบบความปลอดภัยข้อมูล
2. ฝ่ายไอที รายงานว่า ได้ปฏิบัติตามคำแนะนำ โดยได้ติดตั้งระบบเข้ารหัสข้อมูลเพิ่มเติมตามที่

DPO แนะนำ

3. ฝ่ายทรัพยากรบุคคลแจ้งว่า ไม่ได้ปฏิบัติตามคำแนะนำ เนื่องจากข้อจำกัดทางงบประมาณและจัดทำหนังสือชี้แจงเหตุผลประกอบอย่างชัดเจน

มติที่ประชุม:

รับทราบการดำเนินการตามคำแนะนำของ DPO และเหตุการณ์ไม่ปฏิบัติตาม พร้อมติดตามผลในครั้งถัดไป

ลงชื่อ.....

(นายวิทยา ศรีสุข)

หัวหน้าฝ่ายไอที

ลงชื่อ.....

(นางสาวอรรทัย ใจดี)

หัวหน้าฝ่ายทรัพยากรบุคคล

ตัวอย่างหนังสือตอบโต้ / อีเมลล์ / ข้อความในแอป

เรื่อง: ตอบกลับคำแนะนำของ DPO เรื่องการปรับปรุงระบบข้อมูล

เรียน คุณสมชาย (DPO)

ตามที่ท่านได้ให้คำแนะนำเกี่ยวกับการเพิ่มมาตรการรักษาความปลอดภัยข้อมูลในระบบทรัพยากรบุคคลนั้น

ฝ่ายไอที ได้ปฏิบัติตามคำแนะนำ โดยติดตั้งระบบเข้ารหัสและอัปเดตซอฟต์แวร์เรียบร้อยแล้ว

ฝ่ายทรัพยากรบุคคล ไม่ได้ปฏิบัติตามคำแนะนำ เนื่องจากข้อจำกัดทางงบประมาณในไตรมาสนี้ แต่จะจัดทำแผนดำเนินการในไตรมาสถัดไปและรายงานผลอีกครั้ง

จึงเรียนมาเพื่อทราบและติดตาม

ขอแสดงความนับถือ

ลงชื่อ.....

(นายวิทยา ศรีสุข)

หัวหน้าฝ่ายไอที

1.3.5 องค์การปฏิบัติตามคำแนะนำของ DPO ในฐานะผู้เชี่ยวชาญฯ หากไม่ดำเนินการต้องบันทึกไว้

- สิ่งที่ต้องทำ:
- 1) ต้องปฏิบัติตามคำแนะนำ
 - 2) ถ้าไม่ปฏิบัติตาม ต้องให้เหตุผลประกอบ

- หลักฐาน:
- 1) รายงานการประชุมของหัวหน้าฝ่าย
 - 2) หนังสือตอบโต้ อีเมลล์ หรือ app ข้อหารือของ DPO กับฝ่ายงานในองค์กร
- ทั้ง 2 ข้อ ต้องมีข้อความว่า “ได้ปฏิบัติตามคำแนะนำ” ซึ่งอาจมีบันทึกการรายงานผลการปฏิบัติงาน หรือถ้าไม่เห็นด้วยอาจมีบันทึกว่าเพราะเหตุใด โดยอาจมีเอกสารอื่นประกอบ เช่น ข้อหารือของ สคส หรือข้อโต้แย้งฝ่ายกฎหมาย แล้วทำบันทึกไว้

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างรายงานการประชุมของหัวหน้าฝ่าย

บริษัท ตัวอย่าง จำกัด

รายงานการประชุมหัวหน้าฝ่าย

ครั้งที่ 8/2568

วันที่ 2 มิถุนายน 2568

เรื่อง: การปฏิบัติตามคำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ผู้เข้าร่วมประชุม:

- นางสาวอรรทัย ใจดี (หัวหน้าฝ่ายทรัพยากรบุคคล)
- นายวิทยา ศรีสุข (หัวหน้าฝ่ายไอที)
- นายสมชาย จงรักภักดี (DPO)

เนื้อหาการประชุม:

1. DPO ให้คำแนะนำเรื่องการปรับปรุงกระบวนการจัดการข้อมูลส่วนบุคคลในระบบบุคลากร
2. ฝ่ายทรัพยากรบุคคลรายงานว่า ได้ปฏิบัติตามคำแนะนำ โดยแก้ไขแบบฟอร์มเก็บข้อมูลและ
เพิ่มขึ้นตอนตรวจสอบความถูกต้องของข้อมูล
3. ฝ่ายไอทีแจ้งว่า ไม่ได้ปฏิบัติตามคำแนะนำ เนื่องจากมีข้อจำกัดทางเทคนิคและงบประมาณ จึง
เสนอให้เลื่อนการดำเนินการออกไป พร้อมระบุเหตุผลประกอบอย่างละเอียด

มติที่ประชุม:

1. รับทราบการดำเนินงานและเหตุผลการไม่ปฏิบัติตามคำแนะนำในส่วนที่เกี่ยวข้อง
2. กำหนดติดตามผลในประชุมครั้งถัดไป

ลงชื่อ.....

(นางสาวอรรทัย ใจดี)

หัวหน้าฝ่ายทรัพยากรบุคคล

ลงชื่อ.....

(นายวิทยา ศรีสุข)

หัวหน้าฝ่ายไอที

ตัวอย่างหนังสือตอบโต้ / อีเมล / ข้อความในแอป

เรื่อง: ตอบกลับคำแนะนำของ DPO เรื่องการปรับปรุงกระบวนการจัดการข้อมูลส่วนบุคคล

เรียน คุณสมชาย (DPO)

ตามที่ท่านได้ให้คำแนะนำในการปรับปรุงกระบวนการจัดการข้อมูลส่วนบุคคลของฝ่ายไอทีและฝ่ายทรัพยากรบุคคลนั้น

1. ฝ่ายทรัพยากรบุคคล ได้ปฏิบัติตามคำแนะนำ โดยอัปเดตแบบฟอร์มและเพิ่มขั้นตอนตรวจสอบความถูกต้องของข้อมูลตามที่แนะนำ
2. ฝ่ายไอที ไม่ได้ปฏิบัติตามคำแนะนำ เนื่องจากข้อจำกัดทางเทคนิคและงบประมาณในไตรมาสนี้ โดยฝ่ายไอทีได้ส่งเอกสารประกอบข้อจำกัดและข้อเสนอแผนดำเนินการในอนาคตแนบมาพร้อมนี้ จึงเรียนมาเพื่อทราบและพิจารณา

ขอแสดงความนับถือ

ลงชื่อ.....

(นายวิทยา ศรีสุข)

หัวหน้าฝ่ายไอที

1.3.6 DPO ให้ข้อมูลที่เป็นปัจจุบันแก่ผู้บริหารระดับสูงเป็นประจำเกี่ยวกับกฎหมายและการดำเนินการด้าน PDPA

สิ่งที่ต้องทำ: ต้องมีระบบการรายงานข้อมูลต่อผู้บริหารระดับสูง อย่างน้อยปีละ 1 ครั้ง

หลักฐาน: 1) รายงานการประชุม กก.บริษัท หรือองค์กร หรือ กก.กำกับดูแลด้าน PDPA หรือ
2) หนังสือหรือบันทึกของ DPO ที่จัดทำรายงานต่อผู้บริหาร

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างรายงานการประชุมคณะกรรมการบริษัท (กก.บริษัท)

บริษัท ตัวอย่าง จำกัด

รายงานการประชุมคณะกรรมการบริษัท

ครั้งที่ 4/2568

วันที่ 15 เมษายน 2568

เรื่อง: รายงานความคืบหน้าการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

ผู้เข้าร่วมประชุม:

- ประธานกรรมการ
- กรรมการผู้จัดการ
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) นายสมชาย จงรักภักดี
- กรรมการและผู้บริหารระดับสูง

เนื้อหาการประชุม:

1. DPO รายงานข้อมูลที่เป็นปัจจุบันเกี่ยวกับกฎหมาย PDPA และแนวทางปฏิบัติตามมาตรฐานของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
2. รายงานผลการดำเนินงานและความท้าทายในการคุ้มครองข้อมูลส่วนบุคคลในองค์กร
3. มีการอภิปรายและเสนอแนะแนวทางพัฒนาการจัดการข้อมูลส่วนบุคคลในปีถัดไป

มติที่ประชุม:

1. รับทราบรายงานของ DPO และมอบหมายให้ฝ่ายที่เกี่ยวข้องเร่งดำเนินการตามข้อเสนอแนะกำหนดให้ DPO รายงานความคืบหน้าการดำเนินงานด้าน PDPA ต่อที่ประชุมกรรมการอย่างน้อยปีละ 1 ครั้ง

ลงชื่อ.....

(ประธานกรรมการบริษัท)

ตัวอย่างหนังสือรายงานของ DPO ต่อผู้บริหารระดับสูง

บริษัท ตัวอย่าง จำกัด

บันทึกข้อความ

วันที่ 10 เมษายน 2568

เรื่อง: รายงานสถานะและความคืบหน้าการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

เรียน ผู้บริหารระดับสูง

ตามที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของบริษัทฯ ข้าพเจ้าขอรายงานสถานะและความคืบหน้าการดำเนินงานด้าน PDPA ดังนี้

1. สถานะการปฏิบัติตามกฎหมาย PDPA ปัจจุบันบริษัทฯ อยู่ระหว่างการปรับปรุงนโยบายและขั้นตอนการจัดการข้อมูลส่วนบุคคลให้เป็นไปตามข้อกำหนดของกฎหมาย
 2. ผลการตรวจสอบและประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลในไตรมาสที่ผ่านมา
 3. การอบรมและสร้างความตระหนักรู้ให้พนักงานในเรื่อง PDPA
 4. ปัญหาและข้อเสนอแนะเพื่อการปรับปรุงระบบคุ้มครองข้อมูลส่วนบุคคล
- จึงเรียนมาเพื่อทราบและพิจารณา

ลงชื่อ.....

(นายสมชาย จงรักภักดี)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

11.4.1 จบท ที่ปฏิบัติงานเกี่ยวกับ PDPA และกำกับข้อมูล จัดการและดูแลข้อมูลอย่างมีประสิทธิภาพ และรักษาความปลอดภัยฯ อย่างเหมาะสม

สิ่งที่ต้องทำ: ต้องดำเนินการให้จบท ที่ปฏิบัติงานเกี่ยวกับ PDPA และกำกับข้อมูล จัดการและดูแลข้อมูลอย่างมีประสิทธิภาพ และรักษาความปลอดภัยฯ อย่างเหมาะสม

หลักฐาน: 1) รายงานการประชุม กก.บริษัท หรือองค์กร หรือ กก.กำกับดูแลด้าน PDPA หรือ
2) นโยบาย ประกาศ คำสั่ง แนวปฏิบัติที่ระบุถึงมาตรการรักษาความมั่นคงปลอดภัยฯ เอกสารนี้ต้องระบุให้เห็นว่า “มีมาตรการรักษาความมั่นคงปลอดภัยฯ สำหรับพนักงานทุกด้าน”

สภาพบังคับ: 1) มาตรา 37, 40
2) มีโทษทางปกครองมาตรา 83 กรณีไม่ปฏิบัติตาม ม. 37 ปรับไม่เกิน 3 ล้านบาท และโทษทางปกครองมาตรา 84 กรณีไม่ปฏิบัติตาม ม. 40 ปรับไม่เกิน 3 ล้านบาท

ตัวอย่างรายงานการประชุมคณะกรรมการบริษัท (กก.บริษัท)

บริษัท ตัวอย่าง จำกัด

รายงานการประชุมคณะกรรมการบริษัท

ครั้งที่ 5/2568

วันที่ 20 เมษายน 2568

เรื่อง: มาตรการและการกำกับดูแลการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (PDPA)

ผู้เข้าร่วมประชุม:

- ประธานกรรมการ
- กรรมการผู้จัดการ
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) นายสมชาย จงรักภักดี
- กรรมการและผู้บริหารระดับสูง

เนื้อหาการประชุม:

1. รายงานมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่ดำเนินการกับเจ้าหน้าที่ที่เกี่ยวข้องทุกฝ่าย
2. ย้ำความสำคัญของการจัดการและดูแลข้อมูลอย่างมีประสิทธิภาพและปลอดภัยตามกฎหมาย PDPA
3. แนวทางการอบรมพนักงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยข้อมูล

มติที่ประชุม:

1. อนุมัตินโยบายและมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลสำหรับพนักงานทุกด้านอย่างเคร่งครัด
2. กำหนดให้มีการตรวจสอบและประเมินผลความปลอดภัยของระบบข้อมูลอย่างสม่ำเสมอ

ลงชื่อ.....

(ประธานกรรมการบริษัท)

นโยบายรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Data Security Policy)

บริษัท ตัวอย่าง จำกัด

ประกาศ ณ วันที่ 1 มกราคม 2568

วัตถุประสงค์

บริษัทฯ มีความมุ่งมั่นที่จะปกป้องและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ได้รับการเก็บรวบรวม ใช้ และจัดเก็บ เพื่อป้องกันการเข้าถึง การเปิดเผย การเปลี่ยนแปลง หรือการทำลายข้อมูลโดยไม่ได้รับอนุญาต ตามที่กฎหมาย PDPA กำหนด

ขอบเขต

นโยบายนี้ใช้บังคับกับข้อมูลส่วนบุคคลทั้งหมดที่บริษัทฯ ดำเนินการ รวมทั้งบุคลากรทุกคน ทั้งพนักงานประจำ ผู้รับเหมา และบุคคลภายนอกที่ได้รับมอบหมาย

ข้อกำหนดและมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

การกำหนดบทบาทและความรับผิดชอบ

1. กำหนดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) รับผิดชอบดูแลและกำกับการรักษาความปลอดภัยข้อมูล
2. บุคลากรทุกคนต้องรับผิดชอบในการรักษาความปลอดภัยข้อมูลในส่วนที่เกี่ยวข้อง

มาตรการทางเทคนิค

1. ใช้ระบบป้องกันไวรัสและมัลแวร์ที่ได้รับการอัปเดตอย่างสม่ำเสมอ
2. ใช้ระบบไฟร์วอลล์และระบบควบคุมการเข้าถึงเครือข่ายอย่างเข้มงวด
3. กำหนดรหัสผ่านที่มีความซับซ้อนและเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด
4. เข้ารหัสข้อมูลสำคัญทั้งในขณะจัดเก็บและขณะส่งข้อมูล
5. มีระบบสำรองข้อมูล (Backup) และแผนการกู้คืนข้อมูล (Disaster Recovery Plan)

มาตรการทางการบริหาร

1. ฝึกอบรมและสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยข้อมูลให้กับพนักงานทุกระดับอย่างสม่ำเสมอ
2. จัดให้มีนโยบายการใช้งานระบบสารสนเทศและอุปกรณ์ของบริษัทอย่างชัดเจน
3. ตรวจสอบและประเมินความเสี่ยงด้านความปลอดภัยข้อมูลอย่างน้อยปีละ 1 ครั้ง
4. กำหนดกระบวนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยข้อมูล (Incident Response)

การควบคุมการเข้าถึงข้อมูล

1. จำกัดสิทธิ์การเข้าถึงข้อมูลตามหน้าที่และความจำเป็นในการปฏิบัติงาน (Need-to-Know Basis)
2. มีระบบบันทึกการเข้าถึงข้อมูลและตรวจสอบการใช้งานอย่างต่อเนื่อง

การจัดการกับบุคคลภายนอก

1. ผู้รับเหมาและบุคคลภายนอกที่ได้รับอนุญาตเข้าถึงข้อมูลต้องปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยของบริษัท
2. ทำสัญญาหรือข้อตกลงที่ระบุข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยข้อมูล

การรายงานและจัดการเหตุการณ์ผิดปกติ

1. กำหนดช่องทางและขั้นตอนในการรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัยข้อมูลอย่างรวดเร็ว

2. ดำเนินการสอบสวนและแก้ไขปัญหาอย่างทันท่วงที

การปฏิบัติตามและการตรวจสอบ

1. พนักงานทุกคนต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2. บริษัทฯ จะทำการตรวจสอบการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยข้อมูลอย่างสม่ำเสมอ

3. กรณีละเมิดนโยบาย จะมีมาตรการทางวินัยและดำเนินการทางกฎหมายตามความเหมาะสม

ลงชื่อ

(กรรมการผู้จัดการ)

วันที่

11.4.2 จบท ที่ปฏิบัติงานเกี่ยวกับ PDPA และกำกับข้อมูล มีหน้าที่และความรับผิดชอบที่ชัดเจนเพื่อให้องค์กรปฏิบัติตามข้อกำหนด นโยบาย และกฎหมาย

สิ่งที่ต้องทำ: มีการกำหนดหน้าที่ในด้าน PDPA ให้ชัด

หลักฐาน: 1) จบท ที่ปฏิบัติงานเกี่ยวกับ PDPA และกำกับข้อมูล ระบุใน JD หรือข้อตกลง หรือสัญญาจ้างฯ

เอกสารนี้ต้องระบุให้เห็นว่า “มีหน้าที่คุ้มครองข้อมูลส่วนบุคคลของพนักงาน”

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างหลักฐาน 11.4.2: Job Description (JD) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ตำแหน่ง: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO)

แผนก: ฝ่ายบริหารความเสี่ยงและการปฏิบัติตามกฎหมาย

รายงานต่อ: กรรมการผู้จัดการ / คณะกรรมการคุ้มครองข้อมูล

หน้าที่และความรับผิดชอบหลัก

ดำเนินการและกำกับดูแลการปฏิบัติตามกฎหมาย PDPA และนโยบายคุ้มครองข้อมูลขององค์กร

1. ตรวจสอบและประเมินการจัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลขององค์กรให้สอดคล้องกับ PDPA

2. ให้คำแนะนำและคำปรึกษาแก่ฝ่ายต่าง ๆ เกี่ยวกับข้อกำหนดและแนวทางการปฏิบัติที่ถูกต้อง จัดทำและพัฒนานโยบาย แนวปฏิบัติ และมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

1. ดูแลให้นโยบายคุ้มครองข้อมูลได้รับการอัปเดตสม่ำเสมอและถูกต้องตามกฎหมาย

2. ส่งเสริมให้พนักงานทุกคนมีความตระหนักรู้เรื่องการคุ้มครองข้อมูลส่วนบุคคล

รับผิดชอบการจัดการข้อร้องเรียนและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

1. ตรวจสอบและตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับการละเมิดข้อมูล

2. ประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อแก้ไขปัญหาอย่างรวดเร็ว

รายงานข้อมูลและความคืบหน้าต่อผู้บริหารระดับสูง

1. จัดทำรายงานผลการดำเนินงานด้าน PDPA อย่างน้อยปีละ 1 ครั้ง

2. แจ้งข้อกังวลและปัญหาที่พบต่อผู้บริหารอย่างชัดเจนและทันเวลา

รักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคล

1. มีหน้าที่คุ้มครองข้อมูลส่วนบุคคลของพนักงานและลูกค้าอย่างเคร่งครัด

2. ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยข้อมูลที่บริษัทกำหนด

อบรมและสร้างความตระหนักแก่พนักงานเกี่ยวกับ PDPA

1. วางแผนและจัดการอบรมให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลแก่พนักงาน

ลงชื่อเจ้าหน้าที่

(ชื่อ-นามสกุล)

วันที่

11.4.3 มีเครือข่ายสนับสนุนการปฏิบัติงานด้าน PDPA หรือมีโอกาสได้รับการเสนอชื่อ หรือแต่งตั้งเป็น คณะทำงานด้าน PDPA เพื่อช่วยให้การดำเนินการ และธำรงไว้ซึ่งนโยบายด้าน PDPA ในส่วนงานย่อย หรือสายงาน หรือส่วนงานมีประสิทธิภาพมากขึ้น

สิ่งที่ต้องทำ: องค์กรต้องสนับสนุนให้เกิดเครือข่ายด้านการคุ้มครองข้อมูลส่วนบุคคล และสนับสนุนให้ พนง. แต่ละฝ่ายเป็นคณะทำงานของ DPO

หลักฐาน: 1) รายงานการประชุม กก. บริษัท หรือผู้บริหาร หรือ กก.กำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล หรือฝ่ายงาน ต้องมีข้อความให้เห็นว่า “มีการผลักดันเข้าไปเป็นคณะทำงานของ DPO”

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างหลักฐาน 11.4.3: รายงานการประชุมคณะกรรมการบริษัท (หรือฝ่ายบริหาร)

วันที่ประชุม: 30 พฤษภาคม 2568

สถานที่: ห้องประชุมใหญ่ ชั้น 5

ผู้เข้าร่วม: คณะกรรมการบริษัท, ฝ่ายบริหาร, ตัวแทนจากฝ่ายต่าง ๆ

ระเบียบวาระที่ 4: การสนับสนุนการปฏิบัติงานด้าน PDPA และการจัดตั้งคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล

เนื้อหา:

ที่ประชุมรับทราบความจำเป็นในการส่งเสริมและสนับสนุนการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) โดยเห็นชอบให้มีการจัดตั้งเครือข่ายคณะทำงานด้าน PDPA เพื่อช่วย DPO ในการดำเนินงาน และให้แต่ละฝ่ายผลัดเปลี่ยนกันส่งตัวแทนเข้าร่วมเป็นคณะทำงานเพื่อช่วยธำรงนโยบายและแนวทางปฏิบัติในส่วนงานของตน

มติที่ประชุม:

1. อนุมัติให้จัดตั้ง “คณะทำงานด้านคุ้มครองข้อมูลส่วนบุคคล” (PDPA Taskforce) โดยมีสมาชิกมาจากตัวแทนพนักงานแต่ละฝ่าย
2. ให้ฝ่ายทรัพยากรบุคคลและ DPO ร่วมกันกำหนดเกณฑ์การผลัดเปลี่ยนสมาชิกในคณะทำงานอย่างสม่ำเสมอ
3. ให้คณะทำงานฯ รายงานความคืบหน้าการปฏิบัติงานต่อ DPO และผู้บริหารระดับสูงทุกไตรมาส

ข้อความสำคัญ:

“ที่ประชุมมีมติให้มีการผลัดเปลี่ยนตัวแทนจากฝ่ายต่าง ๆ เข้าเป็นคณะทำงานของ DPO เพื่อช่วยส่งเสริมและสนับสนุนการดำเนินการตาม PDPA ในองค์กรอย่างมีประสิทธิภาพ”

ลงชื่อ.....

ประธานที่ประชุม

1.4.4 จบท ที่ปฏิบัติงานเกี่ยวกับ PDPA และการกำกับข้อมูล มีอำนาจ ได้รับการสนับสนุน และได้รับการจัดสรรทรัพยากรในการดำเนินงานอย่างมีประสิทธิภาพ

สิ่งที่ต้องทำ: องค์กรต้องสนับสนุนผู้ปฏิบัติงานอย่างเพียงพอ

หลักฐาน: 1) ภาพถ่ายอุปกรณ์ หรือเครื่องมือที่องค์กรจัดหาให้
2) บันทึกที่แสดงให้เห็นถึงการเข้าถึงฐานข้อมูลภายในองค์กรโดยพนักงานที่เกี่ยวข้อง

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างบันทึกข้อความ (ภายใน) แสดงการสนับสนุนทรัพยากร

บันทึกข้อความ

ส่วนงาน: ฝ่ายกฎหมายและการคุ้มครองข้อมูลส่วนบุคคล

ที่: ลับ/2568

วันที่: 2 มิถุนายน 2568

เรื่อง: การสนับสนุนทรัพยากรเพื่อการปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

เรียน กรรมการผู้จัดการใหญ่

ด้วยฝ่ายกฎหมายและการคุ้มครองข้อมูลส่วนบุคคล โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีภารกิจในการกำกับดูแลให้การดำเนินงานขององค์กรเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างมีประสิทธิภาพ จึงขอเรียนให้ทราบว่:

1. เจ้าหน้าที่ที่เกี่ยวข้องได้รับสิทธิ์เข้าถึงฐานข้อมูลที่จำเป็น เช่น ฐานข้อมูล CRM, ระบบจัดการเอกสารอิเล็กทรอนิกส์ (DMS), ระบบ HR และระบบ Ticket แจ้งเหตุด้านข้อมูล
2. ได้รับการจัดสรรเครื่องมือเพื่อใช้ในการปฏิบัติงาน ได้แก่
 - เครื่องคอมพิวเตอร์พร้อมซอฟต์แวร์วิเคราะห์ข้อมูล
 - โทรศัพท์สำนักงาน
 - ระบบ VPN สำหรับเข้าถึงฐานข้อมูลจากระยะไกล
 - ห้องทำงานเฉพาะแยกจากบุคคลภายนอกเพื่อความปลอดภัยของข้อมูล
3. มีงบประมาณประจำปีเพื่อใช้ในการฝึกอบรม / ตรวจสอบ / ว่าง้างที่ปรึกษาด้านข้อมูล ทั้งนี้เพื่อสนับสนุนให้การดำเนินการด้าน PDPA เป็นไปอย่างต่อเนื่อง และมีประสิทธิภาพสูงสุด

ลงชื่อ

นางสาวธัญญาภรณ์ อินทศรี

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

รับทราบ

นายอดิศักดิ์ ธนโชติ

กรรมการผู้จัดการใหญ่

ภาพถ่าย (แนบในเอกสารหรือไฟล์แยก)

- ภาพโต๊ะทำงานเจ้าหน้าที่ DPO พร้อมเครื่องคอมพิวเตอร์ตั้งโต๊ะ, โทรศัพท์สำนักงาน และเอกสาร PDPA
- ภาพหน้าจอระบบจัดการข้อมูล (Data Management System) แสดงชื่อผู้ใช้ที่มีสิทธิ์เข้าถึง
- ภาพห้องประชุมย่อยเฉพาะของฝ่าย DPO
- ภาพหน้าจอระบบ VPN / โปรแกรม Data Masking หรือ Data Access Control

1.5.1 ต้องจัดให้มีคณะทำงานของ DPO และ DPO เข้าร่วมประชุมกับคณะทำงานของ DPO อย่างสม่ำเสมอ

สิ่งที่ต้องทำ: ต้องตั้งคณะทำงานของ DPO และต้องมีการจัดประชุมอย่างสม่ำเสมอ

หลักฐาน: 1) รายงานการประชุม กก. บริษัท หรือผู้บริหาร หรือ กก.กำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล หรือฝ่ายงาน ต้องมีข้อความให้เห็นว่า “มีการแต่งตั้งคณะทำงานของ DPO โดยต้องปรากฏรายชื่อ DPO เป็นประธาน ปรากฏชื่อคณะทำงาน และภาระงานของคณะทำงานว่ามีหน้าที่อะไรบ้าง”

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างบันทึกรายงานการประชุมคณะทำงาน DPO

รายงานการประชุมคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO Working Group)

ครั้งที่ 1/2568

วัน/เวลา: วันอังคารที่ 5 มีนาคม 2568 เวลา 10.00–12.00 น.

สถานที่: ห้องประชุม 4A อาคารสำนักงานใหญ่

ผู้เข้าร่วมประชุม:

- นางสาวธัญญาภรณ์ อินทศรี – DPO (ประธานคณะทำงาน)
- นายอนุชา สวัสดิ์ – ฝ่าย IT Security
- นางสาวณัฐชา วิริยะ – ฝ่ายทรัพยากรบุคคล
- นายปกรณ์ สุวรรณโชติ – ฝ่ายกฎหมาย
- นางสาวเพ็ญศรี บุญธรรม – ตัวแทนฝ่ายลูกค้าสัมพันธ์ (CRM)

ระเบียบวาระการประชุม:

วาระที่ 1: แจ้งเพื่อทราบ

- ประธานชี้แจงการแต่งตั้งคณะทำงาน DPO เพื่อสนับสนุนการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร
- อ้างอิงคำสั่งที่ 12/2568 ลงวันที่ 1 กุมภาพันธ์ 2568 เรื่องการแต่งตั้งคณะทำงาน DPO

วาระที่ 2: พิจารณาและกำหนดบทบาทหน้าที่คณะทำงาน

ที่ประชุมเห็นชอบให้คณะทำงานมีหน้าที่หลัก ดังนี้

- (1) ประสานงานกับหน่วยงานภายในในการดำเนินการตามคำแนะนำของ DPO
- (2) รวบรวมและประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลของฝ่ายงาน
- (3) รายงานปัญหา ข້อร้องเรียน หรือเหตุละเมิดข้อมูล (Data Breach) ต่อ DPO
- (4) สนับสนุนการจัดทำบันทึกกิจกรรมการประมวลผล (ROPA)

วาระที่ 3: กำหนดรอบการประชุม

ที่ประชุมเห็นชอบให้มีการประชุมคณะทำงาน DPO ทุก 3 เดือน (ไตรมาสละ 1 ครั้ง)

วาระที่ 4: เรื่องอื่น ๆ

มีข้อเสนอให้จัดอบรมเสริมความรู้ PDPA สำหรับคณะทำงาน

มติที่ประชุม: รับทราบการแต่งตั้งคณะทำงาน และอนุมัติภาระงานและรอบการประชุมเรียบร้อยแล้ว

แล้ว

ลงชื่อ:

นางสาวธัญญาภรณ์ อินทศรี

ประธานคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หมายเหตุ: เอกสารแนบท้าย – คำสั่งแต่งตั้งคณะกรรมการ DPO (สำเนา)

1.5.2 DPO เป็นประธานคณะกรรมการ หรือมีบทบาทสำคัญในคณะกรรมการของ DPO

สิ่งที่ต้องทำ: ต้องตั้ง DPO เป็นประธานคณะกรรมการ และให้เป็นผู้มีบทบาทสำคัญ

หลักฐาน: 1) คำสั่งแต่งตั้งคณะกรรมการของ DPO โดยต้องมีรายละเอียดที่แสดงให้เห็นว่า “DPO เป็นประธานหรือผู้ทำงานในคณะกรรมการ และมีภาระงานของคณะกรรมการชัดเจน”
2) รายงานการประชุม กก. บริษัท หรือผู้บริหาร หรือ กก.กำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล หรือฝ่ายงาน

สภาพบังคับ: ไม่มีกฎหมายกำหนด

คำสั่งแต่งตั้งคณะกรรมการด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

คำสั่งที่ 01/2568

เรื่อง แต่งตั้งคณะกรรมการด้านการคุ้มครองข้อมูลส่วนบุคคล

เพื่อให้การดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลขององค์กรเป็นไปอย่างมีประสิทธิภาพ และสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงแต่งตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้:

1. รายชื่อคณะกรรมการ

ประธานคณะกรรมการ

- นาย/นาง/น.ส. [ชื่อ DPO] – เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- กรรมการ
- นาย/นาง/น.ส. [ชื่อ] – ผู้แทนฝ่ายเทคโนโลยีสารสนเทศ
- นาย/นาง/น.ส. [ชื่อ] – ผู้แทนฝ่ายกฎหมาย
- นาย/นาง/น.ส. [ชื่อ] – ผู้แทนฝ่ายทรัพยากรบุคคล
- นาย/นาง/น.ส. [ชื่อ] – ผู้แทนจากหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

เลขานุการ

- นาย/นาง/น.ส. [ชื่อ] – ด้าน PDPAเจ้าหน้าที่สนับสนุนงาน

2. อำนาจหน้าที่ของคณะกรรมการ

คณะกรรมการมีหน้าที่และความรับผิดชอบดังนี้:

- (1) วางแผนและกำหนดแนวทางการดำเนินงานเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- (2) เสนอแนะนโยบาย แนวปฏิบัติ หรือมาตรการคุ้มครองข้อมูลส่วนบุคคลให้ผู้บริหารพิจารณา
- (3) ตรวจสอบ ติดตาม และประเมินการปฏิบัติงานตามแนวปฏิบัติที่กำหนด
- (4) ประสานงานกับฝ่ายต่าง ๆ ภายในองค์กร เพื่อให้การปฏิบัติตาม PDPA เป็นไปโดยทั่วถึง
- (5) จัดประชุมอย่างสม่ำเสมอเพื่อติดตามความก้าวหน้าและแลกเปลี่ยนข้อมูลที่เกี่ยวข้อง
- (6) รายงานผลการดำเนินงานต่อคณะกรรมการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล หรือผู้บริหารองค์กร
- (7) ให้คำปรึกษา และเป็นศูนย์กลางในการติดต่อกับเจ้าของข้อมูลส่วนบุคคล
- (8) กรณีเกิดเหตุการณ์ละเมิดข้อมูล (Data Breach) ต้องจัดการ แจ้งเหตุ และบันทึกตามกระบวนการที่กำหนด
- (9) จัดทำรายงานการประชุม สรุปข้อเสนอแนะ และบันทึกข้อคิดเห็นจาก DPO ในทุกการประชุม

3. ระยะเวลาในการดำรงตำแหน่ง

ให้คณะกรรมการชุดนี้ดำรงตำแหน่งเป็นระยะเวลา 1 ปี นับแต่วันที่ออกคำสั่ง และสามารถต่ออายุหรือแต่งตั้งใหม่ได้ตามความเหมาะสม

สั่ง ณ วันที่ [xx เดือน xxxx]

ลงชื่อ

(.....)

ผู้มีอำนาจสั่งการ/ผู้บริหารองค์กร

รายงานการประชุม

คณะกรรมการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล (PDPA Committee)

ครั้งที่ 2/2568

วันที่: 15 พฤษภาคม 2568

เวลา: 10.00 – 12.00 น.

สถานที่: ห้องประชุมใหญ่ อาคารสำนักงานกลาง

ผู้เข้าร่วมประชุม

1. นาย/นาง/น.ส. [ชื่อ DPO] – ประธานกรรมการ
2. นาย/นาง/น.ส. [ชื่อ] – กรรมการ (ฝ่ายเทคโนโลยีสารสนเทศ)
3. นาย/นาง/น.ส. [ชื่อ] – กรรมการ (ฝ่ายกฎหมาย)
4. นาย/นาง/น.ส. [ชื่อ] – กรรมการ (ฝ่ายทรัพยากรบุคคล)
5. นาย/นาง/น.ส. [ชื่อ] – กรรมการ (ฝ่ายปฏิบัติการ)
6. นาย/นาง/น.ส. [ชื่อ] – เลขานุการ

วาระการประชุม

วาระที่ 1: เรื่องแจ้งเพื่อทราบ

- ประธานแจ้งว่าได้รับคำสั่งแต่งตั้งเป็น **ประธานคณะกรรมการด้านการคุ้มครองข้อมูลส่วนบุคคล (DPO Committee)** ตามคำสั่งที่ 01/2568 และจะดำเนินการตามอำนาจหน้าที่ที่กำหนดในคำสั่งฯ

วาระที่ 2: การกำหนดภารกิจของคณะกรรมการ DPO

คณะกรรมการมีมติเห็นชอบให้กำหนดภาระงานของคณะกรรมการตามข้อเสนอของ DPO ได้แก่:

- (1) การกำกับดูแลการจัดทำ Privacy Notice และบันทึกรายการกิจกรรมการประมวลผล (ROPA)
- (2) การติดตามการประเมินผลกระทบด้านการคุ้มครองข้อมูล (DPIA)
- (3) การกำกับดูแลมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- (4) การให้คำปรึกษาแก่ฝ่ายต่าง ๆ เกี่ยวกับ PDPA
- (5) การจัดทำแผนฝึกอบรมประจำปีให้เจ้าหน้าที่ที่เกี่ยวข้อง

วาระที่ 3: การกำหนดความถี่ในการประชุม

มีมติให้คณะกรรมการ DPO ประชุม **ทุกไตรมาส** และในกรณีมีเหตุฉุกเฉินหรือการละเมิดข้อมูล ให้จับประชุมพิเศษได้ทันที

วาระที่ 4: อื่น ๆ

- สมาชิกเสนอให้จัดทำช่องทางการติดต่อ DPO ภายในอินทราเน็ตขององค์กร เพื่อให้พนักงานสามารถสอบถามหรือแจ้งเหตุได้อย่างรวดเร็ว
- ประธาน (DPO) รับทราบและมอบหมายให้เลขานุการดำเนินการภายในเดือนนี้

มติที่ประชุมสรุปโดยรวม:

- รับทราบบทบาทของ DPO ในฐานะประธานคณะกรรมการ
- รับรองภาระงานของคณะกรรมการตามข้อเสนอ
- เห็นชอบกำหนดการประชุมรายไตรมาส
- มอบหมายให้จัดตั้งช่องทางการติดต่อกับ DPO

ปิดประชุม: เวลา 12.00 น.

ลงชื่อ..... ประธานการประชุม

(นาย/นาง/น.ส. [ชื่อ DPO])

ลงชื่อ..... ผู้บันทึกการประชุม

(นาย/นาง/น.ส. [ชื่อเลขานุการ])

1.5.3 มีการกำหนดเป้าหมายคณะกรรมการของ DPO อย่างชัดเจน

สิ่งที่ต้องทำ: มีการกำหนดเป้าหมายคณะกรรมการของ DPO อย่างชัดเจน และสอดคล้องกับภาระงาน DPO

หลักฐาน: 1) มีวาระการประชุม และรายงานการประชุมคณะกรรมการของ DPO โดยต้องมีข้อความที่แสดงให้เห็นอย่างชัดเจนถึง “เป้าหมาย และแผนการดำเนินงานของคณะกรรมการ”

สภาพบังคับ: ไม่มีกฎหมายกำหนด

วาระการประชุม

คณะกรรมการด้านการคุ้มครองข้อมูลส่วนบุคคล (คณะกรรมการ DPO)

ครั้งที่ 3/2568

วันที่: 5 มิถุนายน 2568

เวลา: 09.30 – 11.30 น.

สถานที่: ห้องประชุม PDPA ชั้น 3

ผู้เข้าร่วมประชุม

1. นาย/นาง/น.ส. [ชื่อ DPO] – ประธานคณะกรรมการ
2. นาย/นาง/น.ส. [ชื่อ] – ฝ่ายเทคโนโลยีสารสนเทศ
3. นาย/นาง/น.ส. [ชื่อ] – ฝ่ายกฎหมาย
4. นาย/นาง/น.ส. [ชื่อ] – ฝ่ายทรัพยากรบุคคล
5. นาย/นาง/น.ส. [ชื่อ] – ฝ่ายจัดการข้อมูล
6. นาย/นาง/น.ส. [ชื่อ] – เลขานุการ

วาระการประชุม

วาระที่ 1: เรื่องแจ้งเพื่อทราบ

ประธานแจ้งถึงการนัดประชุมตามรอบการทำงานไตรมาส 2 และเตรียมทบทวนเป้าหมายการดำเนินงานของคณะกรรมการ

วาระที่ 2: การกำหนดเป้าหมายและแผนการดำเนินงานประจำปี 2568 ของคณะกรรมการ DPO

เป้าหมายของคณะกรรมการ DPO (พ.ศ. 2568):

1. จัดทำและทบทวนนโยบาย PDPA ภายในองค์กร ให้สอดคล้องกับสถานการณ์จริงและแนวทางของ สคส.
2. สร้างความรู้ความเข้าใจแก่พนักงานในทุกระดับ ผ่านการอบรมไม่น้อยกว่า 2 ครั้ง/ปี

3. ควบคุมและกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลของแต่ละฝ่ายงาน ให้มีการบันทึก ROPA ครบถ้วน

4. ประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล และดำเนินการ DPIA ในกิจกรรมที่มีความเสี่ยงสูง

5. จัดให้มีระบบรับเรื่องร้องเรียนหรือแจ้งเหตุการละเมิดข้อมูล และรายงานให้ DPO ภายใน 72 ชั่วโมง

6. สนับสนุนการจัดซื้อ/จัดหาเครื่องมือระบบความปลอดภัยข้อมูล ให้เหมาะสมกับการดำเนินงาน

แผนการดำเนินงานไตรมาส 3-4:

Q3:

- ทบทวน Privacy Notice และ ROPA
- จัดอบรมบุคลากรสายงาน HR และ IT
- ปรับปรุงแบบฟอร์มขอความยินยอม (consent form)

Q4:

- ดำเนินการประเมิน DPIA อย่างน้อย 2 ระบบ
- สรุปผลการดำเนินงานและข้อเสนอแนะต่อฝ่ายบริหาร
- จัดทำแผนการดำเนินงานปี 2569

วาระที่ 3: อื่น ๆ

- สมาชิกเสนอให้เพิ่ม KPI สำหรับฝ่ายงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลโดยตรง เพื่อสะท้อนความสำเร็จของนโยบาย PDPA
- ประธานรับข้อเสนอและจะเสนอฝ่าย HR พิจารณาเพิ่มเติม

มติที่ประชุม:

- เห็นชอบเป้าหมายการดำเนินงานของคณะทำงาน DPO ปี 2568
- เห็นชอบแผนดำเนินงานรายไตรมาส
- มอบหมายให้เลขานุการจัดทำเอกสารเผยแพร่เป้าหมายและแผนไปยังทุกฝ่าย

ปิดประชุม: เวลา 11.30 น.

ลงชื่อ..... ประธานคณะทำงาน

(นาย/นาง/น.ส. [ชื่อ DPO])

ลงชื่อ..... เลขานุการ

(นาย/นาง/น.ส. [ชื่อเลขานุการ])

1.5.4 คณะทำงาน DPO มีการบันทึกรายงานประชุม

สิ่งที่ต้องทำ: คณะทำงาน DPO มีการบันทึกรายงานประชุมอย่างน้อยปีละ 1 ครั้ง และมีรายงานการประชุม

หลักฐาน: 1) มีวาระการประชุม และรายงานการประชุมของคณะทำงานของ DPO โดยต้องมีข้อความที่แสดงให้เห็นอย่างชัดเจนถึง “เป้าหมาย และแผนการดำเนินงานของคณะทำงาน”

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างวาระการประชุมและรายงานการประชุมของคณะทำงาน DPO ที่สามารถใช้เป็น หลักฐานตามเกณฑ์ 1.5.4 ได้ทันที โดยมีเนื้อหาชัดเจนเรื่อง “การประชุมของคณะทำงาน DPO อย่างน้อยปีละ 1 ครั้ง พร้อมระบุเป้าหมายและแผนการดำเนินงาน”

วาระการประชุมคณะทำงาน DPO

ครั้งที่ 1/2568

วันพฤหัสบดีที่ 15 กุมภาพันธ์ 2568

เวลา 09.30 – 11.30 น.

สถานที่: ห้องประชุม PDPA ชั้น 3 อาคารสำนักงานใหญ่

ผู้เข้าร่วมประชุม

1. นายพงศ์เทพ ศรีกาญจน์ – DPO และประธานคณะกรรมการ
2. นางสาวรจนา พิทักษ์ผล – ฝ่ายกฎหมาย
3. นายวิชัย ตันติวรารักษ์ – ฝ่ายเทคโนโลยีสารสนเทศ
4. นางสาวพรพิชชา ลีลาธรรม – ฝ่ายทรัพยากรบุคคล
5. นายศิวะ แสงทอง – ฝ่ายความปลอดภัยข้อมูล
6. นางสาวณลินี ศรีสวัสดิ์ – เลขานุการคณะกรรมการ

วาระการประชุม

วาระที่ 1: เรื่องแจ้งเพื่อทราบ

ประธานแจ้งให้ที่ประชุมทราบถึงเป้าหมายการทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล ปีงบประมาณ 2568

วาระที่ 2: พิจารณาเป้าหมายและแผนการดำเนินงานของคณะกรรมการ DPO ประจำปี 2568

เป้าหมายของคณะกรรมการ DPO ปี 2568

1. พัฒนานโยบายการคุ้มครองข้อมูลส่วนบุคคลให้ครอบคลุมทุกกิจกรรมขององค์กร
2. ส่งเสริมความรู้ ความเข้าใจ และการมีส่วนร่วมของพนักงานทุกฝ่าย
3. ตรวจสอบความสอดคล้องของกิจกรรมประมวลผลข้อมูลกับ PDPA และข้อกำหนดภายใน
4. บริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล และจัดทำรายงาน DPIA สำหรับกิจกรรมที่มีความเสี่ยงสูง
5. พัฒนาระบบรับเรื่องร้องเรียน และจัดการเหตุละเมิดข้อมูลให้มีประสิทธิภาพ

แผนการดำเนินงาน (โดยสรุป)

- ไตรมาส 1: จัดทำคู่มือ PDPA สำหรับฝ่ายงาน
- ไตรมาส 2:อบรมเจ้าหน้าที่ 2 รอบ (แผนก HR, IT)
- ไตรมาส 3: ทบทวนการจัดเก็บข้อมูล HR และจัดทำ DPIA
- ไตรมาส 4: สรุปผลการดำเนินงาน และเสนอแนวทางพัฒนา

วาระที่ 3: เรื่องอื่น ๆ

- เสนอแต่งตั้งเจ้าหน้าที่ประจำสายงานแต่ละฝ่ายให้ประสานกับ DPO โดยตรง เพื่อความรวดเร็ว
- เสนอขอสนับสนุนงบประมาณเพิ่มเติมสำหรับเครื่องมือเข้ารหัสข้อมูลของฝ่ายบัญชี

มติที่ประชุม

- เห็นชอบแผนงานและเป้าหมายของคณะกรรมการ DPO ปี 2568 ตามที่เสนอ
- เห็นชอบให้แต่งตั้งผู้ประสานงานสายงานโดยเสนอชื่อภายใน 1 สัปดาห์

- มอบหมายเลขานุการประชุมจัดส่งบันทึกการประชุมฉบับนี้ให้กรรมการกำกับดูแลข้อมูลส่วนบุคคล
รับทราบ

ปิดประชุมเวลา 11.30 น.

ลงชื่อ.....

นายพงศ์เทพ ศรีกาญจน์

ประธานคณะกรรมการ DPO

ลงชื่อ.....

นางสาวนลินี ศรีสวัสดิ์

เลขานุการคณะกรรมการ

เปรียบเทียบเกณฑ์ข้อ 1.5.3 กับข้อ 1.5.4

ประเด็น	1.5.3: เป้าหมายคณะกรรมการ DPO	1.5.4: รายงานการประชุมคณะกรรมการ
วัตถุประสงค์	แสดง “เป้าหมายและแผน” ของ คณะกรรมการ	แสดงว่า “มีการประชุมจริง” และมี เอกสารรายงาน
เอกสารหลักฐาน	รายงานประชุมที่ระบุเป้าหมาย	รายงานประชุมปีละอย่างน้อย 1 ครั้ง
เกณฑ์บ่งชี้ ความสำเร็จ	มีแผน/วิสัยทัศน์ของคณะกรรมการ	มีเอกสารการประชุมจริง ไม่ใช่แค่แผน

1.5.5 ภาระงานของ DPO ครอบคลุมถึงการดำเนินงานด้าน PDPA ครบถ้วน รวมถึงระบุปัญหา ความ
เสี่ยงด้าน PDPA และการทำตัวชี้วัด (KPI) สำหรับ PDPA ขององค์กร

สิ่งที่ต้องทำ: คณะกรรมการ DPO ต้องมีการเกี่ยวกับ PDPA ดังนี้

- ระบุปัญหา
- ความเสี่ยง
- ทำตัวชี้วัด(KPI) ครอบคลุมการดำเนินงาน PDPA

หลักฐาน: 1) คำสั่งแต่งตั้ง รายงานการประชุม กก.บริหาร หรือผู้บริหาร หรือ กก. กำกับฯ โดยต้องมีข้อความแสดงให้เห็นว่า “คณะทำงาน DPO มีรายชื่อ DPO เป็นประธานหรือผู้ทำงานในคณะทำงานและภาระงานของคณะทำงาน”

สภาพบังคับ: ไม่มีกฎหมายกำหนด

รายงานการประชุมคณะกรรมการบริหาร

วันที่: 15 พฤษภาคม 2568

เวลา: 10:00 – 12:00 น.

สถานที่: ห้องประชุมใหญ่ อาคารสำนักงานใหญ่

ผู้เข้าร่วมประชุม:

1. นายสมชาย ใจดี (ประธานกรรมการ)
2. นางสาวสุดา พูนสุข (กรรมการบริหาร)
3. นายธนกร แก้วใส (กรรมการบริหาร)
4. นางสาวปวีณา ดวงดี (กรรมการบริหาร)
5. นางสาวศิริพร สุขใจ (กรรมการกำกับดูแลข้อมูลส่วนบุคคล)

วาระการประชุมที่ 1: การแต่งตั้งคณะทำงาน DPO

ที่ประชุมได้พิจารณาแต่งตั้งคณะทำงาน DPO เพื่อกำกับดูแลการบริหารจัดการข้อมูลส่วนบุคคล (PDPA) ขององค์กร โดยแต่งตั้ง นางสาวศิริพร สุขใจ เป็นประธานคณะทำงาน DPO มีบทบาทสำคัญในการวางแผน กำกับ ติดตาม และรายงานผลการดำเนินงานด้าน PDPA ให้เป็นไปตามนโยบายและกฎหมายที่เกี่ยวข้อง

วาระการประชุมที่ 2: รายงานปัญหาและความเสี่ยงด้าน PDPA

นางสาวศิริพร รายงานปัญหาและความเสี่ยงที่พบจากการตรวจสอบและประเมินระบบคุ้มครองข้อมูลส่วนบุคคลขององค์กร ดังนี้

ปัญหา

- การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตในบางส่วนของระบบฐานข้อมูล
- ข้อมูลส่วนบุคคลที่เก็บรักษาไว้บางส่วนไม่ได้รับการอัปเดตหรือจำกัดการเข้าถึงอย่างเหมาะสม
- การขาดความตระหนักรู้ของพนักงานบางกลุ่มเกี่ยวกับมาตรการ PDPA

ความเสี่ยง

- ความเสี่ยงในการละเมิดสิทธิเจ้าของข้อมูลส่วนบุคคลจากการรั่วไหลของข้อมูล
- ความเสี่ยงทางกฎหมายและการถูกปรับตามมาตรฐาน PDPA
- ความเสี่ยงที่เกิดจากการจัดการข้อมูลไม่เป็นระบบและไม่ครบถ้วน

วาระการประชุมที่ 3: การกำหนดตัวชี้วัด (KPI) ด้าน PDPA

ที่ประชุมเห็นชอบตัวชี้วัด (KPI) เพื่อประเมินประสิทธิผลของการบริหารจัดการ PDPA โดยคณะกรรมการ DPO ดังนี้

- จำนวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นต่อปี (Target: ไม่เกิน 2 ครั้ง/ปี)
- ระยะเวลาการตอบสนองคำร้องขอของเจ้าของข้อมูล (Target: ตอบภายใน 15 วันทำการ)
- อัตราการเข้าร่วมอบรม PDPA ของพนักงานทั้งหมด (Target: 95% ขึ้นไปต่อปี)
- จำนวนการตรวจสอบและปรับปรุงระบบความปลอดภัยข้อมูล (Target: อย่างน้อย 2 ครั้งต่อปี)

สรุปการประชุม

ที่ประชุมมีมติเห็นชอบแต่งตั้งคณะกรรมการ DPO ตามข้อเสนอ พร้อมรับทราบปัญหาและความเสี่ยงที่รายงาน และอนุมัติตัวชี้วัด (KPI) เพื่อใช้ติดตามและประเมินผลการบริหารจัดการ PDPA อย่างเคร่งครัด

คำสั่งแต่งตั้งคณะกรรมการ DPO (แนบท้ายรายงาน)

คำสั่งเลขที่: 001/2568

เรื่อง: แต่งตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPO)

ตามที่บริษัทฯ ตระหนักถึงความสำคัญในการปกป้องข้อมูลส่วนบุคคล และเพื่อให้การบริหารจัดการข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) บริษัทฯ จึงมีคำสั่งแต่งตั้งคณะกรรมการ DPO โดยมีรายละเอียด ดังนี้

แต่งตั้ง นางสาวศิริพร สุขใจ ดำรงตำแหน่ง ประธานคณะกรรมการ DPO

2. ภาระงานของคณะกรรมการ DPO ประกอบด้วย
 - 2.1 การวางแผนและกำกับดูแลการปฏิบัติตามนโยบาย PDPA
 - 2.2 การระบุและวิเคราะห์ปัญหาและความเสี่ยงด้านข้อมูลส่วนบุคคล
 - 2.3 การจัดทำและติดตามตัวชี้วัด (KPI) เพื่อประเมินผลการดำเนินงานด้าน PDPA
 - 2.4 การจัดประชุมและรายงานผลการดำเนินงานต่อคณะกรรมการบริหารและผู้บริหารอย่างสม่ำเสมอ
 - 2.5 การส่งเสริมการอบรมและสร้างความตระหนักรู้ในองค์กรเกี่ยวกับ PDPA

ลงชื่อ.....

(นายสมชาย ใจดี)

ประธานกรรมการบริหาร

วันที่ 15 พฤษภาคม 2568

1.5.6 คณะทำงานของ DPO มีแผนงาน หรือแผนปฏิบัติการที่ได้รับการติดตามอย่างสม่ำเสมอ

สิ่งที่ต้องทำ: คณะทำงานของ DPO มีแผนงาน หรือแผนปฏิบัติการที่ได้รับการติดตามอย่างน้อยปีละ 1 ครั้ง

หลักฐาน: 1) มีวาระการประชุม และรายงานการประชุมคณะทำงานของ DPO ที่แสดงถึงเป้าหมายและแผนการดำเนินงานของคณะทำงาน

สภาพบังคับ: ไม่มีกฎหมายกำหนด

รายงานการประชุมคณะทำงาน DPO

ครั้งที่: 2/2568

วันที่: 20 มิถุนายน 2568

เวลา: 14:00 – 16:00 น.

สถานที่: ห้องประชุมฝ่ายบริหารข้อมูลส่วนบุคคล

ผู้เข้าร่วมประชุม:

- นางสาวศิริพร สุขใจ (ประธานคณะทำงาน DPO)
- นายธนกร แก้วใส (สมาชิกคณะทำงาน)
- นางสาวปวีณา ดวงดี (สมาชิกคณะทำงาน)
- เจ้าหน้าที่ฝ่าย IT
- เจ้าหน้าที่ฝ่ายบริหารความเสี่ยง

วาระที่ 1: ติดตามแผนงานและแผนปฏิบัติการด้าน PDPA ปี 2568

ประธานคณะทำงานรายงานความคืบหน้าของแผนงานและแผนปฏิบัติการที่วางไว้ในปี 2568 ซึ่งประกอบด้วย

- การอบรมและสร้างความตระหนักรู้เรื่อง PDPA ให้พนักงานทุกฝ่าย ภายในไตรมาส 3/2568
- การตรวจสอบและปรับปรุงระบบรักษาความปลอดภัยข้อมูลในฐานข้อมูลหลัก ภายในไตรมาส 4/2568
- การจัดทำรายงานประเมินความเสี่ยงและแนวทางลดความเสี่ยงด้านข้อมูลส่วนบุคคล ภายในไตรมาส 3/2568

- การทบทวนนโยบายและคู่มือปฏิบัติการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ภายในไตรมาส 4/2568

วาระที่ 2: ประเมินผลการดำเนินงานตามแผนงาน

ที่ประชุมได้พิจารณาผลการดำเนินงานโดยสรุป

- การอบรม PDPA ให้กับพนักงาน ได้ดำเนินการแล้ว 60% ของเป้าหมาย
- ระบบรักษาความปลอดภัยข้อมูล อยู่ระหว่างการปรับปรุงตามแผน
- รายงานความเสี่ยงอยู่ในขั้นตอนรวบรวมข้อมูลเพื่อจัดทำรายงานฉบับสมบูรณ์
- การทบทวนนโยบายอยู่ระหว่างรวบรวมข้อคิดเห็นจากฝ่ายงานต่าง ๆ

วาระที่ 3: ข้อเสนอแนะและแผนการดำเนินงานต่อไป

ที่ประชุมเห็นชอบให้

- เร่งรัดการอบรม PDPA ให้ครอบคลุมพนักงานทั้งหมดภายในสิ้นไตรมาส 3
- ติดตามการปรับปรุงระบบรักษาความปลอดภัยและแจ้งผลความคืบหน้าในที่ประชุมครั้งหน้า
- เร่งรัดการจัดทำรายงานความเสี่ยง และทบทวนนโยบายเพื่อเสนอคณะกรรมการบริหารภายในสิ้นปี

สรุปการประชุม

ที่ประชุมรับทราบและติดตามความคืบหน้าของแผนงานและแผนปฏิบัติการด้าน PDPA ของคณะกรรมการ DPO อย่างใกล้ชิด และจะจัดประชุมติดตามอย่างน้อยปีละ 1 ครั้งตามที่กำหนด

1.5.7 คณะกรรมการบริษัท หรือผู้บริหารระดับสูงพิจารณาประเด็น PDPA และการกำกับดูแลข้อมูล และความเสี่ยงที่รายงานโดยคณะกรรมการของ DPO

สิ่งที่ต้องทำ: คณะทำงานของ DPO รายงานประเด็น PDPA และการกำกับดูแลข้อมูล และความเสี่ยงองค์กรไปยัง คณะ กก.บริษัท หรือผู้บริหารสูงสุด

หลักฐาน: 1) รายงานการประชุมคณะกรรมการของ DPO หรือรายงานที่ประชุม กก.บริษัท หรือผู้บริหารองค์กร หรือคณะ กก.กำกับการดูแลคุ้มครองข้อมูลส่วนบุคคล โดยต้องมีข้อความแสดงให้เห็นว่า “การคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลข้อมูล รวมถึงความเสี่ยงขององค์กร” และเป็นการรายงานโดยคณะกรรมการของ DPO

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างรายงานการประชุมคณะกรรมการทำงานของ DPO

ครั้งที่: 3/2568

วันที่: 15 กันยายน 2568

เวลา: 13:00 – 15:00 น.

สถานที่: ห้องประชุมฝ่ายบริหารข้อมูลส่วนบุคคล

ผู้เข้าร่วม:

1. นางสาวศิริพร สุขใจ (ประธานคณะกรรมการทำงาน DPO)
2. สมาชิกคณะกรรมการทำงาน DPO ทุกฝ่าย
3. เจ้าหน้าที่ฝ่าย IT และความมั่นคงข้อมูล

วาระที่ 1: รายงานสถานะการดำเนินงานด้าน PDPA

ประธานคณะกรรมการทำงานรายงานสรุปประเด็นการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล รวมถึงสถานะความเสี่ยงที่ตรวจพบในองค์กร เช่น

- ปัญหาด้านความปลอดภัยของระบบเก็บข้อมูลลูกค้า
- ความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- แนวทางการแก้ไขและมาตรการป้องกันที่ดำเนินการแล้ว

วาระที่ 2: การจัดทำรายงานเพื่อนำเสนอผู้บริหารระดับสูง

ที่ประชุมมีมติเห็นชอบให้จัดทำรายงานผลการดำเนินงาน PDPA และความเสี่ยง พร้อมข้อเสนอแนะ เพื่อส่งให้คณะกรรมการบริษัทและผู้บริหารระดับสูงพิจารณา

สรุป

คณะกรรมการ DPO รับทราบประเด็นความเสี่ยงด้าน PDPA และวางแผนติดตามผลอย่างต่อเนื่อง พร้อมจัดทำรายงานเพื่อนำเสนอผู้บริหารระดับสูงในครั้งถัดไป

ตัวอย่างรายงานการประชุมคณะกรรมการบริษัท (หรือผู้บริหารระดับสูง)

ครั้งที่: 5/2568

วันที่: 1 ตุลาคม 2568

เวลา: 10:00 – 12:00 น.

สถานที่: ห้องประชุมใหญ่

ผู้เข้าร่วม:

- ประธานกรรมการบริษัท

- กรรมการบริษัททุกท่าน
- ผู้บริหารระดับสูง
- ตัวแทนคณะทำงาน DPO (นางสาวศิริพร สุขใจ)

วาระที่ 4: รายงานการคุ้มครองข้อมูลส่วนบุคคลและความเสี่ยงที่เกี่ยวข้อง

ตัวแทนคณะทำงาน DPO ได้นำเสนอรายงานสถานการณ์การกำกับดูแลข้อมูลส่วนบุคคล และสรุปความเสี่ยงที่เกี่ยวข้องกับ PDPA ขององค์กร ประกอบด้วย

- ประเด็นความเสี่ยงจากระบบข้อมูลและมาตรการความปลอดภัย
- การประเมินผลกระทบด้านความปลอดภัยข้อมูลส่วนบุคคล
- การดำเนินการตามแผนงานแก้ไขปัญหาและลดความเสี่ยง

การพิจารณาและข้อเสนอแนะ

กรรมการและผู้บริหารระดับสูงได้พิจารณารายงานดังกล่าวและให้คำแนะนำในการปรับปรุงมาตรการเพิ่มเติม เช่น การเพิ่มงบประมาณสำหรับระบบรักษาความปลอดภัยข้อมูล และการอบรมพนักงานเพิ่มขึ้น

สรุปการประชุม

ที่ประชุมรับทราบและเห็นชอบแผนงานการคุ้มครองข้อมูลส่วนบุคคลตามที่คณะทำงาน DPO รายงาน พร้อมกำชับให้ติดตามผลอย่างต่อเนื่อง

1.6.1 กลุ่มปฏิบัติการมีการพบปะ และมีเจ้าหน้าที่ที่เกี่ยวข้องเข้าร่วมอย่างสม่ำเสมอ

สิ่งที่ต้องทำ: กลุ่มปฏิบัติการ ซึ่งเป็นพนักงานปฏิบัติการของฝ่าย มีการจัดประชุมสม่ำเสมอ เช่น รายไตรมาส และมีเจ้าหน้าที่ที่เกี่ยวข้องส่วนใหญ่เข้าร่วม

หลักฐาน: 1) วาระการประชุม และรายงานการประชุม โดยต้องมีข้อความแสดงให้เห็นว่า “เอกสารแผนปฏิบัติการสำหรับการทำ PDPA ของกลุ่มปฏิบัติการ”

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างรายงานการประชุมกลุ่มปฏิบัติการ PDPA

ครั้งที่: 2/2568

วันที่: 20 มีนาคม 2568

เวลา: 09:00 – 11:00 น.

สถานที่: ห้องประชุมฝ่ายปฏิบัติการ

ผู้เข้าร่วม:

- นายสมชาย แก้วใส (หัวหน้ากลุ่มปฏิบัติการ)
- เจ้าหน้าที่ฝ่ายปฏิบัติการทุกคน (รวม 10 คน)
- เจ้าหน้าที่ฝ่าย IT และฝ่ายกฎหมาย (ร่วมประชุมบางส่วน)

วาระที่ 1: การติดตามแผนปฏิบัติการ PDPA ของกลุ่มปฏิบัติการ

หัวหน้ากลุ่มปฏิบัติการรายงานความคืบหน้าการดำเนินงานตามแผนปฏิบัติการ PDPA ของกลุ่มปฏิบัติการ โดยมีรายละเอียดดังนี้:

- แผนปฏิบัติการสำหรับการทำ PDPA ของกลุ่มปฏิบัติการ ได้วางกรอบการดำเนินงานเป็นรายไตรมาส
- การอบรมและสร้างความรู้ความเข้าใจให้เจ้าหน้าที่ฝ่ายปฏิบัติการเกี่ยวกับ PDPA
- การตรวจสอบการเก็บรักษาข้อมูลส่วนบุคคลตามมาตรฐานที่กำหนด
- การปรับปรุงขั้นตอนการทำงานเพื่อสอดคล้องกับข้อกำหนด PDPA

วาระที่ 2: การเข้าร่วมประชุมของเจ้าหน้าที่ที่เกี่ยวข้อง

มีการบันทึกว่า เจ้าหน้าที่ฝ่ายปฏิบัติการส่วนใหญ่เข้าร่วมประชุมสม่ำเสมอ และมีเจ้าหน้าที่ฝ่ายสนับสนุน เช่น IT และกฎหมาย ร่วมประชุมอย่างต่อเนื่อง เพื่อให้คำปรึกษาและสนับสนุนงานด้าน PDPA

สรุป

ที่ประชุมรับทราบและเห็นชอบแผนปฏิบัติการ PDPA ของกลุ่มปฏิบัติการ พร้อมติดตามความก้าวหน้าในการดำเนินงานในไตรมาสต่อไป

1.6.2 กลุ่มปฏิบัติการมีการจัดทำรายงานการประชุมและแผนปฏิบัติการ

- สิ่งที่ต้องทำ: กลุ่มปฏิบัติการ ซึ่งเป็นพนักงานระดับปฏิบัติการมีการจัดทำรายงานการประชุมและแผนปฏิบัติการ
- หลักฐาน: 1) วาระการประชุม และรายงานการประชุม โดยต้องมีข้อความแสดงให้เห็นว่า “เอกสารแผนปฏิบัติการสำหรับการทำ PDPA ของกลุ่มปฏิบัติการ”
- สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างรายงานการประชุมกลุ่มปฏิบัติการ PDPA

ครั้งที่: 3/2568

วันที่: 20 มิถุนายน 2568

เวลา: 09:00 – 11:00 น.

สถานที่: ห้องประชุมฝ่ายปฏิบัติการ

ผู้เข้าร่วม:

1. นายสมชาย แก้วใส (หัวหน้ากลุ่มปฏิบัติการ)
2. เจ้าหน้าที่ฝ่ายปฏิบัติการทุกคน (รวม 10 คน)
3. เจ้าหน้าที่ฝ่ายสนับสนุน (IT, กฎหมาย)

วาระที่ 1: การจัดทำและทบทวนแผนปฏิบัติการ PDPA ของกลุ่มปฏิบัติการ

หัวหน้ากลุ่มปฏิบัติการได้นำเสนอแผนปฏิบัติการสำหรับการทำ PDPA ของกลุ่มปฏิบัติการ

ซึ่งประกอบด้วย:

- แผนการดำเนินงานประจำไตรมาสในการบริหารจัดการข้อมูลส่วนบุคคล
- กิจกรรมการอบรมและสร้างความตระหนักรู้แก่เจ้าหน้าที่ฝ่ายปฏิบัติการ
- การปรับปรุงและทบทวนขั้นตอนการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามข้อกำหนด PDPA

วาระที่ 2: การจัดทำรายงานการประชุม

มีการยืนยันว่ากลุ่มปฏิบัติการได้จัดทำรายงานการประชุมทุกครั้งที่มีการประชุมอย่างเป็นทางการ โดยรายงานการประชุมฉบับนี้แสดงถึงประเด็นการหารือและการติดตามแผนงาน PDPA อย่างครบถ้วนสรุป

ที่ประชุมเห็นชอบแผนปฏิบัติการและรายงานการประชุม และมอบหมายให้กลุ่มปฏิบัติการติดตามและรายงานผลการดำเนินงานในครั้งถัดไป

1.6.4 วาระการประชุมแสดงให้เห็นว่ากลุ่มปฏิบัติการได้มีการหารือเกี่ยวกับประเด็น PDPA อย่างเหมาะสมและมีการกำกับดูแลอย่างสม่ำเสมอ

สิ่งที่ต้องทำ: กลุ่มปฏิบัติการ ซึ่งเป็นพนักงานระดับปฏิบัติการมีวาระการประชุมแสดงให้เห็นว่ากลุ่มปฏิบัติการได้มีการหารือเกี่ยวกับประเด็น PDPA อย่างเหมาะสมและมีการกำกับดูแลอย่างสม่ำเสมอ

หลักฐาน: 1) วาระการประชุม และรายงานการประชุม โดยต้องมีข้อความแสดงให้เห็นว่า “เอกสารแผนปฏิบัติการสำหรับการทำ PDPA ของกลุ่มปฏิบัติการ”

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างวาระและรายงานการประชุมกลุ่มปฏิบัติการ PDPA

ครั้งที่: 4/2568

วันที่: 15 กันยายน 2568

เวลา: 13:00 – 15:00 น.

สถานที่: ห้องประชุมฝ่ายปฏิบัติการ

ผู้เข้าร่วม:

- นางสาวพิมพ์ใจ ใจดี (หัวหน้ากลุ่มปฏิบัติการ)
- เจ้าหน้าที่ฝ่ายปฏิบัติการ 12 คน
- ตัวแทนฝ่าย IT และฝ่ายกฎหมาย

วาระที่ 1: รายงานการติดตามแผนปฏิบัติการ PDPA

กลุ่มปฏิบัติการได้นำเสนอรายงานความก้าวหน้าของแผนปฏิบัติการ PDPA ตามที่วางไว้ในไตรมาสที่ผ่านมา โดยมีการตรวจสอบประเด็นสำคัญ เช่น

- การบริหารจัดการความปลอดภัยของข้อมูลส่วนบุคคล
- การอบรมสร้างความตระหนักรู้แก่พนักงานใหม่และพนักงานปัจจุบัน
- การแก้ไขปัญหาที่พบจากการประเมินความเสี่ยงด้าน PDPA

วาระที่ 2: การหารือประเด็น PDPA และการกำกับดูแล

ที่ประชุมได้หารือถึงประเด็นที่เกี่ยวข้องกับการปฏิบัติตาม PDPA เช่น

- การจัดการคำร้องขอเข้าถึงข้อมูลส่วนบุคคล
- การรับมือกับเหตุละเมิดข้อมูล (Data Breach)
- การปรับปรุงแนวทางปฏิบัติเพื่อสอดคล้องกับนโยบาย PDPA ขององค์กร

โดยมีมติให้มีการติดตามและรายงานผลในที่ประชุมครั้งต่อไปอย่างสม่ำเสมอ

สรุป

ที่ประชุมยืนยันความสำคัญของการกำกับดูแลข้อมูลส่วนบุคคลในกลุ่มปฏิบัติการ และมอบหมายให้หัวหน้ากลุ่มติดตามความคืบหน้าของแผนงานและรายงานในทุกไตรมาส

1.6.4 ปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล และความเสี่ยงใด ๆ ที่เกิดขึ้นจะถูกรายงานไปยังคณะทำงานของ DPO

สิ่งที่ต้องทำ: กลุ่มปฏิบัติการ (พนักงานในระดับปฏิบัติการของฝ่ายงาน) รายงานปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูลรวมถึงประเด็นความเสี่ยงใด ๆ ขององค์กรที่เกิดขึ้นไปยังคณะทำงาน

ของ DPO ครบถ้วน

หลักฐาน: 1) วาระการประชุม และรายงานการประชุมของคณะทำงาน DPO หรือกลุ่มปฏิบัติการ โดยต้องมีข้อความแสดงให้เห็นว่า “มีปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล และความเสี่ยงใด ๆ ที่เกิดขึ้น”

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ตัวอย่างวาระและรายงานการประชุมกลุ่มปฏิบัติการและคณะทำงาน DPO

กลุ่มปฏิบัติการฝ่ายปฏิบัติการ

ครั้งที่: 3/2568

วันที่: 10 สิงหาคม 2568

เวลา: 14:00 – 16:00 น.

สถานที่: ห้องประชุมฝ่ายปฏิบัติการ

ผู้เข้าร่วม:

1. นายสมชาย ดีมาก (หัวหน้ากลุ่มปฏิบัติการ)
2. เจ้าหน้าที่ฝ่ายปฏิบัติการ 10 คน
3. ตัวแทนฝ่าย DPO

วาระที่ 2: รายงานปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและความเสี่ยง

กลุ่มปฏิบัติการได้นำเสนอปัญหาและประเด็นความเสี่ยงที่เกิดขึ้นระหว่างการปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

- พบปัญหาการเก็บข้อมูลส่วนบุคคลบางส่วนไม่เป็นไปตามนโยบาย PDPA
- การควบคุมการเข้าถึงข้อมูลยังไม่เข้มงวดพอ

- ความเสี่ยงจากการใช้ระบบไอทีที่ยังขาดมาตรการป้องกันข้อมูลรั่วไหล
- โดยกลุ่มปฏิบัติการได้จัดทำรายงานฉบับสมบูรณ์และส่งต่อให้คณะทำงาน DPO เพื่อพิจารณาแนวทางแก้ไขและติดตามผล

วาระที่ 3: รับทราบปัญหาและความเสี่ยงจากกลุ่มปฏิบัติการ

คณะทำงาน DPO ได้รับรายงานปัญหาและความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลจากกลุ่มปฏิบัติการ พร้อมทั้งพิจารณาแนวทางป้องกันและแก้ไข โดยมีข้อสรุปว่า

- จะจัดทำคู่มือและอบรมเสริมความรู้พนักงาน
- กำหนดมาตรการควบคุมการเข้าถึงข้อมูลให้ชัดเจน
- ตรวจสอบระบบไอทีให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม

2.1.1 องค์การจัดทำนโยบาย PDPA และกรอบการปฏิบัติงาน ที่มาจากแผนเชิงกลยุทธ์ด้าน PDPA และการกำกับข้อมูล ซึ่งมีการรับรองโดยฝ่ายบริหารระดับสูง

สิ่งที่ต้องทำ: จัดทำนโยบาย PDPA และกรอบการปฏิบัติงาน ที่มาจากแผนเชิงกลยุทธ์ด้าน PDPA และการกำกับข้อมูล ซึ่งมีการรับรอง หรือออกโดยฝ่ายบริหารระดับสูง

หลักฐาน: 1) นโยบาย โดยต้องมีข้อความแสดงให้เห็นว่า “มีปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลข้อมูล และความเสี่ยงใด ๆ ที่เกิดขึ้น”

สภาพบังคับ: 1) มาตรา 37 และประกาศฯ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยฯ ข้อ 4(7)
2) โทษทางปกครองปรับ 3 ล้าน

นโยบายการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล

บริษัท เอ็กเซลเลนท์ จำกัด

ประกาศเมื่อวันที่ 1 มกราคม 2568

ได้รับการอนุมัติจากคณะผู้บริหารระดับสูง

บทนำ

บริษัท เอ็กเซลเลนท์ จำกัด ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลของลูกค้า พนักงาน และคู่ค้าทางธุรกิจทุกฝ่าย การปกป้องข้อมูลส่วนบุคคลจึงเป็นหนึ่งในภารกิจหลักขององค์กร เพื่อรักษาความน่าเชื่อถือและความมั่นคงปลอดภัยในการดำเนินธุรกิจ ภายใต้ต้นนโยบายนี้ บริษัทฯ กำหนดกรอบการปฏิบัติงานด้าน PDPA และการกำกับดูแลข้อมูลให้มีประสิทธิภาพและเป็นไปตามกฎหมายและมาตรฐานสากล

วัตถุประสงค์

- สร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสียว่าข้อมูลส่วนบุคคลได้รับการดูแลอย่างเหมาะสม
- ป้องกันปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล
- ระบุและประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลและความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินงานขององค์กร
- สร้างกรอบการปฏิบัติงานที่ครอบคลุมและสามารถติดตามประเมินผลได้

นโยบายหลัก

1. การคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล

บริษัทฯ มีการประเมินและระบุปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล รวมถึงความเสี่ยงใด ๆ ที่เกิดขึ้นจากการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลอย่างสม่ำเสมอ และมีมาตรการแก้ไขและควบคุมความเสี่ยงอย่างเหมาะสม

(ข้อความสำคัญ) : “บริษัทฯ ตระหนักและยอมรับว่ามีปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล และความเสี่ยงใด ๆ ที่เกิดขึ้นจากการดำเนินงาน จึงได้จัดทำนโยบายและมาตรการเพื่อบริหารจัดการความเสี่ยงเหล่านี้อย่างเข้มงวด”

2. กรอบการปฏิบัติงานด้าน PDPA

บริษัทฯ กำหนดกรอบการปฏิบัติงานที่ชัดเจนครอบคลุมการจัดเก็บ ใช้ เปิดเผย และทำลายข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามมาตรฐานของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และประกาศที่เกี่ยวข้อง

- มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- มีการอบรมและสร้างความรู้ความเข้าใจแก่พนักงานทุกระดับ
- จัดทำระบบควบคุมภายในและมาตรการรักษาความปลอดภัยข้อมูลอย่างต่อเนื่อง

3. การบริหารความเสี่ยงด้านการคุ้มครองข้อมูล

บริษัทฯ มีระบบการบริหารความเสี่ยงโดยมุ่งเน้นไปที่ความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งในแง่เทคนิคและนโยบายองค์กร

- ระบุความเสี่ยงและปัญหาที่อาจส่งผลกระทบต่อ การคุ้มครองข้อมูล
- กำหนดตัวชี้วัดประสิทธิภาพ (KPI) สำหรับการบริหารจัดการ PDPA เพื่อติดตามผลการดำเนินงานอย่างสม่ำเสมอ
- มีการทบทวนและปรับปรุงแผนการบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้ง

4. การกำกับดูแลและรับรองโดยฝ่ายบริหารระดับสูง

ฝ่ายบริหารระดับสูงมีบทบาทสำคัญในการกำกับดูแลนโยบายนี้ โดย

- รับรองนโยบายและกรอบการปฏิบัติงานด้าน PDPA อย่างเป็นทางการ
- ติดตาม ตรวจสอบ และทบทวนผลการดำเนินงานและรายงานความเสี่ยงเป็นระยะ
- สนับสนุนทรัพยากรและการฝึกอบรมที่จำเป็นต่อการคุ้มครองข้อมูล

การรับรอง

นโยบายนี้ได้รับการอนุมัติและรับรองโดยคณะผู้บริหารระดับสูงของบริษัทฯ ในการประชุมครั้งที่ 2/2568 เมื่อวันที่ 1 มกราคม 2568

ลงชื่อ.....

(นายสมชาย ดีมาก)

ประธานกรรมการบริหาร

อ้างอิงทางกฎหมาย

- มาตรา 37 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
- ประกาศมาตรการรักษาความมั่นคงปลอดภัยฯ ข้อ 4(7)
- ระเบียบและประกาศอื่น ๆ ที่เกี่ยวข้อง

บทที่ 3

การจัดทำเอกสารด้านนโยบายและแนวปฏิบัติ

นโยบายและแนวปฏิบัติ (Policy & Practice) ถือเป็นหัวใจสำคัญของการคุ้มครองข้อมูลส่วนบุคคลในองค์กร เนื่องจากเป็นกรอบกำหนดทิศทาง มาตรการ และขั้นตอนการดำเนินการที่ชัดเจน เพื่อให้บุคลากรทุกระดับปฏิบัติไปในแนวทางเดียวกันอย่างถูกต้องตามกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) รวมทั้งสอดคล้องกับมาตรฐานสากลและแนวทางปฏิบัติที่ดี (best practices) การมีนโยบายที่เป็นลายลักษณ์อักษรเพียงอย่างเดียวไม่เพียงพอ หากแต่ต้องมีแนวปฏิบัติ (Standard Operating Procedures: SOPs) ที่สามารถนำไปใช้จริงได้ในทุกขั้นตอนของการจัดการข้อมูล ตั้งแต่การเก็บ ใช้ เผยแพร่ แก้ไข ลบ ไปจนถึงการทำลายข้อมูล การกำหนดนโยบายและแนวปฏิบัติอย่างเป็นระบบยังทำให้บุคลากรเข้าใจบทบาทหน้าที่ของตน สามารถปฏิบัติได้อย่างสอดคล้องและลดความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล

นอกจากนี้ การบังคับใช้นโยบายและแนวปฏิบัติจำเป็นต้องมีการเผยแพร่และสื่อสารอย่างทั่วถึง มีการติดตามผล ตรวจสอบ และทบทวนแก้ไขให้สอดคล้องกับบริบทที่เปลี่ยนแปลงอยู่เสมอ องค์กรที่สามารถแสดงให้เห็นว่ามีนโยบายและแนวปฏิบัติที่ครอบคลุม มีการใช้จริง และมีการทบทวนปรับปรุงอย่างต่อเนื่อง ย่อมได้รับการยอมรับว่ามีระบบการจัดการข้อมูลส่วนบุคคลที่เข้มแข็ง และมีแนวโน้มสูงที่จะผ่านเกณฑ์การตรวจรับรองความสอดคล้อง (Trustmark) ในด้านนี้อย่างครบถ้วน

เพื่อให้การบริหารจัดการข้อมูลส่วนบุคคลในองค์กรมีความชัดเจน โปร่งใส และสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) องค์กรจึงต้องกำหนดนโยบายและแนวปฏิบัติที่เป็นทางการ ครอบคลุมทั้งการเก็บ ใช้ เปิดเผย ลบ และทำลายข้อมูล รวมถึงการสื่อสาร การบังคับใช้งาน และการทบทวน ปรับปรุงอย่างต่อเนื่อง ตารางด้านล่างสรุปหัวข้อสำคัญของการจัดทำและดำเนินการด้านนโยบายและแนวปฏิบัติ PDPA พร้อมแนวทางปฏิบัติ เอกสาร/หลักฐานที่ต้องมี และเกณฑ์การให้คะแนนเพื่อประเมินความครบถ้วนและสอดคล้องของมาตรการดังกล่าว

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
2.1 จัดทำนโยบาย PDPA อย่างเป็นทางการ	จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมการเก็บ ใช้ เปิดเผย ลบ และทำลายข้อมูล	เอกสาร “นโยบายคุ้มครองข้อมูลส่วนบุคคล” (Privacy Policy) ที่ลงนามโดยผู้บริหารสูงสุด	มีนโยบายเป็นลายลักษณ์อักษร เผยแพร่ภายในและภายนอกองค์กร
2.2 กำหนดแนวปฏิบัติ (SOPs)	จัดทำคู่มือหรือขั้นตอนปฏิบัติงานสำหรับงานสำคัญ เช่น การรับคำขอสิทธิ การลบข้อมูล การจัดการข้อมูลสำรอง	เอกสาร SOPs/คู่มือปฏิบัติ	มี SOP ครอบคลุมครบถ้วน ใช้งานจริง และเป็นปัจจุบัน
2.3 ความสอดคล้องกับกฎหมาย	ตรวจสอบให้นโยบายและ SOPs สอดคล้องกับ PDPA และกฎหมายที่เกี่ยวข้อง	บันทึกการตรวจสอบกฎหมาย เอกสาร Legal Review	มีหลักฐานการตรวจสอบและอัปเดตตามกฎหมายใหม่
2.4 การเผยแพร่และสื่อสาร	สื่อสารนโยบายและ SOPs ไปยังบุคลากรและผู้มีส่วนเกี่ยวข้องอย่างทั่วถึง	เอกสารประกาศ แจ้งเวียน อีเมล เว็บไซต์	มีการเผยแพร่หลายช่องทาง ตรวจสอบการรับรู้ของบุคลากรได้
2.5 การบังคับใช้ อย่างเป็นทางการเป็นรูปธรรม	นำแนวปฏิบัติไปใช้จริงในหน่วยงาน/งานประจำ	หลักฐานการปฏิบัติ เช่น บันทึกการลบข้อมูล รายงานเหตุการณ์	มีกรณีปฏิบัติจริง (Case Example) ยืนยันการใช้งาน
2.6 การทบทวนและปรับปรุง	ทบทวน/แก้ไขนโยบายและ SOPs อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีกฎหมาย/บริบทเปลี่ยน	บันทึกการประชุม ทะเบียนแก้ไขเวอร์ชัน (Version Control)	มีหลักฐานว่ามีการทบทวน/ปรับปรุงอย่างต่อเนื่อง

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
2.7 การจัดทำคู่มือบุคลากร	จัดทำคู่มือหรือแนวปฏิบัติสำหรับบุคลากร เพื่อให้เข้าใจหน้าที่และข้อห้าม	เอกสาร “คู่มือบุคลากรด้าน PDPA”	มีคู่มือแจก/เผยแพร่ตรวจสอบได้ว่าใช้จริง
2.8 การกำหนดบทลงโทษ/ข้อวินัย	ระบุความผิดและบทลงโทษสำหรับการละเมิดนโยบาย	เอกสารข้อบังคับ/วินัยภายใน	มีข้อบังคับ/บทลงโทษที่ใช้บังคับได้จริง
2.9 การเชื่อมโยงกับการบริหารความเสี่ยง	ผูกโยงนโยบายและแนวปฏิบัติเข้ากับระบบการบริหารความเสี่ยงองค์กร	เอกสาร Risk Register ที่อ้างอิงนโยบาย	มีการบันทึกและติดตามความเสี่ยงตามนโยบาย
2.10 การตรวจสอบภายใน (Internal Review)	ตรวจสอบว่านโยบายและ SOPs ถูกนำไปใช้จริง	รายงานตรวจสอบภายใน/แบบสอบถามบุคลากร	มีรายงาน Audit/Review พร้อมข้อเสนอแนะ

การจัดทำเอกสารตามเกณฑ์แต่ละข้อ

2.1.2 องค์กรจัดทำนโยบาย PDPA ครอบคลุมครบถ้วน เช่น วิธีการคุ้มครองข้อมูลส่วนบุคคล การบริหารจัดการข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยฯ รวมถึงการกำหนดหน้าที่แก่พนักงาน

สิ่งที่ต้องทำ: จัดทำนโยบาย PDPA ที่มีประเด็นครอบคลุมครบถ้วน

หลักฐาน: 1) นโยบาย PDPA โดยต้องมีข้อความแสดงเป็นหมวดหมู่ให้เห็นว่า “การบริหารจัดการข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัยของข้อมูล การกำหนดหน้าที่แก่พนักงาน”

สภาพบังคับ: 1) มาตรา 37(1) และประกาศฯ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยฯ ข้อ 4(7)
2) โทษทางปกครองปรับ 3 ล้าน

ตัวอย่างหลักฐานนโยบาย PDPA ฉบับครอบคลุมครบถ้วน (ข้อ 2.1.2)

นโยบายการคุ้มครองข้อมูลส่วนบุคคลและการบริหารจัดการข้อมูลส่วนบุคคล

บริษัท เอ็กเซลเลนซ์ จำกัด

ประกาศเมื่อวันที่ 1 มกราคม 2568

รับรองโดยคณะผู้บริหารระดับสูง

1. การบริหารจัดการข้อมูลส่วนบุคคล

บริษัทฯ มีกรอบการบริหารจัดการข้อมูลส่วนบุคคลที่ชัดเจน เพื่อให้การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเป็นไปตามหลักเกณฑ์และมาตรฐานที่กฎหมายกำหนด

- กำหนดประเภทของข้อมูลส่วนบุคคลที่สามารถเก็บรวบรวมได้
- กำหนดวัตถุประสงค์และขอบเขตของการใช้ข้อมูล
- การจัดทำฐานข้อมูลและการควบคุมการเข้าถึงข้อมูล

(ข้อความสำคัญ) : “นโยบายนี้ครอบคลุมถึงการบริหารจัดการข้อมูลส่วนบุคคลในทุกขั้นตอนของกระบวนการทำงาน”

2. การรักษาความมั่นคงปลอดภัยของข้อมูล

บริษัทฯ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งทางกายภาพและเทคนิคเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต รวมถึงการป้องกันการสูญหายและความเสียหายของข้อมูล

- ใช้ระบบรักษาความปลอดภัยข้อมูล เช่น การเข้ารหัสข้อมูล การจำกัดสิทธิ์เข้าถึง
- การตรวจสอบและบันทึกการเข้าใช้ข้อมูล
- การสำรองข้อมูลและแผนฟื้นฟูข้อมูลเมื่อเกิดเหตุฉุกเฉิน

(ข้อความสำคัญ) : “บริษัทฯ ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทุกประเภท”

3. การกำหนดหน้าที่และความรับผิดชอบแก่พนักงาน

บริษัทฯ กำหนดหน้าที่ความรับผิดชอบชัดเจนแก่พนักงานทุกระดับเกี่ยวกับการปฏิบัติตามนโยบาย PDPA และการคุ้มครองข้อมูลส่วนบุคคล

- พนักงานต้องปฏิบัติตามนโยบายและมาตรการรักษาความปลอดภัยข้อมูล
- มีการอบรมและสร้างความตระหนักรู้ด้าน PDPA เป็นประจำ
- กำหนดบทลงโทษกรณีละเมิดนโยบาย

(ข้อความสำคัญ) : “พนักงานทุกคนมีหน้าที่รับผิดชอบในการรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคล”

การรับรอง

นโยบายนี้ได้รับการรับรองโดยฝ่ายบริหารระดับสูงและมีผลบังคับใช้ตั้งแต่วันที่ประกาศ

ลงชื่อ.....

(นายสมชาย ติมาก)

ประธานกรรมการบริหาร

2.1.3 องค์การจัดทำขั้นตอนการปฏิบัติงาน แนวทางการปฏิบัติงาน และคู่มืออื่น ๆ เพื่อสนับสนุนนโยบาย PDPA และเพื่อใช้เป็นแนวทางปฏิบัติแก่พนักงานและผู้เกี่ยวข้อง

สิ่งที่ต้องทำ: จัดทำคู่มือแยกเป็นแผนกชัดเจน โดยในคู่มือต้องระบุให้ชัดถึง “บทบาท และหน้าที่ความรับผิดชอบของผู้เกี่ยวข้อง”

หลักฐาน: 1) ทำคู่มือ หรือแนวปฏิบัติด้าน PDPA ของแต่ละแผนก

สภาพบังคับ: ไม่มีกฎหมายกำหนด

คู่มือการปฏิบัติงานด้าน PDPA

ฝ่ายบุคคล (Human Resources Department)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและขั้นตอนปฏิบัติงานของฝ่ายบุคคลในการบริหารจัดการข้อมูลส่วนบุคคลของพนักงาน ให้เป็นไปตามนโยบาย PDPA และกฎหมายที่เกี่ยวข้อง

2. ขอบเขต

ครอบคลุมการเก็บรวบรวม ใช้ เปิดเผย และเก็บรักษาข้อมูลส่วนบุคคลของพนักงานทุกประเภท

3. บทบาทและหน้าที่ความรับผิดชอบ

หัวหน้าฝ่ายบุคคล

- รับผิดชอบดูแลการปฏิบัติตามนโยบาย PDPA ภายในฝ่าย
- อนุมัติและทบทวนคู่มือและแนวทางการปฏิบัติงาน
- รับผิดชอบการรายงานปัญหาและความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของพนักงานต่อ DPO

เจ้าหน้าที่ฝ่ายบุคคล

- ปฏิบัติตามคู่มือและนโยบาย PDPA อย่างเคร่งครัด
- ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลของพนักงานโดยได้รับความยินยอม
- รักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคล
- รายงานเหตุการณ์ที่อาจก่อให้เกิดความเสี่ยงต่อข้อมูลส่วนบุคคล

4. ขั้นตอนการปฏิบัติงาน

4.1 การเก็บรวบรวมข้อมูลส่วนบุคคล

- กำหนดประเภทข้อมูลที่จำเป็นต้องเก็บ เช่น ข้อมูลส่วนตัว ข้อมูลติดต่อ ข้อมูลทางการเงิน
- ขอความยินยอมจากพนักงานอย่างชัดเจนและเป็นลายลักษณ์อักษร
- บันทึกการขอความยินยอมในระบบบริหารจัดการ

4.2 การใช้และเปิดเผยข้อมูล

- ใช้ข้อมูลตามวัตถุประสงค์ที่แจ้งไว้ในนโยบายและแบบฟอร์มความยินยอม
- ห้ามเปิดเผยข้อมูลแก่บุคคลภายนอกโดยไม่ได้รับอนุญาต เว้นแต่จะมีข้อกำหนดกำหนด

4.3 การเก็บรักษาข้อมูล

- เก็บข้อมูลในระบบที่มีมาตรการรักษาความปลอดภัย เช่น การเข้ารหัส การจำกัดสิทธิ์
- จัดเก็บข้อมูลตามระยะเวลาที่กฎหมายกำหนดและทำลายข้อมูลที่หมดอายุตามมาตรฐาน

4.4 การฝึกอบรม

จัดอบรมพนักงานในฝ่ายบุคคลเกี่ยวกับ PDPA อย่างน้อยปีละ 1 ครั้ง

5. การรายงานและการจัดการเหตุการณ์

- รายงานเหตุการณ์ละเมิดข้อมูลทันทีต่อ DPO
- บันทึกเหตุการณ์และมาตรการที่ดำเนินการแก้ไข
- วิเคราะห์ความเสี่ยงและเสนอแนะแนวทางป้องกัน

แนบ: ตัวอย่างแบบฟอร์มขอความยินยอมการเก็บข้อมูลพนักงาน

คู่มือการปฏิบัติงานด้าน PDPA

ฝ่ายลูกค้าหรือสมาชิก (Customer Service Department)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและขั้นตอนปฏิบัติงานของฝ่ายลูกค้าหรือสมาชิกในการจัดการข้อมูลส่วนบุคคลของลูกค้าและสมาชิกอย่างปลอดภัยและเป็นไปตามนโยบาย PDPA

2. ขอบเขต

ครอบคลุมการเก็บ ใช้ เปิดเผย และรักษาข้อมูลส่วนบุคคลของลูกค้าและสมาชิกในทุกช่องทางที่เกี่ยวข้อง

3. บทบาทและหน้าที่ความรับผิดชอบ

หัวหน้าฝ่ายลูกค้าหรือสมาชิก

- กำกับดูแลและรับผิดชอบการดำเนินการตามนโยบาย PDPA ในฝ่าย
- ทบทวนและอนุมัติแนวทางปฏิบัติงานด้าน PDPA
- รายงานความเสี่ยงและเหตุการณ์เกี่ยวกับข้อมูลส่วนบุคคลแก่ DPO

เจ้าหน้าที่ฝ่ายลูกค้าหรือสมาชิก

- ดำเนินการตามแนวทางและขั้นตอนในคู่มือ PDPA อย่างเคร่งครัด
- ขอความยินยอมจากลูกค้าหรือสมาชิกก่อนเก็บรวบรวมข้อมูล
- รักษาความลับและความปลอดภัยของข้อมูลลูกค้า
- แจ้งเหตุการณ์ละเมิดข้อมูลและความเสี่ยงต่อหัวหน้าฝ่ายทันที

4. ขั้นตอนการปฏิบัติงาน

4.1 การเก็บรวบรวมข้อมูลลูกค้า/สมาชิก

- แจ้งวัตถุประสงค์การเก็บข้อมูลอย่างชัดเจน
- ขอความยินยอมก่อนเก็บข้อมูลทุกครั้ง
- บันทึกการให้ความยินยอมในระบบ CRM หรือฐานข้อมูลสมาชิก

4.2 การใช้และเปิดเผยข้อมูล

- ใช้ข้อมูลเพื่อประโยชน์ที่ได้แจ้งลูกค้าหรือสมาชิกไว้เท่านั้น
- หลีกเลี่ยงการเปิดเผยข้อมูลแก่บุคคลที่ไม่ได้รับอนุญาต

4.3 การเก็บรักษาข้อมูล

- จัดเก็บข้อมูลในระบบที่มีการป้องกันความปลอดภัยอย่างเข้มงวด
- กำหนดระยะเวลาการเก็บข้อมูลและทำลายข้อมูลตามนโยบายองค์กร

4.4 การอบรมและสร้างความตระหนัก

- ฝึกอบรมพนักงานในฝ่ายลูกค้าหรือสมาชิกอย่างน้อยปีละ 1 ครั้ง

- จัดทำคู่มือและอัปเดตเป็นประจำ

5. การจัดการเหตุการณ์และรายงาน

- รายงานเหตุการณ์ละเมิดข้อมูลหรือความเสี่ยงต่อหัวหน้าฝ่ายและ DPO ทันที
- บันทึกและติดตามการดำเนินการแก้ไข
- ประเมินความเสี่ยงและปรับปรุงมาตรการ

แนบ: ตัวอย่างแบบฟอร์มขอความยินยอมเก็บข้อมูลลูกค้าหรือสมาชิก

2.1.4 องค์กรจัดทำนโยบาย PDPA และแนวปฏิบัติสำหรับ PDPA มีการกำหนดบทบาทและหน้าที่ความรับผิดชอบชัดเจน

สิ่งที่ต้องทำ: จัดทำนโยบาย PDPA ที่มีประเด็นครอบคลุมครบถ้วน

หลักฐาน: 1) นโยบาย PDPA โดยต้องมีข้อความแสดงเป็นหมวดหมู่ให้เห็นว่า “การบริหารจัดการข้อมูลส่วนบุคคล การรักษาความปลอดภัยของข้อมูล การกำหนดหน้าที่แก่พนักงาน”

สภาพบังคับ: 1) มาตรา 37(1) และประกาศฯ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยฯ ข้อ 4(7)
2) โทษทางปกครองปรับ 3 ล้าน

นโยบายการคุ้มครองข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อกำหนดกรอบการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) และความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในองค์กรอย่างครบถ้วน โดยให้สอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้อง พร้อมทั้งส่งเสริมให้พนักงานและผู้เกี่ยวข้องปฏิบัติตามบทบาทหน้าที่อย่างเคร่งครัด เพื่อปกป้องข้อมูลส่วนบุคคลจากการเข้าถึง การเปิดเผย หรือการใช้ที่ไม่เหมาะสม รวมถึงลดความเสี่ยงที่อาจเกิดขึ้น

2. ขอบเขต

นโยบายนี้ครอบคลุมการบริหารจัดการข้อมูลส่วนบุคคลขององค์กรทุกประเภท ทั้งข้อมูลที่ได้รับจากลูกค้า สมาชิก พนักงาน และผู้มีส่วนได้เสียทุกฝ่าย รวมทั้งครอบคลุมระบบ เทคโนโลยี กระบวนการทำงาน และพนักงานที่เกี่ยวข้อง

3. นโยบายหลัก

3.1 การบริหารจัดการข้อมูลส่วนบุคคล

- องค์กรจะดำเนินการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ชัดเจน โปร่งใส และได้รับความยินยอมจากเจ้าของข้อมูล
- กำหนดบทบาทและความรับผิดชอบของพนักงานและผู้เกี่ยวข้องในแต่ละขั้นตอนของการจัดการข้อมูล เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและถูกต้องตามกฎหมาย
- จัดให้มีระบบการจัดเก็บข้อมูลส่วนบุคคลอย่างเป็นระบบ และสามารถตรวจสอบได้

3.2 การรักษาความมั่นคงปลอดภัยของข้อมูล

- ใช้มาตรการควบคุมการเข้าถึงข้อมูลอย่างเคร่งครัด โดยกำหนดสิทธิ์ตามบทบาทหน้าที่ (Role-Based Access Control) และบังคับใช้ระบบยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication)
- ดำเนินการเข้ารหัสข้อมูลทั้งระหว่างการส่งและการจัดเก็บ เพื่อป้องกันการถูกดักฟังหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
- ติดตั้งและอัปเดตระบบรักษาความปลอดภัย เช่น ไฟร์วอลล์ ซอฟต์แวร์ป้องกันไวรัส และระบบตรวจจับการบุกรุก (IDS/IPS) อย่างสม่ำเสมอ

สำรองข้อมูลอย่างสม่ำเสมอ และเก็บรักษาในสถานที่ปลอดภัยเพื่อป้องกันข้อมูลสูญหายหรือเสียหาย

3.3 การจัดการความเสี่ยงและการกำกับดูแล

- ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลอย่างสม่ำเสมอ พร้อมดำเนินการแก้ไขและป้องกันตามความเหมาะสม
- จัดให้มีการตรวจสอบและทบทวนนโยบาย รวมทั้งกระบวนการดำเนินงานทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญ
- จัดให้มีการอบรมและให้ความรู้แก่พนักงานเกี่ยวกับนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยอย่างต่อเนื่อง
- กำหนดขั้นตอนการรับมือและรายงานเหตุการณ์ละเมิดข้อมูล (Data Breach) อย่างชัดเจน พร้อมทั้งรับมือเหตุการณ์เพื่อดำเนินการแก้ไขอย่างรวดเร็ว

3.4 การกำหนดบทบาทและหน้าที่ความรับผิดชอบ (Role and Responsibility Definition)

องค์กรกำหนดบทบาทและหน้าที่ความรับผิดชอบของแต่ละหน่วยงานและบุคลากรที่เกี่ยวข้องอย่างชัดเจน เพื่อสนับสนุนนโยบาย PDPA และการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

ฝ่ายบริหารระดับสูง

- รับผิดชอบในการรับรองและสนับสนุนการดำเนินงานตามนโยบาย PDPA และมาตรการรักษาความมั่นคงปลอดภัย

- มอบหมายทรัพยากรที่เพียงพอสำหรับการปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคล
- กำกับดูแลให้เกิดการปฏิบัติตามนโยบายอย่างต่อเนื่องและเป็นระบบ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และคณะทำงาน

- ทำหน้าที่ตรวจสอบและติดตามการปฏิบัติตามกฎหมาย PDPA
- ให้คำปรึกษา แนะนำ และประสานงานระหว่างหน่วยงานต่าง ๆ เพื่อให้การจัดการข้อมูลเป็นไปตามมาตรฐาน
- รายงานปัญหาและความเสี่ยงที่เกิดขึ้นให้ฝ่ายบริหารรับทราบ

ฝ่ายไอที

- รับผิดชอบการจัดการด้านเทคนิค เช่น การตั้งค่าระบบรักษาความปลอดภัย การควบคุมการเข้าถึงข้อมูล การสำรองข้อมูล และการเฝ้าระวังภัยคุกคามทางไซเบอร์
- ดูแลระบบเครือข่ายและอุปกรณ์ที่เกี่ยวข้องให้ปลอดภัยและทันสมัย

ฝ่ายบุคคล

- ดูแลการจัดเก็บและคุ้มครองข้อมูลส่วนบุคคลของพนักงาน
- จัดอบรมและสร้างความตระหนักรู้ให้กับพนักงานเรื่อง PDPA และการรักษาความมั่นคงปลอดภัยของข้อมูล

กลุ่มปฏิบัติการและพนักงานในฝ่ายงานต่าง ๆ

- ปฏิบัติตามแนวปฏิบัติและคู่มือที่กำหนดไว้เพื่อคุ้มครองข้อมูลส่วนบุคคลและรักษาความมั่นคงปลอดภัยของข้อมูล
- รายงานปัญหา หรือเหตุการณ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลให้เจ้าหน้าที่ที่รับผิดชอบทราบโดยทันที

4. ข้อกำหนดและบทลงโทษ

องค์กรจะปฏิบัติตามมาตรา 37 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และประกาศฯ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ข้อ 4(7) อย่างเคร่งครัด พร้อมดำเนินมาตรการทางปกครองตามกฎหมาย หากพบการละเมิดนโยบายนี้

5. การทบทวนนโยบาย

นโยบายนี้จะได้รับการทบทวนและปรับปรุงทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เพื่อให้สอดคล้องกับกฎหมายและเทคโนโลยีที่เปลี่ยนแปลงไป

2.2.1 องค์กรมีการทบทวนนโยบาย PDPA และแนวปฏิบัติสำหรับ PDPA ว่าได้มีการปฏิบัติตามรูปแบบและวิธีการที่ได้กำหนดไว้

สิ่งที่ต้องทำ: จัดให้มีกระบวนการทบทวนและอนุมัติทำนโยบายและแนวปฏิบัติ PDPA และได้ผลเป็น โดยต้องมีการกำหนดเวลาแน่นอน

หลักฐาน: 1) ต้องทำรายงานการประชุมทบทวน และอนุมัตินโยบายและแนวปฏิบัติ โดยต้องมีข้อความแสดงเป็นหมวดหมู่ให้เห็นว่า “การบริหารจัดการข้อมูลส่วนบุคคล การรักษาความปลอดภัยของข้อมูล การกำหนดหน้าที่แก่พนักงาน”

สภาพบังคับ: 1) มาตรา 37(1) และประกาศฯ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยฯ ข้อ 4(7) และข้อ 5
2) โทษทางปกครองปรับ 3 ล้านบาท

รายงานการประชุมทบทวนและอนุมัตินโยบายและแนวปฏิบัติ PDPA

วันที่ประชุม: [ระบุวันที่]

สถานที่: [ระบุสถานที่]

ผู้เข้าร่วมประชุม:

1. [ชื่อ-นามสกุล] ตำแหน่ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
2. [ชื่อ-นามสกุล] ตำแหน่ง ผู้จัดการฝ่ายไอที

3. [ชื่อ-นามสกุล] ตำแหน่ง ผู้จัดการฝ่ายบุคคล
4. [ชื่อ-นามสกุล] ตำแหน่ง ฝ่ายกฎหมาย
5. [ชื่อ-นามสกุล] ตำแหน่ง ผู้บริหารระดับสูง
6. [ชื่อ-นามสกุล] ตำแหน่ง ตัวแทนฝ่ายลูกค้าหรือสมาชิก

วาระที่ 1: การทบทวนและประเมินผลการปฏิบัติตามนโยบาย PDPA

ประเด็นที่ทบทวน:

การบริหารจัดการข้อมูลส่วนบุคคล

- ตรวจสอบความสอดคล้องของการเก็บรวบรวม ใช้ เปิดเผย และลบข้อมูลส่วนบุคคล ตามข้อกำหนดของ PDPA
- รายงานการจัดเก็บข้อมูลและการรับความยินยอมจากเจ้าของข้อมูล
- การปรับปรุงกระบวนการจัดการข้อมูลส่วนบุคคลให้มีความโปร่งใสและปลอดภัยมากขึ้น
- **การรักษาความมั่นคงปลอดภัยของข้อมูล**
- ประเมินมาตรการด้านความมั่นคงปลอดภัยที่ใช้อยู่ในปัจจุบัน เช่น การควบคุมการเข้าถึงข้อมูล การเข้ารหัสข้อมูล การสำรองข้อมูล และระบบตรวจจับการบุกรุก
- ตรวจสอบผลการทดสอบความปลอดภัยระบบ (Security Testing) และการตรวจสอบช่องโหว่ (Vulnerability Assessment)
- การอบรมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยให้กับพนักงาน

การกำหนดหน้าที่และบทบาทของพนักงาน

- ทบทวนบทบาทความรับผิดชอบของฝ่ายที่เกี่ยวข้อง ได้แก่ ฝ่ายบริหาร เจ้าหน้าที่คุ้มครองข้อมูล ฝ่ายไอที ฝ่ายบุคคล และพนักงานทั่วไป
- ประเมินผลการปฏิบัติงานและความเข้าใจต่อบทบาทที่ได้รับมอบหมาย
- การแจ้งเตือนและจัดการกับปัญหาการปฏิบัติงานที่พบ

วาระที่ 2: การอนุมัตินโยบายและแนวปฏิบัติ PDPA ฉบับปรับปรุง

- คณะกรรมการรับรองว่า นโยบายและแนวปฏิบัติได้ผ่านการทบทวนตามกรอบเวลาที่กำหนดอย่างน้อยปีละ 1 ครั้ง
- รับรองความครบถ้วนและเหมาะสมของนโยบายในแง่ของการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัย

- เห็นชอบให้นำแนวปฏิบัติและนโยบายฉบับปรับปรุงไปใช้จริงทันที และกำหนดให้มีการติดตามผลการปฏิบัติอย่างต่อเนื่อง

วาระที่ 3: กำหนดแผนการดำเนินงานและทบทวนครั้งถัดไป

- กำหนดวันทบทวนครั้งถัดไปในวันที่ [ระบุวันที่] (โดยทั่วไปเป็นระยะเวลาไม่เกิน 12 เดือน)
- มอบหมายให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจัดทำรายงานสรุปผลการดำเนินงานและเสนอแนะแนวทางแก้ไขในกรณีพบปัญหา
- กำหนดมาตรการเสริมสำหรับการอบรมพนักงานและปรับปรุงระบบรักษาความมั่นคงปลอดภัย

สรุปและข้อเสนอแนะ

คณะกรรมการเห็นว่าองค์กรปฏิบัติตามนโยบาย PDPA และแนวปฏิบัติอย่างเหมาะสม แต่พบข้อจำกัดบางประการที่ควรเร่งแก้ไข เช่น

- การจัดเก็บความยินยอมบางส่วนยังขาดความสมบูรณ์
- ตรวจสอบและติดตามความปลอดภัยระบบควรเพิ่มความถี่
- เสนอให้ฝ่ายที่เกี่ยวข้องดำเนินการปรับปรุงและรายงานผลในการประชุมครั้งต่อไป

ลงชื่ออนุมัติ

(ลงชื่อ).....

[ชื่อ-นามสกุล] เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

(ลงชื่อ).....

[ชื่อ-นามสกุล] ผู้บริหารระดับสูง

(ลงชื่อ).....

[ชื่อ-นามสกุล] ตัวแทนฝ่ายไอที

(ลงชื่อ).....

[ชื่อ-นามสกุล] ตัวแทนฝ่ายบุคคล

2.2.2 องค์กรมีการทบทวนนโยบาย PDPA และแนวปฏิบัติสำหรับ PDPA ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มีความเป็นปัจจุบันและเหมาะสมตามจุดประสงค์และบริบทองค์กร

- สิ่งที่ต้องทำ: จัดให้มีการประชุมเพื่อทบทวนนโยบายและแนวปฏิบัติ โดยต้องประเมินความเหมาะสมของกระบวนการปฏิบัติงานให้เป็นไปตามนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลตามกรอบระยะเวลาที่แน่นอน
- หลักฐาน: 1) รายงานการประชุมเพื่อทบทวนนโยบายและแนวปฏิบัติ โดยต้องมีข้อความแสดงเป็นหมวดหมู่ให้เห็นว่า
 “ก) มีการทบทวนนโยบายและแนวปฏิบัติ ข) ต้องประเมินกระบวนการปฏิบัติงานซึ่งอาจต้องทำแบบประเมิน ค) ระบุว่ามีการรอบระยะเวลาการดำเนินการทุก ๆ.....เดือน”
- สภาพบังคับ: 1) มาตรา 37(1) และประกาศฯ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยฯ ข้อ 4(7) และข้อ 5
 2) โทษทางปกครองปรับ 3 ล้านบาท

รายงานการประชุมทบทวนนโยบายและแนวปฏิบัติ PDPA

หัวข้อ: รายงานการประชุมทบทวนและประเมินความเหมาะสมของนโยบายและแนวปฏิบัติ PDPA

วันที่ประชุม: [ระบุวันที่]

สถานที่: [ระบุสถานที่]

ผู้เข้าร่วมประชุม:

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- ผู้จัดการฝ่ายไอที
- ผู้จัดการฝ่ายบุคคล
- ฝ่ายกฎหมาย
- ผู้บริหารระดับสูง
- ตัวแทนฝ่ายลูกค้าหรือสมาชิก

วาระที่ 1: การทบทวนนโยบายและแนวปฏิบัติ PDPA (ก)

- คณะกรรมการได้ทำการทบทวนเนื้อหาและความครอบคลุมของนโยบายและแนวปฏิบัติ PDPA ฉบับปัจจุบัน เพื่อให้มั่นใจว่ายังคงสอดคล้องกับข้อกำหนดและบริบทขององค์กร
- มีการปรับปรุงเนื้อหา นโยบายให้ทันสมัย ครอบคลุมการบริหารจัดการข้อมูลส่วนบุคคล การรักษาความมั่นคงปลอดภัย และบทบาทหน้าที่ของพนักงานอย่างครบถ้วน
- มีการระบุอย่างชัดเจนถึงกระบวนการขอความยินยอม การจัดการข้อมูล และการตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Data Breach Response)

วาระที่ 2: การประเมินกระบวนการปฏิบัติงานตามนโยบาย PDPA (ข)

- มีการนำแบบประเมินมาตรฐานการปฏิบัติงานด้านคุ้มครองข้อมูลส่วนบุคคลมาใช้ตรวจสอบการดำเนินงานของแต่ละฝ่ายที่เกี่ยวข้อง

- แบบประเมินครอบคลุมหัวข้อหลัก เช่น การปฏิบัติตามนโยบายการเก็บรวบรวมข้อมูล การรักษาความลับ การบริหารจัดการความเสี่ยงด้านข้อมูล และการอบรมพนักงาน
- ผลการประเมินแสดงให้เห็นถึงความสอดคล้องของกระบวนการกับนโยบาย PDPA โดยมีข้อเสนอแนะสำหรับการพัฒนาในส่วนที่ยังมีช่องว่าง
- มีการกำหนดให้ฝ่ายที่เกี่ยวข้องจัดทำรายงานการปฏิบัติตามแนวทางและนำเสนอผลต่อคณะกรรมการในการประชุมครั้งต่อไป

วาระที่ 3: การกำหนดกรอบระยะเวลาการทบทวนและติดตามผล (ค)

- คณะกรรมการเห็นชอบให้กำหนดกรอบการทบทวนและประเมินผลนโยบายและแนวปฏิบัติ PDPA อย่างน้อยทุก ๆ 12 เดือน เพื่อรักษาความทันสมัยและเหมาะสมกับสภาพแวดล้อมองค์กรที่เปลี่ยนแปลง
- มีการมอบหมายเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เป็นผู้รับผิดชอบหลักในการจัดทำตารางกำหนดการประชุมทบทวนประจำปี พร้อมจัดทำรายงานสรุปผลและข้อเสนอแนะต่าง ๆ
- ในกรณีพบประเด็นใหม่ ๆ ที่มีผลกระทบต่อการทำงานของข้อมูลส่วนบุคคล หรือมีการเปลี่ยนแปลงกฎหมาย คณะกรรมการจะจัดประชุมพิเศษเพื่อทบทวนนโยบายทันที

สรุปและข้อเสนอแนะ

- ผลการทบทวนและประเมินความเหมาะสมของนโยบายและแนวปฏิบัติ PDPA อยู่ในระดับที่น่าพอใจ แต่ต้องเสริมสร้างความตระหนักและการอบรมให้ครอบคลุมทุกฝ่ายอย่างต่อเนื่อง
- เน้นย้ำความสำคัญของการติดตามผลและรายงานความคืบหน้าอย่างเป็นระบบ
- เสนอให้ดำเนินการประเมินผลการปฏิบัติงานด้วยแบบประเมินคุณภาพทุก 6 เดือน เพื่อเพิ่มความเข้มข้นของการควบคุมภายใน

ลงชื่ออนุมัติ

(ลงชื่อ).....

[ชื่อ-นามสกุล] เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

(ลงชื่อ).....

[ชื่อ-นามสกุล] ผู้บริหารระดับสูง

(ลงชื่อ).....

[ชื่อ-นามสกุล] ตัวแทนฝ่ายไอที

ตัวอย่างการทำเอกสาร 2.2.3 องค์การมีการทบทวนนโยบาย PDPA และแนวปฏิบัติสำหรับ PDPA ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มีความเป็นปัจจุบันและเหมาะสมตามจุดประสงค์และบริบทองค์กร

รายงานการประชุมทบทวนนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล

ครั้งที่ 1/2568 วันที่ประชุม: 15 พฤษภาคม 2568 เวลา: 09.30 – 11.45 น. สถานที่: ห้องประชุม 3 อาคาร บริหารกลาง

ผู้เข้าร่วมประชุม

1. นาย A – ประธานการประชุมและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
2. นาย B – ผู้แทนฝ่ายกฎหมาย
3. นางสาว C – ผู้แทนฝ่ายเทคโนโลยีสารสนเทศ
4. นางสาว D – ผู้แทนฝ่ายทรัพยากรบุคคล
5. นาย E – ผู้แทนฝ่ายการตลาด
6. นางสาว F – ผู้แทนฝ่ายบริการลูกค้า
7. นาย G – ผู้แทนฝ่ายพัฒนาผลิตภัณฑ์
8. นาย H – ผู้แทนฝ่ายความมั่นคงปลอดภัยสารสนเทศ
9. คณะทำงานฝ่ายสนับสนุนด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งสิ้น 12 คน

ระเบียบวาระการประชุม

วาระที่ 1: การทบทวนนโยบายการคุ้มครองข้อมูลส่วนบุคคล

ที่ประชุมได้ร่วมกันพิจารณานโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับปรับปรุงล่าสุด (เวอร์ชันปี 2567) โดยพิจารณาองค์ประกอบสำคัญ ได้แก่ ขอบเขตของข้อมูลส่วนบุคคล แนวทางการเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล และระยะเวลาการจัดเก็บข้อมูล

มติที่ประชุมเห็นว่านโยบายดังกล่าวยังคงมีความเหมาะสม ครอบคลุม และสอดคล้องกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และแนวปฏิบัติตามประกาศคณะกรรมการ ดังนั้น จึง มีมติให้คงเนื้อหาของนโยบายไว้ตามเดิม พร้อมเสนอให้ปรับปรุงและทบทวนแนวปฏิบัติบางประการให้ ทันสมัยยิ่งขึ้น

วาระที่ 2: การทบทวนแนวปฏิบัติ

2.1 แนวปฏิบัติเรื่องการขอความยินยอม (Consent Management)

ที่ประชุมพิจารณาแนวทางการขอความยินยอมในช่องทางต่าง ๆ ได้แก่ เว็บไซต์ แอปพลิเคชัน แบบฟอร์มกระดาษ และการสนทนาทางโทรศัพท์ พบว่ามีความไม่สอดคล้องกันในด้านถ้อยคำ การบันทึก ข้อมูล และการจัดเก็บหลักฐานการให้ความยินยอม

ที่ประชุมมีมติให้ดำเนินการดังนี้

- กำหนดข้อความมาตรฐานในการขอความยินยอมสำหรับแต่ละวัตถุประสงค์
- จัดทำระบบจัดเก็บและเรียกดูข้อมูลความยินยอม (Consent Log) แบบรวมศูนย์

- มอบหมายให้ฝ่ายเทคโนโลยีสารสนเทศและ DPO ร่วมกันพัฒนาเครื่องมือสนับสนุน

2.2 แนวปฏิบัติเรื่องการแจ้งเหตุข้อมูลรั่วไหล (Data Breach Notification)

ที่ประชุมได้พิจารณาแนวทางการแจ้งเหตุข้อมูลรั่วไหลภายในองค์กร พบว่ายังไม่มีแบบฟอร์มแจ้งเหตุที่ชัดเจน และเจ้าหน้าที่บางหน่วยงานยังไม่เข้าใจขั้นตอนการดำเนินการที่ถูกต้อง

ที่ประชุมมีมติดังนี้

- จัดทำแบบฟอร์มแจ้งเหตุข้อมูลรั่วไหลและคู่มือการใช้งาน
- จัดกิจกรรมจำลองสถานการณ์การรับมือเหตุข้อมูลรั่วไหลอย่างน้อยปีละ 1 ครั้ง
- ให้ฝ่ายความมั่นคงปลอดภัยสารสนเทศจัดทำรายงานความเสี่ยงเพื่อเฝ้าระวัง

วาระที่ 3: การประเมินกระบวนการปฏิบัติงานให้สอดคล้องกับนโยบาย

ที่ประชุมดำเนินการประเมินตนเองตามหัวข้อดังนี้

1. ความเข้าใจนโยบายและบทบาทหน้าที่ของแต่ละฝ่าย
2. ระบบจัดเก็บและควบคุมการเข้าถึงข้อมูล
3. การขอความยินยอมและจัดเก็บหลักฐาน
4. การลบหรือทำลายข้อมูลที่หมดอายุ
5. การรับและตอบคำร้องขอใช้สิทธิของเจ้าของข้อมูล
6. ความพร้อมในการรับมือเหตุการณ์ข้อมูลรั่วไหล

จากผลการประเมิน พบว่าโดยรวมมีความสอดคล้องกับนโยบายและข้อกำหนดทางกฎหมาย อย่างไรก็ตาม ยังพบจุดที่ควรปรับปรุง ได้แก่

- ควรจัดให้มีระบบการลบข้อมูลอัตโนมัติเมื่อครบกำหนดเวลา
- ควรจัดเก็บแบบฟอร์มคำร้องขอเจ้าของข้อมูลในระบบกลาง (DSR Log)
- ควรจัดการฝึกอบรมพนักงานทุกฝ่ายให้เข้าใจขั้นตอนการแจ้งเหตุข้อมูลรั่วไหล

มติที่ประชุมเห็นชอบให้ดำเนินการปรับปรุงกระบวนการตามข้อเสนอข้างต้น และมอบหมายให้แต่ละฝ่ายรับผิดชอบภายในระยะเวลาที่เหมาะสม

วาระที่ 4: การกำหนดกรอบระยะเวลาการทบทวน

ที่ประชุมได้พิจารณาแนวทางการทบทวนนโยบายและแนวปฏิบัติประจำปี โดยอ้างอิงตาม

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(1)
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ข้อ 4(7) และข้อ 5

ที่ประชุมมีมติให้ดำเนินการทบทวนนโยบายและแนวปฏิบัติอย่างน้อยปีละ 1 ครั้ง โดยให้จัดประชุมทบทวนรอบถัดไปภายในเดือนพฤษภาคม 2569

มติที่ประชุมโดยสรุป

1. เห็นชอบให้คงเนื้อหา นโยบายการคุ้มครองข้อมูลส่วนบุคคลเดิม
2. ปรับปรุงแนวปฏิบัติในเรื่องการขอความยินยอม และการแจ้งเหตุข้อมูลรั่วไหล

3. พัฒนาระบบจัดเก็บคำร้องและการลบข้อมูลให้สอดคล้องกับนโยบาย
4. กำหนดให้ทบทวนนโยบายและแนวปฏิบัติทุก 12 เดือน

ลงชื่อ.....

นาย A

ประธานการประชุม / เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

วันที่ลงนาม: 16 พฤษภาคม 2568

ตัวอย่างการทำเอกสาร 2.2.3 องค์กรมีการทบทวนนโยบาย PDPA และแนวปฏิบัติสำหรับ PDPA อย่างไม่ล่าช้า เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อองค์กรที่สำคัญ ๆ การตัดสินใจของสำนักงานคุ้มครองข้อมูลส่วนบุคคล หรือการเปลี่ยนแปลงในแนวทางปฏิบัติของหน่วยงานที่กำลังดูแล

รายงานการประชุมทบทวนนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล (กรณีมีการเปลี่ยนแปลงสำคัญ)

ครั้งที่ 2/2568

วันที่ประชุม: 5 เมษายน 2568

เวลา: 10.00 – 12.00 น.

สถานที่: ห้องประชุม 2 ชั้น 5 อาคารบริหารกลาง

ผู้เข้าร่วมประชุม

1. นาย A – ประธานการประชุมและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
2. นาย B – กรรมการผู้จัดการ (ผู้บริหารระดับอาวุโส)
3. นางสาว C – ผู้แทนฝ่ายกฎหมาย
4. นางสาว D – ผู้แทนฝ่ายเทคโนโลยีสารสนเทศ
5. นาย E – ผู้แทนฝ่ายทรัพยากรบุคคล
6. นาย F – ผู้แทนฝ่ายการตลาด
7. นางสาว G – ผู้แทนฝ่ายความมั่นคงปลอดภัยสารสนเทศ
8. คณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล รวมจำนวนผู้เข้าร่วม 14 คน

เหตุผลในการจัดประชุม

สืบเนื่องจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ได้ออกประกาศเพิ่มเติมในเดือนมีนาคม 2568 เกี่ยวกับแนวปฏิบัติในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในระบบ

ออนไลน์ และกำหนดให้ต้องมีการแสดงสิทธิของเจ้าของข้อมูลส่วนบุคคลในลักษณะที่เข้าใจง่าย และให้สามารถถอนความยินยอมได้ตลอดเวลา

นอกจากนี้ยังมีข้อเสนอแนะจากสำนักงานฯ เพิ่มเติมเกี่ยวกับการจัดเก็บข้อมูลผู้เยาว์และข้อจำกัดในการใช้ข้อมูลเพื่อการตลาดเชิงพฤติกรรม ซึ่งถือเป็นการเปลี่ยนแปลงที่มีนัยสำคัญต่อกระบวนการทำงานขององค์กร

เพื่อให้เป็นไปตามมาตรา 37(1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และข้อ 4(7) และข้อ 5 แห่งประกาศคณะกรรมการฯ เรื่องมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล จึงได้มีการจัดประชุมนี้ขึ้น

ระเบียบวาระการประชุม

วาระที่ 1: การรับทราบการเปลี่ยนแปลงนโยบายหรือประกาศของหน่วยงานกำกับดูแล
ที่ประชุมได้รับทราบประกาศจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ลงวันที่ 18 มีนาคม 2568 เรื่อง

- แนวทางการขอความยินยอมผ่านช่องทางดิจิทัล
- การระบุสิทธิในการถอนความยินยอมของเจ้าของข้อมูล
- คำแนะนำเรื่องการใช้ข้อมูลผู้เยาว์
- แนวทางจำกัดการใช้ข้อมูลส่วนบุคคลเพื่อการตลาดเชิงพฤติกรรม

วาระที่ 2: การประเมินผลกระทบของการเปลี่ยนแปลงต่อองค์กร

คณะทำงานร่วมกับผู้บริหารได้ร่วมกันประเมินว่า ประกาศดังกล่าวจะมีผลกระทบต่อกระบวนการทำงานในด้านต่อไปนี้

- การออกแบบแบบฟอร์มและหน้าเว็บไซต์ที่ขอความยินยอมจากลูกค้า
- ระบบจัดเก็บและถอนความยินยอมในแอปพลิเคชัน
- การโฆษณาและการทำ Remarketing ที่ใช้พฤติกรรมการใช้งาน
- การเก็บข้อมูลเด็กอายุต่ำกว่า 20 ปี ซึ่งองค์กรต้องมีระบบตรวจสอบอายุให้ชัดเจน

มติที่ประชุมเห็นว่า กระบวนการเหล่านี้จำเป็นต้องมีการปรับปรุงในเชิงเทคนิคและนโยบายอย่างเร่งด่วน

วาระที่ 3: การทบทวนและปรับปรุงนโยบายและแนวปฏิบัติขององค์กร

ที่ประชุมมีมติให้ดำเนินการปรับปรุงเอกสารดังต่อไปนี้

1. ปรับแก้คำในแบบฟอร์มความยินยอม (Consent Form) ให้แสดงสิทธิในการถอนความยินยอมอย่างชัดเจน
2. ปรับปรุงนโยบายความเป็นส่วนตัว (Privacy Policy) ให้ระบุวิธีการถอนความยินยอมโดยสะดวก

3. เพิ่มแนวทางการจัดเก็บข้อมูลผู้เยาว์ โดยต้องมีการตรวจสอบอายุและขอความยินยอมจากผู้ปกครอง
4. ปรับปรุงแนวทางการตลาดโดยต้องประเมินความชอบธรรม (Legitimate Interest Assessment) หากใช้ข้อมูลพฤติกรรม
5. ให้ฝ่ายไอทีร่วมกับฝ่ายความมั่นคงปลอดภัยจัดทำระบบจัดเก็บ Log การให้และถอนความยินยอม

วาระที่ 4: การกำหนดกรอบระยะเวลาดำเนินการ

ที่ประชุมมีมติให้ดำเนินการปรับปรุงและทบทวนนโยบายภายใน 45 วันนับจากวันที่ประกาศของสำนักงานคุ้มครองข้อมูลส่วนบุคคลมีผล โดยมีการมอบหมายดังนี้

- ฝ่ายกฎหมายรับผิดชอบจัดทำถ้อยคำใหม่ของนโยบาย
- ฝ่ายเทคโนโลยีสารสนเทศรับผิดชอบพัฒนาระบบถอนความยินยอม
- DPO รับผิดชอบตรวจสอบความสอดคล้องและติดตามผล
- ให้จัดประชุมทบทวนผลอีกครั้งภายในเดือนมิถุนายน 2568

มติที่ประชุมโดยสรุป

1. รับทราบการเปลี่ยนแปลงจากสำนักงานคุ้มครองข้อมูลส่วนบุคคล
2. ประเมินผลกระทบของประกาศต่อองค์กรและเห็นชอบให้ดำเนินการปรับปรุง
3. เห็นชอบให้ปรับนโยบาย แนวปฏิบัติ และระบบที่เกี่ยวข้องภายใน 45 วัน
4. กำหนดให้มีการติดตามผลการดำเนินการอีกครั้งในไตรมาสถัดไป

ลงชื่อ.....

นาย A

ประธานการประชุม / เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

วันที่ลงนาม: 6 เมษายน 2568

ตัวอย่างการทำเอกสาร 2.2.4 องค์กรมีการทบทวนนโยบาย PDPA และแนวปฏิบัติสำหรับ PDPA ขั้นตอนการดำเนินงานที่แสดงให้เห็นถึงการควบคุมเอกสาร รวมถึงเวอร์ชันเอกสาร เจ้าของเอกสาร วันที่ที่ทบทวน และประวัติการเปลี่ยนแปลงเอกสาร

เอกสารในรายการนี้จะแบ่งออกเป็น 3 เรื่อง คือ นโยบายการควบคุมเอกสารด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) กับรายงานการประชุม และหนังสือแต่งตั้งเจ้าของเอกสารด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

นโยบายการควบคุมเอกสารด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการควบคุมเอกสารที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กรให้มีความถูกต้อง เป็นปัจจุบัน สามารถติดตาม ตรวจสอบ และปรับปรุงได้ตามบริบทและข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

2. ขอบเขต

ครอบคลุมถึงเอกสารทั้งหมดที่เกี่ยวข้องกับ PDPA รวมถึงนโยบาย (Policy) แนวปฏิบัติ (Procedure) แบบฟอร์ม (Form) บันทึก (Record) และคำแนะนำ (Guideline) ที่องค์กรจัดทำขึ้น

3. นิยาม

- เอกสารควบคุม (Controlled Document) หมายถึง เอกสารที่อยู่ภายใต้การควบคุมเวอร์ชัน เจ้าของเอกสาร และประวัติการเปลี่ยนแปลง
- เจ้าของเอกสาร (Document Owner) หมายถึง บุคคลที่ได้รับมอบหมายให้รับผิดชอบเนื้อหา และการปรับปรุงเอกสารนั้น ๆ

4. แนวปฏิบัติการควบคุมเอกสาร

4.1 เอกสาร PDPA ทุกฉบับต้องมีหมายเลขเวอร์ชัน กำหนดวันที่มีผลบังคับใช้ และระบุชื่อเจ้าของเอกสารอย่างชัดเจน

4.2 การเปลี่ยนแปลงใด ๆ ต่อเอกสารต้องบันทึกไว้ในส่วน "ประวัติการเปลี่ยนแปลง" (Change History) ของเอกสาร

4.3 ต้องมีการทบทวนเอกสารอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมายหรือแนวปฏิบัติที่เกี่ยวข้อง

4.4 เจ้าของเอกสารต้องรับผิดชอบในการเสนอแก้ไข และนำเสนอการเปลี่ยนแปลงต่อคณะทำงานเพื่ออนุมัติ

5. เวอร์ชันเอกสาร (Document Versioning)

การเปลี่ยนแปลงเอกสารต้องระบุ

- หมายเลขเวอร์ชันใหม่
- วันที่มีผลบังคับใช้
- รายละเอียดของการเปลี่ยนแปลง

6. การเข้าถึงเอกสาร

เอกสารที่ได้รับอนุมัติแล้วต้องจัดเก็บในระบบควบคุมเอกสารกลางขององค์กร และเปิดให้หน่วยงานที่เกี่ยวข้องเข้าถึงได้ตามสิทธิ์

7. การติดตามและประเมินผล

ฝ่าย DPO จะเป็นผู้ติดตามการใช้เอกสารที่ได้รับการควบคุม และรายงานต่อผู้บริหารอย่างน้อยปีละ 1 ครั้ง

รายงานการประชุมทบทวนและปรับปรุงนโยบายการควบคุมเอกสารด้านการคุ้มครองข้อมูลส่วนบุคคล

ครั้งที่: 1/2568

วันที่ประชุม: 20 เมษายน 2568

เวลา: 13.30 – 15.00 น.

สถานที่: ห้องประชุม 3 ชั้น 4 อาคารบริหารกลาง

ผู้เข้าร่วมประชุม:

1. นาย A – ประธานการประชุม (DPO)
2. นาย B – ผู้แทนฝ่ายกฎหมาย
3. นางสาว C – ฝ่ายเทคโนโลยีสารสนเทศ
4. นาย D – ฝ่ายบุคคล
5. นางสาว E – ฝ่ายตรวจสอบภายใน
6. นาย F – ผู้แทนฝ่ายบริหารความเสี่ยง

วาระที่ 1: ทบทวนนโยบายการควบคุมเอกสาร PDPA

ที่ประชุมได้รับทราบร่างนโยบายใหม่ที่จัดทำโดย DPO โดยมีข้อเสนอเพิ่มเติมเกี่ยวกับการระบุชื่อเจ้าของเอกสารในเอกสารทุกฉบับ และการบังคับใช้เวอร์ชันล่าสุดเท่านั้นในระบบการจัดเก็บข้อมูล

วาระที่ 2: การปรับปรุงแนวปฏิบัติ

ได้มีการเพิ่มเติมแนวปฏิบัติการควบคุมเอกสารให้รวมถึง:

- การทบทวนเอกสารอย่างน้อยปีละ 1 ครั้ง
- การจัดทำ "ประวัติการเปลี่ยนแปลง" สำหรับเอกสารทุกฉบับ
- การเก็บรักษาเวอร์ชันเก่าสำหรับการตรวจสอบย้อนหลัง

วาระที่ 3: การแต่งตั้งเจ้าของเอกสาร

ได้มีการแต่งตั้งเจ้าของเอกสารสำหรับนโยบายและแบบฟอร์มที่เกี่ยวข้อง ดังนี้:

- นโยบายหลัก: DPO
- แบบฟอร์มคำร้อง: ฝ่ายกฎหมาย
- แนวปฏิบัติการจัดเก็บข้อมูล: ฝ่าย IT

มติที่ประชุม:

เห็นชอบนโยบายและแนวปฏิบัติที่เสนอ และมอบหมายให้ฝ่าย DPO ร่วมกับแผนกที่เกี่ยวข้องจัดทำเวอร์ชันอย่างเป็นทางการเพื่อบังคับใช้ภายใน 30 วัน

ลงชื่อ:

นาย A

ประธานการประชุม / DPO

วันที่ลงนาม: 21 เมษายน 2568

หนังสือแต่งตั้งเจ้าของเอกสาร
ด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

ตามที่องค์กรได้มีการจัดทำนโยบาย แนวปฏิบัติ และแบบฟอร์มต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรฐานสากล เช่น GDPR และแนวทางของ ICO ประเทศอังกฤษ นั้น

เพื่อให้เอกสารดังกล่าวอยู่ภายใต้การควบคุมที่เหมาะสม มีการกำกับดูแลและปรับปรุงอย่างเป็นระบบ องค์กรจึงขอแต่งตั้งเจ้าของเอกสาร (Document Owner) สำหรับเอกสารที่เกี่ยวข้องกับ PDPA ดังต่อไปนี้

รายการเอกสาร	หน่วยงานที่รับผิดชอบ/เจ้าของเอกสาร
1. นโยบายการคุ้มครองข้อมูลส่วนบุคคล	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
2. แบบฟอร์มคำร้องของเจ้าของข้อมูล	ฝ่ายกฎหมาย
3. แนวปฏิบัติการจัดเก็บข้อมูลส่วนบุคคล	ฝ่ายเทคโนโลยีสารสนเทศ (IT)

หน้าที่ความรับผิดชอบของเจ้าของเอกสาร ได้แก่

1. ดูแลรักษาและปรับปรุงเนื้อหาเอกสารให้ถูกต้อง เป็นปัจจุบัน
2. ทบทวนเอกสารอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมายหรือข้อบังคับที่เกี่ยวข้อง
3. จัดทำประวัติการเปลี่ยนแปลง (Change History) สำหรับเอกสารทุกฉบับ
4. รายงานต่อคณะทำงานด้าน PDPA และผู้บริหารระดับอาวุโสเมื่อมีการเปลี่ยนแปลงสาระสำคัญ

5. ประสานงานกับหน่วยงานอื่น ๆ เพื่อให้การดำเนินงานเป็นไปตามนโยบายที่กำหนด
ทั้งนี้ การแต่งตั้งมีผลตั้งแต่วันที่ลงนามเป็นต้นไป

ลงชื่อ.....

(นาย A)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) / ประธานคณะทำงาน

ลงชื่อ.....

(นาย B)

ผู้แทนฝ่ายกฎหมาย

ลงชื่อ.....

(นางสาว C)

ผู้แทนฝ่ายเทคโนโลยีสารสนเทศ

ลงวันที่: 21 เมษายน 2568

ตัวอย่างการทำเอกสาร 2.2.5 ผู้ที่ทบทวนและอนุมัตินโยบายและแนวปฏิบัติใหม่ ๆ หรือของเดิมที่มีอยู่แล้วมีความอาวุโสเพียงพอ

รายงานการประชุมผู้บริหารอาวุโส

เพื่อทบทวนและอนุมัตินโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล

ครั้งที่: 1/2568

วันประชุม: 10 พฤษภาคม 2568

เวลา: 14.00 – 16.00 น.

สถานที่: ห้องประชุมผู้บริหาร อาคารสำนักงานใหญ่ ชั้น 5

ผู้เข้าร่วมประชุม:

1. นาย X – กรรมการผู้จัดการใหญ่ (ประธานการประชุม)
2. นางสาว Y – รองกรรมการผู้จัดการใหญ่ ฝ่ายกฎหมาย
3. นาย Z – รองกรรมการผู้จัดการใหญ่ ฝ่ายบริหารความเสี่ยง
4. นาย A – เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
5. นาย B – ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ
6. นางสาว C – ผู้อำนวยการฝ่ายสื่อสารองค์กร

วาระที่ 1: การทบทวนและปรับปรุงแนวปฏิบัติการแจ้ง Privacy Notice ให้เหมาะสมกับกลุ่มอายุหรือวัย

ที่ประชุมได้รับทราบข้อเสนอการปรับปรุงแนวปฏิบัติการแจ้งข้อมูลตาม Privacy Notice โดยให้สอดคล้องกับหลักการตาม GDPR และคำแนะนำของ ICO ประเทศอังกฤษ ซึ่งระบุว่าการแจ้งข้อมูลควรมีความเหมาะสมกับความสามารถในการรับรู้ของกลุ่มอายุ เช่น:

- สำหรับเด็กอายุต่ำกว่า 13 ปี ให้ใช้ภาษาที่เรียบง่าย มีภาพประกอบ
- สำหรับผู้สูงอายุ ควรใช้ฟอนต์ขนาดใหญ่และอ่านง่าย พร้อมมีตัวอย่างให้เข้าใจง่าย

ที่ประชุมเห็นชอบให้จัดทำ Privacy Notice แยกตามกลุ่มเป้าหมาย โดยให้ฝ่ายสื่อสารองค์กรร่วมกับ DPO และฝ่ายกฎหมายปรับเอกสารภายในเดือนมิถุนายน 2568

วาระที่ 2: การปรับปรุงแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของข้อมูล โดยกำหนดแนวทางการทำนามแฝง (Pseudonymisation)

ที่ประชุมได้รับทราบร่างแนวปฏิบัติใหม่จากฝ่ายเทคโนโลยีสารสนเทศและฝ่าย DPO ซึ่งอ้างอิงตามมาตรา 32 แห่ง GDPR และคำแนะนำของ European Data Protection Board (EDPB) โดยมีสาระสำคัญ เช่น:

- ข้อมูลส่วนบุคคลบางประเภทที่นำไปวิเคราะห์โดยไม่ต้องระบุตัวตนโดยตรง จะต้องผ่านกระบวนการทำนามแฝงก่อนจัดเก็บหรือประมวลผล
- ข้อมูลตัวจริงและข้อมูลนามแฝงจะต้องแยกเก็บ และมีมาตรการควบคุมการเข้าถึงที่เข้มงวด
- ต้องจัดทำบันทึกการทำนามแฝงและวิธีการถอดรหัสโดยจำกัดผู้มีสิทธิเข้าถึง

ที่ประชุมมีมติเห็นชอบในแนวทางดังกล่าว โดยให้ฝ่าย IT ดำเนินการจัดทำ SOP (Standard Operating Procedure) และให้มีผลใช้ภายในไตรมาสที่ 3 ปี 2568

วาระที่ 3: ทบทวนนโยบายและแนวปฏิบัติเดิมที่มีอยู่แล้ว

ที่ประชุมได้ร่วมกันทบทวนนโยบาย PDPA เวอร์ชัน 1.2 และแนวปฏิบัติเดิมด้านสิทธิของเจ้าของข้อมูล ซึ่งมีการใช้งานตั้งแต่ พ.ศ. 2565 และเห็นควรปรับปรุงเนื้อหาให้สอดคล้องกับคำแนะนำล่าสุดของสำนักงานคุ้มครองข้อมูลส่วนบุคคลและบทเรียนจากกรณีศึกษาที่เกิดขึ้นในประเทศ

มติที่ประชุม: ให้ฝ่ายกฎหมายและ DPO ร่วมกันปรับปรุงเอกสารให้เสร็จภายในเดือนกรกฎาคม 2568 และเสนอเวอร์ชันใหม่ในการประชุมรอบถัดไป

วาระที่ 4: กำหนดกรอบการประชุมทบทวนเป็นประจำ

ที่ประชุมมีมติกำหนดให้มีการประชุมผู้บริหารอาวุโสเพื่อทบทวนและอนุมัตินโยบาย/แนวปฏิบัติเกี่ยวกับ PDPA ทุก 6 เดือน โดยให้ DPO จัดเตรียมวาระและเอกสารที่จำเป็น

มติสรุป: เห็นชอบทั้ง 3 แนวทางการปรับปรุง และกำหนดกรอบการประชุมถาวรทุก 6 เดือน โดยมีผู้บริหารระดับอาวุโสเข้าร่วมและ DPO ทำหน้าที่เลขานุการการประชุม

ลงชื่อ.....

นาย X

กรรมการผู้จัดการใหญ่ (ประธานการประชุม)

ลงชื่อ.....

นาย A

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ลงวันที่: 11 พฤษภาคม 2568

ตัวอย่างการทำเอกสาร 2.3.1 พนักงานได้อ่านและทำความเข้าใจนโยบายและขั้นตอนการปฏิบัติงาน

**การคุ้มครองข้อมูลส่วนบุคคลซึ่งรวมถึงเหตุผลและความจำเป็นที่ต้องมีการปฏิบัติตาม
เอกสารสรุปผลการจัดกิจกรรมฝึกอบรมพนักงานเรื่อง การคุ้มครองข้อมูลส่วนบุคคล (PDPA)**

1. ภาพรวม

องค์กรได้ตระหนักถึงความสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และข้อกำหนดตามประกาศฯ เรื่องมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เพื่อให้พนักงานทุกระดับมีความรู้ ความเข้าใจ และสามารถปฏิบัติตามนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม จึงได้ดำเนินการสื่อสารนโยบายผ่านช่องทางต่าง ๆ และจัดฝึกอบรมสำหรับพนักงานทุกคน

2. การจัดทำนโยบายและแนวปฏิบัติที่เผยแพร่แก่พนักงาน

องค์กรได้จัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (PDPA Policy) และแนวปฏิบัติ (PDPA Guidelines) ซึ่งเผยแพร่ผ่านระบบอินทราเน็ตขององค์กรในหมวด "ระเบียบและนโยบาย"

เอกสารดังกล่าวระบุชัดเจนถึง:

- หลักการสำคัญของ PDPA

- ความจำเป็นของการปฏิบัติตาม
- บทบาทของพนักงานในการคุ้มครองข้อมูล
- บทลงโทษหากมีการละเมิด

พนักงานทุกคนได้รับแจ้งให้ศึกษาเอกสารภายใน 15 วัน และรับรองการอ่านผ่านระบบภายใน

3. การจัดอบรม

- ชื่อหลักสูตร: ความรู้เบื้องต้นและแนวทางปฏิบัติตาม PDPA สำหรับพนักงานองค์กร
- วันที่จัดอบรม: 15 พฤษภาคม 2568
- วิทยากร: นาย A – เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- กลุ่มเป้าหมาย: พนักงานทุกคน (รวมจำนวน 147 คน)
- สถานที่: ห้องประชุมใหญ่ อาคารสำนักงานใหญ่

วัตถุประสงค์

- เพื่อให้พนักงานเข้าใจแนวคิดและหลักการของ PDPA
- เพื่อชี้แจงนโยบายและแนวปฏิบัติที่ต้องปฏิบัติตามในองค์กร
- เพื่อสร้างความตระหนักถึงบทบาทของพนักงานในการรักษาข้อมูลส่วนบุคคล

เนื้อหาหลักสูตร

- ภาพรวมของกฎหมาย PDPA และความรับผิดชอบขององค์กร
- สิทธิของเจ้าของข้อมูลส่วนบุคคล
- แนวปฏิบัติในการเก็บ ใช้ เผยข้อมูลส่วนบุคคลอย่างถูกต้อง
- กรณีศึกษาและบทลงโทษทางปกครอง
- การแจ้งเหตุละเมิดข้อมูลและแนวทางการรับมือ

รูปแบบการอบรม

- การบรรยายประกอบสไลด์
- การจำลองสถานการณ์ (case study)
- แบบทดสอบก่อนและหลังการอบรม (Pre-test / Post-test)

ผลการอบรม

- พนักงานทั้งหมดผ่านการอบรมเรียบร้อยแล้ว
- ผลการทดสอบหลังอบรมเฉลี่ย: 85% (สูงกว่าคะแนนเฉลี่ยก่อนอบรม 60%)
- พนักงานให้คะแนนความพึงพอใจในการอบรมระดับ "ดีมาก"

4. เอกสารประกอบ:

แนบในภาคผนวก:

- สำเนานโยบายและแนวปฏิบัติ PDPA
- รายละเอียดหลักสูตรการอบรม
- แบบทดสอบก่อนและหลังอบรม
- รายชื่อผู้เข้าอบรม
- ภาพถ่ายกิจกรรมการอบรม
- ใบลงทะเบียนการอบรมและแบบประเมินผล

5. บทบาทของพนักงานตามนโยบาย:

- รักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคลที่ตนมีหน้าที่ดูแล
- ปฏิบัติตามแนวทางการจัดเก็บ ใช้ เปิดเผยข้อมูลโดยชอบด้วยกฎหมาย
- รายงานเหตุสงสัยหรือละเมิดข้อมูลแก่ DPO ทันที

ลงชื่อ.....

นาย A

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ลงชื่อ.....

นางสาว Y

รองกรรมการผู้จัดการใหญ่ ฝ่ายทรัพยากรบุคคล

ลงวันที่: 16 พฤษภาคม 2568

หลักสูตรอบรมสร้างความตระหนักรู้ด้าน PDPA สำหรับพนักงาน

ชื่อหลักสูตร: การอบรมความรู้และความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล

(PDPA Awareness Training)

ระยะเวลาอบรม: 3 ชั่วโมง (รวมถามตอบ)

วัตถุประสงค์

- เพื่อให้พนักงานทุกคนเข้าใจความสำคัญของข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลตามกฎหมาย PDPA
- เพื่อสร้างความตระหนักและความรับผิดชอบในการจัดการข้อมูลส่วนบุคคลอย่างถูกต้องและปลอดภัย
- เพื่อให้พนักงานรู้จักสิทธิของเจ้าของข้อมูลส่วนบุคคลและวิธีการสนับสนุนสิทธิเหล่านั้น
- เพื่อชี้แจงนโยบายและแนวปฏิบัติขององค์กรที่เกี่ยวข้องกับ PDPA

กลุ่มเป้าหมาย

พนักงานทุกคนในองค์กร โดยเฉพาะพนักงานที่เกี่ยวข้องกับการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
เนื้อหาหลักสูตร

1. ความรู้พื้นฐานเกี่ยวกับข้อมูลส่วนบุคคลและ PDPA (30 นาที)

- ความหมายของข้อมูลส่วนบุคคลและประเภทของข้อมูล
- ภาพรวมของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)
- ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลในยุคดิจิทัล
- ผลกระทบที่อาจเกิดขึ้นจากการละเมิดข้อมูล

2. สิทธิของเจ้าของข้อมูลส่วนบุคคล (30 นาที)

- สิทธิรับทราบข้อมูล
- สิทธิขอเข้าถึงข้อมูล
- สิทธิแก้ไขข้อมูล
- สิทธิลบข้อมูล
- สิทธิจำกัดการประมวลผล
- สิทธิย้ายข้อมูล
- สิทธิคัดค้านการประมวลผล
- สิทธิถอนความยินยอม

3. ภาระหน้าที่ของพนักงานในการปฏิบัติตาม PDPA (30 นาที)

- การเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลอย่างถูกต้อง
- การรักษาความลับและความปลอดภัยของข้อมูล

- การปฏิบัติตามนโยบายและแนวปฏิบัติขององค์กร
- วิธีการรับมือกับคำขอของเจ้าของข้อมูล
- การแจ้งเหตุข้อมูลรั่วไหลหรือเหตุผิดปกติ

4. นโยบายและแนวปฏิบัติขององค์กรเกี่ยวกับ PDPA (30 นาที)

- นโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร
- แนวทางปฏิบัติสำหรับการจัดการข้อมูลส่วนบุคคล
- การควบคุมการเข้าถึงข้อมูลและการใช้ระบบสารสนเทศ
- การจัดการเอกสารและเวอร์ชันของข้อมูล
- การอบรมและสร้างความตระหนักรู้อย่างต่อเนื่อง

5. กรณีศึกษาและแบบฝึกหัด (30 นาที)

- ตัวอย่างสถานการณ์ที่พนักงานอาจพบเจอในการทำงาน
- วิเคราะห์วิธีการจัดการข้อมูลอย่างถูกต้อง
- การตอบสนองเมื่อพบเหตุการณ์ข้อมูลรั่วไหล
- การแสดงบทบาทและหน้าที่ในสถานการณ์ต่าง ๆ

6. สรุปและถามตอบ (30 นาที)

- ทบทวนประเด็นสำคัญ
- เปิดโอกาสให้พนักงานซักถาม
- ให้คำแนะนำเพิ่มเติมเกี่ยวกับช่องทางการขอข้อมูลหรือแจ้งปัญหา

วิธีการอบรม

- การบรรยายโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- การนำเสนอแบบสไลด์ (Presentation)
- กิจกรรมกลุ่มและการอภิปรายกรณีศึกษา
- แบบทดสอบก่อนและหลังอบรม (Pre-test / Post-test)

เอกสารประกอบการอบรม

- เอกสารสไลด์ประกอบการบรรยาย
- คู่มือการปฏิบัติตาม PDPA สำหรับพนักงาน
- แบบทดสอบและเฉลย
- รายงานสรุปผลการอบรม

การประเมินผล

- การประเมินความเข้าใจจากแบบทดสอบหลังอบรม
- การติดตามพฤติกรรมการทำงานที่สอดคล้องกับ PDPA ในการประเมินประจำปี

ตัวอย่างนโยบายขององค์กรที่นำไปใช้อบรม

นโยบายคุ้มครองข้อมูลส่วนบุคคล (PDPA Policy)

1. บทนำ

ในยุคที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการดำเนินธุรกิจและชีวิตประจำวัน ข้อมูลส่วนบุคคลจึงเป็นทรัพย์สินที่มีคุณค่าและต้องได้รับการคุ้มครองอย่างเหมาะสม องค์กรของเราตระหนักถึงความสำคัญดังกล่าว และให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคลของทุกฝ่ายอย่างเคร่งครัด ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และข้อกำหนดที่เกี่ยวข้องทั้งในประเทศและมาตรฐานสากล เช่น GDPR ของสหภาพยุโรป รวมถึงคำแนะนำของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC)

นโยบายนี้จัดทำขึ้นเพื่อกำหนดกรอบการบริหารจัดการข้อมูลส่วนบุคคลในองค์กร ให้เป็นไปตามหลักเกณฑ์ของกฎหมาย และส่งเสริมวัฒนธรรมการคุ้มครองข้อมูลอย่างรอบด้านและต่อเนื่อง

2. วัตถุประสงค์

- เพื่อสร้างความมั่นใจว่าการจัดการข้อมูลส่วนบุคคลขององค์กรเป็นไปตามกฎหมาย
- เพื่อปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- เพื่อส่งเสริมความโปร่งใสและความรับผิดชอบในการใช้ข้อมูล
- เพื่อกำหนดบทบาทหน้าที่ความรับผิดชอบของบุคลากรในองค์กรทุกระดับที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- เพื่อสนับสนุนการพัฒนาระบบการรักษาความปลอดภัยและการบริหารความเสี่ยงของข้อมูลส่วนบุคคล

3. ขอบเขตของนโยบาย

นโยบายนี้ครอบคลุมถึงข้อมูลส่วนบุคคลที่องค์กรเก็บรวบรวม ใช้ เปิดเผย และเก็บรักษาในทุกกิจกรรมและทุกแผนกขององค์กร ไม่ว่าจะเป็นข้อมูลของลูกค้า ผู้บริหาร พนักงาน คู่ค้า ผู้รับบริการ และบุคคลภายนอกที่เกี่ยวข้อง รวมถึงข้อมูลในรูปแบบต่าง ๆ ทั้งเอกสารกระดาษ ระบบอิเล็กทรอนิกส์ หรือสื่อบันทึกข้อมูลอื่น ๆ

4. คำจำกัดความ

- **ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดา ซึ่งสามารถระบุตัวบุคคลนั้นได้โดยตรงหรือโดยอ้อม เช่น ชื่อ-นามสกุล หมายเลขบัตรประจำตัวประชาชน เบอร์โทรศัพท์ ที่อยู่ วันเดือนปีเกิด ข้อมูลสุขภาพ เป็นต้น
- **เจ้าของข้อมูลส่วนบุคคล** หมายถึง บุคคลเจ้าของข้อมูลส่วนบุคคลนั้น

- **การประมวลผลข้อมูลส่วนบุคคล** หมายถึง การกระทำใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น การเก็บรวบรวม การจัดเก็บ การแก้ไข การเปิดเผย การใช้ หรือการทำลายข้อมูล
- **การนามแฝง (Pseudonymisation)** หมายถึง กระบวนการเปลี่ยนแปลงข้อมูลส่วนบุคคลเพื่อไม่ให้สามารถระบุตัวบุคคลได้โดยตรง แต่ยังสามารถย้อนกลับข้อมูลได้ภายใต้เงื่อนไขการควบคุม
- **ข้อมูลที่ละเอียดอ่อน (Sensitive Data)** หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง สุขภาพ หรือข้อมูลชีวมิติ ซึ่งต้องได้รับการปกป้องเป็นพิเศษ
- **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)** หมายถึง บุคคลที่องค์กรแต่งตั้งให้ทำหน้าที่รับผิดชอบในการดูแลและกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

5. หลักการคุ้มครองข้อมูลส่วนบุคคล

องค์กรยึดมั่นในหลักการสำคัญดังนี้:

5.1 ความชอบด้วยกฎหมายและความเป็นธรรม

การประมวลผลข้อมูลต้องมีฐานทางกฎหมายที่ชัดเจน และต้องดำเนินการอย่างเป็นธรรม ไม่มีการใช้ข้อมูลเกินวัตถุประสงค์หรือโดยไม่ได้รับความยินยอมที่ถูกต้อง

5.2 จำกัดวัตถุประสงค์

ข้อมูลส่วนบุคคลจะเก็บรวบรวมและใช้เฉพาะเพื่อวัตถุประสงค์ที่ชัดเจน และผู้มีข้อมูลได้รับแจ้งอย่างครบถ้วน

5.3 จำกัดปริมาณข้อมูล

เก็บเฉพาะข้อมูลที่จำเป็นและเกี่ยวข้องกับวัตถุประสงค์เท่านั้น

5.4 ความถูกต้องและทันสมัย

องค์กรจะรักษาข้อมูลให้ถูกต้องและอัปเดตอยู่เสมอ หากพบข้อมูลผิดพลาดต้องดำเนินการแก้ไขทันที

5.5 จำกัดระยะเวลาการเก็บรักษา

ข้อมูลจะเก็บรักษาในระยะเวลาที่จำเป็น และต้องดำเนินการทำลายข้อมูลเมื่อครบกำหนดตามกฎหมายหรือวัตถุประสงค์

5.6 ความปลอดภัยของข้อมูล

จัดให้มีมาตรการรักษาความปลอดภัยทั้งทางเทคนิคและองค์กร เพื่อป้องกันการเข้าถึงหรือใช้ข้อมูลโดยไม่ได้รับอนุญาต

5.7 ความรับผิดชอบและความโปร่งใส

องค์กรรับผิดชอบต่อการจัดการข้อมูล และเปิดเผยข้อมูลเกี่ยวกับการประมวลผลข้อมูลตามที่กฎหมายกำหนด

5.8 เคารพสิทธิของเจ้าของข้อมูล

องค์กรให้ความสำคัญกับสิทธิของเจ้าของข้อมูล และดำเนินการสนับสนุนให้เจ้าของข้อมูลใช้สิทธิเหล่านั้นได้อย่างเต็มที่

6. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิพื้นฐานตามกฎหมาย PDPA ซึ่งองค์กรต้องเคารพและสนับสนุนการใช้สิทธิอย่างเต็มที่ ประกอบด้วยสิทธิหลักดังนี้:

6.1 สิทธิรับทราบ (Right to be informed)

เจ้าของข้อมูลมีสิทธิรับทราบข้อมูลที่ถูกเก็บรวบรวม วิธีการใช้ และวัตถุประสงค์ของการใช้ข้อมูล รวมถึงข้อมูลเกี่ยวกับผู้รับข้อมูลและระยะเวลาการเก็บรักษา

6.2 สิทธิในการเข้าถึงข้อมูล (Right of access)

เจ้าของข้อมูลสามารถขอเข้าถึงข้อมูลส่วนบุคคลของตนที่องค์กรเก็บรักษา และขอสำเนาข้อมูลนั้นได้

6.3 สิทธิในการแก้ไขข้อมูล (Right to rectification)

เจ้าของข้อมูลมีสิทธิขอแก้ไขข้อมูลที่ไม่ถูกต้อง หรือไม่สมบูรณ์ได้

6.4 สิทธิในการลบข้อมูล (Right to erasure / Right to be forgotten)

เจ้าของข้อมูลสามารถขอให้ลบข้อมูลส่วนบุคคลในกรณีที่ไม่จำเป็นต้องเก็บข้อมูลต่อ หรือข้อมูลถูกเก็บโดยผิดกฎหมาย ยกเว้นกรณีที่กฎหมายกำหนดให้เก็บข้อมูลไว้

6.5 สิทธิในการจำกัดการประมวลผล (Right to restriction of processing)

เจ้าของข้อมูลสามารถขอให้จำกัดการใช้ข้อมูลในบางกรณี เช่น ข้อมูลไม่ถูกต้อง หรือยังอยู่ระหว่างการพิจารณาขอแก้ไข

6.6 สิทธิในการย้ายข้อมูล (Right to data portability)

เจ้าของข้อมูลมีสิทธิขอรับข้อมูลของตนในรูปแบบที่เป็นมาตรฐานและสามารถถ่ายโอนไปยังผู้ควบคุมข้อมูลรายอื่นได้

6.7 สิทธิในการคัดค้าน (Right to object)

เจ้าของข้อมูลสามารถคัดค้านการใช้ข้อมูลในกรณีที่ใช้เพื่อการตลาดโดยตรง หรือในกรณีที่มีเหตุผลเกี่ยวกับสถานการณ์เฉพาะตัว

6.8 สิทธิในการไม่ถูกตัดสินใจโดยอัตโนมัติ (Rights related to automated decision-making)

เจ้าของข้อมูลมีสิทธิไม่ถูกตัดสินใจโดยอัตโนมัติที่ส่งผลกระทบอย่างมีนัยสำคัญต่อสิทธิและเสรีภาพของตน

6.9 สิทธิถอนความยินยอม (Right to withdraw consent)

เจ้าของข้อมูลสามารถถอนความยินยอมที่ให้ไว้สำหรับการประมวลผลข้อมูลส่วนบุคคลได้ทุกเมื่อ โดยไม่มีผลย้อนหลัง

7. บทบาทและความรับผิดชอบของบุคลากรในองค์กร

7.1 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

- ทำหน้าที่ประสานงานและตรวจสอบการปฏิบัติตามนโยบาย PDPA

- ให้คำปรึกษาและฝึกอบรมพนักงานในเรื่องการคุ้มครองข้อมูล
- ตรวจสอบและทบทวนการปฏิบัติให้เป็นไปตามข้อกำหนดของกฎหมายและมาตรฐานที่เกี่ยวข้อง
- เป็นจุดติดต่อสำหรับเจ้าของข้อมูลและหน่วยงานกำกับดูแล

7.2 ผู้บริหารระดับสูง

- รับผิดชอบในการสนับสนุนทรัพยากร และกำกับดูแลการดำเนินงานด้านการคุ้มครองข้อมูล
- ตรวจสอบให้มีการประเมินความเสี่ยงและจัดการความเสี่ยงด้านข้อมูลอย่างเหมาะสม
- ตรวจสอบและอำนวยความสะดวกในการปฏิบัติงาน

ตัวอย่างการทำเอกสาร 2.3.2 องค์กรแจ้งให้พนักงานได้ทราบเกี่ยวกับนโยบายและแนวปฏิบัติใหม่

1. นโยบายและแนวปฏิบัติที่ปรับปรุงใหม่

นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ฉบับปรับปรุง

วัตถุประสงค์

เพื่อให้สอดคล้องกับข้อกำหนดของกฎหมาย PDPA และแนวทางปฏิบัติที่เป็นปัจจุบัน รวมถึงเสริมสร้างความปลอดภัยและสิทธิของเจ้าของข้อมูลส่วนบุคคลในองค์กร

สาระสำคัญของนโยบายฉบับปรับปรุง

- เพิ่มรายละเอียดสิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น สิทธิในการขอเข้าถึง แก้ไข ลบ และจำกัดการประมวลผลข้อมูล
- กำหนดแนวทางการแจ้ง Privacy Notice ให้สอดคล้องกับช่วงอายุและระดับความเข้าใจของเจ้าของข้อมูล
- เพิ่มแนวทางการใช้เทคนิคการทำนามแฝง (Pseudonymisation) เพื่อเพิ่มความมั่นคงปลอดภัยของข้อมูล
- กำหนดระยะเวลาการทบทวนและปรับปรุงนโยบายทุก 6 เดือน

เสริมมาตรการควบคุมการเข้าถึงและการจัดเก็บข้อมูลให้รัดกุมยิ่งขึ้นโดยมีรายละเอียดดังนี้

1.การควบคุมสิทธิ์การเข้าถึงข้อมูล

- กำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคลตามบทบาทหน้าที่ (Role-Based Access Control) เพื่อให้พนักงานแต่ละฝ่ายเข้าถึงข้อมูลเฉพาะส่วนที่จำเป็นสำหรับการปฏิบัติงานเท่านั้น
- มีการบันทึก Log การเข้าถึงข้อมูลอย่างละเอียด เพื่อใช้ตรวจสอบย้อนหลังในกรณีเกิดเหตุการณ์ผิดปกติ
- ปรับสิทธิ์เข้าถึงข้อมูลอย่างสม่ำเสมอ โดยเฉพาะเมื่อตำแหน่งงานหรือหน้าที่ของพนักงานมีการเปลี่ยนแปลง

2.การจัดเก็บข้อมูลส่วนบุคคลอย่างปลอดภัย

- กำหนดสถานที่และระบบการจัดเก็บข้อมูลที่มีมาตรฐาน เช่น การใช้ระบบจัดเก็บข้อมูลที่ได้รับการรับรองความปลอดภัย หรือใช้ระบบ Cloud ที่มีการเข้ารหัสข้อมูล
- ข้อมูลที่จัดเก็บต้องถูกแบ่งชั้นความลับตามประเภทและความสำคัญ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- มีการสำรองข้อมูลอย่างสม่ำเสมอและจัดทำแผนการกู้คืนข้อมูลในกรณีเกิดภัยพิบัติ (Disaster Recovery Plan)

3.มาตรการเสริมด้านเทคนิค

- การใช้การเข้ารหัส (Encryption) ในการส่งผ่านและจัดเก็บข้อมูลที่มีความละเอียดอ่อน

- ติดตั้งระบบป้องกันไวรัสและมัลแวร์ พร้อมกับการอัปเดตซอฟต์แวร์รักษาความปลอดภัยเป็นประจำ
- กำหนดนโยบายรหัสผ่านที่เข้มงวด เช่น ต้องมีความยาวขั้นต่ำและผสมตัวอักษรพิเศษ เพื่อป้องกันการถูกโจมตีแบบ Brute Force

4.มาตรการเสริมด้านกระบวนการและบุคลากร

- จัดอบรมและสร้างความตระหนักรู้ให้พนักงานเกี่ยวกับความสำคัญของการรักษาความปลอดภัยข้อมูลอย่างต่อเนื่อง
- กำหนดขั้นตอนการแจ้งเหตุการณ์ละเมิดข้อมูล (Data Breach) และการรับมืออย่างรวดเร็ว
- จัดทำข้อตกลงการรักษาความลับข้อมูล (Non-Disclosure Agreement) กับพนักงานและบุคคลภายนอกที่เกี่ยวข้อง

ด้วยมาตรการเหล่านี้ องค์กรสามารถลดความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ และสร้างความมั่นใจแก่เจ้าของข้อมูลว่าข้อมูลของตนได้รับการปกป้องอย่างเหมาะสม

กำหนดบทบาทและความรับผิดชอบของเจ้าของเอกสารนโยบายและเจ้าหน้าที่ที่เกี่ยวข้อง

5.แนวปฏิบัติที่ปรับปรุง

- การแจ้ง Privacy Notice ต้องมีเนื้อหาที่เหมาะสมตามวัยของเจ้าของข้อมูล
- การทำนามแฝงข้อมูล (Pseudonymisation) ต้องเป็นไปตามมาตรฐานความปลอดภัยข้อมูล
- พนักงานต้องเข้ารับการอบรมและทดสอบความเข้าใจเกี่ยวกับนโยบายใหม่ทุกครั้งหลังการปรับปรุง
- จัดทำรายงานและเอกสารควบคุมเวอร์ชันนโยบายให้ชัดเจน

1. รายงานการประชุมชี้แจงนโยบายและแนวปฏิบัติที่ปรับปรุงใหม่

วันที่ประชุม: 20 พฤษภาคม 2568

สถานที่: ห้องประชุมใหญ่ ชั้น 5 อาคารสำนักงานใหญ่

ประธานการประชุม: นาย A (ประธานคณะกรรมการ PDPA)

ผู้เข้าร่วมประชุม:

1. นาย B (ผู้อำนวยการฝ่ายทรัพยากรบุคคล)
2. นาง C (หัวหน้าฝ่าย IT)
3. นาย D (เจ้าหน้าที่กฎหมาย)
4. พนักงานฝ่ายต่าง ๆ รวม 30 คน

วาระการประชุม:

- ชี้แจงเนื้อหา นโยบายและแนวปฏิบัติด้าน PDPA ฉบับปรับปรุง
- อธิบายสิทธิของเจ้าของข้อมูลส่วนบุคคลที่เพิ่มขึ้นในนโยบาย
- แนวทางการแจ้ง Privacy Notice ตามช่วงอายุ
- การทำนามแฝงข้อมูล (Pseudonymisation) เพื่อความมั่นคงปลอดภัย
- กำหนดแผนการอบรมพนักงานและการประเมินผลความเข้าใจ

สรุปเนื้อหาการประชุม:

- นาย A ชี้แจงถึงความจำเป็นในการปรับปรุงนโยบายให้ทันสมัยและสอดคล้องกับข้อกฎหมาย
- นาย D นำเสนอรายละเอียดสิทธิของเจ้าของข้อมูลที่เพิ่มเติมเข้ามา
- นาง C อธิบายแนวทางเทคนิคการทำนามแฝงข้อมูลและความปลอดภัยที่เพิ่มขึ้น

ได้กำหนดให้ฝ่ายทรัพยากรบุคคลจัดอบรมพนักงานภายในเดือนถัดไป

มีมติรับรองนโยบายฉบับปรับปรุงโดยเสียงเอกฉันท์

ลงชื่อ:

ประธานการประชุม นาย A

เลขานุการ นาง E

3. เอกสารอื่น ๆ เพื่อแสดงหลักฐานการแจ้งและอบรมนโยบายและแนวปฏิบัติใหม่

- เอกสารนโยบายและแนวปฏิบัติฉบับปรับปรุง (แจกจ่ายผ่านระบบอินทราเน็ตและอีเมลภายในองค์กร)
- รายละเอียดหลักสูตรอบรม PDPA ฉบับปรับปรุง
- ภาพถ่ายการอบรมพนักงานวันที่ 15 มิถุนายน 2568
- รายงานผลการทดสอบความรู้หลังอบรม (Post-test)
- รายงานสรุปผลการจัดอบรมและการรับทราบนโยบาย

เอกสารตัวอย่างแนวปฏิบัติที่ปรับปรุง (4 ฉบับ)

1. แนวปฏิบัติเรื่องการแจ้ง Privacy Notice ที่เหมาะสมตามวัยของเจ้าของข้อมูล

วัตถุประสงค์

เพื่อให้การแจ้งข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเป็นไปอย่างเหมาะสมตามช่วงวัยและระดับความเข้าใจ เพื่อเพิ่มประสิทธิภาพในการสื่อสารและความโปร่งใส

แนวปฏิบัติ

การแจ้ง Privacy Notice ต้องมีรูปแบบและภาษาที่เข้าใจง่ายตามกลุ่มเป้าหมาย เช่น

- สำหรับผู้เยาว์ ต้องใช้ภาษาง่าย และอาจมีผู้ปกครองให้ความเห็นชอบ
- สำหรับผู้สูงอายุ ควรมีการอธิบายด้วยคำพูดหรือเอกสารเสริมที่อ่านง่ายและมีภาพประกอบ
- ต้องระบุข้อมูลที่จำเป็น เช่น วัตถุประสงค์ของการเก็บข้อมูล สิทธิของเจ้าของข้อมูล ช่องทางติดต่อ และวิธีการถอนความยินยอม
- Privacy Notice ต้องเผยแพร่ในช่องทางที่เจ้าของข้อมูลเข้าถึงได้ง่าย เช่น เว็บไซต์หลัก อินทราเน็ต หรือเอกสารแจ้งในสถานที่บริการ

2. แนวปฏิบัติเรื่องการทำนามแฝงข้อมูล (Pseudonymisation)

วัตถุประสงค์

เพื่อเพิ่มความปลอดภัยของข้อมูลส่วนบุคคลโดยการลดความเสี่ยงจากการเปิดเผยข้อมูลที่สามารถระบุตัวตน

แนวปฏิบัติ

- ข้อมูลที่จำเป็นต้องทำนามแฝงจะถูกแทนที่ด้วยรหัสหรือสัญลักษณ์ที่ไม่สามารถระบุเจ้าของข้อมูลได้โดยตรง
- การจัดเก็บรหัสถอดรหัส (Key) ต้องแยกจากฐานข้อมูลหลักและเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น
- ต้องตรวจสอบและทบทวนกระบวนการทำนามแฝงเป็นประจำ เพื่อให้มั่นใจว่าไม่มีช่องโหว่ด้านความปลอดภัย
- พนักงานที่เกี่ยวข้องต้องได้รับการอบรมและยอมรับข้อตกลงด้านความลับ

3. แนวปฏิบัติเรื่องการอบรมและทดสอบความเข้าใจของพนักงานเกี่ยวกับนโยบายใหม่

วัตถุประสงค์

เพื่อให้พนักงานทุกคนรับทราบและเข้าใจนโยบายและแนวปฏิบัติใหม่ ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

แนวปฏิบัติ

- จัดอบรมพนักงานทุกคนภายใน 30 วันหลังจากมีการประกาศใช้นโยบายใหม่

- กำหนดเนื้อหาการอบรมที่ครอบคลุมทั้งข้อกฎหมาย สิทธิของเจ้าของข้อมูล และมาตรการรักษาความปลอดภัย
- มีการทดสอบก่อน (Pre-test) และหลังอบรม (Post-test) เพื่อประเมินผลความเข้าใจ
- จัดทำรายงานผลการอบรม และเก็บบันทึกการเข้าร่วมอบรมของพนักงานแต่ละคน

4. แนวปฏิบัติเรื่องการจัดทำรายงานและควบคุมเวอร์ชันของนโยบาย

วัตถุประสงค์

เพื่อให้การบริหารจัดการเอกสารนโยบายและแนวปฏิบัติเป็นไปอย่างเป็นระบบ ชัดเจน และสามารถติดตามประวัติการเปลี่ยนแปลงได้

แนวปฏิบัติ

- จัดทำทะเบียนเอกสารที่บันทึกรายละเอียด เช่น ชื่อเอกสาร เวอร์ชัน วันที่ทบทวน เจ้าของเอกสาร และประวัติการแก้ไข
- ทุกครั้งที่มีการปรับปรุงนโยบาย ต้องระบุหมายเลขเวอร์ชันใหม่ พร้อมวันที่มีผลบังคับใช้
- เอกสารเวอร์ชันเก่าต้องเก็บรักษาไว้ตามมาตรฐาน เพื่อใช้ตรวจสอบย้อนหลังได้
- แจ้งให้ผู้เกี่ยวข้องทุกคนทราบเมื่อมีการเปลี่ยนแปลงเอกสาร และเผยแพร่เอกสารฉบับใหม่ผ่านช่องทางที่เหมาะสม เช่น ระบบอินทราเน็ต

ตัวอย่างการทำเอกสาร 2.3.3 องค์กรจัดให้พนักงานสามารถเข้าถึงนโยบายและแนวปฏิบัติ เช่น พนักงานสามารถเข้าถึงอินทราเน็ตขององค์กร หรือด้วยวิธีอื่น ๆ ที่พนักงานสามารถเข้าถึงได้โดยง่าย

เอกสารแนวทางการเข้าถึงนโยบายและแนวปฏิบัติของพนักงาน

1. วัตถุประสงค์

เพื่อให้องค์กรสามารถดำเนินการตามข้อกำหนดด้านกฎหมายและมาตรฐานความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยจัดให้พนักงานสามารถเข้าถึงนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลได้โดยสะดวก ครอบคลุม และมีประสิทธิภาพ พร้อมทั้งสามารถเข้าใจเนื้อหาและปฏิบัติตามได้อย่างถูกต้อง

2. วิธีการดำเนินงาน

2.1 การเผยแพร่และเข้าถึงข้อมูลนโยบายและแนวปฏิบัติ

จัดทำเว็บไซต์ภายใน (Intranet) ซึ่งมีเมนูเฉพาะสำหรับ “นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล” โดยประกอบด้วย:

- นโยบายฉบับเต็ม

- เอกสารแนวปฏิบัติที่เกี่ยวข้อง
- เวอร์ชันและวันที่มีผลบังคับใช้
- คำถามที่พบบ่อย (FAQ)
- ช่องทางติดต่อ DPO หรือฝ่ายกฎหมายในกรณีสงสัย

2.2 การชี้แจงแก่พนักงาน

จัดประชุมหรือสัมมนาเพื่อชี้แจงนโยบายและแนวปฏิบัติใหม่แก่พนักงานในทุกแผนก โดยอาจใช้การประชุมทั้งแบบออนไลน์และออนไซต์

เนื้อหาการชี้แจงประกอบด้วย:

- ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล
- เนื้อหานโยบายและแนวปฏิบัติที่พนักงานต้องรับทราบ
- ช่องทางการเข้าถึงเอกสารผ่านอินทราเน็ต
- วิธีการสอบถามข้อมูลเพิ่มเติม

2.3 ช่องทางการสื่อสารเพิ่มเติม

แจ้งผ่านช่องทางการสื่อสารภายใน ได้แก่:

- อีเมลล์ภายในของพนักงาน
- กลุ่มไลน์ หรือระบบ Chat ภายในที่ใช้งานประจำ
- ป้ายประชาสัมพันธ์ในสำนักงาน
- แบนลิงก์สำหรับเข้าถึงหน้า Intranet พร้อม QR Code

2.4 การประเมินความเข้าใจของพนักงาน

- จัดทำแบบทดสอบออนไลน์หลังจากชี้แจงนโยบาย
- แบบทดสอบประกอบด้วยคำถามเกี่ยวกับสาระสำคัญของนโยบาย เช่น สิทธิของเจ้าของข้อมูล แนวปฏิบัติการแจ้งเหตุละเมิดข้อมูล การเข้าถึงข้อมูล
- กำหนดคะแนนสอบผ่านขั้นต่ำที่ 70%
- พนักงานที่ไม่ผ่านจะต้องเข้ารับการอบรมซ้ำ

3. หลักฐานประกอบการดำเนินการ

ลำดับ	ประเภทเอกสาร	รายละเอียด
1	หน้าเว็บไซต์ Intranet	มีหมวด “PDPA Policy & Practice” ที่แสดงเอกสารทั้งหมดให้พนักงานสามารถเข้าถึงได้
2	รายงานการประชุมชี้แจงนโยบาย	รายงานสรุปการประชุมที่จัดขึ้น ระบุหัวข้อที่ชี้แจง จำนวนพนักงานที่เข้าร่วม วิธีการเผยแพร่ และผลการประเมิน
3	ภาพถ่ายหรือบันทึกการประชุม / อบรม	เป็นหลักฐานที่แสดงการจัดประชุมหรืออบรมจริง

4	ประกาศภายใน / อีเมลล์ ประชาสัมพันธ์	สำเนาข้อความที่แจ้งพนักงาน เช่น แบนลิงก์นโยบาย หรือ ประกาศจาก HR
5	แบบทดสอบออนไลน์ (Pre- test / Post-test)	แสดงคำถาม ตัวอย่างคำตอบ และสถิติผลการสอบของ พนักงานแต่ละแผนก
6	ทะเบียนเวอร์ชันของนโยบาย	บันทึกการอัปเดตนโยบาย เช่น หมายเลขเวอร์ชัน วันที่ ปรับปรุง เจ้าของเอกสาร

4. สภาพบังคับตามกฎหมาย

- มาตรา 37(1): ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัย ข้อ 4(7): ผู้ควบคุมข้อมูลต้องแจ้งให้พนักงานทราบถึงนโยบายและแนวปฏิบัติในการดำเนินการที่เกี่ยวข้อง
- โทษทางปกครอง: หากไม่ปฏิบัติตาม อาจถูกปรับสูงสุดไม่เกิน 3 ล้านบาท

รายงานการประชุมชี้แจงนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ฉบับปรับปรุง

ชื่อการประชุม: การประชุมชี้แจงนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลฉบับปรับปรุง วันที่ประชุม: วันพุธที่ 29 พฤษภาคม 2568 เวลา: 09.00 – 12.00 น. สถานที่: ห้องประชุมใหญ่ อาคารสำนักงานกลาง หรือผ่านระบบ Video Conference (Microsoft Teams) ผู้จัดประชุม: ฝ่ายกฎหมายและฝ่ายทรัพยากรบุคคล ร่วมกับ DPO (Data Protection Officer) ผู้เข้าร่วมประชุม: ผู้บริหารระดับกลาง-สูง และพนักงานทุกแผนก รวมจำนวน 87 คน ระเบียบวาระการประชุม วาระที่ 1: กล่าวเปิดการประชุม โดย คุณสุจิตรา นันทโชติ ผู้อำนวยการฝ่ายบริหารและทรัพยากรบุคคล ได้กล่าวถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และการปรับปรุงนโยบายตามข้อกำหนดกฎหมายล่าสุด

วาระที่ 2: การชี้แจงนโยบายและแนวปฏิบัติฉบับปรับปรุง

โดย คุณพัชรพล ศรีบุญเรือง (DPO) ได้ชี้แจงนโยบาย PDPA ฉบับใหม่ มีสาระสำคัญ ดังนี้:
การอัปเดตเนื้อหา Privacy Notice ให้เหมาะสมตามวัย ของเจ้าของข้อมูล (โดยเฉพาะผู้เยาว์)
แนวทางการ ทำนามแฝงข้อมูล (Pseudonymisation) ที่สอดคล้องกับมาตรฐานความปลอดภัยตาม GDPR และประกาศฯ PDPC

การเพิ่มมาตรการ ควบคุมการเข้าถึงและการจัดเก็บข้อมูลให้รัดกุมยิ่งขึ้น:

- การแยกสิทธิการเข้าถึงตามระดับหน้าที่ (Role-based access control)
- การใช้ระบบล็อกไฟล์และ audit log
- การเข้ารหัสข้อมูลขณะจัดเก็บ (At rest encryption)
- การจัดทำ ระบบทะเบียนควบคุมเวอร์ชันนโยบาย ที่ชัดเจน พร้อมระบุเจ้าของเอกสาร และวันทบทวนล่าสุด
- พนักงานทุกคนจะต้อง เข้ารับการอบรมหลังการปรับปรุงนโยบายทุกครั้ง และผ่านการประเมินความเข้าใจ (Post-test)

วาระที่ 3: ช่องทางการเข้าถึงนโยบาย

แจ้งช่องทางที่พนักงานสามารถเข้าถึงเอกสารนโยบาย ได้แก่:

- เว็บไซต์ Intranet ภายในองค์กร > เมนู “PDPA POLICY”
- อีเมลแจ้งข่าวภายใน พร้อมแนบลิงก์
- QR Code ติดประกาศที่บอร์ดหน้าห้องประชุม
- กลุ่มไลน์องค์กร

วาระที่ 4: การอบรมพนักงาน

คุณเกรียงไกร แสงศิริ ฝ่ายทรัพยากรบุคคล ชี้แจงว่าพนักงานทุกคนต้อง:

- ลงทะเบียนอบรม PDPA ภายใน 7 วัน
- ทำ Post-test หลังอบรม โดยคะแนนผ่านขั้นต่ำ 70%
- พนักงานที่ไม่ผ่านต้องเข้าอบรมซ้ำภายใน 14 วัน

วาระที่ 5: คำถาม-คำตอบ

มีคำถามจากพนักงานฝ่าย IT เรื่องการจัดเก็บ Log การเข้าถึงข้อมูล และคำแนะนำเรื่องการควบคุมสิทธิ์แบบ Role-based access ซึ่งได้รับคำชี้แจงจาก DPO อย่างละเอียด

มติที่ประชุม

1. เห็นชอบนโยบายและแนวปฏิบัติ PDPA ฉบับปรับปรุง
2. ให้เผยแพร่นโยบายแก่พนักงานทุกคนผ่าน Intranet ภายใน 3 วัน
3. ฝ่าย HR รับผิดชอบจัดอบรมภายในเดือนมิถุนายน 2568

ผู้บันทึกการประชุม:

นางสาวนิตยา ธรรมรักษ์
เจ้าหน้าที่ฝ่ายทรัพยากรบุคคล

ผู้ตรวจสอบและอนุมัติรายงาน:
นายพัชรพล ศรีบุญเรือง
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

แบบทดสอบความเข้าใจนโยบายและแนวปฏิบัติด้าน PDPA (จำนวน 10 ข้อ)

คำชี้แจง: จงเลือกคำตอบที่ถูกต้องที่สุดเพียงข้อเดียวในแต่ละคำถาม

1. ข้อใดต่อไปนี้ ไม่ใช่สิทธิของเจ้าของข้อมูลตามกฎหมาย PDPA?

- A. สิทธิในการเข้าถึงข้อมูลของตนเอง
- B. สิทธิในการคัดค้านการประมวลผลข้อมูล
- C. สิทธิในการขอลบข้อมูล
- D. สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้อื่น

เฉลย: D

คำอธิบาย: สิทธิของเจ้าของข้อมูลครอบคลุมเฉพาะข้อมูลของตนเอง ไม่สามารถเข้าถึงข้อมูลของบุคคลอื่นโดยไม่มีฐานทางกฎหมายรองรับ

2. ข้อใดคือวัตถุประสงค์หลักของการทำนามแฝงข้อมูล (Pseudonymisation)?

- A. เพื่อเผยแพร่ข้อมูลให้ประชาชน
- B. เพื่อป้องกันการระบุตัวตนโดยตรง
- C. เพื่อเก็บข้อมูลในระบบคลาวด์
- D. เพื่อให้ข้อมูลหายไปถาวร

เฉลย: B

คำอธิบาย: การทำนามแฝงช่วยลดความเสี่ยงในการระบุตัวบุคคลโดยตรง แม้ข้อมูลยังสามารถใช้ประมวลผลต่อได้หากมีข้อมูลแยกเก็บไว้

3. การเผยแพร่ Privacy Notice ควรมีลักษณะอย่างไรจึงจะเหมาะสม?

- A. ใช้ภาษาทางกฎหมายเท่านั้น
- B. เขียนด้วยภาษาทางการที่เข้าใจยาก
- C. มีรูปแบบเข้าใจง่ายและเหมาะสมตามวัย
- D. เผยแพร่เฉพาะกับผู้ใหญ่เท่านั้น

เฉลย: C

คำอธิบาย: Privacy Notice ควรเขียนด้วยภาษาชัดเจน เข้าใจง่าย และปรับตามวัยของเจ้าของข้อมูล เช่น เด็ก ผู้สูงอายุ หรือบุคคลที่มีข้อจำกัด

4. หากพนักงานเข้าถึงข้อมูลส่วนบุคคลของลูกค้าโดยไม่เกี่ยวข้องกับงาน ถือว่า...

- A. ได้ เพราะเป็นพนักงานบริษัท
- B. ผิดระเบียบ แต่ไม่ผิดกฎหมาย
- C. เป็นการละเมิด PDPA
- D. ทำได้หากไม่เปิดเผย

เฉลย: C

คำอธิบาย: การเข้าถึงข้อมูลโดยไม่ชอบด้วยหน้าที่หรือไม่ได้รับอนุญาตถือเป็นการละเมิด PDPA และอาจมีโทษตามกฎหมาย

5. ข้อใดต่อไปนี้เป็นตัวอย่างของมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล?

- A. แพร่รหัสผ่านให้ทีม
- B. เก็บเอกสารสำคัญในโต๊ะโดยไม่ล็อก
- C. ใช้การยืนยันตัวตนสองชั้น (2FA)
- D. ส่งข้อมูลลูกค้าผ่านแอปแชททั่วไป

เฉลย: C

คำอธิบาย: การใช้ 2FA เป็นหนึ่งในมาตรการควบคุมความมั่นคงปลอดภัยเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

6. พนักงานควรเข้าถึงเอกสารนโยบายและแนวปฏิบัติ PDPA ผ่านช่องทางใดเป็นหลัก?

- A. เว็บไซต์ภายนอก
- B. ระบบอินทราเน็ตขององค์กร
- C. โซเชียลมีเดีย
- D. เอกสารที่แจกในกลุ่มไลน์เท่านั้น

เฉลย: B

คำอธิบาย: ช่องทางหลักคือ Intranet ซึ่งมีการอัปเดตสม่ำเสมอและควบคุมเวอร์ชันได้ ทั้งยังสามารถกำกับการเข้าถึงข้อมูลได้ดีกว่า

7. องค์กรควรประชุมทบทวนนโยบายและแนวปฏิบัติด้าน PDPA บ่อยเพียงใด?

- A. เฉพาะเมื่อถูกฟ้องร้อง
- B. ปีละครั้งพอ
- C. ทุก 6 เดือน หรือตามความเหมาะสม
- D. ไม่มีความจำเป็นต้องทบทวน

เฉลย: C

คำอธิบาย: แนวปฏิบัติควรถูกทบทวนเป็นประจำ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงของกฎหมาย หรือวิธีปฏิบัติในองค์กร

8. การเก็บข้อมูลส่วนบุคคลไว้เกินระยะเวลาที่จำเป็นโดยไม่มีเหตุผล ถือเป็น...

- A. ไม่ผิดหากไม่ได้เปิดเผย
- B. ผิดหลัก PDPA
- C. เป็นสิทธิขององค์กร
- D. ได้ หากเจ้าของข้อมูลไม่ร้องเรียน

เฉลย: B

คำอธิบาย: PDPA กำหนดให้เก็บข้อมูลเพียงพอที่จำเป็นต่อวัตถุประสงค์ที่แจ้งไว้ และต้องลบหรือทำลายเมื่อหมดความจำเป็น

9. แบบฟอร์มขอใช้สิทธิของเจ้าของข้อมูลควรอยู่ภายใต้การดูแลของฝ่ายใด?

- A. ฝ่ายขาย
- B. ฝ่าย IT
- C. ฝ่ายกฎหมาย หรือ DPO
- D. ฝ่ายจัดซื้อ

เฉลย: C

คำอธิบาย: ฝ่ายกฎหมายหรือ DPO มีหน้าที่โดยตรงในการดูแลคำร้องสิทธิและประสานงานภายในองค์กรเพื่อดำเนินการตามสิทธิของเจ้าของข้อมูล

10. หากพนักงานไม่เข้าอบรม PDPA หลังมีการปรับปรุงนโยบาย องค์กรควรทำอย่างไร?

- A. ไม่ต้องสนใจ
- B. รอให้มีการอบรมครั้งหน้า
- C. ต้องจัดอบรมซ้ำเฉพาะบุคคล และทดสอบอีกครั้ง
- D. ทำเป็นหนังสือเตือนทันที

เฉลย: C

คำอธิบาย: พนักงานต้องมีความเข้าใจและผ่านการอบรมทุกครั้งที่มีการปรับปรุงนโยบาย หากไม่ผ่านต้องเข้ารับการอบรมซ้ำเพื่อความเข้าใจและความปลอดภัยขององค์กร

**แบบทดสอบความเข้าใจเกี่ยวกับ นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล
(PDPA) ที่มีจำนวน 10 ข้อ (แต่ละข้อมี 1 คำตอบที่ถูกต้อง)**

เกณฑ์การให้คะแนนแบบทดสอบความเข้าใจนโยบายและแนวปฏิบัติ PDPA

- จำนวนข้อ: 10 ข้อ
- คะแนนเต็ม: 10 คะแนน
- รูปแบบการให้คะแนน:
ตอบถูก 1 ข้อ = 1 คะแนน
ตอบผิด 1 ข้อ = 0 คะแนน

ระดับคะแนนและการแปลผล

คะแนนรวม (เต็ม 10)	ระดับความ เข้าใจ	คำอธิบายผลการประเมิน
9 - 10 คะแนน	ดีมาก	เข้าใจนโยบายและแนวปฏิบัติด้าน PDPA อย่างถูกต้อง ครบถ้วน สามารถนำไปปฏิบัติได้จริง
7 - 8 คะแนน	ดี	เข้าใจโดยรวมได้ดี แต่ควรทบทวนรายละเอียดบางประเด็นเพื่อเพิ่ม ความมั่นใจในการปฏิบัติ
5 - 6 คะแนน	พอใช้	มีความเข้าใจในระดับปานกลาง ควรเข้าร่วมการอบรมเสริมหรืออ่าน เพิ่มเติมในบางเรื่อง
ต่ำกว่า 5 คะแนน	ต้องปรับปรุง	ไม่เข้าใจนโยบายเพียงพอ ควรเข้าร่วมอบรมเพิ่มเติมและทบทวน เอกสารนโยบายโดยละเอียดอีกครั้ง

แนวทางการจัดการตามผลคะแนน

- 7 คะแนนขึ้นไป ถือว่า "ผ่าน" ไม่จำเป็นต้องอบรมเพิ่มเติม แต่สามารถเข้าร่วมการอบรมเสริมได้ตาม
สมัครใจ
- ต่ำกว่า 7 คะแนน ให้พนักงานเข้ารับการอบรมซ้ำเฉพาะจุดที่ยังไม่เข้าใจ พร้อมทดสอบซ้ำอีกครั้ง

- เก็บประวัติผลการทดสอบ ในระบบทรัพยากรบุคคลหรือโดยผู้ดูแลด้าน DPO เพื่อประกอบการประเมินผลด้านการปฏิบัติตามนโยบายขององค์กร

ตัวอย่างการทำเอกสาร 2.3.4 องค์กรจัดทำแนวปฏิบัติ โปสเตอร์ หรือเอกสารตีพิมพ์ต่าง ๆ ที่ช่วยเน้นย้ำสาระสำคัญ สร้างความตระหนักรู้ในนโยบายและแนวปฏิบัติด้าน PDPA

ส่วนที่ 1: รายงานการประชุม

เรื่อง: การจัดทำสื่อสร้างความตระหนักรู้ด้าน PDPA สำหรับพนักงาน

วันที่ประชุม: 15 พฤษภาคม 2568

เวลา: 09:30 - 11:30 น.

สถานที่: ห้องประชุม 3 อาคารสำนักงานใหญ่

ผู้เข้าร่วมประชุม:

1. นาย A (ประธานการประชุม)
2. นาย B (ฝ่ายกฎหมาย)
3. นางสาว C (ฝ่ายทรัพยากรบุคคล)
4. นาย D (ฝ่าย IT)
5. นางสาว E (ฝ่ายสื่อสารองค์กร)
6. นาย F (ตัวแทนจาก DPO Office)

วาระการประชุม

1. เปิดประชุมโดยประธาน

นาย A กล่าวถึงข้อกำหนดตามมาตรา 37(1) ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศฯ เรื่องมาตรการรักษาความมั่นคงปลอดภัยฯ ข้อ 4(7) ว่าองค์กรจำเป็นต้องจัดทำสื่อหรือเอกสารเพื่อสร้างความตระหนักรู้ให้แก่พนักงานอย่างสม่ำเสมอ

2. พิจารณาการจัดทำแนวปฏิบัติเพื่อแปลงเป็นโปสเตอร์และเอกสารเผยแพร่

ที่ประชุมมีมติให้ดำเนินการจัดทำสื่อสร้างความตระหนักรู้ในรูปแบบต่าง ๆ ดังนี้:

รูปแบบสื่อ	เนื้อหาโดยสังเขป	จำนวนที่จัดทำ	ช่องทางการเผยแพร่
โปสเตอร์	“5 สิ่งที่พนักงานต้องรู้เกี่ยวกับ PDPA”	20 แผ่น	ติดตั้งบริเวณสำนักงานทุกชั้น
เอกสารสรุป 1 หน้า	“นโยบายคุ้มครองข้อมูลส่วนบุคคล – ฉบับเข้าใจง่าย”	100 ชุด	แจกในที่ประชุมและแนบอีเมล
PDF Infographic	“สิทธิของเจ้าของข้อมูลส่วนบุคคล”	1 ฉบับ	เผยแพร่ในอินทราเน็ตและไลน์กลุ่ม
Video Clip สั้น	“PDPA กับพนักงานในชีวิตประจำวัน”	1 ตอน	แสดงในจอ Digital Signage ทุกวันศุกร์

3. ปัญหาที่อาจเกิดขึ้น

- ความเข้าใจผิดเกี่ยวกับข้อยกเว้นของ PDPA
- บางหน่วยงานไม่เปิดอ่านเอกสารในระบบ
- ความเข้าใจเรื่อง “การแจ้งความยินยอม” ยังไม่ตรงกัน

4. มติที่ประชุม

- จัดอบรมเสริมสำหรับหัวหน้าแผนก เพื่อเป็นแกนกลางกระจายความรู้
- ส่งสื่อประชาสัมพันธ์ผ่านหลายช่องทาง ทั้งออนไลน์และออฟไลน์
- มอบฝ่ายสื่อสารองค์กรจัดทำ โปสเตอร์ และเอกสารตีพิมพ์ ภายใน 2 สัปดาห์

5. ปิดประชุม: เวลา 11:30 น.

ลงชื่อ.....

นาย A

(ประธานการประชุม)

ส่วนที่ 2: ตัวอย่างเอกสารประชาสัมพันธ์ (แนบท้ายรายงานการประชุม)

โปสเตอร์: “5 สิ่งที่พนักงานต้องรู้เกี่ยวกับ PDPA”

1. ห้ามเปิดเผยข้อมูลส่วนบุคคลของลูกค้า/เพื่อนร่วมงานโดยไม่มีสิทธิ
2. ต้องแจ้ง Privacy Notice ให้เจ้าของข้อมูลทราบเสมอ
3. ใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น และตามวัตถุประสงค์ที่แจ้งไว้
4. ห้ามส่งต่อข้อมูลให้บุคคลภายนอกโดยไม่ได้รับอนุญาต
5. หากพบการรั่วไหล ต้องแจ้ง DPO ภายใน 24 ชั่วโมง

สอบถามเพิ่มเติมได้ที่: DPO Office หรือฝ่ายทรัพยากรบุคคล

ในการจัดทำอาจลงรายละเอียดเพิ่มเติมเพื่อให้เกิดความเข้าใจโดยง่าย ตามตัวอย่างนี้

5 สิ่งที่พนักงานต้องรู้เกี่ยวกับ PDPA

เพื่อคุ้มครองข้อมูลส่วนบุคคลและหลีกเลี่ยงความเสี่ยงทางกฎหมาย

1. ห้ามเปิดเผยข้อมูลส่วนบุคคลของลูกค้า/เพื่อนร่วมงานโดยไม่มีสิทธิ

ห้ามนำข้อมูล เช่น ชื่อ-นามสกุล, เบอร์โทร, ที่อยู่, หมายเลขบัตรประชาชน ฯลฯ ไปเปิดเผยต่อผู้อื่น หรือใช้เกินกว่าหน้าที่

2. ต้องแจ้ง Privacy Notice ให้เจ้าของข้อมูลทราบเสมอ

ทุกครั้งที่มีการเก็บรวบรวมข้อมูลส่วนบุคคล ต้องแจ้งวัตถุประสงค์ วิธีใช้ ระยะเวลาจัดเก็บ และสิทธิของเจ้าของข้อมูล

3. ใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น และตามวัตถุประสงค์ที่แจ้งไว้

ห้ามนำข้อมูลไปใช้ในกิจกรรมอื่น ๆ ที่ไม่ได้แจ้งไว้ล่วงหน้า เช่น การตลาดเพิ่มเติมโดยไม่ได้รับความยินยอม

4. ห้ามส่งต่อข้อมูลให้บุคคลภายนอกโดยไม่ได้รับอนุญาต

การแชร์ข้อมูลไปยังผู้รับจ้าง ผู้ให้บริการ หรือหน่วยงานอื่น ต้องตรวจสอบข้อตกลงเรื่องการประมวลผลข้อมูลส่วนบุคคล (DPA) และได้รับอนุญาตก่อนเสมอ

5. หากพบการรั่วไหล ต้องแจ้ง DPO ภายใน 24 ชั่วโมง

หากพบว่าการรั่วไหลหรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ต้องรีบแจ้ง DPO หรือผู้ประสานงานภายในหน่วยงานทันที เพื่อดำเนินการแจ้งต่อสำนักงานคณะกรรมการฯ ภายใน 72 ชั่วโมง

หากมีข้อสงสัย ติดต่อฝ่ายกฎหมาย หรือ DPO ขององค์กร

Email: DPO@ชื่อองค์กร.com

โทรศัพท์: 02-XXX-XXXX ต่อ 1234

ตัวอย่างการทำเอกสาร 2.4.1 องค์กรจัดทำนโยบายและแนวปฏิบัติสำหรับการคุ้มครองข้อมูลส่วนบุคคล เพื่อสร้างจิตสำนึกให้แก่พนักงานทั่วองค์กร ในเรื่องการกำหนดค่าเริ่มต้นสำหรับการทำงาน

ตัวอย่าง “นโยบายและแนวปฏิบัติสำหรับการคุ้มครองข้อมูลส่วนบุคคล” ที่มุ่งเน้น การกำหนดค่าเริ่มต้นด้านความเป็นส่วนตัว (Privacy by Default) และ การคุ้มครองตั้งแต่การออกแบบ (Privacy by Design)

นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง: การกำหนดค่าเริ่มต้นด้านความเป็นส่วนตัว และการคุ้มครองตั้งแต่การออกแบบ

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0

วันที่มีผลบังคับใช้: [ระบุวันที่]

เจ้าของเอกสาร: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

อารัมภบท

ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และมาตรฐานสากล องค์กรมีหน้าที่ในการดูแลรักษาข้อมูลส่วนบุคคลอย่างรัดกุม ไม่เพียงแต่ในกระบวนการจัดเก็บหรือประมวลผลเท่านั้น แต่ยังรวมถึงขั้นตอนการออกแบบระบบ การวางนโยบาย และการดำเนินงานในทุกระดับ ซึ่งจะต้องคำนึงถึงความเป็นส่วนตัวของเจ้าของข้อมูลตั้งแต่ต้นทาง

เพื่อให้เป็นไปตามหลักการดังกล่าว องค์กรจึงยึดหลักแนวคิด 2 ประการสำคัญ ได้แก่:

แนวคิดที่สำคัญ

1. การคุ้มครองข้อมูลตั้งแต่การออกแบบ (Privacy by Design)

หมายถึงการฝังกลไกหรือมาตรการคุ้มครองข้อมูลส่วนบุคคลไว้ในทุกกระบวนการตั้งแต่การวางแผน ออกแบบระบบ พัฒนาโปรแกรม หรือเริ่มต้นกิจกรรมใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยไม่ถือเป็นภาระที่ต้องเพิ่มในภายหลัง

ตัวอย่าง:

หากมีการพัฒนาแอปพลิเคชันเก็บข้อมูลลูกค้า ฝ่ายพัฒนาจะต้องออกแบบระบบให้มีการขอความยินยอมแบบเลือกได้ และมีเมนูจัดการข้อมูลส่วนบุคคลของผู้ใช้อย่างโปร่งใส

หากมีการจัดทำแบบฟอร์มกระดาษเพื่อเก็บข้อมูลพนักงาน จะต้องออกแบบฟอร์มให้ระบุวัตถุประสงค์และเก็บเฉพาะข้อมูลที่จำเป็น

2. การกำหนดค่าเริ่มต้นที่คุ้มครองความเป็นส่วนตัว (Privacy by Default)

หมายถึงการตั้งค่าระบบหรือบริการให้คุ้มครองความเป็นส่วนตัวในระดับสูงสุดโดยอัตโนมัติ โดยไม่ต้องอาศัยการดำเนินการใด ๆ จากเจ้าของข้อมูล เช่น การปิดการเปิดเผยข้อมูลเป็นค่าตั้งต้น และไม่เก็บข้อมูลเกินความจำเป็น

ตัวอย่าง:

บริการจัดเก็บข้อมูลลูกค้าออนไลน์จะต้องตั้งค่าให้ไม่เปิดเผยข้อมูลส่วนตัวให้แก่บุคคลอื่นโดยอัตโนมัติ

ระบบกล้องวงจรปิด (CCTV) จะต้องตั้งค่าการจับภาพให้น้อยที่สุดเท่าที่จำเป็น และตั้งระยะเวลาการลบอัตโนมัติ

1. วัตถุประสงค์

เพื่อกำหนดแนวทางให้องค์กรสามารถคุ้มครองข้อมูลส่วนบุคคลของลูกค้า พนักงาน และผู้เกี่ยวข้องได้อย่างมีประสิทธิภาพ โดยฝังแนวคิดการออกแบบที่เคารพความเป็นส่วนตัวและกำหนดค่าความปลอดภัยเป็นมาตรฐานสูงสุดทุกขั้นตอน ตั้งแต่การออกแบบจนถึงการใช้งานจริง

2. ขอบเขต

นโยบายนี้ครอบคลุมทุกฝ่ายงาน บุคลากร ลูกจ้าง และบุคคลภายนอกที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลขององค์กร

3. นโยบายและแนวปฏิบัติหลัก

3.1 Privacy by Design

- ทุกระบบ งาน หรือกิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ต้องเริ่มต้นด้วยการวางแผนการคุ้มครองข้อมูลอย่างเป็นระบบ
- ต้องมีการประเมินผลกระทบด้านการคุ้มครองข้อมูล (DPIA) ก่อนเริ่มโครงการใหม่
- ตัวอย่างแนวปฏิบัติ:
- ระบบสมัครงานออนไลน์ จะต้องมีการแจ้งเตือนให้ผู้สมัครยินยอมให้เก็บและใช้ข้อมูล
- ระบบ CRM จะต้องสามารถปิดการเข้าถึงข้อมูลเฉพาะบางส่วนแก่พนักงานที่ไม่ได้รับมอบหมาย

3.2 Privacy by Default

- ระบบหรือบริการใด ๆ ต้องมีการตั้งค่าพื้นฐานที่คุ้มครองข้อมูลสูงสุด
- ไม่ควรมีการเปิดเผยข้อมูลโดยไม่ขอความยินยอมอย่างชัดเจน

ตัวอย่างแนวปฏิบัติ:

- เว็บไซต์ลงทะเบียนลูกค้า ต้องเก็บเฉพาะชื่อ อีเมล และเบอร์โทร หากไม่จำเป็นไม่ควรถามวันเดือนปีเกิดหรือที่อยู่
- ระบบอินเทอร์เน็ตขององค์กร ต้องตั้งค่าเริ่มต้นให้ซ่อนไฟล์หรือข้อมูลส่วนตัวของพนักงานจากผู้อื่น

4. การอบรมและสร้างจิตสำนึก

- จัดการอบรมประจำปีเกี่ยวกับแนวคิด Privacy by Design / Default และ PDPA สำหรับพนักงานทุกระดับ
- มีการจัดทดสอบหลังการอบรมเพื่อวัดความเข้าใจและกำหนดเกณฑ์ผ่านขั้นต่ำ
- ใช้โปสเตอร์ สื่ออินทราเน็ต และอีเมลประชาสัมพันธ์เพื่อย้ำเตือนพนักงานอย่างต่อเนื่อง

5. การประเมินผลและการกำกับดูแล

DPO มีหน้าที่ตรวจสอบและประเมินความสอดคล้องกับนโยบายอย่างสม่ำเสมอ ปรับปรุงแนวทางตามความเหมาะสมเมื่อมีการเปลี่ยนแปลงระบบ กฎหมาย หรือกระบวนการทำงาน

2.4.1 องค์กรมีนโยบายและขั้นตอนเพื่อให้แน่ใจว่าประเด็นการคุ้มครองข้อมูลได้รับการพิจารณาเมื่อมีการออกแบบและดำเนินการระบบ บริการ ผลิตภัณฑ์ และแนวทางธุรกิจที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลได้รับการคุ้มครองโดยค่าเริ่มต้น

นโยบายองค์กร

เรื่อง: นโยบายการกำหนดค่าเริ่มต้นในการออกแบบและพัฒนาระบบ ผลิตภัณฑ์ และบริการ
(Privacy by Design & Privacy by Default Policy)

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0

วันที่ประกาศใช้: [ระบุวันที่]

เจ้าของเอกสาร: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

หน่วยงานที่เกี่ยวข้อง: ทุกฝ่ายที่เกี่ยวข้องกับการพัฒนาระบบ IT, ผลิตภัณฑ์ และบริการ

1. อารัมภบท

ในยุคข้อมูลดิจิทัล การคุ้มครองข้อมูลส่วนบุคคลไม่ควรเป็นเพียงขั้นตอนภายหลังหรือการแก้ไขเมื่อเกิดปัญหา แต่ควรเป็น “ส่วนหนึ่ง” ที่ฝังอยู่ในการออกแบบตั้งแต่แรกของระบบ ผลิตภัณฑ์ หรือบริการ

นโยบายฉบับนี้จัดทำขึ้นเพื่อให้องค์กรสามารถดำเนินการตามหลักการ

- Privacy by Design (คุ้มครองความเป็นส่วนตัวส่วนตัวตั้งแต่การออกแบบ)
- Privacy by Default (การตั้งค่าความเป็นส่วนตัวส่วนตัวเป็นค่าเริ่มต้น)

ซึ่งเป็นหลักการตามมาตรฐานสากล และข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พ.ศ. 2562 (PDPA)

2. วัตถุประสงค์ของนโยบาย

- เพื่อกำหนดแนวทางในการพัฒนาระบบและบริการให้มีการออกแบบที่คำนึงถึงสิทธิของเจ้าของข้อมูล
- เพื่อให้ข้อมูลส่วนบุคคลได้รับการคุ้มครองอย่างสูงสุดตั้งแต่เริ่มต้น
- เพื่อสนับสนุนให้พนักงานและผู้พัฒนาระบบมีจิตสำนึกในด้านความเป็นส่วนตัว
- เพื่อให้ระบบหรือบริการขององค์กรสอดคล้องกับกฎหมายคุ้มครองข้อมูล

3. ขอบเขตการบังคับใช้

นโยบายนี้ครอบคลุมระบบ ผลิตภัณฑ์ หรือบริการทั้งหมดที่มีการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งที่พัฒนาโดยทีมภายใน หรือจัดซื้อจากบุคคลภายนอก และครอบคลุมทุกขั้นตอนของวงจรชีวิตข้อมูล ตั้งแต่การวางแผน การพัฒนา การให้บริการ การบำรุงรักษา ไปจนถึงการยุติการให้บริการ

4. หลักการและแนวทางปฏิบัติ

4.1 การคุ้มครองตั้งแต่การออกแบบ (Privacy by Design)

1. การประเมินความเสี่ยงล่วงหน้า (Pre-assessment):

ก่อนพัฒนาระบบหรือบริการใด ๆ ต้องมีการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (Data Protection Impact Assessment - DPIA) โดยฝ่ายพัฒนาและ DPO

ตัวอย่าง: แบบฟอร์ม DPIA จะถูกแนบกับข้อเสนอโครงการทุกครั้งก่อนอนุมัติ

2. การกำหนดมาตรการควบคุมข้อมูล:

ระบบต้องมีฟังก์ชันควบคุม เช่น การจำกัดการเข้าถึง, การเข้ารหัสข้อมูล, การ log การใช้งาน

3. การจำกัดข้อมูลให้เหลือเท่าที่จำเป็น (Data Minimisation):

ระบบจะต้องเก็บข้อมูลเฉพาะที่จำเป็นสำหรับวัตถุประสงค์ที่ชัดเจนเท่านั้น

ตัวอย่าง: ฟอร์มสมัครงานจะไม่เก็บเลขบัตรประชาชน เว้นแต่มีเหตุผลตามกฎหมาย

4. ฟังก์ชันยินยอมและถอนยินยอม:

ระบบต้องมีเมนูให้เจ้าของข้อมูลสามารถ “ให้” และ “ถอน” ความยินยอมได้ง่าย

5. การจัดเก็บข้อมูลอย่างปลอดภัย:

ต้องมีมาตรการการเข้ารหัส (Encryption), สำรองข้อมูล (Backup), และป้องกันการเข้าถึงโดยมิชอบ

4.2 การตั้งค่าความเป็นส่วนตัวเป็นค่าเริ่มต้น (Privacy by Default)

- ระบบจะต้องตั้งค่าความเป็นส่วนตัวสูงสุดโดยอัตโนมัติ:

เช่น ปิดการเปิดเผยข้อมูลต่อบุคคลภายนอกเป็นค่าเริ่มต้น ไม่เปิดใช้งานการติดตามโดยไม่ได้รับอนุญาต

- เปิดเผยเฉพาะสิ่งจำเป็น:

ระบบจะไม่เก็บหรือเปิดเผยข้อมูลเกินความจำเป็น เว้นแต่เจ้าของข้อมูลได้ยินยอม

- การตั้งค่าระยะเวลาการจัดเก็บ:

ระบบจะตั้งค่าการลบอัตโนมัติเมื่อครบระยะเวลาจัดเก็บตามวัตถุประสงค์

- ตัวอย่าง: Email ยืนยันการสมัครจะลบอัตโนมัติภายใน 90 วันหากไม่ได้ตอบกลับ
- ตัวเลือกต้องเป็นแบบ opt-in ไม่ใช่ opt-out:

เจ้าของข้อมูลต้องติ๊กเลือกให้ข้อมูลตนเองถูกใช้ (ไม่ใช่ติ๊กไว้ล่วงหน้า)

5. บทบาทและความรับผิดชอบ

หน่วยงาน/บุคคล	ความรับผิดชอบ
DPO	กำกับดูแลความสอดคล้องของระบบกับนโยบายนี้
ฝ่ายพัฒนา IT	ดำเนินการตามหลักการ Privacy by Design & Default
เจ้าของระบบ (System Owner)	ทำ DPIA และแจ้งผู้บริหารก่อนพัฒนา
ผู้บริหาร	ตรวจสอบและอนุมัติโครงการตามแนวนโยบาย

6. การอบรมและการสร้างความตระหนักรู้

- พนักงานที่เกี่ยวข้องกับการพัฒนาระบบ เช่น IT, ธุรกิจ, วิจัยและพัฒนา ต้องเข้ารับการอบรมเรื่อง Privacy by Design และ Privacy by Default ทุกปี
- จัดกิจกรรมและสื่อประชาสัมพันธ์ เช่น Infographic, คู่มือ, สื่อวิดีโอ เพื่อให้เข้าใจง่าย

7. การติดตามและตรวจสอบ

- มีการตรวจสอบระบบอย่างน้อยปีละ 1 ครั้ง โดยฝ่ายตรวจสอบภายในและ DPO
- รายงานผลต่อผู้บริหารระดับสูง พร้อมข้อเสนอแนะแก้ไขหากพบจุดอ่อน

8. การทบทวนนโยบาย

นโยบายนี้จะได้รับการทบทวนทุก 12 เดือน หรือเมื่อมีการเปลี่ยนแปลงในกฎหมายที่เกี่ยวข้อง

ตัวอย่างระบบเทคโนโลยีสารสนเทศ

ชื่อระบบ: ระบบจัดการคำขอของลูกค้า (Customer Data Request Management System - CDRMS)

วัตถุประสงค์ของระบบ

- อำนวยความสะดวกให้เจ้าของข้อมูลสามารถใช้สิทธิภายใต้ PDPA ได้อย่างสะดวก เช่น ขอเข้าถึง แก้ไข หรือขอลบข้อมูล
- ทำให้เจ้าหน้าที่สามารถติดตามคำขอได้อย่างเป็นระบบ
- บริหารจัดการข้อมูลตามหลัก **Privacy by Design** และ **Privacy by Default**

ฟีเจอร์หลักของระบบ (ตามแนว Privacy by Design & Default)

ฟีเจอร์	รายละเอียด	หลักการที่สอดคล้อง
1. ระบบยืนยันตัวตนแบบสองขั้น (2FA)	ผู้ยื่นคำขอต้องยืนยันตัวตนผ่าน OTP หรือ อีเมลก่อนเข้าถึงคำขอ	Privacy by Design
2. ตั้งค่าความเป็นส่วนตัวเริ่มต้นสูงสุด	เจ้าของข้อมูลต้อง opt-in สำหรับบริการ เช่น การรับข่าวสาร	Privacy by Default
3. เก็บข้อมูลเท่าที่จำเป็น (Minimisation)	แบบฟอร์มขอข้อมูลระบุเพียงชื่อและ ช่องทางติดต่อเท่านั้น	Privacy by Design
4. บันทึกการเข้าถึงข้อมูล (Audit Log)	ระบบบันทึกว่าใครเข้าถึงข้อมูลใดและ เมื่อใด	Privacy by Design
5. การลบข้อมูลอัตโนมัติ	ตั้งค่าให้ลบข้อมูลคำขอภายใน 90 วัน หลังจากดำเนินการเสร็จสิ้น	Privacy by Default
6. Dashboard สำหรับ DPO	แสดงจำนวนคำขอ ระยะเวลาดำเนินการ และสถานะของแต่ละคำขอ	Privacy by Design
7. แจ้งเตือนการรั่วไหล	หากระบบพบกิจกรรมผิดปกติ จะแจ้ง DPO ภายใน 1 ชม.	Privacy by Design
8. แบบฟอร์มถอนความยินยอมออนไลน์	มีลิงก์ให้เจ้าของข้อมูลสามารถถอน consent ได้ตลอดเวลา	Privacy by Design & Default

ตัวอย่างการใช้งาน

สถานการณ์:

ลูกค้าต้องการถอนความยินยอมในการรับอีเมลโปรโมชั่น

ขั้นตอนระบบ:

1. ลูกค้าเข้าสู่ระบบผ่าน OTP
2. ระบบแสดงเมนู “จัดการความยินยอม”

3. ระบบตั้งค่าการรับอีเมลเป็น "ปิด" โดยอัตโนมัติ (Default)
4. ลูกค้าสามารถยืนยันเพื่อถอนความยินยอมได้
5. ระบบบันทึกกิจกรรม พร้อมแจ้งเจ้าหน้าที่ที่รับทราบผ่าน Dashboard
6. ระบบส่งอีเมลแจ้งลูกค้าว่า “คำร้องขอสำเร็จ” พร้อม timestamp

ระบบนี้เหมาะสำหรับหน่วยงานใด?

- ฝ่าย IT และระบบงาน (สำหรับพัฒนาและปรับปรุงระบบบริการลูกค้า)
- ฝ่ายบริหารข้อมูลลูกค้า (CRM)
- หน่วยงาน DPO เพื่อควบคุมและติดตามการใช้สิทธิของเจ้าของข้อมูล
- หน่วยงาน HR (ในกรณีใช้สำหรับจัดการข้อมูลของพนักงาน)

ประโยชน์ของระบบ

- ป้องกันการใช้ข้อมูลโดยมิชอบ
- รองรับการตรวจสอบจากสำนักงานคุ้มครองข้อมูลส่วนบุคคล
- ลดความเสี่ยงด้านกฎหมาย ปรับ 3 ล้านบาท (ตามมาตรา 37)
- เพิ่มความเชื่อมั่นของลูกค้าและคู่ค้า

2.4.2 องค์กรมีนโยบายและขั้นตอนเพื่อให้แน่ใจว่าประเด็นการ คุ้มครองข้อมูลได้รับการพิจารณา เมื่อมีการออกแบบและดำเนินการระบบ บริการ ผลิตภัณฑ์ และแนวทางธุรกิจที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลได้รับการคุ้มครองโดยค่าเริ่มต้น

นโยบายเกี่ยวกับการกำหนดค่าเริ่มต้นในการออกแบบและพัฒนาระบบ ผลิตภัณฑ์ และบริการ (Privacy by Default Policy)

ประกาศโดย: [ชื่อองค์กร]

วันที่มีผลบังคับใช้: [วันที่]

ผู้มีหน้าที่รับผิดชอบ: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO), ฝ่ายพัฒนาเทคโนโลยี, ฝ่ายความมั่นคงปลอดภัยข้อมูล

1. วัตถุประสงค์ของนโยบาย

เพื่อกำหนดแนวทางในการออกแบบระบบ ผลิตภัณฑ์ และบริการขององค์กร ให้มีการกำหนดค่าความเป็นส่วนตัวที่ปลอดภัยสูงสุดโดยอัตโนมัติ (Privacy by Default) เพื่อให้มั่นใจว่า ข้อมูลส่วนบุคคลจะถูกเก็บรวบรวม ใช้ เผยแพร่ และจัดเก็บเท่าที่จำเป็น และมีมาตรการควบคุมความเป็นส่วนตัวตั้งแต่เริ่มต้น

2. ขอบเขตของนโยบาย

นโยบายนี้ใช้กับ:

- กระบวนการพัฒนาเทคโนโลยีสารสนเทศ (IT System Development)
- ระบบหรือบริการออนไลน์และออฟไลน์ที่เก็บหรือประมวลผลข้อมูลส่วนบุคคล
- ผลิตภัณฑ์ดิจิทัล เช่น แอปพลิเคชัน เว็บไซต์ และอุปกรณ์ IoT
- บุคลากรภายในฝ่ายพัฒนาระบบ ฝ่ายนโยบาย ฝ่ายกฎหมาย และผู้ให้บริการภายนอกที่เกี่ยวข้อง

3. แนวทางปฏิบัติ

3.1 ค่าเริ่มต้นต้องคุ้มครองความเป็นส่วนตัวสูงสุด

- ระบบหรือบริการใด ๆ ต้องถูกออกแบบให้เก็บข้อมูลเฉพาะที่จำเป็น (Data Minimization)
- การเปิดเผยข้อมูลต้องปิดไว้เป็นค่าเริ่มต้น (default setting) โดยผู้ใช้ต้องเป็นผู้เลือกอนุญาต (Opt-in)
- ตัวเลือกแชร์ข้อมูลกับบุคคลที่สามหรือภายนอกต้องถูกปิดไว้โดยอัตโนมัติ

3.2 ไม่ใช่ข้อมูลส่วนบุคคลเกินความจำเป็น

- ทุกฟีเจอร์ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลไว้ชัดเจนตามบทบาทของผู้ใช้งาน (Role-based Access Control)
- ไม่เก็บข้อมูลที่ไม่มีความสำคัญในการใช้งานโดยตรงหรือไม่จำเป็นตามขอบเขตที่แจ้งไว้

3.3 การตั้งค่าต้องโปร่งใสและเข้าใจง่าย

- ผู้ใช้งานต้องสามารถเข้าถึงการตั้งค่าความเป็นส่วนตัวและเปลี่ยนแปลงได้อย่างง่ายดาย
- ให้ข้อมูลประกอบการตัดสินใจที่ชัดเจนในภาษาที่เข้าใจง่าย (Plain Language)

3.4 รวม Privacy by Default ไว้ในขั้นตอนพัฒนา

- ในกระบวนการพัฒนา (DevOps / Agile) ต้องมีการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (Data Protection Impact Assessment - DPIA) ก่อนทุกการเปลี่ยนแปลง
- DPO ต้องเข้าร่วมให้คำแนะนำตั้งแต่ขั้นตอนการออกแบบ (Design Phase)

4. ตัวอย่างแนวปฏิบัติ

กรณีตัวอย่าง	แนวทางการกำหนดค่าเริ่มต้น
แบบฟอร์มออนไลน์	ไม่เลือกค่า opt-in โดยอัตโนมัติ ต้องให้ผู้ใช้เลือกเอง
แอปมือถือ	ปิดการเข้าถึงตำแหน่ง / รายชื่อเป็นค่าเริ่มต้น
ระบบ CRM	เข้าถึงข้อมูลลูกค้าเฉพาะเจ้าหน้าที่ที่ได้รับมอบหมาย
การตั้งค่าข่าวสาร	ผู้ใช้ต้องเลือกสมัครรับข่าวสารเอง (ไม่บังคับ)

5. การอบรมและการตรวจสอบ

- องค์กรจะจัดอบรมเกี่ยวกับ Privacy by Default อย่างน้อยปีละ 1 ครั้ง ให้กับ:
- ทีมพัฒนาและออกแบบระบบ
- ผู้บริหารฝ่ายผลิตภัณฑ์
- ทีม DPO และฝ่ายกฎหมาย
- มีการตรวจสอบนโยบายอย่างน้อยปีละ 1 ครั้ง และจัดทำรายงานต่อผู้บริหาร

6. การไม่ปฏิบัติตาม

หากมีการละเมิดนโยบาย องค์กรจะดำเนินการตามมาตรการทางวินัย รวมถึงอาจมีการแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และอาจมีบทลงโทษทางปกครองสูงสุดถึง 3 ล้านบาทตามที่กฎหมายกำหนด

7. การทบทวนและปรับปรุงนโยบาย

นโยบายฉบับนี้ จะได้รับการทบทวนและปรับปรุงอย่างสม่ำเสมออย่างน้อยทุก 12 เดือน หรือเมื่อมีเหตุอันควร เช่น การเปลี่ยนแปลงทางกฎหมายหรือเทคโนโลยี

ระบบเทคโนโลยีสารสนเทศที่กำหนดค่าเริ่มต้นตามแนวทาง Privacy by Default

1. ระบบลงทะเบียนสมาชิก (Membership Registration System)

ฟีเจอร์ที่ออกแบบตาม Privacy by Default:

- เก็บเฉพาะข้อมูลจำเป็น เช่น ชื่อ เบอร์โทร อีเมล (ไม่บังคับกรอกวันเกิด ที่อยู่ หรือข้อมูลสุขภาพ)
- ตั้งค่าให้ไม่แสดงข้อมูลสมาชิกให้สาธารณะเป็นค่าเริ่มต้น
- มีช่องเลือก “ขอไม่รับการติดต่อทางการตลาด” ถูกติ๊กไว้โดยอัตโนมัติ (opt-in ต้องสมัครใจ)

2. ระบบจัดการทรัพยากรบุคคล (HR Management System)

ฟีเจอร์:

- ข้อมูลสุขภาพและประวัติอาชญากรรม เข้ารหัสและแยกจัดเก็บโดยจำกัดการเข้าถึงเฉพาะ HR และผู้มีอำนาจ
- พนักงานสามารถดูข้อมูลส่วนตัวของตนเองได้แบบ read-only เพื่อป้องกันการแก้ไขโดยไม่ตั้งใจ
- แจ้งสิทธิของพนักงานตาม PDPA เช่น การขอถอนความยินยอม ลบข้อมูล หรือขอเข้าถึงข้อมูล

3. ระบบกล้องวงจรปิดอัจฉริยะ (Smart CCTV System)

ฟีเจอร์:

- แสดงป้ายประกาศการบันทึกภาพอย่างชัดเจนในพื้นที่มีการติดตั้งกล้อง
- กำหนดให้เก็บวิดีโอได้นานไม่เกิน 15 วันโดยอัตโนมัติ เว้นแต่จะมีเหตุจำเป็นที่ขอบด้วยกฎหมาย
- จำกัดสิทธิ์เข้าถึงเฉพาะผู้ดูแลระบบ และมีระบบตรวจสอบ log การเข้าดูย้อนหลัง

4. ระบบเว็บอีคอมเมิร์ซ (E-commerce Platform)

ฟีเจอร์:

- ไม่บังคับให้ลูกค้าสมัครสมาชิกก่อนซื้อของ
- ค่าเริ่มต้นของ “การแบ่งปันข้อมูลกับพันธมิตร” ตั้งเป็น “ปิด” เสมอ
- แสดง privacy notice ทันทีเมื่อเริ่มเก็บข้อมูล เช่น ก่อนกรอกแบบฟอร์มชำระเงิน

5. ระบบบริหารจัดการเอกสารภายใน (Document Management System)

ฟีเจอร์:

- ทุกเอกสารที่มีข้อมูลส่วนบุคคลถูกติดป้าย “ข้อมูลอ่อนไหว” โดยอัตโนมัติ
- ใช้นโยบาย role-based access control: แสดงเฉพาะเอกสารที่พนักงานมีสิทธิเข้าถึง
- มีระบบบันทึก log การดาวน์โหลดหรือแชร์เอกสารทุกครั้ง พร้อมแจ้งเตือนผู้ดูแลระบบ

6. แอปพลิเคชันบนมือถือขององค์กร

ฟีเจอร์:

- ถามความยินยอมก่อนเข้าถึงตำแหน่งกล้อง หรือไฟล์ในเครื่อง
- ไม่เปิดให้แอปซิงค์ข้อมูลรายชื่อติดต่อ (contact) กับเซิร์ฟเวอร์องค์กรโดยค่าเริ่มต้น
- มีปุ่ม “ลบบัญชีและข้อมูลทั้งหมด” ให้ผู้ใช้ดำเนินการได้เองภายในแอป

มาตรการสนับสนุนในระบบทั้งหมด:

- มี การเข้ารหัสข้อมูล (Encryption) ระหว่างรับ-ส่ง และจัดเก็บ
- มี การประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA) สำหรับระบบใหม่ทุกตัว
- มี การกำหนดค่าความปลอดภัยพื้นฐาน (Security Baseline Configuration) เป็นมาตรฐาน

Privacy by Default & Design Implementation Checklist สำหรับการออกแบบและพัฒนาระบบเทคโนโลยีสารสนเทศ ผลิตภัณฑ์ หรือบริการขององค์กรให้สอดคล้องกับหลักการการคุ้มครองข้อมูลตั้งแต่การออกแบบ (Privacy by Design) และ การกำหนดค่าเริ่มต้นที่คุ้มครองความเป็นส่วนตัว (Privacy by Default) ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Privacy by Default & Design Checklist

หมายเลข	รายการตรวจสอบ	ตรวจสอบแล้ว	หมายเหตุ
1	ระบบออกแบบโดย เก็บเฉพาะข้อมูลส่วนบุคคลที่จำเป็น เท่านั้น	☐	เช่น ชื่อ เบอร์โทร ไม่ขอข้อมูลที่ไม่เกี่ยวข้อง
2	มีการ แจ้งวัตถุประสงค์ในการเก็บข้อมูลอย่างชัดเจนก่อนเก็บ	☐	ผ่าน Privacy Notice หรือ กล่องข้อความแจ้งเตือน
3	ข้อมูลส่วนบุคคลจะไม่ถูกใช้เกินวัตถุประสงค์ที่แจ้งไว้	☐	มีระบบควบคุมการใช้ข้อมูล
4	มีการ ขอความยินยอมอย่างชัดเจน หากข้อมูลไม่อยู่ภายใต้ฐานทางกฎหมายอื่น	☐	เช่น กล่องติ๊กยินยอม (opt-in)
5	ตั้งค่าระบบให้เป็น “ไม่เปิดเผยข้อมูลโดยค่าเริ่มต้น” (Default Settings)	☐	เช่น ไม่เปิดแชร์ข้อมูลกับบุคคลภายนอกอัตโนมัติ
6	พนักงานหรือผู้ใช้สามารถ เลือกควบคุมข้อมูลส่วนบุคคลได้เอง	☐	เช่น แก้ไข หรือลบข้อมูลในระบบ
7	ข้อมูลส่วนบุคคลถูก เข้ารหัส (Encryption) ทั้งระหว่างส่งและจัดเก็บ	☐	ใช้ SSL, AES, ฯลฯ
8	มีระบบ แยกการจัดเก็บข้อมูลอ่อนไหว (Sensitive data) และจำกัดสิทธิ์	☐	เช่น สุขภาพ ประวัติ อาชญากรรม
9	ระบบบันทึก log การเข้าถึง แก้ไข หรือ ดาวน์โหลดข้อมูลส่วนบุคคล	☐	และตรวจสอบย้อนหลังได้

10	ระบบมีการแจ้งเตือนเมื่อพบความผิดปกติหรือเหตุการณ์ที่อาจนำไปสู่การรั่วไหลของข้อมูล	☐	เช่น แจ้งเตือนผู้ดูแลระบบ
11	มีการประเมินผลกระทบ (DPIA) ก่อนพัฒนาระบบใหม่หรือเปลี่ยนแปลงระบบที่มี	☐	โดย DPO หรือทีมที่ได้รับมอบหมาย
12	ระบบแสดง Privacy Notice ที่เหมาะสมตามวัยของเจ้าของข้อมูล	☐	เช่น เวอร์ชันสำหรับเด็ก หรือผู้สูงอายุ
13	มีการกำหนด Role-based Access Control เพื่อป้องกันการเข้าถึงโดยไม่จำเป็น	☐	จำกัดตามหน้าที่ของผู้ใช้
14	มี การเก็บหลักฐานความยินยอม (Consent Records)	☐	ระบุว่าใครให้ ยินยอมเมื่อไร และเกี่ยวกับอะไร
15	ระบบรองรับสิทธิของเจ้าของข้อมูล เช่น ขอเข้าถึง ลบ ระบุใช้ หรือคัดค้าน	☐	ผ่านแบบฟอร์มหรือเมนูในระบบ
16	พนักงานผู้เกี่ยวข้องได้รับการ อบรมเกี่ยวกับ Privacy by Design & Default	☐	มีหลักสูตร และแบบทดสอบความเข้าใจ
17	มีระบบ ควบคุมเวอร์ชันของนโยบายความเป็นส่วนตัว เป็นส่วนตัว (Policy Version Control)	☐	แสดงเวอร์ชันในระบบหรือเว็บไซต์
18	มีการจัดทำ โปสเตอร์/คู่มือ/สื่ออินโฟกราฟิก ภายในองค์กรเพื่อสื่อสารแนวปฏิบัติ	☐	เพื่อสร้างจิตสำนึกต่อเนื่อง

หมายเหตุเพิ่มเติม:

- การตรวจสอบควรทำทุกครั้งก่อน เปิดใช้ระบบจริง
- ควรจัดเก็บผลการประเมิน และลงลายมือชื่อของผู้รับผิดชอบ (เช่น DPO หรือทีมไอที)

2.4.3 องค์กรจัดให้มีวิธีการที่ไปสู่การปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคล การป้องกันสิทธิส่วนบุคคล ที่รวมถึงการจำกัดข้อมูลให้น้อยที่สุด การจำกัดวัตถุประสงค์การใช้งาน และการทำเป็นข้อมูลแฝง โดยมีการกำหนดไว้ในนโยบายและแนวปฏิบัติ

แนวปฏิบัติเพื่อกำหนดค่าเริ่มต้น (Privacy by Default) โดยมุ่งเน้น 3 ด้านหลัก ได้แก่

1. การจำกัดข้อมูลให้น้อยที่สุด (Data Minimisation)
2. การจำกัดวัตถุประสงค์การใช้งาน (Purpose Limitation)

3. การทำข้อมูลเป็นข้อมูลแฝง (Pseudonymisation)

แนวปฏิบัติเพื่อกำหนดค่าเริ่มต้นในการออกแบบและดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล (Privacy by Default Guidelines)

อาร์มภพ

เพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และหลักสากลของ “Privacy by Default” องค์กรต้องกำหนดให้ระบบ เทคโนโลยี และกระบวนการทำงานต่าง ๆ ตั้งค่าเริ่มต้นในการจัดการข้อมูลส่วนบุคคลอย่างปลอดภัยที่สุด โดยไม่ต้องอาศัยการกระทำเพิ่มเติมจากเจ้าของข้อมูล เช่น การตั้งค่าไม่ให้เปิดเผยข้อมูลโดยไม่จำเป็น หรือไม่บังคับให้กรอกข้อมูลที่ไม่เกี่ยวข้อง

เอกสารฉบับนี้จึงจัดทำขึ้นเพื่อเป็นแนวปฏิบัติเพื่อกำหนดค่าเริ่มต้นใน 3 ประเด็นสำคัญ ได้แก่ การจำกัดข้อมูลให้น้อยที่สุด การจำกัดวัตถุประสงค์การใช้งาน และการทำข้อมูลแฝง (pseudonymisation)

1. การจำกัดข้อมูลให้น้อยที่สุด (Data Minimisation)

แนวปฏิบัติ:

- ออกแบบแบบฟอร์ม / ระบบให้เก็บเฉพาะข้อมูลที่จำเป็น (need-to-know basis)
- หลีกเลี่ยงการขอข้อมูลส่วนบุคคลที่ไม่มีความเกี่ยวข้อง เช่น วันเกิด รหัสบัตรประชาชน เว้นแต่มีเหตุผลชัดเจนและชอบด้วยกฎหมาย
- ใช้ฟิลด์ “ไม่บังคับ” (optional) ให้ชัดเจน หากข้อมูลนั้นไม่จำเป็น
- ทบทวนฟอร์มและระบบเป็นระยะเพื่อคัดกรองข้อมูลที่ไม่จำเป็นออก

ตัวอย่าง:

ระบบสมัครสมาชิกควรเก็บเพียงชื่อ-นามสกุล และอีเมล โดยไม่จำเป็นต้องเก็บข้อมูลสุขภาพ ยกเว้นระบบที่เกี่ยวข้องกับการแพทย์

2. การจำกัดวัตถุประสงค์การใช้งาน (Purpose Limitation)

แนวปฏิบัติ:

- ระบุมัตถุประสงค์ของการเก็บรวบรวมข้อมูลอย่างชัดเจนใน Privacy Notice
- ห้ามใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นที่ไม่สอดคล้องกับวัตถุประสงค์เดิม เว้นแต่ได้ขอความยินยอมใหม่จากเจ้าของข้อมูล
- แยกข้อมูลตามวัตถุประสงค์ เช่น ฐานข้อมูลลูกค้า / ฐานข้อมูลพนักงาน / ฐานข้อมูลผู้สมัครงาน

- ติดตามสิทธิการเข้าถึง (access control) ให้ตรงกับบทบาทของผู้ใช้ระบบ เพื่อไม่ให้ใช้ข้อมูลข้ามวัตถุประสงค์

ตัวอย่าง:

ข้อมูลของผู้สมัครงานที่ไม่ผ่านการคัดเลือก ต้องไม่ถูกนำไปใช้เพื่อการตลาดหรือเสนอขายสินค้า เว้นแต่ได้รับความยินยอมใหม่

3. การทำข้อมูลแฝง (Pseudonymisation)

แนวปฏิบัติ:

- ใช้รหัสแทน (pseudonym) เช่น ID หรือ Token แทนข้อมูลระบุตัวบุคคลจริงในการประมวลผลข้อมูลภายใน
- แยกตารางหรือไฟล์ข้อมูลหลัก (ที่สามารถระบุตัวบุคคลได้) ออกจากข้อมูลที่ใช้วิเคราะห์ เพื่อป้องกันการย้อนกลับ
- กำหนดให้มีผู้มีอำนาจเท่านั้นที่สามารถเชื่อมข้อมูลกลับไปยังตัวบุคคลได้ (key-holders)
- ใช้เทคโนโลยีเข้ารหัส (encryption) และการควบคุมสิทธิการเข้าถึงร่วมกับ pseudonymisation เพื่อให้มีประสิทธิภาพสูงสุด

ตัวอย่าง:

การวิจัยเกี่ยวกับสุขภาพของพนักงานในองค์กร ควรใช้รหัสประจำตัวแทนชื่อ และตัดข้อมูลระบุตัวบุคคลออก (เช่น ชื่อ เบอร์โทร อีเมล) ก่อนส่งต่อให้ทีมวิเคราะห์

การควบคุมและติดตาม

- มีแบบฟอร์ม Privacy Impact Assessment (PIA) หรือ Data Protection Impact Assessment (DPIA) ทุกครั้งก่อนพัฒนาระบบที่มีการเก็บข้อมูลส่วนบุคคล
- DPO หรือคณะกรรมการคุ้มครองข้อมูลต้องตรวจสอบว่ามีการปฏิบัติตามแนวทางข้างต้นจริง
- พนักงานทุกฝ่ายต้องได้รับการฝึกอบรมเกี่ยวกับ Privacy by Default อย่างต่อเนื่อง

เอกสารตัวอย่างเกี่ยวกับ ระบบเทคโนโลยีสารสนเทศเพื่อกำหนดค่าเริ่มต้น (Privacy by Default) ซึ่งเน้น 3 ด้านสำคัญ ได้แก่

1. การจำกัดข้อมูลให้น้อยที่สุด (Data Minimisation)
2. การจำกัดวัตถุประสงค์การใช้งาน (Purpose Limitation)
3. การทำข้อมูลแฝง (Pseudonymisation)

ระบบเทคโนโลยีสารสนเทศเพื่อกำหนดค่าเริ่มต้นด้านความเป็นส่วนตัว
(Privacy by Default IT System)

1. วัตถุประสงค์ของระบบ

เพื่อสนับสนุนนโยบายและแนวปฏิบัติด้าน PDPA โดยระบบนี้ถูกออกแบบให้รองรับมาตรการ Privacy by Design และ Privacy by Default สำหรับการจัดเก็บ ประมวลผล และใช้งานข้อมูลส่วนบุคคล อย่างปลอดภัยและเหมาะสม

2. ฟีเจอร์และการทำงานของระบบ

2.1 การจำกัดข้อมูลให้น้อยที่สุด (Data Minimisation)

แนวทางระบบที่ใช้รองรับ:

- แบบฟอร์มอิเล็กทรอนิกส์ทุกประเภทมีฟีเจอร์ “smart field control”:
- ระบุว่า field ไหน “จำเป็น” และ field ไหน “ทางเลือก” (optional)
- ปิดการใช้งานช่องกรอกที่ไม่เกี่ยวข้องกับวัตถุประสงค์หลักของระบบ
- แบบฟอร์มผ่านการตรวจสอบโดย DPO หรือผู้รับผิดชอบ PDPA ก่อนใช้งานจริง
- ระบบแจ้งเตือนอัตโนมัติเมื่อมีการเพิ่มฟิลด์ใหม่ที่อาจละเมิดหลัก data minimisation

ตัวอย่าง:

ระบบสมัครงานจะเก็บเพียงข้อมูล ชื่อ-นามสกุล, อีเมล, หมายเลขโทรศัพท์ และคุณสมบัติตามตำแหน่ง โดยไม่มีการเก็บข้อมูลสุขภาพหรือศาสนา

2.2 การจำกัดวัตถุประสงค์การใช้งาน (Purpose Limitation)

แนวทางระบบที่ใช้รองรับ:

- ระบบแยกฐานข้อมูล (Database Segmentation) ตามประเภทของผู้ใช้งาน เช่น:
- ฐานข้อมูลลูกค้า
- ฐานข้อมูลพนักงาน
- ฐานข้อมูลผู้สมัครงาน
- มีระบบ Role-based Access Control (RBAC) ที่กำหนดให้ผู้ใช้งานเข้าถึงข้อมูลได้เฉพาะในขอบเขตของหน้าที่เท่านั้น
- การกำหนด “Tag วัตถุประสงค์” ให้ข้อมูลแต่ละชุด โดยระบบจะเตือนหากมีการนำข้อมูลไปใช้งานข้ามวัตถุประสงค์

ตัวอย่าง:

พนักงานฝ่ายบัญชีจะเข้าถึงข้อมูลของลูกค้าเพื่อออกใบเสร็จเท่านั้น ไม่สามารถนำไปใช้ในระบบ CRM หรือการตลาดได้

2.3 การทำข้อมูลแฝง (Pseudonymisation)

แนวทางระบบที่ใช้รองรับ:

ระบบ Data Processing Engine แยก 2 ชุดข้อมูล:

- ข้อมูลระบุตัวตน (PII) เช่น ชื่อ, เบอร์โทร
- ข้อมูลหลักที่ใช้ประมวลผล เช่น พฤติกรรมการใช้งาน, ผลประเมิน
- มีระบบสร้าง “Pseudonym Token” โดยใช้ UUID หรือ Token-based Identifier แทนข้อมูลระบุตัวตน
- ข้อมูลที่ใช้ในระบบวิเคราะห์จะถูก pseudonymise ทั้งหมดก่อนส่งต่อ (เช่น ระบบ BI หรือ AI)
- มี Key Vault แยกเก็บ mapping ระหว่าง Token กับข้อมูลตัวจริง โดยจำกัดสิทธิ์สูงสุดในการเข้าถึง

ตัวอย่าง:

ระบบวิเคราะห์ผลสุขภาพพนักงานใช้ Token “EMP_8xD92s” แทนชื่อจริง โดยไม่มีข้อมูลระบุตัวบุคคลใน dataset

3. องค์ประกอบเทคโนโลยีที่เกี่ยวข้อง

หมวดหมู่	เทคโนโลยี
แบบฟอร์มอัจฉริยะ	Web Form with Conditional Logic (เช่น Google Form + Add-on, Typeform, Microsoft Power Apps)
การจัดการฐานข้อมูล	PostgreSQL, MongoDB พร้อมการตั้งค่า RBAC
ระบบสร้าง Token	JSON Web Token (JWT), UUID Generator
ระบบเข้ารหัส/Key Vault	Azure Key Vault, AWS KMS, HashiCorp Vault
ระบบตรวจสอบสิทธิ์	LDAP/SSO, Role-based Access Control System
ระบบแจ้งเตือนการเปลี่ยนแปลงข้อมูล	Log Audit, Email Alert, Real-time Monitoring Tools (เช่น Splunk, ELK Stack)

4. การควบคุมและประเมินผล

- DPO ตรวจสอบแบบฟอร์มและระบบเป็นระยะทุก 6 เดือน
- ทุกครั้งที่มีการอัปเดตระบบ ต้องมี DPIA และการทดสอบ data minimisation
- จัดอบรมพนักงานประจำปี พร้อมแบบทดสอบ (Pre/Post-test) เกี่ยวกับ Privacy by Default

2.4.4 องค์การจัดให้มีนโยบายและแนวปฏิบัติสำหรับข้อมูลส่วนบุคคลของกลุ่มคนที่เปราะบาง เช่น เด็ก เยาวชน ผู้พิการให้ได้รับการป้องกันเป็นพิเศษ

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มเปราะบาง (Vulnerable Data Subjects Privacy Protection Policy)

1. บทนำ

องค์กรตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในสถานะเปราะบาง ซึ่งมีความเสี่ยงสูงต่อการถูกละเมิดสิทธิหรือได้รับผลกระทบมากกว่ากลุ่มทั่วไป องค์กรจึงจัดทำนโยบายฉบับนี้ขึ้นโดยยึดแนวทางของ GDPR (General Data Protection Regulation) และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. คำนิยามที่สำคัญ

"กลุ่มเปราะบาง" (Vulnerable Data Subjects) หมายถึง บุคคลที่อาจไม่สามารถใช้สิทธิคุ้มครองข้อมูลของตนเองได้อย่างเต็มที่ หรือมีสถานะความสัมพันธ์กับองค์กรที่ไม่สมดุล เช่น:

1. เด็ก (อายุต่ำกว่า 18 ปี)
2. ผู้สูงอายุ
3. ผู้พิการ
4. ผู้ที่มีข้อจำกัดด้านร่างกาย จิตใจ หรือสติปัญญา
5. ผู้ลี้ภัย / ผู้อพยพ / ผู้ขอลี้ภัย
6. ผู้ป่วยในสถานพยาบาล
7. ลูกจ้าง (ในความสัมพันธ์ที่มีอำนาจไม่สมดุล)
8. ผู้ต้องขัง
9. ผู้ที่ขาดแคลนโอกาสหรือความรู้ในการปกป้องสิทธิของตน
10. บุคคลในสถานการณ์ที่ถูกบังคับให้ให้ข้อมูล (ไม่สมัครใจอย่างแท้จริง)
- 11.

3. วัตถุประสงค์

เพื่อกำหนดแนวทางเฉพาะสำหรับการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลของกลุ่มเปราะบางอย่างเหมาะสม โดยต้องให้ความระมัดระวังเป็นพิเศษ

4. แนวปฏิบัติเฉพาะสำหรับกลุ่มเปราะบาง

4.1 เด็ก

- ต้องมีการขอความยินยอมจากผู้ปกครองก่อนเก็บข้อมูล
- การแจ้ง Privacy Notice ต้องใช้ภาษาที่เหมาะสมกับระดับอายุของเด็ก
- หลีกเลี่ยงการเก็บข้อมูลที่ไม่จำเป็น เช่น หมายเลขบัตรประจำตัวประชาชน

4.2 ผู้สูงอายุ / ผู้พิการ / ผู้มีข้อจำกัด

- แจ้งนโยบายด้วยภาษาที่เข้าใจง่าย

- หากมีตัวแทนทางกฎหมาย ต้องมีขั้นตอนชัดเจนในการยืนยันสิทธิของตัวแทน

4.3 ผู้ลี้ภัย / ผู้อพยพ / ผู้ที่ขาดความรู้

- ใช้ภาษาท้องถิ่นหรือจัดให้มีล่ามแปล
- เน้นการสร้างความเข้าใจถึงสิทธิในการถอนความยินยอม

4.4 ผู้ป่วย / ผู้ต้องขัง / บุคคลที่มีสถานะไม่สมดุลกับองค์กร

- ห้ามใช้ความยินยอมเป็นพื้นฐานทางกฎหมาย เว้นแต่จะพิสูจน์ได้ว่าเป็นความยินยอมโดยเสรีอย่างแท้จริง
- ส่งเสริมการใช้ฐานประโยชน์สาธารณะ หรือหน้าที่ตามกฎหมายแทน

5. มาตรการคุ้มครองเพิ่มเติม

- การจำกัดการเข้าถึงข้อมูลของเจ้าหน้าที่เฉพาะผู้มีหน้าที่โดยตรง
- การใช้มาตรการ "นามแฝงข้อมูล" (Pseudonymisation) ทุกครั้งที่สามารถทำได้
- มี DPO หรือเจ้าหน้าที่เฉพาะทางคอยให้คำปรึกษา
- อบรมเจ้าหน้าที่ให้ตระหนักถึงความเสี่ยงของการละเมิดสิทธิกลุ่มเปราะบาง

6. การแจ้งนโยบายและความโปร่งใส

- มีเอกสาร/สื่อเฉพาะกลุ่ม เช่น โปสเตอร์ วิดีโอ หรือคู่มือ ที่อธิบายสิทธิของเจ้าของข้อมูลกลุ่มเปราะบาง
- นโยบายฉบับนี้เผยแพร่ผ่านอินเทอร์เน็ต เว็บไซต์องค์กร และเอกสารแนบสัญญา (ถ้ามี)

7. การประเมินผลกระทบด้านการคุ้มครองข้อมูล (DPIA)

ทุกกรณีที่มีการประมวลผลข้อมูลของกลุ่มเปราะบาง ต้องดำเนินการทำ DPIA อย่างครบถ้วน

8. การปรับปรุงนโยบาย

องค์กรจะทบทวนและปรับปรุงนโยบายอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีกฎหมายหรือแนวทางใหม่จากหน่วยงานกำกับดูแล

Checklist: การประเมินกลุ่มเปราะบาง (Vulnerable Data Subject Assessment)

คำแนะนำการใช้งาน: ใช้เช็คลิสต์นี้ในการวิเคราะห์ข้อมูลส่วนบุคคลว่าเจ้าของข้อมูลเข้าข่ายเป็นกลุ่มเปราะบางหรือไม่ ก่อนดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ข้อ	คำถามประเมิน	ใช่ (✓)	ไม่ใช่ (✗)	หมายเหตุ
1	เจ้าของข้อมูลเป็นเด็กอายุต่ำกว่า 20 ปี หรือ ต่ำกว่าเกณฑ์ตามกฎหมายที่เกี่ยวข้องหรือไม่?			
2	เจ้าของข้อมูลเป็นผู้สูงอายุที่มีข้อจำกัดด้านร่างกายหรือจิตใจหรือไม่?			

3	เจ้าของข้อมูลเป็นผู้พิการทางร่างกาย จิตใจ หรือสติปัญญาหรือไม่?			
4	เจ้าของข้อมูลเป็นผู้ต้องโทษจำคุก หรืออยู่ในการควบคุมของรัฐหรือไม่?			
5	เจ้าของข้อมูลเป็นผู้มีปัญหาด้านสุขภาพจิต หรือไม่สามารถตัดสินใจด้วยตนเองได้หรือไม่?			
6	เจ้าของข้อมูลเป็นผู้พึ่งพิงทางเศรษฐกิจหรือการปกครอง เช่น ลูกจ้าง แรงงานข้ามชาติ หรือผู้ขอลี้ภัยหรือไม่?			
7	เจ้าของข้อมูลอยู่ในสถานการณ์ที่มีความเหลื่อมล้ำเชิงอำนาจกับผู้ควบคุมข้อมูล (เช่น นักเรียน - โรงเรียน, คนไข้ - โรงพยาบาล) หรือไม่?			
8	เจ้าของข้อมูลเป็นบุคคลที่อยู่ในภาวะฉุกเฉินหรือภัยพิบัติที่อาจไม่สามารถใช้สิทธิของตนได้เต็มที่หรือไม่?			
9	การประมวลผลข้อมูลนั้นเกี่ยวข้องกับข้อมูลอ่อนไหว (เช่น สุขภาพ ศาสนา เชื้อชาติ หรือความเชื่อทางการเมือง) หรือไม่?			
10	เจ้าของข้อมูลไม่สามารถเข้าถึงนโยบาย Privacy Notice ได้อย่างเข้าใจหรือไม่?			

คำแนะนำหลังจากประเมิน

หากตอบ “ใช่” ตั้งแต่ 1 ข้อขึ้นไป: ควรพิจารณาว่าเจ้าของข้อมูลนั้นอาจเป็น กลุ่มเปราะบาง และต้องมีมาตรการคุ้มครองเป็นพิเศษตาม GDPR เช่น:

- การขอความยินยอมโดยชัดแจ้ง
- อธิบายนโยบายให้เข้าใจง่าย
- ลดปริมาณข้อมูลที่เก็บให้น้อยที่สุด
- ทำ Pseudonymisation หรือ Anonymisation
- ให้สามารถถอนความยินยอมได้ง่าย
- หากตอบ “ใช่” มากกว่า 3 ข้อ: ต้องมีการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA) อย่างเคร่งครัด

แบบฟอร์มขอความยินยอมจากผู้ปกครองสำหรับการเก็บ รวบรวม และประมวลผลข้อมูลส่วนบุคคลของเด็ก (Parental Consent Form for Child Data Processing)

ส่วนที่ 1: ข้อมูลพื้นฐานองค์กร

ชื่อองค์กร/หน่วยงาน :

ที่อยู่ :

เบอร์ติดต่อ/อีเมล :

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) :

ชื่อ-สกุล :

เบอร์โทรศัพท์ :

อีเมล :

ส่วนที่ 2: คำนำและวัตถุประสงค์

เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) องค์กร/หน่วยงานต้องได้รับความยินยอมจากผู้ปกครองก่อนดำเนินการเก็บ รวบรวม และประมวลผลข้อมูลส่วนบุคคลของเด็กผู้เยาว์ (อายุต่ำกว่า 18 ปี) ข้อมูลส่วนบุคคลเหล่านี้จะถูกใช้เพื่อวัตถุประสงค์ที่ชัดเจน ดังรายละเอียดในแบบฟอร์มนี้ หากท่านยินยอม กรุณากรอกข้อมูลและลงลายมือชื่อในส่วนที่กำหนด

ส่วนที่ 3: ข้อมูลเกี่ยวกับเด็ก

ข้อมูล	รายละเอียด
1. ชื่อ-นามสกุลเด็ก	_____
2. วันเดือนปีเกิด	____ / ____ / _____ (พ.ศ.) (เด็กอายุ _____ ปี)
3. หมายเลขประจำตัวประชาชน/หนังสือเดินทาง (ถ้ามี)	_____
4. โรงเรียน / สถานศึกษา (หากเกี่ยวข้อง)	_____

ส่วนที่ 4: ข้อมูลเกี่ยวกับผู้ปกครอง

ข้อมูล	รายละเอียด
1. ชื่อ-นามสกุลผู้ปกครอง	_____
2. ความสัมพันธ์กับเด็ก	_____
3. หมายเลขประจำตัวประชาชน/หนังสือเดินทาง	_____
4. ที่อยู่ที่สามารถติดต่อได้	_____
5. หมายเลขโทรศัพท์	_____
6. อีเมล (ถ้ามี)	_____

ส่วนที่ 5: ประเภทข้อมูลส่วนบุคคลที่จะเก็บรวบรวม

โปรดทำเครื่องหมาย ✓ ในช่องข้อมูลที่ท่านยินยอมให้เก็บรวบรวมและประมวลผล (สามารถเลือกได้มากกว่า 1 ประเภท)

หมวดหมู่ข้อมูล	คำอธิบาย / ตัวอย่างข้อมูล	ยินยอม (✓)
ข้อมูลระบุตัวตนเบื้องต้น	ชื่อ-นามสกุล, วันเดือนปีเกิด, หมายเลขบัตรประชาชน / หนังสือเดินทาง	
ข้อมูลติดต่อ	ที่อยู่ปัจจุบัน, เบอร์โทรศัพท์, อีเมล	
ข้อมูลด้านสุขภาพ	ประวัติการเจ็บป่วย, ภูมิแพ้, ข้อมูลสุขภาพทั่วไป	
ข้อมูลการศึกษา	ชื่อโรงเรียน, ระดับชั้น, ผลการเรียน	
ข้อมูลภาพถ่าย/วิดีโอ	ภาพถ่ายใบหน้า, ภาพกิจกรรม, วิดีโอที่ถ่ายในกิจกรรมขององค์กร	
ข้อมูลพฤติกรรมออนไลน์	ประวัติการเข้าชมเว็บไซต์, ข้อมูลการใช้งานในแอปพลิเคชันขององค์กร	
ข้อมูลความเห็นหรือความคิดเห็น	ข้อความหรือคำถามที่เด็กเขียนหรือส่งให้กับองค์กร	
ข้อมูลอื่น ๆ (โปรดระบุ)	_____	

ส่วนที่ 6: วัตถุประสงค์ในการใช้ข้อมูล

โปรดอ่านวัตถุประสงค์แต่ละข้อ แล้วทำเครื่องหมาย ✓ ในช่องที่ท่านยินยอมให้เด็กได้รับการประมวลผลข้อมูลตามวัตถุประสงค์นั้น (สามารถเลือกได้มากกว่า 1 ข้อ)

วัตถุประสงค์	รายละเอียดการใช้งาน	ยินยอม (✓)

1. การให้บริการ / กิจกรรมการศึกษา	ใช้ข้อมูลสำหรับจัดกิจกรรมสอนหนังสือ จัดค่ายส่งเสริมการเรียนรู้ หรือโครงการพัฒนาทักษะ	
2. การดูแลด้าน สุขภาพและความปลอดภัย	ใช้ข้อมูลสุขภาพเพื่อติดตามการเจ็บป่วย หรือแจ้งเตือนในกรณีฉุกเฉิน	
3. การถ่ายภาพ/ วิดีโอเพื่อ ประชาสัมพันธ์	ใช้ภาพถ่ายหรือวิดีโอของเด็กเผยแพร่บนเว็บไซต์หรือสื่อสังคมขององค์กร (เช่น เฟซ Facebook, YouTube) เพื่อประชาสัมพันธ์กิจกรรม	
4. การประมวลผล ข้อมูลเชิงสถิติ / วิจัย	ใช้ข้อมูลแบบทำเป็นนามแฝง (pseudonymised) เพื่อวิเคราะห์ สร้างรายงาน หรือวิจัย มิได้เปิดเผยตัวตน	
5. การติดต่อแจ้ง ข่าวสาร / กิจกรรมอื่น ๆ	ส่งอีเมลหรือ SMS แจ้งข่าวสาร กิจกรรมค่ายเสริมทักษะ หรืองานประชุมผู้ปกครอง	
6. การประเมินการใช้งานแพลตฟอร์ม / ผลตอบรับ	ใช้ข้อมูลพฤติกรรมออนไลน์เพื่อปรับปรุงระบบเว็บไซต์, แอปพลิเคชัน หรือสื่อการสอนให้เหมาะสมกับเด็ก	
7. อื่น ๆ (โปรดระบุ)	_____	

ส่วนที่ 7: ระยะเวลาการเก็บรักษาข้อมูล

- ข้อมูลส่วนบุคคลของเด็กจะถูกเก็บรักษา **ไม่เกินจนสิ้นสุดโครงการหรือกิจกรรม และ ไม่เกิน 5 ปี** นับจากวันที่สิ้นสุดกิจกรรม
- ข้อมูลสุขภาพจะถูกเก็บรักษา **ไม่เกิน 1 ปี** หลังสิ้นสุดโครงการ หรือจนกว่าบิดามารดาจะร้องขอลบข้อมูล
- ภาพถ่าย/วิดีโอที่ใช้เพื่อประชาสัมพันธ์ จะถูกเผยแพร่ **ไม่เกิน 3 ปี** บริหารจัดการโดยฝ่ายสื่อสารองค์กร หากต้องการเก็บเกินกำหนด ต้องมีการขอความยินยอมใหม่

ส่วนที่ 8: สิทธิของเจ้าของข้อมูลและผู้ปกครอง

ผู้ปกครองมีสิทธิดังนี้ (สำหรับข้อมูลของบุตรหลาน)

1. สิทธิรับทราบ: รับทราบข้อมูลวัตถุประสงค์ วิธีการเก็บใช้ และเปิดเผยข้อมูล
2. สิทธิเข้าถึงข้อมูล: ขอเข้าดูข้อมูลส่วนบุคคลที่บุตรหลานให้ไว้
3. สิทธิแก้ไขข้อมูล: ขอแก้ไขข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์
4. สิทธิลบข้อมูล: ขอให้ลบข้อมูลเมื่อหมดความจำเป็นหรือหากให้ความยินยอมโดยไม่ได้รับอนุญาต

5. สิทธิจำกัดการใช้ข้อมูล: ขอจำกัดการใช้ข้อมูลจนกว่าจะมีการพิสูจน์ความถูกต้อง
6. สิทธิคัดค้านการประมวลผล: ขอคัดค้านหากเชื่อว่าการใช้ข้อมูลบุตรหลานขัดต่อความเป็นส่วนตัว
7. สิทธิย้ายข้อมูล: ขอรับข้อมูลในรูปแบบที่องค์กรกำหนดให้เพื่อนำไปใช้กับผู้ควบคุมข้อมูลรายอื่นได้
8. สิทธิถอนความยินยอม: ถอนความยินยอมที่เคยให้ไว้ได้ทุกเมื่อ โดยไม่ต้องให้เหตุผล
เพื่อใช้สิทธิใด ๆ โปรดติดต่อ
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
โทร. _____
อีเมล _____

ส่วนที่ 9: การลงลายมือชื่อรับทราบและยินยอม

ข้าพเจ้า (ผู้ปกครอง/ผู้มีอำนาจปกครอง)

ชื่อ-สกุล: _____

ลายมือชื่อ: _____

วันที่: ____ / ____ / ____ (พ.ศ.)

ข้าพเจ้าได้อ่าน นโยบาย/Privacy Notice และแนวปฏิบัติขององค์กรแล้ว และให้ความยินยอมในการเก็บ รวบรวม ใช้ และประมวลผลข้อมูลส่วนบุคคลของบุตรหลานตามรายละเอียดข้างต้นเป็นไปตามวัตถุประสงค์ที่กำหนดไว้ข้างต้น

ส่วนที่ 10: สำหรับเจ้าหน้าที่องค์กร

สรุปรายการข้อมูลที่ได้รับ ความยินยอม:

ประเภทข้อมูลที่เก็บ: _____

วัตถุประสงค์ที่ได้รับการยินยอม: _____

ระยะเวลาการเก็บรักษา: _____

เจ้าหน้าที่รับเรื่อง:

ชื่อ-สกุล: _____

ตำแหน่ง: _____

ลายมือชื่อ: _____

วันที่: ____ / ____ / ____ (พ.ศ.)

หมายเหตุสำคัญ:

1. หากท่านไม่ให้ความยินยอม องค์กรอาจไม่สามารถให้บริการหรือจัดกิจกรรมที่เกี่ยวข้องกับบุตรหลานของท่านได้ครบถ้วน

2. ในกรณีที่ข้อมูลมีการเปลี่ยนแปลง (เช่น เบอร์โทรศัพท์หรือที่อยู่) โปรดแจ้งองค์กรเพื่ออัปเดตข้อมูลทันที
3. หากมีข้อสงสัยเพิ่มเติมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล กรุณาติดต่อ DPO ขององค์กร

บทที่ 4

การจัดทำเอกสารที่เกี่ยวกับการอบรมและการสร้างความตระหนักรู้

การสร้างความตระหนักรู้และความรู้ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นหัวใจสำคัญในการสร้างวัฒนธรรมการปฏิบัติตาม PDPA ขององค์กร การอบรมบุคลากรและการจัดทำเอกสารประกอบช่วยให้พนักงานทุกระดับเข้าใจหน้าที่ สิทธิ และข้อกำหนดที่เกี่ยวข้อง ทั้งในการเก็บ ใช้ เปิดเผย และรักษาความลับของข้อมูลส่วนบุคคล ด้านนี้จึงมุ่งเน้นการจัดทำเอกสารการอบรม คู่มือ แนวทางปฏิบัติ และสื่อสร้างความตระหนักรู้ ที่สามารถตรวจสอบได้ และนำไปใช้จริง เพื่อประเมินผลการรับรู้และการปฏิบัติตามมาตรการคุ้มครองข้อมูลอย่างครบถ้วน

การคุ้มครองข้อมูลส่วนบุคคลเป็นประเด็นสำคัญที่องค์กรทุกประเภทต้องให้ความสนใจอย่างจริงจัง เนื่องจากข้อมูลส่วนบุคคลถือเป็นทรัพย์สินที่มีคุณค่าและมีความละเอียดอ่อน การละเมิดหรือการจัดการข้อมูลที่ไม่เหมาะสมอาจส่งผลกระทบต่อความเชื่อมั่นของผู้เกี่ยวข้องทั้งภายในและภายนอกองค์กร รวมถึงอาจมีผลทางกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ดังนั้น การสร้างความตระหนักรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้กับบุคลากรทุกระดับ จึงเป็นหนึ่งในกลไกสำคัญของการบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลและการสร้างวัฒนธรรมองค์กรที่ใส่ใจด้านความปลอดภัยของข้อมูล การอบรมและการสร้างความตระหนักรู้เกี่ยวกับ PDPA ไม่ใช่เพียงการสอนเนื้อหากฎหมายหรือข้อกำหนดทางเทคนิคเท่านั้น แต่ยังเป็นกระบวนการสร้างความเข้าใจในบทบาท หน้าที่ และความรับผิดชอบของบุคลากรในการจัดเก็บ ใช้ เปิดเผย และรักษาความลับของข้อมูลส่วนบุคคลอย่างเหมาะสม การจัดทำเอกสารประกอบการอบรม เช่น คู่มือ สไลด์ แผ่นพับ หรือสื่อออนไลน์ รวมถึงการเผยแพร่สื่อสร้างความตระหนักรู้ผ่านโปสเตอร์ อีเมล หรือ Infographic จะช่วยให้ข้อมูลสามารถเข้าถึงบุคลากรได้ทุกกลุ่ม ทั้งยังเป็นหลักฐานที่สามารถตรวจสอบและยืนยันได้ว่าองค์กรได้ดำเนินการสร้างความตระหนักรู้อย่างจริงจัง

นอกจากนี้ การอบรมควรครอบคลุมทั้งการอบรมทั่วไปสำหรับพนักงานทุกระดับ และการอบรมเฉพาะกลุ่ม (Role-based Training) สำหรับหน่วยงานหรือบุคลากรที่มีหน้าที่จัดการข้อมูลสำคัญ เช่น ฝ่ายบุคคล ฝ่าย IT หรือหน่วยงานที่เกี่ยวข้องโดยตรง เพื่อให้แน่ใจว่าผู้ปฏิบัติงานมีความรู้และทักษะที่สอดคล้องกับบทบาทและหน้าที่ของตน การประเมินผลหลังการอบรม เช่น แบบสอบถามก่อน-หลังการอบรม การทำ Quiz

หรือการติดตามผลการปฏิบัติจริง จะช่วยให้สามารถปรับปรุงเนื้อหาและรูปแบบการอบรมให้มีประสิทธิภาพมากขึ้น

สุดท้าย การบันทึกและจัดเก็บหลักฐานการอบรมเป็นสิ่งสำคัญสำหรับการตรวจสอบ Compliance ขององค์กร การมีระบบบันทึกที่เป็นระเบียบ ครอบคลุมการเข้าร่วมอบรมของบุคลากรทุกคน พร้อมกับการทบทวนและปรับปรุงเอกสารอบรมอย่างต่อเนื่อง จะช่วยสร้างวัฒนธรรมการปฏิบัติตาม PDPA อย่างยั่งยืน และเป็นหลักฐานที่สามารถนำเสนอในการประเมินหรือการตรวจสอบภายในและภายนอกองค์กรได้อย่างชัดเจน

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
3.1 การจัดทำแผนอบรม PDPA	จัดทำแผนการอบรมและกิจกรรมสร้างความตระหนักรู้สำหรับบุคลากรทุกระดับ พร้อมกำหนดความถี่และหัวข้อ	แผนอบรม/Training Plan ระบุผู้เข้าร่วมและหัวข้อ	มีแผนอบรมชัดเจน ครอบคลุมทุกกลุ่มบุคลากร และเป็นปัจจุบัน
3.2 การจัดทำเอกสารประกอบการอบรม	จัดทำสไลด์ เอกสารประกอบ หรือคู่มือสำหรับใช้ในการอบรมและเวิร์กช็อป	เอกสารประกอบการอบรม เช่น สไลด์ คู่มือ เอกสารแจก	มีเอกสารครบถ้วน ใช้งานได้จริง และอัปเดตตามกฎหมายหรือแนวทางใหม่
3.3 การสร้างสื่อสร้างความตระหนักรู้	จัดทำโปสเตอร์ อีเมลแจ้งเตือน สื่อออนไลน์ หรือ Infographic เพื่อเผยแพร่ความรู้ด้าน PDPA	ตัวอย่างสื่อสร้างความตระหนักรู้ เช่น โปสเตอร์ ภาพประกาศ อีเมลข่าวสาร	มีการเผยแพร่หลายช่องทาง ตรวจสอบได้ว่าพนักงานเข้าถึงและรับรู้
3.4 การอบรมเฉพาะกลุ่ม (Role-based Training)	จัดอบรมเฉพาะกลุ่มตามหน้าที่ เช่น ฝ่ายบุคคล ฝ่าย IT หรือหน่วยงานที่จัดการข้อมูลสำคัญ	บันทึกการอบรมเฉพาะกลุ่ม ระบุหัวข้อและผู้เข้าร่วม	มีหลักฐานการอบรมที่เหมาะสมกับบทบาทและหน้าที่ของแต่ละกลุ่ม

3.5 การติดตามและประเมินผล	ประเมินผลการอบรม เช่น แบบสอบถามก่อน-หลัง การทำ Quiz หรือการประเมินผลปฏิบัติจริง	แบบสอบถาม คะแนน Quiz รายงาน ประเมินผลการอบรม	มีหลักการประเมินผล และแสดงให้เห็นว่ามีการปรับปรุงตามผลประเมิน
3.6 การบันทึกและจัดเก็บหลักฐานการอบรม	เก็บข้อมูลการอบรมของบุคลากรแต่ละคนอย่างเป็นระบบ เพื่อใช้ตรวจสอบ Compliance	รายการเข้าร่วมอบรม Attendance Sheet, ระบบ e-Learning Log	มีระบบบันทึกและจัดเก็บครบถ้วน ตรวจสอบย้อนหลังได้
3.7 การทบทวนและปรับปรุงสื่อ/เอกสารอบรม	ปรับปรุงเนื้อหาอบรมและเอกสารประกอบอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมาย/นโยบาย	บันทึก Version Control ของเอกสารอบรม รายงานการประชุมปรับปรุง	มีหลักการปรับปรุงเอกสารและสื่ออย่างต่อเนื่อง
3.8 การสร้างวัฒนธรรมความตระหนักรู้ต่อเนื่อง	จัดกิจกรรมเสริม เช่น การประกวด การประชาสัมพันธ์ภายใน หรือ แคมเปญความตระหนักรู้	รายงานกิจกรรม ผลตอบรับจากบุคลากร ภาพกิจกรรม	มีหลักฐานกิจกรรมต่อเนื่อง แสดงให้เห็นการสร้างวัฒนธรรมองค์กร PDPA

การจัดทำเอกสารตามเกณฑ์

3.1.1 องค์กรจัดทำหลักสูตรการอบรมแก่พนักงานเพื่อสร้างความตระหนักเรื่องการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย

รายงานการประชุมผู้บริหารอาวุโส เรื่อง การพิจารณาและอนุมัติหลักสูตรอบรมสร้างความตระหนักด้านการคุ้มครองข้อมูลส่วนบุคคล ครั้งที่: 1/2568 วันที่ประชุม: 22 มิถุนายน 2568 เวลา: 10.00 – 11.30 น. สถานที่: ห้องประชุมผู้บริหาร อาคารสำนักงานใหญ่ ชั้น 3 ผู้เข้าร่วมประชุม: - นาย X — ประธานเจ้าหน้าที่บริหาร (CEO) (ประธานการประชุม) - นางสาว Y — รองกรรมการผู้จัดการใหญ่ ฝ่ายทรัพยากรบุคคล (COO)

3. นาย Z — รองกรรมการผู้จัดการใหญ่ ฝ่ายกฎหมาย (CLO)
4. นาย A — ประธานเจ้าหน้าที่เทคโนโลยี (CTO)
5. นางสาว B — ประธานเจ้าหน้าที่ปฏิบัติการ (COO)
6. นาย C — เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
7. นางสาว D — ผู้อำนวยการฝ่ายฝึกอบรมและพัฒนา (L&D Director)
8. นางสาว E — หัวหน้าฝ่ายตรวจสอบภายใน
9. เจ้าหน้าที่ฝ่ายทรัพยากรบุคคล ฝ่ายกฎหมาย และฝ่ายไอที รวม 15 คน

วาระการประชุม

วาระที่ 1: กล่าวเปิดการประชุม

ประธานการประชุม (CEO) กล่าวถึงข้อกำหนดตาม มาตรา 37(1) ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4(7) ว่าผู้ควบคุมข้อมูลส่วนบุคคล ต้องจัดให้มีการสร้างความตระหนักแก่พนักงานเกี่ยวกับนโยบายและแนวปฏิบัติ เพื่อหลีกเลี่ยงบทลงโทษ ปรับทางปกครองสูงสุดไม่เกิน 3 ล้านบาท (ตามบทลงโทษของมาตรา 37)

วาระที่ 2: นำเสนอหลักสูตรอบรมสร้างความตระหนักด้าน PDPA

ผู้อำนวยการฝ่ายฝึกอบรมและพัฒนา (L&D Director) ได้นำเสนอ โครงร่างหลักสูตรอบรม ซึ่งแบ่งเนื้อหาออกเป็น 4 โมดูลหลัก:

ภาพรวมของกฎหมาย PDPA และประกาศฯ ที่เกี่ยวข้อง

- สิทธิของเจ้าของข้อมูล, พ.ร.บ. PDPA, ประกาศ คปภ. ข้อ 4(7)
- บทลงโทษ (ปรับสูงสุด 3 ล้านบาท)

นโยบายและแนวปฏิบัติขององค์กร

- นโยบายคุ้มครองข้อมูล (Privacy Policy)
- แนวปฏิบัติการจัดการข้อมูล (Data Handling Guidelines)
- การกำหนดค่าเริ่มต้นด้านความเป็นส่วนตัว (Privacy by Default)

กรณีศึกษาและบทเรียนจากเหตุการณ์ละเมิดข้อมูล

- ตัวอย่างที่เกิดขึ้นทั้งในและต่างประเทศ
- แนวทางปฏิบัติเมื่อเกิดเหตุ (Incident Response)

เทคนิคการปฏิบัติตาม PDPA ในงานประจำวัน

- การตรวจสอบคำขอใช้สิทธิจากเจ้าของข้อมูล
- การขอความยินยอมและการเก็บรักษา Consent Log
- การดูแลรักษาความมั่นคงปลอดภัยเบื้องต้น (เช่น การเข้ารหัสด้วย 2FA, การเข้ารหัสไฟล์, การกำหนดสิทธิ์เข้าถึง)

จุดเน้นสำคัญ:

- เนื้อหาสอดคล้องกับ นโยบาย: เช่น “เมื่อใดที่ต้องขอความยินยอม” “การกำหนดค่าเริ่มต้นให้ปลอดภัย”
- ใช้ รูปแบบการสื่อสารหลายช่องทาง ได้แก่ สไลด์บรรยาย วิดีโอสั้น กรณศึกษา และแบบทดสอบ (Pre- / Post- Test)
- กำหนด ระยะเวลาอบรม: 3 ชั่วโมง (9.00 – 12.00 น.)

กลุ่มเป้าหมาย: พนักงานทุกคน โดยเฉพาะพนักงานฝ่ายกฎหมาย, ไอที, ฝ่ายบริการลูกค้า, ฝ่าย HR และผู้เกี่ยวข้องกับการจัดการข้อมูล

วาระที่ 3: พิจารณาความสอดคล้องกับนโยบายองค์กร

รองกรรมการผู้จัดการใหญ่ ฝ่ายกฎหมาย (CLO) ชี้แจงว่าเนื้อหาหลักสูตรสอดคล้องกับ มาตรา 37(1) ซึ่งกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องรักษามาตรการรักษาความมั่นคงปลอดภัยโดยคำนึงถึงพฤติกรรมผู้ใช้ และ ประกาศ คปภ. ข้อ 4(7) ที่ระบุว่าให้จัดให้มีการฝึกอบรมแก่พนักงาน

ยืนยันหลักสูตรครอบคลุมประเด็นตามกฎหมาย และลิงก์ไปยังเอกสารทางกฎหมาย (PDPA, ประกาศ คปภ.) เพื่อให้พนักงานศึกษาตามลำดับ

วาระที่ 4: การขออนุมัติจากผู้บริหารอาวุโส

ประธานการประชุม (CEO) สอบถามว่าหลักสูตรนี้มีความสอดคล้องกับ กลยุทธ์องค์กรด้านการคุ้มครองข้อมูล ที่กำหนดไว้หรือไม่

L&D Director ตอบว่า

1. หลักสูตรเชื่อมโยงกับนโยบาย “Privacy by Default” และ “Privacy by Design” ขององค์กร
2. มีเป้าหมายสร้างวัฒนธรรมองค์กรในการคุ้มครองข้อมูลตั้งแต่ต้นทาง
3. ใช้กรณีศึกษาให้เห็นภาพการละเมิดข้อมูล เพื่อสร้างความตระหนัก

รองกรรมการผู้จัดการใหญ่ ฝ่ายทรัพยากรบุคคล (COO) ยืนยันว่าเนื้อหาหลักสูตรตอบโจทย์การพัฒนาทรัพยากรบุคคลและลดความเสี่ยงองค์กร

ดีพลิง DPO ยืนยันความครบถ้วนของสาระ สำคัญด้านสิทธิเจ้าของข้อมูล เทคนิคทางเทคนิค และแนวทางรับมือเหตุละเมิด

วาระที่ 5: มติที่ประชุม

มติที่ 1: อนุมัติหลักสูตรอบรมสร้างความตระหนักด้าน PDPA ฉบับปรับปรุงตามที่เสนอ โดยเสียงเอกฉันท์

มติที่ 2: กำหนดให้จัดอบรมพนักงานทั้งหมดครั้งแรกภายใน 30 วัน นับจากวันที่ประชุม

มติที่ 3: กำหนดให้ ทบพวนหลักสูตร ทุกปี หรือตามการเปลี่ยนแปลงกฎหมาย/นโยบายใหม่

มติที่ 4: ให้ ฝ่ายทรัพยากรบุคคล (HR) รับผิดชอบการจัดตารางอบรม และ ฝ่ายกฎหมาย/ DPO
รับผิดชอบสรุปเนื้อหากฎหมาย

ผู้บันทึกการประชุม

นางสาว D — ผู้อำนวยการฝ่ายฝึกอบรมและพัฒนา (L&D Director)

ผู้ตรวจสอบและอนุมัติรายงาน

นาย X — ประธานเจ้าหน้าที่บริหาร (CEO)

ลงวันที่: 22 มิถุนายน 2568

เอกสารอ้างอิง:

1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1)
2. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (7)
3. บทลงโทษปรับทางปกครอง (สูงสุดไม่เกิน 3 ล้านบาท) ตามมาตรา 37 ผลการฝ่าฝืนไม่จัดอบรมตามกำหนด

หมายเหตุ:

- หลังการประชุม HR จะจัดส่งอีเมลแจ้งพนักงานทุกแผนก พร้อมแนบโครงสร้างหลักสูตรและ Link ลงทะเบียนอบรม
- เมื่อพนักงานเข้ารับการอบรมเสร็จสิ้น จะจัดทำรายงานสรุปคะแนน Pre-Test / Post-Test และ เก็บในแฟ้มประวัติบุคคล

จบบทงาน กระแสดำเนินการตามที่ประชุม.

3.1.2 หลักสูตรการอบรมมีความครอบคลุมและรวมถึงการ ฝึกอบรมให้แก่พนักงานทั้งหมดในเรื่องที่สำคัญ ๆ หรือไม่เช่น การจัดการคำขอต่าง ๆ การแชร์ข้อมูล การรักษาความ มั่นคงปลอดภัยของข้อมูล การ ละเมิดข้อมูล การบริหาร จัดการต่าง ๆ ที่เกี่ยวข้องกัข้อมูลส่วนบุคคล

รายงานการประชุมผู้บริหารอาวุโส

เรื่อง การพิจารณาและอนุมัติหลักสูตรอบรมสร้างความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล

(PDPA Awareness & Compliance Workshop)

ครั้งที่: 1/2568

วันที่ประชุม: วันอังคารที่ 22 มิถุนายน 2568

เวลา: 10.00 – 12.00 น.

สถานที่: ห้องประชุมผู้บริหาร อาคารสำนักงานใหญ่ ชั้น 3

ผู้เข้าร่วมประชุม (ผู้บริหารระดับสูง และผู้เกี่ยวข้อง):

- นาย A — ประธานเจ้าหน้าที่บริหาร (CEO) (ประธานการประชุม)
- นาย B — ประธานเจ้าหน้าที่ปฏิบัติการ (COO)
- นาย C — รองกรรมการผู้จัดการใหญ่ ฝ่ายทรัพยากรบุคคล (CHRO)
- นาย D — รองกรรมการผู้จัดการใหญ่ ฝ่ายกฎหมาย (CLO)
- นาย E — ประธานเจ้าหน้าที่เทคโนโลยี (CTO)
- นาย F — ประธานเจ้าหน้าที่ตรวจสอบภายใน (CAO)
- นาย G — เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- นางสาว H — ผู้อำนวยการฝ่ายฝึกอบรมและพัฒนา (L&D Director)
- ผู้แทนจากฝ่ายไอที (IT), ฝ่ายกฎหมาย (Legal), ฝ่ายทรัพยากรบุคคล (HR), ฝ่ายบริการลูกค้า (Customer Service) รวมทั้งสิ้น 15 คน

ระเบียบวาระการประชุม

วาระที่ 1: กล่าวเปิดการประชุม (10.00 – 10.10 น.)

นาย A (CEO) กล่าวเปิดประชุมโดยย้ำถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 37(1) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยฯ พ.ศ. 2565 ข้อ 4(7)

เน้นว่า “องค์กรต้องจัดให้มีการอบรมพนักงานทุกคน เพื่อสร้างความตระหนักรู้ และหากไม่ปฏิบัติตามอาจถูกปรับทางปกครองสูงสุด 3 ล้านบาท”

ย้ำเป้าหมายว่าหลักสูตรต้องเชื่อมโยงกับ กลยุทธ์องค์กรด้านการกำกับดูแลข้อมูลและวัฒนธรรมความเป็นส่วนตัว (Data Governance & Privacy Culture)

วาระที่ 2: นำเสนอร่างหลักสูตรอบรม PDPA (PDPA Awareness & Compliance Workshop) (10.10 – 10.40 น.)

นางสาว H (ผู้อำนวยการฝ่ายฝึกอบรมและพัฒนา) ได้นำเสนอโครงสร้างหลักสูตรอบรม ซึ่งมีรายละเอียดดังนี้:

2.1 ภาพรวมหลักสูตร

ชื่อหลักสูตร: “อบรมสร้างความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA Awareness & Compliance Workshop)”

ระยะเวลาอบรม: 3 ชั่วโมง (09.00–12.00 น.)

กลุ่มเป้าหมาย:

- พนักงานทุกคนในองค์กร (ทุกหน่วยงาน)
- พนักงานฝ่ายไอที (IT), ฝ่ายกฎหมาย (Legal), ฝ่ายทรัพยากรบุคคล (HR), ฝ่ายบริการลูกค้า (Customer Service), ฝ่ายการตลาด (Sales & Marketing)
- หัวหน้างานและผู้จัดการทุกระดับ

วิธีการสอน:

- บรรยายพร้อมสไลด์ (Slide Presentation)
- กรณีศึกษาเชิงโต้ตอบ (Interactive Case Studies)
- แบบฝึกปฏิบัติ (Hands-on Exercises)
- แบบทดสอบก่อนและหลังอบรม (Pre-Test / Post-Test)
- การอภิปรายกลุ่มย่อย (Breakout Discussions)

2.2 โครงสร้างหลักสูตร (โมดูล)

โมดูลที่ 1: ภาพรวมกฎหมาย PDPA และประกาศ คปภ. (30 นาที)

รายละเอียดเนื้อหา:

1.1 โครงสร้างและเจตนารมณ์ของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

1.2 บทบาทหน้าที่ของ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC)

1.3 สิทธิของเจ้าของข้อมูล (Data Subject Rights):

- สิทธิรับทราบ (Right to be Informed)
- สิทธิขอเข้าถึง (Right of Access)
- สิทธิแก้ไข (Right to Rectification)
- สิทธิลบข้อมูล (Right to Erasure / “Right to be Forgotten”)
- สิทธิจำกัดการประมวลผล (Right to Restrict Processing)
- สิทธิคัดค้านการประมวลผล (Right to Object)
- สิทธิย้ายข้อมูล (Right to Data Portability)
- สิทธิถอนความยินยอม (Right to Withdraw Consent)

1.4 บทลงโทษตามมาตรา 37(1) (โทษปรับไม่เกิน 3 ล้านบาท) หากไม่จัดอบรมหรือไม่ปฏิบัติตาม

1.5 ข้อกำหนดตาม ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคง

ปลอดภัยฯ พ.ศ. 2565 ข้อ 4(7) ว่า “ผู้ควบคุมข้อมูลต้องจัดอบรมพนักงาน และวางมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล”

วิธีการสอน:

- บรรยายพร้อมสไลด์สรุปบทกฎหมาย
- แสดงกรณีตัวอย่างการละเมิดข้อมูลจริง (Domestic & International)

- ถาม-ตอบ (Q&A) เพื่อให้เข้าใจข้อกำหนด

โมดูลที่ 2: นโยบายและแนวปฏิบัติเครื่องจักรกลองค์กร (40 นาที)

รายละเอียดเนื้อหา:

2.1 การคุ้มครองข้อมูลตั้งแต่การออกแบบ (Privacy by Design):

- ความหมายและหลักการ
- การฝังมาตรการคุ้มครองข้อมูลตั้งแต่ขั้นตอนออกแบบระบบ (Data Minimisation, Role-Based Access, Encryption)

- ตัวอย่าง: การออกแบบฟอร์มสมัครงานให้เก็บเฉพาะข้อมูลจำเป็น

2.2 การกำหนดค่าเริ่มต้นที่คุ้มครองความเป็นส่วนตัว (Privacy by Default):

- การตั้งค่าระบบให้ปลอดภัยสูงสุดเป็นค่าเริ่มต้น (Default Secure Settings)
- ตัวอย่าง: แอปพลิเคชันองค์กรตั้งค่าไม่แชร์ข้อมูลตำแหน่งโดยอัตโนมัติ

2.3 หลักการกำหนดค่าเริ่มต้น (Default Settings):

- การแยกสิทธิ์ (Segregation of Duties)
- การบังคับใช้การเข้ารหัส (Encryption) และการบันทึกเหตุการณ์ (Logging) เป็นค่าเริ่มต้น

2.4 แนวปฏิบัตินโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Corporate Privacy Policy):

- การกำหนดเจ้าของเอกสารนโยบาย (Document Owner)
- การทบทวนเวอร์ชันนโยบายเป็นระยะ

2.5 การคุ้มครองข้อมูลกลุ่มเปราะบาง (Privacy for Vulnerable Data Subjects):

- เด็ก, ผู้สูงอายุ, ผู้พิการ, ผู้ลี้ภัย ฯลฯ
- การขอความยินยอมจากผู้ปกครอง (กรณีเด็ก)
- การใช้วิธีทำนามแฝง (Pseudonymisation) / การทำให้ไม่สามารถระบุตัวบุคคล (Anonymisation)

วิธีการสอน:

นำเสนอสไลด์ตัวอย่างนโยบายองค์กร

แบ่งกลุ่มอภิปรายกรณีศึกษาการออกแบบระบบที่ไม่สอดคล้อง (Breakout Discussion)

ฝึกปฏิบัติตั้งค่า Default ในระบบจำลอง (IT Sandbox Exercise)

โมดูลที่ 3: การจัดการคำขอของเจ้าของข้อมูล (Data Subject Request Handling) (30 นาที)

รายละเอียดเนื้อหา:

3.1 ประเภทคำขอ (DSR):

- การเข้าถึง (Access), ปรับปรุง (Rectification), ลบ (Erasure), จำกัดการใช้ (Restriction), ย้ายข้อมูล (Portability), คัดค้าน (Objection), ถอนความยินยอม (Withdrawal)

3.2 กระบวนการรับคำขอ:

- ช่องทางรับคำขอ (อีเมล, เว็บไซต์, จดหมาย)
- การตรวจสอบตัวตน (Identity Verification)
- การบันทึกคำขอลงระบบ (DSR Log)

3.3 การดำเนินการภายใน 30 วัน:

- การประเมินคำขอ
- การอนุมัติหรือปฏิเสธ พร้อมอ้างเหตุผลทางกฎหมาย

3.4 การบันทึกหลักฐานและการแจ้งกลับเจ้าของข้อมูล

วิธีการสอน:

- สาธิตการกรอก “ฟอร์มคำขอของเจ้าของข้อมูล (DSR Form)” บนระบบจำลอง
- แบบฝึกปฏิบัติ (Role Play) รับคำขอและดำเนินการในระบบจำลอง
- ถาม-ตอบ (Q&A) เพื่อแยกแยะกรณีต่าง ๆ (เช่น คำขอลบข้อมูล vs คำขอเข้าถึงข้อมูล)

โมดูลที่ 4: การแชร์ข้อมูลอย่างปลอดภัย (Data Sharing & Third-Party Management) (30 นาที)

รายละเอียดเนื้อหา:

4.1 หลักการการแบ่งปันข้อมูลภายในองค์กร:

- หลักการจำเป็นต้องใช้ (Need-to-Know Basis)
- การควบคุมการเข้าถึงตามบทบาท (Role-Based Access Control, RBAC)

4.2 การแชร์ข้อมูลกับบุคคลหรือองค์กรภายนอก:

- การทำข้อตกลง “สัญญาประมวลผลข้อมูล (Data Processing Agreement, DPA)”
- การประเมินความเสี่ยงบุคคลภายนอก (Third-Party Risk Assessment)
- การเข้ารหัสไฟล์ และการส่งผ่านช่องทางปลอดภัย (SFTP, HTTPS)

4.3 การแชร์ข้อมูลกับหน่วยงานรัฐ:

ข้อกฎหมายที่อนุญาตให้แชร์ (Legal Basis: หน่วยงานราชการ, คำสั่งศาล)

4.4 กรณีตัวอย่าง การรั่วไหลข้อมูลจากการแชร์ไฟล์ไม่เข้ารหัส

วิธีการสอน:

- นำเสนอผังโครงสร้างกระบวนการแบ่งปันข้อมูล (Data Sharing Workflow Diagram)
- แจกตัวอย่าง “สัญญาประมวลผลข้อมูล (DPA Template)” ให้นั่งอ่านและวิเคราะห์เงื่อนไขข้ออื่น ๆ
- ถาม-ตอบ (Q&A) เพื่อให้เห็นความเสี่ยงจากแต่ละกรณีการแชร์ข้อมูล

โมดูลที่ 5: การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security Best Practices) (40 นาที)

รายละเอียดเนื้อหา:

5.1 การยืนยันตัวตนและการควบคุมการเข้าถึง (Authentication & Access Control):

- นโยบายรหัสผ่าน (Password Policy: ความยาวขั้นต่ำ, การผสมอักขระ, การเปลี่ยนรหัสทุก 90 วัน)
- การเปิดใช้งานการยืนยันตัวตนสองชั้น (Two-Factor Authentication, 2FA / Multi-Factor Authentication, MFA)
- การใช้ระบบ “เซ็นชื่อครั้งเดียว” (Single Sign-On, SSO)

5.2 การเข้ารหัสข้อมูล (Encryption):

- ข้อมูลขณะส่ง (Transport Encryption: TLS 1.2+)
- ข้อมูลขณะจัดเก็บ (At-Rest Encryption: AES-256, Database Encryption)

5.3 ความมั่นคงปลอดภัยเครือข่าย (Network Security):

- Firewall, ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection/Prevention, IDS/IPS)
- การแยกเครือข่าย (Network Segmentation) สำหรับระบบข้อมูลอ่อนไหว

5.4 ความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Security):

- การติดตั้งโปรแกรมป้องกันไวรัส/มัลแวร์ (Antivirus/Antimalware)
- การตั้งค่า “การเข้ารหัสทั้งดิสก์ (Full-Disk Encryption)” บนอุปกรณ์คอมพิวเตอร์/โน้ตบุ๊ก
- หลีกเลี่ยงการใช้ USB/External Drive ที่ไม่ได้รับอนุญาต

5.5 การจัดการช่องโหว่และแพตช์ (Patch Management & Vulnerability Management):

- สแกนหา “ช่องโหว่ทางระบบ (Vulnerabilities)” รายสัปดาห์
- อัปเดตแพตช์ความปลอดภัยทันทีเมื่อมีประกาศแพตช์

5.6 การสำรองข้อมูลและกู้คืน (Data Backup & Recovery):

- นโยบายสำรองข้อมูลรายวัน/รายสัปดาห์
- ทดสอบกระบวนการกู้คืนข้อมูล (Disaster Recovery / Business Continuity Plan)

5.7 ความปลอดภัยอุปกรณ์พกพาและมือถือ (Mobile & Device Security):

- การตั้งค่า “การจัดการอุปกรณ์พกพา (Mobile Device Management, MDM)” สำหรับอุปกรณ์ขององค์กร
- การเข้ารหัสและการล็อกหน้าจออัตโนมัติ

5.8 การตรวจสอบและแจ้งเตือนความปลอดภัย (Security Monitoring & Alerting):

- ใช้ระบบ “การจัดการข้อมูลเหตุการณ์ความปลอดภัย (Security Information and Event Management, SIEM)” เช่น Splunk, ELK
- ตั้งค่า “แจ้งเตือน (Alert)” เมื่อพบพฤติกรรมผิดปกติ (Unauthorized Access, Multiple Failed Login Attempts)

วิธีการสอน:

- สาธิตการตั้งค่า 2FA บนระบบองค์กร (เช่น Microsoft 365 หรือ Google Workspace)

- ให้นักงานปฏิบัติ “การเข้ารหัสและถอดรหัสไฟล์ (Encrypt & Decrypt a File)” โดยใช้ซอฟต์แวร์ OpenSSL หรือ VeraCrypt
- สาธิตการใช้ “เครื่องมือสแกนหาช่องโหว่ (Vulnerability Scanner)” เช่น Nessus หรือ OpenVAS บนระบบจำลอง
- ถาม-ตอบ (Q&A) เพื่อให้เข้าใจมาตรการป้องกันเชิงเทคนิค

โมดูลที่ 6: การจัดการเหตุละเมิดข้อมูล (Data Breach Response & Management) (30 นาที)

รายละเอียดเนื้อหา:

6.1 คำนิยาม “เหตุละเมิดข้อมูลส่วนบุคคล (Data Breach)” ตาม PDPA และ GDPR

6.2 ขั้นตอนการตรวจจับและประเมินเหตุละเมิด (Detection & Assessment):

- การตรวจพบสัญญาณเตือนภัย (Indicators of Compromise, IoC)
- การประเมิน “ความรุนแรง (Severity)” และ “ผลกระทบ (Impact)” ของเหตุละเมิด

6.3 กระบวนการแจ้งภายในองค์กร (Internal Notification):

- แจ้ง DPO และทีมรักษาความปลอดภัยภายใน 24 ชั่วโมง (หรือทันทีเมื่อพบเหตุ)
- การบันทึก “แบบบันทึกเหตุละเมิดข้อมูล (Incident Report Form)”

6.4 กระบวนการแจ้งภายนอก (External Notification):

- แจ้งการแจ้ง “สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” ภายใน 72 ชั่วโมง
- แจ้งการแจ้งเจ้าของข้อมูล (Data Subject) เมื่อมีความเสี่ยงต่อสิทธิ/เสรีภาพ

6.5 มาตรการจำกัดความเสียหายและเยียวยา:

- เปลี่ยนรหัสผ่านที่ได้รับผลกระทบ ยกเลิกการเข้าถึง (Revoke Access) อัปเดตแพตช์
- แนะนำเจ้าของข้อมูลที่ได้รับผลกระทบ (Data Subject Guidance)

6.6 การทำรายงานสรุปหลังเหตุการณ์ (After-Action Review, AAR):

- สรุปรายงานเหตุการณ์ (Post-Incident Report)
- การปรับปรุงมาตรการป้องกันและนโยบาย

วิธีการสอน:

- จำลองสถานการณ์ “เหตุรั่วไหลของบัญชีผู้ใช้ (Database Exfiltration)” ให้กลุ่มย่อยแบ่งบทบาทเป็น IT, DPO, ฝ่ายกฎหมาย จัดกระบวนการตอบสนอง
- แจก “ฟอร์มบันทึกเหตุละเมิดข้อมูล (Incident Report Form)” ให้นักเรียนกรอกข้อมูลจำลอง
- ถาม-ตอบ (Q&A) เพื่อปรับปรุงแผนตอบสนอง

3. การอบรมเชิงปฏิบัติการ (Hands-on Workshop)

(จัดแยกต่างหากเป็นวันถัดไป 2 ชั่วโมง)

Scenario 1: การจัดการคำขอเข้าถึงข้อมูล (DSR Exercise)

พนักงานจับคู่ดำเนินการรับคำขอ ตรวจสอบตัวตน ดำเนินการในระบบ ส่งอีเมลแจ้งผล

Scenario 2: การตั้งค่า 2FA บนบัญชีพนักงาน

ให้พนักงานตั้งค่า 2FA บนอุปกรณ์จำลอง (เช่น Google Authenticator)

Scenario 3: การทำข้อมูลเป็นนามแฝง (Pseudonymisation) ในชุดข้อมูลจำลอง

ใช้ Excel/VBA หรือสคริปต์พื้นฐาน (Python) เพื่อเปลี่ยนข้อมูลระบุตัวบุคคลเป็น Token

Scenario 4: การตอบสนองเหตุละเมิดข้อมูล

จำลองเหตุ “Database Exfiltration” ให้พนักงานทำ “แบบบันทึกเหตุละเมิดข้อมูล (Incident Report)” และสรุป “รายงานหลังเหตุการณ์ (After-Action Report)”

4. แบบทดสอบวัดผล (Pre-Test & Post-Test)

- Pre-Test (ก่อนอบรม): 10 คำถามปรนัย เน้นพื้นฐาน PDPA และความรู้ทั่วไปเกี่ยวกับข้อมูลกลุ่มเปราะบาง
- Post-Test (หลังอบรม): 20 คำถามปรนัย + 2 กรณีศึกษา ให้วิเคราะห์แนวทางปฏิบัติ

เกณฑ์ผ่าน: 80% ขึ้นไป

บันทึกผล:

- ฝ่ายฝึกอบรมและพัฒนา (L&D) จะเก็บผล Pre-/Post-Test ไว้ในแฟ้มประวัติพนักงาน
- หัวหน้างานจะได้รับรายงานสำหรับพนักงานที่ไม่ผ่านและกำหนดแผนอบรมซ้ำ

5. เอกสารประกอบการอบรม

5.1 คู่มือการปฏิบัติตาม PDPA (PDPA Compliance Handbook) (PDF)

สรุปบทกฎหมาย แนวทางองค์กร คำถามที่พบบ่อย (FAQ)

5.2 สไลด์ PowerPoint สำหรับแต่ละโมดูล

โมดูล 1–6 แยกสไลด์

5.2 แบบฟอร์มคำขอของเจ้าของข้อมูล (Data Subject Request Form)

รูปแบบ PDF/Word และตัวอย่างฉบับกรอกจริง

5.3 ตัวอย่างสัญญาประมวลผลข้อมูล (Data Processing Agreement, DPA Template)

สำหรับใช้กับบุคคลภายนอกที่ประมวลผลข้อมูล

5.4 Checklist แนวปฏิบัติการแชร์ข้อมูล & การเข้ารหัส (Data Sharing & Encryption Best Practices Checklist)

ตารางให้พนักงานติดตามแนวปฏิบัติ

5.5 แบบฟอร์มบันทึกเหตุละเมิดข้อมูล (Incident Report Form)

สำหรับบันทึกข้อมูลเหตุการณ์ละเมิด

5.6 Checklist การตั้งค่ารหัสผ่าน & การเปิดใช้งาน 2FA (Password & 2FA Configuration Checklist)

แนวทางที่ละขั้นตอนให้ปฏิบัติ

6. หลักฐานการอบรม

- รายชื่อผู้เข้าอบรมพร้อมลายเซ็นรับรอง
- ภาพถ่ายบรรยากาศการอบรม
- แบบ Pre-Test & Post-Test พร้อมสรุปคะแนน
- ผลการประเมินความพึงพอใจ (Training Evaluation Form)
- รายงานสรุปการอบรม (Training Summary Report)

7. มติการประชุมและการอนุมัติ

7.1 อนุมัติหลักสูตรอบรม PDPA Awareness & Compliance Workshop ตามโครงสร้างและเนื้อหาในเอกสารนี้ โดยเสียงเอกฉันท์

7.2 กำหนดให้จัดอบรมพนักงานทุกคนครั้งแรก ภายในวันที่ 22 กรกฎาคม 2568

ฝ่ายทรัพยากรบุคคล (HR) ร่วมกับ ฝ่ายฝึกอบรมและพัฒนา (L&D) และ DPO รับผิดชอบ:

- สร้างตารางอบรมและแจ้งพนักงานทุกแผนก
- จัดเตรียมเอกสารประกอบการอบรมและสื่อการสอน
- ดำเนิน Pre-/Post-Test และจัดเก็บผลคะแนน

7.3 ฝ่ายตรวจสอบภายใน (Internal Audit) รับผิดชอบติดตามผลการอบรม:

- ตรวจสอบรายชื่อผู้เข้าอบรมและผลการทดสอบ
- สรุปประสิทธิภาพการอบรมเป็นรายไตรมาส

7.4 กำหนดให้มีการทบทวนหลักสูตร ทุกปี หรือตามการเปลี่ยนแปลงของกฎหมายและนโยบายองค์กร

ผู้บันทึกการประชุม:

นางสาว H (ผู้อำนวยการฝ่ายฝึกอบรมและพัฒนา, L&D Director)

ผู้ตรวจสอบและอนุมัติรายงาน:

นาย A (ประธานเจ้าหน้าที่บริหาร, CEO)

ลงวันที่: 22 มิถุนายน 2568

เอกสารอ้างอิง:

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1)
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (7)
- บทลงโทษปรับทางปกครองสูงสุด 3 ล้านบาท (กรณีไม่จัดอบรมหรือไม่ปฏิบัติตามมาตรา 37)

หมายเหตุ:

- หลังประชุม ฝ่ายทรัพยากรบุคคล (HR) จะจัดส่งอีเมลแจ้งพนักงานทุกแผนก พร้อมแนบโครงสร้างหลักสูตรและลิงก์ลงทะเบียนอบรม
- ฝ่ายฝึกอบรมและพัฒนา (L&D) จะออกเอกสารความคืบหน้า (Progress Report) ทุกเดือนจนกว่าการอบรมจะเสร็จสิ้น

จบรายงาน

3.1.3 มีการทบทวนหลักสูตรการอบรมเพื่อสร้างความตระหนักในการปฏิบัติงานให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครอง ข้อมูลส่วนบุคคล และแนวทางการฝึกอบรมเพื่อให้มีความเหมาะสม ถูกต้อง และเป็นปัจจุบัน

รายงานการประชุมทบทวนหลักสูตรการอบรมสร้างความตระหนักด้าน PDPA

รายงานการประชุมทบทวนหลักสูตรอบรม PDPA

วันที่ประชุม: 15 พฤษภาคม 2568

สถานที่: ห้องประชุมใหญ่ ชั้น 4 อาคารสำนักงานใหญ่

ผู้เข้าร่วม:

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- ผู้จัดการฝ่ายบุคคล
- ผู้จัดการฝ่ายไอที
- ผู้แทนฝ่ายกฎหมาย
- ตัวแทนพนักงานทุกแผนก

วาระที่ 1: การทบทวนหลักสูตรอบรมสร้างความตระหนักด้าน PDPA

- ได้รับรายงานผลการใช้งานหลักสูตรอบรมเดิมที่จัดขึ้นเมื่อปี 2566
- วิเคราะห์เนื้อหาและหัวข้ออบรม ว่าครอบคลุมเนื้อหาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการฯ ล่าสุดหรือไม่
- ตรวจสอบความสอดคล้องกับมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล และแนวปฏิบัติที่เปลี่ยนแปลงตามสถานการณ์ภัยคุกคามข้อมูลใหม่ ๆ

- ประเมินความเหมาะสมของวิธีการอบรมและรูปแบบการสื่อสาร เพื่อให้สอดคล้องกับความเข้าใจของพนักงานทุกระดับ

วาระที่ 2: ข้อเสนอปรับปรุงหลักสูตร

- เพิ่มเนื้อหาเกี่ยวกับภัยคุกคามข้อมูลประเภทใหม่ เช่น การฟิชซิง (Phishing), การโจมตีผ่านมัลแวร์, และการรั่วไหลของข้อมูลในระบบคลาวด์
- เสริมบทเรียนเชิงปฏิบัติ (Case Studies) ที่เกี่ยวข้องกับเหตุการณ์จริงในวงการธุรกิจและข้อมูลส่วนบุคคล
- ปรับรูปแบบการสื่อสารให้เป็น Interactive มากขึ้น เช่น ใช้แบบทดสอบออนไลน์ (Quiz) และ Workshop ฝึกปฏิบัติจริง
- กำหนดระยะเวลาการทบทวนหลักสูตรใหม่ทุก ๆ 12 เดือน หรือเมื่อมีกฎหมายลำดับรองที่เกี่ยวข้อง และ/หรือมีภัยคุกคามข้อมูลส่วนบุคคลที่เกิดขึ้นใหม่

วาระที่ 3: กำหนดกรอบเวลาและผู้รับผิดชอบ

- กำหนดให้ฝ่ายบุคคลและฝ่ายไอทีร่วมกันจัดทำและปรับปรุงหลักสูตร
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เป็นผู้ประสานงานหลัก และรับผิดชอบตรวจสอบความสอดคล้องของเนื้อหา
- กำหนดจัดอบรมพนักงานทุกปี ปีละอย่างน้อย 1 ครั้ง และเมื่อมีความเปลี่ยนแปลงสำคัญต้องจัดอบรมซ้ำ

ลงชื่ออนุมัติ

(ลงชื่อ).....

[ชื่อ-นามสกุล] เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

(ลงชื่อ).....

[ชื่อ-นามสกุล] ผู้จัดการฝ่ายบุคคล

หัวข้อหลักสูตร	หลักสูตรเก่า (ปี 2566)	หลักสูตรปรับปรุง (ปี 2568)
กฎหมาย PDPA	อธิบายภาพรวม PDPA และบทบาทขององค์กร	อธิบายภาพรวมพร้อมกรณีศึกษาล่าสุด และบทบาทเฉพาะฝ่ายต่าง ๆ
การบริหารจัดการข้อมูล	การเก็บรวบรวม ใช้งาน และเปิดเผยข้อมูลส่วนบุคคล	เพิ่มหัวข้อการประเมินความเสี่ยง และมาตรการป้องกันข้อมูลรั่วไหล
การรักษาความมั่นคงข้อมูล	มาตรการรักษาความปลอดภัยข้อมูลเบื้องต้น	เสริมเทคนิคการรักษาความปลอดภัยขั้นสูง รวมถึงภัยคุกคามไซเบอร์ใหม่ ๆ

การตอบสนองเหตุ ละเมิด	แนวทางการแจ้งเตือนและแก้ไข เหตุการณ์ละเมิดข้อมูล	เพิ่มขั้นตอนการรับมือและฟื้นฟู รวมถึงการ สื่อสารกับลูกค้าและหน่วยงานที่เกี่ยวข้อง
วิธีการอบรม	บรรยายและนำเสนอ PowerPoint	เพิ่ม Workshop, แบบทดสอบออนไลน์, และ วิดีโอจำลองเหตุการณ์จริง
ความถี่ในการ อบรม	ทุก 2 ปี	ทุกปีและเมื่อมีกฎหมาย/ภัยคุกคามใหม่ ๆ

หลักสูตรอบรมสร้างความตระหนักรู้ด้าน PDPA (ปี 2568)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นกฎหมายสำคัญที่มีผลบังคับใช้เพื่อคุ้มครองสิทธิส่วนบุคคลของประชาชนในยุคดิจิทัล ที่ข้อมูลส่วนบุคคลถูกเก็บรวบรวม และใช้ประโยชน์ในหลายมิติของชีวิตประจำวัน การปฏิบัติตามกฎหมาย PDPA อย่างถูกต้องไม่เพียงแต่ช่วยรักษาความเชื่อมั่นของเจ้าของข้อมูล แต่ยังช่วยให้องค์กรสามารถดำเนินงานอย่างมีประสิทธิภาพและปลอดภัยจากความเสี่ยงทางกฎหมายและชื่อเสียง

หลักสูตรนี้จึงถูกออกแบบขึ้นเพื่อให้พนักงานทุกระดับในองค์กรได้เข้าใจบทบาทหน้าที่ของตนในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงเรียนรู้มาตรการรักษาความมั่นคงปลอดภัยที่จำเป็น เพื่อให้เกิดความตระหนักรู้และความรับผิดชอบอย่างแท้จริงในการทำงานตามข้อกำหนดของ PDPA

วิทยากร:

รองศาสตราจารย์ตรีเนตร สาระพงษ์

ผู้เชี่ยวชาญด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล และการบริหารความมั่นคงปลอดภัยข้อมูล

สถานที่จัดอบรม:

ห้องประชุมใหญ่ อาคาร 5 ชั้น 3 สำนักงานใหญ่ บริษัท XYZ จำกัด

(หรือระบุสถานที่อื่นตามที่เหมาะสม)

วัตถุประสงค์ของหลักสูตร

- เพื่อให้ผู้เข้ารับการอบรมเข้าใจแนวทางและข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

- เพื่อสร้างความตระหนักรู้และเสริมสร้างทักษะการปฏิบัติงานให้สอดคล้องกับกฎหมายและมาตรฐานความมั่นคงปลอดภัยข้อมูล
- เพื่อให้ผู้เข้ารับการอบรมสามารถปฏิบัติตามบทบาทหน้าที่ความรับผิดชอบในการดูแลและรักษาข้อมูลส่วนบุคคลอย่างถูกต้อง
- เพื่อเตรียมพร้อมรับมือและแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ

ระยะเวลาอบรม:

4 ชั่วโมง (แบ่งเป็น 2 ช่วง)

กลุ่มเป้าหมาย: พนักงานทุกระดับ ตั้งแต่ระดับปฏิบัติการจนถึงผู้บริหาร

วิธีการอบรม:

- บรรยายประกอบสไลด์
- กรณีศึกษาจากสถานการณ์จริง (Case Studies)
- Workshop / กิจกรรมกลุ่ม
- แบบทดสอบออนไลน์ (Quiz)
- ถาม-ตอบ

เนื้อหาหลักสูตร (แบ่งเป็น 2 ช่วง)

ช่วงที่ 1: ความรู้พื้นฐานและกรอบกฎหมาย PDPA (2 ชั่วโมง)

บทนำและความสำคัญของ PDPA

- ความหมายของข้อมูลส่วนบุคคล
- วัตถุประสงค์ของกฎหมาย PDPA
- ผลกระทบหากไม่ปฏิบัติตามกฎหมาย

กรอบกฎหมายและข้อกำหนดสำคัญ

- การใช้และการเปิดเผยข้อมูล
- การรักษาความปลอดภัยข้อมูล
- การแจ้งเหตุละเมิดข้อมูล

การบริหารจัดการข้อมูลส่วนบุคคลภายในองค์กร

- นโยบายและแนวปฏิบัติขององค์กร
- การกำหนดผู้รับผิดชอบข้อมูล (Data Protection Officer - DPO)
- ช่องทางและวิธีการร้องเรียนหรือแจ้งปัญหา

บทลงโทษและผลทางกฎหมาย

กรณีตัวอย่างบทลงโทษในองค์กรที่ละเมิด PDPA

ช่วงที่ 2: การปฏิบัติและการรักษาความมั่นคงปลอดภัยข้อมูล (2 ชั่วโมง)

มาตรการรักษาความมั่นคงปลอดภัยข้อมูล

- การรักษาความปลอดภัยทางกายภาพ (Physical Security)
- การรักษาความปลอดภัยทางเทคนิค (Technical Security) เช่น การใช้รหัสผ่าน การเข้ารหัสข้อมูล
- การรักษาความมั่นคงของระบบเครือข่าย

ภัยคุกคามและแนวทางป้องกัน

- ภัยคุกคามที่พบบ่อย เช่น ฟิชชิง (Phishing), มัลแวร์ (Malware), การโจมตีแบบแรนซัมแวร์ (Ransomware)
- วิธีสังเกตและป้องกันภัยคุกคาม
- กรณีศึกษาการละเมิดข้อมูลที่เกิดขึ้นจริงและบทเรียนที่ได้

การตอบสนองต่อเหตุการณ์ละเมิดข้อมูล (Data Breach Response)

- ขั้นตอนการแจ้งเตือนและรายงานเหตุการณ์
- การสอบสวนและวิเคราะห์เหตุการณ์
- วิธีการแก้ไขและฟื้นฟูข้อมูล
- การสื่อสารกับเจ้าของข้อมูลและหน่วยงานที่เกี่ยวข้อง

Workshop / กิจกรรมกลุ่ม

- วิเคราะห์กรณีศึกษาจากเหตุการณ์จริง
- การฝึกตอบคำถามและรับมือกับสถานการณ์ละเมิดข้อมูล
- การสร้างแนวทางปฏิบัติส่วนบุคคลในการรักษาความปลอดภัยข้อมูลในงานประจำวัน

แบบทดสอบออนไลน์ (Quiz)

- ประเมินความเข้าใจของผู้เข้าร่วมอบรม
- เน้นคำถามเรื่องบทบาทหน้าที่และมาตรการรักษาความมั่นคงปลอดภัย

ผลลัพธ์ที่คาดหวังหลังการอบรม

- พนักงานมีความเข้าใจลึกซึ้งในกฎหมาย PDPA และข้อกำหนดทางกฎหมาย
- สามารถระบุบทบาทหน้าที่และความรับผิดชอบของตนเองในการคุ้มครองข้อมูลส่วนบุคคล
- เข้าใจและนำมาตราการรักษาความมั่นคงปลอดภัยข้อมูลไปปฏิบัติอย่างถูกต้อง
- พร้อมรับมือและแก้ไขเหตุการณ์ละเมิดข้อมูลอย่างมีประสิทธิภาพ
- สร้างวัฒนธรรมการคุ้มครองข้อมูลส่วนบุคคลในองค์กรอย่างยั่งยืน

เวลา	รายละเอียดกิจกรรม	วิธีการ

08:30-09:00	ลงทะเบียนและรับเอกสารประกอบการอบรม	ลงทะเบียน
09:00-09:15	กล่าวเปิดการอบรม และแนะนำวิทยากร	บรรยาย
09:15-10:45	ช่วงที่ 1: ความรู้พื้นฐานและกรอบกฎหมาย PDPA	บรรยาย + กรณีศึกษา
10:45-11:00	พักเบรก	พัก
11:00-12:30	ช่วงที่ 2: การปฏิบัติและการรักษาความมั่นคงปลอดภัยข้อมูล	บรรยาย + Workshop
12:30-13:00	แบบทดสอบและถาม-ตอบ	แบบทดสอบ + ถาม-ตอบ
13:00	ปิดการอบรมและมอบเกียรติบัตร	มอบเกียรติบัตร

3.1.4 องค์การมีการพิจารณาความต้องการด้านการฝึกอบรมจากพนักงาน และใช้ข้อมูลนี้เพื่อจัดหลักสูตรการอบรม เพื่อสร้างความตระหนักในเรื่องการปฏิบัติงานให้สอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย

สิ่งที่ต้องทำ: มีการพิจารณา โดย ทำแบบสอบถาม ความต้องการฝึกอบรมในการปฏิบัติงานจากพนักงาน ตาม Job Description ของแต่ละตำแหน่ง

หลักฐาน: 1) แบบสอบถามพนักงานในด้านความต้องการของการอบรม ไม่ใช่ข้อบังคับตามกฎหมาย

สภาพบังคับ: ไม่มีกฎหมายกำหนด

แบบสอบถามความต้องการฝึกอบรม

เรื่อง: ความต้องการในการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

วัตถุประสงค์: เพื่อสำรวจความต้องการของพนักงานในการฝึกอบรมเกี่ยวกับแนวปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามบริบทของการทำงาน

คำชี้แจง: กรุณาทำเครื่องหมาย ✓ ในช่องที่ตรงกับความคิดเห็นของท่านมากที่สุด และกรอกข้อความเพิ่มเติมในช่องว่างเมื่อจำเป็น

ส่วนที่ 1: ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

1. ตำแหน่งงานของท่าน: _____

2. หน่วยงาน/แผนก: _____

3. ลักษณะงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (เลือกได้มากกว่า 1 ข้อ)

- ☐ การเก็บรวบรวมข้อมูล
- ☐ การใช้หรือประมวลผลข้อมูล
- ☐ การจัดเก็บ/เข้าถึงข้อมูล
- ☐ การเปิดเผยหรือถ่ายโอนข้อมูล
- ☐ อื่น ๆ (โปรดระบุ): _____

ส่วนที่ 2: ความต้องการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล

หัวข้อการฝึกอบรมที่ต้องการ	ต้องการมาก	ต้องการ	ไม่แน่ใจ	ไม่ต้องการ
ความรู้พื้นฐานเกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	☐	☐	☐	☐
บทบาทและหน้าที่ของเจ้าหน้าที่ตามตำแหน่งงานของท่าน (ตาม Job Description)	☐	☐	☐	☐
การขอความยินยอมจากเจ้าของข้อมูล	☐	☐	☐	☐
การจัดเก็บและรักษาความมั่นคงปลอดภัยของข้อมูล	☐	☐	☐	☐
การรายงานเหตุละเมิดข้อมูล (Data Breach Notification)	☐	☐	☐	☐
แนวทางปฏิบัติเมื่อต้องถ่ายโอนข้อมูลไปยังบุคคลภายนอก/ต่างประเทศ	☐	☐	☐	☐
กรณีศึกษา/สถานการณ์จำลองที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล	☐	☐	☐	☐
การประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล	☐	☐	☐	☐
การจัดทำบันทึกการกิจกรรมการประมวลผลข้อมูล (Record of Processing Activities)	☐	☐	☐	☐
การใช้เทคโนโลยีเพื่อสนับสนุนการคุ้มครองข้อมูล	☐	☐	☐	☐
การรับเรื่องร้องเรียนจากเจ้าของข้อมูล	☐	☐	☐	☐

บทบาทของ DPO (Data Protection Officer) ในองค์กร	☐	☐	☐	☐
แนวทางการฝึกอบรมภายใน (In-house PDPA awareness)	☐	☐	☐	☐
การจัดการข้อมูลส่วนบุคคลของนักเรียน/นักศึกษาและผู้ปกครอง	☐	☐	☐	☐
ข้อควรระวังในการใช้ระบบ Cloud และแอปพลิเคชันภายนอกในงานการศึกษา	☐	☐	☐	☐

ส่วนที่ 3: ความเห็นเพิ่มเติม

ท่านต้องการให้การฝึกอบรมในรูปแบบใด (เลือกได้มากกว่า 1 ข้อ)

- ☐ อบรมในห้องเรียน
- ☐ อบรมออนไลน์ (E-learning)
- ☐ Workshop แบบมีกรณีศึกษา
- ☐ อื่น ๆ (โปรดระบุ): _____

หัวข้ออื่น ๆ ที่ท่านอยากให้มีการอบรมเพิ่มเติม:

ขอขอบคุณสำหรับความร่วมมือ

(เอกสารฉบับนี้ใช้เพื่อวัตถุประสงค์ในการพัฒนาหลักสูตรการฝึกอบรมเท่านั้น)

3.1.5 องค์กรจัดให้มีการฝึกอบรมด้านการจัดการข้อมูลและการคุ้มครองข้อมูลส่วนบุคคลทั่วทั้งองค์กร โดยพิจารณาจากความต้องการของพนักงานอย่างเหมาะสม และมีแผนหรือกลยุทธ์การฝึกอบรมภายในระยะเวลาที่กำหนด

สิ่งที่ต้องทำ: มีการจัดอบรมแก่พนักงานโดยคำนึงถึงความต้องการของพนักงานในการปฏิบัติงาน และ มีการสอบประเมินผลหลังจากการอบรม โดยกำหนดคะแนนขั้นต่ำ

หลักฐาน: 1) แบบประเมินจากพนักงานต่อการอบรม
2) แบบทดสอบประเมินผลหลังจากการอบรมว่าผลการประเมินผ่านเกณฑ์หรือไม่

สภาพบังคับ: ไม่มีกฎหมายกำหนด

แบบประเมินจากพนักงานต่อการอบรม

คำชี้แจง:

กรุณาทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับความคิดเห็นของท่านมากที่สุด และกรอกความคิดเห็นเพิ่มเติมตามความเหมาะสม

หัวข้อการประเมิน	มากที่สุด	มาก	ปานกลาง	น้อย
1. เนื้อหาการอบรมตรงกับลักษณะงานของท่าน	☐	☐	☐	☐
2. วิทยากรถ่ายทอดความรู้ได้ชัดเจน	☐	☐	☐	☐
3. สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานได้	☐	☐	☐	☐
4. สื่อประกอบการอบรมมีประโยชน์	☐	☐	☐	☐
5. ระยะเวลาในการอบรมเหมาะสม	☐	☐	☐	☐
6. สถานที่ / ระบบการอบรมเหมาะสม	☐	☐	☐	☐
7. ภาพรวมของการอบรมครั้งนี้เป็นที่น่าพึงพอใจ	☐	☐	☐	☐

ความคิดเห็นเพิ่มเติม:

.....

แบบทดสอบประเมินผลความรู้เกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

คำชี้แจง: กรุณาเลือกคำตอบที่ถูกต้องที่สุดเพียงข้อเดียวในแต่ละข้อ

1. ข้อใดคือวัตถุประสงค์หลักของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- ก. เพื่อส่งเสริมการค้าออนไลน์
- ข. เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล
- ค. เพื่อให้หน่วยงานรัฐสามารถเข้าถึงข้อมูลได้สะดวก
- ง. เพื่อจัดเก็บภาษีจากข้อมูลส่วนบุคคล

เฉลย: ข. เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล

อธิบาย: จุดมุ่งหมายของกฎหมายนี้คือการกำหนดสิทธิของเจ้าของข้อมูล และหน้าที่ของผู้ควบคุมข้อมูลในการจัดการข้อมูลส่วนบุคคลอย่างปลอดภัยและโปร่งใส

2. ข้อใดต่อไปนี้ไม่ถือเป็นข้อมูลส่วนบุคคล

- ก. ชื่อ-นามสกุล
- ข. คะแนนสอบเฉพาะตัวบุคคล
- ค. รหัสนักศึกษา
- ง. ผลรวมคะแนนสอบของชั้นเรียนโดยไม่ระบุชื่อบุคคล

เฉลย: ง. ผลรวมคะแนนสอบของชั้นเรียนโดยไม่ระบุชื่อบุคคล

อธิบาย: ข้อมูลส่วนบุคคลต้องสามารถระบุถึงตัวบุคคลได้โดยตรงหรือโดยอ้อม หากไม่มีตัวระบุ เช่น ชื่อหรือรหัส ก็ไม่ถือว่าเป็นข้อมูลส่วนบุคคล

3. ข้อมูลใดต่อไปนี้ เป็นข้อมูลอ่อนไหว (Sensitive Data) ตามกฎหมาย

- ก. เบอร์โทรศัพท์
- ข. ศาสนา
- ค. อีเมลส่วนตัว
- ง. ที่อยู่ปัจจุบัน

เฉลย: ข. ศาสนา

อธิบาย: ข้อมูลที่เกี่ยวข้องกับเชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ ฯลฯ จัดเป็น "ข้อมูลอ่อนไหว" ซึ่งต้องได้รับความยินยอมเป็นพิเศษในการเก็บ ใช้ หรือเปิดเผย

4. หน่วยงานใดมีหน้าที่กำกับดูแลการบังคับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- ก. คณะกรรมการสิทธิมนุษยชน
- ข. คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.)
- ค. กระทรวงการคลัง
- ง. สำนักงานตำรวจแห่งชาติ

เฉลย: ข. คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (กคส.)

อธิบาย: เป็นหน่วยงานตามกฎหมายที่มีหน้าที่ออกแนวทางและกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล

5. การเก็บข้อมูลส่วนบุคคลสามารถทำได้โดยไม่ต้องขอความยินยอมในกรณีใด

ก. ใช้เพื่อการโฆษณา

ข. ใช้เพื่อวิเคราะห์พฤติกรรมลูกค้า

ค. ใช้เพื่อปฏิบัติตามกฎหมาย

ง. ใช้เพื่อทำวิจัยด้านการตลาด

เฉลย: ค. ใช้เพื่อปฏิบัติตามกฎหมาย

อธิบาย: กฎหมายยกเว้นการขอความยินยอมในบางกรณี เช่น การปฏิบัติตามหน้าที่ตามกฎหมาย หรือเพื่อประโยชน์สาธารณะ

6. หากเกิดเหตุข้อมูลรั่วไหล ผู้ควบคุมข้อมูลต้องแจ้งสำนักงานภายในกี่ชั่วโมง

ก. 24 ชั่วโมง

ข. 48 ชั่วโมง

ค. 72 ชั่วโมง

ง. 96 ชั่วโมง

เฉลย: ค. 72 ชั่วโมง

อธิบาย: ตามมาตรา 37/4 แห่ง พ.ร.บ. PDPA กำหนดให้แจ้งสำนักงานภายใน 72 ชั่วโมงนับแต่ทราบเหตุ

7. เจ้าของข้อมูลมีสิทธิใดต่อไปนี้ตามกฎหมาย

ก. สิทธิในการเรียกเก็บค่าธรรมเนียมจากผู้ควบคุมข้อมูล

ข. สิทธิในการเปิดเผยข้อมูลให้บุคคลภายนอก

ค. สิทธิในการถอนความยินยอม

ง. สิทธิในการควบคุมการตลาดโดยตรง

เฉลย: ค. สิทธิในการถอนความยินยอม

อธิบาย: เจ้าของข้อมูลมีสิทธิต่าง ๆ เช่น การเข้าถึง ลบ แก้ไข และถอนความยินยอมในการเก็บ/ใช้ข้อมูลส่วนบุคคล

8. การเก็บข้อมูลส่วนบุคคลของนักเรียนต้องคำนึงถึงข้อใดเป็นหลัก

ก. ความสะดวกของครูผู้สอน

ข. การจัดกิจกรรมการตลาด

ค. ความยินยอมจากนักเรียนหรือผู้ปกครอง

ง. จำนวนนักเรียนในห้องเรียน

เฉลย: ค. ความยินยอมจากนักเรียนหรือผู้ปกครอง

อธิบาย: นักเรียนเป็น "เจ้าของข้อมูล" หรือผู้เยาว์ ซึ่งต้องมีความยินยอมจากผู้ปกครองหากอายุต่ำกว่า 20 ปี

9. ผู้ควบคุมข้อมูลควรมีมาตรการใดเพื่อป้องกันการละเมิดข้อมูล

ก. ใช้รหัสผ่านที่ง่ายต่อการจำ

ข. เปิดเผยข้อมูลผ่านช่องทางออนไลน์

ค. ให้สิทธิ์เข้าถึงกับทุกคนในองค์กร

ง. เข้ารหัส (encryption) และจำกัดสิทธิ์การเข้าถึงข้อมูล

เฉลย: ง. เข้ารหัส (encryption) และจำกัดสิทธิ์การเข้าถึงข้อมูล

อธิบาย: การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นข้อกำหนดทางกฎหมาย เพื่อป้องกันการเข้าถึงโดยมิชอบ

10. หากหน่วยงานฝ่าฝืน PDPA อาจได้รับโทษอย่างไร

ก. แค่อักเตือนด้วยวาจา

ข. ถูกเพิกถอนสถานะหน่วยงานราชการ

ค. ถูกปรับทางปกครองและทางอาญา

ง. ไม่มีโทษใด

เฉลย: ค. ถูกปรับทางปกครองและทางอาญา

อธิบาย: กฎหมายกำหนดโทษทั้งในรูปแบบ "ทางแพ่ง" "ทางปกครอง" และ "ทางอาญา" เช่น ปรับเป็นเงิน สูงสุดหลายล้านบาท และจำคุกในบางกรณี

3.1.6 องค์กรจัดให้มีทรัพยากรที่จำเป็นสำหรับการดำเนินการฝึกอบรมให้แก่พนักงานทั้งหมด

สิ่งที่ต้องทำ: มีเอกสารที่ใช้ในการอบรมซึ่งสามารถเข้าถึงได้โดยง่าย โดยจัดทำในรูปแบบต่าง ๆ เช่น

อิเล็กทรอนิกส์ หรือส่งผ่านทางอีเมล เป็นต้น

หลักฐาน: 1) เอกสารที่ใช้ในการอบรม อาจจัดทำในรูปแบบอิเล็กทรอนิกส์

สภาพบังคับ: ไม่มีกฎหมายกำหนด

เรื่อง: องค์กรจัดให้มีทรัพยากรที่จำเป็นสำหรับการดำเนินการฝึกอบรมให้แก่พนักงานทั้งหมด

รายละเอียดของสิ่งที่ดำเนินการ

องค์กรได้จัดเตรียม เอกสารประกอบการอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ไว้อย่างเป็นระบบ เพื่อให้พนักงานสามารถเข้าถึงและศึกษาเพิ่มเติมได้ทุกเวลา โดยมีรูปแบบเอกสารดังนี้:

1. เอกสารอบรมในรูปแบบไฟล์ PDF / PowerPoint

หัวข้อ: ความรู้เบื้องต้นเกี่ยวกับ PDPA

เนื้อหา:

- ความหมายและความสำคัญของข้อมูลส่วนบุคคล
- หน้าที่ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล
- สิทธิของเจ้าของข้อมูล
- กรณศึกษาการละเมิดข้อมูลและบทเรียนสำหรับองค์กร

ลิงก์เข้าถึง:

- ไฟล์ถูกอัปโหลดในระบบคลังความรู้ภายใน (Intranet)
- ตัวอย่างลิงก์: \\fileserver\HR\Training\PDPA_Training2025.pdf

2. เอกสารประกอบบทเรียนรูปแบบ Infographic

หัวข้อ:

- สิทธิของเจ้าของข้อมูล 8 ประการ
- ข้อมูลอ่อนไหวคืออะไร?
- ขั้นตอนแจ้งเหตุละเมิดข้อมูลภายใน 72 ชั่วโมง

ลักษณะการเข้าถึง:

- ส่งให้พนักงานทุกคนผ่านอีเมลในหัวข้อ "เอกสารความรู้ PDPA ฉบับย่อ"
- แนบในเว็บไซต์หรือระบบ LMS ขององค์กร

3. เอกสารรูปแบบวิดีโอความรู้เบื้องต้น

เนื้อหา: วิดีโอ 5 นาทีสรุปสาระสำคัญของ PDPA

ช่องทาง:

- เผยแพร่ผ่านระบบอบรมออนไลน์ภายในองค์กร (LMS)
- แนบลิงก์ในอีเมลประจำเดือนเรื่อง “PDPA Awareness Update”
- QR Code ติดประกาศที่บอร์ด HR สำหรับสแกนดูได้ง่าย

4. แบบฝึกหัด/แบบทดสอบฝึกคิด (PDPA Quiz)

- แบบทดสอบตัวอย่าง 10 ข้อ พร้อมเฉลยและอธิบาย
- จัดทำในรูปแบบ Google Forms และ PDF ดาวน์โหลดได้
- ใช้เพื่อกระตุ้นความเข้าใจและทบทวนเนื้อหาหลังอบรม

สรุป

องค์กรได้ดำเนินการตามข้อกำหนดของมาตรฐานการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล โดยจัดทำ สื่อและเอกสารประกอบที่หลากหลายและเข้าถึงได้ง่าย ทั้งในรูปแบบไฟล์เอกสาร วิดีโอ และ Infographic เพื่อให้พนักงานสามารถศึกษาด้วยตนเอง และใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

3.1.7 ผู้บริหารระดับสูงมีการลงนามรับรองหลักสูตรการฝึกอบรมเพื่อสร้างความตระหนักในการคุ้มครองข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: มีการประชุมของผู้บริหารระดับสูงเพื่อให้ความเห็นชอบต่อเนื้อหาของการฝึกอบรมที่ได้รับ การทบทวน

หลักฐาน: 1) รายงานการประชุมของผู้บริหารระดับสูงเพื่อทบทวนโปรแกรมการฝึกอบรม

สภาพบังคับ: ไม่มีกฎหมายกำหนด

รายงานการประชุมคณะผู้บริหารระดับสูง

เรื่อง: การพิจารณาและให้ความเห็นชอบต่อหลักสูตรการฝึกอบรมเพื่อสร้างความตระหนักในการคุ้มครองข้อมูลส่วนบุคคล

ครั้งที่: 3/2568

วัน/เวลา: วันพฤหัสบดีที่ 20 มีนาคม พ.ศ. 2568 เวลา 09.30–11.00 น.

สถานที่: ห้องประชุมใหญ่ อาคารสำนักงานกลาง ชั้น 5

ผู้เข้าร่วมประชุม:

1. นายอนุชา วัฒนกิจ กรรมการผู้จัดการใหญ่ (ประธานการประชุม)
2. นางสาวสุพัตรา อินทรโชติ รองกรรมการผู้จัดการฝ่ายบริหาร
3. นายพิชญ์พงศ์ รุ่งเรืองผล ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ
4. นางสาวอุษณีย์ นาคพยัคฆ์ ผู้อำนวยการฝ่ายทรัพยากรบุคคล
5. นางอรอนงค์ สุทธิวรชัย ผู้จัดการฝ่ายกฎหมาย
6. นายสิริพงศ์ จิรเวช เลขานุการการประชุม

ระเบียบวาระการประชุม

วาระที่ 1: เรื่องแจ้งเพื่อทราบ

ไม่มี

วาระที่ 2: เรื่องเพื่อพิจารณา

2.1 พิจารณาหลักสูตรอบรม “การสร้างความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล” สำหรับพนักงานองค์กร

เลขานุการการประชุมได้เสนอร่างโครงสร้างหลักสูตรการฝึกอบรมเพื่อสร้างความตระหนักเกี่ยวกับกฎหมายและแนวปฏิบัติที่เกี่ยวข้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งจัดทำโดยฝ่ายทรัพยากรบุคคลร่วมกับฝ่ายกฎหมายและฝ่ายไอที โดยมีสาระสำคัญ ได้แก่:

- แนวคิดและหลักการพื้นฐานของ PDPA
- สิทธิของเจ้าของข้อมูลส่วนบุคคล
- บทบาทหน้าที่ของพนักงานและองค์กร
- กรณีศึกษาและบทลงโทษจากการละเมิด

- แบบทดสอบหลังอบรมเพื่อประเมินผลการเรียนรู้
- ผู้บริหารได้ร่วมกันอภิปรายและเสนอแนะแนวทางการปรับปรุงเพิ่มเติม อาทิ
- เพิ่มกรณีศึกษาในบริบทของแผนกต่าง ๆ
- จัดทำ Infographic และสื่อสรุปย่อแนบในระบบภายใน

ที่ประชุม มีมติเห็นชอบในหลักสูตรการอบรมดังกล่าว และให้ลงนามรับรองโดยกรรมการผู้จัดการใหญ่ พร้อมมอบหมายให้ฝ่ายทรัพยากรบุคคลนำไปดำเนินการอบรมแก่พนักงานทุกระดับภายในไตรมาส 2 ปี 2568

วาระที่ 3 เรื่องอื่น ๆ (ถ้ามี)

ไม่มี

มติที่ประชุม

ที่ประชุมมีมติ เป็นเอกฉันท์ ให้ความเห็นชอบต่อหลักสูตรอบรม “การสร้างความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล” และมอบหมายให้ฝ่ายทรัพยากรบุคคลเป็นผู้ประสานดำเนินการอบรมภายในกำหนด

ลงชื่อ.....

(นายอนุชา วัฒนกิจ)

ประธานการประชุม

กรรมการผู้จัดการใหญ่

ลงวันที่: 20 มีนาคม 2568

3.2.1 พนักงานได้รับการฝึกอบรมที่เป็นการทบทวนและฟื้นฟูความรู้พื้นฐาน

โดยไม่คำนึงถึงระยะเวลาที่พนักงานนั้นได้ปฏิบัติงานกับองค์กร สถานะของการจ้างงาน หรือระดับของพนักงาน

สิ่งที่ต้องทำ: มีการอบรมและแบบทดสอบเพื่อประเมินผลพนักงานในการทบทวนและฟื้นฟูความรู้พื้นฐาน โดยไม่คำนึงถึงระยะเวลาที่พนักงานปฏิบัติงานกับองค์กร สถานะของการจ้าง หรือระดับของพนักงาน

หลักฐาน: 1) เอกสารเกี่ยวกับการจัดอบรมเพื่อทบทวนและฟื้นฟูความรู้พื้นฐาน
2) แบบทดสอบเพื่อทบทวนและฟื้นฟูความรู้

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล

บุคคล พ.ศ. 2565 ข้อ 4 (7) และข้อ 5 โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 มีโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

เอกสารเกี่ยวกับการจัดอบรมเพื่อทบทวนและฟื้นฟูความรู้พื้นฐาน

ชื่อหลักสูตร: "การทบทวนและฟื้นฟูความรู้พื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคล
(PDPA Refresher Training 2568)"

วัตถุประสงค์:

- เพื่อให้พนักงานทุกระดับได้รับการทบทวนความรู้ด้าน PDPA อย่างสม่ำเสมอ
- เพื่อให้พนักงานตระหนักถึงหน้าที่ของตนเองตามบทบาทในกระบวนการจัดการข้อมูลส่วนบุคคล
- ป้องกันความเสี่ยงจากการละเมิดข้อมูลโดยมิได้เจตนา

กลุ่มเป้าหมาย:

- พนักงานทุกระดับ โดยไม่จำกัดระยะเวลาการทำงาน
- ทั้งแบบประจำ ชั่วคราว พนักงานจ้างเหมา หรือพนักงานฝึกงาน

รูปแบบการอบรม:

- อบรมออนไลน์ผ่านระบบ LMS (Learning Management System)
- ความยาว 45 นาที พร้อมแบบทดสอบท้ายบท
- ต้องทำแบบทดสอบผ่านเกณฑ์ 80% จึงถือว่า "ผ่านการอบรม"

หัวข้อเนื้อหา:

- ความรู้เบื้องต้นเกี่ยวกับ PDPA
- สิทธิของเจ้าของข้อมูล
- การจัดการข้อมูลส่วนบุคคลในงานประจำ
- การรายงานเหตุละเมิดข้อมูล
- กรณีศึกษาในองค์กร

รอบการอบรม:

- อบรม 1 ครั้งต่อปี (ตามแผนอบรมประจำปี)
- กำหนดให้พนักงานต้องอบรมภายในเดือนมิถุนายนของทุกปี

ตัวอย่าง เอกสารประกอบการบรรยายในรูปแบบสไลด์ สำหรับการอบรมเพื่อทบทวนและฟื้นฟูความรู้พื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA Refresher Training)

สไลด์ที่ 1: ชื่อเรื่อง

การอบรมทบทวนและฟื้นฟูความรู้พื้นฐาน

ด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA Refresher Training)

รอบอบรม: ปี 2568

จัดโดย: ฝ่ายทรัพยากรบุคคล ร่วมกับฝ่ายกฎหมาย

สไลด์ที่ 2: วัตถุประสงค์ของการอบรม

- ทบทวนความรู้พื้นฐานด้านกฎหมาย PDPA
- เพิ่มความเข้าใจในบทบาทของพนักงานทุกระดับ
- ป้องกันความเสี่ยงในการละเมิดข้อมูล
- เสริมสร้างวัฒนธรรมองค์กรด้านความปลอดภัยของข้อมูล

สไลด์ที่ 3: ความหมายของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Data) คือ

- ข้อมูลที่สามารถระบุถึงตัวบุคคล ไม่ว่าจะทางตรงหรือทางอ้อม เช่น:
- ชื่อ-นามสกุล
- เลขบัตรประชาชน
- เบอร์โทร อีเมล
- รูปถ่าย ใบหน้า เสี่ยง
- หมายเลขนักเรียน / พนักงาน

สไลด์ที่ 4: ข้อมูลอ่อนไหว (Sensitive Personal Data)

ข้อมูลส่วนบุคคลที่มีความอ่อนไหวตาม มาตรา 26 ได้แก่:

เชื้อชาติ/ศาสนา

- ความคิดเห็นทางการเมือง
- ข้อมูลสุขภาพ / ประวัติการแพทย์
- พฤติกรรมทางเพศ
- ข้อมูลชีวภาพ (ไบโอเมตริกซ์) เช่น ลายนิ้วมือ, ใบหน้า
- ต้องมี "ความจำเป็นและได้รับความยินยอมโดยชัดแจ้ง"

สไลด์ที่ 5: บทบาทของพนักงาน

พนักงานทุกระดับ มีหน้าที่ต้อง:

- ปฏิบัติตามมาตรการภายในองค์กร
- เก็บ ใช้ และเปิดเผยข้อมูลอย่างระมัดระวัง

- แจ้งเหตุละเมิดข้อมูลทันทีที่พบ
- หลีกเลี่ยงการส่งข้อมูลโดยไม่เข้ารหัส / ไม่มีสิทธิ์

สไลด์ที่ 6: สิทธิของเจ้าของข้อมูล

- เจ้าของข้อมูลมีสิทธิตาม มาตรา 30-36 เช่น:
- สิทธิขอเข้าถึงข้อมูล
- สิทธิให้แก้ไข ลบ หรือทำลาย
- สิทธิระงับการใช้
- สิทธิในการถอนความยินยอม
- สิทธิร้องเรียนต่อคณะกรรมการ

สไลด์ที่ 7: กรณีศึกษาจริง (องค์กรไทย)

ตัวอย่าง: พนักงานฝ่ายบริการลูกค้า แชร์ข้อมูลลูกค้าทาง LINE ส่วนตัว

ผลกระทบ: ลูกค้าร้องเรียน, องค์กรเสียชื่อเสียง, ถูกสอบจากคณะกรรมการ

บทเรียน: ห้ามใช้ช่องทางไม่เป็นทางการในการส่งข้อมูล

สไลด์ที่ 8: บทลงโทษตามกฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดโทษไว้ดังนี้:

- โทษทางแพ่ง: ชดเชยค่าเสียหาย
- โทษทางปกครอง: ปรับสูงสุด 5 ล้านบาท
- โทษทางอาญา: จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ

สไลด์ที่ 9: สิ่งที่พนักงานควรทำ / ไม่ควรทำ

ควรทำ:

- ใช้ระบบองค์กรเท่านั้นในการจัดการข้อมูล
- ตรวจสอบสิทธิ์ก่อนเปิดเผยข้อมูล
- เก็บข้อมูลอย่างปลอดภัย
- รายงานเหตุผิดปกติทันที

ไม่ควรทำ:

- ใช้ LINE / Facebook ส่วนตัวส่งข้อมูล
- พุดถึงข้อมูลลูกค้ากับบุคคลภายนอก
- เก็บเอกสารสำคัญไว้นอกระบบ

สไลด์ที่ 10: แบบทดสอบและประเมินผล

- หลังการอบรม ผู้เข้าอบรมจะต้องทำแบบทดสอบจำนวน 10 ข้อ

- เกณฑ์ผ่าน: 80% (ตอบถูกต้องอย่างน้อย 8 ข้อ)
- หากไม่ผ่าน ต้องอบรมซ้ำและทำแบบทดสอบใหม่ภายใน 7 วัน
- ผลการอบรมจะบันทึกในระบบเพื่อการติดตามประจำปี

แบบทดสอบเพื่อทบทวนและฟื้นฟูความรู้พื้นฐาน

ชื่อแบบทดสอบ: แบบทดสอบประเมินความเข้าใจหลังการอบรม PDPA (Refresher)

จำนวนข้อ: 10 ข้อ (ปรนัย 4 ตัวเลือก)

ข้อ ที่	คำถามตัวอย่าง	คำตอบที่ถูกต้อง	คำอธิบาย
1	ข้อมูลใดต่อไปนี้ไม่ถือเป็น “ข้อมูลส่วนบุคคล”?	ง) รหัสสินค้า	ไม่สามารถระบุถึงบุคคลใดได้โดยตรงหรือโดยอ้อม
2	พนักงานควรทำอะไรหากได้รับคำร้องขอลบข้อมูลจากเจ้าของข้อมูล?	ค) แจ้งหน่วยงานที่รับผิดชอบโดยทันที	ต้องไม่ดำเนินการเองโดยพลการ
3	มาตรา 37 ของ พ.ร.บ. PDPA กล่าวถึงเรื่องใด?	ข) หน้าที่ของผู้ควบคุมข้อมูล	เป็นบทบัญญัติหลักขององค์กร
4	ระยะเวลาที่องค์กรต้องแจ้งเหตุละเมิดข้อมูลคือกี่ชั่วโมง?	ก) 72 ชั่วโมง	ตามข้อ 7 ของประกาศปี 2565
5	ข้อมูลอ่อนไหว (sensitive data) เช่นอะไร?	ข) ความเชื่อทางศาสนา	ระบุไว้ชัดเจนใน มาตรา 26

(คำถามที่ 6-10 สามารถเพิ่มเติมตามหัวข้ออบรมเพื่อประเมินความเข้าใจในแต่ละบท)

เกณฑ์ผ่าน:

- ต้องได้คะแนน 8 ข้อขึ้นไป (80%)
- หากไม่ผ่าน ต้องอบรมซ้ำภายใน 7 วัน

3.2.2 พนักงานได้รับการฝึกอบรมเพื่อเป็นการเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล ภายในระยะเวลาที่เหมาะสม หรือได้รับการฝึกอบรมภายใน 1 เดือน นับตั้งแต่วันที่เริ่มต้นปฏิบัติงาน

สิ่งที่ต้องทำ: มีการอบรมและแบบทดสอบเพื่อประเมินผล เพื่อเป็นการเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล ภายในระยะเวลาที่เหมาะสม หรือได้รับการฝึกอบรมภายใน 1 เดือน นับตั้งแต่วันที่เริ่มต้นปฏิบัติงาน

หลักฐาน: 1) เอกสารเกี่ยวกับการจัดอบรมเกี่ยวกับการเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล

2) แบบทดสอบเกี่ยวกับการเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (7)

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 มีโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

เอกสารประกอบการอบรม: การเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล

หัวข้อการอบรม: การเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล

กลุ่มเป้าหมาย: พนักงานใหม่ทุกตำแหน่งที่มีหน้าที่เกี่ยวข้องกับการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ระยะเวลาอบรม: 2 ชั่วโมง

รูปแบบการอบรม: บรรยายเชิงปฏิบัติการ + กรณีศึกษา + แบบทดสอบ

ระยะเวลาดำเนินการ: ภายใน 30 วัน นับจากวันที่เริ่มปฏิบัติงาน

เนื้อหาหลักในการอบรม:

- ความรู้เบื้องต้นเกี่ยวกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ความหมายและประเภทของข้อมูลส่วนบุคคล
- สิทธิของเจ้าของข้อมูล และหน้าที่ของผู้ปฏิบัติงาน
- ขั้นตอนและข้อควรระวังก่อนการเข้าถึงข้อมูลส่วนบุคคล
- การรักษาความมั่นคงปลอดภัยของข้อมูล (Security Measures)
- กรณีศึกษาการละเมิดข้อมูลที่เกิดขึ้นในองค์กรต่าง ๆ
- แนวทางปฏิบัติเมื่อเกิดเหตุการณ์ข้อมูลรั่วไหล

หมายเหตุ:

ผู้เข้าอบรมต้องทำแบบทดสอบหลังการอบรม และต้องได้คะแนนไม่น้อยกว่า 80% จึงถือว่าผ่านเกณฑ์ การอบรมนี้เป็นเงื่อนไขก่อนการได้รับสิทธิ์เข้าถึงระบบหรือฐานข้อมูลที่มีข้อมูลส่วนบุคคล

แบบทดสอบหลังการอบรม (10 ข้อ พร้อมเฉลย)

หัวข้อ: การเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล

คำชี้แจง: โปรดเลือกคำตอบที่ถูกต้องที่สุดเพียงข้อเดียว

1. ข้อมูลส่วนบุคคลหมายถึงข้อใด

- ก. ข้อมูลที่ไม่สามารถระบุตัวตนของบุคคลได้
- ข. ข้อมูลทั่วไปที่ทุกคนสามารถเข้าถึงได้
- ค. ข้อมูลที่เกี่ยวข้องกับบุคคลธรรมดา และสามารถระบุตัวตนได้
- ง. ข้อมูลเกี่ยวกับองค์กร

เฉลย: ค

คำอธิบาย: ข้อมูลส่วนบุคคลคือข้อมูลที่สามารถระบุถึงตัวบุคคลได้โดยตรงหรือโดยอ้อม เช่น ชื่อ ที่อยู่ หมายเลขบัตรประชาชน

2. การฝึกอบรมเพื่อเตรียมความพร้อมต้องจัดให้เสร็จภายในระยะเวลาใด

- ก. 15 วัน
- ข. 30 วัน
- ค. 45 วัน
- ง. ภายใน 3 เดือน

เฉลย: ข

คำอธิบาย: กฎหมายและแนวปฏิบัติภายในองค์กรกำหนดให้พนักงานต้องได้รับการอบรมภายใน 1 เดือน (30 วัน) นับตั้งแต่เริ่มงาน

3. ข้อใดไม่ใช่ตัวอย่างของข้อมูลอ่อนไหว (Sensitive Data)

- ก. ข้อมูลสุขภาพ
- ข. ความคิดเห็นทางการเมือง
- ค. สถานะสมรส
- ง. พฤติกรรมทางเพศ

เฉลย: ค

คำอธิบาย: “สถานะสมรส” ไม่ถือเป็นข้อมูลอ่อนไหวตามมาตรา 26 ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4. ก่อนเข้าถึงข้อมูลส่วนบุคคล พนักงานควรทำสิ่งใดก่อน

- ก. ตรวจสอบสิทธิ์การเข้าถึง
- ข. ส่งให้เพื่อนร่วมงานเพื่อขอความคิดเห็น
- ค. บันทึกข้อมูลลง USB ทันทที
- ง. แชร์ผ่านอีเมลภายนอก

เฉลย: ก

คำอธิบาย: ต้องตรวจสอบสิทธิ์ในการเข้าถึงก่อนเสมอเพื่อป้องกันการละเมิดข้อมูล

5. ผู้ที่มีหน้าที่ควบคุมดูแลข้อมูลในองค์กรเรียกว่าอะไร

- ก. เจ้าของข้อมูล
- ข. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
- ค. ผู้จัดการเก็บ
- ง. ผู้ให้บริการไอที

เฉลย: ข

คำอธิบาย: ผู้ควบคุมข้อมูลส่วนบุคคลคือบุคคลหรือนิติบุคคลที่มีหน้าที่ตัดสินใจเกี่ยวกับการเก็บ ใช้ หรือเปิดเผยข้อมูล

6. กรณีพบเห็นการเข้าถึงข้อมูลโดยมิชอบ ควรทำอย่างไร

- ก. เพิกเฉย
- ข. แจ้งหัวหน้าทันที
- ค. โพสต์ลงโซเชียล
- ง. ลบข้อมูลออกจากระบบ

เฉลย: ข

คำอธิบาย: ต้องรายงานเหตุการณ์ให้หัวหน้าหรือ DPO โดยเร็ว เพื่อดำเนินการตรวจสอบและแจ้งเหตุละเมิด

7. พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีผลบังคับใช้เมื่อใด

- ก. 1 มกราคม 2563
- ข. 27 พฤษภาคม 2563
- ค. 1 มิถุนายน 2565
- ง. 1 ตุลาคม 2562

เฉลย: ค

คำอธิบาย: มีผลบังคับใช้เต็มรูปแบบในวันที่ 1 มิถุนายน 2565

8. ข้อใดเป็นความรับผิดชอบของพนักงานในการปกป้องข้อมูล

- ก. แชร์ไฟล์ผ่าน Cloud ส่วนตัว
- ข. ปิดหน้าจอเมื่อไม่ใช้งาน
- ค. ใช้รหัสผ่านเดียวกันทุกระบบ
- ง. ส่งเอกสารผ่านแอปแชท

เฉลย: ข

คำอธิบาย: เป็นมาตรการรักษาความมั่นคงปลอดภัยทางกายภาพที่พนักงานควรปฏิบัติ

9. ข้อมูลใดต่อไปนี้ต้องมี “ความยินยอมโดยชัดแจ้ง” ก่อนเก็บ

ก. ชื่อและนามสกุล

ข. หมายเลขโทรศัพท์

ค. ข้อมูลชีวภาพ เช่น ลายนิ้วมือ

ง. ที่อยู่อีเมลบริษัท

เฉลย: ค

คำอธิบาย: ข้อมูลไบโอเมตริกซ์จัดเป็นข้อมูลอ่อนไหว ต้องได้รับความยินยอมโดยชัดแจ้งก่อนการเก็บหรือใช้

10. หากองค์กรไม่อบรมพนักงานใหม่ภายใน 1 เดือน มีความเสี่ยงอย่างไร

ก. ไม่มีผลใด ๆ

ข. พนักงานเข้าใจเองได้

ค. เสี่ยงต่อการถูกลงโทษทางปกครอง

ง. ไม่กระทบองค์กร

เฉลย: ค

คำอธิบาย: เป็นการไม่ปฏิบัติตามมาตรา 37 (1) ซึ่งอาจะมีโทษปรับทางปกครองสูงสุด 3 ล้านบาท

3.2.3 ผู้บริหารระดับสูง หรือพนักงานในตำแหน่งที่มีความเหมาะสม

เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จะเป็นผู้ดูแลหรืออนุมัติหลักสูตรการฝึกอบรมเบื้องต้น เพื่อเป็นการเตรียมความพร้อมก่อนเข้าทำงาน

สิ่งที่ต้องทำ: มีการอบรมเพื่อเตรียมความพร้อมก่อนเข้าปฏิบัติงาน และมีการกำกับดูแลหรืออนุมัติหลักสูตร

โดยผู้บริหารระดับสูง หรือพนักงานในตำแหน่งที่มีความเหมาะสม เช่น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หลักฐาน: 1) รายงานการประชุมผู้บริหารระดับสูงเพื่อให้เห็นชอบหลักสูตรการอบรม
2) ผลการทดสอบหลังจากพนักงานได้รับการฝึกอบรม

สภาพบังคับ: ไม่มีกฎหมายกำหนด

รายงานการประชุมผู้บริหารระดับสูง เพื่อให้เห็นชอบหลักสูตรการอบรมเบื้องต้น
รายงานการประชุมคณะผู้บริหารระดับสูง

ครั้งที่ 2/2568

วันที่ 10 พฤษภาคม 2568

เวลา 10.00 – 11.30 น.

สถานที่: ห้องประชุม 1 ชั้น 5 อาคารสำนักงานใหญ่

ผู้เข้าร่วมประชุม:

1. นายณรงค์ ศรีธรรม ประธานเจ้าหน้าที่บริหาร
2. นางสาววิภาวดี แสงทอง รองประธานฝ่ายทรัพยากรบุคคล
3. นายอภิวัฒน์ ปัญญาธรรม เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
4. ผู้บริหารแผนกต่าง ๆ รวม 8 คน

วาระที่ 3: พิจารณานุมัติหลักสูตรการอบรมเบื้องต้นก่อนเริ่มปฏิบัติงาน

เสนอโดย: นายอภิวัฒน์ ปัญญาธรรม (DPO)

สรุปสาระการประชุม:

DPO ได้นำเสนอร่างหลักสูตรอบรมเรื่อง "ความรู้เบื้องต้นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและมาตรการความปลอดภัย" สำหรับพนักงานใหม่ โดยมีวัตถุประสงค์เพื่อเตรียมความพร้อมและสร้างความเข้าใจเกี่ยวกับข้อกำหนด สติของเจ้าของข้อมูล และบทบาทของพนักงานในการดูแลข้อมูลส่วนบุคคล

ประเด็นที่ได้รับการพิจารณา:

- ความเหมาะสมของเนื้อหา
- ความสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ระยะเวลาในการอบรม (2 ชั่วโมง)
- การประเมินผลด้วยแบบทดสอบหลังอบรม

มติที่ประชุม:

ที่ประชุมมีมติเห็นชอบร่างหลักสูตรการอบรมเบื้องต้นฉบับที่เสนอโดย DPO และมอบหมายให้ฝ่ายทรัพยากรบุคคลจัดอบรมแก่พนักงานใหม่ทุกราย ภายใน 30 วันนับจากวันที่เริ่มปฏิบัติงาน โดยบังคับให้มีการประเมินผลหลังการอบรมและต้องได้คะแนนไม่ต่ำกว่า 80%

ลงชื่อ

(ลงชื่อ)

นายณรงค์ ศรีธรรม

ประธานการประชุม

ผลการทดสอบหลังอบรมเบื้องต้น สำหรับพนักงานใหม่

ชื่อพนักงาน: นายศุภกิจ สมบูรณ์

ตำแหน่ง: เจ้าหน้าที่ธุรการ

วันที่เข้าร่วมอบรม: 14 พฤษภาคม 2568

ชื่อหลักสูตร: ความรู้เบื้องต้นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ระยะเวลาอบรม: 2 ชั่วโมง (13.00 – 15.00 น.)

รูปแบบ: บรรยาย + ตัวอย่างกรณีศึกษา + แบบทดสอบ

คะแนนที่ได้รับจากแบบทดสอบหลังอบรม:

8.5 จาก 10 คะแนน (85%)

สถานะ: ผ่านเกณฑ์

หมายเหตุ: พนักงานจะได้รับสิทธิ์ในการเข้าระบบฐานข้อมูลของหน่วยงานหลังจากผ่านการอบรมเท่านั้น

ผู้ตรวจสอบและรับรองผล:

(ลงชื่อ)

นางสาวอรพิน พิทักษ์ธรรม

เจ้าหน้าที่ฝ่ายบุคคล

(ลงชื่อ)

นายอภิวัฒน์ ปัญญาธรรม

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

แบบทดสอบหลังการอบรม

จำนวนข้อ: 10 ข้อ

คะแนนเต็ม: 10 คะแนน

เกณฑ์ผ่านขั้นต่ำ: 8 คะแนน (80%)

ข้อ ที่	คำถามสรุปสั้น ๆ	คำตอบที่เลือก	คำตอบที่ ถูก	คะแนนที่ ได้
1	PDPA ย่อมาจากอะไร?	PDPA		1
2	เจ้าของข้อมูลหมายถึงใคร?	บุคคลที่ข้อมูลนั้นเกี่ยวข้อง		1
3	หน่วยงานต้องขอความยินยอมเมื่อใด?	เมื่อเก็บข้อมูลที่ไม่จำเป็น		1

4	การส่งข้อมูลให้บุคคลที่สามต้อง...?	ขอความยินยอมก่อนเสมอ		1
5	ข้อมูลอ่อนไหว ได้แก่...?	ข้อมูลสุขภาพ, ศาสนา ฯลฯ		1
6	หน้าที่ของ DPO คืออะไร?	กำกับ ดูแล แนะนำองค์กรเรื่อง PDPA		1
7	การลบข้อมูลต้อง...?	ทำเมื่อหมดความจำเป็น		1
8	การรักษาความมั่นคงปลอดภัยต้องมี...?	มาตรการทางเทคนิคและองค์กร		1
9	การฝ่าฝืน PDPA มีโทษอะไร?	โทษทางแพ่ง อาญา และปกครอง		0
10	พนักงานต้อง...?	ระมัดระวังในการจัดการข้อมูล		1

คะแนนรวม: 9 / 10

สถานะ: ผ่าน

หมายเหตุ

- พนักงานผ่านเกณฑ์ตามข้อกำหนดที่กำหนด ($\geq 80\%$)
- ได้รับสิทธิ์เข้าระบบสารสนเทศของหน่วยงานตั้งแต่วันที่ 15 พฤษภาคม 2568
- จะต้องเข้าร่วมการอบรมต่อเนื่องในรอบ 12 เดือนข้างหน้า

ลงชื่อผู้ตรวจสอบ:

(ลงชื่อ)

นางสาวอรพิน พิทักษ์ธรรม)

เจ้าหน้าที่ฝ่ายบุคคล

ลงชื่อผู้รับรอง:

(ลงชื่อ)

นายอภิวัฒน์ ปัญญาธรรม

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

วันที่ออกเอกสาร: 15 พฤษภาคม 2568

3.2.4 พนักงานจะต้องเข้ารับการฝึกอบรมเพิ่มเติมในช่วงเวลาที่เหมาะสม

สิ่งที่ต้องทำ: มีการจัดให้พนักงานได้รับการฝึกอบรมเพิ่มเติม ภายในระยะเวลาที่เหมาะสม เช่น ทุก ๆ 6 เดือน และมีการทดสอบเพื่อประเมินผลหลังการฝึกอบรม

หลักฐาน: 1) เอกสารเกี่ยวกับการฝึกอบรมเพิ่มเติม
2) แบบทดสอบเพื่อประเมินผลหลังการฝึกอบรมเพิ่มเติม

สภาพบังคับ: ไม่มีกฎหมายกำหนด

เอกสารเกี่ยวกับการฝึกอบรมเพิ่มเติม

ชื่อหลักสูตร: การเสริมสร้างความเข้าใจและแนวปฏิบัติที่เหมาะสมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA Refresh & Practice)

วัตถุประสงค์ของการอบรม:

- เพื่อให้พนักงานทบทวนความรู้เกี่ยวกับกฎหมาย PDPA
- เพื่ออัปเดตแนวทางปฏิบัติและแนวโน้มความเสี่ยงจากการจัดการข้อมูล
- เพื่อยกระดับการปฏิบัติงานให้เป็นไปตามข้อกำหนดขององค์กร

กลุ่มเป้าหมาย: พนักงานทุกตำแหน่งที่มีหน้าที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

รูปแบบการอบรม:

- ออนไลน์ผ่านระบบ LMS หรือ Zoom
- เอกสารประกอบการอบรม (PDF)
- วิดีทัศน์ตัวอย่างเหตุการณ์ผิดพลาด
- แบบทดสอบออนไลน์ (10 ข้อ)

ระยะเวลาการอบรม: 90 นาที

ความถี่: ทุก 6 เดือน (มิถุนายน และธันวาคมของทุกปี)

กำหนดการอบรมรอบปัจจุบัน:

วันที่: 20 มิถุนายน 2568

เวลา: 13.30 – 15.00 น.

ผู้ดำเนินการอบรม: นางสาวพรวิภา พิชชา ศิริพันธ์ (เจ้าหน้าที่ DPO)

หมายเหตุ: ผู้ที่ไม่ผ่านการประเมินจะต้องเข้ารับการอบรมเสริมภายใน 2 สัปดาห์

แบบทดสอบเพื่อประเมินผลหลังการฝึกอบรมเพิ่มเติม

หัวข้อ: ทบทวนและเสริมสร้างความรู้การคุ้มครองข้อมูลส่วนบุคคล

คำชี้แจง: กรุณาเลือกคำตอบที่ถูกต้องที่สุดเพียงข้อเดียวในแต่ละข้อ

จำนวนข้อ: 10 ข้อ

คะแนนเต็ม: 10 คะแนน

เกณฑ์ผ่าน: 8 คะแนน

แบบทดสอบ

1. ข้อใดเป็นข้อมูลส่วนบุคคลที่อ่อนไหว (sensitive personal data)?
 - ก. หมายเลขโทรศัพท์
 - ข. วันเดือนปีเกิด
 - ค. ข้อมูลทางเชื้อชาติ ☒
 - ง. สถานภาพสมรส
2. การจัดเก็บข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักใดเป็นสำคัญ?
 - ก. ความรวดเร็ว
 - ข. ความเป็นส่วนตัว
 - ค. ความจำเป็น ☒
 - ง. ความสะดวกขององค์กร
3. พนักงานสามารถใช้ข้อมูลส่วนบุคคลที่ได้มาเพื่อวัตถุประสงค์อื่นได้หรือไม่?
 - ก. ได้ หากมีข้อมูลอยู่แล้ว
 - ข. ได้ หากเป็นภายในองค์กร
 - ค. ไม่ได้ ยกเว้นได้รับความยินยอมใหม่ ☒
 - ง. ได้ หากไม่เปลี่ยนแปลงเนื้อหา
4. สิทธิใดของเจ้าของข้อมูลส่วนบุคคลที่สำคัญที่สุดในกรณีต้องการถอนความยินยอม?
 - ก. สิทธิในการแจ้งเตือน
 - ข. สิทธิในการจำกัดการใช้
 - ค. สิทธิในการลบข้อมูล ☒
 - ง. สิทธิในการคัดค้าน
5. หากมีเหตุการณ์ข้อมูลรั่วไหล องค์กรควรทำสิ่งใดเป็นอันดับแรก?
 - ก. แจ้งสื่อมวลชน
 - ข. แจ้งเจ้าของข้อมูลและสำนักงาน กคส. ☒
 - ค. ลบข้อมูลทันที
 - ง. สอบสวนพนักงาน

6. คำว่า “Data Subject” หมายถึงใคร?

ก. เจ้าหน้าที่ดูแลข้อมูล

ข. เจ้าของข้อมูล 

ค. เจ้าหน้าที่ไอที

ง. ผู้ควบคุมข้อมูล

7. ข้อใดไม่ใช่มาตรการรักษาความมั่นคงปลอดภัยตาม PDPA?

ก. การกำหนดสิทธิ์เข้าถึง

ข. การใช้รหัสผ่านที่เข้มงวด

ค. การสื่อสารผ่านไลน์ส่วนตัว 

ง. การบันทึกการเข้าถึงระบบ

8. หากพนักงานลาออก องค์กรควรทำอย่างไรกับข้อมูลที่คุณคนนั้นมี?

ก. โอนให้พนักงานคนใหม่

ข. ลบทิ้งทั้งหมด

ค. เก็บไว้ตามความจำเป็นและลบภายหลัง 

ง. ไม่ต้องทำอะไร

9. การประมวลผลข้อมูลที่ผิดกฎหมายอาจนำไปสู่...?

ก. การขอรับสิทธิเพิ่มเติม

ข. การรับคำชมจากลูกค้า

ค. การดำเนินคดีและโทษทางปกครอง 

ง. การจัดอบรมอีกครั้ง

10. ข้อใดคือหน้าที่ของพนักงานเกี่ยวกับข้อมูลส่วนบุคคล?

ก. ส่งข้อมูลให้หน่วยงานอื่นทันที

ข. เก็บข้อมูลไว้โดยไม่แจ้งเจ้าของข้อมูล

ค. ตรวจสอบและปฏิบัติตามแนวปฏิบัติขององค์กร 

ง. รวบรวมข้อมูลจากแหล่งใดก็ได้

สรุปผลคะแนน:

ตัวอย่าง: นางสาวกัญญารัตน์ พนักงานบัญชี ได้คะแนน 9/10 : ผ่านเกณฑ์

3.3.2 องค์การดำเนินการวิเคราะห์ความต้องการการฝึกอบรม

สำหรับพนักงานด้านการจัดการข้อมูลและการคุ้มครองข้อมูลส่วนบุคคล เพื่อจัดทำแผนการฝึกอบรม และเพื่อให้แน่ใจว่าแผนการฝึกอบรมมีความเฉพาะเจาะจงตามความรับผิดชอบของพนักงานในแต่ละตำแหน่ง

สิ่งที่ต้องทำ: มีการจัดทำแบบสอบถาม และการจัดอบรมตามความต้องการหรือตามความเฉพาะเจาะจงของแต่ละบทบาทพิเศษและหน้าที่ความรับผิดชอบของพนักงาน

หลักฐาน: 1) เอกสารการจัดฝึกอบรม

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1)ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) และ (7)

โทษทางปกครอง: หากไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับไม่เกิน 3 ล้านบาท

เอกสารการจัดฝึกอบรมตามความต้องการเฉพาะบทบาท

เรื่อง: แผนการฝึกอบรมเฉพาะบทบาทและหน้าที่ความรับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA Role-Based Training Plan)

หน่วยงาน: ฝ่ายทรัพยากรบุคคล / ฝ่ายบริหารความเสี่ยงและคุ้มครองข้อมูลส่วนบุคคล (DPO Office)

วันที่จัดทำ: 1 มิถุนายน 2568

ผู้จัดทำ: นางสาวพรวิภา พิชชา ศิริพันธ์ (DPO)

1. วัตถุประสงค์

- เพื่อวิเคราะห์และระบุความต้องการฝึกอบรมเฉพาะบทบาทของพนักงานแต่ละตำแหน่งที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคล
- เพื่อจัดทำแผนฝึกอบรมที่มีความเฉพาะเจาะจง ตรงตามหน้าที่ความรับผิดชอบ และบทบาทพิเศษของพนักงาน
- เพื่อยกระดับความรู้และความสามารถของพนักงานในการปฏิบัติงานตามกฎหมาย PDPA และมาตรการรักษาความมั่นคงปลอดภัย

2. ขอบเขตของการฝึกอบรม

- ครอบคลุมพนักงานทุกฝ่ายที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคล
- เจาะจงกลุ่มพนักงานที่มีบทบาทสำคัญ เช่น

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- ผู้ดูแลระบบไอทีและความปลอดภัยข้อมูล
- ฝ่ายบุคคล (HR)
- ฝ่ายการตลาดและการสื่อสาร
- ฝ่ายกฎหมายและการปฏิบัติตามข้อกำหนด

3. การวิเคราะห์ความต้องการฝึกอบรม

3.1 การเก็บข้อมูลความต้องการฝึกอบรม

- ใช้แบบสอบถามเพื่อเก็บข้อมูลความต้องการด้านการฝึกอบรมจากพนักงานตาม Job Description และบทบาทหน้าที่
- ประเมินความรู้ปัจจุบันและช่องว่างความรู้ที่ต้องได้รับการเสริมเติม
- สำรวจทักษะที่จำเป็น เช่น การจัดการข้อมูล การใช้ระบบรักษาความปลอดภัย และความเข้าใจกฎหมาย PDPA

3.2 ตัวอย่างคำถามในแบบสอบถาม

- คุณเคยได้รับการอบรมเกี่ยวกับ PDPA หรือไม่?
- ความเข้าใจของคุณเกี่ยวกับหน้าที่ความรับผิดชอบในบทบาทของคุณด้านการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างไร?
- คุณต้องการเรียนรู้หัวข้อใดเพิ่มเติม เช่น การจัดการข้อมูล, การรักษาความปลอดภัย, การตอบสนองเหตุการณ์ข้อมูลรั่วไหล ฯลฯ
- ระยะเวลาที่เหมาะสมสำหรับการอบรมครั้งต่อไป

แผนการฝึกอบรมเฉพาะบทบาท (Role-Based Training Plan)

กลุ่มเป้าหมาย	เนื้อหาการฝึกอบรมหลัก	วิธีการอบรม	ความถี่ในการอบรม	ผู้รับผิดชอบ
เจ้าหน้าที่ DPO	กฎหมาย PDPA ระดับสูง, การตรวจสอบระบบ, การจัดการเหตุการณ์ข้อมูลรั่วไหล	อบรมเชิงปฏิบัติการ, Webinar	6 เดือน/ครั้ง	DPO, ฝ่ายกฎหมาย
ฝ่ายไอทีและความปลอดภัย	ระบบรักษาความปลอดภัยข้อมูล, การเข้ารหัสข้อมูล, การ	การอบรมภาคปฏิบัติ, e-Learning	6 เดือน/ครั้ง	ฝ่ายไอที

	ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต			
ฝ่ายบุคคล (HR)	การจัดการข้อมูลส่วนบุคคล พนักงาน, การเก็บข้อมูลอย่างปลอดภัย	สัมมนา, Workshop	1 ปี/ครั้ง	ฝ่าย HR, DPO
ฝ่ายการตลาดและสื่อสาร	การใช้ข้อมูลลูกค้าอย่างถูกต้อง, แนวทางการขอความยินยอม	Webinar, e-Learning	1 ปี/ครั้ง	ฝ่ายการตลาด
ฝ่ายกฎหมายและ Compliance	การติดตามกฎหมายใหม่, การจัดการความเสี่ยง	Workshop, การประชุม	ตามความจำเป็น	ฝ่ายกฎหมาย

5. การประเมินผลและติดตามผล

- มีการทดสอบก่อนและหลังอบรม (Pre-Test/Post-Test) เพื่อวัดระดับความรู้และความเข้าใจ
- สอบถามความพึงพอใจและความต้องการเพิ่มเติมหลังการอบรม
- รายงานสรุปผลการฝึกอบรมและความคืบหน้าต่อผู้บริหาร

6. เอกสารแนบ

- แบบสอบถามความต้องการฝึกอบรม (แนบตัวอย่าง)
- รายงานผลการวิเคราะห์ความต้องการ
- ตารางแผนการฝึกอบรมเฉพาะบทบาท
- แบบฟอร์มประเมินผลการอบรม

ลงชื่อ.....

(นางสาวพรวิภา พิชชา ศิริรินทร์)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

วันที่: 1 มิถุนายน 2568

แบบสอบถามชุดที่ 1: ฝ่ายไอที (IT)

คำถาม

1. ข้อมูลส่วนบุคคลควรเก็บไว้ในรูปแบบใดเพื่อความปลอดภัยสูงสุด?
2. การเข้ารหัสข้อมูล (Encryption) มีประโยชน์อย่างไร?
3. Firewall คืออะไรและทำหน้าที่อะไรในระบบไอที?
4. การตั้งรหัสผ่านที่ดีควรมีลักษณะอย่างไร?
5. อะไรคือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized access)?

6. การอัปเดตระบบปฏิบัติการและซอฟต์แวร์มีความสำคัญอย่างไรต่อความปลอดภัยข้อมูล?
7. ควรจัดการอย่างไรเมื่อพบการรั่วไหลของข้อมูลส่วนบุคคลในระบบ?
8. VPN ช่วยปกป้องข้อมูลได้อย่างไร?
9. การสำรองข้อมูล (Backup) ควรทำบ่อยแค่ไหน?
10. กฎหมาย PDPA กำหนดบทบาทใครเป็นผู้ดูแลความปลอดภัยข้อมูลส่วนบุคคลในองค์กร?

เฉลยและคำอธิบาย

1. **เก็บในรูปแบบที่เข้ารหัส (Encrypted)** — เพื่อป้องกันไม่ให้ข้อมูลถูกอ่านหรือถูกนำไปใช้โดยผู้ไม่ได้รับอนุญาต
2. **ช่วยป้องกันการเข้าถึงข้อมูลจากบุคคลที่ไม่ได้รับอนุญาต** โดยการแปลงข้อมูลเป็นรหัสที่ต้องถอดรหัสก่อนอ่านได้
3. **Firewall** คือระบบป้องกันเครือข่าย ที่ช่วยควบคุมและกรองข้อมูลเข้า-ออก เพื่อป้องกันการโจมตีจากภายนอก
4. **รหัสผ่านที่ดีควรประกอบด้วยตัวอักษรใหญ่-เล็ก ตัวเลข และอักขระพิเศษ และมีความยาวอย่างน้อย 8 ตัว** เพื่อเพิ่มความปลอดภัย
5. **การเข้าถึงโดยไม่ได้รับอนุญาตคือการเข้าถึงข้อมูลหรือระบบโดยบุคคลที่ไม่มีสิทธิ์** เช่น แฮกเกอร์หรือพนักงานที่ไม่มีสิทธิ์
6. **เพื่อแก้ไขช่องโหว่ของระบบและป้องกันการโจมตีทางไซเบอร์**
7. **แจ้งผู้รับผิดชอบทันที ดำเนินการตรวจสอบและจำกัดความเสียหาย รวมถึงแจ้งผู้ที่ได้รับผลกระทบตามข้อกำหนด**
8. **VPN** สร้างการเชื่อมต่อที่ปลอดภัยและเข้ารหัสข้อมูลระหว่างผู้ใช้กับเครือข่าย ป้องกันการดักข้อมูล
9. **ขึ้นอยู่กับนโยบายองค์กร แต่ควรทำอย่างน้อยสัปดาห์ละครั้งหรือเดือนละครั้ง**
10. **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)**

แบบสอบถามชุดที่ 2: ฝ่ายบุคคล (HR)

คำถาม

1. ข้อมูลส่วนบุคคลของพนักงานที่ฝ่ายบุคคลเก็บต้องปฏิบัติตามกฎหมายใด?
2. ควรเก็บข้อมูลส่วนบุคคลของพนักงานไว้นานแค่ไหน?
3. การขอความยินยอมในการเก็บข้อมูลส่วนบุคคลต้องทำอย่างไร?
4. การเปิดเผยข้อมูลส่วนบุคคลของพนักงานโดยไม่ได้รับอนุญาตเป็นสิ่งที่ผิดหรือไม่?
5. ฝ่ายบุคคลควรจัดการอย่างไรเมื่อได้รับคำขอจากพนักงานในการเข้าถึงข้อมูลส่วนบุคคลของตนเอง?
6. การส่งข้อมูลพนักงานผ่านอีเมล ควรมีมาตรการป้องกันอย่างไร?
7. การลบข้อมูลส่วนบุคคลของพนักงานเมื่อสิ้นสุดการทำงาน ต้องดำเนินการอย่างไร?
8. ควรจัดฝึกอบรมเรื่องการคุ้มครองข้อมูลส่วนบุคคลกับฝ่ายบุคคลบ่อยแค่ไหน?
9. การแบ่งปันข้อมูลส่วนบุคคลกับบุคคลภายนอกองค์กร ต้องมีเงื่อนไขอย่างไร?
10. ใครคือผู้รับผิดชอบสูงสุดในการคุ้มครองข้อมูลส่วนบุคคลของพนักงานในองค์กร?

เฉลยและคำอธิบาย

1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
2. เก็บเท่าที่จำเป็นสำหรับวัตถุประสงค์ และตามระยะเวลาที่กฎหมายหรือองค์กรกำหนด
3. ต้องแจ้งวัตถุประสงค์การเก็บ ใช้และเปิดเผยข้อมูล พร้อมให้พนักงานยินยอมอย่างชัดเจน
4. ผิด เพราะเป็นการละเมิดสิทธิความเป็นส่วนตัวและกฎหมายคุ้มครองข้อมูล
5. ต้องดำเนินการตามคำขอภายในเวลาที่กฎหมายกำหนด และให้ข้อมูลที่ถูกต้องและครบถ้วน
6. ใช้การเข้ารหัสข้อมูล หรือส่งผ่านช่องทางที่ปลอดภัย เช่น VPN หรือระบบที่มีการรักษาความปลอดภัย
7. ต้องลบหรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้ ตามนโยบายและกฎหมายที่เกี่ยวข้อง
8. อย่างน้อยปีละ 1 ครั้ง หรือบ่อยตามความจำเป็นและนโยบายองค์กร
9. ต้องได้รับความยินยอมจากเจ้าของข้อมูล และมีสัญญาคุ้มครองข้อมูลกับผู้รับข้อมูล
10. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และผู้บริหารระดับสูง

แบบสอบถามชุดที่ 3: ฝ่ายการตลาด (Marketing)

คำถาม

1. การเก็บข้อมูลลูกค้าสำหรับการตลาดต้องได้รับความยินยอมหรือไม่?
2. การใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อส่งโฆษณาต้องปฏิบัติตามข้อใด?
3. ควรแจ้งให้ลูกค้าทราบอะไรบ้างเมื่อเก็บข้อมูลส่วนบุคคล?
4. การส่งข้อมูลลูกค้าให้บุคคลที่สามเพื่อทำการตลาด ต้องมีเงื่อนไขอะไร?
5. การเก็บข้อมูลผ่านเว็บไซต์ ต้องมีมาตรการอะไรเพื่อคุ้มครองข้อมูล?
6. การเก็บข้อมูลส่วนบุคคลเกินกว่าความจำเป็นในงานการตลาดถือว่าผิดหรือไม่?
7. การจัดเก็บฐานข้อมูลลูกค้าเพื่อการตลาดควรเก็บไว้ในระบบแบบใด?
8. เมื่อมีคำขอให้ลบข้อมูลส่วนบุคคล ลูกค้าสามารถขอได้หรือไม่?
9. ฝ่ายการตลาดควรมีการฝึกอบรมเรื่องการคุ้มครองข้อมูลส่วนบุคคลบ่อยแค่ไหน?
10. ข้อใดต่อไปนี้เป็นไม่ใช่ข้อมูลส่วนบุคคล?
 - ก) ชื่อและนามสกุล
 - ข) เบอร์โทรศัพท์
 - ค) ข้อมูลสภาพอากาศที่ลูกค้าอยู่
 - ง) ที่อยู่บ้าน

เฉลยและคำอธิบาย

1. ต้องได้รับความยินยอมอย่างชัดเจนจากลูกค้า (Consent)
2. ต้องปฏิบัติตามกฎหมาย PDPA และต้องไม่เกินวัตถุประสงค์ที่ได้รับอนุญาต
3. แจ้งวัตถุประสงค์การเก็บข้อมูล วิธีใช้ และสิทธิของลูกค้าในการยกเลิกหรือถอนความยินยอม
4. ต้องได้รับความยินยอมจากเจ้าของข้อมูลและมีสัญญาคุ้มครองข้อมูลกับผู้รับข้อมูล
5. ใช้การเข้ารหัสข้อมูล มีนโยบายความเป็นส่วนตัว และมาตรการป้องกันการโจมตีจากภายนอก
6. ถือว่าผิดเพราะละเมิดหลักการเก็บข้อมูลอย่างจำกัดวัตถุประสงค์
7. ควรเก็บในระบบที่มีการรักษาความปลอดภัยสูง เช่น ฐานข้อมูลที่เข้ารหัสและจำกัดการเข้าถึง
8. สามารถขอให้ลบได้ตามสิทธิใน PDPA
9. อย่างน้อยปีละครั้ง เพื่อให้ทันกับกฎหมายและแนวทางปฏิบัติใหม่ๆ
10. ค) ข้อมูลสภาพอากาศที่ลูกค้าอยู่ เพราะไม่ใช่ข้อมูลส่วนบุคคลโดยตรง

แบบทดสอบ ฝ่ายกฎหมาย (Legal)

คำถาม

1. อธิบายความแตกต่างระหว่าง **Data Controller** กับ **Data Processor** ภายใต้ GDPR
2. อะไรคือหลักการ “**Accountability Principle**” และองค์กรต้องปฏิบัติอย่างไรเพื่อให้สอดคล้องกับหลักการนี้?
3. อธิบายความหมายของ **Lawful Basis for Processing** พร้อมยกตัวอย่างเหตุผลที่ถูกต้องตามกฎหมาย
4. ข้อมูลประเภทใดบ้างที่ถูกจัดให้อยู่ในกลุ่ม **Special Category Data** และการประมวลผลข้อมูลเหล่านี้มีข้อจำกัดอย่างไร?
5. GDPR กำหนดว่า Data Subject มีสิทธิอะไรบ้างที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล?
6. การถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม (Third Country Transfer) ต้องปฏิบัติตามเงื่อนไขอะไรภายใต้ GDPR?
7. ในกรณีที่เกิดการละเมิดข้อมูลส่วนบุคคล (Data Breach) องค์กรต้องแจ้งต่อหน่วยงานคุ้มครองข้อมูล (Data Protection Authority) ภายในกี่ชั่วโมง?
8. อธิบายความหมายของ **Data Protection Impact Assessment (DPIA)** และองค์กรควรจัดทำเมื่อใด?
9. GDPR มีบทลงโทษทางการเงินสูงสุดสำหรับการละเมิดอย่างร้ายแรงคือเท่าใด?
10. ในกรณีที่ Data Subject ขอใช้สิทธิ “**Right to be forgotten**” องค์กรต้องดำเนินการอย่างไรและมีข้อยกเว้นอะไรบ้าง?

เฉลยและคำอธิบาย

1. **Data Controller** คือองค์กรหรือบุคคลที่กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล ขณะที่ **Data Processor** คือองค์กรหรือบุคคลที่ประมวลผลข้อมูลส่วนบุคคลในนามของ Data Controller ตัวอย่าง: บริษัทเป็น Controller และผู้ให้บริการคลาวด์เป็น Processor
เหตุผล: เพื่อกำหนดความรับผิดชอบและการควบคุมข้อมูลอย่างชัดเจน
2. **Accountability Principle** คือหลักการที่องค์กรต้องรับผิดชอบและสามารถแสดงหลักฐานได้ว่าปฏิบัติตาม GDPR ต้องมีนโยบาย กฎเกณฑ์ การบันทึก และการตรวจสอบที่เหมาะสม ตัวอย่างเช่น การจัดทำ DPIA การอบรมพนักงาน และการบันทึกการประมวลผลข้อมูล
3. **Lawful Basis for Processing** หมายถึงเหตุผลทางกฎหมายที่อนุญาตให้องค์กรประมวลผลข้อมูลได้ เช่น Consent (ความยินยอม) Contractual necessity (จำเป็นตามสัญญา) Legal obligation (ข้อผูกพันตามกฎหมาย) Legitimate interests (ผลประโยชน์ชอบด้วยกฎหมายขององค์กร)

4. **Special Category Data** ได้แก่ข้อมูลเชิงอ่อนไหว เช่น ข้อมูลสุขภาพ, ชาติพันธุ์, ความคิดเห็นทางการเมือง, ศาสนา การประมวลผลต้องมีเหตุผลพิเศษและต้องมีมาตรการคุ้มครองเข้มงวด เช่น ต้องได้รับความยินยอมเฉพาะ หรือเพื่อประโยชน์ทางสุขภาพ
5. Data Subject มีสิทธิ เช่น Right of access (ขอเข้าถึงข้อมูล) Right to rectification (แก้ไขข้อมูล)
Right to erasure (ลบข้อมูล) Right to restrict processing (จำกัดการประมวลผล) Right to data portability (ย้ายข้อมูล) Right to object (คัดค้านการประมวลผล)
6. การถ่ายโอนข้อมูลไปยังประเทศที่สามต้องมีการรับรองความปลอดภัย เช่น อยู่ในรายชื่อประเทศที่ได้รับการยอมรับ (Adequacy Decision)
ใช้สัญญามาตรฐาน (Standard Contractual Clauses)
มีมาตรการป้องกันที่เหมาะสม (Appropriate Safeguards)
7. ต้องแจ้ง Data Protection Authority ภายใน **72 ชั่วโมง** หลังจากพบเหตุการณ์ Data Breach
DPIA คือกระบวนการประเมินความเสี่ยงและผลกระทบต่อสิทธิและเสรีภาพของบุคคลจากการประมวลผลข้อมูล
8. ควรจัดทำเมื่อมีการประมวลผลข้อมูลที่อาจมีความเสี่ยงสูง เช่น การใช้เทคโนโลยีใหม่ หรือการเก็บข้อมูลเชิงอ่อนไหวจำนวนมากโทษปรับสูงสุดคือ **20 ล้านยูโร หรือ 4% ของรายได้ทั่วโลกประจำปีขององค์กร (แล้วแต่จำนวนใดสูงกว่า)**
9. องค์กรต้องลบข้อมูลส่วนบุคคลตามคำขอเว้นแต่จะมีข้อยกเว้น เช่น ข้อมูลยังจำเป็นสำหรับการปฏิบัติตามภาระผูกพันทางกฎหมาย เพื่อการป้องกันการทุจริตหรือการฟ้องร้องการใช้ข้อมูลเพื่อเสรีภาพในการแสดงออกหรือปฏิบัติหน้าที่ของรัฐ

3.3.3 มีการกำหนดความต้องการด้านการฝึกอบรมและทักษะที่จำเป็นต้องมีตามหน้าที่ความรับผิดชอบสำหรับงานที่ปฏิบัติของพนักงาน (Job Description)

สิ่งที่ต้องทำ: มีการจัดทำแบบทดสอบ และจัดการอบรมตามความต้องการในการฝึกอบรมและทักษะที่จำเป็นต้องมีตามหน้าที่ความรับผิดชอบสำหรับงานที่ปฏิบัติของพนักงาน (Job Description)

หลักฐาน: 1) แบบสอบถามความต้องการฝึกอบรมของพนักงาน
2) เอกสารการจัดฝึกอบรม

สภาพบังคับ: ไม่มีกฎหมายกำหนด

1) แบบสอบถามความต้องการฝึกอบรมของพนักงาน (Training Needs Assessment Questionnaire)

แบบสอบถามความต้องการฝึกอบรมสำหรับพนักงาน

วัตถุประสงค์: เพื่อระบุความต้องการด้านการฝึกอบรมและทักษะที่จำเป็นตามหน้าที่รับผิดชอบของพนักงานแต่ละตำแหน่ง

ส่วนที่ 1: ข้อมูลทั่วไปของพนักงาน

ชื่อ-นามสกุล: _____

ตำแหน่งงาน: _____

แผนก/ฝ่าย: _____

ระยะเวลาการทำงานในตำแหน่งนี้: _____ เดือน/ปี

ส่วนที่ 2: ความต้องการฝึกอบรมตามหน้าที่ความรับผิดชอบ

โปรดทำเครื่องหมาย (✓) ในช่องที่ตรงกับความต้องการฝึกอบรมของท่าน

หมวดหมู่ทักษะ/หัวข้อการฝึกอบรม	ความจำเป็นในการฝึกอบรม (✓)	หมายเหตุ เพิ่มเติม
ความรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA GDPR)	☐ สูง ☐ ปานกลาง ☐ ต่ำ	
การรักษาความปลอดภัยของข้อมูล (Data Security)	☐ สูง ☐ ปานกลาง ☐ ต่ำ	
การจัดการข้อมูลส่วนบุคคลในระบบ IT	☐ สูง ☐ ปานกลาง ☐ ต่ำ	
การปฏิบัติตามกฎหมายและนโยบายองค์กร	☐ สูง ☐ ปานกลาง ☐ ต่ำ	
การจัดการเหตุการณ์ละเมิดข้อมูล (Data Breach Response)	☐ สูง ☐ ปานกลาง ☐ ต่ำ	
การใช้เครื่องมือและซอฟต์แวร์ที่เกี่ยวข้อง	☐ สูง ☐ ปานกลาง ☐ ต่ำ	
ทักษะการสื่อสารและอบรมภายในองค์กร	☐ สูง ☐ ปานกลาง ☐ ต่ำ	
การบริหารจัดการความเสี่ยงด้านข้อมูล	☐ สูง ☐ ปานกลาง ☐ ต่ำ	
ทักษะเฉพาะทางอื่น ๆ (โปรดระบุ): _____	☐ สูง ☐ ปานกลาง ☐ ต่ำ	

ส่วนที่ 3: ข้อเสนอแนะเพิ่มเติม

โปรดระบุความเห็นหรือข้อเสนอแนะเกี่ยวกับการฝึกอบรมที่ต้องการเพิ่มเติม

2) เอกสารการจัดฝึกอบรม (Training Documentation)

รายงานการฝึกอบรมตามความต้องการและหน้าที่รับผิดชอบของพนักงาน

วัน/เดือน/ปี	หัวข้อการฝึกอบรม	กลุ่มเป้าหมาย	ผู้จัดอบรม	สถานที่	สรุปผลการอบรมและความคิดเห็น
15/03/2025	การคุ้มครองข้อมูลส่วนบุคคลตาม PDPA/GDPR	ฝ่ายกฎหมาย ฝ่าย IT ฝ่ายบุคคล	นิติกรและที่ปรึกษา กฎหมาย	ห้องประชุมใหญ่	พนักงานมีความเข้าใจหลักการและข้อบังคับดีขึ้น
02/04/2025	การจัดการเหตุการณ์ละเมิดข้อมูล (Data Breach Response)	ฝ่าย IT ฝ่ายบริหาร	ผู้เชี่ยวชาญด้านความปลอดภัยข้อมูล	ห้องฝึกอบรม	สามารถตอบสนองต่อเหตุการณ์ได้รวดเร็วและเหมาะสม
10/06/2025	การใช้ซอฟต์แวร์จัดการข้อมูลส่วนบุคคล	ฝ่ายบุคคลและฝ่ายการตลาด	ทีมเทคนิค IT	ออนไลน์	พนักงานมีทักษะใช้งานซอฟต์แวร์เพิ่มขึ้น

สรุป

แบบสอบถามจะช่วยให้องค์กรรู้ความต้องการฝึกอบรมเฉพาะตามตำแหน่งงาน (Job Description) เอกสารการจัดฝึกอบรมแสดงการดำเนินงานจริง สอดคล้องกับความต้องการและหน้าที่ความรับผิดชอบของพนักงาน

3.3.4 มีการจัดเก็บสำเนาของเอกสารการฝึกอบรม รวมทั้งรายละเอียดของผู้เข้ารับการฝึกอบรม

สิ่งที่ต้องทำ: การจัดเก็บสำเนาเอกสารการฝึกอบรม รวมทั้งรายละเอียดของผู้เข้ารับการฝึกอบรม พร้อมลายมือชื่อเข้ารับการอบรม และผลการประเมิน สรุปผู้ที่ผ่านเกณฑ์ขั้นต่ำของการอบรม

หลักฐาน: 1) รายละเอียดของผู้เข้ารับการฝึกอบรม
2) ผลการประเมินหลังจากเข้ารับการอบรม
3) ลายมือชื่อผู้เข้ารับการอบรม

สภาพบังคับ: ไม่มีกฎหมายกำหนด

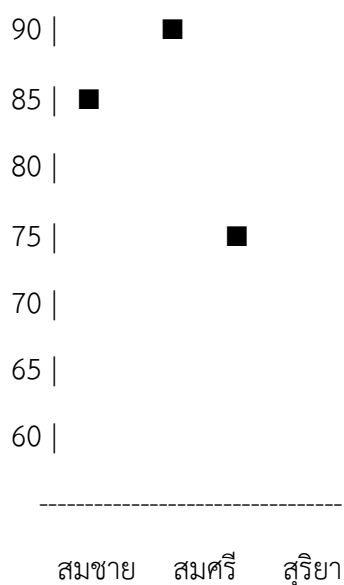
ตัวอย่าง รายละเอียดของผู้เข้ารับการฝึกอบรม (Training Attendance List)

ลำดับ	ชื่อ-นามสกุล	ตำแหน่งงาน	แผนก/ฝ่าย	วันที่อบรม	เวลาอบรม	หมายเหตุ
1	นายสมชาย ใจดี	เจ้าหน้าที่ไอที	ฝ่ายเทคโนโลยีสารสนเทศ	1 มิ.ย. 2566	09:00-12:00	เข้าร่วมครบถ้วน
2	นางสาวสมศรี พูนสุข	เจ้าหน้าที่บุคคล	ฝ่ายบุคคล	1 มิ.ย. 2566	09:00-12:00	ขาดเรียน 30 นาที
3	นายสุริยา สังข์ทอง	นักกฎหมาย	ฝ่ายกฎหมาย	1 มิ.ย. 2566	09:00-12:00	เข้าร่วมครบถ้วน

ผลการประเมินหลังจากเข้ารับการอบรม (Training Evaluation Results)

ลำดับ	ชื่อ-นามสกุล	คะแนนการประเมิน (เต็ม 100)	ผ่านเกณฑ์ (≥ 70)	หมายเหตุ
1	นายสมชาย ใจดี	85	ผ่าน	มีความเข้าใจดีมาก
2	นางสาวสมศรี พูนสุข	68	ไม่ผ่าน	ควรได้รับการอบรมซ้ำ
3	นายสุริยา สังข์ทอง	75	ผ่าน	ทบทวนเพิ่มเติมเล็กน้อย

คะแนนการประเมิน (เต็ม 100)



ลายมือชื่อผู้เข้ารับการอบรม (Training Attendance Signature Sheet)

ลำดับ	ชื่อ-นามสกุล	ลงชื่อรับรองการเข้ารับการอบรม	วันที่ลงชื่อ
1	นายสมชาย ใจดี		1 มิ.ย. 2566
2	นางสาวสมศรี พูนสุข		1 มิ.ย. 2566
3	นายสุริยา สังข์ทอง		1 มิ.ย. 2566

3.4.1 มีการประเมินในตอนท้ายของการฝึกอบรมเพื่อทดสอบความรู้และความเข้าใจของพนักงาน และเพื่อให้เกิดความมั่นใจว่าการฝึกอบรมนั้นได้ผล โดยมีการกำหนดคะแนนขั้นต่ำเพื่อใช้ในการประเมินผลการผ่านการฝึกอบรม

สิ่งที่ต้องทำ: มีการประเมินผลภายหลังการอบรม และมีการรายงานต่อพนักงานอาวุโสเกี่ยวกับผลการทดสอบของพนักงาน เพื่อวางแผนการฝึกอบรมในอนาคต

หลักฐาน: 1) แบบทดสอบประเมินผลการอบรมของพนักงาน
2) สรุปผลว่าผ่านเกณฑ์การประเมินหรือไม่

สภาพบังคับ: ไม่มีกฎหมายกำหนด

แบบทดสอบประเมินผลการอบรมของพนักงาน (Training Evaluation Test)

ตัวอย่างแบบทดสอบ 10 ข้อ (เน้นความรู้เรื่องการคุ้มครองข้อมูลส่วนบุคคล)

1. ข้อมูลส่วนบุคคลหมายถึงอะไร?

- ก. ข้อมูลที่ระบุตัวบุคคลได้
- ข. ข้อมูลสาธารณะ
- ค. ข้อมูลที่ไม่เกี่ยวข้องกับบุคคล
- ง. ข้อมูลที่ใช้ในงานบัญชี

2. การขอความยินยอม (Consent) ในการเก็บข้อมูลส่วนบุคคลต้องเป็นอย่างไร?

- ก. ต้องเป็นความสมัครใจ แจ่มชัดเจน และสามารถถอนความยินยอมได้
- ข. ขอครั้งเดียวใช้ได้ตลอดไป
- ค. ไม่ต้องแจ้งให้ทราบ
- ง. ขอความยินยอมผ่านบุคคลที่สามได้

3. พนักงานควรทำอะไรเมื่อพบว่าข้อมูลส่วนบุคคลรั่วไหล?

- ก. รายงานทันทีต่อเจ้าหน้าที่คุ้มครองข้อมูล
- ข. ลบข้อมูลทันที
- ค. ไม่ต้องแจ้งใคร
- ง. ส่งต่อให้เพื่อนร่วมงาน

(ตัวอย่างคำถามอื่น ๆ ตามเนื้อหาอบรมจริง)

เกณฑ์ผ่าน: คะแนนขั้นต่ำ 70% (ได้ 7 ข้อขึ้นไป)

2) สรุปผลการประเมิน

ชื่อพนักงาน	คะแนนที่ได้	ผ่านเกณฑ์ (≥70%)	หมายเหตุ
นายสมชาย	85	ผ่าน	ความรู้ดีมาก
นางสาวสมศรี	68	ไม่ผ่าน	ต้องอบรมเสริมเพิ่มเติม
นายสุริยา	75	ผ่าน	ความรู้อยู่ในเกณฑ์ที่ดี

รายงานสรุป

- พนักงานจำนวน 3 คนเข้ารับการฝึกอบรม
- 2 คนผ่านเกณฑ์การประเมิน
- 1 คนต้องได้รับการอบรมเพิ่มเติมในหัวข้อที่คะแนนต่ำ

ข้อเสนอแนะ:

- จัดอบรมเสริมให้พนักงานที่ไม่ผ่านภายใน 1 เดือน
- ทบทวนและปรับปรุงหลักสูตรเพื่อเพิ่มประสิทธิภาพ

3.4.2 มีการจัดเก็บสำเนาของเอกสารการฝึกอบรม รวมทั้งรายละเอียดของผู้เข้ารับการฝึกอบรม

สิ่งที่ต้องทำ: มีการจัดเก็บรายละเอียดของผู้เข้ารับการฝึกอบรม ผลการประเมินหลังจากเข้ารับการอบรม พร้อมลายมือชื่อ และมีการจัดให้ง่ายต่อการเข้าถึงเอกสารการอบรม (อาจอยู่ในรูปแบบอิเล็กทรอนิกส์)

หลักฐาน: 1) ผลการประเมินหลังการฝึกอบรม
2) หลักฐานแสดงตนของผู้เข้ารับการอบรม
3) เอกสารการอบรมที่เข้าถึงได้ง่าย

สภาพบังคับ: ไม่มีกฎหมายกำหนด

ผลการประเมินหลังการฝึกอบรม (Training Evaluation Results)

ลำดับ	ชื่อผู้เข้ารับการอบรม	วันที่อบรม	คะแนนที่ได้	ผ่านเกณฑ์ (≥70%)	หมายเหตุ
1	นายสมชาย	01/06/2025	85	ผ่าน	ความรู้ดีมาก
2	นางสาวสมศรี	01/06/2025	68	ไม่ผ่าน	ต้องอบรมเสริมเพิ่มเติม
3	นายสุริยา	01/06/2025	75	ผ่าน	ความรู้อยู่ในเกณฑ์ดี

หลักฐานแสดงตนของผู้เข้ารับการอบรม (Attendee Identification Evidence)

ตัวอย่าง:

- สำเนาบัตรประจำตัวพนักงาน (Employee ID Card) หรือบัตรประชาชนที่พนักงานใช้ลงทะเบียนเข้าร่วมอบรม
- มีการจัดเก็บสำเนาบัตรพร้อมลายเซ็นรับรองการเข้าร่วมอบรมของแต่ละคน

ตัวอย่างข้อมูลในเอกสาร

- ชื่อ-สกุล
- หมายเลขพนักงาน
- วันที่อบรม
- ลายเซ็นผู้เข้ารับการอบรม

เอกสารการอบรมที่เข้าถึงได้ง่าย (Accessible Training Materials)

1. เอกสารการอบรมในรูปแบบอิเล็กทรอนิกส์ (เช่น PDF, PowerPoint) ถูกจัดเก็บในระบบแชร์ไฟล์ขององค์กร เช่น SharePoint, Google Drive, หรือระบบ LMS (Learning Management System)

2. มีโฟลเดอร์ที่ชัดเจนแยกตามหัวข้อการอบรมและปีที่จัดอบรม

ตัวอย่างโครงสร้างไฟล์ เช่น swift CopyEdit/TrainingMaterials/ /DataPrivacy/ /2025/

- DataPrivacy_Training_Slide.pdf
- DataPrivacy_Quiz.pdf
- TrainingSummary_2025.pdf

3. ผู้มีสิทธิ์เข้าถึงเอกสาร เช่น ผู้บริหาร, เจ้าหน้าที่ HR, DPO สามารถเปิดอ่านดาวน์โหลดได้ง่าย และมีระบบควบคุมสิทธิ์ (Access Control)

3.4.3 มีการติดตามและประเมินผลภายหลังการฝึกอบรม โดยกำหนดคะแนนขั้นต่ำสำหรับการผ่านแบบทดสอบขององค์กร และมีการติดตามพนักงานที่ไม่ผ่านแบบทดสอบ หรือยังไม่ได้เข้ารับการอบรม จนกว่าจะผ่านเกณฑ์คะแนนขั้นต่ำของแบบทดสอบ

สิ่งที่ต้องทำ: มีการกำหนดคะแนนขั้นต่ำของแบบทดสอบ และมีการติดตามพนักงานที่ไม่ผ่านการประเมิน หรือมีการจัดอบรมใหม่ให้กับพนักงานที่ยังไม่ได้เข้ารับการอบรม

หลักฐาน: 1) แบบทดสอบ
2) รายงานการประเมินผลของพนักงานจากการฝึกอบรม

สภาพบังคับ: ไม่มีกฎหมายกำหนด

แบบทดสอบ (Quiz for Post-Training Assessment)

หัวข้อ: การฝึกอบรมคุ้มครองข้อมูลส่วนบุคคล (Data Protection Training)

จำนวนข้อ: 10 ข้อ

คะแนนเต็ม: 100 คะแนน

คะแนนขั้นต่ำผ่าน: 70 คะแนน

ตัวอย่างคำถาม (Multiple Choice)

1. ข้อมูลส่วนบุคคล (Personal Data) หมายถึงอะไร?

- ก) ข้อมูลที่เกี่ยวข้องกับตัวบุคคลที่ระบุตัวตนได้
- ข) ข้อมูลสาธารณะที่ทุกคนเข้าถึงได้
- ค) ข้อมูลที่ไม่เกี่ยวข้องกับบุคคล
- ง) ข้อมูลทางการเงินของบริษัท

2. GDPR กำหนดให้ผู้ควบคุมข้อมูลต้องดำเนินการอย่างไรเมื่อมีการละเมิดข้อมูลส่วนบุคคล?

- ก) แจ้งหน่วยงานภายใน 72 ชั่วโมง
- ข) ปิดระบบข้อมูลทันที
- ค) แจ้งเจ้าของข้อมูลภายใน 1 เดือน
- ง) ไม่ต้องแจ้งอะไร

3. การ pseudonymisation คืออะไร?

- ก) การเข้ารหัสข้อมูลที่ระบุบุคคลได้
- ข) การเปลี่ยนชื่อผู้ใช้งาน
- ค) การแทนที่ข้อมูลส่วนบุคคลด้วยข้อมูลที่ไม่ระบุตัวตน
- ง) การลบข้อมูลทั้งหมด

(และอื่น ๆ รวม 10 ข้อ)

คำแนะนำ:

- คะแนน 70 ขึ้นไปถือว่าผ่าน
- คะแนนต่ำกว่าต้องเข้ารับการอบรมซ้ำและทดสอบใหม่

รายงานการประเมินผลของพนักงานจากการฝึกอบรม (Training Evaluation Report)

ลำดับ	ชื่อพนักงาน	ตำแหน่ง	วันที่อบรม	คะแนนทดสอบ	ผ่านเกณฑ์ (70+)	สถานะติดตาม
1	นายสมชาย ใจดี	เจ้าหน้าที่ IT	1 มิ.ย. 2568	85	ผ่าน	-
2	นางสาวสุภาวดี	เจ้าหน้าที่ HR	1 มิ.ย. 2568	65	ไม่ผ่าน	ส่งเข้าอบรมซ้ำ 15 มิ.ย. 2568
3	นายวิทยา สาระ	เจ้าหน้าที่ การตลาด	2 มิ.ย. 2568	75	ผ่าน	-
4	นางสาวลลิตา	เจ้าหน้าที่ บัญชี	2 มิ.ย. 2568	-	ยังไม่ได้สอบ	นัดอบรมครั้งถัดไป 10 มิ.ย. 2568

สรุปผล

- จำนวนพนักงานผ่าน: 2 คน (50%)
- จำนวนพนักงานไม่ผ่าน: 1 คน (25%)
- จำนวนพนักงานยังไม่เข้ารับการอบรม: 1 คน (25%)

3.4.4 พนักงานสามารถให้ข้อเสนอแนะ (feedback) เกี่ยวกับการฝึกอบรมที่ได้รับ

สิ่งที่ต้องทำ: มีการประเมินผลจากพนักงานภายหลังการอบรม และนำผลที่ได้จากการประเมินไปวิเคราะห์ และสรุปผล

หลักฐาน: 1) แบบประเมินความคิดเห็นจากพนักงานต่อการอบรม

สภาพบังคับ: ไม่มีกฎหมายกำหนด

แบบประเมินความคิดเห็นจากพนักงานต่อการอบรม (Training Feedback Form)

หัวข้อ: การประเมินความพึงพอใจและข้อเสนอแนะต่อการฝึกอบรมคุ้มครองข้อมูลส่วนบุคคล

ชื่อผู้ประเมิน: _____

ตำแหน่ง: _____

วันที่อบรม: _____

ส่วนที่ 1: ความพึงพอใจต่อนโยบายการอบรม

โปรดให้คะแนนความพึงพอใจในแต่ละหัวข้อโดยใช้คะแนน 1 - 5

(1 = น้อยที่สุด, 5 = มากที่สุด)

หัวข้อ	1	2	3	4	5
1. ความชัดเจนของเนื้อหา					
2. ความเหมาะสมของเนื้อหา					
3. ความรู้ที่ได้รับเป็นประโยชน์					
4. ความสามารถของวิทยากร					
5. การจัดการและอำนวยความสะดวก					

ส่วนที่ 2: ความคิดเห็นและข้อเสนอแนะ

1. คุณมีความคิดเห็นอย่างไรเกี่ยวกับการอบรมครั้งนี้?

2. ส่วนใดของการอบรมที่คุณคิดว่าควรปรับปรุง?

3. คุณต้องการให้มีหัวข้อการอบรมเพิ่มเติมในเรื่องใด?

4. ข้อเสนอแนะอื่น ๆ

ส่วนที่ 3: ความคิดเห็นเพิ่มเติม (ถ้ามี)

หมายเหตุ: แบบประเมินนี้จะช่วยให้องค์กรนำไปพัฒนาคุณภาพการฝึกอบรมในอนาคตให้ดียิ่งขึ้น

3.5.1 มีหลักฐานเพื่อแสดงว่าองค์กรมีการสื่อสารเพื่อสร้างความตระหนักแก่พนักงานที่เกี่ยวข้องกับการคุ้มครองและการกำกับดูแลข้อมูลส่วนบุคคล เช่น ผ่านช่องทางอีเมล การประชุมทีม โพสต์เตอร์ คู่มือ หรือทำเป็นบล็อกให้ความรู้

สิ่งที่ต้องทำ: มีการจัดให้มีการสื่อสารผ่านช่องทางต่าง ๆ ภายในองค์กรเพื่อสร้างความตระหนักในเรื่องการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย ช่องทางอีเมล การประชุมทีม โพสต์เตอร์ คู่มือ บล็อก ให้ความรู้

หลักฐาน: 1) ช่องทางการสื่อสารในรูปแบบต่าง ๆ ภายในองค์กรเพื่อสร้างความตระหนักในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: ไม่มีกฎหมายกำหนด

หลักฐานช่องทางการสื่อสารเพื่อสร้างความตระหนักเรื่องการคุ้มครองข้อมูลส่วนบุคคล

1) ตัวอย่างอีเมลแจ้งข่าวสารและให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

- อีเมลข่าวสารส่งให้พนักงานทุกคนเป็นประจำทุกเดือน
- เนื้อหาเกี่ยวกับข้อกำหนดสำคัญ ตัวอย่างเหตุการณ์ และแนวทางปฏิบัติที่ถูกต้อง

2) รายงานการประชุมทีมที่มีการพูดคุยและเน้นย้ำเรื่องการคุ้มครองข้อมูลส่วนบุคคล

- บันทึกการประชุมพร้อมหัวข้อที่เกี่ยวข้อง เช่น การแจ้งเตือนนโยบายใหม่ การเตรียมอบรม เป็นต้น

3) ภาพโปสเตอร์รณรงค์สร้างความตระหนักในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

- โปสเตอร์ติดตามพื้นที่ทำงาน เช่น ห้องพักรับรอง ห้องประชุม

4) ตัวอย่างคู่มือหรือเอกสารให้ความรู้เรื่องการคุ้มครองข้อมูลส่วนบุคคล

- คู่มือแจกจ่ายในรูปแบบอิเล็กทรอนิกส์หรือเล่มหนังสือที่พนักงานสามารถเข้าถึงได้ง่าย

5) บทความหรือบล็อกให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เผยแพร่ในอินเทอร์เน็ตขององค์กร

- ลิงก์บทความและจำนวนผู้เข้าชม

1) ตัวอย่างอีเมลแจ้งข่าวสารและให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

หัวข้อ: การรณรงค์สร้างความตระหนักเรื่องการคุ้มครองข้อมูลส่วนบุคคล

เนื้อหา:

เรียน ทีมงานทุกท่าน

เนื่องจากความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ทางองค์กรจึงขอแจ้งให้ทุกท่านทราบถึงแนวทางและนโยบายใหม่เกี่ยวกับการจัดการข้อมูลส่วนบุคคลอย่างปลอดภัย โปรดศึกษาและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล สามารถดาวน์โหลดคู่มือฉบับเต็มได้ที่ [ลิงก์คู่มือ]

ขอบคุณครับ/ค่ะ

ฝ่ายบริหารความเสี่ยงและคุ้มครองข้อมูล

2) รายงานการประชุมที่มีการพูดคุยและเน้นย้ำเรื่องการคุ้มครองข้อมูลส่วนบุคคล

วันที่ประชุม: 15 มีนาคม 2568

หัวข้อการประชุม: การเตรียมความพร้อมด้านการคุ้มครองข้อมูลส่วนบุคคล

เนื้อหา:

- แจ้งนโยบายการปฏิบัติงานเกี่ยวกับ PDPA
- แผนการฝึกอบรมและกิจกรรมสร้างความตระหนัก
- มอบหมายหน้าที่การติดตามผลและรายงานผล
- พูดคุยปัญหาและข้อเสนอแนะจากทีมงาน

ผู้เข้าร่วม: ฝ่ายบริหาร ฝ่ายไอที ฝ่ายบุคคล

ลงชื่อ:

(ประธานการประชุม)

3) ภาพโปสเตอร์ณรงค์สร้างความตระหนักในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

ข้อความบนโปสเตอร์:

"คุ้มครองข้อมูลส่วนบุคคล คือความรับผิดชอบของเราอย่าปล่อยให้ข้อมูลของคุณรั่วไหล!"

ภาพประกอบ: รูปกุญแจล็อกข้อมูล และสัญลักษณ์ PDPA

สถานที่ติดตั้ง: ห้องพนักงาน, บริเวณทางเข้าอาคาร, ห้องประชุม

4) ตัวอย่างคู่มือหรือเอกสารให้ความรู้เรื่องการคุ้มครองข้อมูลส่วนบุคคล

ชื่อเอกสาร: คู่มือการปฏิบัติงานเพื่อการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

สารบัญ:

- ความหมายของข้อมูลส่วนบุคคล
- หลักการและแนวทางปฏิบัติตาม PDPA
- สิทธิของเจ้าของข้อมูล
- วิธีการป้องกันและจัดการข้อมูลอย่างปลอดภัย
- ตัวอย่างกรณีศึกษา

รูปแบบ: ไฟล์ PDF ส่งผ่านอีเมลและเก็บไว้ในระบบอินทราเน็ตขององค์กร

5) บทความหรือบล็อกให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

หัวข้อบทความ: “ทำความเข้าใจ PDPA: สิทธิและหน้าที่ของพนักงานในยุคดิจิทัล”

เนื้อหา:

- บทนำเกี่ยวกับ PDPA
- ข้อควรระวังในการจัดการข้อมูลส่วนบุคคล
- ตัวอย่างการละเมิดข้อมูลและบทลงโทษ
- แนวทางการปฏิบัติในชีวิตประจำวัน

จำนวนผู้อ่าน: 350 คนในเดือนที่ผ่านมา

เผยแพร่บน: อินทราเน็ตองค์กร (Intranet)

3.5.2 มีการจัดเตรียมเอกสารหรือเนื้อหาที่พนักงานสามารถเข้าถึงได้ง่ายที่เกี่ยวข้องกับการคุ้มครองและการกำกับดูแลข้อมูลส่วนบุคคล รวมทั้งสามารถค้นหาหน่วยงานหรือผู้รับผิดชอบที่สามารถติดต่อได้ ถ้ามีคำถามใด ๆ ที่เกี่ยวกับการคุ้มครองและการกำกับดูแลข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: มีการจัดทำเอกสารหรือเนื้อหาที่พนักงานสามารถเข้าถึงได้ง่าย โดยแยกเป็นแต่ละแผนก หรือ มีวิดีโอ เพื่อสาธิตสถานการณ์ต่าง ๆ ที่อาจเกิดขึ้นในการปฏิบัติงาน

หลักฐาน: 1) คู่มือเกี่ยวกับการคุ้มครองและการกำกับดูแลข้อมูลส่วนบุคคลขององค์กร โดยอาจแยกเป็น แผนกและมีวิดีโอสาธิตการปฏิบัติงานในสถานการณ์ต่าง ๆ

สภาพบังคับ: ไม่มีกฎหมายกำหนด

คู่มือการคุ้มครองและกำกับดูแลข้อมูลส่วนบุคคลสำหรับฝ่ายทรัพยากรบุคคล (Human Resources Department)

บทนำ

การคุ้มครองข้อมูลส่วนบุคคลถือเป็นภารกิจสำคัญขององค์กรในยุคดิจิทัล โดยเฉพาะฝ่ายทรัพยากรบุคคล ซึ่งมีหน้าที่ดูแลและประมวลผลข้อมูลที่มีความละเอียดอ่อนของพนักงานตั้งแต่ขั้นตอนการสรรหา การจ้างงาน การประเมินผล การให้สิทธิประโยชน์ จนถึงการพัฒนาจากการทำงาน คู่มือนี้จัดทำขึ้นเพื่อเป็นแนวทางให้เจ้าหน้าที่ฝ่ายบุคคลสามารถปฏิบัติงานได้อย่างถูกต้องตามหลักกฎหมาย โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และแนวทางปฏิบัติที่เกี่ยวข้อง

หมวดที่ 1: หลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

1.1 ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลที่สามารถระบุตัวบุคคลได้ ไม่ว่าจะทางตรงหรือทางอ้อม เช่น ชื่อ-สกุล หมายเลขประจำตัวประชาชน หมายเลขโทรศัพท์ อีเมล ที่อยู่ รูปถ่าย ประวัติการทำงาน

1.2 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data)

ข้อมูลด้านสุขภาพ ประวัติอาชญากรรม ศาสนา เชื้อชาติ ความเห็นทางการเมือง พฤติกรรมทางเพศ ข้อมูลชีวมิติ (biometric)

1.3 หลักการพื้นฐาน 7 ประการ (Derived from GDPR and PDPA)

- ความชอบด้วยกฎหมาย (Lawfulness)
- ความเป็นธรรม (Fairness)
- ความโปร่งใส (Transparency)
- การจำกัดวัตถุประสงค์ (Purpose Limitation)
- การลดปริมาณข้อมูล (Data Minimization)
- ความถูกต้อง (Accuracy)
- การจัดเก็บอย่างปลอดภัย (Storage Limitation)

หมวดที่ 2: ขอบเขตและประเภทของข้อมูลที่ฝ่ายบุคคลดูแล

2.1 ขั้นตอนการสรรหาและคัดเลือก

- ข้อมูลประวัติผู้สมัคร
- ประวัติการศึกษา
- ประวัติการทำงาน
- ผลการสัมภาษณ์
- ผลการตรวจสอบสุขภาพก่อนเริ่มงาน

2.2 ระหว่างการจ้างงาน

- ข้อมูลการทำงาน รายงานการประเมินผล
- ข้อมูลการลางาน/การขาดงาน
- ข้อมูลการเข้าร่วมกิจกรรมองค์กร
- ข้อมูลประกันสุขภาพและสิทธิประโยชน์
- ภาพจากกล้องวงจรปิด (หากมี)

2.3 หลังพ้นสภาพการจ้าง

- เอกสารรับรองการผ่านงาน
- บันทึกการพ้นสภาพและเหตุผล

หมวดที่ 3: ฐานทางกฎหมายในการประมวลผลข้อมูล (Legal Basis)

3.1 การประมวลผลตามสัญญา (Contractual necessity)

3.2 การปฏิบัติตามกฎหมาย (Legal obligation) 3.3 ความยินยอม (Consent) 3.4 ประโยชน์โดยชอบธรรมขององค์กร (Legitimate interest)

หมวดที่ 4: มาตรการควบคุมภายใน

4.1 การจำกัดสิทธิ์ในการเข้าถึงข้อมูล (Access Control)

- กำหนดบทบาทและสิทธิ์การเข้าถึงข้อมูลในระบบ HRMS
- ใช้รหัสผ่าน และระบบสองชั้น (2FA)

4.2 การเก็บรักษาเอกสารและข้อมูลอิเล็กทรอนิกส์

- การจัดเก็บเอกสารสำคัญในพื้นที่ปลอดภัย มีการล็อกตู้
- การกำหนดระยะเวลาการเก็บรักษา และการทำลายข้อมูลตามรอบเวลา

4.3 การจัดทำบันทึกกิจกรรมการประมวลผลข้อมูล (Record of Processing Activities)

4.4 การรายงานเหตุการณ์ข้อมูลรั่วไหล (Data Breach Notification)

ขั้นตอนการแจ้งภายในองค์กร และแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง

หมวดที่ 5: การให้สิทธิของเจ้าของข้อมูล

5.1 สิทธิในการเข้าถึงข้อมูล (Right of access)

5.2 สิทธิในการแก้ไขข้อมูล (Right to rectification)

5.3 สิทธิในการลบข้อมูล (Right to erasure)

5.4 สิทธิในการคัดค้านการประมวลผล (Right to object)

5.5 สิทธิในการ ย้ายข้อมูล (Right to data portability)

แนวปฏิบัติ

ฝ่ายบุคคลต้องจัดช่องทาง เช่น แบบฟอร์มคำร้อง หรือระบบออนไลน์ เพื่อให้พนักงานใช้สิทธิตามกฎหมายได้โดยง่าย พร้อมจัดระบบตอบกลับภายในระยะเวลาที่กำหนด

หมวดที่ 6: การฝึกอบรมและการสร้างความตระหนัก

6.1 จัดการฝึกอบรมตามบทบาทหน้าที่ของพนักงาน HR

6.2 จัดอบรมเบื้องต้น (onboarding) ด้าน PDPA สำหรับพนักงานใหม่

6.3 มีการทดสอบหลังอบรม พร้อมบันทึกผลและติดตามผู้ไม่ผ่าน

6.4 จัดเก็บลายเซ็นเข้าร่วมการอบรม รายงานผล และข้อเสนอแนะ

6.5 มีการสื่อสารภายในเพื่อสร้างความตระหนัก เช่น อีเมล पोสเตอร์ อินทราเน็ต คู่มือ ฯลฯ

หมวดที่ 7: การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

7.1 ฝ่ายบุคคลต้องตรวจสอบว่าการโอนข้อมูล เช่น การใช้บริการ HR Cloud อยู่ภายใต้มาตรฐานความปลอดภัย

7.2 หากโอนไปยังประเทศที่ไม่มีระดับการคุ้มครองเพียงพอ ต้องมีมาตรการป้องกันเพิ่มเติม เช่น SCCs

7.3 แจ้งให้พนักงานทราบและขอความยินยอมหากจำเป็น

หมวดที่ 8: บทบาทของเจ้าหน้าที่คุ้มครองข้อมูล (DPO)

8.1 ฝ่ายบุคคลต้องสามารถประสานงานกับ DPO ในกรณีมีคำร้องเรียนหรือการรั่วไหลของข้อมูล

8.2 จัดทำบันทึกความร่วมมือหรือช่องทางติดต่อกับ DPO อย่างชัดเจน

หมวดที่ 9: แนวทางในการตรวจสอบและการประเมินความเสี่ยง

9.1 ฝ่ายบุคคลต้องเข้าร่วมกิจกรรมการตรวจสอบความเสี่ยงด้านข้อมูลอย่างสม่ำเสมอ

9.2 ประเมิน DPIA สำหรับกิจกรรมใหม่ เช่น การเก็บข้อมูลชีวมิติ หรือการใช้ AI ในการสรรหา

หมวดที่ 10: ภาคผนวก

10.1 ตัวอย่างฟอร์มการใช้สิทธิของเจ้าของข้อมูล

10.2 เช็กलिस्टการฝึกอบรมพนักงาน

10.3 แนวทางจัดเก็บเอกสารในระบบอิเล็กทรอนิกส์

10.4 แบบฟอร์มประเมินความเสี่ยง DPIA

10.5 คำอธิบายคำศัพท์ทางกฎหมายที่ใช้ในคู่มือนี้

หมวดที่ 10: ภาคผนวก

10.1 ตัวอย่างฟอร์มการใช้สิทธิของเจ้าของข้อมูล

แบบฟอร์มคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ชื่อ-นามสกุล:

รหัสพนักงาน/รหัสสมาชิก:

อีเมล:

เบอร์โทรศัพท์ที่ติดต่อได้:

ประเภทสิทธิที่ต้องการใช้: ☐ ขอเข้าถึงข้อมูล ☐ ขอให้แก้ไขข้อมูลให้ถูกต้อง ☐ ขอให้ลบข้อมูล ☐

ขอให้ระงับการใช้ข้อมูล ☐ ขอให้โอนย้ายข้อมูล ☐ คัดค้านการประมวลผลข้อมูล ☐ ถอนความยินยอมในการประมวลผลข้อมูล

รายละเอียดคำร้อง (โปรดระบุเพิ่มเติมถ้ามี):

.....

วิธีการที่ต้องการรับการตอบกลับ: ☐ อีเมล ☐ โทรศัพท์ ☐ ทางไปรษณีย์

ลงชื่อ ผู้ยื่นคำร้อง วันที่/...../.....

เจ้าหน้าที่ผู้รับเรื่อง: วันที่รับเรื่อง:/...../.....

10.2 เช็กลิสต์การฝึกอบรมพนักงาน

ลำดับ	ชื่อ พนักงาน	ตำแหน่ง	วันที่ อบรม	หัวข้อ อบรม	ผลการทดสอบ หลังอบรม	ข้อเสนอแนะ	ลายเซ็นผู้ เข้าอบรม

10.3 แบบฟอร์มประเมินความเสี่ยง DPIA (Data Protection Impact Assessment)

1. รายละเอียดโครงการ/กิจกรรม ชื่อโครงการ/กิจกรรม: ผู้รับผิดชอบ:
..... วัตถุประสงค์:

2. ประเภทของข้อมูลส่วนบุคคลที่ประมวลผล ☐ ทั่วไป เช่น ชื่อ ที่อยู่ อีเมล ☐ อ่อนไหว เช่น สุขภาพ
ชีวมิติ ความเชื่อ ฯลฯ

3. วิธีการเก็บและประมวลผลข้อมูล ☐ เอกสาร ☐ อิเล็กทรอนิกส์ ☐ ระบบอัตโนมัติ ☐ ผ่านบุคคลที่
สาม

4. ระยะเวลาการจัดเก็บ: 5. การแบ่งปันข้อมูล/โอนข้อมูลให้

บุคคลภายนอก: ☐ ไม่มี ☐ มี (ระบุชื่อผู้รับข้อมูล):

6. การโอนข้อมูลไปต่างประเทศ: ☐ ไม่มี ☐ มี (ประเทศ):

7. ความเสี่ยงที่อาจเกิดขึ้น

.....

8. มาตรการควบคุมที่นำมาใช้ ☐ การเข้ารหัสข้อมูล ☐ การควบคุมสิทธิ์การเข้าถึง ☐ การตรวจสอบ
การเข้าถึงข้อมูล (log) ☐ การทำสัญญากับผู้ประมวลผลข้อมูลภายนอก ☐ อื่น ๆ

.....

9. ความเห็นจาก DPO (ถ้ามี): ลงชื่อ

..... วันที่...../...../.....

10.4 คำอธิบายศัพท์ทางกฎหมาย

- เจ้าของข้อมูล (Data Subject): บุคคลธรรมดาที่ข้อมูลนั้นสามารถระบุถึงตัวเขาได้
- ข้อมูลส่วนบุคคล (Personal Data): ข้อมูลที่สามารถระบุถึงตัวบุคคลได้ ไม่ว่าจะโดยทางตรงหรือทางอ้อม
- ข้อมูลอ่อนไหว (Sensitive Personal Data): ข้อมูลที่เกี่ยวข้องกับสุขภาพ ความเชื่อ ศาสนา ความคิดเห็น
- ทางทางเมือง ฯลฯ

- **ผู้ควบคุมข้อมูล (Data Controller):** บุคคล/หน่วยงานที่มีอำนาจในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูล
- **ผู้ประมวลผลข้อมูล (Data Processor):** บุคคล/หน่วยงานที่ประมวลผลข้อมูลตามคำสั่งของผู้ควบคุมข้อมูล
- **ความยินยอม (Consent):** การแสดงเจตนาโดยชัดแจ้งของเจ้าของข้อมูลในการอนุญาตให้ประมวลผลข้อมูล
- **การประเมินผลกระทบ (DPIA):** กระบวนการประเมินความเสี่ยงจากการประมวลผลข้อมูลต่อสิทธิของเจ้าของข้อมูล
- **ข้อมูล**
- **DPO (Data Protection Officer):** เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่องค์กรแต่งตั้ง
- **Data Breach (การรั่วไหลของข้อมูล):** เหตุการณ์ที่ข้อมูลถูกเข้าถึง ดัดแปลง หรือนำไปใช้โดยไม่ได้รับอนุญาต

คู่มือการคุ้มครองและกำกับดูแลข้อมูลส่วนบุคคลสำหรับฝ่ายทะเบียนสมาชิก (Membership Registration Department)

บทนำ

ฝ่ายทะเบียนสมาชิกมีบทบาทสำคัญในการจัดเก็บ ประมวลผล และดูแลข้อมูลส่วนบุคคลของสมาชิก ไม่ว่าจะเป็นสมาชิกทั่วไป สมาชิกองค์กร หรือสมาชิกที่ได้รับสิทธิพิเศษต่าง ๆ คู่มือนี้จัดทำขึ้นเพื่อให้เจ้าหน้าที่ปฏิบัติงานตามหลักเกณฑ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และแนวปฏิบัติสากลที่เกี่ยวข้อง เพื่อให้เกิดความมั่นใจในความปลอดภัยและความเป็นส่วนตัวของข้อมูลสมาชิก

หมวดที่ 1: ข้อมูลส่วนบุคคลที่ฝ่ายทะเบียนสมาชิกเกี่ยวข้อง

1.1 ประเภทของข้อมูลที่จัดเก็บ

- ชื่อ-นามสกุล
- เลขบัตรประชาชน / หนังสือเดินทาง
- วันเดือนปีเกิด
- ที่อยู่ / หมายเลขโทรศัพท์ / อีเมล

- รูปถ่าย (บนบัตรสมาชิก)
- ข้อมูลการเป็นสมาชิก เช่น วันที่เริ่ม/หมดอายุ, สิทธิประโยชน์
- ประวัติการใช้สิทธิ / การเข้าร่วมกิจกรรม / คะแนนสะสม (ถ้ามี)

1.2 ข้อมูลอ่อนไหว (Sensitive Personal Data)

- ข้อมูลสุขภาพหรือความพิการ (หากมีสิทธิพิเศษรองรับ)
- ข้อมูลชีวมิติ เช่น ลายนิ้วมือ ใบหน้า (กรณีใช้กับระบบเข้าถึงสถานที่/บริการ)

หมวดที่ 2: วัตถุประสงค์ในการประมวลผลข้อมูล

- 2.1 เพื่อจัดทำบัตรสมาชิกและลงทะเบียน
- 2.2 เพื่อให้บริการที่เกี่ยวข้องกับสถานภาพสมาชิก
- 2.3 เพื่อจัดส่งข่าวสาร กิจกรรม และสิทธิประโยชน์
- 2.4 เพื่อการวิเคราะห์และปรับปรุงบริการ
- 2.5 เพื่อปฏิบัติตามกฎหมายหรือระเบียบข้อบังคับขององค์กร

หมวดที่ 3: ฐานทางกฎหมายในการประมวลผลข้อมูล

- 3.1 ความยินยอม (Consent)
 - สำหรับข้อมูลอ่อนไหว หรือการส่งข่าวสารการตลาด
- 3.2 การปฏิบัติตามสัญญา (Contractual Necessity)
 - การออกบัตรสมาชิก การต่ออายุ การมอบสิทธิพิเศษ
- 3.3 ภาระหน้าที่ตามกฎหมาย (Legal Obligation)
 - การจัดเก็บข้อมูลภาษี หรือการตรวจสอบจากหน่วยงานราชการ

หมวดที่ 4: สิทธิของเจ้าของข้อมูล

- 4.1 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล
- 4.2 สิทธิในการขอแก้ไขข้อมูล
- 4.3 สิทธิในการลบหรือขอให้ระงับการใช้ข้อมูล
- 4.4 สิทธิในการคัดค้านการประมวลผล
- 4.5 สิทธิในการเพิกถอนความยินยอม

แนวปฏิบัติ: ฝ่ายทะเบียนสมาชิกต้องมีแบบฟอร์ม หรือระบบร้องขอสิทธิของเจ้าของข้อมูล พร้อมคู่มือหรือคำแนะนำการยื่นคำขอและระยะเวลาตอบกลับ

หมวดที่ 5: มาตรการรักษาความปลอดภัยของข้อมูล

- 5.1 การจำกัดสิทธิ์เข้าถึงระบบข้อมูลสมาชิก (Access Control)
- 5.2 การเก็บรักษาเอกสารทางกายภาพ (จัดเก็บในพื้นที่ปลอดภัย มีการล็อก)
- 5.3 การใช้รหัสผ่านและระบบยืนยันตัวตน 2 ชั้นสำหรับระบบสารสนเทศ
- 5.4 การเข้ารหัสข้อมูลสำคัญ และการสำรองข้อมูลอย่างสม่ำเสมอ
- 5.5 การทำลายข้อมูลเมื่อพ้นระยะเวลาการเก็บรักษา (Data Retention Policy)

หมวดที่ 6: การจัดการเหตุการณ์ข้อมูลรั่วไหล (Data Breach)

- 6.1 การตรวจพบและประเมินผลกระทบ
- 6.2 การแจ้ง DPO และผู้บริหารทันทีที่เกิดเหตุการณ์
- 6.3 การแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง
- 6.4 การแจ้งเจ้าของข้อมูลหากความเสี่ยงสูง
- 6.5 การบันทึกเหตุการณ์และดำเนินมาตรการป้องกันในอนาคต

หมวดที่ 7: การฝึกอบรมและการสร้างความตระหนักรู้

- 7.1 การอบรมเบื้องต้นสำหรับพนักงานใหม่
- 7.2 การอบรมประจำปีเกี่ยวกับ PDPA และแนวปฏิบัติในการจัดการข้อมูลสมาชิก
- 7.3 การทดสอบหลังอบรมและเก็บหลักฐานการเข้าร่วม

หมวดที่ 8: การโอนข้อมูลไปต่างประเทศ

- 8.1 ตรวจสอบบริการ Cloud หรือซอฟต์แวร์ CRM ที่ใช้ว่าโฮสต์อยู่ในประเทศใด
- 8.2 หากอยู่นอกประเทศ ต้องประเมินระดับการคุ้มครอง และใช้มาตรการเสริม เช่น SCCs
- 8.3 ขอความยินยอมจากเจ้าของข้อมูลหากจำเป็น

หมวดที่ 9: การจัดทำ DPIA และบันทึกกิจกรรมการประมวลผล

- 9.1 การประเมิน DPIA สำหรับกิจกรรมใหม่ เช่น การเปิดระบบสมัครสมาชิกออนไลน์
- 9.2 การจัดทำบันทึกกิจกรรมการประมวลผล (RoPA) สำหรับระบบทะเบียนสมาชิกทั้งหมด

หมวดที่ 10: ภาคผนวก

- 10.1 ตัวอย่างฟอร์มขอใช้สิทธิของเจ้าของข้อมูล
- 10.2 เช็คลิสต์ฝึกอบรมพนักงานฝ่ายทะเบียนสมาชิก
- 10.3 แบบฟอร์ม DPIA สำหรับระบบสมัครสมาชิก
- 10.4 คำอธิบายศัพท์สำคัญทางกฎหมาย

บทที่ 5

สิทธิของเจ้าของข้อมูลส่วนบุคคล

การเคารพสิทธิของเจ้าของข้อมูลส่วนบุคคลถือเป็นหัวใจสำคัญของการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และเป็นปัจจัยสำคัญในการสร้างความเชื่อมั่นระหว่างองค์กรกับผู้เกี่ยวข้อง การตระหนักถึงสิทธิของเจ้าของข้อมูลช่วยให้องค์กรสามารถจัดการข้อมูลส่วนบุคคลได้อย่างโปร่งใส ถูกต้อง และเหมาะสม ตลอดจนสามารถตอบสนองต่อคำขอของเจ้าของข้อมูลได้อย่างรวดเร็วและเป็นธรรม สิทธิของเจ้าของข้อมูลครอบคลุมหลายมิติ ได้แก่ สิทธิในการเข้าถึงข้อมูล สิทธิในการขอแก้ไขข้อมูล สิทธิในการขอให้ลบหรือทำลายข้อมูล สิทธิในการระงับการประมวลผลข้อมูล สิทธิในการคัดค้านการประมวลผล และสิทธิในการโอนย้ายข้อมูล การรับรองสิทธิเหล่านี้ไม่เพียงแต่สอดคล้องกับข้อกำหนดทางกฎหมาย แต่ยังช่วยส่งเสริมวัฒนธรรมองค์กรที่เคารพความเป็นส่วนตัวและความปลอดภัยของข้อมูล

เพื่อให้การปฏิบัติตามสิทธิของเจ้าของข้อมูลเป็นไปอย่างมีประสิทธิภาพ องค์กรจำเป็นต้องมีกระบวนการและเอกสารที่ชัดเจน ครอบคลุมทั้งการรับคำขอ การตรวจสอบและยืนยันตัวตน การดำเนินการตามคำขอ และการจัดเก็บหลักฐานการปฏิบัติ นอกจากนี้ การอบรมบุคลากรที่เกี่ยวข้อง การจัดทำคู่มือแนวปฏิบัติ และการสื่อสารข้อมูลเกี่ยวกับสิทธิของเจ้าของข้อมูลไปยังผู้เกี่ยวข้องทุกกลุ่ม เป็นสิ่งจำเป็นเพื่อให้เจ้าของข้อมูลสามารถใช้สิทธิของตนได้อย่างแท้จริงและเกิดประสิทธิผล

การจัดทำเอกสารและบันทึกที่ชัดเจนเกี่ยวกับการปฏิบัติตามสิทธิของเจ้าของข้อมูล ไม่เพียงเป็นเครื่องมือสำคัญสำหรับการตรวจสอบภายในและภายนอกองค์กร แต่ยังเป็นหลักฐานสำคัญที่แสดงให้เห็นถึงความมุ่งมั่นขององค์กรในการเคารพสิทธิของเจ้าของข้อมูลและปฏิบัติตาม PDPA อย่างครบถ้วน

สิทธิของเจ้าของข้อมูลส่วนบุคคลถือเป็นหัวใจสำคัญของการคุ้มครองข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) การปฏิบัติตามสิทธิของเจ้าของข้อมูลไม่เพียงแต่เป็นข้อกำหนดทางกฎหมาย แต่ยังสะท้อนถึงความรับผิดชอบขององค์กรในการบริหารจัดการข้อมูลอย่างโปร่งใส ถูกต้อง และเหมาะสม การสร้างกระบวนการที่ชัดเจนสำหรับการใช้สิทธิของเจ้าของข้อมูล เช่น สิทธิในการเข้าถึง แก้ไข ลบ ระงับการประมวลผล การคัดค้าน หรือโอนย้ายข้อมูล เป็นสิ่งจำเป็นเพื่อให้เจ้าของข้อมูลสามารถใช้สิทธิของตนได้อย่างแท้จริง องค์กรจำเป็นต้องจัดทำเอกสารและระบบสนับสนุนที่ครอบคลุม ตั้งแต่การสื่อสารสิทธิของเจ้าของข้อมูล การจัดตั้งช่องทางรับคำขอ การตรวจสอบและยืนยันตัวตน การดำเนินการตามคำขอ รวมถึงการสื่อสารผลและการบันทึกหลักฐานการปฏิบัติ ทั้งนี้เพื่อให้สามารถตรวจสอบ Compliance ได้อย่างชัดเจน นอกจากนี้ การอบรมบุคลากรที่เกี่ยวข้องและการสร้างความตระหนักรู้เกี่ยวกับสิทธิของเจ้าของข้อมูลก็เป็นกลไกสำคัญที่ช่วยให้แน่ใจว่าบุคลากรทุกระดับมีความเข้าใจและสามารถปฏิบัติได้อย่างถูกต้อง

ตารางด้านล่างสรุปหัวข้อสำคัญของการจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล พร้อมแนวทางปฏิบัติ เอกสาร/หลักฐานที่ต้องมี และเกณฑ์การให้คะแนน เพื่อให้มั่นใจว่าการดำเนินการขององค์กรสอดคล้อง ครบถ้วนกับ PDPA และสามารถตรวจสอบได้อย่างชัดเจน

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
4.1 การให้ข้อมูลเกี่ยวกับสิทธิของเจ้าของข้อมูล	แจ้งให้เจ้าของข้อมูลทราบถึงสิทธิของตน เช่น สิทธิในการเข้าถึง แก้ไข ลบ ระงับคัดค้าน และโอนย้ายข้อมูล	Privacy Notice, เอกสารแจ้งสิทธิ, เว็บไซต์องค์กร, อีเมลประกาศ	มีการแจ้งสิทธิครบถ้วน ชัดเจน และเข้าถึงได้ทุกกลุ่มผู้เกี่ยวข้อง
4.2 การจัดตั้งช่องทางรับคำขอใช้สิทธิ	จัดทำช่องทางรับคำขอสิทธิที่สะดวก เช่น แบบฟอร์มออนไลน์ อีเมล หรือช่องทางติดต่อเจ้าหน้าที่	แบบฟอร์มคำขอ สิทธิ (Data Subject Request Form), บันทึกการรับคำขอ	มีช่องทางชัดเจน สามารถใช้ได้จริง และตรวจสอบย้อนหลังได้
4.3 การตรวจสอบและยืนยันตัวตน	ตรวจสอบตัวตนเจ้าของข้อมูลก่อนดำเนินการตามคำขอ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	แบบฟอร์ม/กระบวนการตรวจสอบตัวตน, บันทึกการยืนยันตัวตน	มีขั้นตอนตรวจสอบตัวตนอย่างปลอดภัยและสอดคล้องกับ PDPA
4.4 การดำเนินการตามคำขอของเจ้าของข้อมูล	ปฏิบัติตามคำขอ เช่น ให้เข้าถึง แก้ไข ลบ ระงับ หรือโอนย้ายข้อมูลภายในระยะเวลาที่กฎหมายกำหนด	บันทึกคำขอ รายงานการดำเนินการ, e-Log ระบบการจัดการคำขอ	มีหลักฐานการดำเนินการครบถ้วนและภายในเวลาที่กำหนด
4.5 การสื่อสารผลการดำเนินการ	แจ้งผลการดำเนินการให้เจ้าของข้อมูลทราบอย่างชัดเจน	จดหมาย/อีเมลแจ้งผลการดำเนินการ, รายงาน Internal Tracking	แจ้งผลครบถ้วน ชัดเจน และสามารถตรวจสอบได้
4.6 การบันทึกและจัดเก็บหลักฐานการปฏิบัติ	เก็บบันทึกคำขอ สิทธิ และผลการดำเนินการอย่างเป็นระบบเพื่อการตรวจสอบ Compliance	ระบบบันทึกคำขอ, รายงาน Audit, e-Log, แบบฟอร์มจัดเก็บ	มีระบบจัดเก็บครบถ้วน ตรวจสอบย้อนหลังได้ และเป็นปัจจุบัน

4.7 การทบทวนและปรับปรุงกระบวนการ	ปรับปรุงกระบวนการและเอกสารที่เกี่ยวข้องกับการใช้สิทธิของเจ้าของข้อมูลอย่างต่อเนื่อง	รายงาน Version Control, บันทึกการประชุมปรับปรุงกระบวนการ	มีหลักฐานการปรับปรุงต่อเนื่อง และสอดคล้องกับกฎหมายหรือแนวทางใหม่
4.8 การอบรมและสร้างความตระหนักรู้	อบรมบุคลากรเกี่ยวกับสิทธิของเจ้าของข้อมูล วิธีรับคำขอ และกระบวนการปฏิบัติ	แผนอบรม, สไลด์, แบบสอบถามประเมินผล, Attendance Sheet	บุคลากรทุกระดับได้รับการอบรม มีหลักฐานชัดเจน และสามารถใช้ความรู้ได้จริง

การจัดทำเอกสารตามเกณฑ์

4.2.1 พนักงานได้รับการฝึกอบรมเฉพาะทางเพื่อจัดการคำขอ รวมถึงการฝึกอบรมเพิ่มเติมอย่างสม่ำเสมอ (refresher training)

สิ่งที่ต้องทำ: มีการจัดอบรมเฉพาะทางให้พนักงานผู้มีหน้าที่ในการดำเนินการต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

หลักฐาน: 1) เอกสารแสดงบุคลากรหรือกลุ่มงานที่ทำงานในส่วนดำเนินการต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (7)

เอกสารแสดงการฝึกอบรมเฉพาะทางแก่พนักงานผู้ดำเนินการต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ชื่อองค์กร: [ชื่อองค์กรของคุณ]

หน่วยงานที่รับผิดชอบ: [ระบุหน่วยงาน เช่น ฝ่ายทรัพยากรบุคคล / ฝ่ายทะเบียนนักศึกษา / ฝ่ายบัตรสมาชิก]

วันที่จัดทำเอกสาร: [ระบุวันที่]

1. รายชื่อบุคลากรผู้มีหน้าที่ดำเนินการต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ลำดับ	ชื่อ-สกุล	ตำแหน่ง	หน่วยงาน	อีเมล	หมายเหตุ
1	นายสุรศักดิ์ รัตนพงศ์	เจ้าหน้าที่ทะเบียนนักศึกษา	ฝ่ายทะเบียน	surasak.r@org.ac.th	หัวหน้ากลุ่มงานข้อมูล

2	นางสาวพิมพ์ชนก แสงทอง	เจ้าหน้าที่ HR	ฝ่ายทรัพยากรบุคคล	Pim.hanok.s@org.ac.th	ดูแลสิทธิพนักงาน
3	นายอดิศักดิ์ ศรีโสภ	เจ้าหน้าที่ดูแลระบบสมาชิก	ฝ่ายบัตรสมาชิก	Adisak.s@org.ac.th	รับผิดชอบข้อมูลสมาชิก

2. รายละเอียดการฝึกอบรมเฉพาะทาง

ชื่อหลักสูตร: การจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลอย่างถูกต้องและปลอดภัย

ผู้จัดอบรม: [ชื่อองค์กร เช่น สำนักงาน DPO / แผนกกฎหมายองค์กร / ผู้ให้บริการอบรมภายนอก]

รูปแบบการอบรม: Onsite / Online (Live Webinar) / e-Learning

ระยะเวลาอบรม: 1 วัน (6 ชั่วโมง)

วัน/เวลาอบรม: 20 มีนาคม 2568 เวลา 09.00–16.00 น.

เนื้อหาครอบคลุม:

- ภาพรวมของสิทธิของเจ้าของข้อมูลตาม PDPA
- กระบวนการตอบสนองคำขอ (เช่น ขอเข้าถึง/แก้ไข/ลบ/คัดค้าน/โอนย้ายข้อมูล)
- วิธีการยืนยันตัวตนผู้ร้อง
- การจัดเก็บบันทึกการใช้สิทธิ
- การประสานงานกับเจ้าหน้าที่คุ้มครองข้อมูล (DPO)
- ระยะเวลาและรูปแบบการตอบกลับตามข้อกำหนด
- แนวปฏิบัติเมื่อต้องปฏิเสธคำขอ
- การบริหารความเสี่ยงจากคำขอที่ซับซ้อนหรือประสงค์ร้าย

วิทยากร: นายนพเก้า พัฒนานุกูล (ผู้เชี่ยวชาญด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล)

3. รายชื่อผู้เข้าร่วมอบรมและผลการอบรม

ลำดับ	ชื่อ-สกุล	ผ่านเกณฑ์การอบรม	ข้อเสนอแนะเพิ่มเติม
1	นายสุรศักดิ์ รัตนพงศ์	ผ่าน	ขอเอกสารแนวทางสรุปในรูปภาพประกอบ
2	นางสาวพิมพ์ชนก แสงทอง	ผ่าน	อยากให้มีการฝึกศึกษาจริงมากขึ้น
3	นายอดิศักดิ์ ศรีโสภ	ผ่าน	สนใจอบรมซ้ำใน 6 เดือนข้างหน้า

4. แนวทางการอบรมต่อเนื่อง (Refresher Training)

องค์กรกำหนดให้มีการอบรมซ้ำทุก 12 เดือน เพื่อทบทวนแนวทางการตอบสนองคำขอใช้สิทธิ โดยมีการประเมินกรณีศึกษาใหม่ และอัปเดตการตีความตามคำวินิจฉัยหรือแนวทางปฏิบัติของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

5. แนบเอกสารประกอบ (ถ้ามี)

- Slide การอบรม (PDF)
- คู่มือการตอบคำขอใช้สิทธิ
- แบบทดสอบหลังการอบรม
- แบบประเมินความพึงพอใจจากผู้เข้าอบรม

4.2.2 มีบุคคลหรือคณะทำงานเฉพาะที่มีหน้าที่รับผิดชอบในการจัดการและตอบสนองต่อคำขอใช้สิทธิตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(อาจเป็น DPO หรือกลุ่มงานด้านกฎหมาย หรือกลุ่มงานอื่นที่เหมาะสม เป็นต้น)

สิ่งที่ต้องทำ: จัดให้มีบุคคลหรือคณะทำงานเฉพาะที่มีหน้าที่รับผิดชอบในการจัดการและตอบสนองต่อคำขอใช้สิทธิ

หลักฐาน: 1) แนะนำเกี่ยวกับวิธีการจัดการคำขอใช้สิทธิและการส่งต่อคำขอใช้สิทธิ

สภาพบังคับ: ไม่มีกฎหมายกำหนด

เอกสารแสดงการจัดตั้งคณะทำงานรับผิดชอบการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ชื่อองค์กร: [ชื่อองค์กรของคุณ]

หน่วยงานที่รับผิดชอบ: [ชื่อหน่วยงานที่ดูแลการคุ้มครองข้อมูลส่วนบุคคล เช่น สำนักงาน DPO / ฝ่ายกฎหมาย / คณะทำงาน PDPA]

วันที่จัดทำเอกสาร: [ระบุวันที่]

1. รายชื่อบุคคลหรือคณะทำงานเฉพาะที่รับผิดชอบคำขอใช้สิทธิ

ลำดับ	ชื่อ-สกุล	ตำแหน่ง	หน่วยงาน	บทบาทในกระบวนการ
1	นายเกรียงศักดิ์ อินทรสุข	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	สำนักนโยบายองค์กร	ตรวจสอบคำขอ / วิเคราะห์ความชอบด้วยกฎหมาย

2	น.ส. อรพินท์ ศรีวัฒน์	นักกฎหมาย	ฝ่ายกฎหมาย	ให้คำแนะนำทางกฎหมาย / ประเมินเหตุผลในการอนุมัติ หรือปฏิเสธ
3	นายประวิทย์ สุธรรม	เจ้าหน้าที่ฝ่าย IT Security	ฝ่ายเทคโนโลยีสารสนเทศ	ตรวจสอบระบบและการเข้าถึงข้อมูลส่วนบุคคล
4	น.ส. พิชชาภา พิพัฒน์	เจ้าหน้าที่ข้อมูลสมาชิก	ฝ่ายบัตรสมาชิก	ตรวจสอบฐานข้อมูลสมาชิก / ประสาน DPO
5	นางสาวณัฐกานต์ จันทร์ลอย	เจ้าหน้าที่บุคคล	ฝ่าย HR	ตรวจสอบสิทธิของพนักงาน / ดำเนินการตามคำขอ

2. แนวทางการจัดการและส่งต่อคำขอใช้สิทธิ

2.1 ช่องทางการรับคำขอ

- เว็บไซต์ขององค์กร (แบบฟอร์มออนไลน์)
- อีเมลเฉพาะกิจ: dataprivacy@org.ac.th
- เอกสารยื่นคำขอที่สำนักงานตามแบบฟอร์ม “แบบคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (DPR-01)”

2.2 ขั้นตอนการดำเนินการรับคำขอ

- เจ้าหน้าที่ประจำช่องทางรับคำขอจะตรวจสอบความครบถ้วนของข้อมูล และส่งต่อไปยัง DPO ภายใน 1 วันทำการ

ยืนยันตัวตนผู้ร้องขอ

- DPO ประสานเจ้าหน้าที่ฝ่ายที่เกี่ยวข้องเพื่อยืนยันตัวตนของเจ้าของข้อมูลตามมาตรฐานความปลอดภัย
- หากเป็นคำขอที่สามารถดำเนินการได้ทันที (เช่น แก้ไขข้อมูลผิดพลาด) ให้ฝ่ายที่รับผิดชอบดำเนินการโดยตรง
- หากเป็นคำขอที่ซับซ้อนหรือมีข้อจำกัดตามกฎหมาย ให้ส่งต่อฝ่ายกฎหมายเพื่อวิเคราะห์ความเป็นไปได้
- แจ้งผลต่อเจ้าของข้อมูล
- ภายใน 30 วัน นับจากวันที่รับคำขอ (ตามมาตรา 36 พ.ร.บ.ฯ) โดยอาจขยายเวลาได้อีก 30 วันหากมีเหตุอันสมควร และต้องแจ้งเจ้าของข้อมูลทราบ

บันทึกการดำเนินการและเก็บเอกสาร

- ทุกคำขอและการดำเนินการจะถูกจัดเก็บไว้ในระบบ PDPA Log สำหรับการตรวจสอบย้อนหลัง

3. การประสานงานภายใน

- กรณีคำขอเกี่ยวข้องกับข้อมูลสมาชิก: ฝ่ายบัตรสมาชิกมีหน้าที่รวบรวมและจัดส่งข้อมูลให้ DPO ภายใน 3 วันทำการ
- กรณีคำขอเกี่ยวข้องกับข้อมูลพนักงาน: ฝ่าย HR รวบรวมข้อมูลและส่งต่อ DPO
DPO และฝ่ายกฎหมายมีอำนาจให้ความเห็นเกี่ยวกับการยกเว้นสิทธิหรือการปฏิเสธคำขอโดยชอบ

4. การประเมินและปรับปรุงแนวทาง

องค์กรมีการประเมินผลการดำเนินการเกี่ยวกับคำขอใช้สิทธิทุก 6 เดือน โดยมีการรายงานต่อผู้บริหารระดับสูง และทบทวนกระบวนการตามกรณีปัญหาหรือคำวินิจฉัยของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

4.2.3 องค์กรจัดสรรทรัพยากรอย่างเพียงพอเพื่อจัดการกับคำขอใช้สิทธิตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เช่น แบบฟอร์มการขอใช้สิทธิ หรือระบบเทคโนโลยีสารสนเทศในการดำเนินการต่อการขอใช้สิทธิ

สิ่งที่ต้องทำ: มีแบบฟอร์มและระบบเทคโนโลยีต่อการจัดการข้อเรียกร้องหรือการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

หลักฐาน: 1) เอกสารแบบฟอร์มต่าง ๆ ในการขอใช้สิทธิตามกฎหมายของเจ้าของข้อมูลส่วนบุคคล
2) ระบบเทคโนโลยีสารสนเทศเพื่อดำเนินการต่อข้อเรียกร้องหรือคำขอใช้สิทธิ

สภาพบังคับ: ไม่มีกฎหมายกำหนด

เอกสารหลักฐานข้อ 4.2.3: การจัดสรรทรัพยากรเพื่อจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

1) เอกสารแบบฟอร์มต่าง ๆ ในการขอใช้สิทธิตามกฎหมายของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างแบบฟอร์มการขอใช้สิทธิของเจ้าของข้อมูล

แบบคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (DPR-01)

รายการ	รายละเอียด
ชื่อ-นามสกุล	

เลขประจำตัว ประชาชน / หมายเลข พนักงาน	
เบอร์โทรศัพท์	
อีเมล	
ที่อยู่สำหรับ ติดต่อ	
ประเภทสิทธิที่ ต้องการใช้ (โปรดเลือก)	☐ ขอเข้าถึงข้อมูล ☐ ขอแก้ไขข้อมูล ☐ ขอให้ลบข้อมูล ☐ ขอคัดค้านการ ประมวลผล ☐ ขอย้ายข้อมูล ☐ อื่นๆ:
รายละเอียด เพิ่มเติม (ถ้ามี)	
วันที่ยื่นคำร้อง	
ลายมือชื่อของ เจ้าของข้อมูล	

แนวทางการยื่นคำขอ

- ส่งทางอีเมล: dataprivacy@org.ac.th
- ส่งแบบฟอร์มผ่านระบบออนไลน์ [ลิงก์ระบบ]
- ยื่นด้วยตนเองที่สำนักงานฝ่ายบริหารสมาชิก

2) ระบบเทคโนโลยีสารสนเทศเพื่อดำเนินการต่อข้อเรียกร้องหรือคำขอใช้สิทธิ

รายละเอียดระบบบริหารจัดการคำขอใช้สิทธิ (Data Subject Rights Management System - DSRMS)

รายการ	รายละเอียด
ชื่อระบบ	DSRMS (Data Subject Rights Management System)
ฟังก์ชันหลัก	- รับคำขอผ่านแบบฟอร์มออนไลน์- ระบบยืนยันตัวตนผู้ขอใช้สิทธิ- บันทึกข้อมูลคำขอและ สถานะการดำเนินการ- แจ้งเตือนเจ้าหน้าที่ที่รับผิดชอบ- รายงานสรุปสถานะคำขอให้ ผู้บริหาร

การเข้าถึง	จำกัดสิทธิ์เฉพาะเจ้าหน้าที่ที่รับผิดชอบตามบทบาท (Role-Based Access Control)
ความปลอดภัย	- ระบบใช้การเข้ารหัสข้อมูล (Encryption)- มีระบบสำรองข้อมูลและกู้คืน- ระบบล็อกกิจกรรมผู้ใช้ (Audit Log)
การเชื่อมต่อ	เชื่อมต่อกับฐานข้อมูลสมาชิกและฐานข้อมูลบุคลากร เพื่ออำนวยความสะดวกในการตรวจสอบข้อมูล
การรองรับการรายงาน	รายงานการดำเนินการตามคำขอใช้สิทธิ และเวลาตอบกลับเป็นไฟล์ Excel/PDF
ผู้ดูแลระบบ	ฝ่าย IT Security ร่วมกับ DPO

ภาพรวมกระบวนการใช้ระบบ DSRMS

- เจ้าของข้อมูลยื่นคำขอผ่านแบบฟอร์มออนไลน์ในระบบ
- ระบบตรวจสอบความครบถ้วนของข้อมูลและส่งต่อคำขอให้เจ้าหน้าที่ที่รับผิดชอบ
- เจ้าหน้าที่ตรวจสอบและดำเนินการคำขอ
- ระบบแจ้งเตือนสถานะและส่งผลตอบกลับเจ้าของข้อมูลภายในเวลาที่กฎหมายกำหนด
- เจ้าหน้าที่บันทึกผลการดำเนินการและปิดคำขอในระบบ

4.2.4 ในกรณีที่ผู้รับผิดชอบด้านคำขอใช้สิทธิไม่สามารถปฏิบัติหน้าที่ได้ องค์กรจัดให้มีพนักงานคนอื่นหรือระบบเทคโนโลยีทำหน้าที่ดังกล่าวแทนได้

สิ่งที่ต้องทำ: มีพนักงานหรือมีระบบเทคโนโลยีปฏิบัติหน้าที่ทดแทนต่อการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

หลักฐาน: 1) คู่มือการปฏิบัติงานแทนในกรณีที่ผู้รับผิดชอบด้านคำขอใช้สิทธิไม่สามารถปฏิบัติหน้าที่ได้
2) คำสั่งมอบหมายการปฏิบัติหน้าที่แทนกรณีผู้รับผิดชอบไม่สามารถปฏิบัติหน้าที่แทนได้

สภาพบังคับ: ไม่มีกฎหมายกำหนด

1) คู่มือการปฏิบัติงานแทนในกรณีผู้รับผิดชอบด้านคำขอใช้สิทธิไม่สามารถปฏิบัติหน้าที่ได้
 คู่มือการปฏิบัติงานแทนกรณีผู้รับผิดชอบคำขอใช้สิทธิไม่สามารถปฏิบัติหน้าที่ได้

วัตถุประสงค์:

เพื่อให้การจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลดำเนินต่อเนื่องอย่างไม่มีสะดุด กรณีผู้รับผิดชอบหลักไม่สามารถปฏิบัติหน้าที่ได้

ขั้นตอนการปฏิบัติ:

- เมื่อผู้รับผิดชอบหลักแจ้งขาดงาน ลาหยุด หรือไม่สามารถปฏิบัติหน้าที่ได้ ให้แจ้งผู้บริหารฝ่ายบุคคลหรือ DPO ทราบโดยทันที
- ผู้บริหารฝ่ายบุคคลหรือ DPO จะมอบหมายงานให้พนักงานสำรองที่ได้รับการฝึกอบรมและมีความรู้ด้าน PDPA ดำเนินการแทน
- พนักงานสำรองจะได้รับสิทธิเข้าถึงระบบและข้อมูลที่เกี่ยวข้องเพื่อดำเนินการคำขอใช้สิทธิ
- หากมีระบบเทคโนโลยีสนับสนุน เช่น ระบบจัดการคำขออัตโนมัติ (DSRMS) ระบบจะส่งคำขอไปยังผู้ปฏิบัติงานแทนโดยอัตโนมัติ
- พนักงานสำรองจัดการคำขอและรายงานผลการดำเนินงานให้ผู้บริหารฝ่ายบุคคลและ DPO ทราบตามระยะเวลาที่กำหนด
- เมื่อผู้รับผิดชอบหลักกลับมาปฏิบัติหน้าที่ ให้รายงานสรุปการดำเนินการในช่วงเวลาที่สำรองปฏิบัติหน้าที่แทน

หมายเหตุ:

พนักงานสำรองต้องผ่านการฝึกอบรมและมีความเข้าใจในกฎหมายคุ้มครองข้อมูลส่วนบุคคล ควรมีการจัดทำบันทึกการมอบหมายงานและการฝึกอบรมเป็นหลักฐาน

2) คำสั่งมอบหมายการปฏิบัติหน้าที่แทนกรณีผู้รับผิดชอบไม่สามารถปฏิบัติหน้าที่ได้

คำสั่งมอบหมายการปฏิบัติหน้าที่แทน

เลขที่คำสั่ง: [หมายเลข]

วันที่: [วัน/เดือน/ปี]

เรื่อง: การมอบหมายการปฏิบัติหน้าที่แทนผู้รับผิดชอบด้านคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามที่ [ชื่อผู้รับผิดชอบหลัก] ตำแหน่ง [ตำแหน่ง] ไม่สามารถปฏิบัติหน้าที่ด้านการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลได้ ตั้งแต่วันที่ [วัน/เดือน/ปี] ถึงวันที่ [วัน/เดือน/ปี] เพื่อให้การดำเนินการเป็นไป อย่างต่อเนื่องและไม่เกิดความล่าช้า

จึงขอมอบหมายให้

ชื่อ: [ชื่อผู้รับมอบหมาย]

ตำแหน่ง: [ตำแหน่งผู้รับมอบหมาย]

ปฏิบัติหน้าที่แทนในด้านการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตั้งแต่วันที่ [วัน/เดือน/ปี] เป็นต้นไป จนกว่าผู้รับผิดชอบหลักจะสามารถปฏิบัติหน้าที่ได้ตามปกติ

ทั้งนี้ ผู้รับมอบหมายต้องปฏิบัติตามกฎหมายและนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กรอย่างเคร่งครัด

ลงชื่อ

.....

(ผู้มอบหมาย)

ตำแหน่ง: [ตำแหน่งผู้มอบหมาย]

ลงชื่อ

.....

(ผู้รับมอบหมาย)

ตำแหน่ง: [ตำแหน่งผู้รับมอบหมาย]

4.2.5 องค์กรมีความสามารถในการจัดการกับคำขอที่เพิ่มขึ้นได้ หรือยังสามารถบริหารจัดการได้แม้ว่าจะมีการลดจำนวนพนักงานที่รับผิดชอบคำขอลง

- สิ่งที่ต้องทำ: มีแผนสำรองสนับสนุนในกรณีที่ต้องมีการจัดการคำขอที่เพิ่มขึ้น และพร้อมดำเนินการได้ทันที
- หลักฐาน: 1) เอกสารแสดงบุคลากรที่ทำงานในส่วนดำเนินการต่อข้อเรียกร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- 2) ระบบเทคโนโลยีเพื่อดำเนินการต่อข้อเรียกร้องหรือการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- สภาพบังคับ: ไม่มีกฎหมายกำหนด

1) เอกสารแสดงบุคลากรที่ทำงานในส่วนดำเนินการต่อข้อเรียกร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

รายชื่อบุคลากรที่รับผิดชอบงานคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ลำดับ	ชื่อ-นามสกุล	ตำแหน่งงาน	หน้าที่รับผิดชอบ	เบอร์ติดต่อ/อีเมล	หมายเหตุ
1	นายสมชาย ใจดี	เจ้าหน้าที่คุ้มครองข้อมูล	รับคำขอและดำเนินการตอบสนองคำขอใช้สิทธิ	somchai@example.com	มีประสบการณ์ 3 ปี
2	นางสาวพรทิพย์ แก้วใส	เจ้าหน้าที่สำรอง	รองรับการปฏิบัติงานแทนในกรณีผู้รับผิดชอบหลักไม่ว่าง	porntip@example.com	ผ่านการฝึกอบรม PDPA
3	นายวิชัย เก่งงาน	เจ้าหน้าที่ IT สนับสนุนระบบคำขอ	ดูแลระบบเทคโนโลยีสารสนเทศที่ใช้จัดการคำขอ	wichai@example.com	พร้อมช่วยเหลือกรณีคำขอเพิ่มขึ้น

หมายเหตุ:

บุคลากรในส่วนนี้ได้รับการฝึกอบรมและมีความพร้อมในการรองรับคำขอที่เพิ่มขึ้น

กรณีมีการลดจำนวนพนักงาน ยังมีบุคลากรสำรองที่ได้รับการเตรียมพร้อมไว้

2) ระบบเทคโนโลยีเพื่อดำเนินการต่อข้อเรียกร้องหรือการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ระบบจัดการคำขอใช้สิทธิ (Data Subject Rights Management System - DSRMS)

1) ฟังก์ชันหลักของระบบ:

- รับคำขอผ่านช่องทางออนไลน์และออฟไลน์
- บันทึกคำขอและติดตามสถานะการดำเนินงานแบบเรียลไทม์
- แจ้งเตือนพนักงานที่รับผิดชอบเมื่อมีคำขอใหม่หรือใกล้ถึงกำหนดตอบกลับ
- รายงานสรุปจำนวนคำขอและเวลาตอบสนอง เพื่อการบริหารจัดการทรัพยากรอย่างมีประสิทธิภาพ
- มีระบบสำรองข้อมูลและสามารถรองรับคำขอจำนวนมากได้พร้อมกัน

2) การรองรับการจัดการคำขอที่เพิ่มขึ้น:

- ระบบสามารถขยายขีดความสามารถ (scalable) เพื่อตอบสนองคำขอที่เพิ่มขึ้นได้ทันที
- มีทีม IT คอยดูแลและสนับสนุนระบบตลอด 24 ชั่วโมง
- ระบบสามารถตั้งคำถามมอบหมายงานอัตโนมัติและเพิ่มพนักงานเสมือน (virtual agents) เพื่อช่วยจัดการคำขอในช่วงที่มีปริมาณสูง

4.3.1 องค์กรมีกระบวนการเพื่อให้แน่ใจว่าบันทึกการเข้าระบบ (log record) มีความถูกต้องและได้รับการปรับปรุงให้เป็นปัจจุบันตามความเหมาะสม

สิ่งที่ต้องทำ: มีกระบวนการในการบันทึกการเข้าระบบ (log record) ด้วยระบบเทคโนโลยีสารสนเทศตามมาตรฐานขั้นต่ำที่เป็นที่ยอมรับ

หลักฐาน: เอกสารการบันทึกการเข้าระบบ
ระบบเทคโนโลยีสารสนเทศในการบันทึกการเข้าระบบ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารกระบวนการบันทึกการเข้าระบบ (Log Record Process Document)

ชื่อเอกสาร: กระบวนการบันทึกและตรวจสอบการเข้าระบบ
(System Access Log Management Process)

รหัสเอกสาร: IT-SOP-LOG-001

เวอร์ชัน: 1.0

วันที่บังคับใช้: 1 มิถุนายน 2568

จัดทำโดย: ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)

วัตถุประสงค์

เพื่อกำหนดกระบวนการในการบันทึกและตรวจสอบการเข้าถึงระบบสารสนเทศขององค์กร ให้แน่ใจว่าบันทึกการเข้าระบบ (log record) มีความถูกต้องและได้รับการปรับปรุงอย่างสม่ำเสมอ

ขอบเขต

ครอบคลุมระบบสารสนเทศทุกระบบที่ใช้ในองค์กร รวมถึงระบบฐานข้อมูล ระบบแอปพลิเคชัน และระบบเครือข่าย

ขั้นตอนปฏิบัติ

การบันทึก Log

- ระบบเทคโนโลยีสารสนเทศทุกระบบต้องเปิดใช้งานการบันทึกข้อมูลการเข้าสู่ระบบ (login/logout) ของผู้ใช้
- บันทึกรายละเอียดอย่างน้อย ได้แก่ ชื่อผู้ใช้, เวลาเข้าและออกระบบ, ที่อยู่ IP ของอุปกรณ์, และกิจกรรมที่เกี่ยวข้อง

การตรวจสอบ Log

- ฝ่าย IT ต้องตรวจสอบ log อย่างน้อยเดือนละครั้ง เพื่อวิเคราะห์ความผิดปกติหรือการเข้าถึงที่ไม่ได้รับอนุญาต
- จัดเก็บ log ไว้อย่างปลอดภัยและมีการสำรองข้อมูลตามนโยบายการสำรองข้อมูลขององค์กร

การปรับปรุงและบำรุงรักษา

อัปเดตระบบบันทึก log ตามเทคโนโลยีใหม่และมาตรฐานความปลอดภัยที่เหมาะสมอย่างน้อยปีละ 1 ครั้ง

ฝ่าย IT รับผิดชอบในการตรวจสอบและปรับปรุงระบบบันทึก log ให้เป็นปัจจุบันอยู่เสมอ

ผู้รับผิดชอบ

- ฝ่าย IT รับผิดชอบดูแลระบบบันทึก log
- ผู้จัดการฝ่าย IT ตรวจสอบรายงานและอนุมัติการดำเนินการที่เกี่ยวข้อง

เอกสารอ้างอิง

- นโยบายความปลอดภัยสารสนเทศองค์กร (Information Security Policy)
- คู่มือปฏิบัติงานฝ่าย IT (IT Operation Manual)

ตัวอย่างบันทึกการเข้าระบบ (Log Record Sample)

วันที่/เวลา	ชื่อผู้ใช้	กิจกรรม	IP Address	หมายเหตุ
2025-06-02 09:15:23	user001	เข้าสู่ระบบ	192.168.1.101	เข้าสู่ระบบสำเร็จ
2025-06-02 09:45:10	user002	ล็อกเอาต์	192.168.1.102	ออกจากระบบปกติ
2025-06-02 10:05:47	admin01	ล้มเหลวล็อกอิน	192.168.1.103	รหัสผ่านไม่ถูกต้อง
2025-06-02 10:15:30	User001	เข้าถึงไฟล์	192.168.1.101	เปิดไฟล์เอกสารสำคัญ

ระบบเทคโนโลยีสารสนเทศที่ใช้บันทึกการเข้าระบบ

ระบบบริหารจัดการเครือข่าย (Network Management System) ที่มีฟังก์ชันบันทึกและรายงาน Log ระบบจัดการสิทธิ์ผู้ใช้งาน (Access Management System) ที่เชื่อมโยงกับ Active Directory ระบบ SIEM (Security Information and Event Management) สำหรับรวบรวม วิเคราะห์ และแจ้งเตือนเหตุการณ์ผิดปกติ

4.3.2 บันทึกการเข้าระบบ (log record) แสดงวันที่ดำเนินการตามคำขอ และผลการดำเนินการตามคำขอ

สิ่งที่ต้องทำ: มีการบันทึกการเข้าระบบที่แสดงวันที่ดำเนินการตามคำขอและผลการดำเนินการตามคำขอได้โดยง่าย มีความถูกต้อง และเป็นปัจจุบัน

หลักฐาน: ตัวอย่างเอกสารแสดงการบันทึกคำขอเข้าระบบที่แสดงวันที่และผลการดำเนินการตามคำขอ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารแสดงการบันทึกคำขอเข้าระบบ (Access Request Log)

ชื่อเอกสาร: บันทึกคำขอเข้าถึงระบบและผลการดำเนินการ (Access Request and Action Log)

รหัสเอกสาร: IT-LOG-ACCESS-002

เวอร์ชัน: 1.0

วันที่บังคับใช้: 1 มิถุนายน 2568

จัดทำโดย: ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)

วัตถุประสงค์

เพื่อบันทึกและติดตามคำขอเข้าถึงระบบสารสนเทศและผลการดำเนินการตามคำขออย่างถูกต้องและเป็นปัจจุบัน

รูปแบบการบันทึก

ลำดับที่	วันที่คำขอ	ชื่อผู้ขอ	ระบบ/แอปพลิเคชันที่ขอเข้าถึง	วันที่ดำเนินการ	ผลการดำเนินการ	ผู้ดำเนินการ	หมายเหตุ
1	2025-06-01	user001	ระบบบริหารสมาชิก	2025-06-02	อนุมัติ	admin0	เข้าถึงระบบได้
2	2025-06-02	user002	ระบบฐานข้อมูลลูกค้า	2025-06-03	ปฏิเสธ	admin02	ไม่มีสิทธิ์เข้าถึง
3	2025-06-03	user00	ระบบอีเมลองค์กร	2025-06-04	อนุมัติ	admin01	เข้าถึงได้

กระบวนการและระบบที่ใช้บันทึก

ใช้ระบบ IT Service Management (ITSM) สำหรับรับคำขอและบันทึกสถานะการดำเนินการ บันทึกข้อมูลในฐานข้อมูลที่สามารถสืบค้นได้ง่าย และสร้างรายงานผลการดำเนินการได้ทันที ระบบตั้งค่าการแจ้งเตือนเมื่อมีการอัปเดตสถานะคำขอ

ตัวอย่างบันทึกการเข้าระบบ

วันที่/เวลา	ชื่อผู้ใช้	กิจกรรม	ผลการดำเนินการ	หมายเหตุ
2525-06-02 09:15	user001	ขอสิทธิ์เข้าระบบ	อนุมัติเข้าถึงระบบ	อนุมัติโดย admin01
2025-06-03 10:00	user002	ขอสิทธิ์เข้าระบบ	ปฏิเสธสิทธิ์	ไม่มีสิทธิ์เข้าถึง
2025-06-04 11:30	user003	ขอสิทธิ์เข้าระบบ	อนุมัติเข้าถึงระบบ	อนุมัติโดย admin01

4.3.3 องค์กรจัดให้มีรายการการตรวจสอบที่บันทึกขั้นตอนสำคัญในกระบวนการจัดการคำขอ เช่น ระบบ หรือแผนกใดที่ดำเนินการตามคำขอใช้สิทธิแล้ว ซึ่งอาจเป็นส่วนหนึ่งของบันทึกหรือเอกสารแยกต่างหาก

สิ่งที่ต้องทำ: การรายงานการตรวจสอบที่บันทึกขั้นตอนสำคัญในกระบวนการจัดการคำขอ โดยแยกประเภทของคำขอใช้สิทธิ

หลักฐาน: รายงานการตรวจสอบบันทึกขั้นตอนสำคัญในกระบวนการจัดการคำขอ โดยอาจแยกเป็นแผนก

สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานการตรวจสอบขั้นตอนสำคัญในกระบวนการจัดการคำขอใช้สิทธิ (Audit Trail Report)

1. ชื่อเอกสาร: รายงานการตรวจสอบบันทึกขั้นตอนสำคัญในกระบวนการจัดการคำขอใช้สิทธิ (Data Subject

Request Management Audit Report)

2. รหัสเอกสาร: DPO-LOG-AUDIT-003

3. เวอร์ชัน: 1.0

4. วันที่จัดทำ: 3 มิถุนายน 2568

5. จัดทำโดย: ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO Office)

6. วัตถุประสงค์

เพื่อแสดงรายงานการตรวจสอบและติดตามบันทึกขั้นตอนนี้สำคัญในกระบวนการจัดการคำขอใช้สิทธิของเจ้าของข้อมูล โดยแยกตามประเภทคำขอและแผนกที่ดำเนินการ เพื่อให้สามารถตรวจสอบความถูกต้องและความสมบูรณ์ของกระบวนการได้อย่างมีประสิทธิภาพ

7. ขอบเขตของรายงาน

รายงานนี้ครอบคลุมคำขอใช้สิทธิในระบบสารสนเทศขององค์กรในช่วงเวลาที่ระบุ รวมถึงบันทึกการส่งต่อคำขอ การดำเนินงานของแต่ละแผนก และผลการดำเนินการตามคำขอ

8. รายละเอียดรายงาน

หมายเลขคำขอ	วันที่คำขอ	ประเภทคำขอใช้สิทธิ	แผนกที่รับผิดชอบดำเนินการ	วันที่เริ่มดำเนินการ	วันที่เสร็จสิ้น	ผลการดำเนินการ	ผู้รับผิดชอบ	หมายเหตุ
REQ-20250601-01	2025-06-01	ขอเข้าถึงข้อมูล (Access)	ฝ่ายบริการลูกค้า	2025-06-02	2025-06-04	ดำเนินการเสร็จสิ้น	พนักงาน A	อนุมัติคำขอ
REQ-20250602-02	2025-06-02	ขอแก้ไขข้อมูล (Rectification)	ฝ่ายระบบข้อมูล	2025-06-03	2025-06-05	ดำเนินการเสร็จสิ้น	พนักงาน B	ข้อมูลถูกแก้ไขเรียบร้อยแล้ว
REQ-20250602-03	2025-06-02	ขอระงับการใช้ข้อมูล (Restriction)	ฝ่ายกฎหมาย	2025-06-04	2025-06-06	ปฏิเสธคำขอ	พนักงาน C	ข้อมูลไม่ตรงเงื่อนไข
REQ-20250603-04	2025-06-03	ขอให้ลบข้อมูล (Erasure)	ฝ่ายบริการลูกค้า	2025-06-04	2025-06-06	ดำเนินการเสร็จสิ้น	พนักงาน A	ลบข้อมูลเรียบร้อยแล้ว

9. คำอธิบาย

- **ประเภทคำขอใช้สิทธิ** ได้แก่ Access (ขอเข้าถึงข้อมูล), Rectification (ขอแก้ไขข้อมูล), Restriction (ขอระงับการใช้ข้อมูล), Erasure (ขอให้ลบข้อมูล), และอื่น ๆ ตามกฎหมาย
- **แผนกที่รับผิดชอบ** ระบุหน่วยงานหรือทีมที่ดำเนินการจัดการคำขอนั้น ๆ
- **วันที่เริ่มดำเนินการ** และ **วันที่เสร็จสิ้น** ช่วยแสดงความรวดเร็วและติดตามกระบวนการ
- **ผลการดำเนินการ** เช่น อนุมัติ, ปฏิเสธ, อยู่ระหว่างดำเนินการ
- **ผู้รับผิดชอบ** ชื่อผู้ปฏิบัติงานหรือเจ้าหน้าที่ที่ดำเนินการตามคำขอ

- หมายเหตุ บันทึกข้อมูลเพิ่มเติม เช่น เหตุผลปฏิเสธหรือคำชี้แจงอื่น ๆ

10. การใช้รายงาน

รายงานนี้จัดทำขึ้นเพื่อใช้ตรวจสอบภายในประจำเดือนหรือประจำไตรมาส ใช้เป็นหลักฐานในการตรวจสอบความถูกต้องของการจัดการคำขอใช้สิทธิของเจ้าของข้อมูล สนับสนุนการบริหารจัดการความเสี่ยงและการปรับปรุงกระบวนการให้ดีขึ้น

4.3.4 องค์กรจัดให้มีบันทึกของการตอบสนองต่อคำขอใช้สิทธิตามกฎหมาย รวมถึงข้อมูลที่เปิดเผยหรือไม่เปิดเผยจากคำขอ (ในกรณีของการขอเข้าถึงข้อมูลส่วนบุคคล)

สิ่งที่ต้องทำ: บันทึกการตอบสนองต่อคำขอใช้สิทธิตามกฎหมาย โดยแยกประเภทของคำขอใช้สิทธิ
 หลักฐาน: บันทึกการตอบสนองต่อคำขอใช้สิทธิตามกฎหมาย
 สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารหลักฐานข้อ 4.3.4: บันทึกการตอบสนองต่อคำขอใช้สิทธิตามกฎหมาย (Response Record for Data Subject Requests)

1. ชื่อเอกสาร: บันทึกการตอบสนองต่อคำขอใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Data Subject Request Response Record)
2. รหัสเอกสาร: DPO-RESP-LOG-004
3. เวอร์ชัน: 1.0
4. วันที่จัดทำ: 3 มิถุนายน 2568
5. จัดทำโดย: ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO Office)
6. วัตถุประสงค์

เพื่อเก็บบันทึกข้อมูลการตอบสนองต่อคำขอใช้สิทธิตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยแยกประเภทของคำขอและระบุข้อมูลที่เปิดเผยหรือไม่เปิดเผยในกรณีคำขอเข้าถึงข้อมูลส่วนบุคคล

7. ขอบเขต

ครอบคลุมคำขอใช้สิทธิที่ได้รับจากเจ้าของข้อมูลทุกประเภทคำขอ ทั้งการขอเข้าถึงข้อมูล แก้ไข ลบ หรือระงับการใช้ข้อมูล โดยบันทึกผลการตอบสนองอย่างครบถ้วน

8. รายละเอียดบันทึก

หมายเลขคำขอ	วันที่คำขอ	ประเภทคำขอใช้สิทธิ	วันที่ตอบกลับ	ผลการตอบสนอง	ข้อมูลที่เปิดเผย/ไม่เปิดเผย	เหตุผลหากไม่เปิดเผยข้อมูล	ผู้ตอบสนอง	หมายเหตุ
REQ-20250601-01	2025-06-01	ขอเข้าถึงข้อมูล (Access)	2025-06-01	เปิดเผยข้อมูลบางส่วน	เปิดเผย: ข้อมูลส่วนตัวทั่วไป ไม่เปิดเผย: ข้อมูลทางการเงิน	ข้อมูลทางการเงินเป็นข้อมูลที่จำเป็นต้องปกป้องตามนโยบาย	พนักงาน A	ดำเนินการภายใน 3 วันทำการ
REQ-20250602-02	2025-06-02	ขอแก้ไขข้อมูล (Rectification)	2025-06-05	แก้ไขข้อมูลเรียบร้อยแล้ว		-	พนักงาน B	ข้อมูลที่แก้ไข: ที่อยู่และเบอร์โทร
REQ-20250603-03	2025-06-03	ขอให้ลบข้อมูล (Erasure)	2025-06-06	ปฏิเสธคำขอ	ไม่เปิดเผย	ข้อมูลมีความจำเป็นทางกฎหมายต้องเก็บไว้	พนักงาน C	แจ้งเหตุผลให้เจ้าของข้อมูลทราบ
REQ-20250604-04	2025-06-04	ขอระงับการใช้ข้อมูล (Restriction)	2025-06-07	อนุมัติคำขอ	-	-	พนักงาน D	ระงับข้อมูลชั่วคราว

9. คำอธิบาย

- **ประเภทคำขอใช้สิทธิ:** เช่น ขอเข้าถึงข้อมูล (Access) ขอแก้ไข (Rectification) ขอให้ลบ (Erasure) ขอระงับการใช้ข้อมูล (Restriction)
- **ผลการตอบสนอง:** เปิดเผยข้อมูล, เปิดเผยบางส่วน, ปฏิเสธคำขอ, อนุมัติคำขอ ฯลฯ

- ข้อมูลที่เปิดเผย/ไม่เปิดเผย: ระบุชัดเจนว่าข้อมูลส่วนใดถูกเปิดเผยหรือถูกปกปิดพร้อมเหตุผล
- เหตุผลหากไม่เปิดเผยข้อมูล: เพื่อความโปร่งใส เช่น ปกป้องความลับทางการค้า หรือข้อมูลที่กฎหมายกำหนดให้เก็บรักษาไว้
- ผู้ตอบสนอง: ชื่อพนักงานหรือเจ้าหน้าที่ที่รับผิดชอบตอบคำขอ

10. การใช้บันทึก

ใช้ในการตรวจสอบย้อนหลังและติดตามการจัดการคำขอใช้สิทธิ
เป็นหลักฐานแสดงความโปร่งใสและความรับผิดชอบขององค์กรในการตอบสนองคำขอ
สนับสนุนการปรับปรุงกระบวนการจัดการคำขอให้ดีขึ้น

4.4.1 องค์กรดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลทั้งหมดภายในระยะเวลาตาม

กฎหมาย

สิ่งที่ต้องทำ: การดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายในระยะเวลาที่
กฎหมายกำหนด หรือตามความเหมาะสม

หลักฐาน: เอกสารหลักฐานการดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30 โทษทางปกครองในกรณีที่ไม่ปฏิบัติตามมาตรา 30 วรรคสาม ปรับทางปกครองไม่เกิน 1 ล้านบาท

การดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลภายในระยะเวลาที่กฎหมายกำหนด

1. ชื่อเอกสาร: ทะเบียนการดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights Request Log)

2. รหัสเอกสาร: DPO-RIGHTS-LOG-004

3. หน่วยงานที่รับผิดชอบ: ฝ่ายคุ้มครองข้อมูลส่วนบุคคล / คณะทำงานจัดการสิทธิของเจ้าของข้อมูล

4. วันที่จัดทำ: 3 มิถุนายน 2568

5. สารสำคัญ

เอกสารนี้แสดงบันทึกการดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดภายใน 30 วันนับแต่วันที่ได้รับคำขอ ตามมาตรา 30 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ตัวอย่างแบบฟอร์มบันทึกการดำเนินการตามคำขอ

หมายเลขคำขอ	วันที่ได้รับคำขอ	ประเภทคำขอ	วันที่ดำเนินการแล้วเสร็จ	ระยะเวลาดำเนินการ (วัน)	สถานะ	หมายเหตุ
REQ-20250601-01	1 มิ.ย. 2568	ขอเข้าถึงข้อมูล	25 มิ.ย. 2568	24 วัน	ดำเนินการเสร็จแล้ว	ภายในระยะเวลาตามกฎหมาย
REQ-20250602-02	2 มิ.ย. 2568	ขอให้ลบข้อมูล	29 มิ.ย. 2568	27 วัน	ดำเนินการเสร็จแล้ว	-
REQ-20250515-03	15 พ.ค. 2568	ขอระงับการใช้	13 มิ.ย. 2568	29 วัน	ดำเนินการเสร็จแล้ว	มีเอกสารยืนยัน

หมายเหตุด้านกฎหมาย

ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30 วรรคหนึ่ง

- เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลดำเนินการตามสิทธิภายใน สามสิบวัน นับแต่วันที่ผู้ควบคุมข้อมูลได้รับคำขอ
- หากไม่ดำเนินการตามคำขอภายในเวลาที่กำหนดตาม มาตรา 30 วรรคสาม
- ผู้ควบคุมข้อมูลอาจต้องรับ โทษทางปกครองไม่เกิน 1,000,000 บาท

ขั้นตอนการดำเนินการที่ใช้ในองค์กร

- เจ้าหน้าที่ DPO หรือผู้รับคำขอ ลงทะเบียนคำขอภายใน 1 วันทำการ
- ตรวจสอบความถูกต้องของคำขอภายใน 3 วัน
- ประสานฝ่ายที่เกี่ยวข้องเพื่อจัดการคำขอภายใน 20-25 วัน
- ตอบกลับผลคำขอแก่เจ้าของข้อมูลภายในไม่เกิน 30 วัน
- บันทึกผลลงในระบบ log และรายงานต่อผู้มีอำนาจตามโครงสร้างองค์กร

4.4.2 ในกรณีที่องค์กรจะปฏิเสธการดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล องค์กรจะมีบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในบันทึกการ (ROPA) และแจ้งเหตุผลของการปฏิเสธหรือขอยกเว้นใด ๆ ไปยังเจ้าของข้อมูลส่วนบุคคลที่ขอใช้สิทธิ

สิ่งที่ต้องทำ: มีช่องสำหรับบันทึกการปฏิเสธคำขอพร้อมด้วยเหตุผลในบันทึกการ (ROPA) และมีกระบวนการแจ้งเหตุผลการปฏิเสธดังกล่าวไปยังเจ้าของข้อมูลส่วนบุคคล

หลักฐาน: ที่รายการที่มีช่องสำหรับบันทึกการปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เอกสารการแจ้งเหตุผลการปฏิเสธคำขอใช้สิทธิไปยังเจ้าของข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30 วรรคสอง วรรคสาม, 31 วรรคสาม, 32 วรรคสาม, 36, 39 (7)

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 39 วรรคหนึ่ง กำหนดโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

การบันทึกการปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล พร้อมเหตุผล และกระบวนการแจ้งต่อเจ้าของข้อมูล

1. ชื่อเอกสาร: บันทึกการรายการกิจกรรม (Record of Processing Activities - ROPA): ส่วนการปฏิเสธคำขอแบบฟอร์มแจ้งเหตุผลการปฏิเสธคำขอใช้สิทธิ

2. รหัสเอกสาร:

ROPA-DATA-SUBJECT-REQUEST-REJECT-001

NOTI-DATA-SUBJECT-REFUSE-001

3. หน่วยงานที่รับผิดชอบ: DPO หรือฝ่ายกฎหมาย / ฝ่ายบริหารสิทธิของเจ้าของข้อมูล

4. ตัวอย่างฟอร์มที่ใช้: ตัวอย่างจากบันทึกการรายการกิจกรรม (ROPA)

ลำดับ	ประเภทคำขอ	วันที่รับคำขอ	เหตุผลที่ปฏิเสธ	วันที่แจ้งการปฏิเสธ	ช่องทางการแจ้ง	หมายเหตุ
1	ขอให้ลบข้อมูลส่วนบุคคล	2 มิ.ย. 2568	ปฏิเสธการร้องขอให้ดำเนินการข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด (ม. ๓๖ ว.๑)	6 มิ.ย. 2568	อีเมล	อ้างอิง ม.33 (2)

2	ขอให้ระงับการใช้	10 พ.ค. 2568	ปฏิเสธตามกฎหมาย หรือคำสั่งศาลและการเข้าถึงนั้นจะกระทบสิทธิและเสรีภาพผู้อื่น (ม.๓๐ วรรค ๓)	14 พ.ค. 2568	จดหมายลงทะเบียน	แจ้งตาม ม.36

แบบฟอร์มแจ้งเหตุผลการปฏิเสธคำขอใช้สิทธิ

เรื่อง: แจ้งผลการพิจารณาคำขอใช้สิทธิภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เรียน [ชื่อเจ้าของข้อมูล]

อ้างอิงถึงคำขอใช้สิทธิของท่านที่ยื่นต่อองค์กรเมื่อวันที่ [xx เดือน xxxx]

องค์กรได้ดำเนินการตรวจสอบคำขอดังกล่าวแล้ว และขอแจ้งว่าไม่สามารถดำเนินการตามคำขอของท่านได้ โดยมีเหตุผลดังนี้:

- ข้อมูลส่วนบุคคลดังกล่าวยังจำเป็นต้องเก็บรักษาไว้เพื่อการปฏิบัติตามหน้าที่ตามกฎหมาย
- การลบข้อมูลจะมีผลกระทบต่อการดำเนินการตามสัญญาหรือการให้บริการ
- ไม่มีสิทธิในการลบข้อมูลตามมาตรา 33 วรรคหนึ่ง

หากท่านมีข้อโต้แย้งเกี่ยวกับการพิจารณาดังกล่าว ท่านสามารถยื่นเรื่องร้องเรียนต่อสำนักงาน

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอแสดงความนับถือ

[ชื่อ-ตำแหน่งเจ้าหน้าที่]

ผู้ควบคุมข้อมูลส่วนบุคคล

[ชื่อองค์กร]

วันที่: [xx/xx/xxxx]

5. กระบวนการที่เกี่ยวข้อง

ขั้นตอน	รายละเอียด
1. รับคำขอ	เจ้าหน้าที่บันทึกในระบบ ROPA
2. ตรวจสอบเหตุผล	ตรวจสอบคำขอเทียบกับฐานกฎหมายตาม มาตรา 30, 33, 36
3. พิจารณาและเสนออนุมัติ	DPO หรือผู้บริหารมีอำนาจอนุมัติการปฏิเสธ
4. แจ้งเจ้าของข้อมูล	ส่งแบบฟอร์มแจ้งเหตุผลผ่านอีเมล/ไปรษณีย์
5. เก็บรักษาหลักฐาน	เก็บในระบบ ROPA และแนบสำเนาแบบแจ้งเหตุผล

4.4.3 เจ้าหน้าที่ที่รับผิดชอบในการจัดการคำขอจะประชุมกันเป็นประจำ เพื่อหารือเกี่ยวกับปัญหาต่าง ๆ และตรวจสอบ จัดลำดับความสำคัญ หรือยกระดับกรณีที่น่าสงสัยใด ๆ

สิ่งที่ต้องทำ: การจัดประชุมหรือหารือเกี่ยวกับการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นประจำ

หลักฐาน: รายงานการประชุมหรือรายงานประเมินประสิทธิภาพของการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานการประชุมคณะกรรมการ/เจ้าหน้าที่ผู้ดูแลคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights - DSR Meeting Minutes)

1. ชื่อเอกสาร:

รายงานการประชุมคณะกรรมการด้านสิทธิของเจ้าของข้อมูลส่วนบุคคล

2. รหัสเอกสาร: DSR-MTG-REPORT-001

3. หน่วยงานที่รับผิดชอบ:

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

คณะกรรมการฝ่ายจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล (DSR Task Force)

4. ความถี่ในการประชุม:

ทุกเดือน (เช่น วันอังคารสุดท้ายของทุกเดือน) หรือกรณีมีคำขอเกิน 5 เรื่องในเดือนนั้น

5. ตัวอย่างรายงานการประชุม

รายงานการประชุมคณะกรรมการด้านสิทธิของเจ้าของข้อมูลส่วนบุคคล

วันที่ประชุม: 30 พฤษภาคม 2568

เวลา: 13:30 – 15:00 น.

สถานที่: ห้องประชุม 3A, อาคารบริหารกลาง

ผู้เข้าร่วม:

1. นายอภิชัย รัตนติลล (DPO)
2. นางสาวณัฐกานต์ วิศาลจิต (ฝ่ายกฎหมาย)
3. นายพงศกร วัฒนกิจ (IT Support – Log System)
4. น.ส. วริศรา ชูสกุล (ผู้ดูแลระบบรับคำขอ)

วาระการประชุม

1.สรุปคำขอใช้สิทธิที่ได้รับในรอบเดือนพฤษภาคม 2568

- คำขอเข้าถึงข้อมูล: 7 ราย
- คำขอแก้ไขข้อมูล: 2 ราย
- คำขอลบข้อมูล: 3 ราย
- คำขอระงับการใช้: 1 ราย

2.กรณีที่ล่าช้าหรือมีปัญหาในการดำเนินการ

- คำขอของคุณ A (ล่าช้า 5 วัน เนื่องจากการรอเอกสารยืนยันตัวตน)
- คำขอของคุณ C (ประเด็นเกี่ยวกับคำขอลบข้อมูลที่ต้องเก็บไว้ตาม พ.ร.บ.บัญชีฯ)

3.การจัดลำดับความสำคัญ

- คำขอของคุณ G (ข้อมูลสุขภาพ) ได้รับจัดลำดับสูงสุด
- คำขอทั่วไปภายใน 15 วันทำการ

4.แนวทางการปรับปรุง

- เสนอปรับปรุงฟอร์มคำขอใหม่ให้แจ้งเตือนอัตโนมัติเมื่อถึงครึ่งระยะเวลาการดำเนินการ
- เสนอจัดทำ Dashboard รายงานสถานะคำขอแบบ real-time

มติที่ประชุม:

- อนุมัติให้อัปเดตรบบติดตามสถานะคำขอ
- แต่งตั้ง น.ส. วริศรา เป็นผู้ประสานงานเร่งรัดคำขอที่เกิน 20 วัน

บันทึกโดย:

นายอภิชัย รัตนติลล (DPO)

วันที่บันทึก: 31 พฤษภาคม 2568

แนบไฟล์หรือหลักฐานเพิ่มเติม (หากจำเป็น)

- ภาพถ่ายหน้าจอ Dashboard แสดงสถานะคำขอ
- แบบฟอร์มติดตามการประเมิน SLA (Service Level Agreement)

4.4.4 หากองค์กรต้องการขยายเวลาการจัดการคำขอใช้สิทธิตามกฎหมายของเจ้าของข้อมูลส่วนบุคคล องค์กรจะรายงานความก้าวหน้าของการดำเนินการตามคำขอ และแจ้งให้บุคคลนั้นทราบ

สิ่งที่ต้องทำ: มีการรายงานความก้าวหน้าในการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล และแจ้งไปยังเจ้าของข้อมูลส่วนบุคคลให้ทราบ

หลักฐาน: บันทึกรายงานความก้าวหน้าในการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

บันทึกรายงานความก้าวหน้าในการดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

รหัสเอกสาร: DSR-PROG-01

หน่วยงานที่รับผิดชอบ: กลุ่มงานคุ้มครองข้อมูลส่วนบุคคล

วันที่จัดทำ/ปรับปรุงล่าสุด: [กรอกวันที่]

1. ข้อมูลเบื้องต้นของคำขอ

รายการ	รายละเอียด
เลขที่คำขอ	DSR-REQ-2025-0452
ชื่อเจ้าของข้อมูล	นายสมชาย ใจดี
ประเภทคำขอใช้สิทธิ	ขอเข้าถึงข้อมูลส่วนบุคคล
วันที่ได้รับคำขอ	5 มิถุนายน 2568
วันที่ครบกำหนดดำเนินการ	5 กรกฎาคม 2568

2. รายงานความก้าวหน้า

ลำดับ	วันที่ดำเนินการ	รายละเอียดการดำเนินการ	ผู้รับผิดชอบ	หมายเหตุ
1	6 มิ.ย. 2568	รับคำขอและบันทึกเข้าสู่ระบบ	เจ้าหน้าที่รับคำขอ	
2	10 มิ.ย. 2568	ตรวจสอบความครบถ้วนของข้อมูล	DPO	
3	15 มิ.ย. 256	ประชุมร่วมฝ่าย IT และฝ่าย HR	ทีม DSR Team	ต้องใช้เวลาเพิ่มเพื่อรวบรวมข้อมูลจาก 2 ระบบ

4	20 มิ.ย. 2568	ส่งอีเมลแจ้งเจ้าของข้อมูล เรื่องขยายเวลา	DPO	แนบแบบฟอร์มแจ้งเหตุผล และกำหนดใหม่แล้ว

3. สำเนาการแจ้งเจ้าของข้อมูล

เรื่อง: แจ้งการขยายเวลาการดำเนินการคำขอใช้สิทธิ

เรียน คุณสมชาย ใจดี

ตามที่ท่านได้ยื่นคำขอใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลเมื่อวันที่ 5 มิถุนายน 2568 ทางเราขอแจ้งให้ทราบว่า คำขอของท่านจำเป็นต้องใช้ระยะเวลาเพิ่มเติมในการดำเนินการ เนื่องจากต้องรวบรวมข้อมูลจากหลายระบบ ซึ่งต้องได้รับการตรวจสอบอย่างรอบคอบ

องค์กรจะดำเนินการให้เสร็จสิ้นภายในวันที่ 25 กรกฎาคม 2568 และจะรายงานผลให้ท่านทราบโดยเร็ว

ขอภัยในความไม่สะดวก และขอขอบคุณที่ให้ความร่วมมือ

ขอแสดงความนับถือ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

บริษัท/องค์กร [ชื่อองค์กร]

4.5.1 เจ้าหน้าที่ที่รับผิดชอบในการจัดการคำขอจะประชุมหารือกันเป็นประจำ เพื่อปรึกษาปัญหาเกี่ยวกับประเด็นต่าง ๆ ในเรื่องการจัดการต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: มีการประชุมเพื่อหารือเกี่ยวกับประเด็นในเรื่องจัดการดำเนินการตามคำขอใช้สิทธิของเจ้าของ

ข้อมูลส่วนบุคคลเป็นประจำในฝ่ายงาน

หลักฐาน: รายงานการประชุม

สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานการประชุมเจ้าหน้าที่ผู้รับผิดชอบคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ครั้งที่: 3/2568

วัน/เวลา: วันจันทร์ที่ 3 มิถุนายน 2568 เวลา 10:00 – 11:30 น.

สถานที่: ห้องประชุม PDPA ชั้น 5 อาคารบริหารกลาง

ผู้เข้าร่วมประชุม:

1. นางสาวสุภาวดี พิทักษ์ธรรม – DPO (ประธาน)
2. นายณัฐวุฒิ สายตรง – เจ้าหน้าที่ฝ่ายกฎหมาย
3. นางสาวศิริพร ใจมั่น – เจ้าหน้าที่ระบบสารสนเทศ
4. นายธีรวัฒน์ ธรรมรงค์ – เจ้าหน้าที่รับคำขอ (DSR)
5. น.ส.ปิยะฉัตร จันทร์ – ผู้ช่วยเลขานุการ

ระเบียบวาระการประชุม

วาระที่ 1: แจ้งเพื่อทราบ

ประธานแจ้งผลการดำเนินงานเดือนที่ผ่านมา มีคำขอใช้สิทธิ 9 รายการ ร้อยละ 88 ของคำขอสามารถดำเนินการได้ภายใน SLA 30 วัน

วาระที่ 2: พิจารณาประเด็นปัญหาในการจัดการคำขอ

ปัญหาการประสานข้อมูลจากระบบเก่า (Legacy System) ทำให้เกิดความล่าช้า
ข้อเสนอ: พิจารณาจัดอบรมให้ฝ่าย IT เพิ่มเติมเกี่ยวกับโครงสร้างข้อมูลส่วนบุคคล

วาระที่ 3: การจัดลำดับความสำคัญของคำขอ

เห็นควรใช้ “ระดับความเร่งด่วน” (Urgency Tag) บน Dashboard เพื่อกำกับลำดับการดำเนินการ

วาระที่ 4: ข้อเสนอเพิ่มเติม

มีข้อเสนอให้เพิ่มช่อง “บันทึกเหตุการณ์ล่าช้า” ในระบบคำขออัตโนมัติ
พิจารณาจัดประชุมเชิงปฏิบัติการร่วมระหว่าง DSR, กฎหมาย และ IT ทุกไตรมาส

มติที่ประชุม

ให้ฝ่าย IT ปรับปรุงระบบ Dashboard ภายใน 15 วัน
ให้เลขานุการจัดทำแบบฟอร์มแจ้งเหตุผลการล่าช้าและแจกจ่ายเจ้าหน้าที่
นัดประชุมครั้งต่อไปในวันที่ 8 กรกฎาคม 2568

ผู้บันทึกการประชุม

น.ส.ปิยะฉัตร จันทร์

ผู้ช่วยเลขานุการ

(ลงชื่อ)

วันที่ 3 มิถุนายน 2568

ผู้รับรองการประชุม

นางสาวสุภาวดี พิทักษ์ธรรม

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

(ลงชื่อ)

วันที่ 3 มิถุนายน 2568

4.5.2 องค์การจัดทำรายงานการประเมินประสิทธิภาพของการจัดการคำขอเพื่อให้แน่ใจว่าคำขอได้รับการจัดการอย่างเหมาะสม

- สิ่งที่ต้องทำ: มีการทำรายงานการประเมินประสิทธิภาพของการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ผ่านการประชุมหารือร่วมกันในฝ่ายงาน
- หลักฐาน: รายงานการประเมินประสิทธิภาพการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
รายงานการประชุมหารือร่วมกันในฝ่ายงาน
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานการประเมินประสิทธิภาพการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

1. ชื่อหน่วยงาน: ฝ่าย/กลุ่มงานที่รับผิดชอบ: กลุ่มงานบริหารจัดการคำขอใช้สิทธิข้อมูลส่วนบุคคล

2. รอบระยะเวลาการประเมิน: ไตรมาสที่ 2 ปีงบประมาณ 2568

3. วัตถุประสงค์ของการประเมิน

เพื่อประเมินความมีประสิทธิภาพของกระบวนการรับเรื่อง ดำเนินการ และตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงเพื่อระบุจุดที่ควรปรับปรุงพัฒนาการให้บริการและการดำเนินงาน

4. สรุปผลการประเมิน

– จำนวนคำขอใช้สิทธิที่ได้รับ

ช่วงระยะเวลาที่ประเมิน มีคำขอใช้สิทธิรวมทั้งสิ้น 52 รายการ โดยมีประเภทคำขอหลัก ได้แก่ การขอเข้าถึงข้อมูล การคัดค้านการใช้ข้อมูล การขอลบข้อมูล และการขอระงับการใช้ข้อมูล

– ระยะเวลาการดำเนินการต่อคำขอ

ร้อยละ 94 ของคำขอได้รับการดำเนินการและแจ้งผลภายในระยะเวลาไม่เกิน 30 วัน

ร้อยละ 6 มีการขยายเวลาออกไปตามความเหมาะสม พร้อมมีการแจ้งเหตุผลและความ

คืบหน้าให้เจ้าของข้อมูลทราบ

– **การปฏิเสธคำขอ**

มีจำนวน 3 รายการที่มีการปฏิเสธการดำเนินการตามคำขอ โดยมีการบันทึกเหตุผลในระบบ และมีการแจ้งให้เจ้าของข้อมูลทราบเป็นลายลักษณ์อักษร

– **ระบบการติดตามและรายงานผล**

มีการใช้ระบบเทคโนโลยีสารสนเทศติดตามสถานะของคำขอแต่ละรายการ พร้อมทั้งมีแบบฟอร์มติดตามการประเมิน SLA เป็นรายเดือน

– **ความพร้อมของบุคลากรและทรัพยากร**

เจ้าหน้าที่ผู้รับผิดชอบได้รับการฝึกอบรมประจำไตรมาส และมีการประชุมทบทวนแนวทางการดำเนินงานทุกเดือนเพื่อเพิ่มประสิทธิภาพการตอบสนองคำขอ

5. ข้อเสนอแนะ

ควรพัฒนาระบบแจ้งเตือนอัตโนมัติให้เจ้าของข้อมูลรับทราบสถานะคำขอแบบเรียลไทม์ เสนอให้จัดอบรมการเขียนเหตุผลในการปฏิเสธคำขออย่างเป็นระบบและเหมาะสมมากขึ้น

6. ผู้จัดทำรายงาน

นายวสันต์ จิตสาธารณะ

เจ้าหน้าที่บริหารข้อมูลส่วนบุคคล

7.วันที่จัดทำรายงาน: 3 มิถุนายน 2568

รายงานการประชุมหารือร่วมกันในฝ่ายงาน

วันที่ประชุม: 27 พฤษภาคม 2568

สถานที่: ห้องประชุมกลุ่มงานบริหารจัดการข้อมูล

ผู้เข้าร่วมประชุม: เจ้าหน้าที่ฝ่ายบริหารคำขอใช้สิทธิ จำนวน 6 คน

ประธานการประชุม: นางสาวสุธิดา วัชรียะกิจ ผู้จัดการฝ่าย

วาระการประชุม

- ทบทวนผลการดำเนินงานคำขอใช้สิทธิในช่วง 3 เดือนที่ผ่านมา
- ปัญหาและอุปสรรคที่พบในการดำเนินการ
- การประเมิน SLA และข้อเสนอในการปรับปรุงกระบวนการ
- แนวทางการสื่อสารกับเจ้าของข้อมูลเมื่อเกิดความล่าช้าหรือมีเหตุจำเป็นในการปฏิเสธคำขอ
- การจัดเตรียมรายงานประสิทธิภาพการดำเนินงาน

มติที่ประชุม

- ให้จัดทำรายงานประเมินประสิทธิภาพประจำไตรมาสและนำเสนอต่อผู้บริหาร
- ให้พัฒนาแผนเพื่อลดจุดหมายแจ้งเหตุผลการปฏิเสธคำขอให้มีความชัดเจนมากขึ้น
- ให้มีการประชุมทบทวนผลการดำเนินงานทุกเดือน

ผู้บันทึกการประชุม: นางสาวณัฐวดี ขจรกิจ

4.5.3 องค์การรายงานต่อผู้บริหารระดับสูง เพื่อทบทวนและมีคำสั่งให้ดำเนินการจัดการคำขอใช้สิทธิ ตามความเหมาะสม

สิ่งที่ต้องทำ: มีการประชุมระหว่างหน่วยงานกับผู้บริหารอาวุโส เพื่อรายงานและทบทวนคำสั่งเกี่ยวกับการดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นประจำ

หลักฐาน: รายงานการประชุม

สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานการประชุมระหว่างหน่วยงานและผู้บริหารอาวุโส

(การรายงานและทบทวนคำสั่งเกี่ยวกับการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล)

ชื่อองค์กร:

ชื่อหน่วยงาน: กลุ่มงานบริหารจัดการคำขอใช้สิทธิข้อมูลส่วนบุคคล

ผู้บริหารระดับสูงที่เข้าร่วม: นายปริญญา เกษมศักดิ์ รองผู้อำนวยการสำนักงาน

วันที่ประชุม: 24 พฤษภาคม 2568

สถานที่: ห้องประชุม 1 อาคารบริหารกลาง

หัวข้อการประชุม

- รายงานภาพรวมการดำเนินงานเกี่ยวกับคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล ไตรมาสที่ 2 ปีงบประมาณ 2568
- ปัญหาและอุปสรรคในการดำเนินการ รวมถึงการขอขยายระยะเวลาและกรณีปฏิเสธคำขอ
- การประเมินประสิทธิภาพของระบบติดตามคำขอและ SLA
- การเสนอแนะนโยบายและคำสั่งจากผู้บริหารระดับสูงเพื่อสนับสนุนการดำเนินงาน

สรุปสาระสำคัญ

- จำนวนคำขอใช้สิทธิในช่วงไตรมาสนี้รวม 52 รายการ มีการจัดการแล้วเสร็จภายในระยะเวลา 49 รายการ (94%)
- มี 3 รายการที่มีเหตุจำเป็นในการปฏิเสธคำขอ โดยแจ้งเหตุผลตามขั้นตอน และบันทึกไว้ใน ROPA
- ระบบติดตามคำขอเริ่มมีการใช้งาน Dashboard แบบรายวัน และมีแบบฟอร์มติดตาม SLA รายเดือน
- มีข้อเสนอให้เพิ่มบุคลากรสำรองในกรณีคำขอเพิ่มขึ้นอย่างฉับพลัน และพัฒนาระบบแจ้งเตือนอัตโนมัติไปยังเจ้าของข้อมูล

มติ/ข้อสั่งการจากผู้บริหาร

- ให้มีการปรับปรุงระบบ Dashboard ให้แสดงผลการดำเนินงานแบบ real-time และสามารถสรุปภาพรวมประจำสัปดาห์
- อนุมัติแผนจัดอบรมเพิ่มเติมสำหรับเจ้าหน้าที่ฝ่ายรับคำขอ

- ให้จัดส่งรายงานผลการดำเนินการต่อคำขอเป็นรายเดือนต่อผู้บริหาร พร้อมแนบกรณีศึกษาที่มีความซับซ้อนหรือเกิดข้อโต้แย้ง
- ให้กลุ่มงานดำเนินการตามข้อเสนอเรื่องระบบแจ้งเตือนอัตโนมัติ และรายงานความคืบหน้าภายใน 30 วัน

ผู้บันทึกการประชุม

นางสาวสุภาวดี คำแก้ว

เจ้าหน้าที่วิเคราะห์นโยบายและแผน

วันที่จัดทำรายงาน: 3 มิถุนายน 2568

4.5.4 องค์การวิเคราะห์แนวโน้มจากคำขอใช้สิทธิต่าง ๆ ที่มี เพื่อหาสาเหตุของคำขอ และจะได้นำไปปรับปรุงประสิทธิภาพหรือลดปริมาณคำขอต่อไปในอนาคต

- สิ่งที่ต้องทำ: มีการวิเคราะห์ข้อมูลหรือผลสรุปจากการดำเนินการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล และนำผลการวิเคราะห์ไปปรับปรุงแนวทางการดำเนินงาน
- หลักฐาน: รายงานผลการวิเคราะห์จากคำขอใช้สิทธิต่าง ๆ ถึงสาเหตุและปัญหา
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานผลการวิเคราะห์แนวโน้มคำขอใช้สิทธิข้อมูลส่วนบุคคล

(การวิเคราะห์แนวโน้มและนำผลไปปรับปรุงประสิทธิภาพการจัดการคำขอ)

ชื่อองค์กร: บริษัท เอ็กเซลเลนซ์ จำกัด

ฝ่ายงาน: ฝ่ายคุ้มครองข้อมูลส่วนบุคคล

วันที่จัดทำรายงาน: 15 มิถุนายน 2568

ระยะเวลาการวิเคราะห์: ไตรมาสที่ 2 ปีงบประมาณ 2568

1. บทนำ

รายงานฉบับนี้จัดทำขึ้นเพื่อวิเคราะห์แนวโน้มของคำขอใช้สิทธิข้อมูลส่วนบุคคลที่ได้รับในไตรมาสที่ 2 ปีงบประมาณ 2568 โดยมีวัตถุประสงค์เพื่อระบุสาเหตุและปัญหาที่เกิดขึ้น พร้อมเสนอแนวทางปรับปรุงประสิทธิภาพในการจัดการคำขอและลดปริมาณคำขอในอนาคต

2. ข้อมูลและแนวโน้มคำขอใช้สิทธิ

- จำนวนคำขอใช้สิทธิทั้งหมด: 52 รายการ
- ประเภทคำขอที่พบมากที่สุด:
- ขอเข้าถึงข้อมูลส่วนบุคคล (Access request) 40%
- ขอแก้ไขข้อมูล (Rectification) 25%
- ขอให้ลบข้อมูล (Erasure) 15%

- ขอร้งับการใช้ข้อมูล (Restriction) 10%
- อื่น ๆ (รวมถึงโอนย้ายข้อมูล) 10%

3. สาเหตุของคำขอใช้สิทธิที่พบ

- เจ้าของข้อมูลต้องการตรวจสอบความถูกต้องของข้อมูลที่เก็บไว้
- ความไม่ชัดเจนในการแจ้งวัตถุประสงค์การเก็บข้อมูลในขั้นตอนแรก
- ความกังวลเกี่ยวกับความปลอดภัยและการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ปัญหาการสื่อสารที่ไม่ชัดเจนระหว่างเจ้าของข้อมูลกับองค์กร

4. ปัญหาและอุปสรรคที่พบ

- ระยะเวลาการดำเนินงานบางคำขอล่าช้าเนื่องจากข้อมูลไม่ครบถ้วน
- ขาดระบบแจ้งเตือนอัตโนมัติสำหรับติดตามสถานะคำขอ
- บุคลากรมีความรู้ไม่เท่ากันในการจัดการคำขอที่ซับซ้อน

5. แนวทางปรับปรุง

- พัฒนาระบบแจ้งเตือนและติดตามคำขอแบบอัตโนมัติ เพื่อเพิ่มความรวดเร็วและความถูกต้อง
- จัดทำคำชี้แจงที่ชัดเจนเกี่ยวกับวัตถุประสงค์การเก็บและใช้ข้อมูลแก่เจ้าของข้อมูลตั้งแต่ขั้นตอนแรก
- เพิ่มการฝึกอบรมพนักงานให้มีความรู้และความเข้าใจเชิงลึกในประเด็นกฎหมายและเทคนิคการจัดการคำขอ
- จัดทำ FAQ หรือคู่มือคำถามที่พบบ่อย เพื่อให้เจ้าของข้อมูลเข้าใจขั้นตอนและลดคำขอซ้ำซ้อน

สรุปและวิเคราะห์แนวโน้มการขอใช้สิทธิข้อมูลส่วนบุคคล

จากการวิเคราะห์ข้อมูลคำขอใช้สิทธิในไตรมาสที่ 2 ปีงบประมาณ 2568 พบว่าแนวโน้มคำขอใช้สิทธิมีการเปลี่ยนแปลงและขยายตัวอย่างต่อเนื่อง โดยมีลักษณะสำคัญดังนี้

แนวโน้มประเภทคำขอใช้สิทธิที่เพิ่มขึ้น

คำขอประเภท “ขอเข้าถึงข้อมูลส่วนบุคคล” ยังคงเป็นคำขอที่พบมากที่สุด เนื่องจากเจ้าของข้อมูลต้องการตรวจสอบข้อมูลส่วนบุคคลที่องค์กรเก็บรวบรวมว่าถูกต้อง ครบถ้วน และมีการใช้ข้อมูลไปในวัตถุประสงค์ที่ชัดเจนหรือไม่ อีกทั้งคำขอประเภท “ขอแก้ไขข้อมูล” และ “ขอให้ลบข้อมูล” มีแนวโน้มเพิ่มขึ้นสอดคล้องกับการตระหนักรู้ของเจ้าของข้อมูลที่สูงขึ้นเกี่ยวกับสิทธิของตนเองตามกฎหมาย

เหตุผลสำคัญของคำขอใช้สิทธิ

- ความไม่มั่นใจในความถูกต้องของข้อมูล: เจ้าของข้อมูลต้องการตรวจสอบความถูกต้องและความเป็นปัจจุบัน
- ของข้อมูลส่วนบุคคล เพื่อป้องกันการนำข้อมูลไปผิดพลาดส่งผลกระทบต่อสิทธิและผลประโยชน์ของตนเอง

- **ความต้องการควบคุมข้อมูลส่วนบุคคล:** เจ้าของข้อมูลต้องการใช้สิทธิในการแก้ไข ลบ หรือจำกัดการใช้ข้อมูลส่วนบุคคลเพื่อป้องกันการใช้อ้างอิงข้อมูลในทางที่ไม่เหมาะสม หรือเพื่อปกป้องความเป็นส่วนตัวส่วนตัวของตนเอง
- **ความกังวลด้านความปลอดภัยและความเป็นส่วนตัว:** มีเจ้าของข้อมูลจำนวนหนึ่งที่มีความกังวลเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลในปริมาณมาก และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต จึงใช้สิทธิในการตรวจสอบและควบคุมข้อมูล
- **การตระหนักรู้เกี่ยวกับสิทธิของตนเองเพิ่มขึ้น:** จากการรณรงค์และการเผยแพร่ข้อมูลเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล เจ้าของข้อมูลเริ่มรู้จักสิทธิและกระบวนการในการใช้สิทธิมากขึ้น ส่งผลให้มีคำขอใช้สิทธิในทุกประเภทเพิ่มจำนวนขึ้น

ปัจจัยส่งผลกระทบต่อปริมาณคำขอ

- การเปิดเผยข้อมูลในช่องทางสื่อสังคมออนไลน์และช่องทางดิจิทัลอื่น ๆ ส่งผลให้เจ้าของข้อมูลมีความสนใจและความกังวลต่อการใช้อ้างอิงข้อมูลส่วนบุคคลมากขึ้น
- การดำเนินงานขององค์กรที่เกี่ยวข้องกับการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลอย่างต่อเนื่อง ส่งผลให้มีคำถามและข้อสงสัยจากเจ้าของข้อมูลที่ต้องการใช้สิทธิในการตรวจสอบ
- ความซับซ้อนและความไม่ชัดเจนในบางกระบวนการขององค์กร อาจทำให้เจ้าของข้อมูลต้องการสอบถามหรือขอคำชี้แจงเพิ่มเติมผ่านการใช้สิทธิ

ผลกระทบและข้อเสนอแนะ

แนวโน้มคำขอใช้สิทธิที่เพิ่มขึ้นถือเป็นสัญญาณที่ดีที่สะท้อนการรับรู้สิทธิของเจ้าของข้อมูล แต่ก็มีความท้าทายสำหรับองค์กรในการบริหารจัดการคำขอให้มีประสิทธิภาพและรวดเร็ว เพื่อรักษาความเชื่อมั่นและปฏิบัติตามกฎหมายอย่างถูกต้อง โดยองค์กรควรเร่งพัฒนาระบบการจัดการคำขอ และสื่อสารข้อมูลที่ชัดเจนกับเจ้าของข้อมูล รวมทั้งเพิ่มประสิทธิภาพของบุคลากรที่เกี่ยวข้อง เพื่อลดปัญหาความล่าช้าและความสับสนในกระบวนการ

ผู้จัดทำรายงาน

นางสาวสุภาวดี คำแก้ว

เจ้าหน้าที่วิเคราะห์ข้อมูลคุ้มครองข้อมูลส่วนบุคคล

วันที่จัดทำรายงาน: 15 มิถุนายน 2568

4.6.1 องค์กรมีขั้นตอนและกระบวนการตามความเหมาะสม ได้สัดส่วนและสมเหตุสมผลในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่เก็บไว้ และหากจำเป็น ก็สามารถทำการแก้ไขข้อมูลนั้นได้

สิ่งที่ต้องทำ: มีขั้นตอนและระบบเทคโนโลยีสารสนเทศในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล

- ที่มีการเก็บรวบรวม
- หลักฐาน: เอกสารแสดงขั้นตอนและกระบวนการในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมระบบเทคโนโลยีสารสนเทศในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35 มาตรา 36 โทษทางปกครองในกรณีที่ไม่ปฏิบัติตามมาตรา 35 มาตรา 36 ซึ่งมีความเชื่อมโยงกับมาตรา 39 กำหนดโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

การตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล

1. เอกสารแสดงขั้นตอนและกระบวนการในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

หัวข้อ: ขั้นตอนการตรวจสอบและแก้ไขข้อมูลส่วนบุคคล

วัตถุประสงค์: เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่องค์กรเก็บรวบรวมมีความถูกต้อง ครบถ้วน และทันสมัย สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35 และ 36

รายละเอียดขั้นตอน:

1. การกำหนดความถี่ในการตรวจสอบข้อมูล

กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลเป็นระยะเวลาอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีคำขอแก้ไขข้อมูลจากเจ้าของข้อมูล

2. การใช้ระบบเทคโนโลยีสารสนเทศในการตรวจสอบ

ใช้ระบบฐานข้อมูลกลาง (Database Management System) ที่มีฟังก์ชันตรวจสอบความสมบูรณ์ของข้อมูล เช่น การแจ้งเตือนข้อมูลผิดพลาด ข้อมูลซ้ำซ้อน หรือข้อมูลที่มีค่าไม่สมเหตุผล

3. การแจ้งเตือนและการสอบทานข้อมูลที่ผิดปกติ

ระบบจะแจ้งเตือนเจ้าหน้าที่ผู้รับผิดชอบเมื่อพบข้อมูลที่ผิดปกติ เช่น วันที่เกิดเหตุการณ์ไม่สมเหตุผล หรือข้อมูลที่ขัดแย้งกับฐานข้อมูลอื่น

4. การดำเนินการตรวจสอบโดยเจ้าหน้าที่

เจ้าหน้าที่จะตรวจสอบข้อมูลตามแจ้งเตือน พร้อมประสานกับเจ้าของข้อมูลเพื่อตรวจสอบและยืนยันความถูกต้อง

5. การแก้ไขข้อมูล

หากพบว่าข้อมูลไม่ถูกต้อง เจ้าหน้าที่จะดำเนินการแก้ไขข้อมูลตามคำร้องของเจ้าของข้อมูล โดยต้องบันทึกข้อมูลการแก้ไข พร้อมเหตุผลและวันที่แก้ไขไว้ในระบบ

6. การเก็บบันทึกประวัติการตรวจสอบและแก้ไขข้อมูล

ระบบจะเก็บประวัติการตรวจสอบและแก้ไขข้อมูลเพื่อใช้เป็นหลักฐาน และตรวจสอบย้อนหลังได้

7. การประเมินและปรับปรุงกระบวนการ

หน่วยงานควบคุมคุณภาพข้อมูลจะจัดทำรายงานประเมินประสิทธิภาพของกระบวนการตรวจสอบข้อมูล และปรับปรุงระบบอย่างสม่ำเสมอ

2. ระบบเทคโนโลยีสารสนเทศในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล

ชื่อระบบ: ระบบบริหารจัดการข้อมูลส่วนบุคคล (Personal Data Management System - PDMS)

ฟังก์ชันหลักที่เกี่ยวข้อง:

- ตรวจสอบความสมบูรณ์ของข้อมูล (Data Integrity Check)
- แจ้งเตือนข้อมูลซ้ำหรือผิดพลาด

- ระบบอนุญาตการแก้ไขข้อมูลตามคำขอที่ได้รับอนุมัติ
- บันทึกประวัติการแก้ไขข้อมูล (Audit Trail)
- รายงานสถานะและผลการตรวจสอบข้อมูลเป็นรายงวด

ตัวอย่างภาพหน้าจอระบบ:

- หน้าจอแสดงรายการข้อมูลที่มีการแจ้งเตือนความผิดปกติ
- หน้าจอแบบฟอร์มยืนยันข้อมูลจากเจ้าของข้อมูล
- หน้าจอบันทึกประวัติการแก้ไขข้อมูลพร้อมรายละเอียดวันที่และผู้ดำเนินการ

สรุป

ด้วยขั้นตอนและระบบเทคโนโลยีสารสนเทศดังกล่าว องค์กรสามารถตรวจสอบและรักษาความถูกต้องของข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ ลดความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล และปฏิบัติตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ครบถ้วน พร้อมบันทึกหลักฐานที่ชัดเจนสำหรับการตรวจสอบภายในและภายนอก

4.6.2 หากองค์กรมั่นใจว่าข้อมูลถูกต้องแล้ว จะต้อง มีขั้นตอนในการอธิบายและแจ้งแก่เจ้าของข้อมูลส่วนบุคคล นอกจากนี้ องค์กรต้องแจ้งสิทธิของบุคคลนั้นในการร้องเรียน (มาตรา 73) และควรบันทึกลงในระบบว่าบุคคลนั้นมีข้อโต้แย้งเกี่ยวกับความถูกต้องของข้อมูลตามหลักการปฏิบัติที่ดี

สิ่งที่ต้องทำ: มีขั้นตอนในการอธิบายความถูกต้องและแจ้งไปยังเจ้าของข้อมูลส่วนบุคคล

หลักฐาน: เอกสารขั้นตอนในการอธิบายความถูกต้องของข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35 มาตรา 36 มาตรา 39
โทษทางปกครองในกรณีที่ไม่ปฏิบัติตามมาตรา 35 มาตรา 36 และมาตรา 39 กำหนดโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

หลักฐานข้อ 4.6.2 ขั้นตอนการอธิบายความถูกต้องของข้อมูลส่วนบุคคลและการแจ้งสิทธิการร้องเรียน

1. เอกสารขั้นตอนในการอธิบายความถูกต้องของข้อมูลส่วนบุคคลและการแจ้งสิทธิของเจ้าของข้อมูล

หัวข้อ: ขั้นตอนการแจ้งความถูกต้องของข้อมูลส่วนบุคคลและสิทธิในการร้องเรียน

วัตถุประสงค์: เพื่อให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบถึงความถูกต้องของข้อมูลที่เก็บไว้ พร้อมแจ้งสิทธิในการร้องเรียนตามกฎหมาย และจัดเก็บบันทึกข้อโต้แย้ง (ถ้ามี) เพื่อปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35, 36 และ 39

รายละเอียดขั้นตอน:

1. การตรวจสอบและยืนยันความถูกต้องของข้อมูล

เจ้าหน้าที่ตรวจสอบข้อมูลส่วนบุคคลตามคำร้องขอแก้ไข หรือประจำรอบตรวจสอบข้อมูล

2. การจัดทำเอกสารชี้แจง

หากพบว่าข้อมูลถูกต้อง เจ้าหน้าที่จัดทำเอกสารอธิบายสาเหตุและเหตุผลที่ยืนยันความถูกต้องของข้อมูล พร้อมระบุรายละเอียดข้อมูลที่ตรวจสอบ

3. การแจ้งเจ้าของข้อมูลส่วนบุคคล

ส่งเอกสารชี้แจงความถูกต้องของข้อมูลให้เจ้าของข้อมูลผ่านช่องทางที่ตกลงกันได้ เช่น อีเมล จดหมาย หรือระบบออนไลน์ขององค์กร

4. การแจ้งสิทธิในการร้องเรียน

แจ้งให้เจ้าของข้อมูลทราบถึงสิทธิในการร้องเรียนต่อหน่วยงานกำกับดูแลข้อมูลส่วนบุคคล ตามมาตรา 73 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยระบุช่องทางและวิธีการร้องเรียนอย่างชัดเจน

5. การบันทึกข้อโต้แย้ง (ถ้ามี)

หากเจ้าของข้อมูลมีข้อโต้แย้งเกี่ยวกับความถูกต้องของข้อมูล ให้เจ้าหน้าที่บันทึกข้อโต้แย้งดังกล่าวลงในระบบฐานข้อมูล พร้อมบันทึกวันที่และรายละเอียดของข้อโต้แย้ง เพื่อเป็นหลักฐานและใช้ปรับปรุงข้อมูลต่อไป

6. การติดตามและประเมินผล

เจ้าหน้าที่จะติดตามผลการร้องเรียนและข้อโต้แย้งจนกว่าจะได้ข้อยุติ และรายงานผลให้เจ้าของข้อมูลทราบอย่างสม่ำเสมอ

2. ตัวอย่างแบบฟอร์มแจ้งความถูกต้องของข้อมูลและสิทธิในการร้องเรียน

รายละเอียด ข้อมูล	คำชี้แจงความถูกต้อง	สิทธิในการร้องเรียน
ชื่อ-นามสกุล	ข้อมูลตรงตามที่เจ้าของ ข้อมูลให้ไว้ ณ วันที่ ตรวจสอบ	เจ้าของข้อมูลมีสิทธิร้องเรียนต่อ สคบ. หรือหน่วยงาน กำกับดูแลข้อมูลส่วนบุคคลภายใน 30 วันนับจากวันที่ ได้รับแจ้ง
วันเดือนปีเกิด	ถูกต้องและได้รับการยืนยัน จากเอกสารที่เกี่ยวข้อง	ช่องทางการร้องเรียน: เว็บไซต์ สคบ. อีเมล หรือ หมายเลขโทรศัพท์
ที่อยู่	ข้อมูลถูกต้องตามหลักฐานที่ เจ้าของข้อมูลส่งให้	-

3. ข้อกฎหมายที่เกี่ยวข้อง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- มาตรา 35: เจ้าของข้อมูลมีสิทธิขอให้แก้ไขข้อมูลที่ไม่ถูกต้อง
- มาตรา 36: เจ้าของข้อมูลมีสิทธิขอให้ลบหรือทำลายข้อมูลที่ผิดกฎหมาย
- มาตรา 39: องค์กรต้องจัดให้มีมาตรการและบันทึกการปฏิบัติตามสิทธิของเจ้าของข้อมูล
- มาตรา 73: เจ้าของข้อมูลมีสิทธิร้องเรียนต่อหน่วยงานกำกับดูแลข้อมูลส่วนบุคคล

4.6.3 หากข้อมูลส่วนบุคคลได้รับการเปิดเผยให้กับผู้อื่น องค์กรจะต้องติดต่อแต่ละผู้รับข้อมูลเพื่อแจ้งให้ทราบถึงการแก้ไขข้อมูลนั้น เว้นแต่ว่าจะเป็นไปไม่ได้หรือมีความพยายามที่ไม่สมเหตุผล

สิ่งที่ต้องทำ: มีขั้นตอนในการดำเนินการแจ้งต่อผู้รับข้อมูลในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น โดยมีแบบฟอร์มการแจ้งที่ชัดเจน

หลักฐาน: แบบฟอร์มการแจ้งต่อผู้รับข้อมูล ในกรณีข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ขั้นตอนและแบบฟอร์มการแจ้งผู้รับข้อมูลกรณีข้อมูลส่วนบุคคลถูกแก้ไขหลังจากเปิดเผย

1. เอกสารขั้นตอนการแจ้งผู้รับข้อมูลเมื่อมีการแก้ไขข้อมูลส่วนบุคคล

หัวข้อ: ขั้นตอนการแจ้งผู้รับข้อมูลส่วนบุคคลเมื่อมีการแก้ไขข้อมูลหลังการเปิดเผย

วัตถุประสงค์: เพื่อให้แน่ใจว่าผู้รับข้อมูลส่วนบุคคลได้รับแจ้งการแก้ไขข้อมูลที่ถูกเปิดเผยไปแล้วอย่างเหมาะสม ยกเว้นกรณีที่ไม่สามารถดำเนินการได้หรือมีความพยายามที่ไม่สมเหตุผล

รายละเอียดขั้นตอน:

1. ตรวจสอบรายการผู้รับข้อมูล

เจ้าหน้าที่รวบรวมรายชื่อและช่องทางการติดต่อของผู้รับข้อมูลส่วนบุคคลที่ได้รับข้อมูลนั้นไปก่อนหน้านี้

2. จัดทำเอกสารแจ้งการแก้ไขข้อมูล

จัดทำแบบฟอร์มแจ้งข้อมูลที่ถูกแก้ไขโดยระบุข้อมูลเดิม ข้อมูลใหม่ วันที่แก้ไข และเหตุผลการแก้ไข

3. ส่งแจ้งให้ผู้รับข้อมูลทราบ

แจ้งผ่านช่องทางที่เหมาะสม เช่น อีเมล จดหมาย หรือระบบสื่อสารภายในองค์กร พร้อมแนบเอกสารแจ้งการแก้ไข

4. บันทึกการแจ้ง

บันทึกข้อมูลการแจ้งไว้ในระบบฐานข้อมูล รวมถึงวันที่แจ้ง วิธีการแจ้ง และชื่อผู้รับข้อมูลที่ได้รับแจ้ง

5. กรณีไม่สามารถแจ้งได้

หากมีเหตุผลที่ไม่สามารถแจ้งผู้รับข้อมูลได้ เช่น ขาดช่องทางการติดต่อ หรือมีความพยายามที่ไม่สมเหตุผล เจ้าหน้าที่ต้องบันทึกเหตุผลประกอบไว้เป็นหลักฐาน

2. ตัวอย่างแบบฟอร์มแจ้งการแก้ไขข้อมูลส่วนบุคคลให้ผู้รับข้อมูลทราบ

แบบฟอร์มแจ้งการแก้ไขข้อมูลส่วนบุคคล

เรียน ผู้รับข้อมูลที่เคารพ

ด้วยทางองค์กรได้ดำเนินการแก้ไขข้อมูลส่วนบุคคลที่ท่านได้รับจากองค์กรของเรา รายละเอียดข้อมูลที่แก้ไขมีดังนี้

รายการข้อมูล	ข้อมูลเดิม	ข้อมูลใหม่	วันที่แก้ไข	เหตุผลในการแก้ไข
ชื่อ	สมชาย	สมศักดิ์	1 มิถุนายน 2568	แก้ไขข้อมูลตามคำขอเจ้าของข้อมูล
ที่อยู่	123 หมู่ 5	456 หมู่	1 มิถุนายน 2568	อัปเดตข้อมูลที่อยู่ใหม่

กรุณาทราบว่า การแก้ไขข้อมูลนี้มีผลต่อการใช้ข้อมูลส่วนบุคคลตามข้อตกลงที่ได้กำหนดไว้ หากท่านมีข้อสงสัยหรือต้องการสอบถามข้อมูลเพิ่มเติม สามารถติดต่อเจ้าหน้าที่ผู้ดูแลข้อมูลส่วนบุคคลได้ที่ [ช่องทางติดต่อ เช่น อีเมล เบอร์โทรศัพท์]

ขอแสดงความนับถือ

[ชื่อผู้รับผิดชอบ]

[ตำแหน่ง]

[ชื่อองค์กร]

[วันที่]

4.6.4 หากถูกขอ องค์กรสามารถระบุและแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่าบุคคลที่สามารถรายใดได้รับข้อมูลส่วนบุคคลไปบ้าง

สิ่งที่ต้องทำ: มีขั้นตอนและการทำบันทึกแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่าบุคคลที่สามารถรายใดได้รับข้อมูลส่วนบุคคลใดบ้าง โดยมีแบบฟอร์มการแจ้งที่ชัดเจน

หลักฐาน: บันทึกการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลในกรณีข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ขั้นตอนและแบบฟอร์มการแจ้งเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการเปิดเผยข้อมูลให้บุคคลที่สาม

1. เอกสารขั้นตอนการแจ้งเจ้าของข้อมูลส่วนบุคคลกรณีข้อมูลถูกเปิดเผยต่อบุคคลที่สาม

หัวข้อ: ขั้นตอนการแจ้งเจ้าของข้อมูลส่วนบุคคลเมื่อมีการเปิดเผยข้อมูลให้บุคคลที่สาม

วัตถุประสงค์: เพื่อให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบว่าข้อมูลของตนได้ถูกเปิดเผยให้บุคคลที่สามรายใดบ้างอย่างชัดเจนและโปร่งใส

รายละเอียดขั้นตอน

1. ตรวจสอบข้อมูลการเปิดเผย

เจ้าหน้าที่รวบรวมข้อมูลบุคคลที่สามที่ได้รับข้อมูลส่วนบุคคลของเจ้าของข้อมูลตามคำขอหรือการดำเนินงาน

2. จัดทำรายงานข้อมูลการเปิดเผย

รวบรวมรายการข้อมูลที่ถูกเปิดเผย รายชื่อบุคคลที่สาม วันที่เปิดเผย และวัตถุประสงค์ของการเปิดเผย

3. จัดทำเอกสารแจ้งเจ้าของข้อมูล

จัดทำแบบฟอร์มแจ้งข้อมูลการเปิดเผยที่ชัดเจนและเข้าใจง่าย

4. ส่งแจ้งให้เจ้าของข้อมูล

แจ้งผ่านช่องทางที่เจ้าของข้อมูลระบุ เช่น อีเมล จดหมาย หรือระบบออนไลน์ พร้อมแนบเอกสาร

5. บันทึกการแจ้ง

บันทึกข้อมูลการแจ้งไว้ในระบบ รวมถึงวันที่ แจ้งช่องทาง และชื่อเจ้าของข้อมูลที่ได้รับแจ้ง

2. ตัวอย่างแบบฟอร์มแจ้งการเปิดเผยข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบ

แบบฟอร์มแจ้งการเปิดเผยข้อมูลส่วนบุคคล

เรียน เจ้าของข้อมูลส่วนบุคคลที่เคารพ

ทางองค์กรขอแจ้งให้ท่านทราบว่า ข้อมูลส่วนบุคคลของท่านได้ถูกเปิดเผยให้กับบุคคลที่สามตามรายละเอียดดังนี้

รายชื่อบุคคลที่สาม	ข้อมูลส่วนบุคคลที่เปิดเผย	วันที่เปิดเผย	วัตถุประสงค์ของการเปิดเผย
บริษัท ABC จำกัด	ชื่อ ที่อยู่ เบอร์โทร	10 พฤษภาคม 2568	เพื่อวัตถุประสงค์ในการจัดส่งสินค้า
บริษัท XYZ จำกัด	ชื่อ อีเมล	15 พฤษภาคม 2568	เพื่อวัตถุประสงค์ในการให้บริการลูกค้า

หากท่านมีข้อสงสัยหรือต้องการข้อมูลเพิ่มเติม กรุณาติดต่อเจ้าหน้าที่ผู้ดูแลข้อมูลส่วนบุคคลได้ที่ [ช่องทางติดต่อ]

ขอแสดงความนับถือ

[ชื่อผู้รับผิดชอบ]

[ตำแหน่ง]

[ชื่อองค์กร]

[วันที่]

4.7.1 องค์กรจะลบข้อมูลส่วนบุคคลจากระบบสำรองข้อมูล รวมถึงระบบที่ใช้งานอยู่เมื่อจำเป็น และทำการชี้แจงให้บุคคลนั้นทราบอย่างชัดเจนว่าข้อมูลของพวกเขาจะถูกจัดการอย่างไร

สิ่งที่ต้องทำ: มีการดำเนินการแก่เจ้าของข้อมูลส่วนบุคคลที่ขอใช้สิทธิดำเนินการลบข้อมูลส่วนบุคคลออกจากระบบสำรองและระบบใช้งานจริง โดยใช้ระบบเทคโนโลยีสารสนเทศ

- หลักฐาน:
- 1) แบบฟอร์มการขอใช้สิทธิลบข้อมูลส่วนบุคคล
 - 2) แบบฟอร์มและเอกสารสำหรับชี้แจงแก่เจ้าของข้อมูลส่วนบุคคลเกี่ยวกับขั้นตอนหรือวิธีการในการลบหรือทำลายข้อมูลส่วนบุคคล
 - 3) ระบบเทคโนโลยีสารสนเทศในการลบข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22, 27 และ 33 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567 ข้อ 3

โทษทางปกครอง ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 33 กำหนดโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

แบบฟอร์มการขอใช้สิทธิลบข้อมูลส่วนบุคคล

ชื่อ-นามสกุล: _____

เลขบัตรประชาชน/หนังสือเดินทาง: _____

เบอร์ติดต่อ: _____

อีเมล: _____

วันที่ขอใช้สิทธิ: _____

รายละเอียดข้อมูลส่วนบุคคลที่ต้องการลบ:

เหตุผลในการขอลบข้อมูล:

ข้าพเจ้ายินยอมให้ตรวจสอบข้อมูลดังกล่าวและดำเนินการลบข้อมูลตามคำขอ

ลงชื่อ _____ (ผู้ขอใช้สิทธิ)

วันที่ _____

แบบฟอร์มและเอกสารชี้แจงขั้นตอนการลบข้อมูลแก่เจ้าของข้อมูล

เอกสารชี้แจงการดำเนินการลบข้อมูลส่วนบุคคล

เรียน เจ้าของข้อมูลส่วนบุคคลที่เคารพ

ตามคำขอใช้สิทธิลบข้อมูลส่วนบุคคลของท่าน ทางองค์กรขอแจ้งให้ทราบว่า ข้อมูลส่วนบุคคลของท่านจะถูกดำเนินการลบออกจากระบบใช้งานจริงและระบบสำรองข้อมูล (Backup) การลบข้อมูลจะดำเนินการโดยใช้ระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและได้มาตรฐาน เพื่อให้มั่นใจว่าข้อมูลจะไม่สามารถกู้คืนได้หลังจากถูกลบ

การดำเนินการลบข้อมูลนี้อาจใช้เวลาประมาณ [ระบุจำนวนวันทำการ] วันทำการ หากมีข้อสงสัยหรือข้อร้องเรียน กรุณาติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลผ่านช่องทาง [ช่องทางติดต่อ]

ขอขอบพระคุณที่ให้ความร่วมมือ

ขอแสดงความนับถือ

[ชื่อผู้รับผิดชอบ]

[ตำแหน่ง]

[ชื่อองค์กร]

[วันที่]

ระบบเทคโนโลยีสารสนเทศในการลบข้อมูลส่วนบุคคล

รายละเอียดระบบเทคโนโลยีสารสนเทศที่ใช้ในการลบข้อมูล

- ใช้ซอฟต์แวร์บริหารจัดการข้อมูลที่รองรับการลบข้อมูลแบบถาวร (Data Erasure) ตามมาตรฐานสากล เช่น DoD 5220.22-M หรือ NIST SP 800-88
- ระบบสำรองข้อมูล (Backup System) มีฟังก์ชันการลบข้อมูลแบบครบถ้วน รวมทั้งระบบอัตโนมัติในการจัดเก็บและลบข้อมูลที่หมดอายุหรือได้รับคำขอ
- มีระบบบันทึกประวัติการลบข้อมูล (Audit Log) เพื่อแสดงหลักฐานว่าข้อมูลส่วนบุคคลได้ถูกลบอย่างสมบูรณ์ในวันและเวลาที่ระบุ
- เจ้าหน้าที่ฝ่าย IT และฝ่ายคุ้มครองข้อมูลส่วนบุคคลได้รับการอบรมและมีขั้นตอนปฏิบัติในการดำเนินการลบข้อมูลอย่างเคร่งครัด

4.7.2 หากข้อมูลส่วนบุคคลได้รับการเผยแพร่สู่สาธารณะในรูปแบบออนไลน์ องค์กรจะดำเนินการตามขั้นตอนที่เหมาะสมเพื่อแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นทราบ เพื่อให้ลบลิงก์ที่เชื่อมโยงไปยังข้อมูลหยุดการคัดลอก หรือหยุดการทำซ้ำข้อมูลนั้น

สิ่งที่ต้องทำ: มีการใช้ระบบเทคโนโลยีสารสนเทศในการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นทราบ เพื่อให้ลบลิงก์ที่เชื่อมโยงไปยังข้อมูล หยุดการคัดลอก หรือหยุดการทำซ้ำข้อมูลนั้น

หลักฐาน: บันทึกการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลในกรณีข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น ระบบในการดำเนินการลบลิงก์ที่เชื่อมโยงไปยังข้อมูล หยุดการคัดลอก หรือหยุดการทำซ้ำข้อมูลนั้น ในกรณีที่ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยต่อสาธารณะ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 วรรคสาม

1. บันทึกการแจ้งต่อเจ้าของข้อมูลส่วนบุคคล

บันทึกการแจ้งกรณีข้อมูลส่วนบุคคลเผยแพร่สู่สาธารณะ

ชื่อเจ้าของข้อมูล: _____

วันที่แจ้ง: _____

ช่องทางเผยแพร่ข้อมูล: _____

รายละเอียดข้อมูลที่เผยแพร่: _____

ลิงก์ที่เกี่ยวข้อง: _____

องค์กรได้ดำเนินการแจ้งผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นที่เกี่ยวข้อง เพื่อขอให้ดำเนินการลบลิงก์ หยุดการคัดลอก หรือหยุดการเข้าถึงข้อมูลดังกล่าว โดยรายละเอียดของการดำเนินการมีดังนี้

วันที่แจ้งผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น: _____

ช่องทางการแจ้ง (อีเมล/จดหมาย/ระบบอิเล็กทรอนิกส์): _____

ผู้รับแจ้ง: _____

สถานะการดำเนินการ:

☐ ดำเนินการลบลิงก์เรียบร้อยแล้ว

☐ อยู่ระหว่างดำเนินการ

☐ ไม่สามารถดำเนินการได้ (เหตุผล: _____)

ลงชื่อผู้รายงาน _____

ตำแหน่ง _____

วันที่ _____

2. ระบบเทคโนโลยีสารสนเทศในการแจ้งและดำเนินการลบลิงก์/หยุดการทำซ้ำข้อมูล

รายละเอียดระบบการจัดการลบข้อมูลเผยแพร่สู่สาธารณะ

- ระบบแจ้งเตือนอัตโนมัติ (Automated Notification System) ใช้ส่งคำขอลบลิงก์หรือหยุดการคัดลอกไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นผ่านอีเมลหรือแพลตฟอร์มบริหารจัดการข้อมูล
- มีระบบติดตามสถานะการแจ้งเตือนและการตอบกลับจากผู้รับแจ้งอย่างเป็นระบบ (Tracking & Audit Log) เพื่อให้สามารถตรวจสอบความคืบหน้าและความสมบูรณ์ของการดำเนินงานได้
- ใช้เครื่องมือด้านความปลอดภัยและป้องกันการทำซ้ำข้อมูล เช่น การตั้งค่าการเข้าถึง การป้องกันการดาวน์โหลด หรือการใช้งานลิงก์แบบมีเวลาจำกัด (Expiring Links)
- มีเจ้าหน้าที่รับผิดชอบติดตามและประสานงานในกรณีที่ผู้ควบคุมข้อมูลรายอื่นไม่ดำเนินการตามคำขอ
- ระบบสามารถสร้างรายงานสรุปการดำเนินงานและแจ้งเตือนเจ้าหน้าที่เมื่อมีการละเมิดซ้ำ

4.7.3 หากข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น องค์กรจะติดต่อผู้รับแต่ละรายเพื่อแจ้งให้ทราบเกี่ยวกับการลบหรือทำลาย เว้นแต่จะเป็นการเปิดเผยโดยที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลมีบทบัญญัติหรือให้อำนาจเปิดเผยได้

สิ่งที่ต้องทำ: มีการทำบันทึกแจ้งต่อผู้รับแต่ละราย ในกรณีข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น โดยมีแบบฟอร์มการแจ้งที่ชัดเจน

หลักฐาน: บันทึกการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลในกรณีข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 วรรคสาม
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567

บันทึกการแจ้งผู้รับข้อมูลส่วนบุคคลกรณีลบหรือทำลายข้อมูล

ข้อมูลเจ้าของข้อมูลส่วนบุคคล

ชื่อเจ้าของข้อมูล: _____

วันที่ได้รับคำขอใช้สิทธิ: _____

ประเภทข้อมูลส่วนบุคคล: _____

ช่องทางเผยแพร่ข้อมูล: _____

ข้อมูลผู้รับข้อมูลส่วนบุคคล

ชื่อผู้รับข้อมูล: _____

หน่วยงาน/บริษัท: _____

วันที่ได้รับข้อมูล: _____

ลักษณะการเปิดเผยข้อมูล: _____

รายละเอียดการแจ้งลบ/ทำลายข้อมูล

องค์กรได้ดำเนินการแจ้งผู้รับข้อมูลส่วนบุคคลรายนี้ เพื่อแจ้งให้ทราบเกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคลที่ได้รับเปิดเผยแล้ว โดยมีรายละเอียดดังนี้

วันที่แจ้ง: _____

วิธีการแจ้ง (เช่น อีเมล จดหมาย โทรศัพท์): _____

เนื้อหาการแจ้ง:

แจ้งให้ลบข้อมูลส่วนบุคคลตามคำขอใช้สิทธิ

แจ้งให้ทำลายหรือไม่ใช้ข้อมูลส่วนบุคคลดังกล่าวต่อไป

แจ้งข้อกำหนดตามกฎหมายที่เกี่ยวข้อง

การตอบกลับจากผู้รับข้อมูล:

☐ ยืนยันลบ/ทำลายข้อมูลแล้ว

☐ อยู่ระหว่างดำเนินการ

☐ ไม่สามารถดำเนินการได้ (ระบุเหตุผล): _____

ลงชื่อผู้รายงาน _____

ตำแหน่ง _____

วันที่ _____

เอกสารแนบท้าย

- แบบฟอร์มแจ้งลบ/ทำลายข้อมูลส่วนบุคคล (Template)

- แนวทางและกระบวนการติดต่อแจ้งผู้รับข้อมูลส่วนบุคคล
- รายการตรวจสอบการดำเนินการตามคำขอใช้สิทธิ

4.7.4 หากถูกร้องขอ องค์กรสามารถระบุและแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบได้ว่าบุคคลที่สามหรือผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นใดที่ได้รับข้อมูลส่วนบุคคลไป

- สิ่งที่ต้องทำ: มีบันทึกแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบได้ว่าบุคคลที่สามหรือผู้ควบคุมข้อมูลส่วนบุคคลรายใดได้รับข้อมูลส่วนบุคคลบ้าง โดยมีแบบฟอร์มที่ชัดเจน
- หลักฐาน: เอกสารหรือหลักฐานแสดงการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงรายชื่อของบุคคลที่สาม หรือผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นที่เปิดเผยข้อมูลส่วนบุคคลไป
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

บันทึกแจ้งเจ้าของข้อมูลส่วนบุคคลกรณีเปิดเผยข้อมูลให้บุคคลที่สามหรือผู้ควบคุมข้อมูลรายอื่น

ข้อมูลเจ้าของข้อมูลส่วนบุคคล

ชื่อเจ้าของข้อมูล: _____

เลขที่คำขอใช้สิทธิ: _____

วันที่ร้องขอข้อมูล: _____

รายละเอียดข้อมูลส่วนบุคคลที่เปิดเผย

ประเภทข้อมูลส่วนบุคคล: _____

วันที่เปิดเผยข้อมูล: _____

รายชื่อบุคคลที่สามหรือผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นที่ได้รับข้อมูล

ลำดับ ที่	ชื่อบุคคลที่สาม/ผู้ควบคุมข้อมูลราย อื่น	หน่วยงาน/ บริษัท	วันที่เปิดเผย ข้อมูล	หมายเหตุ (ถ้ามี)
1	_____	_____	_____	_____
2	_____	_____	_____	_____
3	_____	_____	_____	_____

ข้อความแจ้งเจ้าของข้อมูล

เรียน คุณ _____

ตามที่ท่านได้ร้องขอข้อมูลเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลของท่าน ทางองค์กรขอแจ้งให้ทราบว่า ข้อมูลส่วนบุคคลของท่านได้ถูกเปิดเผยต่อบุคคลที่สามหรือผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น ดังรายละเอียดตามตารางข้างต้น

หากท่านมีข้อสงสัยหรือต้องการข้อมูลเพิ่มเติม กรุณาติดต่อ _____ (ชื่อ
เจ้าหน้าที่) โทรศัพท์ _____ หรืออีเมล _____

ขอแสดงความนับถือ

(ชื่อผู้แจ้ง)

ตำแหน่ง _____

วันที่ _____

ลงชื่อเจ้าของข้อมูล (เพื่อยืนยันการรับแจ้ง)

ลงชื่อ _____

วันที่ _____

เอกสารแนบท้าย

- แบบฟอร์มแจ้งรายชื่อผู้รับข้อมูลส่วนบุคคล
- รายงานการดำเนินการตามคำขอ

หมายเหตุ

- เอกสารนี้เป็นไปตามข้อกำหนดการบริหารจัดการข้อมูลส่วนบุคคลขององค์กร
- กฎหมายไม่ได้กำหนดเฉพาะเจาะจง แต่เป็นการปฏิบัติที่ดีเพื่อความโปร่งใสและสร้างความเชื่อมั่นกับเจ้าของข้อมูล

4.7.5 องค์กรให้ความสำคัญเป็นพิเศษกับคำขอให้ลบซึ่งเกี่ยวเนื่องกับความยินยอมของผู้เยาว์ โดยเฉพาะอย่างยิ่งเมื่อเป็นการประมวลผลข้อมูลส่วนบุคคลใด ๆ บนอินเทอร์เน็ต (มี "ความยินยอม" เป็นฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์)

สิ่งที่ต้องทำ: มีการขอความยินยอมจากผู้ปกครองของผู้เยาว์ ในกรณีผู้ขอลบข้อมูลส่วนบุคคลเป็นผู้เยาว์ โดยมีแบบฟอร์มการขอความยินยอม

หลักฐาน: แบบฟอร์มการให้ความยินยอมจากผู้ปกครองในกรณีผู้ขอลบข้อมูลส่วนบุคคลเป็นผู้เยาว์

สภาพบังคับ: กฎหมายไม่ได้กำหนด

แบบฟอร์มขอความยินยอมจากผู้ปกครองสำหรับการลบข้อมูลส่วนบุคคลของผู้เยาว์

ข้อมูลผู้เยาว์

ชื่อ-นามสกุล: _____

วันเดือนปีเกิด: _____

เลขบัตรประชาชน/เลขประจำตัวผู้เยาว์ (ถ้ามี): _____

ข้อมูลผู้ปกครอง

ชื่อ-นามสกุล: _____

ความสัมพันธ์กับผู้เยาว์: _____

หมายเลขโทรศัพท์: _____

อีเมล: _____

รายละเอียดคำขอลบข้อมูลส่วนบุคคล

วันที่ยื่นคำขอ: _____

รายละเอียดข้อมูลส่วนบุคคลที่ต้องการให้ลบ:

ข้อความขอความยินยอม

ข้าพเจ้าในฐานะผู้ปกครองของ

ชื่อ-นามสกุลผู้เยาว์: _____

ขอให้ความยินยอมในการดำเนินการลบข้อมูลส่วนบุคคลของผู้เยาว์ตามคำขอข้างต้น และรับทราบว่าการลบข้อมูลนี้จะส่งผลให้ข้อมูลส่วนบุคคลของผู้เยาว์ถูกลบออกจากฐานข้อมูลขององค์กรทั้งในระบบหลักและระบบสำรอง

ข้าพเจ้ายืนยันว่าได้ให้ความยินยอมโดยเสรี โดยไม่มีการบังคับ หรือชักจูง และเข้าใจผลกระทบของการลบข้อมูลดังกล่าว

ลงชื่อผู้ปกครอง: _____

วันที่: _____

คำชี้แจงเพิ่มเติม

องค์กรจะดำเนินการลบข้อมูลส่วนบุคคลของผู้เยาว์เมื่อได้รับความยินยอมจากผู้ปกครองแล้วเท่านั้น

หากมีข้อสงสัยเพิ่มเติม กรุณาติดต่อเจ้าหน้าที่ที่รับผิดชอบ โทรศัพท์ _____ หรือ

อีเมล _____

4.8.1 องค์กรสามารถระงับหรือจำกัดการประมวลผลข้อมูลส่วนบุคคลในลักษณะที่เหมาะสมกับประเภทของการประมวลผลและระบบที่เกี่ยวข้อง เช่น การย้ายข้อมูลไปยังระบบอื่นชั่วคราวหรือลบออกจากเว็บไซต์

สิ่งที่ต้องทำ: มีขั้นตอนในการขอใช้สิทธิในการระงับ (อาจใช้ระบบเทคโนโลยีสารสนเทศ) หรือจำกัดการประมวลผลข้อมูลส่วนบุคคล

หลักฐาน: แบบฟอร์มการขอใช้สิทธิระงับหรือจำกัดการประมวลผลข้อมูลส่วนบุคคล
ระบบเทคโนโลยีสารสนเทศในการระงับหรือจำกัดการประมวลผลข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 34
โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตามมาตรา 33 กำหนดโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

แบบฟอร์มการขอใช้สิทธิระงับหรือจำกัดการประมวลผลข้อมูลส่วนบุคคล

ข้อมูลเจ้าของข้อมูลส่วนบุคคล

ชื่อ-นามสกุล: _____

หมายเลขโทรศัพท์: _____

อีเมล: _____

เลขบัตรประชาชน/หมายเลขประจำตัวอื่น (ถ้ามี): _____

ประเภทคำขอ (โปรดเลือก)

☐ ขอระงับการประมวลผลข้อมูลส่วนบุคคล

☐ ขอจำกัดการประมวลผลข้อมูลส่วนบุคคล

รายละเอียดคำขอ

(โปรดระบุเหตุผลและข้อมูลที่ต้องการระงับหรือจำกัดการประมวลผล)

วันที่ยื่นคำขอ _____

ข้อความรับรอง

ข้าพเจ้ายืนยันว่าข้อมูลข้างต้นเป็นความจริง และขอใช้สิทธิระงับ/จำกัดการประมวลผลข้อมูลส่วนบุคคลตามคำขอข้างต้น โดยเข้าใจสิทธิและผลกระทบจากการระงับหรือจำกัดนี้

ลงชื่อเจ้าของข้อมูล: _____

วันที่: _____

ระบบเทคโนโลยีสารสนเทศในการระงับหรือจำกัดการประมวลผลข้อมูลส่วนบุคคล

- องค์กรมีระบบบริหารจัดการข้อมูลส่วนบุคคล (Data Management System) ที่สามารถระบุและทำเครื่องหมายข้อมูลส่วนบุคคลที่ต้องการระงับหรือจำกัดการประมวลผลได้ทันที โดยไม่ส่งผลกระทบต่อข้อมูลอื่น ๆ
- ระบบสามารถจัดเก็บสถานะคำขอและติดตามความคืบหน้าในการระงับหรือจำกัดการประมวลผลข้อมูลได้อย่างมีประสิทธิภาพ
- ในกรณีการระงับการประมวลผล ระบบสามารถทำให้ข้อมูลนั้นไม่แสดงผลในระบบใช้งาน หรือย้ายข้อมูลไปยังพื้นที่จัดเก็บแยกต่างหากอย่างปลอดภัย
- กรณีการจำกัดการประมวลผล ระบบจะจำกัดการใช้งานข้อมูลในบางฟังก์ชันตามคำขอ เช่น ไม่อนุญาตให้นำข้อมูลไปใช้ในกิจกรรมทางการตลาด หรือการวิเคราะห์เพิ่มเติม

- มีระบบแจ้งเตือนเจ้าหน้าที่เมื่อคำขอครบกำหนดหรือจำเป็นต้องทบทวนสถานะการระงับ/จำกัด

4.8.2 หากข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น องค์กรจะติดต่อผู้รับแต่ละรายเพื่อแจ้งเกี่ยวกับการระงับใช้ข้อมูลส่วนบุคคล

- สิ่งที่ต้องทำ: มีขั้นตอนในการดำเนินการแจ้งต่อผู้รับแต่ละราย ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น โดยมีแบบฟอร์มบันทึกการแจ้งที่ชัดเจน
- หลักฐาน: บันทึกการแจ้งต่อผู้รับแต่ละรายเกี่ยวกับการระงับใช้ข้อมูลส่วนบุคคล ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

แบบฟอร์มบันทึกการแจ้งต่อผู้รับข้อมูลส่วนบุคคลเกี่ยวกับการระบุใช้ข้อมูลส่วนบุคคล

ชื่อผู้รับข้อมูล: _____

หน่วยงาน/องค์กร: _____

ช่องทางติดต่อ (โทรศัพท์/อีเมล): _____

วันที่ได้รับข้อมูลส่วนบุคคล: _____

วันที่แจ้งการระบุใช้ข้อมูล: _____

รายละเอียดข้อมูลส่วนบุคคลที่ได้รับเปิดเผย

เหตุผลในการระบุใช้ข้อมูลส่วนบุคคล

คำชี้แจงเพิ่มเติม (ถ้ามี)

ผู้แจ้งข้อมูล (เจ้าหน้าที่ผู้รับผิดชอบ)

ชื่อ-นามสกุล: _____

ตำแหน่ง: _____

ลงชื่อ: _____

วันที่: _____

ขั้นตอนการดำเนินการแจ้งการระบุใช้ข้อมูลส่วนบุคคลต่อผู้รับข้อมูล

- เมื่อองค์กรได้รับคำขอใช้สิทธิในการระบุหรือจำกัดการประมวลผลข้อมูลส่วนบุคคลที่เคยเปิดเผยต่อบุคคลที่สาม
- ฝ่ายที่รับผิดชอบจะตรวจสอบรายชื่อผู้รับข้อมูลทั้งหมดที่ได้รับข้อมูลส่วนบุคคลนั้น
- จัดทำแบบฟอร์มบันทึกการแจ้งเพื่อส่งต่อไปยังผู้รับข้อมูลแต่ละราย โดยระบุรายละเอียดข้อมูลที่ได้รับ, วันที่แจ้ง, และเหตุผลของการระบุใช้ข้อมูล
- ส่งแบบฟอร์มการแจ้งผ่านช่องทางที่เหมาะสม เช่น อีเมล หนังสือ หรือระบบสารสนเทศภายในองค์กร
- บันทึกข้อมูลการแจ้งลงในระบบติดตามคำขอและเก็บรักษาหลักฐานการแจ้งไว้อย่างครบถ้วน
- ติดตามผลการดำเนินการจากผู้รับข้อมูลเพื่อยืนยันว่ามีการระบุใช้ข้อมูลตามคำขอเรียบร้อยแล้ว

4.8.3 หากถูกร้องขอ องค์กรสามารถระบุและแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบได้ว่าบุคคลที่สามารถใดได้รับข้อมูลส่วนบุคคลไปบ้าง

- สิ่งที่ต้องทำ: มีบันทึกแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่าบุคคลที่สามารถรายได้รับข้อมูลส่วนบุคคลบ้าง โดยมีแบบฟอร์มที่ชัดเจน
- หลักฐาน: บันทึกการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลในกรณีข้อมูลส่วนบุคคลถูกเปิดเผยต่อผู้อื่น
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

แบบฟอร์มบันทึกการแจ้งเจ้าของข้อมูลส่วนบุคคล
เรื่อง แจ้งรายชื่อบุคคลที่สามที่ได้รับข้อมูลส่วนบุคคล

ข้อมูลเจ้าของข้อมูลส่วนบุคคล

ชื่อ-นามสกุล: _____

หมายเลขประจำตัวประชาชน/เลขทะเบียน: _____

ที่อยู่/ช่องทางติดต่อ: _____

วันที่ได้รับคำขอข้อมูล: _____

วันที่แจ้งตอบกลับ: _____

รายละเอียดข้อมูลส่วนบุคคลที่เปิดเผย

รายชื่อบุคคลที่สามหรือผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นที่ได้รับข้อมูลส่วนบุคคล

ชื่อ: _____

หน่วยงาน/องค์กร: _____

ช่องทางติดต่อ: _____

ชื่อ: _____

หน่วยงาน/องค์กร: _____

ช่องทางติดต่อ: _____

(เพิ่มเติมได้ตามความเหมาะสม)

คำชี้แจงเพิ่มเติม (ถ้ามี)

ผู้แจ้งข้อมูล

ชื่อ-นามสกุล: _____

ตำแหน่ง: _____

ลงชื่อ: _____

วันที่: _____

ขั้นตอนการดำเนินงาน

- เมื่อได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคล องค์กรจะตรวจสอบรายชื่อบุคคลที่สามหรือผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นที่ได้รับข้อมูล
- จัดทำบันทึกแจ้งตามแบบฟอร์มที่กำหนด
- ส่งแบบฟอร์มแจ้งเจ้าของข้อมูลส่วนบุคคลผ่านช่องทางที่เหมาะสม เช่น อีเมล หรือไปรษณีย์

- บันทึกหลักฐานการแจ้งและเก็บรักษาไว้อย่างครบถ้วนในระบบบริหารจัดการข้อมูล

4.9.1 เมื่อได้รับการร้องขอ องค์กรจะจัดเตรียมข้อมูลส่วนบุคคลที่อยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไป ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ

สิ่งที่ต้องทำ: มีการจัดทำข้อมูลส่วนบุคคลที่อยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไป ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ และการส่งหรือโอนข้อมูลส่วนบุคคลมีความปลอดภัยเป็นไปตามมาตรฐานขั้นต่ำตามที่กฎหมายกำหนด

หลักฐาน: รูปแบบการจัดทำข้อมูลส่วนบุคคลที่สามารถอ่านได้หรือใช้งานโดยทั่วไปด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 31
ไม่มีกฎหมายกำหนดโทษ

การจัดเตรียมข้อมูลส่วนบุคคลในรูปแบบที่อ่านหรือใช้งานได้โดยทั่วไป

1. แนวทางการดำเนินงาน

- องค์กรจะจัดเตรียมข้อมูลส่วนบุคคลตามคำขอของเจ้าของข้อมูลในรูปแบบไฟล์ดิจิทัลที่เปิดอ่านหรือใช้งานได้ง่าย เช่น ไฟล์ CSV, JSON, XML หรือ PDF ที่สามารถเปิดด้วยโปรแกรมทั่วไป
- ใช้เครื่องมือหรือระบบเทคโนโลยีสารสนเทศในการแปลงข้อมูลให้อยู่ในรูปแบบที่สอดคล้องกับมาตรฐานเปิด (Open Standard) เพื่อให้อ่านและนำไปใช้ได้โดยอัตโนมัติ
- การส่งหรือโอนข้อมูลจะใช้ช่องทางที่ปลอดภัย เช่น การเข้ารหัสข้อมูล (Encryption) หรือระบบส่งข้อมูลที่ผ่านการรับรองความปลอดภัยตามมาตรฐานที่กฎหมายหรือองค์กรกำหนด

แบบฟอร์มตัวอย่าง: รายงานข้อมูลส่วนบุคคลตามคำขอ

หมายเลข	รายการข้อมูล	รายละเอียดข้อมูล	รูปแบบข้อมูล	หมายเหตุ
1	ชื่อ-นามสกุล	นายสมชาย ใจดี	ข้อความ (Text)	
2	วันเกิด	01/01/2530	ข้อความ (Text)	
3	เบอร์โทรศัพท์	081-234-5678	ข้อความ (Text)	
4	ที่อยู่	123/45 หมู่บ้าน...	ข้อความ (Text)	
5	อีเมล	somchai@email.com	ข้อความ (Text)	

รายงานข้อมูลนี้ถูกจัดเก็บในรูปแบบ CSV (Comma-Separated Values) เพื่อให้เปิดใช้งานได้ง่ายด้วย

- โปรแกรม spreadsheet หรือระบบอื่น ๆ
- มีการเข้ารหัสไฟล์ก่อนส่ง เพื่อความปลอดภัยของข้อมูล

3. ตัวอย่างข้อความแจ้งเจ้าของข้อมูล

เรียน คุณ _____

ตามคำร้องขอข้อมูลส่วนบุคคลของท่าน องค์กรได้จัดเตรียมข้อมูลในรูปแบบไฟล์ CSV ที่สามารถเปิดอ่านได้ด้วยโปรแกรมทั่วไป เช่น Microsoft Excel หรือโปรแกรม spreadsheet อื่น ๆ โดยข้อมูลถูกจัดเตรียมให้ครบถ้วนตามคำขอ

เพื่อความปลอดภัยของข้อมูลไฟล์ดังกล่าวถูกเข้ารหัสไว้ และรหัสผ่านจะถูกส่งแยกทางช่องทางอื่น (เช่น SMS หรือโทรศัพท์)

กรุณาติดต่อกลับหากมีข้อสงสัยเพิ่มเติม

ขอแสดงความนับถือ

(ชื่อผู้รับผิดชอบ) _____

ตำแหน่ง

วันที่

4. สภาพบังคับตามกฎหมาย

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 31 เจ้าของข้อมูลมีสิทธิได้รับข้อมูลส่วนบุคคลในรูปแบบที่อ่านหรือใช้งานได้โดยทั่วไปด้วยระบบอัตโนมัติ

องค์กรต้องจัดเตรียมข้อมูลให้สอดคล้องกับคำขอ โดยไม่มีกฎหมายกำหนดโทษหากไม่ปฏิบัติ

4.9.2 ในกรณีที่เป็นไปได้และหากบุคคลร้องขอ องค์กรสามารถส่งข้อมูลไปยังองค์กรอื่นด้วยวิธีการทางอิเล็กทรอนิกส์ได้โดยตรง

- สิ่งที่ต้องทำ: จัดให้มีการส่งข้อมูลไปยังองค์กรอื่นด้วยวิธีการทางอิเล็กทรอนิกส์ได้โดยตรง และการส่งหรือโอน ข้อมูลส่วนบุคคลมีความปลอดภัยเป็นไปตามมาตรฐานขั้นต่ำตามที่กฎหมายกำหนด
- หลักฐาน: เอกสารหรือหลักฐานแสดงการส่งข้อมูลไปยังองค์กรอื่นด้วยวิธีการทางอิเล็กทรอนิกส์
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 31
ไม่มีกฎหมายกำหนดโทษ

การส่งข้อมูลส่วนบุคคลไปยังองค์กรอื่นด้วยวิธีการทางอิเล็กทรอนิกส์

1. แนวทางการดำเนินงาน

- องค์กรจัดเตรียมระบบหรือวิธีการที่สามารถส่งข้อมูลส่วนบุคคลไปยังองค์กรอื่นโดยตรงผ่านช่องทางอิเล็กทรอนิกส์ เช่น การส่งผ่าน API ที่เข้ารหัส, การส่งไฟล์ข้อมูลที่เข้ารหัสผ่านอีเมล หรือระบบถ่ายโอนข้อมูลที่มีการยืนยันตัวตน
- ต้องมีมาตรการความปลอดภัยที่เหมาะสม เช่น การเข้ารหัสข้อมูล (Encryption), การยืนยันตัวตนของผู้รับข้อมูล, การตรวจสอบสิทธิ์ในการรับข้อมูล
- ในกรณีที่เจ้าของข้อมูลร้องขอ การส่งข้อมูลต้องดำเนินการโดยเร็วและมีบันทึกที่ชัดเจนเพื่อเป็นหลักฐาน

2. ตัวอย่างแบบฟอร์มคำร้องขอส่งข้อมูลไปยังองค์กรอื่น (Request for Direct Data Transfer)

ชื่อผู้ร้องขอข้อมูล	
หมายเลขบัตรประชาชน/รหัสพนักงาน	
วันที่ร้องขอ	
องค์กรปลายทางที่ต้องการส่งข้อมูล	
ประเภทข้อมูลที่ต้องการส่ง	
ช่องทางการส่งข้อมูล	() API เข้ารหัส () อีเมลเข้ารหัส () อื่น ๆ:
ลายมือชื่อผู้ร้องขอ	
วันที่	

3. ตัวอย่างบันทึกการส่งข้อมูลทางอิเล็กทรอนิกส์ (Data Transfer Log)

วันที่/ เวลา	ชื่อผู้ส่งข้อมูล	องค์กร ผู้รับ ข้อมูล	ประเภท ข้อมูลที่ส่ง	ช่อง ทางการ ส่ง	วิธีการรักษา ความปลอดภัย	หมายเหตุ
1 มิถุนายน 2568 09:30	นางสาวสมหญิง สายทอง	บริษัท ABC จำกัด	ข้อมูล ลูกค้า	API เข้ารหัส	การเข้ารหัสแบบ TLS และ OAuth2	ส่งข้อมูล ตามคำ ร้องขอ

4. ตัวอย่างข้อความแจ้งเจ้าของข้อมูล (Notification to Data Subject)

เรียน คุณ _____

ตามคำร้องขอของท่าน องค์กรได้ดำเนินการส่งข้อมูลส่วนบุคคลของท่านไปยังองค์กร

_____ โดยใช้ช่องทางอิเล็กทรอนิกส์ที่มีมาตรการรักษาความปลอดภัยอย่างเคร่งครัด เพื่อให้
ข้อมูลของท่านได้รับการจัดการอย่างถูกต้อง

กรุณาติดต่อเรา หากท่านมีคำถามหรือข้อสงสัยเพิ่มเติม

ขอแสดงความนับถือ

(ชื่อผู้รับผิดชอบ) _____

ตำแหน่ง

วันที่

4.10.1 องค์กรดำเนินการตรวจสอบเพิ่มเติมสำหรับกลุ่มเปราะบาง เช่น ผู้เยาว์ ผู้พิการ สำหรับการ ประมวลผลโดยระบบอัตโนมัติและการทำโปรไฟล์อัตโนมัติ

สิ่งที่ต้องทำ: มี Privacy Policy/Privacy Notice โดยอธิบายถึงการปกป้องสิทธิที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่

เกี่ยวข้องกับการตัดสินใจโดยอัตโนมัติและการทำโปรไฟล์ และระบุประเภทของข้อมูลที่จะ
จัดให้มีการตัดสินใจโดยอัตโนมัติและการทำโปรไฟล์อย่างชัดเจน

หลักฐาน: Privacy Policy/Privacy Notice ที่อธิบายการประมวลผลโดยระบบอัตโนมัติ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

Privacy Policy / Privacy Notice

องค์กรของเราให้ความสำคัญสูงสุดกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน และยึดมั่นในหลักความโปร่งใส ความปลอดภัย และการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) อย่างเคร่งครัด เพื่อสร้างความมั่นใจและความไว้วางใจในการใช้บริการของเรา

1. วัตถุประสงค์ของนโยบายความเป็นส่วนตัว

- เพื่อชี้แจงถึงแนวทางการเก็บรวบรวม ใช้ เปิดเผย และปกป้องข้อมูลส่วนบุคคลของท่าน
- เพื่ออธิบายสิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กำหนดในมาตรา 23 ของ PDPA
- เพื่อแจ้งให้เจ้าของข้อมูลทราบถึงวิธีการและช่องทางในการใช้สิทธิในการเข้าถึงข้อมูล แก้ไขข้อมูล และอื่น ๆ
- เพื่อแจ้งให้ทราบถึงการประมวลผลข้อมูลส่วนบุคคลโดยระบบอัตโนมัติและการทำโปรไฟล์ (Profiling)

2. การประมวลผลข้อมูลส่วนบุคคลโดยระบบอัตโนมัติและโปรไฟล์

องค์กรมีการใช้ระบบอัตโนมัติและเทคโนโลยีโปรไฟล์เพื่อวัตถุประสงค์ดังนี้

- ปรับปรุงการให้บริการให้เหมาะสมและตรงตามความต้องการของผู้ใช้บริการแต่ละราย
- พัฒนาประสบการณ์ผู้ใช้ (User Experience) ให้ดีขึ้นอย่างต่อเนื่อง
- วิเคราะห์แนวโน้มและพฤติกรรมการใช้งานเพื่อเพิ่มประสิทธิภาพของระบบ

การคุ้มครองกลุ่มเปราะบาง

องค์กรให้ความสำคัญเป็นพิเศษกับกลุ่มเปราะบาง เช่น

- ผู้เยาว์ (อายุต่ำกว่า 18 ปี)
- ผู้พิการหรือผู้ที่มีข้อจำกัดทางร่างกายและจิตใจ
- ผู้สูงอายุ (Elderly Persons)
- กลุ่มที่มีความเปราะบางทางสังคมหรือเศรษฐกิจ (Socially or Economically Disadvantaged Groups)

กลุ่มที่อยู่ในสถานการณ์เฉพาะ (Specific Situations)

เช่น ผู้ที่อยู่ในโรงพยาบาล โรงเรียน หรือองค์กรที่ต้องดูแลเป็นพิเศษ

โดยดำเนินการมาตรการดังนี้

- จำกัดประเภทข้อมูลส่วนบุคคลที่ใช้ในการประมวลผลโดยอัตโนมัติและโปรไฟล์ เพื่อไม่ให้กระทบต่อสิทธิและเสรีภาพของกลุ่มเปราะบาง
- ให้สิทธิแก่เจ้าของข้อมูลในการขอชี้แจงผลการตัดสินใจจากระบบอัตโนมัติและมีสิทธิในการขอทบทวนหรือคัดค้าน
- ดำเนินการประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment - PIA) ก่อนเปิดใช้งานระบบดังกล่าวในกลุ่มเปราะบาง
- แจ้งข้อมูลให้เจ้าของข้อมูลทราบอย่างชัดเจนก่อนเริ่มประมวลผล

3. ประเภทข้อมูลส่วนบุคคลที่ใช้ในการประมวลผลโดยระบบอัตโนมัติและโปรไฟล์

- ข้อมูลทั่วไป เช่น ชื่อ อายุ เพศ สถานภาพทางการศึกษา
- ข้อมูลพฤติกรรม เช่น ประวัติการเข้าชมเว็บไซต์, ประวัติการใช้งาน, ความชอบ หรือพฤติกรรมออนไลน์
- ข้อมูลสุขภาพหรือข้อมูลพิเศษ (ถ้ามีการประมวลผลโดยได้รับความยินยอมเป็นลายลักษณ์อักษร หรือมีข้อกำหนดตามกฎหมาย)

4. สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 23 PDPA

- เจ้าของข้อมูลมีสิทธิดังนี้
- ขอเข้าถึงข้อมูลส่วนบุคคลของตนที่องค์กรได้เก็บรวบรวม
- ขอให้แก้ไขข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์
- ขอให้ลบหรือทำลายข้อมูลส่วนบุคคลในกรณีที่ไม่มีความจำเป็นต้องเก็บรักษา
- ขอให้ระงับหรือจำกัดการประมวลผลข้อมูล
- คัดค้านการประมวลผลข้อมูลส่วนบุคคล โดยเฉพาะในกรณีการประมวลผลโดยระบบอัตโนมัติ
- ขอให้โอนย้ายข้อมูลส่วนบุคคลในรูปแบบที่ใช้งานได้โดยทั่วไป (Data Portability)

ช่องทางในการใช้สิทธิ

- เจ้าของข้อมูลสามารถติดต่อผ่านช่องทางดังนี้เพื่อใช้สิทธิของตน
- อีเมล: privacy@example.com
- โทรศัพท์: 012-345-6789
- ที่อยู่: ฝ่ายคุ้มครองข้อมูลส่วนบุคคล องค์กร
- องค์กรจะดำเนินการตามคำขอภายในระยะเวลาที่กฎหมายกำหนด (ไม่เกิน 30 วัน) และจะแจ้งเหตุผลหากไม่สามารถดำเนินการได้

5. การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

องค์กรใช้มาตรการรักษาความปลอดภัยที่เหมาะสม เช่น

- การเข้ารหัสข้อมูล (Encryption)
- การควบคุมสิทธิ์การเข้าถึงข้อมูล
- การตรวจสอบและบันทึกการเข้าถึงข้อมูล
- การฝึกอบรมพนักงานให้ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล

6. การเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลภายนอก

องค์กรจะไม่เปิดเผยข้อมูลส่วนบุคคลของท่านแก่บุคคลภายนอก ยกเว้นในกรณีดังต่อไปนี้

- ได้รับความยินยอมจากเจ้าของข้อมูลแล้ว
- ตามคำสั่งของกฎหมายหรือหน่วยงานที่มีอำนาจ
- เพื่อวัตถุประสงค์ในการให้บริการตามที่ตกลงกันไว้ โดยมีการทำสัญญาคุ้มครองข้อมูลกับผู้รับข้อมูล

7. การเปลี่ยนแปลงนโยบายความเป็นส่วนตัว

องค์กรสงวนสิทธิ์ในการแก้ไขหรือปรับปรุงนโยบายความเป็นส่วนตัวนี้ตามความจำเป็น โดยจะแจ้งให้ทราบล่วงหน้าผ่านช่องทางเว็บไซต์หรือช่องทางการสื่อสารอื่น ๆ

8. การติดต่อสอบถาม

หากท่านมีคำถามหรือข้อสงสัยเกี่ยวกับนโยบายนี้ หรือการจัดการข้อมูลส่วนบุคคลขององค์กร กรุณาติดต่อ

อีเมล: privacy@example.com

โทร: 012-345-6789

4.10.2 องค์กรเก็บข้อมูลเท่าที่จำเป็นและมีนโยบายการเก็บรักษาข้อมูลที่ชัดเจนสำหรับโปรไฟล์ที่สร้างขึ้น

สิ่งที่ต้องทำ: มีการแจ้งให้ทราบและกำหนดระยะเวลาการเก็บข้อมูลใน Privacy Notice/Privacy Policy อย่างชัดเจนสำหรับโปรไฟล์ที่สร้างขึ้น

หลักฐาน: Privacy Notice ที่มีการให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการประมวลผล โดยระบบอัตโนมัติ และมีการกำหนดระยะเวลาในการเก็บข้อมูลส่วนบุคคลอย่างชัดเจนสำหรับโปรไฟล์ที่สร้างขึ้น

Privacy Policy ที่อธิบายถึงวัตถุประสงค์และการประมวลผลโดยระบบอัตโนมัติ รวมถึงกำหนดระยะเวลาในการเก็บข้อมูลส่วนบุคคลอย่างชัดเจนสำหรับโปรไฟล์ที่สร้างขึ้น

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ตัวอย่างหลักฐาน Privacy Notice / Privacy Policy (ส่วนที่เกี่ยวข้องกับโปรไฟล์และการเก็บรักษาข้อมูล)

1. ความเป็นมาของการประมวลผลข้อมูลส่วนบุคคลโดยระบบอัตโนมัติและโปรไฟล์

องค์กรของเราให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน โดยเฉพาะข้อมูลที่ถูกนำไปใช้ในระบบอัตโนมัติ เช่น การทำโปรไฟล์ เพื่อวัตถุประสงค์ในการปรับปรุงบริการให้เหมาะสมและตรงกับความต้องการของผู้ใช้

การประมวลผลดังกล่าวดำเนินการโดยยึดหลักการเก็บข้อมูลเท่าที่จำเป็น และเพื่อประโยชน์ที่ชัดเจนตามวัตถุประสงค์ที่ได้แจ้งไว้

2. ประเภทข้อมูลส่วนบุคคลที่เก็บเพื่อโปรไฟล์

- ข้อมูลพื้นฐาน เช่น อายุ เพศ สถานะทางสังคม
- ข้อมูลพฤติกรรม เช่น ประวัติการใช้งาน ความสนใจ หรือผลตอบรับ
- ข้อมูลเพิ่มเติมที่จำเป็นสำหรับการวิเคราะห์และปรับปรุงบริการ

3. หลักการเก็บรักษาข้อมูลและระยะเวลาการเก็บข้อมูล

องค์กรเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อวัตถุประสงค์ที่ได้ระบุไว้ในนโยบายนี้ กำหนดระยะเวลาการเก็บข้อมูลอย่างชัดเจน โดยทั่วไปข้อมูลโปรไฟล์จะถูกเก็บไว้ไม่เกิน [ระบุระยะเวลา เช่น 1 ปี, 3 ปี] นับจากวันที่ได้รับข้อมูลหรือวันสุดท้ายที่มีการใช้งานข้อมูลนั้น เมื่อครบกำหนดระยะเวลาการเก็บรักษา องค์กรจะดำเนินการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ (pseudonymization) อย่างปลอดภัยและเป็นไปตามมาตรฐานที่กำหนด

4. สิทธิของเจ้าของข้อมูล

เจ้าของข้อมูลมีสิทธิในการขอเข้าถึง แก้ไข หรือลบข้อมูลส่วนบุคคลของตน รวมถึงสิทธิในการคัดค้าน การประมวลผลโดยระบบอัตโนมัติและโปรไฟล์ โดยสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของ องค์กรเพื่อใช้สิทธิเหล่านี้ได้

5. การแจ้งให้ทราบเกี่ยวกับการเก็บรักษาข้อมูล

องค์กรจะทำการแจ้งให้เจ้าของข้อมูลทราบเกี่ยวกับประเภทของข้อมูลที่เก็บ ระยะเวลาในการเก็บรักษา และวิธีการประมวลผลโดยระบบอัตโนมัติผ่าน Privacy Notice / Privacy Policy ที่เผยแพร่ใน เว็บไซต์หรือช่องทางการสื่อสารที่เหมาะสม

6. การรักษาความปลอดภัยของข้อมูล

องค์กรได้จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อปกป้องข้อมูลส่วนบุคคลจากการเข้าถึง โดยไม่ได้รับอนุญาต การเปิดเผย การแก้ไข หรือการทำลายที่ไม่เหมาะสม

ตัวอย่างข้อความใน Privacy Notice ที่สอดคล้องกับเกณฑ์ 4.10.2 และ มาตรา 23 PDPA

การประมวลผลข้อมูลโดยระบบอัตโนมัติและโปรไฟล์

องค์กรของเราจะมีการเก็บและประมวลผลข้อมูลส่วนบุคคลโดยใช้ระบบอัตโนมัติ รวมถึงการทำโปรไฟล์ เพื่อวัตถุประสงค์ในการปรับปรุงการให้บริการและประสบการณ์ของผู้ใช้ ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับโปรไฟล์จะถูกเก็บเท่าที่จำเป็นและจะถูกเก็บรักษาไว้เป็นระยะเวลาไม่เกิน 2 ปี หลังจากนั้นข้อมูลจะถูกลบหรือทำให้ไม่สามารถระบุตัวบุคคลได้ตามมาตรฐานความปลอดภัยที่เหมาะสม

ท่านมีสิทธิขอเข้าถึง แก้ไข หรือลบข้อมูลส่วนบุคคล รวมถึงคัดค้านการประมวลผลด้วยระบบอัตโนมัติและโปรไฟล์ได้โดยติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของเรา

ข้อมูลเพิ่มเติมเกี่ยวกับวิธีการจัดการข้อมูลส่วนบุคคลสามารถดูได้จาก Privacy Policy ของเรา
ตัวอย่างเอกสารหลักฐานประกอบ

รายการ	รายละเอียด
ชื่อเอกสาร	Privacy Notice / Privacy Policy (ส่วนโปรไฟล์และการเก็บรักษาข้อมูล)
เนื้อหา	ระบุประเภทข้อมูลที่เก็บเพื่อโปรไฟล์ ระยะเวลาเก็บรักษาข้อมูลอย่างชัดเจน วิธีการลบข้อมูล, สิทธิของเจ้าของข้อมูล
ช่องทางเผยแพร่	เว็บไซต์ขององค์กร แผ่นพับ ช่องทางแจ้งข่าวสารต่าง ๆ
ระบบสนับสนุน	ระบบจัดการข้อมูลส่วนบุคคลที่สามารถติดตามระยะเวลาเก็บข้อมูล และระบบลบข้อมูลอัตโนมัติเมื่อครบกำหนด
การอัปเดต	มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีกฎหมายเปลี่ยนแปลง

4.10.3 หากองค์กรใช้การประมวลผลโดยระบบอัตโนมัติ องค์กรมีกระบวนการที่บันทึกไว้เป็นหลักฐานว่า การตัดสินใจเหล่านี้เกิดขึ้นภายใต้ข้อกำหนดของกฎหมายหรือเงื่อนไขอย่างไร และองค์กรต้องดำเนินการประเมินความเสี่ยงและผลกระทบความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลด้วย (DPIA)

สิ่งที่ต้องทำ: มีบันทึกหลักฐานการประมวลผลโดยระบบอัตโนมัติ และจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ในกรณีที่มีการประมวลผลโดยระบบอัตโนมัติ

หลักฐาน: บันทึกหลักฐานการประมวลผลโดยระบบอัตโนมัติ
เอกสารการดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ในกรณีที่มีการประมวลผลโดยระบบอัตโนมัติ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เรื่อง: การบันทึกหลักฐานการประมวลผลโดยระบบอัตโนมัติและการดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

1. วัตถุประสงค์

เพื่อแสดงให้เห็นว่าการตัดสินใจที่เกิดจากการประมวลผลโดยระบบอัตโนมัตินั้นเป็นไปตามข้อกำหนดของกฎหมายและเงื่อนไขที่กำหนด รวมทั้งเพื่อประเมินและจัดการความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment - DPIA) อย่างเป็นระบบและมีเอกสารบันทึกไว้เป็นหลักฐาน

2. ขอบเขต

ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลโดยระบบอัตโนมัติทั้งหมดที่องค์กรนำมาใช้ในการตัดสินใจ หรือการสร้างโปรไฟล์บุคคล รวมถึงกรณีที่มีการประเมินความเสี่ยงโดย DPIA

3. ขั้นตอนปฏิบัติ

3.1 การบันทึกหลักฐานการประมวลผลโดยระบบอัตโนมัติ

- บันทึกข้อมูลการตัดสินใจที่เกิดขึ้นจากระบบอัตโนมัติ โดยระบุข้อมูลสำคัญ เช่น
- ประเภทข้อมูลที่ใช้ในการตัดสินใจ
- กฎเกณฑ์หรือเงื่อนไขตามกฎหมายที่นำมาใช้ในการตัดสินใจ
- วันที่และเวลาที่เกิดการประมวลผลและตัดสินใจ
- ผู้รับผิดชอบหรือเจ้าหน้าที่ที่ตรวจสอบผลการตัดสินใจ (ถ้ามี)
- บันทึกสถานะการปฏิบัติตามกฎหมายและข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง (เช่น การได้รับความยินยอม การแจ้งล่วงหน้า)

3.2 การดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

- ระบุขอบเขตและลักษณะของการประมวลผลข้อมูลส่วนบุคคลโดยระบบอัตโนมัติ
- วิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูล เช่น ความเป็นส่วนตัว ความถูกต้องของข้อมูล ความปลอดภัยข้อมูล
- กำหนดมาตรการและแนวทางจัดการเพื่อลดความเสี่ยงเหล่านั้น
- จัดทำรายงาน DPIA ที่มีรายละเอียดชัดเจนและจัดเก็บเป็นหลักฐาน
- ทบทวน DPIA อย่างสม่ำเสมอหรือตามความจำเป็นเมื่อมีการเปลี่ยนแปลงระบบหรือวิธีการประมวลผล

4. ตัวอย่างเอกสารหลักฐาน

4.1 แบบฟอร์มบันทึกหลักฐานการประมวลผลโดยระบบอัตโนมัติ

รายการ	รายละเอียด
วันที่และเวลา	[วันที่และเวลาที่มีการประมวลผล]
ประเภทข้อมูล	[ข้อมูลที่ถูกใช้ในการประมวลผล]
เงื่อนไข/กฎเกณฑ์	[อธิบายเงื่อนไขทางกฎหมายหรือข้อกำหนดที่ใช้]
ผลลัพธ์การตัดสินใจ	[ผลลัพธ์ที่ได้จากการประมวลผล]
ผู้ตรวจสอบ (ถ้ามี)	[ชื่อและตำแหน่ง]
หมายเหตุเพิ่มเติม	[ข้อมูลเพิ่มเติม เช่น การแจ้งเจ้าของข้อมูล]

4.2 ตัวอย่างรายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

ชื่อโครงการ/ระบบ: ระบบตัดสินใจอัตโนมัติ [ชื่อระบบ]

วัตถุประสงค์: [ระบุวัตถุประสงค์ของระบบ]

ประเภทข้อมูลที่ประมวลผล: [ระบุข้อมูลที่เกี่ยวข้อง]

การวิเคราะห์ความเสี่ยง:

ความเสี่ยงที่พบ: [รายละเอียดความเสี่ยง เช่น ความผิดพลาดของระบบ, การละเมิดข้อมูล]

ผลกระทบที่อาจเกิดขึ้น: [ผลกระทบต่อเจ้าของข้อมูล]

มาตรการควบคุมความเสี่ยง: [มาตรการที่นำมาใช้ เช่น การเข้ารหัสข้อมูล, การตรวจสอบโดยมนุษย์]

ผู้รับผิดชอบดำเนินการ: [ชื่อผู้รับผิดชอบ]

วันที่จัดทำ: [วัน/เดือน/ปี]

การทบทวนครั้งต่อไป: [วัน/เดือน/ปี]

5. การจัดเก็บและการเข้าถึงหลักฐาน

- เอกสารบันทึกหลักฐานและรายงาน DPIA ต้องถูกจัดเก็บในระบบสารบรรณหรือระบบบริหารจัดการข้อมูลขององค์กร
- มีการกำหนดสิทธิ์การเข้าถึงเฉพาะเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น
- มีการสำรองข้อมูลและเก็บรักษาตามมาตรฐานความปลอดภัยข้อมูล

6. ช่องทางติดต่อ

หากเจ้าของข้อมูลหรือตัวแทนมีข้อสงสัยเกี่ยวกับการประมวลผลโดยระบบอัตโนมัติและการทำ DPIA สามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ที่

อีเมล: privacy@example.com

โทรศัพท์: 012-345-6789

4.10.4 ในกรณีที่การตัดสินใจเป็นไปโดยระบบอัตโนมัติ (ไม่มีบุคคลตรวจสอบ) และมีผลทางกฎหมายหรือในทางอื่นอย่างมีนัยสำคัญต่อบุคคล องค์กรจัดให้มีกระบวนการที่บันทึกไว้เพื่อช่วยให้บุคคลสามารถร้องขอให้มีการตรวจสอบและทบทวนโดยมนุษย์ได้ และบุคคลสามารถคัดค้านการตัดสินใจโดยระบบอัตโนมัติ

สิ่งที่ต้องทำ: มีบันทึกหลักฐานการประมวลผลโดยระบบอัตโนมัติ และแบบฟอร์มในการคัดค้านการประมวลผลโดยอัตโนมัติ

หลักฐาน: บันทึกหลักฐานการประมวลผลโดยระบบอัตโนมัติ
 แบบฟอร์มในการคัดค้านการประมวลผลโดยอัตโนมัติ
 สภาพบังคับ: กฎหมายไม่ได้กำหนด

หลักฐานตามเกณฑ์ 4.10.4

เรื่อง: การจัดการการตัดสินใจโดยระบบอัตโนมัติที่ไม่มีการตรวจสอบโดยบุคคล และการให้สิทธิคัดค้านและร้องขอทบทวน

1. วัตถุประสงค์

เพื่อรับประกันสิทธิของเจ้าของข้อมูลในการร้องขอให้มีการตรวจสอบและทบทวนการตัดสินใจที่เกิดขึ้นจากระบบอัตโนมัติอย่างเต็มที่ และให้สิทธิในการคัดค้านการตัดสินใจโดยระบบอัตโนมัติ ซึ่งเป็นไปตามหลักการความเป็นธรรมและความโปร่งใสในการประมวลผลข้อมูลส่วนบุคคล

2. ขอบเขต

ครอบคลุมทุกกรณีที่ต้องการใช้การตัดสินใจโดยระบบอัตโนมัติแบบไม่มีบุคคลตรวจสอบ และมีผลทางกฎหมายหรือมีผลสำคัญในทำนองเดียวกันต่อเจ้าของข้อมูล

3. ขั้นตอนปฏิบัติ

3.1 การบันทึกหลักฐานการประมวลผลโดยระบบอัตโนมัติ

จัดเก็บบันทึกข้อมูลสำคัญของแต่ละกรณี เช่น

- วันที่และเวลาที่ระบบดำเนินการตัดสินใจ
- รายละเอียดข้อมูลที่ใช้ในการประมวลผล

ผลการตัดสินใจของระบบ

ระบุว่าไม่มีบุคคลตรวจสอบการตัดสินใจนี้

- ช่องทางและวิธีการแจ้งเจ้าของข้อมูลถึงผลการตัดสินใจและสิทธิที่เกี่ยวข้อง
- จัดเก็บบันทึกนี้ในระบบสารสนเทศที่ปลอดภัยและสามารถเข้าถึงได้โดยผู้ที่มีหน้าที่รับผิดชอบ

3.2 กระบวนการให้เจ้าของข้อมูลร้องขอทบทวนโดยมนุษย์

- เจ้าของข้อมูลสามารถส่งคำร้องขอทบทวนการตัดสินใจโดยระบบอัตโนมัติได้ผ่านช่องทางที่กำหนด เช่น แบบฟอร์มออนไลน์ อีเมล หรือจดหมาย
- เจ้าหน้าที่หรือผู้มีอำนาจจะทำการตรวจสอบการตัดสินใจและข้อมูลที่เกี่ยวข้องโดยมนุษย์
- แจ้งผลการทบทวนให้เจ้าของข้อมูลทราบภายในระยะเวลาที่เหมาะสม
- บันทึกหลักฐานการร้องขอและผลการทบทวนไว้ในระบบ

3.3 สิทธิในการคัดค้านการประมวลผลโดยระบบอัตโนมัติ

จัดทำแบบฟอร์มสำหรับเจ้าของข้อมูลใช้ยื่นคำคัดค้านการประมวลผลโดยระบบอัตโนมัติ เมื่อได้รับคำคัดค้าน องค์กรต้องพิจารณาและแจ้งผลการดำเนินการให้เจ้าของข้อมูลทราบ จัดเก็บแบบฟอร์มคำคัดค้านและผลการพิจารณาเป็นหลักฐาน

4. ตัวอย่างเอกสารหลักฐาน

4.1 ตัวอย่างแบบฟอร์มบันทึกหลักฐานการประมวลผลโดยระบบอัตโนมัติ

รายการ	รายละเอียด
วันที่และเวลา	[วันที่/เวลาที่ประมวลผล]
ประเภทข้อมูลที่ใช้	[ข้อมูลที่ระบบใช้ในการตัดสินใจ]
ผลการตัดสินใจของระบบ	[รายละเอียดผลลัพธ์]
การมีบุคคลตรวจสอบ	ไม่มีบุคคลตรวจสอบ
การแจ้งเจ้าของข้อมูล	[วิธีการแจ้งและวันที่แจ้ง]
หมายเหตุ	[ข้อมูลเพิ่มเติม]

4.2 ตัวอย่างแบบฟอร์มคำคัดค้านการประมวลผลโดยระบบอัตโนมัติ

แบบฟอร์มคำคัดค้านการประมวลผลโดยระบบอัตโนมัติ

ข้อมูลเจ้าของข้อมูลส่วนบุคคล

ชื่อ-นามสกุล: _____

เลขบัตรประชาชน / หมายเลขผู้ใช้: _____

เบอร์ติดต่อ: _____

อีเมล: _____

รายละเอียดการคัดค้าน

ข้าพเจ้า ขอคัดค้านการประมวลผลข้อมูลส่วนบุคคลโดยระบบอัตโนมัติในเรื่อง:

เหตุผลของการคัดค้าน

คำร้องขอทบทวนการตัดสินใจโดยมนุษย์

() ขอ

() ไม่ขอ

ลงชื่อเจ้าของข้อมูล: _____

วันที่: _____

5. การจัดเก็บเอกสาร

เอกสารบันทึกและแบบฟอร์มคำคัดค้านจะถูกจัดเก็บในระบบสารบรรณหรือระบบจัดการข้อมูลขององค์กร

- มีการจำกัดสิทธิ์เข้าถึงข้อมูลเหล่านี้เฉพาะเจ้าหน้าที่ที่รับผิดชอบ
- มีการสำรองข้อมูลและรักษาความปลอดภัยตามมาตรฐานที่เหมาะสม

6. ช่องทางติดต่อ

หากเจ้าของข้อมูลต้องการใช้สิทธิในการร้องขอทบทวนหรือคัดค้าน สามารถติดต่อได้ที่

อีเมล: privacy@example.com

โทรศัพท์: 012-345-6789

4.10.5 องค์กรดำเนินการตรวจสอบความถูกต้องและอคติของระบบอัตโนมัติเป็นประจำเพื่อให้แน่ใจว่าระบบทำงานตามที่ตั้งใจไว้ และองค์กรจะนำข้อมูลนี้กลับเข้าสู่กระบวนการออกแบบ (เพื่อเพิ่มความถูกต้องของการตัดสินใจและลดอคติของระบบ)

สิ่งที่ต้องทำ: มีการตรวจสอบความถูกต้องและอคติของระบบอัตโนมัติเป็นประจำ

หลักฐาน: เอกสารการดำเนินการตรวจสอบความถูกต้องและอคติของระบบอัตโนมัติ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

หลักฐานการตรวจสอบความถูกต้องและอคติของระบบอัตโนมัติ (ตามเกณฑ์ 4.10.5)

1. วัตถุประสงค์

เพื่อให้มั่นใจว่าระบบอัตโนมัติที่องค์กรใช้งานมีความถูกต้องในการตัดสินใจและไม่มีอคติที่ส่งผลกระทบต่อเจ้าของข้อมูลหรือผู้ได้รับผลกระทบ และให้องค์กรนำข้อมูลที่ได้จากการตรวจสอบกลับไปปรับปรุงระบบอย่างต่อเนื่อง

2. ขอบเขต

การตรวจสอบนี้ครอบคลุมระบบอัตโนมัติทุกประเภทที่ใช้ในกระบวนการตัดสินใจและประมวลผลข้อมูลส่วนบุคคล รวมถึงระบบโปรไฟล์ที่อาจส่งผลกระทบต่อเจ้าของข้อมูล

3. ขั้นตอนการดำเนินการตรวจสอบ

3.1 การวางแผนและจัดทำรายการตรวจสอบ

- กำหนดความถี่การตรวจสอบ เช่น รายไตรมาส รายปี
- ระบุขอบเขตของระบบและโมดูลที่ต้องตรวจสอบ
- กำหนดตัวชี้วัดความถูกต้อง (Accuracy Metrics) เช่น อัตราความถูกต้อง (Accuracy Rate), ค่า False Positive/Negative
- กำหนดวิธีการตรวจสอบอคติ (Bias Audit) เช่น การวิเคราะห์ผลลัพธ์ตามกลุ่มประชากร (เช่น เพศ อายุ เชื้อชาติ)

3.2 การเก็บข้อมูลและทดสอบระบบ

- ดึงข้อมูลจากระบบอัตโนมัติในช่วงเวลาที่กำหนด
- ประเมินผลการตัดสินใจหรือการประมวลผลตามตัวชี้วัดที่กำหนด
- วิเคราะห์หาจุดที่มีอคติ เช่น ผลลัพธ์ที่ผิดปกติในกลุ่มเปราะบางหรือกลุ่มเฉพาะ
- จัดทำรายงานผลการตรวจสอบความถูกต้องและอคติ

3.3 การรายงานและแผนการปรับปรุง

- นำเสนอผลการตรวจสอบต่อผู้บริหารและทีมพัฒนาระบบ
- วางแผนการปรับปรุงแก้ไขระบบ (ถ้าพบอคติหรือความผิดพลาด) เช่น ปรับโมเดลข้อมูล ปรับอัลกอริทึม
- กำหนดมาตรการป้องกันไม่ให้อคติกลับมาเกิดซ้ำ
- ประเมินและอัปเดตนโยบายการประมวลผลอัตโนมัติและโปรไฟล์
- อัปเดตเอกสารที่เกี่ยวข้อง เช่น Privacy Policy, DPIA
- ฝึกอบรมทีมงานเกี่ยวกับผลการตรวจสอบและแนวทางป้องกันอคติ

4. ตัวอย่างเอกสารการตรวจสอบความถูกต้องและอคติของระบบอัตโนมัติ

รายงานการตรวจสอบระบบอัตโนมัติ

รายการ	รายละเอียด
ชื่อระบบ	ระบบประมวลผลคำขอสินเชื่ออัตโนมัติ
วันที่ตรวจสอบ	1 เมษายน 2025

ผู้ตรวจสอบ	ทีม Data Science / ฝ่ายคุ้มครองข้อมูล
ตัวชี้วัดความถูกต้อง	Accuracy Rate: 92%, False Positive: 5%, False Negative: 3%
การวิเคราะห์อคติ	พบอคติเล็กน้อยในกลุ่มอายุ 18-25 ปี โดยระบบมีแนวโน้มปฏิเสธคำขอมากกว่ากลุ่มอื่น
ข้อเสนอแนะ	ปรับอัลกอริทึมการประเมินเครดิตเพื่อลดอคติในกลุ่มเยาวชน
การดำเนินการปรับปรุง	เริ่มพัฒนาโมเดลใหม่ตั้งแต่ 15 เมษายน 2025
หมายเหตุ	ระบบจะได้รับการตรวจสอบซ้ำในไตรมาสถัดไป

5. บันทึกการประชุมและแผนการปรับปรุง

วันที่	รายละเอียดการประชุม	ผู้เข้าร่วม	มติและแผนปฏิบัติ
5 เมษายน 2025	รายงานผลตรวจสอบและอคติ	ฝ่ายเทคนิค, ฝ่ายคุ้มครองข้อมูล	ยืนยันปรับปรุงโมเดลและเพิ่มมาตรการตรวจสอบประจำเดือน

6. เอกสารประกอบอื่น ๆ

- แบบฟอร์มตรวจสอบระบบอัตโนมัติ (Audit Checklist)
- ผลการประเมิน DPIA ที่เกี่ยวข้องกับระบบอัตโนมัติ
- รายงานการฝึกอบรมทีมงานเกี่ยวกับการจัดการอคติ

7. ช่องทางติดต่อ

หากต้องการสอบถามข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบระบบอัตโนมัติ ติดต่อได้ที่

อีเมล: privacy@example.com

โทร: 012-345-6789

4.11.1 ข้อมูลการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูล (DPO) หรือช่องทางการติดต่ออื่น ๆ จะต้องเปิดเผยแก่สาธารณะ หากบุคคลต้องการยื่นข้อร้องเรียนเกี่ยวกับการใช้ข้อมูลส่วนบุคคลของตน

สิ่งที่ต้องทำ: มีการแจ้งรายละเอียดการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต่อสาธารณะ

หลักฐาน: เอกสารหรือหลักฐานแสดงการแจ้งรายละเอียดการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (5), 41 วรรคห้า

ไม่มีมีกฎหมายกำหนดโทษ เว้นแต่ในทางปฏิบัติ องค์กรหรือหน่วยงานถูกร้องเรียน
หน่วยงานผู้กำกับดูแล (สคส.) เรียกให้ผู้ที่ถูกร้องเรียนมาชี้แจง หรือให้ข้อมูล หรือส่งเอกสาร
หลักฐานใด ๆ

ในกรณีที่ไมื่อยอมดำเนินการ หรือไม่ปฏิบัติตาม หรือไม่อำนวยความสะดวก นำโทษปรับทาง
ปกครองมาใช้บังคับ กำหนดโทษปรับทางปกครองไม่เกิน 5 แสนบาท

หลักการเปิดเผยข้อมูลการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

1. วัตถุประสงค์

เพื่อให้เจ้าของข้อมูลและผู้เกี่ยวข้องสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของ
องค์กรได้อย่างสะดวกและโปร่งใส ในกรณีต้องการยื่นคำร้องเรียน ขอคำชี้แจง หรือสอบถามเกี่ยวกับการใช้
ข้อมูลส่วนบุคคลของตน

2. ขอบเขต

การเปิดเผยข้อมูลการติดต่อของ DPO จะถูกเผยแพร่ต่อสาธารณะผ่านช่องทางหลักขององค์กร เช่น
เว็บไซต์หลัก หรือเอกสารนโยบายความเป็นส่วนตัว เพื่อให้ประชาชนทั่วไปสามารถเข้าถึงข้อมูลได้โดยง่าย

3. รายละเอียดข้อมูลการติดต่อ DPO ที่เปิดเผย

รายการ	รายละเอียด
ชื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	นายสมชาย ใจดี
ตำแหน่ง	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)
อีเมล	dpo@example.com
โทรศัพท์	02-123-4567
ที่อยู่สำนักงาน	อาคารเอ ชั้น 5 บริษัทตัวอย่าง จำกัด 123 ถนนสุขสวัสดิ์ เขตบางรัก กรุงเทพฯ 10500
ช่องทางเพิ่มเติม	แบบฟอร์มร้องเรียนออนไลน์ (ลิงก์ https://example.com/dpo-complaint)

4. วิธีการเผยแพร่ข้อมูลการติดต่อ DPO

- ประกาศในหน้าเว็บไซต์หลักขององค์กรในเมนู “นโยบายความเป็นส่วนตัว” และหน้า “ติดต่อเรา”
- ระบุในเอกสาร Privacy Policy / Privacy Notice ที่เผยแพร่สู่สาธารณะ

- รวมในเอกสารคู่มือหรือประกาศที่ใช้ภายในองค์กรและให้บริการลูกค้า
- แจ้งผ่านช่องทางสื่อสารออนไลน์ เช่น Facebook, Line Official (ถ้ามี)

5. ตัวอย่างข้อความแจ้งในเว็บไซต์

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO)

หากท่านมีข้อสงสัย หรือประสงค์จะยื่นคำร้องเรียนเกี่ยวกับการใช้ข้อมูลส่วนบุคคลของท่าน สามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลของเราได้ที่

อีเมล: dpo@example.com

โทรศัพท์: 02-123-4567

ที่อยู่: อาคารเอ ชั้น 5 บริษัทตัวอย่าง จำกัด 123 ถนนสุขสวัสดิ์ เขตบางรัก กรุงเทพฯ 10500

หรือกรอกแบบฟอร์มร้องเรียนออนไลน์ได้ที่ <https://example.com/dpo-complaint>

6. หลักฐานประกอบ

- ภาพหน้าจอเว็บไซต์ ที่แสดงข้อมูลการติดต่อ DPO
- สำเนาเอกสาร Privacy Policy/Privacy Notice ที่ระบุข้อมูลการติดต่อ DPO
- สำเนาเอกสารประกาศภายในองค์กร ที่แจ้งข้อมูลการติดต่อ DPO
- บันทึกการประชุม ที่มีมติอนุมัติการเปิดเผยข้อมูลการติดต่อ DPO

7. สภาพบังคับทางกฎหมายและผลที่ตามมา

- การเปิดเผยข้อมูลการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลเป็นไปตามมาตรา 23 (5) และมาตรา 41 (5) ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- หากองค์กรไม่ดำเนินการเปิดเผยข้อมูลนี้ หรือไม่ให้ความร่วมมือกับหน่วยงานกำกับดูแล อาจถูกเรียกชี้แจงและถูกปรับทางปกครองสูงสุดไม่เกิน 500,000 บาท

8. ช่องทางติดต่อเพิ่มเติมสำหรับสอบถามเรื่องคุ้มครองข้อมูลส่วนบุคคล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

เว็บไซต์: <https://www.pdpc.go.th>

โทรศัพท์: 02-123-4567

4.11.2 องค์กรแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับสิทธิในการร้องเรียนต่อสำนักงาน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือกรรมการผู้เชี่ยวชาญในประกาศการคุ้มครองข้อมูลส่วนบุคคล ขององค์กร (Privacy Notice)

สิ่งที่ต้องทำ: มีรายละเอียดแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับสิทธิในการร้องเรียนต่อสำนักงาน
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือกรรมการผู้เชี่ยวชาญในประกาศการคุ้มครอง
ข้อมูลส่วนบุคคลขององค์กร (Privacy Notice) พร้อมแนะนำขั้นตอนในการร้องเรียนอย่าง
ชัดเจน

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Privacy Notice)

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (6)
ไม่มีกฎหมายกำหนดโทษ เว้นแต่ในทางปฏิบัติ องค์กรหรือหน่วยงานถูกร้องเรียน
หน่วยงานผู้กำกับดูแล (สคส.) เรียกให้ผู้ที่ถูกร้องเรียนมาชี้แจง หรือให้ข้อมูล หรือส่งเอกสาร
หลักฐานใด ๆ
ในกรณีที่ไม่ยอมดำเนินการ หรือไม่ปฏิบัติตาม หรือไม่อำนวยความสะดวก นำโทษปรับทาง
ปกครองมาใช้บังคับ กำหนดโทษปรับทางปกครองไม่เกิน 5 แสนบาท

ตัวอย่างประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice) การแจ้งสิทธิในการร้องเรียน

1.ประกาศการคุ้มครองข้อมูลส่วนบุคคล

องค์กรของเราตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลของท่าน และมุ่งมั่นในการ
ดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงการรับรองสิทธิของเจ้าของข้อมูลส่วน
บุคคลทุกประการ

2.สิทธิในการร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) หรือกรรมการ ผู้เชี่ยวชาญ

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการร้องเรียนหากท่านเชื่อว่าการประมวลผลข้อมูลส่วนบุคคลของท่าน
ไม่เป็นไปตามข้อกำหนดของกฎหมาย หรือท่านไม่ได้รับการคุ้มครองตามสิทธิที่กฎหมายให้ไว้ โดยสามารถ
ดำเนินการได้ดังนี้

2.1 ติดต่อร้องเรียนโดยตรงกับองค์กรของเรา

ท่านสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของเรา เพื่อแจ้งปัญหา ขอคำชี้แจง
หรือยื่นคำร้องเรียน

อีเมล: dpo@example.com

โทรศัพท์: 02-123-4567

2.2.ร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

หากท่านไม่พอใจหรือไม่ได้รับการตอบสนองอย่างเหมาะสมจากองค์กร ท่านสามารถยื่นคำร้องเรียนต่อ สคส. ได้โดยตรงผ่านช่องทางต่าง ๆ ดังนี้

เว็บไซต์: <https://www.pdpc.go.th>

อีเมล: complaint@pdpc.go.th

โทรศัพท์: 02-123-4567

ที่อยู่: สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เลขที่ 1 ถนนนนทรี แขวงช่องนนทรี เขตยานนาวา กรุงเทพมหานคร 10120

2.3 การดำเนินการหลังยื่นคำร้องเรียน

สคส. จะทำการตรวจสอบข้อร้องเรียนและดำเนินการตามกฎหมายอย่างเป็นธรรมและโปร่งใส หากพบว่าการละเมิดกฎหมาย องค์กรอาจถูกสั่งให้แก้ไข ปรับปรุง หรือถูกลงโทษตามกฎหมาย

3.ข้อเสนอแนะสำคัญ

กรุณาเก็บหลักฐานหรือข้อมูลที่เกี่ยวข้องเพื่อใช้ประกอบคำร้องเรียน ระบุรายละเอียดให้ครบถ้วน เช่น ลักษณะการละเมิด สิทธิที่ได้รับผลกระทบ ข้อมูลการติดต่อของท่าน องค์กรของเรามุ่งมั่นที่จะตอบสนองคำร้องเรียนอย่างรวดเร็วและเป็นธรรม

4.เอกสารประกอบหลักฐาน

- ประกาศ Privacy Notice ที่เผยแพร่ในเว็บไซต์ขององค์กร
- ตัวอย่างข้อความแจ้งสิทธิในการร้องเรียนในเอกสารนโยบายความเป็นส่วนตัว
- ภาพหน้าจอเว็บไซต์ที่แสดงข้อความแจ้งสิทธิในการร้องเรียน
- เอกสารประชาสัมพันธ์หรือประกาศภายในองค์กร

5.สภาพบังคับตามกฎหมาย

การแจ้งสิทธิในการร้องเรียนเป็นไปตามมาตรา 23 (6) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หากองค์กรไม่ปฏิบัติตามหรือไม่อำนวยความสะดวก อาจถูกปรับทางปกครองสูงสุดไม่เกิน 500,000 บาท

4.11.3 องค์กรมีกระบวนการในการจัดการข้อร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และรายงานการแก้ไขปัญหาให้กับผู้บริหารระดับสูงทราบ

- สิ่งที่ต้องทำ: มีขั้นตอนในการจัดการข้อร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และรายงานการแก้ไขปัญหาให้กับผู้บริหารระดับสูงทราบ
- หลักฐาน: Privacy Notice/Privacy Policy ที่มีรายละเอียดเกี่ยวกับขั้นตอนในการจัดการข้อร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลรายงานการแก้ไขปัญหา
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

การจัดการข้อร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและรายงานผู้บริหาร

1. นโยบายหรือประกาศความเป็นส่วนตัว (Privacy Notice / Privacy Policy)

รายละเอียดขั้นตอนการจัดการข้อร้องเรียนเกี่ยวกับข้อมูลส่วนบุคคล

องค์กรของเรามุ่งมั่นในการคุ้มครองข้อมูลส่วนบุคคลและให้ความสำคัญกับสิทธิของเจ้าของข้อมูลในการร้องเรียนเมื่อมีข้อสงสัยหรือไม่พอใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล โดยมีขั้นตอนดังนี้

ขั้นตอนการจัดการข้อร้องเรียน

– รับเรื่องร้องเรียน

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือทีมงานที่ได้รับมอบหมาย จะรับเรื่องร้องเรียนจากเจ้าของข้อมูลผ่านช่องทางต่าง ๆ ได้แก่ อีเมล โทรศัพท์ หรือแบบฟอร์มร้องเรียนบนเว็บไซต์องค์กร

– บันทึกข้อมูลร้องเรียน

ทุกข้อร้องเรียนจะถูกบันทึกในระบบจัดการข้อร้องเรียน เพื่อให้สามารถติดตามสถานะและประวัติได้อย่างมีประสิทธิภาพ

– พิจารณาและตรวจสอบข้อร้องเรียน

ทีมงานจะทำการตรวจสอบข้อเท็จจริงที่เกี่ยวข้อง และประเมินผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูล

– ดำเนินการแก้ไขและตอบกลับ

เมื่อได้รับการตรวจสอบแล้ว องค์กรจะดำเนินการแก้ไขปัญหาหรือดำเนินมาตรการแก้ไข พร้อมแจ้งผลการดำเนินงานให้เจ้าของข้อมูลทราบภายในระยะเวลาที่เหมาะสม

– ปิดข้อร้องเรียน

หลังจากดำเนินการครบถ้วนและเจ้าของข้อมูลยอมรับผลการแก้ไข ข้อร้องเรียนจะถูกปิดในระบบจัดการข้อร้องเรียน

– เก็บรักษาเอกสาร

ข้อมูลและเอกสารเกี่ยวกับข้อร้องเรียนทั้งหมดจะถูกเก็บรักษาไว้อย่างปลอดภัยและเป็นความลับ

2. รายงานการแก้ไขปัญหาและข้อร้องเรียนต่อผู้บริหารระดับสูง

องค์กรจัดทำรายงานสรุปข้อร้องเรียนที่ได้รับ การดำเนินการแก้ไข และผลลัพธ์ที่เกิดขึ้นในแต่ละรอบระยะเวลา (เช่น รายเดือนหรือรายไตรมาส) เพื่อเสนอให้กับผู้บริหารระดับสูงรับทราบและกำกับดูแล เพื่อประเมินประสิทธิภาพการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมทั้งใช้ข้อมูลเป็นฐานในการปรับปรุงนโยบายและมาตรการภายในองค์กร

3. ตัวอย่างหลักฐานที่จัดเก็บและแสดง

- Privacy Notice / Privacy Policy ที่ระบุขั้นตอนจัดการข้อร้องเรียน
- แบบฟอร์มรับเรื่องร้องเรียน ที่ใช้ในการบันทึกข้อร้องเรียนของเจ้าของข้อมูล
- ระบบหรือสมุดบันทึกข้อร้องเรียน ที่แสดงรายละเอียดการรับเรื่อง ตรวจสอบ และสถานะของข้อร้องเรียน
- รายงานสรุปข้อร้องเรียนและการแก้ไขปัญหา ที่ส่งให้ผู้บริหารระดับสูง
- บันทึกการประชุมผู้บริหาร ที่มีการรายงานและติดตามผลการจัดการข้อร้องเรียน

4. สภาพบังคับและข้อสังเกต

- แม้กฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะไม่ได้กำหนดขั้นตอนจัดการข้อร้องเรียนอย่างชัดเจน แต่การมีระบบบริหารจัดการนี้ช่วยให้องค์กรปฏิบัติตามหลักการความรับผิดชอบและโปร่งใส (Accountability)
- ช่วยสร้างความเชื่อมั่นแก่เจ้าของข้อมูล และลดความเสี่ยงจากข้อร้องเรียนหรือการตรวจสอบจากหน่วยงานกำกับดูแล

บทที่ 6

การจัดทำเอกสารด้านการแจ้งวัตถุประสงค์และความโปร่งใส

ความโปร่งใสและการแจ้งวัตถุประสงค์ในการเก็บ ใช้ และประมวลผลข้อมูลส่วนบุคคลถือเป็นหลักการพื้นฐานของการคุ้มครองข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) การชี้แจงวัตถุประสงค์อย่างชัดเจนไม่เพียงช่วยสร้างความเชื่อมั่นแก่เจ้าของข้อมูล แต่ยังทำให้บุคลากรและหน่วยงานภายในองค์กร

ปฏิบัติตามนโยบายและแนวปฏิบัติได้อย่างถูกต้องและสอดคล้องกับกฎหมาย การจัดทำเอกสารเพื่อแจ้งวัตถุประสงค์และความโปร่งใสครอบคลุมทั้งการกำหนดวัตถุประสงค์ของการประมวลผลข้อมูล การชี้แจงประเภทและวิธีการใช้ข้อมูล รวมถึงการเผยแพร่ข้อมูลเหล่านี้แก่เจ้าของข้อมูลอย่างชัดเจนและเข้าถึงง่าย เอกสารเหล่านี้ไม่เพียงเป็นเครื่องมือสำหรับสื่อสาร แต่ยังเป็นหลักฐานสำคัญที่สามารถตรวจสอบได้ว่าองค์กรมีความมุ่งมั่นในการบริหารจัดการข้อมูลอย่างโปร่งใส

นอกจากนี้ การจัดทำเอกสารและช่องทางการสื่อสารที่ชัดเจน ยังช่วยให้เจ้าของข้อมูลสามารถตระหนักถึงสิทธิและความรับผิดชอบของตน รวมถึงสามารถตัดสินใจเกี่ยวกับการให้ความยินยอม หรือการใช้งานข้อมูลของตนได้อย่างรอบคอบ การสร้างวัฒนธรรมความโปร่งใสภายในองค์กรจึงเป็นกระบวนการต่อเนื่องที่ต้องมีการสื่อสาร ประเมินผล และปรับปรุงเอกสารและแนวทางปฏิบัติอย่างสม่ำเสมอ

บทนี้จึงมุ่งเน้นการจัดทำเอกสารด้านความโปร่งใสและการแจ้งวัตถุประสงค์ เพื่อให้มั่นใจว่าองค์กรสามารถสื่อสารกับเจ้าของข้อมูลได้อย่างชัดเจน ครบถ้วน และสอดคล้องกับข้อกำหนดของ PDPA ทั้งในด้าน การสร้างความเชื่อมั่น การปฏิบัติที่ถูกต้อง และการตรวจสอบ Compliance ขององค์กร

การบริหารจัดการข้อมูลส่วนบุคคลอย่างโปร่งใสและมีวัตถุประสงค์ชัดเจนถือเป็นหลักการพื้นฐานของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) การแจ้งวัตถุประสงค์ช่วยสร้างความเชื่อมั่นให้เจ้าของข้อมูลว่าข้อมูลส่วนบุคคลของตนจะถูกเก็บ ใช้ และประมวลผลอย่างถูกต้อง เหมาะสม และสอดคล้องกับกฎหมาย นอกจากนี้ยังช่วยให้บุคลากรและหน่วยงานภายในองค์กรมีแนวทางปฏิบัติที่ชัดเจน ลดความเสี่ยงจากการจัดการข้อมูลผิดวัตถุประสงค์หรือไม่โปร่งใส การจัดทำเอกสารด้านความโปร่งใสและการแจ้งวัตถุประสงค์ครอบคลุมหลายด้าน ทั้งการระบุวัตถุประสงค์ของการประมวลผลข้อมูล การกำหนดประเภทข้อมูลและขอบเขตการใช้ การอธิบายวิธีการใช้ข้อมูล การสื่อสารให้เจ้าของข้อมูลรับทราบ การจัดทำเอกสารขอความยินยอม การบันทึกหลักฐาน และการทบทวนปรับปรุงเอกสารอย่างต่อเนื่อง นอกจากนี้ การอบรมบุคลากรเกี่ยวกับวัตถุประสงค์การประมวลผลและแนวทางความโปร่งใสเป็นสิ่งสำคัญ เพื่อให้แน่ใจว่าการดำเนินงานสอดคล้องกับนโยบายและสามารถปฏิบัติได้จริง

บทนี้จึงมุ่งเน้นการสร้างกรอบการปฏิบัติที่ครอบคลุมและตรวจสอบได้สำหรับการแจ้งวัตถุประสงค์และความโปร่งใสของข้อมูลส่วนบุคคล ทั้งเพื่อสร้างความเชื่อมั่นแก่เจ้าของข้อมูล และเพื่อให้การดำเนินงานภายในองค์กรสอดคล้องกับ PDPA อย่างครบถ้วน

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/ หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
5.1 การระบุ วัตถุประสงค์ใน การประมวลผล ข้อมูล	ระบุวัตถุประสงค์ในการเก็บ ใช้ ประมวลผล และเปิดเผย ข้อมูลส่วนบุคคลอย่างชัดเจน สำหรับทุกกระบวนการ	เอกสารวัตถุประสงค์การ ประมวลผลข้อมูล (Data Processing Purpose Statement)	มีเอกสารชัดเจน ครอบคลุมทุกประเภท ข้อมูลและกระบวนการ
5.2 การกำหนด ขอบเขตและ ประเภทข้อมูล	ระบุประเภทข้อมูลที่เก็บและ ใช้ รวมถึงขอบเขตการ ประมวลผลที่สอดคล้องกับ วัตถุประสงค์	ตาราง/เอกสารสรุป ประเภทข้อมูล Data Inventory Data Mapping	ครอบคลุมทุกประเภท ข้อมูลที่เกี่ยวข้องและ สัมพันธ์กับวัตถุประสงค์
5.3 การชี้แจง วิธีการใช้ข้อมูล	อธิบายวิธีการเก็บ ใช้ และ ประมวลผลข้อมูลอย่าง โปร่งใส รวมถึงผู้เข้าถึงข้อมูล และระยะเวลาการเก็บ	Privacy Notice Policy Flowchart การ ประมวลผลข้อมูล	มีเอกสารชัดเจน สื่อสาร ได้เข้าใจง่าย และ ตรวจสอบได้
5.4 การเผยแพร่ และสื่อสารแก่ เจ้าของข้อมูล	แจ้งวัตถุประสงค์และ นโยบายความโปร่งใสให้ เจ้าของข้อมูลรับทราบผ่าน หลายช่องทาง	เว็บไซต์องค์กร Email Notice Board โปสเตอร์ e-Learning Modules	มีการเผยแพร่ครบถ้วน หลายช่องทาง ตรวจสอบ ได้ว่าเจ้าของข้อมูลเข้าถึง จริง
5.5 การจัดทำ เอกสารการ ยินยอม (Consent)	จัดทำเอกสาร/แบบฟอร์มขอ ความยินยอมการประมวลผล ข้อมูลตามวัตถุประสงค์	Consent Form e- Consent Record Log การให้ยินยอม	มีหลักฐานชัดเจนของการ ให้ยินยอม สามารถ ตรวจสอบย้อนหลังได้
5.6 การบันทึก และจัดเก็บ หลักฐาน	เก็บเอกสารและหลักฐาน เกี่ยวกับวัตถุประสงค์ ความ โปร่งใส และการยินยอม อย่างเป็นระบบ	ระบบจัดเก็บเอกสาร Data Inventory Log e-Log Version Control	มีระบบบันทึกครบถ้วน ตรวจสอบย้อนหลังได้ และอัปเดตตามเวอร์ชัน เอกสาร
5.7 การทบทวน และปรับปรุง เอกสาร	ทบทวนและปรับปรุงเอกสาร วัตถุประสงค์และความ โปร่งใสอย่างต่อเนื่องอย่าง น้อยปีละ 1 ครั้งหรือเมื่อ กฎหมายเปลี่ยน	บันทึก Version Control รายงานประชุม ปรับปรุงเอกสาร Memo การแก้ไขเอกสาร	มีหลักฐานการปรับปรุง ต่อเนื่อง แสดงการอัป เดตตามกฎหมายและ แนวทางใหม่

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/ หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
5.8 การอบรมและ สร้างความ ตระหนักรู้	อบรมบุคลากรเกี่ยวกับ วัตถุประสงค์การประมวลผล และแนวทางการสื่อสาร ความโปร่งใส	แผนอบรม สไลด์ แบบสอบถามก่อน-หลัง การอบรม Attendance Sheet	บุคลากรทุกระดับได้รับ การอบรม มีหลักฐาน ชัดเจน และสามารถ ปฏิบัติได้จริง
5.9 การเชื่อมโยง กับการบริหาร ความเสี่ยง	ผูกโยงวัตถุประสงค์และความ โปร่งใสเข้ากับระบบบริหาร ความเสี่ยงองค์กร	Risk Register รายงาน Audit ที่อ้างอิง วัตถุประสงค์และความ โปร่งใส	มีหลักฐานการติดตาม และจัดการความเสี่ยงที่ เกี่ยวข้องกับ ความโปร่งใส ครบถ้วน
5.10 การ ตรวจสอบภายใน (Internal Review)	ตรวจสอบว่าการสื่อสาร วัตถุประสงค์และความ โปร่งใสถูกนำไปใช้จริงและ สอดคล้องกับเอกสารที่จัดทำ ไว้	รายงานตรวจสอบภายใน แบบสอบถามบุคลากร Audit Checklist	มีรายงาน Audit/Review พร้อม ข้อเสนอแนะและ หลักฐานการปฏิบัติจริง

การจัดทำเอกสารตามเกณฑ์

5.1.1 มีการแจ้งรายละเอียดเกี่ยวกับข้อมูลการติดต่อที่เกี่ยวข้อง ได้แก่

- (1) ข้อมูลชื่อและรายละเอียด รวมถึงสถานที่ติดต่อและวิธีการติดต่อของผู้ควบคุมข้อมูลส่วนบุคคล
- (2) ข้อมูลชื่อและรายละเอียด รวมถึงสถานที่ติดต่อและวิธีการติดต่อของตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล (ถ้ามี)
- (3) ข้อมูลชื่อและรายละเอียด รวมถึงสถานที่ติดต่อและวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล (ถ้ามี)

สิ่งที่ต้องทำ: แจ้งรายละเอียดเกี่ยวกับข้อมูลการติดต่อของผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทน (ถ้ามี) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลครบถ้วนตามมาตรา 23 (5)

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (5)

โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตาม มาตรา 23 กำหนดโทษปรับทางปกครอง ไม่เกิน 1 ล้านบาท

ประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)

บทนำ

บริษัท ตัวอย่าง จำกัด (“บริษัท” หรือ “เรา”) มีความมุ่งมั่นที่จะปกป้องและเคารพสิทธิส่วนบุคคลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”) รวมทั้งกฎหมายและข้อบังคับที่เกี่ยวข้องทั้งหมด เพื่อให้ท่านมั่นใจว่า ข้อมูลส่วนบุคคลของท่านจะได้รับการเก็บรักษาและประมวลผลอย่างปลอดภัย โปร่งใส และเป็นธรรม

ประกาศนี้จัดทำขึ้นเพื่อแจ้งให้ท่านทราบเกี่ยวกับวิธีที่บริษัทเก็บรวบรวม ใช้ เปิดเผย และปกป้องข้อมูลส่วนบุคคลของท่าน รวมถึงแจ้งรายละเอียดเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทน และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท ซึ่งท่านสามารถติดต่อเพื่อใช้สิทธิต่าง ๆ หรือสอบถามข้อมูลเพิ่มเติมได้

1. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ผู้ควบคุมข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลที่มีอำนาจและรับผิดชอบในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล

รายละเอียดของผู้ควบคุมข้อมูลส่วนบุคคลของบริษัท มีดังนี้:

ชื่องค์กร: บริษัท ตัวอย่าง จำกัด

ที่อยู่: 123 ถนนตัวอย่าง แขวงตัวอย่าง เขตตัวอย่าง กรุงเทพมหานคร 10100

โทรศัพท์: 02-123-4567

อีเมล: contact@example.com

เว็บไซต์: www.example.com

ผู้ควบคุมข้อมูลส่วนบุคคลนี้เป็นผู้รับผิดชอบหลักในเรื่องการเก็บรวบรวม ใช้ และดูแลข้อมูลส่วนบุคคลของท่าน รวมทั้งรับผิดชอบในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและนโยบายของบริษัท

2. ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller’s Representative)

ในกรณีที่บริษัทเป็นนิติบุคคลต่างประเทศและมีการประมวลผลข้อมูลส่วนบุคคลของผู้ที่อาศัยอยู่ในประเทศไทย บริษัทได้แต่งตั้งตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลที่ตั้งอยู่ในประเทศไทย เพื่ออำนวยความสะดวกในการติดต่อและตอบข้อสงสัยต่าง ๆ

รายละเอียดตัวแทนผู้ควบคุมข้อมูลส่วนบุคคล:

ชื่อ: นาย สมชาย ตัวแทน

ที่อยู่: 456 ซอยตัวแทน แขวงตัวแทน เขตตัวแทน กรุงเทพมหานคร 10200

โทรศัพท์: 02-765-4321

อีเมล: representative@example.com

ในกรณีที่บริษัทไม่มีตัวแทนในประเทศไทย จะระบุว่า “ไม่มีตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทย”

3. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO)

เพื่อให้มั่นใจว่าการดำเนินงานทั้งหมดเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล บริษัทได้แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นผู้รับผิดชอบในการดูแลระบบและการปฏิบัติตามกฎหมาย รวมทั้งให้คำปรึกษาและรับเรื่องร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล:

ชื่อ: นางสาว สายใจ คุ้มครอง

ที่อยู่: ฝ่ายคุ้มครองข้อมูล บริษัท ตัวอย่าง จำกัด 123 ถนนตัวอย่าง แขวงตัวอย่าง เขตตัวอย่าง กรุงเทพมหานคร 10100

โทรศัพท์: 02-123-4568

อีเมล: dpo@example.com

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทำหน้าที่เป็นผู้ประสานงานหลักกับหน่วยงานกำกับดูแลและผู้ควบคุมข้อมูลส่วนบุคคลภายในองค์กร รวมถึงรับเรื่องร้องเรียนและให้คำแนะนำแก่เจ้าของข้อมูลส่วนบุคคล

4. ประเภทและวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล

บริษัทเก็บรวบรวมข้อมูลส่วนบุคคลประเภทต่าง ๆ จากท่าน เพื่อใช้ในวัตถุประสงค์ต่าง ๆ ที่ชัดเจน และเป็นธรรมตามกฎหมาย เช่น

- ข้อมูลส่วนบุคคลพื้นฐาน เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ และอีเมล
- ข้อมูลทางการเงิน เช่น ข้อมูลบัญชีธนาคาร สำหรับการชำระเงิน
- ข้อมูลการทำธุรกรรมและประวัติการใช้บริการ
- ข้อมูลสำหรับการตลาด เช่น ความสนใจและพฤติกรรมการใช้งาน

การเก็บรวบรวมข้อมูลดังกล่าวมีวัตถุประสงค์เพื่อให้บริการที่มีคุณภาพ การปรับปรุงบริการ การรักษาความปลอดภัย และปฏิบัติตามข้อกำหนดทางกฎหมาย

5. สิทธิของเจ้าของข้อมูลส่วนบุคคล

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ท่านมีสิทธิดังนี้:

- สิทธิในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล
- สิทธิในการขอแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้องหรือไม่สมบูรณ์
- สิทธิในการขอให้ลบข้อมูลส่วนบุคคลในกรณีที่ไม่จำเป็นหรือผิดกฎหมาย
- สิทธิในการคัดค้านการประมวลผลข้อมูลในบางกรณี
- สิทธิในการขอระงับการประมวลผลข้อมูล
- สิทธิในการย้ายข้อมูล (data portability)

หากท่านประสงค์ใช้สิทธิดังกล่าว กรุณาติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามข้อมูลติดต่อข้างต้น

6. ช่องทางการร้องเรียนและการติดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หากท่านมีข้อสงสัยหรือประสงค์จะร้องเรียนเกี่ยวกับการใช้ข้อมูลส่วนบุคคลของท่าน ท่านสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท หรือสามารถยื่นคำร้องต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ได้ตามรายละเอียดดังนี้:

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เว็บไซต์: www.pdpc.go.th

โทรศัพท์: 02-123-4567

อีเมล: complaints@pdpc.go.th

7. การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

บริษัทมีมาตรการทางเทคนิคและองค์กรที่เหมาะสมในการปกป้องข้อมูลส่วนบุคคลของท่านไม่ให้สูญหาย ถูกเข้าถึงโดยไม่ได้รับอนุญาต หรือถูกเปลี่ยนแปลงโดยไม่ชอบด้วยกฎหมาย รวมถึงมีการฝึกอบรมพนักงานเพื่อให้ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล

8. การเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลที่สาม

บริษัทจะไม่เปิดเผยข้อมูลส่วนบุคคลของท่านแก่บุคคลที่สาม นอกเสียจากได้รับความยินยอมจากท่าน หรือมีเหตุจำเป็นตามกฎหมาย เช่น การเปิดเผยข้อมูลให้หน่วยงานของรัฐที่มีอำนาจตามกฎหมาย

9. การเปลี่ยนแปลงประกาศความเป็นส่วนตัวนี้

บริษัทขอสงวนสิทธิ์ในการปรับปรุงหรือแก้ไขประกาศนี้ตามความเหมาะสมและตามการเปลี่ยนแปลงของกฎหมายหรือข้อกำหนดต่าง ๆ โดยจะแจ้งให้ท่านทราบล่วงหน้าทางเว็บไซต์ของบริษัทหรือช่องทางอื่น ๆ

10. สภาพบังคับและบทลงโทษ

ตามมาตรา 23 (5) แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ควบคุมข้อมูลส่วนบุคคลต้องเปิดเผยรายละเอียดข้อมูลการติดต่อที่เกี่ยวข้องครบถ้วนและชัดเจน หากไม่ปฏิบัติตาม อาจถูกปรับทางปกครองสูงสุดไม่เกิน 1,000,000 บาท

สรุป

ประกาศนี้จัดทำขึ้นเพื่อให้ท่านได้รับทราบถึงสิทธิและข้อมูลการติดต่อที่ชัดเจนในการติดต่อสอบถามหรือร้องเรียน

5.1.2 มีการแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ฐานทางกฎหมายที่ใช้ และอาจรวมถึงประโยชน์โดยชอบด้วยกฎหมายของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลนั้น
สิ่งที่ต้องทำ: แจ้งวัตถุประสงค์ ฐานทางกฎหมาย และประโยชน์โดยชอบด้วยกฎหมาย ครบถ้วน

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (1)
 แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูล
 ส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.
 2562
 โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตาม มาตรา 23 กำหนดโทษปรับทางปกครอง ไม่เกิน 1
 ล้านบาท

ประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)

วัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

บริษัท ตัวอย่าง จำกัด (“บริษัท” หรือ “เรา”) ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน และจึงได้จัดทำประกาศนี้เพื่อแจ้งให้ท่านทราบถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล รวมทั้งฐานทางกฎหมายและประโยชน์โดยชอบด้วยกฎหมายที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของท่าน ดังรายละเอียดต่อไปนี้

1. วัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

บริษัทเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์หลัก ดังนี้

– การให้บริการและบริหารจัดการลูกค้า

เพื่อให้บริการตามที่ท่านร้องขอ เช่น การจัดส่งสินค้า การให้คำปรึกษา และการจัดการบัญชีผู้ใช้งาน รวมถึงการจัดการเรื่องการชำระเงินและการออกใบเสร็จ

– การพัฒนาและปรับปรุงผลิตภัณฑ์และบริการ

ใช้ข้อมูลเพื่อวิเคราะห์ พัฒนา และปรับปรุงคุณภาพของผลิตภัณฑ์และบริการของบริษัทให้ตรงกับความต้องการของลูกค้าและตลาด

– การตลาดและการสื่อสาร

ใช้ข้อมูลส่วนบุคคลในการส่งข้อมูลข่าวสาร โปรโมชั่น หรือกิจกรรมที่เกี่ยวข้องกับผลิตภัณฑ์และบริการของบริษัท ผ่านช่องทางต่าง ๆ เช่น อีเมล ข้อความ หรือโทรศัพท์

– การปฏิบัติตามกฎหมายและข้อกำหนดทางกฎหมาย

เพื่อให้บริษัทสามารถปฏิบัติตามพันธกรณีตามกฎหมาย ข้อบังคับ หรือคำสั่งของหน่วยงานรัฐที่มีอำนาจ รวมถึงการป้องกันและตรวจสอบการทุจริต

- การบริหารความเสี่ยงและการรักษาความปลอดภัย

เพื่อป้องกันและจัดการความเสี่ยงที่อาจเกิดขึ้นต่อบริษัท รวมถึงการรักษาความปลอดภัยของระบบและข้อมูล

2. ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

บริษัทดำเนินการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของท่านโดยอาศัยฐานทางกฎหมายที่ชัดเจนและเหมาะสม ดังนี้

- การยินยอมของเจ้าของข้อมูล (Consent)

บริษัทจะเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลตามความยินยอมที่ได้รับจากท่าน เช่น การสมัครสมาชิก การสมัครใช้บริการ หรือการรับข่าวสารทางการตลาด

- การปฏิบัติตามสัญญา (Contractual Necessity)

การประมวลผลข้อมูลเพื่อดำเนินการตามสัญญาที่ท่านได้ทำกับบริษัท เช่น การจัดส่งสินค้า หรือการให้บริการต่าง ๆ

- การปฏิบัติตามกฎหมาย (Legal Obligation)

บริษัทต้องเก็บรวบรวมและประมวลผลข้อมูลเพื่อให้เป็นไปตามข้อกำหนดของกฎหมาย เช่น การรายงานภาษี หรือการให้ข้อมูลกับหน่วยงานรัฐตามคำสั่ง

- ผลประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interests)

บริษัทอาจเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่เกี่ยวข้องกับผลประโยชน์โดยชอบด้วยกฎหมายของบริษัท เช่น การบริหารจัดการความเสี่ยง การป้องกันการทุจริต หรือการพัฒนาธุรกิจ โดยจะพิจารณาให้เหมาะสมกับสิทธิและเสรีภาพของเจ้าของข้อมูล

3. ประโยชน์โดยชอบด้วยกฎหมายของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล

การประมวลผลข้อมูลส่วนบุคคลของท่านจะถูกดำเนินการภายใต้หลักการความชอบธรรมและความสมดุล ระหว่างผลประโยชน์ของบริษัทกับสิทธิและเสรีภาพของท่าน โดยมีประโยชน์ดังนี้

- เพื่อส่งมอบบริการและผลิตภัณฑ์ที่มีคุณภาพและตรงตามความต้องการของลูกค้า
- เพื่อรักษาความปลอดภัยและป้องกันความเสียหายที่อาจเกิดขึ้นต่อบริษัท ลูกค้า และบุคคลที่เกี่ยวข้อง
- เพื่อปฏิบัติตามพันธกรณีทางกฎหมายที่บริษัทต้องรับผิดชอบ
- เพื่อส่งเสริมการดำเนินธุรกิจอย่างโปร่งใส มีประสิทธิภาพ และสามารถตอบสนองต่อความคาดหวังของลูกค้าได้อย่างเหมาะสม

4. การเปิดเผยข้อมูลส่วนบุคคล

บริษัทอาจเปิดเผยข้อมูลส่วนบุคคลของท่านในกรณีต่าง ๆ ดังนี้

- เปิดเผยให้แก่หน่วยงานของรัฐหรือหน่วยงานกำกับดูแลตามที่กฎหมายกำหนด
- เปิดเผยให้กับผู้ให้บริการภายนอกที่ได้รับการแต่งตั้งจากบริษัทเพื่อช่วยดำเนินการตามวัตถุประสงค์ เช่น ผู้ให้บริการด้านไอที ผู้ให้บริการจัดส่งสินค้า
- เปิดเผยในกรณีที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- เปิดเผยเมื่อจำเป็นต้องใช้ในการป้องกันหรือดำเนินคดีทางกฎหมาย

บริษัทจะเปิดเผยข้อมูลโดยคำนึงถึงความปลอดภัยและสิทธิของเจ้าของข้อมูลเสมอ

5. วิธีการติดต่อและใช้สิทธิของเจ้าของข้อมูล

ท่านมีสิทธิในการเข้าถึง ขอแก้ไข ลบ หรือคัดค้านการประมวลผลข้อมูลส่วนบุคคล รวมถึงขอระงับหรือย้ายข้อมูลได้ โดยสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทตามข้อมูลที่ระบุในประกาศนี้

6. การปรับปรุงประกาศความเป็นส่วนตัวนี้

บริษัทอาจมีการปรับปรุงประกาศนี้ให้เหมาะสมและเป็นปัจจุบันตามกฎหมายและสถานการณ์ที่เปลี่ยนแปลง โดยจะแจ้งให้ท่านทราบผ่านช่องทางที่เหมาะสม

5.1.3 มีการแจ้งประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวม และแหล่งที่มาของข้อมูลส่วนบุคคล ในกรณีที่ข้อมูลส่วนบุคคลดังกล่าวได้มาจากแหล่งอื่น

สิ่งที่ต้องทำ: มีการแจ้งประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวม และแหล่งที่มาของข้อมูลส่วนบุคคล ครบถ้วน

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25
แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตาม มาตรา 25 กำหนดโทษปรับทางปกครอง ไม่เกิน 1 ล้านบาท

ประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)

ประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวมและแหล่งที่มาของข้อมูล

บริษัท ตัวอย่าง จำกัด (“บริษัท” หรือ “เรา”) ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน และแจ้งรายละเอียดเกี่ยวกับประเภทของข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวม รวมถึงแหล่งที่มาของข้อมูลส่วนบุคคลที่ไม่ได้เก็บรวบรวมโดยตรงจากเจ้าของข้อมูล ดังรายละเอียดต่อไปนี้

1. ประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวม

บริษัทเก็บรวบรวมข้อมูลส่วนบุคคลประเภทต่าง ๆ ตามความจำเป็นและวัตถุประสงค์ของการประมวลผล ซึ่งอาจรวมถึงแต่ไม่จำกัดเพียง

- ข้อมูลระบุตัวตน เช่น ชื่อ นามสกุล วันเกิด หมายเลขบัตรประจำตัวประชาชน หรือหนังสือเดินทาง
- ข้อมูลติดต่อ เช่น ที่อยู่ เบอร์โทรศัพท์ อีเมล
- ข้อมูลด้านการเงิน เช่น หมายเลขบัญชีธนาคาร ข้อมูลการชำระเงิน
- ข้อมูลด้านการทำงาน เช่น ตำแหน่งงาน ประวัติการทำงาน และข้อมูลการฝึกอบรม
- ข้อมูลด้านสุขภาพและความปลอดภัย (หากเกี่ยวข้อง)
- ข้อมูลพฤติกรรมการใช้งาน เช่น ประวัติการเข้าใช้บริการ ประวัติการซื้อสินค้า
- ข้อมูลที่ได้จากการติดต่อสื่อสาร เช่น ข้อความ อีเมล หรือบันทึกเสียง
- ข้อมูลอื่น ๆ ที่เกี่ยวข้องและจำเป็นสำหรับการดำเนินธุรกิจและการให้บริการของบริษัท

2. แหล่งที่มาของข้อมูลส่วนบุคคล

โดยปกติ บริษัทจะเก็บรวบรวมข้อมูลส่วนบุคคลจากท่านโดยตรงผ่านทางช่องทางต่าง ๆ เช่น แบบฟอร์มออนไลน์ การลงทะเบียน หรือการติดต่อสื่อสารกับบริษัท อย่างไรก็ตาม ในบางกรณี บริษัทอาจได้รับข้อมูลส่วนบุคคลของท่านจากแหล่งข้อมูลอื่นโดยชอบด้วยกฎหมายและภายใต้เงื่อนไขที่เหมาะสม ดังนี้

- จากผู้ให้บริการหรือพันธมิตรทางธุรกิจ เช่น บริษัทที่ให้บริการด้านการตลาด ผู้ให้บริการจัดส่งสินค้า หรือหน่วยงานที่ได้รับมอบหมายให้ดำเนินการแทนบริษัท
- จากฐานข้อมูลสาธารณะหรือแหล่งข้อมูลที่เปิดเผยต่อสาธารณะ เช่น ข้อมูลที่มีอยู่ในเว็บไซต์ขององค์กรภาครัฐ หรือฐานข้อมูลที่ได้รับอนุญาตให้ใช้ได้ตามกฎหมาย
- จากหน่วยงานของรัฐหรือหน่วยงานกำกับดูแล ในกรณีที่มีความจำเป็นต้องปฏิบัติตามกฎหมายหรือข้อบังคับ
- จากบุคคลที่สามที่ท่านได้มอบหมายหรือยินยอมให้ส่งข้อมูลมาให้บริษัท เช่น ตัวแทน หรือตัวกลางในการดำเนินการบางประการ
- จากระบบและเทคโนโลยีของบริษัทเอง เช่น ข้อมูลที่ได้จากการใช้งานเว็บไซต์ หรือแอปพลิเคชันของบริษัท

3. การใช้ข้อมูลจากแหล่งอื่น

เมื่อบริษัทได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น บริษัทจะดำเนินการตรวจสอบความถูกต้องและความเหมาะสมของข้อมูลก่อนนำไปใช้ และจะดำเนินการภายใต้หลักการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัดเพื่อรักษาสิทธิและเสรีภาพของเจ้าของข้อมูล

4. สิทธิของเจ้าของข้อมูล

เจ้าของข้อมูลมีสิทธิที่จะเข้าถึง ขอแก้ไข หรือลบข้อมูลส่วนบุคคลของตนที่บริษัทเก็บรวบรวมไว้ รวมทั้งสิทธิในการร้องเรียนหากมีข้อสงสัยหรือไม่พอใจเกี่ยวกับการเก็บรวบรวมและใช้ข้อมูล

5. วิธีการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ท่านสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทได้ตามรายละเอียดที่ระบุไว้ในประกาศนี้ เพื่อใช้สิทธิต่าง ๆ หรือสอบถามข้อมูลเพิ่มเติมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

5.1.4 มีการแจ้งประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย รวมถึงรายละเอียดการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

สิ่งที่ต้องทำ: มีการแจ้งประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย รวมถึงรายละเอียดการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศครบถ้วน

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (4)
 แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
 โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตาม มาตรา 23 กำหนดโทษปรับทางปกครอง ไม่เกิน 1 ล้านบาท

ประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)

การเปิดเผยข้อมูลส่วนบุคคลและการส่งโอนข้อมูลไปยังต่างประเทศ

บริษัท ตัวอย่าง จำกัด (“บริษัท” หรือ “เรา”) ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน และในประกาศนี้จะชี้แจงรายละเอียดเกี่ยวกับประเภทของบุคคลหรือหน่วยงานที่ข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวมอาจถูกเปิดเผย รวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ เพื่อความโปร่งใสและสร้างความมั่นใจแก่เจ้าของข้อมูล

1. ประเภทของบุคคลหรือหน่วยงานที่อาจได้รับข้อมูลส่วนบุคคลของท่าน

ข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวมอาจถูกเปิดเผยให้กับบุคคลหรือหน่วยงานดังต่อไปนี้ เพื่อวัตถุประสงค์ในการดำเนินธุรกิจ การให้บริการ การปฏิบัติตามกฎหมาย หรือภายใต้เงื่อนไขที่เหมาะสมและได้รับความยินยอมจากเจ้าของข้อมูล

- บุคลากรภายในบริษัท ที่มีหน้าที่รับผิดชอบดูแลข้อมูลและดำเนินงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- บริษัทในเครือและพันธมิตรทางธุรกิจ ที่ร่วมดำเนินกิจกรรมหรือโครงการกับบริษัท
- ผู้ให้บริการภายนอก (Third Party Service Providers) เช่น ผู้ให้บริการด้านเทคโนโลยีสารสนเทศ การตลาด การชำระเงิน และผู้ให้บริการจัดเก็บข้อมูล (Data Hosting Providers)
- หน่วยงานราชการและหน่วยงานกำกับดูแล ตามที่กฎหมายหรือข้อบังคับกำหนด
- ผู้รับโอนกิจการ ในกรณีที่บริษัทมีการโอนกิจการหรือร่วมธุรกิจกับองค์กรอื่น
- บุคคลภายนอกอื่น ๆ ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่แทนบริษัทภายใต้ข้อตกลงที่เหมาะสมเพื่อคุ้มครองข้อมูล

บริษัทจะตรวจสอบให้แน่ใจว่าผู้รับข้อมูลภายนอกมีมาตรการรักษาความปลอดภัยและคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสมตามกฎหมายและข้อตกลงที่เกี่ยวข้อง

2. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ในกรณีที่บริษัทจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลของท่านไปยังต่างประเทศ เช่น เพื่อสนับสนุนการให้บริการข้ามประเทศ การทำงานร่วมกับพันธมิตร หรือการจัดเก็บข้อมูลบนระบบคลาวด์ บริษัทจะดำเนินการภายใต้ข้อกำหนดและมาตรฐานความปลอดภัยที่เข้มงวด รวมทั้งปฏิบัติตามข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีรายละเอียดดังนี้

- บริษัทจะดำเนินการโอนข้อมูลเฉพาะไปยังประเทศที่ได้รับการรับรองว่ามีมาตรฐานการคุ้มครองข้อมูลที่เหมาะสม หรือมีมาตรการคุ้มครองข้อมูลเทียบเท่ากับมาตรฐานของประเทศไทย
- หากข้อมูลถูกโอนไปยังประเทศที่ไม่มีมาตรฐานคุ้มครองข้อมูลที่เทียบเท่า บริษัทจะใช้ข้อตกลงทางกฎหมายที่เหมาะสม เช่น ข้อตกลงแบบสัญญาคุ้มครองข้อมูลส่วนบุคคล (Standard Contractual Clauses) หรือมาตรการอื่น ๆ ที่ได้รับการยอมรับตามกฎหมาย
- บริษัทจะให้ข้อมูลเกี่ยวกับประเทศที่ข้อมูลถูกโอนไป และจุดประสงค์ของการโอนข้อมูลแก่เจ้าของข้อมูลเมื่อมีคำร้องขอ
- บริษัทจะติดตามและทบทวนมาตรการคุ้มครองข้อมูลเพื่อให้มั่นใจว่าการโอนข้อมูลยังคงปลอดภัยและเป็นไปตามกฎหมาย

3. สิทธิของเจ้าของข้อมูลเกี่ยวกับการเปิดเผยข้อมูลและการโอนข้อมูล

เจ้าของข้อมูลมีสิทธิที่จะขอรับข้อมูลเกี่ยวกับบุคคลหรือหน่วยงานที่ข้อมูลของตนถูกเปิดเผย รวมถึงสิทธิในการคัดค้านหรือจำกัดการเปิดเผยและการโอนข้อมูลตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด ท่านสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทเพื่อใช้สิทธิดังกล่าว

4. วิธีการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หากท่านมีข้อสงสัย หรือต้องการใช้สิทธิในข้อมูลส่วนบุคคลของท่าน กรุณาติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทผ่านช่องทางดังนี้

อีเมล: dpo@examplecompany.com

เบอร์โทรศัพท์: 0x-xxx-xxxx

ที่อยู่สำนักงาน: 123 อาคารตัวอย่าง ถนนตัวอย่าง แขวงตัวอย่าง เขตตัวอย่าง กรุงเทพมหานคร 10100

5.1.5 มีการแจ้งระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนด ระยะเวลาดังกล่าวได้ชัดเจน มีการแจ้งระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม สิ่งที่ต้องทำ: มีการแจ้งระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลครบถ้วน

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคลเอกสารแสดงการอ้างอิงกฎหมายที่กำหนดไว้เป็นการ เฉพาะ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (3)
แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูล ส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โทษทางปกครอง: ในกรณีที่未按ปฏิบัติตาม มาตรา 23 กำหนดโทษปรับทางปกครอง ไม่เกิน 1 ล้านบาท

ประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)

ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล

บริษัท ตัวอย่าง จำกัด (“บริษัท” หรือ “เรา”) ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน และแจ้งให้ทราบถึงระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลที่บริษัทเก็บรวบรวมจากท่านดังนี้

1. ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลของท่านเฉพาะในระยะเวลาที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ที่เก็บรวบรวมข้อมูลนั้น ๆ ตามที่ได้แจ้งไว้ในประกาศนี้ หรือในระยะเวลาที่กฎหมายที่เกี่ยวข้องกำหนด เช่น

- ข้อมูลที่เกี่ยวข้องกับการให้บริการแก่ลูกค้า จะเก็บไว้จนกว่าการให้บริการจะสิ้นสุด และในระยะเวลาต่อเนื่องเพื่อวัตถุประสงค์ทางบัญชี หรือทางกฎหมาย ตามที่กฎหมายกำหนด
- ข้อมูลที่เก็บเพื่อวัตถุประสงค์ทางการตลาด หรือการส่งเสริมการขาย จะเก็บไว้จนกว่าท่านจะถอนความยินยอมหรือไม่ประสงค์จะรับข้อมูล
- ข้อมูลที่เก็บเพื่อปฏิบัติตามข้อกำหนดทางกฎหมาย เช่น ภาษี การตรวจสอบบัญชี หรือข้อพิพาททางกฎหมาย บริษัทจะเก็บไว้ตามระยะเวลาที่กฎหมายกำหนด
- ในกรณีที่ไม่สามารถกำหนดระยะเวลาเก็บรักษาข้อมูลได้ชัดเจน บริษัทจะเก็บข้อมูลในระยะเวลาที่เหมาะสมที่สุดตามมาตรฐานปฏิบัติในอุตสาหกรรมหรือธุรกิจนั้น ๆ

2. ตัวอย่างระยะเวลาที่คาดหวังได้ของการเก็บข้อมูลส่วนบุคคลตามประเภทข้อมูล

ประเภทข้อมูลส่วนบุคคล	ระยะเวลาเก็บรักษาข้อมูล	เหตุผล/วัตถุประสงค์ในการเก็บรักษา
ข้อมูลลูกค้าและ การทำธุรกรรม	5 ปี หลังสิ้นสุดการให้บริการ	ปฏิบัติตามกฎหมายภาษี และวัตถุประสงค์ทางบัญชี
ข้อมูลผู้สมัครงาน	1 ปี หลังสิ้นสุดกระบวนการสรรหา	เพื่อรักษาข้อมูลสำหรับการสรรหาในอนาคต และปฏิบัติตามกฎหมายแรงงาน
ข้อมูลพนักงาน	ตามระยะเวลาที่กฎหมายแรงงานกำหนด (อย่างน้อย 50 ปี)	ปฏิบัติตามกฎหมายแรงงานและกฎหมายประกันสังคม
ข้อมูลสำหรับการตลาด	จนกว่าจะได้รับคำขอถอนความยินยอมหรือไม่เกิน 3 ปี	เพื่อการตลาดและส่งเสริมการขาย

3. การจัดการข้อมูลเมื่อครบกำหนดระยะเวลา

เมื่อครบกำหนดระยะเวลาการเก็บรักษาข้อมูลตามที่ระบุไว้ บริษัทจะดำเนินการลบ หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ (Anonymization) โดยเร็วและปลอดภัย เพื่อป้องกันการใช้งานในทางที่ผิด

4. สิทธิของเจ้าของข้อมูลในการสอบถามระยะเวลาการเก็บข้อมูล

ท่านมีสิทธิขอสอบถามข้อมูลเกี่ยวกับระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลของท่าน หรือขอให้ลบข้อมูลตามเงื่อนไขที่กฎหมายกำหนด โดยติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทตามรายละเอียดด้านล่าง

5. ช่องทางติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

อีเมล: dpo@examplecompany.com

โทรศัพท์: 0x-xxx-xxxx

ที่อยู่: 123 อาคารตัวอย่าง ถนนตัวอย่าง แขวงตัวอย่าง เขตตัวอย่าง กรุงเทพมหานคร 10100

เอกสารอ้างอิงกฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
มาตรา 23 (3) กำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งระยะเวลาในการเก็บรักษาข้อมูลหรือเกณฑ์การกำหนดระยะเวลาที่ชัดเจนแก่เจ้าของข้อมูล
- กรมสอบสวนคดีพิเศษ. (2563). แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล
- คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.). (2563). แนวทางการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

5.1.6 มีการแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงสิทธิในการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล (กรณีมีการขอความยินยอม) และสิทธิในการร้องเรียนในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: มีการแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคลทราบครบถ้วน

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (6)

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตาม มาตรา 23 กำหนดโทษปรับทางปกครอง ไม่เกิน 1 ล้านบาท

ประกาศการคุ้มครองข้อมูลส่วนบุคคล

หัวข้อ: การแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคล

บริษัท ตัวอย่าง จำกัด (“บริษัท” หรือ “เรา”) มีความมุ่งมั่นในการคุ้มครองข้อมูลส่วนบุคคลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยท่านในฐานะเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่สามารถใช้ได้ภายใต้กฎหมายดังกล่าวดังนี้

สิทธิของเจ้าของข้อมูลส่วนบุคคล

1. สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right of Access)

ท่านมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลของท่านที่อยู่ภายใต้ความรับผิดชอบของบริษัท รวมถึงขอให้บริษัทเปิดเผยแหล่งที่มาของข้อมูลส่วนบุคคลหากได้รับจากแหล่งอื่น

2. สิทธิในการแก้ไขข้อมูล (Right to Rectification)

ท่านมีสิทธิขอให้บริษัทแก้ไขข้อมูลส่วนบุคคลของท่านให้ถูกต้อง สมบูรณ์ และเป็นปัจจุบัน

3. สิทธิในการลบข้อมูล (Right to Erasure)

ท่านมีสิทธิขอให้บริษัทลบข้อมูลส่วนบุคคลของท่าน หากข้อมูลนั้นไม่มีความจำเป็นในการเก็บรักษาอีกต่อไป หรือเมื่อมีการถอนความยินยอม (ถ้ามี)

4. สิทธิในการจำกัดการประมวลผลข้อมูล (Right to Restriction of Processing)

ท่านมีสิทธิขอให้บริษัทระงับการใช้ข้อมูลของท่านเป็นการชั่วคราวในบางกรณี เช่น อยู่ระหว่างการตรวจสอบความถูกต้องของข้อมูล

5. สิทธิในการคัดค้านการประมวลผลข้อมูล (Right to Object)

ท่านมีสิทธิคัดค้านการประมวลผลข้อมูลของท่านในบางกรณี เช่น การประมวลผลเพื่อการตลาดทางตรง หรือการประมวลผลที่เกี่ยวข้องกับประโยชน์โดยชอบด้วยกฎหมาย

6. สิทธิในการโอนย้ายข้อมูล (Right to Data Portability)

ท่านมีสิทธิขอรับข้อมูลส่วนบุคคลของท่านในรูปแบบที่สามารถอ่านหรือใช้งานได้โดยทั่วไป และส่งต่อข้อมูลนั้นไปยังผู้ควบคุมข้อมูลรายอื่นได้

การถอนความยินยอม (ในกรณีที่ให้ความยินยอมเป็นฐานทางกฎหมาย)

หากบริษัทประมวลผลข้อมูลส่วนบุคคลของท่านโดยอาศัยความยินยอม ท่านมีสิทธิถอนความยินยอมได้ทุกเมื่อ โดยการถอนความยินยอมจะไม่กระทบต่อการประมวลผลข้อมูลที่เกิดขึ้นก่อนหน้านั้น ท่านสามารถถอนความยินยอมได้โดยติดต่อผ่านอีเมลหรือช่องทางติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่ระบุด้านล่าง

สิทธิในการร้องเรียนต่อหน่วยงานกำกับดูแล

หากท่านเห็นว่าบริษัทได้กระทำการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ท่านมีสิทธิร้องเรียนต่อ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

เว็บไซต์: www.pdpc.go.th

ช่องทางติดต่อเพื่อใช้สิทธิ

ท่านสามารถใช้สิทธิต่าง ๆ ข้างต้นโดยติดต่อผ่าน

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ชื่อ: คุณสมพร ข้อมูลดี

อีเมล: dpo@example.com

โทรศัพท์: 02-123-4567

ที่อยู่: บริษัท ตัวอย่าง จำกัด 123 ถนนสุขุมวิท แขวงคลองเตย เขตคลองเตย กรุงเทพฯ 10110

บริษัทจะดำเนินการตอบสนองคำขอของท่านโดยไม่ล่าช้า ภายในระยะเวลาไม่เกิน 30 วันนับแต่วันที่ได้รับคำขอ โดยไม่คิดค่าธรรมเนียม เว้นแต่เป็นกรณีที่มีความซับซ้อนหรือมีคำขอซ้ำซ้อนกันหลายครั้ง

5.1.7 มีการแจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย หรือสัญญา หรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล (ถ้าหากมี หรือในกรณีที่เก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล)

สิ่งที่ต้องทำ: มีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบครบถ้วน

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (2)

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตาม มาตรา 23 กำหนดโทษปรับทางปกครอง ไม่เกิน 1 ล้านบาท

ประกาศการคุ้มครองข้อมูลส่วนบุคคล

หัวข้อ: การแจ้งภาระหน้าที่ในการให้ข้อมูล และผลกระทบจากการไม่ให้ข้อมูลส่วนบุคคล

บริษัท ตัวอย่าง จำกัด (“บริษัท” หรือ “เรา”) ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน และมุ่งมั่นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (2) บริษัทขอแจ้งรายละเอียดสำคัญดังต่อไปนี้

1. กรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลตามกฎหมาย

ในบางกรณี การให้ข้อมูลส่วนบุคคลเป็นข้อกำหนดตามกฎหมาย เช่น

- กฎหมายแรงงาน ที่กำหนดให้เก็บข้อมูลส่วนบุคคลของพนักงาน เช่น สำเนาบัตรประชาชน ใบสำคัญการสมรส ใบสำคัญการหย่า ฯลฯ
- กฎหมายภาษีอากร เช่น การเก็บเลขประจำตัวผู้เสียภาษีของพนักงานเพื่อการยื่นภาษีเงินได้หัก ณ ที่จ่าย
- กฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ที่กำหนดให้สถาบันการเงินตรวจสอบและยืนยันตัวตนของลูกค้า

หากท่านไม่ให้ข้อมูลที่กฎหมายกำหนด อาจส่งผลให้บริษัทไม่สามารถปฏิบัติตามข้อกำหนดของกฎหมายหรือให้บริการท่านได้

2. กรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลเพื่อเข้าสู่สัญญา

ในหลายกรณี ข้อมูลส่วนบุคคลจำเป็นสำหรับการทำสัญญาหรือการให้บริการ เช่น

- ข้อมูลเพื่อทำสัญญาจ้างงาน ได้แก่ ชื่อ-นามสกุล ข้อมูลบัญชีธนาคาร รายละเอียดติดต่อของผู้สมัครงาน
- ข้อมูลที่ใช้ทำสัญญากับลูกค้าหรือคู่ค้า เช่น เลขประจำตัวประชาชน ที่อยู่ เลขที่บัญชี หรือข้อมูลทางการเงิน

หากท่านไม่ให้ข้อมูลส่วนบุคคลดังกล่าว บริษัทอาจไม่สามารถทำสัญญา หรือให้บริการตามข้อตกลงได้

3. ผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

หากท่านปฏิเสธที่จะให้ข้อมูลในกรณีที่กฎหมายหรือสัญญากำหนด อาจก่อให้เกิดผลกระทบ เช่น

- ไม่สามารถเข้าสู่กระบวนการสมัครงาน หรือจ้างงานได้
- ไม่สามารถให้บริการหรือทำธุรกรรมตามสัญญาได้
- ไม่สามารถเข้าถึงสิทธิประโยชน์ตามนโยบายของบริษัท เช่น ประกันสุขภาพหรือสวัสดิการต่าง ๆ

บริษัทอาจมีความจำเป็นต้องปฏิเสธการให้บริการหรือยกเลิกความสัมพันธ์ทางสัญญา เพื่อปฏิบัติตามกฎหมาย

ช่องทางติดต่อเพิ่มเติม

หากท่านมีคำถามเกี่ยวกับเหตุผลในการเก็บรวบรวมข้อมูล หรือผลกระทบจากการไม่ให้ข้อมูล ท่านสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ที่:

ชื่อ: คุณสมพร ข้อมูลดี

อีเมล: dpo@example.com

โทรศัพท์: 02-123-4567

ที่อยู่: บริษัท ตัวอย่าง จำกัด 123 ถนนสุขุมวิท แขวงคลองเตย เขตคลองเตย กรุงเทพฯ 10110

5.1.8 ในกรณีของการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง องค์กรได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงแหล่งที่มาของข้อมูลนั้น เช่น จากสื่อสังคมออนไลน์ ข้อมูลการลงทะเบียนต่าง ๆ ที่เปิดเผยเป็นสาธารณะ หรือจากฐานข้อมูลนิติบุคคล เป็นต้น

สิ่งที่ต้องทำ: มีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบครบถ้วน

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตาม มาตรา 25 กำหนดโทษปรับทางปกครอง ไม่เกิน 3 ล้านบาท

ประกาศการคุ้มครองข้อมูลส่วนบุคคล

หัวข้อ: การแจ้งแหล่งที่มาของข้อมูลส่วนบุคคลในกรณีที่ไม่ได้รับโดยตรงจากเจ้าของข้อมูล

บริษัท ตัวอย่าง จำกัด ให้ความสำคัญกับสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูลทุกท่าน และมุ่งมั่นในการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25 บริษัทขอแจ้งให้ทราบถึงการดำเนินการในกรณีที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรง ดังนี้

1. แหล่งที่มาของข้อมูลส่วนบุคคลที่บริษัทอาจได้รับจากแหล่งอื่น

ในบางกรณี บริษัทอาจได้รับข้อมูลส่วนบุคคลจากแหล่งอื่นที่มีใช้การให้ข้อมูลโดยตรงจากเจ้าของข้อมูล เช่น

- ข้อมูลจากสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, LinkedIn, Twitter โดยเฉพาะในกรณีที่มีการเปิดเผยข้อมูลเป็นสาธารณะ
- ข้อมูลจากผู้ให้บริการข้อมูลทางธุรกิจ เช่น ฐานข้อมูลนิติบุคคล หรือฐานข้อมูลจัดซื้อจัดจ้างภาครัฐ
- ข้อมูลจากผู้ให้บริการจัดหางาน หรือบริษัทรับสมัครงาน
- ข้อมูลจากพันธมิตรทางธุรกิจหรือผู้รับมอบอำนาจของเจ้าของข้อมูล
- ข้อมูลจากแหล่งที่มีการให้ความยินยอมล่วงหน้าแล้ว เช่น ระบบลงทะเบียนออนไลน์ในกิจกรรมต่าง ๆ
- ข้อมูลจากหน่วยงานภาครัฐที่เปิดเผยเป็นสาธารณะโดยชอบด้วยกฎหมาย เช่น กรมพัฒนาธุรกิจการค้า

2. วัตถุประสงค์ของการเก็บรวบรวมข้อมูลจากแหล่งอื่น

ข้อมูลที่ได้รับจากแหล่งอื่นอาจนำมาใช้เพื่อวัตถุประสงค์ดังต่อไปนี้

- การตรวจสอบคุณสมบัติในการรับเข้าทำงานหรือรับทุนสนับสนุน
- การติดต่อเพื่อให้ข้อมูลข่าวสารเกี่ยวกับผลิตภัณฑ์หรือบริการ
- การพิจารณาความเหมาะสมในการเป็นคู่ค้าทางธุรกิจ
- การดำเนินกิจกรรมทางการตลาดที่ไม่ละเมิดสิทธิส่วนบุคคล
- การประเมินความเสี่ยงตามข้อกำหนดของกฎหมายหรือระเบียบภายในองค์กร

3. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เมื่อบริษัทได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น บริษัทจะแจ้งให้ท่านทราบถึงสิทธิของท่านภายในระยะเวลาอันสมควร เช่น

- สิทธิขอเข้าถึงและรับสำเนาข้อมูล
- สิทธิขอแก้ไขข้อมูลให้ถูกต้อง
- สิทธิขอให้ลบหรือทำลายข้อมูล
- สิทธิขอให้ระงับการใช้ข้อมูล
- สิทธิในการคัดค้านการประมวลผลข้อมูล
- สิทธิในการร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

4. วิธีการแจ้งเจ้าของข้อมูล

เมื่อได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น บริษัทจะดำเนินการแจ้งให้เจ้าของข้อมูลทราบถึง:

- แหล่งที่มาของข้อมูล
- วัตถุประสงค์ในการใช้
- ฐานทางกฎหมาย
- สิทธิของเจ้าของข้อมูล
- ข้อมูลการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

โดยจะมีการแจ้งผ่านวิธีการที่เหมาะสม เช่น ทางอีเมล แบบฟอร์มออนไลน์ หรือการแจ้งผ่านเว็บไซต์ของบริษัท ภายในระยะเวลาไม่เกิน 30 วัน นับแต่วันที่ได้รับข้อมูล

5. ข้อยกเว้นตามกฎหมาย

บริษัทอาจไม่มีความจำเป็นต้องแจ้งเจ้าของข้อมูล ในกรณีที่:

- เจ้าของข้อมูลได้รับการแจ้งแล้วก่อนหน้านี้
- เป็นการใช้ข้อมูลเพื่อประโยชน์สาธารณะ หรือตามหน้าที่ราชการ
- การแจ้งอาจทำให้การบรรลุวัตถุประสงค์ของการใช้ข้อมูลล้มเหลว
- กฎหมายเฉพาะบัญญัติไว้เป็นอย่างอื่น

ช่องทางติดต่อ

หากท่านต้องการสอบถามเกี่ยวกับแหล่งที่มาของข้อมูล หรือใช้สิทธิของเจ้าของข้อมูล กรุณาติดต่อ:

ชื่อ: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

อีเมล: dpo@example.com

โทรศัพท์: 02-123-4567

ที่อยู่: บริษัท ตัวอย่าง จำกัด 123 ถนนสุขุมวิท กรุงเทพฯ 10110

5.2.1 เจ้าของข้อมูลส่วนบุคคลได้รับแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล ในขณะที่ข้อมูลส่วนบุคคลถูกเก็บรวบรวม อาทิ ในขณะที่กรอกแบบฟอร์ม หรือจากกรณีที่อาจสังเกตเห็นได้เอง (or by observation) เช่น การถูกบันทึกภาพโดยระบบกล้องวงจรปิด หรือการถูกติดตามพฤติกรรมออนไลน์ เป็นต้น

สิ่งที่ต้องทำ: มีหลักฐานการได้รับแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล ครบถ้วน

หลักฐาน: หลักฐานการได้รับแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่น ข้อความในรูปแบบ SMS, email, ภาพถ่าย ป้ายที่แสดงว่ามีการเก็บข้อมูลผ่านกล้องวงจรปิด เป็นต้น

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23
แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตาม มาตรา 23 กำหนดโทษปรับทางปกครอง ไม่เกิน 1 ล้านบาท

ข้อเอกสาร: หลักฐานการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล ณ จุดเก็บรวบรวม

ตามเกณฑ์ข้อ 5.2.1

1. วัตถุประสงค์

เพื่อใช้เป็นหลักฐานแสดงว่าองค์กรได้แจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบถึงวัตถุประสงค์และรายละเอียดที่เกี่ยวข้องอย่างชัดเจน ขณะมีการเก็บรวบรวมข้อมูล ตามที่กำหนดไว้ในมาตรา 23 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ตัวอย่างการแจ้งที่ใช้จริง

2.1 แบบฟอร์มออนไลน์/ออฟไลน์ที่มีการแจ้งวัตถุประสงค์

แบบฟอร์มลงทะเบียนพนักงาน/ลูกค้า มีข้อความต่อไปนี้แนบไว้ก่อนช่องให้กรอกข้อมูล:

“บริษัทจะใช้ข้อมูลส่วนบุคคลที่ท่านกรอกในแบบฟอร์มนี้เพื่อวัตถุประสงค์ในการติดต่อกลับ ประเมินคุณสมบัติการรับสมัคร และจัดเก็บเป็นประวัติภายใน ไม่เปิดเผยแก่บุคคลภายนอก เว้นแต่ได้รับความยินยอมจากท่าน หรือมีเหตุจำเป็นตามกฎหมาย...”

แนบ: ภาพถ่ายหน้าฟอร์ม หรือ screenshot หน้าเว็บไซต์ที่มีการแจ้ง

2.2 SMS หรือ Email ที่ใช้แจ้งขณะเก็บข้อมูล

ตัวอย่างข้อความ SMS:

“เรียนคุณสมชาย บริษัทเก็บข้อมูลเบอร์โทรศัพท์ของท่านเพื่อใช้ยืนยันตัวตนในการใช้งานระบบบริการลูกค้า รายละเอียดเพิ่มเติม: www.example.com/privacy”

แนบ: ภาพถ่ายหน้าจอ SMS / อีเมลที่มีข้อความดังกล่าว

2.3 ป้ายแจ้งหน้ากล้องวงจรปิด (CCTV Notice)

ข้อความในป้าย:

“บริเวณนี้มีกล้องวงจรปิดบันทึกภาพเพื่อความปลอดภัยในชีวิตและทรัพย์สินของพนักงานและบุคคลภายนอก หากต้องการทราบข้อมูลเพิ่มเติมกรุณาติดต่อแผนกบุคคล โทร 02-xxx-xxxx หรือดูนโยบายได้ที่ www.example.com/privacy”

แนบ: ภาพถ่ายป้ายที่ติดตั้งบริเวณทางเข้าอาคารหรือภายในสถานที่

2.4 การแจ้งผ่านเว็บไซต์ (Cookie & Tracking Policy)

ตัวอย่างแบนเนอร์แจ้ง:

“เว็บไซต์ของเรามีการใช้คุกกี้เพื่อวิเคราะห์การใช้งานและปรับปรุงประสบการณ์ของผู้ใช้ โดยการใช้งานเว็บไซต์ต่อไปถือว่าท่านยอมรับการใช้คุกกี้ตามนโยบายของเรา [อ่านเพิ่มเติม]”

แนบ: ภาพหน้าจอหน้าแรกของเว็บไซต์ พร้อมแบนเนอร์แจ้ง

ตัวอย่างข้อความในฟอร์ม (แบบฟอร์มลงทะเบียน/สมัครงาน/แบบสอบถาม)

แบบฟอร์มลงทะเบียนเข้าร่วมอบรมภายในองค์กร

ชื่อ-นามสกุล:

อีเมล:

หมายเลขโทรศัพท์:

ประกาศเรื่องการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลที่ท่านให้ไว้ในแบบฟอร์มนี้ จะถูกเก็บรวบรวม ใช้ และเปิดเผยโดยหน่วยงาน [ชื่อหน่วยงาน] เพื่อวัตถุประสงค์ในการจัดการลงทะเบียน ติดต่อกลับ ประเมินผลการเข้าร่วม และรายงานต่อผู้เกี่ยวข้อง

หน่วยงานจะไม่เปิดเผยข้อมูลของท่านต่อบุคคลภายนอก เว้นแต่ได้รับความยินยอมจากท่าน หรือมีเหตุจำเป็นตามกฎหมาย

สามารถศึกษารายละเอียดนโยบายความเป็นส่วนตัวเพิ่มเติมได้ที่ [ลิงก์]

☐ ข้าพเจ้าได้อ่านและรับทราบประกาศการคุ้มครองข้อมูลส่วนบุคคล

ตัวอย่างป้ายแจ้งการบันทึกภาพจากกล้องวงจรปิด (CCTV Notice)

บริเวณนี้มีการบันทึกภาพด้วยกล้องวงจรปิด (CCTV)

เพื่อวัตถุประสงค์ด้านความปลอดภัยในชีวิตและทรัพย์สินของพนักงาน ผู้มาติดต่อ และทรัพย์สินขององค์กร ภาพจากกล้องจะถูกจัดเก็บและเข้าถึงโดยเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น และจะจัดเก็บไว้ไม่เกิน [ระยะเวลา เช่น 30 วัน] นับจากวันที่บันทึก

หากท่านต้องการสอบถามข้อมูลเพิ่มเติมเกี่ยวกับนโยบายคุ้มครองข้อมูลส่วนบุคคล กรุณาติดต่อ:
ฝ่ายบริหารความปลอดภัย: 02-XXX-XXXX
หรืออ่านรายละเอียดได้ที่: [www.example.com/privacy]

ตัวอย่างแบนเนอร์แจ้งเตือนการใช้คุกกี้และการติดตาม (Cookie Banner / Web Notification)

เว็บไซต์ของเรามีการใช้คุกกี้เพื่อให้ท่านได้รับประสบการณ์ที่ดีที่สุด รวมถึงวิเคราะห์การใช้งานเว็บไซต์ โดยการใช้งานเว็บไซต์นี้ต่อไป ถือว่าท่านยินยอมให้เราใช้คุกกี้ตาม นโยบายความเป็นส่วนตัว
[อ่านเพิ่มเติม] | [ยินยอมและปิดหน้าต่างนี้]

5.2.2 ในกรณีของการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น (other sources) ที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง องค์กรได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกิน 30 วันนับแต่วันที่ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: มีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายใน 30 วัน

หลักฐาน: หลักฐานการบันทึกข้อมูลวันที่ได้รับข้อมูลจากแหล่งอื่น และวันที่แจ้งข้อมูลและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

หลักฐานการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตาม มาตรา 25 กำหนดโทษปรับทางปกครอง ไม่เกิน 1 ล้านบาท

แบบฟอร์มบันทึกการเก็บข้อมูลจากแหล่งอื่น และการแจ้งเจ้าของข้อมูล

ชื่อเอกสาร: แบบฟอร์มบันทึกการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

หน่วยงาน: [ชื่อหน่วยงานหรือองค์กร]

รายการ

รายละเอียด

วันที่ได้รับข้อมูลจากแหล่งอื่น	3 พฤษภาคม 2568
แหล่งที่มา	ฐานข้อมูลสมาชิกองค์กรพันธมิตร: บริษัท ABC จำกัด
ประเภทของข้อมูลที่ได้รับ	ชื่อ-นามสกุล เบอร์โทรศัพท์ อีเมล
วัตถุประสงค์ในการเก็บข้อมูล	เพื่อส่งข้อมูลข่าวสารและกิจกรรมส่งเสริมการตลาดขององค์กร
วันที่แจ้งเจ้าของข้อมูลส่วนบุคคล	10 พฤษภาคม 2568
วิธีการแจ้ง	Email โดยแนบประกาศแจ้งการเก็บข้อมูลส่วนบุคคล
หลักฐานการแจ้ง	สำเนา Email พร้อมเวลาส่ง (แนบไว้ท้ายเอกสาร)
วันที่ได้รับความยินยอม	15 พฤษภาคม 2568
ช่องทางการยินยอม	ผ่านลิงก์แบบฟอร์มออนไลน์ (Google Form / Microsoft Form)
แนบไฟล์	สำเนาหน้าจอฟอร์มยินยอมและรายการผู้ตอบแบบฟอร์ม

ตัวอย่างประกาศแจ้งเจ้าของข้อมูล

ประกาศแจ้งการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น

เรียน คุณ [ชื่อเจ้าของข้อมูล]

หน่วยงาน [ชื่อหน่วยงาน] ได้รับข้อมูลของท่านจาก [ระบุแหล่งที่มา เช่น ฐานข้อมูลของบริษัท ABC จำกัด ซึ่งเป็นพันธมิตรทางธุรกิจขององค์กร] โดยมีข้อมูล ได้แก่ ชื่อ-นามสกุล อีเมล และเบอร์โทรศัพท์ ข้อมูลนี้จะถูกใช้เพื่อวัตถุประสงค์ในการ [เช่น การแจ้งข้อมูลข่าวสาร กิจกรรมโปรโมชัน หรือการติดต่อสื่อสารที่จำเป็น] ตามนโยบายความเป็นส่วนตัวของเรา

หากท่านไม่ประสงค์ให้เราใช้ข้อมูลของท่าน กรุณาคลิกด้านล่างเพื่อลบข้อมูล หรือยืนยันการให้ความยินยอมได้ที่ [ลิงก์ฟอร์มยินยอม]

ศึกษารายละเอียดเพิ่มเติมได้ที่: [ลิงก์ประกาศคุ้มครองข้อมูล]

ขอแสดงความนับถือ

[ชื่อเจ้าหน้าที่/แผนกติดต่อ]

[เบอร์โทรศัพท์] | [อีเมลติดต่อ]

แบบฟอร์มยินยอมออนไลน์ (ตัวอย่างเนื้อหา)

แบบฟอร์มยินยอมการใช้ข้อมูลส่วนบุคคล

ข้าพเจ้ารับทราบว่า ข้อมูลส่วนบุคคลของข้าพเจ้า (ชื่อ, เบอร์โทร, อีเมล) ได้ถูกเก็บมาจากบริษัทพันธมิตร และข้าพเจ้ายินยอมให้องค์กร [ชื่อหน่วยงาน] ใช้ข้อมูลของข้าพเจ้าสำหรับการส่งข้อมูลข่าวสารและกิจกรรมที่เกี่ยวข้องตามที่ระบุในประกาศการคุ้มครองข้อมูลส่วนบุคคล

☐ ข้าพเจ้ายินยอมให้มีการใช้ข้อมูลส่วนบุคคลตามประกาศดังกล่าว

ชื่อ-นามสกุล:

วันที่ยินยอม:

5.3.1 ใช้กระบวนการเชิงรุกในการแจ้งให้บุคคลทราบถึงวัตถุประสงค์และรายละเอียดต่าง ๆ และมีวิธีเข้าถึงข้อมูลดังกล่าวได้ง่ายและไม่มีค่าใช้จ่าย

สิ่งที่ต้องทำ: มีกระบวนการเชิงรุก และมีวิธีเข้าถึงข้อมูลดังกล่าวได้ง่ายและไม่มีค่าใช้จ่าย

หลักฐาน: หลักฐานแสดงกระบวนการเชิงรุกในการแจ้งให้บุคคลทราบถึงวัตถุประสงค์และรายละเอียดต่าง ๆ วิธีการเข้าถึงข้อมูล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เอกสารหลักฐานประกอบเกณฑ์ 5.3.1

เรื่อง: กระบวนการเชิงรุกในการแจ้งข้อมูลส่วนบุคคล และการเข้าถึงข้อมูลโดยไม่มีค่าใช้จ่าย

หน่วยงาน: [ชื่อหน่วยงานหรือองค์กร]

1. แนวทางดำเนินงานเชิงรุก

องค์กรมีการดำเนินการแจ้งรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล ผ่านช่องทางต่าง ๆ อย่างต่อเนื่องและชัดเจน โดยไม่รอให้เจ้าของข้อมูลร้องขอ ดังนี้:

ช่องทาง	รายละเอียด
เว็บไซต์ทางการ	มีประกาศนโยบายความเป็นส่วนตัวและรายละเอียดการใช้ข้อมูลในหน้าแรก และเมนูเฉพาะ “ข้อมูลส่วนบุคคล” โดยเข้าถึงได้โดยไม่ต้องลงชื่อเข้าใช้
แบนเนอร์/ป้ายประชาสัมพันธ์	ติดตั้ง ณ จุดบริการ เช่น หน้าสำนักงาน, จุดบริการลูกค้า, และบริเวณทางเข้ากล้องวงจรปิด
แบบฟอร์มออนไลน์และออฟไลน์	ทุกแบบฟอร์มที่มีการเก็บข้อมูลจะแนบประกาศคุ้มครองข้อมูลส่วนบุคคล หรือแนบลิงก์เพื่อศึกษาเพิ่มเติม
Email/SMS	ส่งข้อความแจ้งวัตถุประสงค์ในการใช้ข้อมูลให้ผู้มีส่วนเกี่ยวข้องในกรณีที่มีการเก็บข้อมูลใหม่

QR Code	ติดไว้ในเอกสารทางราชการ เอกสารใบสมัคร และจุดบริการ เพื่อให้สแกนอ่านนโยบายข้อมูลได้สะดวก

2. วิธีการเข้าถึงข้อมูลได้ง่าย และไม่มีค่าใช้จ่าย

เว็บไซต์หลักของหน่วยงาน

ผู้ใช้งานสามารถเข้าถึงเอกสารเกี่ยวกับนโยบายความเป็นส่วนตัวได้จาก:

www.example.org/privacy

โดยไม่มีค่าใช้จ่าย และไม่ต้องลงทะเบียน

QR Code เข้าถึงข้อมูล

ติด QR Code บน:

- แบบฟอร์มใบสมัคร
- ป้ายบริเวณสำนักงาน
- เอกสารประกาศรับสมัครงาน/กิจกรรมต่าง ๆ

สำเนาเอกสารฉบับพิมพ์

เจ้าของข้อมูลสามารถขอรับเอกสารนโยบายฉบับพิมพ์ที่จุดบริการลูกค้า/ประชาสัมพันธ์ได้โดยไม่มีค่าใช้จ่าย

ระบบตอบกลับอัตโนมัติ (Auto-reply)

ระบบอีเมลขององค์กรมีข้อความตอบกลับอัตโนมัติแนบลิงก์นโยบายความเป็นส่วนตัวส่วนตัวทุกครั้งเมื่อมีการติดต่อเข้ามา

3. ตัวอย่างข้อความเชิงรุกที่ใช้จริง

“องค์กรของเรามุ่งมั่นในการคุ้มครองข้อมูลส่วนบุคคลของท่าน ท่านสามารถศึกษารายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล รวมถึงสิทธิของท่าน ได้ที่ www.example.org/privacy หรือโดยการสแกน QR Code บนเอกสารฉบับนี้”

5.3.2 องค์กรแจ้งให้ทราบในรูปแบบอิเล็กทรอนิกส์และเอกสาร โดยใช้เทคนิคที่เหมาะสมร่วมกัน เช่น วิธีการทำหัวข้อและมีการขีดเส้นใต้ข้อความเพื่อเชื่อมต่อ (Link) ไปยังวัตถุประสงค์และรายละเอียด (Layered Approach) การใช้รูปสัญลักษณ์ (Icons) และมีคุณสมบัติการแจ้งได้อย่างเหมาะสมและมีประสิทธิภาพบนอุปกรณ์เคลื่อนที่และอุปกรณ์อัจฉริยะ (Smart Devices)

สิ่งที่ต้องทำ: มีการแจ้งวัตถุประสงค์ครบถ้วนทั้งรูปแบบอิเล็กทรอนิกส์และเอกสาร

หลักฐาน: หลักฐานแสดงวิธีการที่องค์กรแจ้งวัตถุประสงค์ทั้งช่องทางอิเล็กทรอนิกส์และเอกสาร

สภาพบังคับ: กฎหมายไม่ได้กำหนด

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูล
ส่วน บุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.
2562

เรื่อง: การแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลผ่านช่องทางอิเล็กทรอนิกส์และเอกสาร
หน่วยงาน: [ชื่อหน่วยงานหรือองค์กร]

1. รูปแบบการแจ้งวัตถุประสงค์ (Multi-format Notification)

ช่องทาง	วิธีการแจ้ง	รายละเอียดเทคนิค
เว็บไซต์	Banner หน้าแรก + ลิงก์นโยบาย	ใช้หัวข้อสรุปในหน้าแรก พร้อมไฮเปอร์ลิงก์ “อ่าน เพิ่มเติม” ไปยังรายละเอียดแต่ละข้อ (Layered Approach)
Mobile/Tablet	Responsive Design	การออกแบบนโยบายให้อ่านง่ายบนหน้าจอขนาดเล็ก เช่น ย่อข้อความ แสดงหัวข้อหลักก่อนรายละเอียด
แบบฟอร์มกระดาษ	แนบประกาศความ เป็นส่วนตัว	เอกสารแนบประกาศความเป็นส่วนตัวท้ายฟอร์ม พร้อม QR Code สำหรับอ่านฉบับเต็ม
Email/SMS	แจ้งย่อโดยตรง + ลิงก์	ระบุข้อความสั้น “องค์กรขอแจ้งว่าได้เก็บข้อมูลของท่าน ตามวัตถุประสงค์... อ่านเพิ่มเติมได้ที่ [ลิงก์]”
Infographic / Icons	ใช้ในทั้งเว็บไซต์และ เอกสาร	สื่อสารสิทธิพื้นฐาน เช่น การถอนความยินยอม การ ร้องเรียน ด้วยภาพไอคอนเข้าใจง่าย

ตัวอย่าง Layered Approach บนเว็บไซต์

ชั้นที่ 1 (Summary Layer):

- ข้อมูลของคุณมีความสำคัญต่อเรา
องค์กรจะใช้ข้อมูลของคุณเพื่อวัตถุประสงค์ในการให้บริการ/ติดต่อกลับ และไม่ใช่เพื่อวัตถุประสงค์อื่นโดยไม่ได้รับความยินยอม
- [อ่านรายละเอียดเพิ่มเติม](#)

ชั้นที่ 2 (Detailed Layer):

- วัตถุประสงค์ในการเก็บข้อมูลแต่ละประเภท
- แหล่งที่มาของข้อมูล (ถ้าไม่ได้เก็บจากเจ้าของข้อมูลโดยตรง)
- สิทธิของเจ้าของข้อมูล
- วิธีถอนความยินยอม
- วิธีร้องเรียน

3. ตัวอย่างประกาศเอกสารแนบแบบฟอร์ม

ประกาศการคุ้มครองข้อมูลส่วนบุคคลแนบท้ายแบบฟอร์ม พร้อม QR Code สำหรับอ่านฉบับเต็ม

หัวข้อประกาศประกอบด้วย

- วัตถุประสงค์ในการเก็บข้อมูล
- ระยะเวลาการเก็บ
- สิทธิของเจ้าของข้อมูล
- ช่องทางการติดต่อ

4. คุณสมบัติการใช้งานบน Smart Devices

- เว็บไซต์และระบบฟอร์มออนไลน์ใช้ Responsive Design
- รองรับการแสดงผลในอุปกรณ์ขนาดเล็ก เช่น มือถือ และแท็บเล็ต
- ใช้ขนาดตัวอักษรเหมาะสม และปุ่มกดที่ใช้งานง่าย
- รองรับ screen reader และมาตรฐาน WCAG ขั้นพื้นฐาน

5.3.3 ภาษาและข้อความที่ใช้ในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล มีความชัดเจนและสามารถเข้าใจได้โดยง่าย และสื่อสารสอดคล้องกับกลุ่มเป้าหมาย (ลักษณะหรือประเภทของเจ้าของข้อมูลส่วนบุคคล)

สิ่งที่ต้องทำ: มีการแจ้งวัตถุประสงค์โดยใช้ภาษาและข้อความที่ชัดเจน เข้าใจง่าย รูปแบบและวิธีการสื่อสารสอดคล้องกับกลุ่มเป้าหมาย

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล

หลักฐานแสดงกระบวนการจัดทำประกาศการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมกับ
กลุ่มเป้าหมาย เช่น นโยบายหรือแนวปฏิบัติขององค์กร รายงานการประชุม ฯลฯ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูล
ส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.
2562

เอกสารหลักฐานประกอบเกณฑ์ 5.3.3

เรื่อง: การใช้ภาษาและข้อความในการแจ้งวัตถุประสงค์ให้เหมาะสมกับกลุ่มเป้าหมาย

หน่วยงาน: [ชื่อหน่วยงานหรือองค์กร]

1. นโยบายหรือแนวปฏิบัติขององค์กร

หัวข้อ: แนวปฏิบัติในการจัดทำประกาศการคุ้มครองข้อมูลส่วนบุคคลให้เหมาะสมกับกลุ่มเป้าหมาย

สาระสำคัญ:

ใช้ ภาษาระดับทั่วไป (Plain Language) หลีกเลี่ยงศัพท์กฎหมายหรือศัพท์เทคนิคที่ซับซ้อน

แยก เวอร์ชันของประกาศตามกลุ่มเป้าหมาย เช่น

- บุคลากรภายใน
- ผู้สมัครงาน
- ลูกค้า / ผู้รับบริการ
- ผู้เยี่ยมชมเว็บไซต์

ทุกเวอร์ชันมีการตรวจสอบความเข้าใจ (ผ่านการอ่านโดยบุคคลภายนอกหรือพนักงานที่ไม่เกี่ยวข้องกับการ
จัดทำนโยบาย)

2. ตัวอย่างข้อความในประกาศการคุ้มครองข้อมูลส่วนบุคคล

สำหรับลูกค้าทั่วไป:

เราขอแจ้งให้ท่านทราบว่า ข้อมูลของท่านจะถูกนำมาใช้เพื่อวัตถุประสงค์ในการให้บริการ ติดต่อกลับ
และปรับปรุงประสบการณ์การใช้งานของท่าน ข้อมูลของท่านจะไม่ถูกเปิดเผยแก่บุคคลภายนอกโดยไม่ได้
รับความยินยอมจากท่าน

สำหรับผู้สมัครงาน:

ข้อมูลส่วนบุคคลของท่าน เช่น ประวัติการศึกษา ประวัติการทำงาน และข้อมูลการติดต่อ จะถูกใช้
เพื่อพิจารณาคุณสมบัติในการรับเข้าทำงานเท่านั้น

สำหรับพนักงานภายในองค์กร:

องค์กรจะเก็บรวบรวมข้อมูลของท่านเพื่อการบริหารงานบุคคล เช่น การจ่ายค่าจ้าง การประเมินผลงาน และการดูแลสวัสดิการต่าง ๆ โดยไม่ใช้ข้อมูลในทางอื่น

3. กระบวนการจัดทำประกาศที่เหมาะสมกับกลุ่มเป้าหมาย

รายงานการประชุมคณะทำงานคุ้มครองข้อมูลส่วนบุคคล

วันที่: [ระบุวันที่]

วาระ: การปรับปรุงถ้อยคำในประกาศให้เหมาะสมกับกลุ่มเป้าหมาย

สรุปการดำเนินการ:

- แต่งตั้งคณะอนุกรรมการย่อยพิจารณาภาษา
- ได้ดำเนินการเปรียบเทียบถ้อยคำตามเกณฑ์ Plain Language
- ให้เจ้าหน้าที่ HR, ฝ่ายลูกค้าสัมพันธ์ และฝ่ายสื่อสารองค์กร ร่วมตรวจสอบข้อความ
- นำร่างไปทดสอบกับกลุ่มเป้าหมาย (ตัวอย่าง 10 คนต่อกลุ่ม) แล้วปรับปรุงถ้อยคำตามผลตอบรับ

4. หลักฐานสนับสนุนเพิ่มเติม (แนบได้ตามต้องการ)

- สำเนาประกาศในแต่ละเวอร์ชัน
- รายงานการประชุมคณะทำงาน
- สคริปต์หรือคู่มือสำหรับเจ้าหน้าที่ที่ต้องแจ้งด้วยวาจา
- แบบฟอร์มประเมินความเข้าใจหรือข้อเสนอแนะจากผู้ใช้งาน

5.3.4 ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ ภาษาที่ใช้ในการสื่อสารต้องเหมาะสมกับช่วงวัยของผู้เยาว์ในกลุ่มดังกล่าว และต้องอธิบายถึงความเสี่ยงที่เกี่ยวข้องจากการเก็บรวบรวมข้อมูลส่วนบุคคลและมาตรการปกป้องที่เหมาะสม (Safeguards) เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: 1) ใช้ภาษาที่เหมาะสมกับกลุ่มผู้เยาว์
2) มีการอธิบายความเสี่ยง
3) มีมาตรการปกป้องที่เหมาะสม

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การแจ้งข้อมูลส่วนบุคคลสำหรับผู้เยาว์

หน่วยงาน: [ชื่อหน่วยงาน/องค์กร]

กลุ่มเป้าหมาย: เยาวชนอายุไม่เกิน 20 ปี (ตามกฎหมายแพ่งและพาณิชย์ มาตรา 19)

1. ประกาศคุ้มครองข้อมูลส่วนบุคคล (เวอร์ชันผู้เยาว์)

เราจะดูแลข้อมูลของหนูเป็นอย่างดี

เมื่อหนูเข้าร่วมกิจกรรมกับเรา เช่น กรอกแบบฟอร์ม หรือสมัครใช้งานเว็บไซต์ ข้อมูลอย่างชื่อนามสกุล วันเกิด และเบอร์ติดต่อของผู้ปกครอง จะถูกเก็บไว้เพื่อให้พี่ๆ ติดต่อกลับได้ พี่ๆ จะเก็บข้อมูลของหนูไว้แค่เฉพาะที่จำเป็น และจะไม่นำไปให้คนอื่นดูหรือใช้โดยไม่ได้รับอนุญาต ถ้าหนูอยากให้ลบข้อมูล หรือไม่อยากให้ใช้ข้อมูลต่อ หนูหรือคุณพ่อคุณแม่สามารถบอกพี่ๆ ได้ทุกเมื่อเลยนะ

2. อธิบายความเสี่ยง (ในรูปแบบที่เหมาะสม)

ข้อมูลที่หนูให้กับพี่ๆ อาจเสี่ยงต่อการหลุดไปยังบุคคลอื่นที่ไม่เกี่ยวข้อง ถ้าไม่มีการปกป้องอย่างดี เช่น ถ้าใครแอบดูข้อมูลของหนูแล้วนำไปใช้ในทางที่ไม่เหมาะสม เช่น การหลอกลวง การส่งข้อความไม่พึงประสงค์ หรือการใช้ข้อมูลไปสมัครบริการโดยไม่ได้รับอนุญาต

3. มาตรการปกป้อง (Safeguards)

พี่ๆ มีวิธีป้องกันข้อมูลของหนู ดังนี้:

- เก็บข้อมูลไว้ในระบบที่มีรหัสผ่าน และจำกัดเฉพาะพนักงานที่ได้รับอนุญาต
- เข้ารหัสข้อมูลของหนูในระบบคอมพิวเตอร์
- มีการอบรมพนักงานทุกคนเรื่องการคุ้มครองข้อมูลของเด็ก

ถ้าต้องเปิดเผยข้อมูล จะทำเฉพาะในกรณีที่กฎหมายกำหนด และจะขอความยินยอมจากคุณพ่อคุณแม่ก่อนทุกครั้ง

4. กระบวนการและหลักฐานเพิ่มเติม

แนบหลักฐานประกอบ:

- แบบร่างประกาศคุ้มครองข้อมูลสำหรับผู้เยาว์ (PDF หรือ Word)
- เอกสารการประชุมคณะกรรมการด้านการสื่อสารข้อมูลสำหรับกลุ่มเป้าหมายพิเศษ
- ตัวอย่างแบบฟอร์มคำยินยอมจากผู้ปกครอง
- หลักฐานการทดสอบถ้อยคำ (user testing) กับกลุ่มเด็ก 7-12 ปี และ 13-17 ปี
- แบบบันทึกความยินยอมในรูปแบบสองชั้น (Layered Consent): เด็ก + ผู้ปกครอง

5.4.1 องค์การมีขั้นตอนหรือแนวปฏิบัติสำหรับเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลส่วนบุคคลที่องค์กรใช้ในการสร้างโปรไฟล์ เพื่อให้สามารถตรวจสอบความถูกต้องและแก้ไขได้หากจำเป็น

สิ่งที่ต้องทำ: มีขั้นตอนและแนวปฏิบัติให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงข้อมูลของตนได้โดยง่าย

หลักฐาน: ขั้นตอนและแนวปฏิบัติสำหรับเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลส่วนบุคคลที่องค์กรใช้ในการสร้างโปรไฟล์

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ขั้นตอนและแนวปฏิบัติในการเข้าถึงและแก้ไขข้อมูลโปรไฟล์ส่วนบุคคล

หน่วยงาน: [ชื่อองค์กร]

วัตถุประสงค์: เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลส่วนบุคคลที่องค์กรใช้ในการสร้างโปรไฟล์ และตรวจสอบความถูกต้อง พร้อมแก้ไขข้อมูลได้หากจำเป็น

1. แนวปฏิบัติสำหรับเจ้าของข้อมูลในการเข้าถึงข้อมูลโปรไฟล์ส่วนบุคคล

เจ้าของข้อมูลสามารถยื่นคำร้องขอเข้าถึงข้อมูลส่วนบุคคลที่ใช้ในการสร้างโปรไฟล์ได้ ผ่านช่องทางดังนี้

- เว็บไซต์องค์กร (แบบฟอร์มคำขอออนไลน์)
- อีเมลฝ่ายคุ้มครองข้อมูลส่วนบุคคล [email@example.com]
- ศูนย์บริการลูกค้า โทร. [หมายเลขโทรศัพท์]
- ติดต่อด้วยตนเองที่สำนักงาน
- เจ้าของข้อมูลต้องกรอกข้อมูลประจำตัวและรายละเอียดที่จำเป็นในแบบฟอร์มคำขอ เพื่อยืนยันตัวตนอย่างถูกต้อง
- ภายใน 15 วันทำการ หลังจากได้รับคำขอ องค์กรจะดำเนินการตรวจสอบและจัดส่งข้อมูลโปรไฟล์ให้เจ้าของข้อมูลผ่านช่องทางที่เลือก (อีเมล ไปรษณีย์ หรือรับด้วยตนเอง)
- เจ้าของข้อมูลสามารถแจ้งความไม่ถูกต้องหรือขอแก้ไขข้อมูลในโปรไฟล์ได้ โดยระบุข้อมูลที่ต้องการแก้ไข พร้อมแนบหลักฐานประกอบ (ถ้ามี)
- องค์กรจะดำเนินการแก้ไขข้อมูลตามคำร้อง และแจ้งผลการดำเนินการให้เจ้าของข้อมูลทราบภายใน 30 วันทำการ

กรณีที่คำขอเข้าถึงหรือแก้ไขข้อมูลไม่สามารถดำเนินการได้ องค์กรจะแจ้งเหตุผลและวิธีการร้องเรียนแก่เจ้าของข้อมูล

2. ตัวอย่างแบบฟอร์มคำขอเข้าถึงข้อมูลโปรไฟล์ส่วนบุคคล (สำหรับใช้บนเว็บไซต์หรือเอกสาร)

แบบฟอร์มคำขอเข้าถึงข้อมูลส่วนบุคคล

ชื่อ-นามสกุล: _____

หมายเลขบัตรประชาชน/หนังสือเดินทาง: _____

ช่องทางติดต่อ (โทรศัพท์/อีเมล): _____

ข้อมูลที่ต้องการเข้าถึง: ☐ ข้อมูลโปรไฟล์ส่วนบุคคล ☐ ข้อมูลอื่น ๆ _____

คำชี้แจงเพิ่มเติม: _____

ลงชื่อ: _____

วันที่: _____

3. แนวทางการดูแลรักษาข้อมูลและความปลอดภัย

ข้อมูลของเจ้าของข้อมูลจะถูกเก็บรักษาอย่างปลอดภัยตามมาตรฐานความปลอดภัยขององค์กร เจ้าหน้าที่รับผิดชอบจะต้องผ่านการอบรมเรื่องการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความลับ

4. ช่องทางการติดต่อฝ่ายคุ้มครองข้อมูลส่วนบุคคล

อีเมล: privacy@[ชื่อบริษัท].com

โทรศัพท์: [หมายเลขโทรศัพท์]

ที่อยู่: [ที่อยู่สำนักงาน]

5.4.2 หากในกิจกรรมการประมวลผลนั้นมีการตัดสินใจโดยระบบอัตโนมัติเพียงอย่างเดียวและมีผลกระทบ ต่อสิทธิและหน้าที่ตามกฎหมายของบุคคลหรือนัยสำคัญในทำนองเดียวกัน องค์กรได้แจ้งให้เจ้าของข้อมูล ส่วนบุคคลทราบเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในลักษณะดังกล่าว รวมถึง ข้อมูลที่องค์กรใช้ วัตถุประสงค์ และผลกระทบที่อาจจะมี

สิ่งที่ต้องทำ: 1) มีการแจ้งในประกาศการคุ้มครองข้อมูลส่วนบุคคลเรื่องการประมวลผลข้อมูลโดยใช้ระบบ อัตโนมัติตัดสินใจเพียงอย่างเดียว และ
2) มีการแจ้งข้อมูลที่ใช้ วัตถุประสงค์ และผลกระทบที่อาจจะมี

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ประกาศการคุ้มครองข้อมูลส่วนบุคคล

(ส่วนที่เกี่ยวข้องกับการประมวลผลโดยระบบอัตโนมัติที่มีผลกระทบ)

ข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลด้วยระบบอัตโนมัติ

ในกรณีที่องค์กรมีการใช้ระบบประมวลผลข้อมูลส่วนบุคคลด้วยเทคโนโลยีระบบอัตโนมัติ (Automated Decision-Making) โดยไม่มีการแทรกแซงจากบุคคล เพื่อดำเนินการตัดสินใจที่มีผลกระทบต่อสิทธิและ

หน้าที่ตามกฎหมาย หรือผลกระทบที่มีความสำคัญในลักษณะทำนองเดียวกัน องค์กรมีความมุ่งมั่นที่จะเปิดเผยข้อมูลดังต่อไปนี้ให้เจ้าของข้อมูลได้รับทราบอย่างครบถ้วนและชัดเจน:

1. ข้อมูลที่ใช้ในการประมวลผล

องค์กรจะเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลประเภทต่าง ๆ ที่เกี่ยวข้องกับการตัดสินใจโดยระบบอัตโนมัติ เช่น ข้อมูลส่วนบุคคลพื้นฐาน ข้อมูลพฤติกรรม ข้อมูลทางเทคนิค หรือข้อมูลอื่น ๆ ที่จำเป็นสำหรับการดำเนินการประมวลผล

2. วัตถุประสงค์ของการประมวลผล

วัตถุประสงค์ของการใช้ระบบอัตโนมัติในการประมวลผลข้อมูลส่วนบุคคล ได้แก่ การประเมินคุณสมบัติและความเหมาะสมในการให้บริการ การวิเคราะห์พฤติกรรมหรือแนวโน้มเพื่อปรับปรุงบริการ การตัดสินใจในการอนุมัติหรือปฏิเสธคำขอบริการ การบริหารความเสี่ยงและป้องกันการทุจริต

3. ผลกระทบที่อาจเกิดขึ้นจากการตัดสินใจโดยระบบอัตโนมัติ

การตัดสินใจโดยระบบอัตโนมัติอาจมีผลกระทบต่อสิทธิและหน้าที่ของเจ้าของข้อมูล เช่น การจำกัดสิทธิในการเข้าถึงบริการ การเปลี่ยนแปลงเงื่อนไข หรือผลกระทบในทางการเงินและสัญญาต่าง ๆ ซึ่งองค์กรจะดำเนินการอย่างรอบคอบเพื่อให้เกิดความเป็นธรรมและสามารถทบทวนหรืออุทธรณ์ผลการตัดสินใจได้

4. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิในการ:

- ขอรับข้อมูลเกี่ยวกับกระบวนการตัดสินใจโดยระบบอัตโนมัติ
- ขอให้ทบทวนหรือระงับการตัดสินใจที่เป็นผลกระทบ
- ขอให้แก้ไขหรือชี้แจงข้อมูลที่เกี่ยวข้องกับการตัดสินใจ

ติดต่อสอบถามหรือขอข้อมูลเพิ่มเติม

ฝ่ายคุ้มครองข้อมูลส่วนบุคคล

อีเมล: [privacy@\[ชื่อองค์กร\].com](mailto:privacy@[ชื่อองค์กร].com)

โทรศัพท์: [หมายเลขโทรศัพท์]

5.4.3 หากวัตถุประสงค์ไม่ชัดเจนในตอนแรก องค์กรจะแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบว่าองค์กรจะใช้หรือเปิดเผยข้อมูลส่วนบุคคลของพวกเขาอย่างไร และองค์กรจะปรับปรุงข้อมูลต่าง ๆ ที่แจ้งและประกาศการคุ้มครองข้อมูลส่วนบุคคลในเชิงรุกเมื่อมีความชัดเจนมากขึ้นเกี่ยวกับวัตถุประสงค์ในการใช้หรือเปิดเผยข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: ใช้กระบวนการเชิงรุกในการแจ้งวัตถุประสงค์ในการใช้หรือเปิดเผยข้อมูลส่วนบุคคลเมื่อมี

ความชัดเจนขึ้น

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคล
หลักฐานแสดงการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ประกาศการคุ้มครองข้อมูลส่วนบุคคล

(ส่วนที่เกี่ยวข้องกับการแจ้งวัตถุประสงค์ที่ยังไม่ชัดเจนในตอนแรก)

การแจ้งวัตถุประสงค์ในการใช้หรือเปิดเผยข้อมูลส่วนบุคคล

เนื่องจากบางกรณีวัตถุประสงค์ในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลของท่านอาจยังไม่ชัดเจนในช่วงแรก องค์กรขอแจ้งให้ท่านทราบว่า:

ขณะนี้องค์กรใช้ข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์เบื้องต้น ดังที่ได้แจ้งในประกาศการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้

หากองค์กรมีความชัดเจนเกี่ยวกับวัตถุประสงค์เพิ่มเติมในการใช้หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน ในภายหลัง องค์กรจะดำเนินการแจ้งให้ท่านทราบโดยเร็วและเชิงรุก ผ่านช่องทางต่าง ๆ เช่น อีเมล ข้อความ หรือประกาศบนเว็บไซต์องค์กร

องค์กรมีหน้าที่และความมุ่งมั่นในการปรับปรุงประกาศการคุ้มครองข้อมูลส่วนบุคคลให้ทันสมัยและสอดคล้องกับการใช้งานข้อมูลส่วนบุคคลจริงในทุกช่วงเวลา

ท่านสามารถติดต่อสอบถามหรือขอข้อมูลเพิ่มเติมเกี่ยวกับวัตถุประสงค์การใช้ข้อมูลส่วนบุคคลได้ทุกเมื่อ

หลักฐานแสดงการแจ้งให้เจ้าของข้อมูลทราบเชิงรุก

- รายการบันทึกการส่งอีเมลแจ้งข่าวสารและอัปเดตเกี่ยวกับวัตถุประสงค์การใช้ข้อมูลส่วนบุคคล
- สำเนาข้อความแจ้งเตือนผ่าน SMS หรือระบบแจ้งเตือนอื่น ๆ
- การประกาศหรืออัปเดตประกาศการคุ้มครองข้อมูลส่วนบุคคลบนเว็บไซต์องค์กร พร้อมระบุวันที่ปรับปรุง
- รายงานการประชุมหรือบันทึกภายในที่แสดงขั้นตอนและนโยบายการแจ้งข้อมูลเชิงรุก

ติดต่อฝ่ายคุ้มครองข้อมูลส่วนบุคคล

อีเมล: [privacy@\[ชื่อองค์กร\].com](mailto:privacy@[ชื่อองค์กร].com)

โทรศัพท์: [หมายเลขโทรศัพท์]

5.4.4 หากในกิจกรรมการประมวลผลนั้นมีการตัดสินใจโดยระบบอัตโนมัติเพียงอย่างเดียวและมีผลกระทบ ต่อสิทธิและหน้าที่ตามกฎหมายของบุคคลหรือนัยสำคัญในตนเองเดียวกัน องค์กรได้อธิบายการ ประมวลผลนั้นอย่างชัดเจน ซึ่งช่วยให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิของตนได้ รวมถึงการ คัดค้านการประมวลผลโดยระบบอัตโนมัติดังกล่าว หรือการขอให้ได้รับการแทรกแซงจากมนุษย์ (ดำเนินการตัดสินใจโดยบุคคล)

สิ่งที่ต้องทำ: มีกลไกและมีการอธิบายอย่างชัดเจนให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิของตนได้
 หลักฐาน: กระบวนการหรือกลไกที่ทำให้เจ้าของข้อมูลส่วนบุคคลส่งคำขอให้ได้รับการแทรกแซงจาก มนุษย์ในการประมวลผลข้อมูลส่วนบุคคล
 สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารหลักฐาน: กระบวนการและกลไกการจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคลในการประมวลผล โดยระบบอัตโนมัติ

1. นโยบายการประมวลผลข้อมูลโดยระบบอัตโนมัติและสิทธิของเจ้าของข้อมูลส่วนบุคคล

องค์กรได้จัดให้มีการประมวลผลข้อมูลส่วนบุคคลโดยระบบอัตโนมัติในบางกรณี ซึ่งอาจมีผลกระทบ ต่อสิทธิและหน้าที่ตามกฎหมายของเจ้าของข้อมูลส่วนบุคคล องค์กรมีความมุ่งมั่นที่จะอธิบายการ ประมวลผลดังกล่าวอย่างชัดเจนเพื่อให้เจ้าของข้อมูลได้รับทราบและสามารถใช้สิทธิต่าง ๆ ได้อย่างเต็มที่

2. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการ:

คัดค้านการประมวลผลข้อมูลส่วนบุคคลที่ทำโดยระบบอัตโนมัติเพียงอย่างเดียว หากส่งผลกระทบต่อ สิทธิและเสรีภาพของตน

ขอให้มีการแทรกแซงจากมนุษย์ (การทบทวนโดยบุคคลจริง) ในการตัดสินใจที่เกิดขึ้นจากระบบ อัตโนมัติ

ขอชี้แจงหรือขอข้อมูลเพิ่มเติมเกี่ยวกับกระบวนการประมวลผลข้อมูล

3. กลไกการใช้สิทธิ

องค์กรได้จัดให้มีช่องทางและกระบวนการดังนี้ เพื่อให้เจ้าของข้อมูลสามารถใช้สิทธิได้อย่างง่ายดาย และมีประสิทธิภาพ:

ช่องทางการส่งคำขอ

อีเมล: [privacy@\[ชื่อองค์กร\].com](mailto:privacy@[ชื่อองค์กร].com)

แบบฟอร์มออนไลน์บนเว็บไซต์องค์กร: [URL แบบฟอร์มขอทบทวนการตัดสินใจโดยระบบอัตโนมัติ]

ติดต่อโดยตรงที่ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO)

ขั้นตอนการดำเนินการ

1. เจ้าของข้อมูลส่งคำขอคัดค้านหรือขอให้มีการแทรกแซงจากมนุษย์
2. ฝ่ายคุ้มครองข้อมูลส่วนบุคคลรับเรื่องและแจ้งยืนยันการรับคำขอแก่เจ้าของข้อมูล
3. ดำเนินการทบทวนข้อมูลและการตัดสินใจโดยเจ้าหน้าที่ที่เกี่ยวข้อง
4. แจ้งผลการพิจารณาและดำเนินการแก้ไขหรือปรับปรุงตามคำขอแก่เจ้าของข้อมูลภายในระยะเวลาที่เหมาะสม

4. ตัวอย่างข้อความแจ้งสิทธิในประกาศการคุ้มครองข้อมูลส่วนบุคคล

"ในกรณีที่องค์กรใช้ระบบอัตโนมัติในการตัดสินใจซึ่งอาจมีผลกระทบต่อตน ท่านมีสิทธิขอให้บุคคลเข้ามาทบทวนการตัดสินใจดังกล่าว และสามารถคัดค้านการประมวลผลข้อมูลโดยระบบอัตโนมัติได้ โดยสามารถติดต่อเราได้ที่ [privacy@\[ชื่อองค์กร\].com](mailto:privacy@[ชื่อองค์กร].com) หรือผ่านแบบฟอร์มในเว็บไซต์ของเรา"

5.5.1 มีการสื่อสารและสร้างความตระหนักรู้แก่พนักงาน/เจ้าหน้าที่ของทั้งองค์กรเกี่ยวกับประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร ข้อมูลเกี่ยวกับวัตถุประสงค์ และรายละเอียดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: มีการสื่อสารหรือสร้างความตระหนักรู้ให้กับพนักงาน

หลักฐาน: เอกสารหลักฐานการสื่อสารหรือแจ้งพนักงานทราบเกี่ยวกับประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร เช่น อีเมล ประกาศแจ้งพนักงาน การจัดประชุม

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (7) โทษทางปกครองในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การสื่อสารและสร้างความตระหนักรู้เกี่ยวกับประกาศการคุ้มครองข้อมูลส่วนบุคคลแก่พนักงาน

1. วัตถุประสงค์

เพื่อให้พนักงานและเจ้าหน้าที่ทุกระดับในองค์กรมีความเข้าใจและตระหนักรู้เกี่ยวกับประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร ข้อมูลวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล รวมถึงบทบาทหน้าที่และความรับผิดชอบของพนักงานในการปฏิบัติตามกฎหมาย PDPA และนโยบายองค์กร

2. วิธีการสื่อสาร

- การส่งอีเมลแจ้งพนักงานทุกคน
- การประชุมชี้แจงผ่านออนไลน์หรือพบปะกลุ่ม
- การฝึกอบรมหรือสัมมนาเกี่ยวกับ PDPA
- การจัดทำเอกสารแจกจ่าย (ประกาศ/คู่มือ)

3. ตัวอย่างอีเมลแจ้งพนักงาน

เรื่อง: แจ้งประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กรและการสร้างความตระหนักรู้

เรียน พนักงานทุกท่าน

ตามที่องค์กรของเราได้จัดทำประกาศการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy) เพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และข้อกำหนดด้านความปลอดภัยของข้อมูล

องค์กรจึงขอแจ้งให้ท่านทราบเกี่ยวกับวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล รวมถึงบทบาทหน้าที่ของพนักงานในการรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคลดังกล่าว กรณศึกษาและปฏิบัติตามนโยบายอย่างเคร่งครัด เพื่อปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคล และป้องกันความเสี่ยงทางกฎหมายที่อาจเกิดขึ้น

หากมีข้อสงสัยหรือต้องการข้อมูลเพิ่มเติม กรุณาติดต่อฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO) ที่อีเมล [privacy@\[ชื่อองค์กร\].com](mailto:privacy@[ชื่อองค์กร].com)

ขอขอบคุณทุกท่านที่ให้ความร่วมมือ

ฝ่ายบริหารองค์กร

[ชื่อองค์กร]

4. ตัวอย่างบันทึกการประชุมชี้แจง PDPA

บันทึกการประชุม:

วันที่: 10 มิถุนายน 2568

เวลา: 14.00 – 15.30 น.

สถานที่: ห้องประชุมใหญ่ อาคารสำนักงานใหญ่

หัวข้อ: การสร้างความตระหนักรู้เกี่ยวกับประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

ผู้เข้าร่วม: พนักงานทุกแผนก รวม 50 คน

เนื้อหา:

- แนะนำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- วัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล
- บทบาทและหน้าที่ของพนักงานในการปฏิบัติตาม PDPA
- แนวทางปฏิบัติที่ต้องปฏิบัติ เช่น การรักษาความลับของข้อมูล, การจัดเก็บและทำลายข้อมูลอย่างปลอดภัย
- ช่องทางติดต่อฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO)

ผลการประชุม: พนักงานทุกคนรับทราบและเข้าใจในนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร พร้อมปฏิบัติตามอย่างเคร่งครัด

5.5.2 พนักงาน/เจ้าหน้าที่ที่อยู่หน้างาน (Frontline staff) ได้รับการอบรมเป็นพิเศษเกี่ยวกับข้อมูลต่าง ๆ ตามประกาศการคุ้มครองข้อมูลส่วนบุคคล (เนื่องจากติดต่อสื่อสารกับเจ้าของข้อมูลส่วนบุคคลโดยตรง) สิ่งที่ต้องทำ: มีการอบรมพิเศษให้กับพนักงานที่อยู่หน้างาน

หลักฐาน: เอกสารหลักฐานการฝึกอบรมให้กับพนักงาน/เจ้าหน้าที่ที่อยู่หน้างาน (front line staff)

เอกสารหลักฐานการทดสอบพนักงาน

บันทึกข้อมูลผู้ผ่านการทดสอบและไม่ผ่านการทดสอบ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (7)

โทษทางปกครองในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การอบรมพิเศษพนักงาน/เจ้าหน้าที่หน้างาน (Frontline Staff) เรื่องประกาศการคุ้มครองข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อให้พนักงานที่อยู่หน้างานซึ่งติดต่อสื่อสารกับเจ้าของข้อมูลส่วนบุคคลโดยตรง มีความรู้และความเข้าใจอย่างชัดเจนเกี่ยวกับประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร รวมถึงบทบาทหน้าที่ในการรักษาความลับและการปฏิบัติตามกฎหมาย PDPA อย่างถูกต้อง

2. รายละเอียดการอบรม

เนื้อหาอบรม:

- ความรู้เบื้องต้นเกี่ยวกับ PDPA
- ประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
- ข้อมูลส่วนบุคคลที่หน่วยงานต้องรับผิดชอบ
- วิธีปฏิบัติและข้อควรระวังในการติดต่อกับเจ้าของข้อมูล
- สิทธิของเจ้าของข้อมูลและการตอบสนองต่อคำร้อง
- กรณีศึกษาที่เกี่ยวข้อง
- ระยะเวลาอบรม: 3 ชั่วโมง
- วันที่จัดอบรม: 15 มิถุนายน 2568
- สถานที่: ห้องอบรม ชั้น 2 อาคารสำนักงานใหญ่
- ผู้เข้าอบรม: พนักงานบริการลูกค้า, เจ้าหน้าที่ฝ่ายรับเรื่องร้องเรียน รวม 20 คน

ตัวอย่างเอกสารหลักฐาน

ใบลงทะเบียนเข้าร่วมอบรม

ลำดับ	ชื่อ-นามสกุล	ตำแหน่ง	ลงชื่อ	วันที่
1	นายสมชาย ใจดี	เจ้าหน้าที่บริการลูกค้า	(ลายเซ็น)	15/06/2568
2	นางสาวสุมิตรา กล้าหาญ	เจ้าหน้าที่รับเรื่องร้องเรียน	(ลายเซ็น)	15/06/2568
...				

แบบทดสอบหลังการอบรม (ตัวอย่างคำถาม)

1.ข้อใดคือข้อมูลส่วนบุคคลที่ต้องได้รับการปกป้องอย่างเคร่งครัด?

- ก. ชื่อและนามสกุล
- ข. เบอร์โทรศัพท์
- ค. รายละเอียดสุขภาพ
- ง. ถูกทุกข้อ

2.หากเจ้าของข้อมูลขอเข้าถึงข้อมูลส่วนบุคคล ต้องดำเนินการอย่างไร?

- ก. ปฏิเสธ
- ข. แจ้งฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO)

ค. ให้ข้อมูลทันที

ง. ไม่ตอบสนอง

3. พนักงานหน้างานควรปฏิบัติอย่างไรเมื่อได้รับข้อมูลส่วนบุคคลจากลูกค้า?

ก. เก็บรักษาอย่างปลอดภัย

ข. ห้ามเปิดเผยข้อมูลแก่บุคคลอื่นโดยไม่ได้รับอนุญาต

ค. แจ้งเจ้าของข้อมูลเกี่ยวกับวัตถุประสงค์การใช้ข้อมูล

ง. ถูกทุกข้อ

รายงานผลการทดสอบพนักงานหลังอบรม

ชื่อ-นามสกุล	ตำแหน่ง	คะแนนที่ได้	ผ่าน/ไม่ผ่าน	หมายเหตุ
นายสมชาย ใจดี	เจ้าหน้าที่บริการลูกค้า	90/100	ผ่าน	
นางสาวสุมิตรา กล้าหาญ	เจ้าหน้าที่รับเรื่องร้องเรียน	75/100	ผ่าน	
นายวิทยา สุขใจ	เจ้าหน้าที่บริการลูกค้า	50/100	ไม่ผ่าน	ต้องอบรมซ้ำ

สรุป

องค์กรได้จัดอบรมพิเศษให้กับพนักงานหน้างานแล้ว พร้อมดำเนินการทดสอบเพื่อประเมินความเข้าใจและบันทึกผลการทดสอบตามมาตรฐานกฎหมาย PDPA และแนวทางประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

5.5.3 พนักงาน/เจ้าหน้าที่ตระหนักและรับทราบถึงวิธีการต่าง ๆ ที่องค์กรใช้เป็นช่องทางในการแจ้งข้อมูลเกี่ยวกับวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: พนักงานทั้งหมดทราบช่องทางในการแจ้งข้อมูล

หลักฐาน: หลักฐานการรับทราบข้อมูลของพนักงาน/เจ้าหน้าที่

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (7)

โทษทางปกครองในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การแจ้งข้อมูลเกี่ยวกับวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อให้พนักงานและเจ้าหน้าที่ทุกคนรับทราบช่องทางและวิธีการที่องค์กรใช้ในการแจ้งข้อมูลเกี่ยวกับวัตถุประสงค์และรายละเอียดของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามข้อกำหนดของ PDPA

2. ช่องทางการแจ้งข้อมูลที่ต้องการใช้

- ประกาศในเว็บไซต์องค์กร (ลิงก์ประกาศนโยบายความเป็นส่วนตัว)
- ระบบอีเมลองค์กร
- ป้ายประกาศที่ติดตั้งในพื้นที่ทำงาน
- การประชุมและอบรมภายในองค์กร
- คู่มือพนักงานและเอกสารประกอบการทำงาน
- ระบบแจ้งเตือนผ่านแอปพลิเคชันภายในองค์กร

5. แบบฟอร์มรับทราบข้อมูลของพนักงาน

ลำดับ	ชื่อ-นามสกุล	ตำแหน่ง	ช่องทางที่รับทราบข้อมูล (เลือกได้มากกว่า 1 ช่องทาง)	ลงชื่อ รับทราบ	วันที่
1	นายสมชาย ใจดี	เจ้าหน้าที่บริการลูกค้า	อีเมลองค์กร, ประกาศในเว็บไซต์องค์กร	(ลายเซ็น)	3/6/2568
2	นางสาวสุมิตรา กล้าหาญ	เจ้าหน้าที่ฝ่ายทรัพยากรบุคคล	ป้ายประกาศในสำนักงาน, การประชุมภายในองค์กร	(ลายเซ็น)	3/6/2568
3	นายวิทยา สุขใจ	เจ้าหน้าที่ฝ่ายไอที	อีเมลองค์กร, ระบบแจ้งเตือนแอปพลิเคชันภายในองค์กร	(ลายเซ็น)	3/6/2568

6. สรุป

พนักงานและเจ้าหน้าที่ขององค์กรทุกคนได้รับข้อมูลและตระหนักถึงช่องทางต่าง ๆ ที่องค์กรใช้ในการแจ้งข้อมูลเกี่ยวกับวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างครบถ้วนและถูกต้อง

5.6.1 หากองค์กรจะใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ใหม่/เปลี่ยนแปลงวัตถุประสงค์ (New Purpose) องค์กรมีขั้นตอนในการปรับปรุงประกาศการคุ้มครองข้อมูลส่วนบุคคลและมีการสื่อสารการเปลี่ยนแปลงดังกล่าวไปยังเจ้าของข้อมูลส่วนบุคคลก่อนที่จะเริ่มการใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ใหม่ดังกล่าว สิ่งที่ต้องทำ: มีขั้นตอนในการปรับปรุงประกาศการคุ้มครองข้อมูลส่วนบุคคลและมีการสื่อสารการเปลี่ยนแปลงไปยังเจ้าของข้อมูลส่วนบุคคลครบถ้วน

หลักฐาน: ขั้นตอนในการปรับปรุงประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
วิธีการที่จะใช้ในการสื่อสารไปยังเจ้าของข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21
โทษทางปกครองในกรณีที่ไม่ปฏิบัติตามมาตรา 21 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ขั้นตอนการปรับปรุงประกาศการคุ้มครองข้อมูลส่วนบุคคลและการสื่อสารการเปลี่ยนแปลงวัตถุประสงค์ใหม่ (New Purpose)

1. วัตถุประสงค์

เพื่อให้การใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ใหม่หรือการเปลี่ยนแปลงวัตถุประสงค์มีความชัดเจนและโปร่งใส โดยองค์กรมีขั้นตอนในการปรับปรุงประกาศการคุ้มครองข้อมูลส่วนบุคคลและแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนเริ่มใช้ข้อมูลตามวัตถุประสงค์ใหม่

2. ขั้นตอนการปรับปรุงประกาศการคุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ขั้นตอน	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา (วัน)
1	ตรวจสอบความจำเป็นในการเปลี่ยนแปลงวัตถุประสงค์	พิจารณาวัตถุประสงค์ใหม่ที่ต้องใช้ข้อมูลส่วนบุคคล	ฝ่ายกฎหมาย/ฝ่ายคุ้มครองข้อมูลส่วนบุคคล	1
2	จัดทำร่างประกาศการคุ้มครองข้อมูลส่วนบุคคลฉบับปรับปรุง	ระบุวัตถุประสงค์ใหม่และรายละเอียดที่เกี่ยวข้อง	ฝ่ายกฎหมาย/ฝ่ายคุ้มครองข้อมูลส่วนบุคคล	3
3	ตรวจสอบและอนุมัติประกาศฉบับปรับปรุง	รับรองความถูกต้องของเนื้อหาและความเหมาะสม	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	2

4	จัดเตรียมช่องทางและวิธีการสื่อสารแจ้งเจ้าของข้อมูล	กำหนดช่องทางสื่อสาร เช่น อีเมล เว็บไซต์ หรือจดหมายแจ้ง	ฝ่ายสื่อสารองค์กร/ฝ่ายไอที	2
3	แจ้งเจ้าของข้อมูลส่วนบุคคลก่อนเริ่มใช้ข้อมูลตามวัตถุประสงค์ใหม่	ส่งข้อความแจ้งเตือนพร้อมลิงก์ประกาศฉบับปรับปรุง	ฝ่ายสื่อสารองค์กร/ฝ่ายบริการลูกค้า	3
6	บันทึกหลักฐานการแจ้งและรับทราบจากเจ้าของข้อมูล	เก็บสำเนาหลักฐานและรายงานสรุป	ฝ่ายคุ้มครองข้อมูลส่วนบุคคล	ต่อเนื่อง

3. วิธีการสื่อสารแจ้งเจ้าของข้อมูลส่วนบุคคล

- ส่งอีเมลแจ้งรายละเอียดการเปลี่ยนแปลงพร้อมแนบลิงก์ประกาศฉบับปรับปรุง
- แจ้งผ่านหน้าเว็บไซต์องค์กรที่มีประกาศนโยบายความเป็นส่วนตัว
- ส่งข้อความผ่านระบบแจ้งเตือนแอปพลิเคชันขององค์กร (ถ้ามี)
- ส่งจดหมายแจ้งเป็นเอกสารสำหรับเจ้าของข้อมูลที่ต้องการเอกสารฉบับจริง
- ประกาศผ่านช่องทางสื่อสารภายใน เช่น ประชุมเจ้าหน้าที่หรือข่าวสารภายในองค์กร

4. สรุป

องค์กรมีระบบขั้นตอนที่ชัดเจนในการปรับปรุงประกาศการคุ้มครองข้อมูลส่วนบุคคล และมีช่องทางที่เหมาะสมในการแจ้งข้อมูลการเปลี่ยนแปลงวัตถุประสงค์ให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบก่อนเริ่มการใช้ข้อมูลตามวัตถุประสงค์ใหม่อย่างครบถ้วนและโปร่งใส

5.6.2 องค์กรมีการทบทวนประกาศการคุ้มครองข้อมูลส่วนบุคคลโดยการพิจารณาเปรียบเทียบกับการบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA: records of processing activities) เพื่อให้แน่ใจว่าข้อมูลดังกล่าวเป็นปัจจุบันและอธิบายสิ่งที่เกิดขึ้นกับข้อมูลส่วนบุคคลของบุคคลได้จริง

สิ่งที่ต้องทำ: มีการทบทวนประกาศการคุ้มครองข้อมูลส่วนบุคคลโดยการพิจารณาเปรียบเทียบกับบันทึกการอย่างครบถ้วน

หลักฐาน: หลักฐานการทบทวนประกาศข้อมูลส่วนบุคคลแสดงการเปรียบเทียบกับการบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA: records of processing activities) เช่น การจัดประชุมของผู้ที่มีส่วนเกี่ยวข้องหรือได้รับมอบหมาย

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1)
โทษทางปกครองในกรณีที่ไม่ปฏิบัติตามมาตรา 21 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การทบทวนประกาศการคุ้มครองข้อมูลส่วนบุคคลโดยการเปรียบเทียบกับบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA)

1. วัตถุประสงค์

เพื่อให้ประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กรมีความถูกต้อง เป็นปัจจุบัน และสอดคล้องกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เกิดขึ้นจริงในองค์กร

2. ขั้นตอนการทบทวนประกาศการคุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ขั้นตอน	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา (วัน)
1	นัดหมายผู้มีส่วนเกี่ยวข้อง	รวมผู้ดูแลข้อมูลส่วนบุคคล ฝ่ายกฎหมาย ฝ่ายไอที และฝ่ายบริหาร	ฝ่ายคุ้มครองข้อมูลส่วนบุคคล	1
2	ตรวจสอบประกาศการคุ้มครองข้อมูลส่วนบุคคล	นำประกาศฉบับปัจจุบันมาทบทวนอย่างละเอียด	ฝ่ายกฎหมาย/ฝ่ายคุ้มครองข้อมูลส่วนบุคคล	1

3	เปรียบเทียบประกาศ กับบันทึกรายการ ROPA	ตรวจสอบกิจกรรมการ ประมวลผลข้อมูลที่บันทึกไว้ใน ROPA ว่าตรงกับประกาศหรือไม่	ฝ่ายคุ้มครองข้อมูล ส่วนบุคคล/ฝ่ายไอที	2
4	วิเคราะห์ความ แตกต่างและปรับปรุง ประกาศ	หากพบความแตกต่าง ให้จัดทำ ข้อเสนอปรับปรุงประกาศ	ฝ่ายกฎหมาย/ฝ่าย คุ้มครองข้อมูลส่วน บุคคล	2
5	รายงานผลการ ทบทวน	จัดทำรายงานสรุปผลการ ทบทวน พร้อมข้อเสนอแนะ	ฝ่ายคุ้มครองข้อมูล ส่วนบุคคล	1
6	อนุมัติและบันทึก หลักฐาน	นำเสนอรายงานต่อผู้บริหารเพื่อ อนุมัติ และเก็บเป็นหลักฐาน	ฝ่ายบริหาร/ฝ่าย คุ้มครองข้อมูลส่วน บุคคล	1

3. หลักฐานที่จัดทำไว้

- รายงานผลการทบทวนประกาศการคุ้มครองข้อมูลส่วนบุคคล (มีการเปรียบเทียบกับ ROPA)
- รายงานการประชุมผู้มีส่วนเกี่ยวข้องที่ทำการทบทวน
- บันทึกการอนุมัติรายงานจากผู้บริหาร
- สำเนาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) ที่ใช้ในการเปรียบเทียบ

4. ตัวอย่างข้อความรายงานการประชุมทบทวนประกาศ

"ในวันที่ xx/xx/xxxx คณะทำงานคุ้มครองข้อมูลส่วนบุคคลได้จัดประชุมเพื่อทบทวนประกาศการคุ้มครองข้อมูลส่วนบุคคล โดยเปรียบเทียบกับบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) เพื่อยืนยันความถูกต้องและความสอดคล้องกัน ผลการตรวจสอบพบว่าประกาศดังกล่าวมีข้อมูลครบถ้วนสอดคล้องกับกิจกรรมประมวลผลในปัจจุบัน และได้เสนอแนะการปรับปรุงในส่วนรายละเอียดเกี่ยวกับการใช้ข้อมูลในบางกิจกรรม โดยจะนำไปปรับปรุงประกาศในรอบถัดไป"

5. สรุป

องค์กรได้ดำเนินการทบทวนประกาศการคุ้มครองข้อมูลส่วนบุคคลเป็นประจำโดยเปรียบเทียบกับบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) อย่างครบถ้วนและมีหลักฐานการประชุมและรายงานผลประกอบ ทำให้มั่นใจได้ว่าข้อมูลที่แจ้งแก่เจ้าของข้อมูลเป็นปัจจุบันและสอดคล้องกับกิจกรรมจริง

5.6.3 องค์การเก็บบันทึกประกาศการคุ้มครองข้อมูลส่วนบุคคลที่เคยใช้บังคับ รวมถึงวันที่ทำการเปลี่ยนแปลง เพื่อให้สามารถตรวจสอบว่าข้อมูลเกี่ยวกับวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใดบ้างที่ได้แจ้งและแจ้งเมื่อใด

สิ่งที่ต้องทำ: การเก็บบันทึกประกาศการคุ้มครองข้อมูลส่วนบุคคลที่เคยใช้บังคับ และข้อมูลวันที่ทำการเปลี่ยนแปลงอย่างครบถ้วน

หลักฐาน: ข้อมูลการเก็บบันทึกประกาศการคุ้มครองข้อมูลส่วนบุคคลที่เคยใช้บังคับ และข้อมูลวันที่ทำการเปลี่ยนแปลง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การเก็บบันทึกประกาศการคุ้มครองข้อมูลส่วนบุคคลที่เคยใช้บังคับ พร้อมวันที่เปลี่ยนแปลง

1. วัตถุประสงค์

เพื่อให้สามารถตรวจสอบย้อนหลังได้ว่า ประกาศการคุ้มครองข้อมูลส่วนบุคคลฉบับใดบ้างที่เคยใช้บังคับ และข้อมูลที่แจ้งแก่เจ้าของข้อมูลมีรายละเอียดอย่างไร รวมถึงวันเวลาที่มีการเปลี่ยนแปลงประกาศดังกล่าว

2. ขั้นตอนการเก็บบันทึกประกาศการคุ้มครองข้อมูลส่วนบุคคลที่เคยใช้บังคับ

ลำดับ	รายการ	รายละเอียด
1	รวบรวมประกาศฉบับปัจจุบันและฉบับเก่า	รวบรวมประกาศการคุ้มครองข้อมูลที่เคยใช้บังคับทุกฉบับ
2	ระบุหมายเลขเวอร์ชันของประกาศแต่ละฉบับ	กำหนดหมายเลขเวอร์ชันหรือชื่อฉบับ เช่น v1.0 v2.0

3	บันทึกวันที่ประกาศเริ่มใช้และวันที่มีการเปลี่ยนแปลง	บันทึกวัน/เดือน/ปี ที่ประกาศเริ่มใช้และวันที่แก้ไขล่าสุด
4	จัดทำสารบัญบันทึกประกาศการคุ้มครองข้อมูล	สรุปประกาศแต่ละฉบับและวันที่เปลี่ยนแปลงในรูปแบบสารบัญ
5	เก็บรักษาเอกสารในระบบจัดเก็บกลาง	เก็บในระบบเอกสารอิเล็กทรอนิกส์ (DMS) หรือในแฟ้มเอกสารที่ควบคุมได้
6	อนุมัติและรับรองเอกสารโดยผู้บริหาร	ผู้บริหารลงนามรับรองการจัดเก็บและการบันทึกข้อมูล

3. ตัวอย่างสารบัญการเก็บบันทึกประกาศการคุ้มครองข้อมูลส่วนบุคคล

เวอร์ชัน	วันที่ประกาศใช้	วันที่เปลี่ยนแปลง ล่าสุด	หมายเหตุ
v1.0	01 มกราคม 2562	-	ฉบับแรกประกาศใช้
v1.1	15 กรกฎาคม 2563	15 กรกฎาคม 2563	แก้ไขเนื้อหาเพิ่มความชัดเจนเรื่องวัตถุประสงค์
v2.0	01 มีนาคม 2565	-	ปรับปรุงประกาศตาม พ.ร.บ.ใหม่และมาตรฐานสากล

4. ตัวอย่างแบบฟอร์มบันทึกประกาศที่เคยใช้บังคับ

ชื่อประกาศ: ประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร ABC

เวอร์ชัน: v1.1

วันที่เริ่มใช้: 15 กรกฎาคม 2563

วันที่เปลี่ยนแปลงล่าสุด: 15 กรกฎาคม 2563

รายละเอียดการเปลี่ยนแปลง: เพิ่มความชัดเจนในส่วนของวัตถุประสงค์การใช้ข้อมูลและวิธีการแจ้งเจ้าของข้อมูล

จัดเก็บโดย: ฝ่ายคุ้มครองข้อมูลส่วนบุคคล

รับรองโดย: ผู้จัดการฝ่ายกฎหมาย

5. สรุป

องค์กรได้ดำเนินการเก็บบันทึกประกาศการคุ้มครองข้อมูลส่วนบุคคลที่เคยใช้บังคับอย่างครบถ้วน รวมถึงวันที่ที่มีการเปลี่ยนแปลง ทำให้สามารถตรวจสอบย้อนหลังได้ว่าในแต่ละช่วงเวลามีประกาศใดบ้างที่นำมาใช้และมีรายละเอียดอย่างไร สร้างความโปร่งใสและสอดคล้องกับหลักการจัดการข้อมูลส่วนบุคคลที่ดี

5.6.4 องค์การดำเนินการทดสอบโดยผู้ใช้เพื่อประเมินประสิทธิภาพของการแจ้งข้อมูลเกี่ยวกับวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: มีการทดสอบกับผู้ใช้และประเมินประสิทธิภาพ

หลักฐาน: หลักฐานการทดสอบกับผู้ใช้เพื่อประเมินประสิทธิภาพของการแจ้ง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การทดสอบกับผู้ใช้เพื่อประเมินประสิทธิภาพของการแจ้งข้อมูลเกี่ยวกับวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อประเมินว่าการแจ้งข้อมูลแก่เจ้าของข้อมูลส่วนบุคคลในประกาศหรือสื่ออื่น ๆ มีความชัดเจน เข้าใจง่าย และมีประสิทธิภาพในการสื่อสารข้อมูลที่จำเป็นเกี่ยวกับวัตถุประสงค์และรายละเอียดการประมวลผลข้อมูล

2. ขั้นตอนการทดสอบ

กำหนดกลุ่มผู้ทดสอบ (User Testing Group):

– ตัวอย่างเช่น เจ้าของข้อมูลจริง หรือกลุ่มตัวแทนจากพนักงาน ลูกค้า หรือผู้เกี่ยวข้อง
จัดเตรียมเอกสารหรือสื่อแจ้งข้อมูล:

– ประกาศการคุ้มครองข้อมูลส่วนบุคคล ตัวอย่างข้อความแจ้งวัตถุประสงค์ และรายละเอียดการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล

ดำเนินการทดสอบ:

– ให้ผู้ทดสอบลองอ่าน/รับทราบข้อมูล
– ใช้แบบสอบถาม หรือสัมภาษณ์เพื่อประเมินความเข้าใจ ความชัดเจน และความพึงพอใจ

รวบรวมผลการประเมิน:

– บันทึกข้อคิดเห็น ความเข้าใจที่ถูกต้องหรือผิดพลาด
– ประเมินคะแนนความเข้าใจและประสิทธิภาพ

สรุปผลและปรับปรุง:

– รายงานผลการทดสอบ
– กำหนดแนวทางแก้ไขปรับปรุงการแจ้งข้อมูลหากจำเป็น

3. ตัวอย่างแบบฟอร์มการประเมินผู้ใช้

คำถามประเมิน	คำตอบ (เลือก/เขียน)

คุณเข้าใจวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคลหรือไม่?	☐ เข้าใจชัดเจน ☐ ค่อนข้างเข้าใจ ☐ ไม่เข้าใจ
ข้อมูลที่แจ้งมีความชัดเจนและเข้าใจง่ายหรือไม่?	☐ ชัดเจนมาก ☐ ปานกลาง ☐ ไม่ชัดเจน
คุณรู้สึกว่าการแจ้งข้อมูลนี้เพียงพอหรือไม่?	☐ เพียงพอ ☐ ไม่แน่ใจ ☐ ไม่เพียงพอ
ข้อเสนอแนะเพิ่มเติม	_____

4. ตัวอย่างรายงานสรุปผลการทดสอบ

วันที่ทดสอบ: 15 พฤษภาคม 2568

จำนวนผู้เข้าร่วม: 10 คน

ผลการประเมิน:

- 80% เข้าใจวัตถุประสงค์การเก็บข้อมูลชัดเจน
- 70% ระบุว่าข้อมูลแจ้งมีความชัดเจนและเข้าใจง่าย
- ข้อเสนอแนะหลัก: ควรเพิ่มตัวอย่างประกอบคำอธิบายเพื่อความเข้าใจที่ดีขึ้น

แนวทางแก้ไข: ปรับปรุงข้อความในประกาศและเพิ่ม FAQ ตัวอย่าง

5.6.5 องค์การวิเคราะห์ข้อร้องเรียนจากสาธารณะเกี่ยวกับวิธีที่องค์กรใช้ข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งข้อร้องเรียนใด ๆ เกี่ยวกับวิธีที่องค์กรอธิบายถึงการใช้ข้อมูลส่วนบุคคลนั้น (การแจ้งในประกาศการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการใช้)

สิ่งที่ต้องทำ: มีการวิเคราะห์ข้อร้องเรียนจากสาธารณะเกี่ยวกับวิธีที่องค์กรใช้ข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพและครบถ้วน

หลักฐาน: แนวปฏิบัติขององค์กรในการวิเคราะห์ข้อร้องเรียนสาธารณะในส่วนที่เกี่ยวข้องกับวิธีที่องค์กรอธิบายถึงการใช้ข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

แนวปฏิบัติการวิเคราะห์ข้อร้องเรียนจากสาธารณะเกี่ยวกับวิธีที่องค์กรอธิบายถึงการใช้ข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อให้การจัดการข้อร้องเรียนเกี่ยวกับการใช้ข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพ โดยเฉพาะข้อร้องเรียนที่เกี่ยวข้องกับการแจ้งข้อมูลตามประกาศการคุ้มครองข้อมูลส่วนบุคคล เพื่อปรับปรุงและเพิ่มความชัดเจนในการสื่อสารแก่เจ้าของข้อมูลส่วนบุคคล

2. แนวปฏิบัติในการวิเคราะห์ข้อร้องเรียน

การรับข้อร้องเรียน

- ช่องทางรับข้อร้องเรียนจากสาธารณะ เช่น ทางอีเมล โทรศัพท์ เว็บไซต์ หรือจดหมาย
- บันทึกรายละเอียดข้อร้องเรียน เช่น วันที่ ผู้ร้องเรียน เนื้อหาข้อร้องเรียน

การจำแนกประเภทข้อร้องเรียน

- แยกข้อร้องเรียนที่เกี่ยวข้องกับการอธิบายวิธีใช้ข้อมูลส่วนบุคคลจากประเภทอื่น ๆ

การวิเคราะห์ข้อร้องเรียน

- ตรวจสอบรายละเอียดในประกาศการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- วิเคราะห์ข้อร้องเรียนเพื่อค้นหาสาเหตุของปัญหา เช่น ความไม่ชัดเจนในการแจ้งข้อมูล
- ประเมินผลกระทบต่อเจ้าของข้อมูลและองค์กร

การรายงานและเสนอแนะการแก้ไข

- จัดทำรายงานสรุปผลการวิเคราะห์ข้อร้องเรียน
- เสนอแนวทางแก้ไข ปรับปรุงประกาศการคุ้มครองข้อมูลส่วนบุคคล หรือช่องทางสื่อสารข้อมูล

การติดตามผล

- ตรวจสอบการนำข้อเสนอแนะไปปฏิบัติ
- ประเมินผลหลังการปรับปรุงอย่างสม่ำเสมอ

3. ตัวอย่างแบบฟอร์มบันทึกข้อร้องเรียนและการวิเคราะห์

วันที่ รับ เรื่อง	ผู้ ร้องเรียน	ประเภทข้อ ร้องเรียน	รายละเอียดข้อ ร้องเรียน	ผลการ วิเคราะห์	แนว ทางแก้ไข/ ปรับปรุง	สถานะการ ดำเนินการ
1 มิ.ย. 2568	นาย สมชาย	การแจ้ง ข้อมูลไม่ ชัดเจน	ไม่เข้าใจ วัตถุประสงค์ใน การเก็บข้อมูล ส่วนบุคคล	ข้อความ ประกาศไม่ ชัดเจนและ ซับซ้อน	ปรับข้อความ ให้ง่ายขึ้นและ เพิ่มตัวอย่าง	ดำเนินการ แก้ไข เรียบร้อยแล้ว
10 มิ.ย. 2568	นางสาว อร	ช่อง ทางการ	ไม่ทราบว่าข้อมูล ใช้ไปเพื่อ วัตถุประสงค์ใด	ช่องทาง สื่อสารข้อมูล	เพิ่มช่องทาง แจ้งข้อมูลผ่าน แอปพลิเคชัน	รอ ดำเนินการ

		สื่อสารไม่ ครบถ้วน		ไม่หลากหลาย พอ		

5.7.1 ประกาศการคุ้มครองข้อมูลส่วนบุคคลมีความชัดเจนและง่ายสำหรับสาธารณะในการเข้าถึง

สิ่งที่ต้องทำ: มีประกาศการคุ้มครองข้อมูลส่วนบุคคลชัดเจนและง่ายในการเข้าถึง

หลักฐาน: ช่องทางในการเผยแพร่ประกาศการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ช่องทางในการเผยแพร่ประกาศการคุ้มครองข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อแสดงให้เห็นว่าองค์กรมีความโปร่งใสในการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวิธีการใช้ข้อมูลของตน โดยเผยแพร่ประกาศการคุ้มครองข้อมูลส่วนบุคคลในช่องทางที่เข้าถึงได้ง่าย และมีความชัดเจนในการสื่อสาร

2. ช่องทางเผยแพร่ประกาศการคุ้มครองข้อมูลส่วนบุคคล

องค์กรได้ดำเนินการเผยแพร่ประกาศการคุ้มครองข้อมูลส่วนบุคคลผ่านช่องทางต่อไปนี้

2.1 เว็บไซต์ขององค์กร

ประกาศฯ ถูกเผยแพร่ในหน้าเว็บไซต์หลักขององค์กร โดยสามารถเข้าถึงได้จากแถบเมนู “นโยบายความเป็นส่วนตัว” หรือ “นโยบายคุ้มครองข้อมูลส่วนบุคคล”

ตัวอย่าง URL: <https://www.organizationname.or.th/privacy-policy>

รูปแบบที่เข้าใจง่าย มีภาษาที่เหมาะสมกับบุคคลทั่วไป รวมถึงผู้เยาว์ (มีฉบับย่อและฉบับเต็มให้เลือกอ่าน)

2.2 สื่อสิ่งพิมพ์และแผ่นพับ (ในสำนักงาน)

มีการติดประกาศฉบับย่อในพื้นที่ให้บริการ เช่น เคาน์เตอร์ต้อนรับ จุดลงทะเบียน และจุดบริการลูกค้า

มี QR Code สำหรับสแกนเพื่ออ่านฉบับเต็มทางออนไลน์

2.3 แอปพลิเคชันขององค์กร (ถ้ามี)

ในหน้า “ตั้งค่า” หรือ “ข้อมูลผู้ใช้” มีลิงก์ไปยังประกาศการคุ้มครองข้อมูลส่วนบุคคล จัดรูปแบบให้อ่านง่ายทั้งบนโทรศัพท์มือถือและแท็บเล็ต

2.4 แบบฟอร์มออนไลน์และแบบฟอร์มกระดาษ

แนบประกาศฯ ฉบับย่อไว้ท้ายแบบฟอร์มการลงทะเบียน ข้อมูลสมัครงาน และเอกสารอื่นที่มีการเก็บข้อมูลผู้ใช้งานต้องอ่านก่อนคลิก “ยอมรับ” หรือ “ให้ความยินยอม”

3. คุณลักษณะของประกาศการคุ้มครองข้อมูลส่วนบุคคล

- มีโครงสร้างที่เข้าใจง่าย แบ่งหัวข้อชัดเจน ได้แก่:
- วัตถุประสงค์ของการประมวลผลข้อมูล
- ประเภทของข้อมูลที่เก็บ
- สิทธิของเจ้าของข้อมูล
- ช่องทางการติดต่อ DPO หรือองค์กร
- ใช้ภาษาที่เป็นมิตร เหมาะกับผู้ใช้งานทั่วไป
- สำหรับข้อมูลของผู้เยาว์ มีเวอร์ชันที่เรียบเรียงให้เหมาะสมกับช่วงวัย

5.7.2 องค์กรมีเครื่องมือให้กับเจ้าของข้อมูลส่วนบุคคล เช่น ระบบการบริการตนเองที่ปลอดภัย แดชบอร์ด (Dashboards) และการแจ้งเตือนแบบทันเวลา (just-in-time notices) เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึง กำหนด และจัดการกับข้อมูลส่วนบุคคลของพวกเขาได้

สิ่งที่ต้องทำ: มีเครื่องมือที่มีประสิทธิภาพ เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึง กำหนด และจัดการกับข้อมูลส่วนบุคคลได้จริง

หลักฐาน: หลักฐานแสดงเครื่องมือที่ทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึง กำหนด และจัดการกับข้อมูลส่วนบุคคลได้

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เครื่องมือที่ให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึง กำหนด และจัดการกับข้อมูลส่วนบุคคลของตนได้

1. ระบบบริการตนเอง (Self-Service Platform)

องค์กรได้พัฒนาระบบบริการตนเองสำหรับเจ้าของข้อมูลส่วนบุคคล โดยระบบนี้มีฟังก์ชันการใช้งานดังนี้:

- เข้าสู่ระบบด้วยรหัส OTP หรือบัญชีผู้ใช้ที่ลงทะเบียนไว้ล่วงหน้า
- สามารถดูข้อมูลส่วนบุคคลที่องค์กรจัดเก็บไว้ได้
- สามารถแก้ไขข้อมูลบางรายการ เช่น ข้อมูลติดต่อ ที่อยู่ และความยินยอม
- สามารถดาวน์โหลดสำเนาข้อมูลของตนในรูปแบบ JSON หรือ PDF
- สามารถส่งคำขอเพื่อลบหรือระงับการใช้ข้อมูลได้ทันที

URL ระบบ: <https://dataportal.organizationname.or.th>

2. แดชบอร์ด (Data Privacy Dashboard)

แดชบอร์ดสำหรับผู้ที่ใช้ที่เข้าสู่ระบบแล้ว มีฟังก์ชันดังนี้:

- แสดงสถานะความยินยอมแต่ละประเภท (Consent Management)
- ประวัติการให้ความยินยอมและการเพิกถอนความยินยอม
- รายการการเข้าถึงข้อมูลย้อนหลัง (access logs)
- คำขอที่อยู่ระหว่างดำเนินการ และผลการดำเนินการ

หน้าแดชบอร์ดถูกออกแบบให้ใช้งานง่าย รองรับทั้งภาษาไทยและภาษาอังกฤษ และสามารถแสดงผลบนมือถือได้อย่างเหมาะสม

3. การแจ้งเตือนแบบทันเวลา (Just-In-Time Notices)

องค์กรมีระบบแสดง “การแจ้งเตือนแบบทันเวลา” ทุกครั้งที่มีการเก็บรวบรวมข้อมูลผ่านระบบออนไลน์หรือแอปพลิเคชัน เช่น:

- เมื่อมีการลงทะเบียนสมัครสมาชิก
- เมื่อเริ่มทำแบบสำรวจที่มีการเก็บข้อมูล
- ก่อนเก็บ cookies หรือข้อมูลเชิงพฤติกรรม

ตัวอย่างข้อความการแจ้ง:

“เราใช้ข้อมูลอีเมลของท่านเพื่อจัดส่งข่าวสารและสิทธิประโยชน์ หากไม่ต้องการรับข้อมูลนี้ ท่านสามารถเลือก ‘ไม่ยินยอม’ ได้ทันที”

ข้อความดังกล่าวจะแสดงเป็น Pop-up หรือ Banner ก่อนที่ระบบจะเก็บข้อมูล หรือให้ผู้ใช้ “คลิกตกลง” ในลักษณะที่เป็นไปตามหลัก Privacy by Design

4. เอกสารแนบ

- ภาพหน้าจอระบบบริการตนเอง
- ภาพหน้าจอแดชบอร์ดการจัดการข้อมูล
- ตัวอย่าง Pop-up แจ้งเตือน Just-in-time notice
- URL ทดลองใช้งานระบบ (หากมีเวอร์ชันสาธิต)

5.7.3 องค์กรกำหนดค่าเริ่มต้นความเป็นส่วนตัวที่ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล (Strong Privacy as Default) รวมถึงตัวเลือกและการควบคุมที่ใช้งานง่ายสำหรับเจ้าของข้อมูลส่วนบุคคล

- สิ่งที่ต้องทำ: มีการกำหนดค่าเริ่มต้นตามที่กำหนด และมีตัวเลือกและการควบคุมที่ใช้งานง่าย
- หลักฐาน: นโยบายหรือกระบวนการออกแบบโดยมีพื้นฐานมาจากการกำหนดค่าเริ่มต้นความเป็นส่วนตัวที่ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล (strong privacy as default)
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการกำหนดค่าเริ่มต้นความเป็นส่วนตัว (Privacy by Default Policy)

องค์กรได้จัดทำนโยบายการออกแบบระบบและบริการโดยคำนึงถึงความเป็นส่วนตัวตั้งแต่เริ่มต้น

ซึ่งรวมถึงการตั้งค่าความเป็นส่วนตัวเริ่มต้นที่ปลอดภัยและลดความเสี่ยง ดังนี้

- การตั้งค่าความเป็นส่วนตัวเริ่มต้นเป็น "ไม่ให้เผยแพร่ข้อมูล" หรือ "ไม่ยินยอม" เว้นแต่เจ้าของข้อมูลจะเลือกยินยอมเอง (Opt-in)
- ไม่เปิดเผยข้อมูลส่วนบุคคลต่อบุคคลภายนอกโดยอัตโนมัติ
- ข้อมูลส่วนบุคคลจะถูกรวบรวมเฉพาะเท่าที่จำเป็นต่อวัตถุประสงค์
- การเก็บ cookies ถูกจำกัดเฉพาะ cookies ที่จำเป็นโดยเริ่มต้น จนกว่าจะได้รับความยินยอมจากผู้ใช้
- ระบบแจ้งเตือนการเข้าถึงข้อมูลส่วนบุคคล เช่น การเข้าสู่ระบบจากอุปกรณ์ใหม่ หรือการเปลี่ยนรหัสผ่าน

2. การออกแบบ UI/UX เพื่อให้ควบคุมข้อมูลได้ง่าย

องค์กรได้พัฒนาการออกแบบที่เน้นผู้ใช้งานสามารถเข้าถึงและควบคุมการตั้งค่าความเป็นส่วนตัวได้ง่าย ดังนี้

- มีแดชบอร์ดความเป็นส่วนตัว (Privacy Dashboard) ให้เจ้าของข้อมูลสามารถ:
 - เปิด/ปิดการเก็บข้อมูลบางประเภท
 - จัดการสิทธิ์การเข้าถึงข้อมูลของบุคคลที่สาม
 - ดาวน์โหลด/ลบข้อมูลของตนได้ด้วยตนเอง
- ข้อความแจ้งความเป็นส่วนตัวถูกเขียนให้เข้าใจง่าย ไม่ใช้ศัพท์ทางเทคนิค

- ทุกการเก็บข้อมูลมี just-in-time notices อธิบายก่อนจะมีการดำเนินการจริง

3. กระบวนการออกแบบระบบที่อิงตามหลักการ Privacy by Design & Default

องค์กรมีแนวทางการพัฒนาระบบหรือผลิตภัณฑ์ดิจิทัลโดยพิจารณาเรื่องความเป็นส่วนตัวตั้งแต่ขั้นตอนการออกแบบ ได้แก่

- การทบทวน Privacy Impact Assessment (PIA/DPIA) ก่อนพัฒนา/ปรับปรุงระบบ
- การใช้การตั้งค่าเริ่มต้นให้ปลอดภัย (secure and minimal by default)
- มีแนวทางควบคุมการแบ่งปันข้อมูลภายในและภายนอกองค์กรโดยผ่านการอนุมัติล่วงหน้า
- อัปเดตแนวทางการออกแบบปีละอย่างน้อย 1 ครั้ง ตามมาตรฐานสากล เช่น ISO/IEC 27701, OWASP, GDPR

4. เอกสารแนบ

- สำเนานโยบาย Privacy by Default
- คู่มือ UI/UX สำหรับการออกแบบแดชบอร์ดและเมนูควบคุมความเป็นส่วนตัวส่วนตัว
- ภาพหน้าจอแดชบอร์ดและหน้าจอแจ้งความยินยอม
- เอกสารเวิร์กโฟลว์การพัฒนาโปรเจกต์ใหม่ที่รวม Privacy by Design

5.7.4 ในกรณีที่เกี่ยวข้อง องค์กรมีกระบวนการเพื่อช่วยให้ผู้เยาว์สามารถใช้สิทธิในการปกป้องความเป็นส่วนตัวของข้อมูลส่วนบุคคลด้วยวิธีที่เข้าถึงได้ง่ายและที่พวกเขาเข้าใจได้

สิ่งที่ต้องทำ: มีมาตรการสำหรับผู้เยาว์ และมีวิธีที่เข้าถึงได้ง่ายสำหรับผู้เยาว์

หลักฐาน: มาตรการเพื่อช่วยให้ผู้เยาว์สามารถใช้สิทธิในการปกป้องความเป็นส่วนตัวของข้อมูลส่วนบุคคลด้วยวิธีที่เข้าถึงได้ง่ายที่พวกเขาเข้าใจได้ เช่น การแจ้งเตือนแบบทันเวลา (just-in-time notices)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

มาตรการเพื่อช่วยให้ผู้เยาว์สามารถใช้สิทธิในการปกป้องความเป็นส่วนตัวของข้อมูลส่วนบุคคล ด้วยวิธีที่เข้าถึงได้ง่าย และที่พวกเขาเข้าใจได้ (หลักฐานตามเกณฑ์ข้อ 5.7.4)

1. นโยบายองค์กรเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของผู้เยาว์

องค์กรมีนโยบายเฉพาะด้านที่กำหนดการปฏิบัติต่อข้อมูลของผู้เยาว์โดยตรง ซึ่งรวมถึง

- การจำกัดการเก็บข้อมูลส่วนบุคคลของผู้เยาว์เฉพาะเท่าที่จำเป็น
- การกำหนดกลไกการให้ความยินยอมที่แตกต่างจากผู้ใหญ่ (เช่น ความยินยอมจากผู้ปกครอง)
- การมุ่งเน้น “Best Interest of the Child” ตามแนวทางของสหประชาชาติ

2. ช่องทางการใช้สิทธิที่เหมาะสมกับผู้เยาว์

องค์กรได้ออกแบบช่องทางการใช้สิทธิที่เหมาะสมกับระดับความเข้าใจของผู้เยาว์ เช่น

- หน้าเว็บไซต์พิเศษสำหรับเด็ก ที่ใช้ภาษาง่าย ไม่มีศัพท์ทางกฎหมาย
- การ์ตูนแอนิเมชัน หรือ วิดีโออธิบาย สิทธิข้อมูลส่วนบุคคล เช่น สิทธิขอเข้าถึง, ลบ, คัดค้าน
- เมนูคำสั่งแบบไอคอน ที่ออกแบบโดยนักออกแบบ UX ร่วมกับนักจิตวิทยาเด็ก

3. ตัวอย่างเครื่องมือที่ใช้

ระบบแดชบอร์ด “My Info for Kids”

เด็กสามารถเข้าสู่ระบบได้ผ่านรหัสสมาชิก (ไม่ใช่ชื่อจริง) แล้วเห็นรายการข้อมูลที่ระบบเก็บเกี่ยวกับพวกเขา พร้อมตัวเลือก “ขอลบข้อมูลนี้”, “แก้ไข”, หรือ “ไม่ให้เก็บอีก” พร้อมสัญลักษณ์เข้าใจง่าย

Just-in-time notices สำหรับเด็ก

ข้อความสั้นที่แจ้งเหตุผลในการเก็บข้อมูลแบบป๊อปอัพ เช่น:

“เราขอเก็บคะแนนเกมของคุณไว้ เพื่อให้คุณได้ลุ้นรางวัลทุกเดือน ตกลงไหม?” พร้อมปุ่ม "ตกลง" / "ไม่ตกลง"

ข้อความนี้ใช้ระดับภาษา CEFR A1-A2 (ประถม-ต้นมัธยม)

- การประเมินความเข้าใจของผู้เยาว์ (Child comprehension testing)
องค์กรได้ดำเนินการทดสอบความเข้าใจของผู้เยาว์ที่มีต่อการแจ้งเตือนและสิทธิของตน
- ใช้กลุ่มเด็กอายุ 8-12 ปี และ 13-17 ปี ในการทดสอบต้นแบบการแจ้งสิทธิ
- แบบสอบถามหลังใช้งาน ที่ประเมินว่าผู้เยาว์สามารถอธิบายสิทธิของตนกลับมาได้หรือไม่
ผลการทดสอบ (ปีล่าสุด): ร้อยละ 84 ของกลุ่มเป้าหมายสามารถระบุสิทธิของตนและใช้เครื่องมือได้ถูกต้อง

5. การอบรมบุคลากรเกี่ยวกับข้อมูลของผู้เยาว์

- เจ้าหน้าที่บริการลูกค้าและฝ่ายเทคโนโลยีได้รับการฝึกอบรมเพิ่มเติมเรื่อง
- ความเข้าใจทางพฤติกรรมเด็ก
- การอธิบายสิทธิของข้อมูลส่วนบุคคลให้เด็กเข้าใจ
- การจัดการกับคำขอจากผู้เยาว์โดยไม่ละเมิดสิทธิผู้ปกครองหรือกฎหมายอื่นที่เกี่ยวข้อง

6. การจัดเก็บหลักฐานการดำเนินงาน

- Log การใช้แดชบอร์ด “My Info for Kids”
- สถิติการใช้ just-in-time notices โดยเด็ก
- รายงานผลการทดสอบความเข้าใจผู้เยาว์
- บันทึกการสื่อสารทางอีเมลหรือโทรศัพท์ที่เกี่ยวข้องกับการใช้สิทธิของผู้เยาว์

- เอกสารการประชุมฝ่ายพัฒนา UX/Legal/Data เพื่อปรับปรุงบริการ

7.การประเมินและปรับปรุงประจำปี

- มีรอบการทบทวนเครื่องมือและภาษาที่ใช้ทุก 12 เดือน โดยรวมความคิดเห็นจาก
- เด็กที่ใช้บริการ
- ผู้ปกครอง
- ครู/นักจิตวิทยา
- ทีม Data Protection

5.7.5 องค์กรใช้มาตรการที่เหมาะสมเพื่อปกป้องผู้เยาว์ที่ใช้บริการดิจิทัลขององค์กร

สิ่งที่ต้องทำ: มีมาตรการสำหรับผู้เยาว์ที่เหมาะสมและมีประสิทธิภาพ

หลักฐาน: มาตรการปกป้องผู้เยาว์ที่ใช้บริการดิจิทัลขององค์กร เช่น มี Age verification tools

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารหลักฐานการดำเนินมาตรการปกป้องผู้เยาว์ที่ใช้บริการดิจิทัลขององค์กร (ตามเกณฑ์ 5.7.5 – การใช้มาตรการที่เหมาะสมเพื่อปกป้องผู้เยาว์)

1. นโยบายการปกป้องผู้เยาว์ (Child Online Protection Policy)

องค์กรมีนโยบายเป็นลายลักษณ์อักษรในการให้ความคุ้มครองผู้เยาว์ที่ใช้บริการดิจิทัล โดยมีเนื้อหาหลัก ดังนี้

- นิยามของ "ผู้เยาว์" ตามกฎหมายแห่งราชอาณาจักรไทย (อายุต่ำกว่า 20 ปีบริบูรณ์ หรือในบางกรณีตามนิยามของ GDPR คืออายุต่ำกว่า 16 ปี)
- หลักการให้บริการแบบ "Child-first design" คือ ออกแบบโดยยึดผลประโยชน์สูงสุดของเด็ก
- การเก็บข้อมูลเท่าที่จำเป็นและมีวัตถุประสงค์ชัดเจน
- ห้ามใช้ข้อมูลผู้เยาว์เพื่อการโฆษณาพฤติกรรมแบบระบุตัวตน (Behavioral Advertising)

2. มาตรการตรวจสอบอายุ (Age Verification Tools)

องค์กรมีระบบตรวจสอบอายุเพื่อแยกแยะผู้เยาว์ออกจากผู้ใหญ่ โดยใช้เทคโนโลยีและกระบวนการต่อไปนี้

2.1 ขั้นตอนยืนยันอายุขณะสมัครสมาชิก

- กลไก Double Confirmation: ให้ผู้สมัครกรอกวันเดือนปีเกิด + ยืนยันอายุผ่านอีเมลหรือ SMS
- ระบบอัลกอริทึมการตรวจจับอายุ: สำหรับบริการที่มีการใช้งานผ่านกล้อง (เช่น Video Chat) มีระบบระบุอายุโดยประมาณผ่านการวิเคราะห์ภาพใบหน้า (อิงจากมาตรฐานของ ICO และ age estimation AI)

2.2 ขั้นตอนเพิ่มเติมสำหรับผู้เยาว์

- เมื่อระบบตรวจพบว่าเป็นผู้ใช้อายุต่ำกว่าเกณฑ์ มีการ
- จำกัดฟีเจอร์ เช่น ไม่สามารถเปิดเผยข้อมูลสาธารณะ
- ปิดโฆษณาแบบกำหนดกลุ่มเป้าหมาย
- เปิดโหมด “คุ้มครองขั้นสูง” (High Privacy Mode) โดยอัตโนมัติ

3. ระบบควบคุมโดยผู้ปกครอง (Parental Control Tools)

- ผู้ปกครองสามารถผูกบัญชีของตนเข้ากับบัญชีของผู้เยาว์ เพื่อ
- ตรวจสอบกิจกรรมที่ได้รับอนุญาต
- ปรับระดับการเปิดเผยข้อมูลส่วนบุคคล
- จำกัดเวลาในการใช้งาน (เช่น ไม่เกิน 2 ชั่วโมงต่อวันในวันเรียน)
- รับแจ้งเตือนเมื่อมีการแชร์ข้อมูลหรือมีผู้ติดต่อใหม่

4. การออกแบบอินเทอร์เฟซที่ปลอดภัยและเข้าใจง่ายสำหรับผู้เยาว์

- UI/UX ใช้ภาษาธรรมดา (Plain Language)
- มีไอคอนสำหรับ “ความเป็นส่วนตัว”, “ขอความช่วยเหลือ” และ “อธิบายสิทธิ”
- แจ้งเตือนแบบ Just-in-time สำหรับการเก็บข้อมูล เช่น:
“เราขอเก็บเสียงของคุณเพื่อให้คุณเล่นเกมนี้ได้ คุณโอเคไหม?” [ใช่] [ไม่ใช่]

5. กระบวนการจัดการความเสี่ยงต่อผู้เยาว์ (Child Data Protection Risk Assessment)

- มีแบบฟอร์มเฉพาะสำหรับประเมินความเสี่ยงต่อผู้เยาว์ในการพัฒนา/เปิดตัวฟีเจอร์ใหม่
- มีคณะกรรมการย่อย (Child Data Panel) ทำหน้าที่ทบทวนบริการที่มีผลกระทบต่อเด็กก่อนเปิดใช้จริง
- ตัวอย่างคำถามในการประเมิน:
- เด็กสามารถเข้าใจได้ไหมว่าข้อมูลใดจะถูกเก็บ?
- เด็กสามารถขอให้ลบข้อมูลได้อย่างไร?
- เด็กจะถูกผลักดันให้แชร์ข้อมูลมากเกินไปหรือไม่?

6. การฝึกอบรมพนักงานและผู้ดูแลระบบ

- เจ้าหน้าที่ฝ่ายบริการลูกค้า, พนักงานฝ่ายพัฒนา IT, ฝ่ายนโยบายข้อมูล ได้รับการฝึกอบรม
- เรื่อง “การรับรู้ข้อมูลของผู้เยาว์”
- การสนทนาและรับเรื่องร้องเรียนจากผู้เยาว์
- การแจ้งสิทธิและแนวทางการยินยอมที่เหมาะสมกับเด็ก

7. การบันทึกและประเมินผลการใช้มาตรการ

- บันทึกการใช้งาน Age Verification (จำนวนผู้สมัครที่อายุต่ำกว่า 18 ปี)
- รายงานการใช้ Parental Control Dashboard
- ผลการสำรวจผู้ใช้เยาว์ประจำปี (User Satisfaction Survey for Minors)
- ตัวชี้วัด เช่น ความเข้าใจสิทธิ, ความรู้สึกปลอดภัย, ความสะดวกในการควบคุมข้อมูล
- กรณีร้องเรียนเกี่ยวกับเด็ก (เช่น การใช้ถ้อยคำล่อลวง, ความเข้าใจผิดของเด็ก ฯลฯ) มีการวิเคราะห์และปรับปรุงมาตรการอย่างต่อเนื่อง

การจัดทำบันทึกการรายการและฐานทางกฎหมาย

การจัดทำบันทึกการรายการและฐานทางกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลถือเป็นหนึ่งในหลักการสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ซึ่งสอดคล้องกับหลักการความรับผิดชอบ (Accountability) และการปฏิบัติตามข้อกำหนดทางกฎหมาย การจัดทำบันทึกการรายการอย่างเป็นระบบช่วยให้องค์กรสามารถตรวจสอบได้ว่า ข้อมูลส่วนบุคคลแต่ละประเภทถูกเก็บ ใช้ และเปิดเผยบนฐานทางกฎหมายที่ถูกต้อง และมีการจัดการอย่างเหมาะสมตามวัตถุประสงค์ที่กำหนด บันทึกการรายการข้อมูลและฐานทางกฎหมายยังช่วยให้การบริหารความเสี่ยงด้านข้อมูลเป็นไปอย่างมีประสิทธิภาพ เนื่องจากสามารถระบุและติดตามกระบวนการประมวลผลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้อย่างชัดเจน รวมถึงช่วยสนับสนุนการตรวจสอบภายในและภายนอกองค์กร การจัดทำเอกสารดังกล่าวครอบคลุมทั้งการระบุประเภทข้อมูล เจ้าของข้อมูล วัตถุประสงค์ของการประมวลผล ผู้เข้าถึงข้อมูล ระยะเวลาการเก็บรักษา และฐานทางกฎหมายที่ใช้รองรับการประมวลผล เช่น การยินยอม ข้อผูกพันตามสัญญา ความจำเป็นตามกฎหมาย หรือผลประโยชน์ชอบด้วยกฎหมายขององค์กร

นอกจากนี้ การบันทึกและจัดเก็บเอกสารอย่างเป็นระบบยังช่วยให้บุคลากรทุกระดับสามารถปฏิบัติตามแนวทางที่กำหนด ตรวจสอบการเข้าถึงและการใช้ข้อมูลได้อย่างชัดเจน รวมถึงเป็นหลักฐานสำคัญที่แสดงถึงความมุ่งมั่นขององค์กรในการปฏิบัติตาม PDPA อย่างครบถ้วน การทบทวนและปรับปรุงบันทึกการรายการและฐานทางกฎหมายอย่างต่อเนื่องยังเป็นกลไกสำคัญในการรักษาความสอดคล้องกับกฎหมายที่เปลี่ยนแปลงและบริบทการประมวลผลข้อมูลที่ปรับตัวตามเทคโนโลยีและความต้องการขององค์กร

บทนี้จึงเน้นไปที่การจัดทำบันทึกการรายการข้อมูลส่วนบุคคลและฐานทางกฎหมายที่ครบถ้วน ถูกต้อง และตรวจสอบได้ เพื่อให้มั่นใจว่าการดำเนินงานด้านข้อมูลส่วนบุคคลขององค์กรสอดคล้องกับ PDPA และสามารถสร้างความเชื่อมั่นแก่เจ้าของข้อมูลได้อย่างยั่งยืน

โดยในการจัดทำบันทึกการรายการข้อมูลส่วนบุคคลและฐานทางกฎหมายถือเป็นองค์ประกอบสำคัญของการบริหารจัดการข้อมูลอย่างมีความรับผิดชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) บันทึกเหล่านี้ช่วยให้องค์กรสามารถตรวจสอบได้ว่าแต่ละรายการข้อมูลส่วนบุคคลถูกเก็บ ใช้ และเปิดเผยบนฐานทางกฎหมายที่ถูกต้อง และสอดคล้องกับวัตถุประสงค์ที่กำหนดไว้ ทั้งยังเป็นเครื่องมือสำคัญในการบริหารความเสี่ยงด้านข้อมูลและสนับสนุนการตรวจสอบ Compliance ภายในและภายนอกองค์กร การจัดทำบันทึกการรายการข้อมูลส่วนบุคคลควรครอบคลุมหลายมิติ ได้แก่ ประเภทข้อมูล เจ้าของข้อมูล วัตถุประสงค์ของการประมวลผล ผู้เข้าถึงข้อมูล ระยะเวลาเก็บรักษา และฐานทางกฎหมายที่รองรับการประมวลผล เช่น การยินยอม ข้อผูกพันตามสัญญา ความจำเป็นตามกฎหมาย หรือผลประโยชน์ชอบด้วยกฎหมาย การบันทึกข้อมูลเหล่านี้ยังเป็นระบบช่วยให้บุคลากรทุกระดับสามารถปฏิบัติตามแนวทางได้อย่างชัดเจน ตรวจสอบการเข้าถึงและการใช้ข้อมูลได้อย่างโปร่งใส และสร้างความมั่นใจว่าองค์กรปฏิบัติตามข้อกำหนดของ PDPA อย่างครบถ้วน นอกจากนี้ การทบทวนและปรับปรุงบันทึกอย่างต่อเนื่องเป็นสิ่งสำคัญ เพื่อให้สอดคล้องกับการ

เปลี่ยนแปลงของกฎหมายหรือบริบทการประมวลผลข้อมูลใหม่ การอบรมบุคลากรเกี่ยวกับวิธีการจัดทำบันทึก
รายการและการระบุฐานทางกฎหมายยังเป็นกลไกสำคัญที่ช่วยให้การปฏิบัติงานเป็นไปอย่างถูกต้องและยั่งยืน

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/ หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
6.1 การระบุ ประเภทข้อมูล ส่วนบุคคล	ระบุข้อมูลส่วนบุคคลทุก ประเภทที่องค์กรเก็บ ใช้ และ ประมวลผล	Data Inventory, Data Mapping, ตารางสรุป ประเภทข้อมูล	ครอบคลุมทุกประเภท ข้อมูลที่เกี่ยวข้องและ ตรวจสอบได้
6.2 การระบุ เจ้าของข้อมูล	บันทึกเจ้าของข้อมูลแต่ละ รายการอย่างชัดเจน เช่น พนักงาน ลูกค้า คู่ค้า	Data Inventory, รายการเจ้าของข้อมูล, Record Log	มีข้อมูลเจ้าของ ครบถ้วน ตรวจสอบ ย้อนหลังได้
6.3 การระบุ วัตถุประสงค์ของ การประมวลผล	ระบุวัตถุประสงค์ในการเก็บ ใช้ ประมวลผล และเปิดเผยข้อมูล ของแต่ละรายการ	Documented Purpose Statement, Data Processing Records	ครอบคลุม วัตถุประสงค์ทุก กระบวนการและ สอดคล้องกับการใช้ งานจริง
6.4 การระบุผู้ เข้าถึงและ ผู้เกี่ยวข้อง	ระบุว่าใครมีสิทธิ์เข้าถึงหรือ ประมวลผลข้อมูลแต่ละประเภท	Access Control List, Role-based Permission Matrix	ระบุชัดเจนและ สอดคล้องกับบทบาท หน้าที่ของผู้เข้าถึง ข้อมูล
6.5 การระบุ ระยะเวลาเก็บ รักษาข้อมูล	กำหนดระยะเวลาการเก็บข้อมูล แต่ละประเภทและการลบหรือ ทำลายข้อมูลเมื่อครบกำหนด	Data Retention Policy, Retention Schedule, Record Log	ระบุครบทุกประเภท ข้อมูล มีระบบติดตาม การเก็บรักษาและลบ ตามกำหนด
6.6 การระบุฐาน ทางกฎหมายใน การประมวลผล	ระบุฐานทางกฎหมายแต่ละ รายการ เช่น ความยินยอม ข้อ ผูกพันตามสัญญา ความจำเป็น ตามกฎหมาย หรือผลประโยชน์ ชอบด้วยกฎหมาย	Legal Basis Register, Compliance Checklist, Documented Justification	ระบุฐานกฎหมาย ครบถ้วน สอดคล้อง กับวัตถุประสงค์และ ตรวจสอบได้

หัวข้อย่อ	สิ่งที่ต้องดำเนินการ	เอกสาร/ หลักฐานที่ต้องมี	เกณฑ์การให้คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
6.7 การบันทึก และจัดเก็บบันทึก รายการ	จัดเก็บบันทึกการประมวลผล ข้อมูลและฐานทางกฎหมาย อย่างเป็นระบบ	Data Inventory System, Record Log, Version Control	มีระบบจัดเก็บ ครบถ้วน ตรวจสอบ ย้อนหลังได้และอัปเดต ตามเวอร์ชันเอกสาร
6.8 การทบทวน และปรับปรุง บันทึกรายการ	ทบทวนและปรับปรุงบันทึก รายการและฐานทางกฎหมาย อย่างต่อเนื่อง อย่างน้อยปีละ 1 ครั้ง หรือเมื่อกฎหมายเปลี่ยน	Version Control Log, รายงานประชุมปรับปรุง, Memo การแก้ไข เอกสาร	มีหลักฐานการ ปรับปรุงต่อเนื่อง แสดงการอัปเดตตาม กฎหมายหรือแนวทาง ใหม่
6.9 การอบรม และสร้างความ ตระหนักรู้	อบรมบุคลากรเกี่ยวกับการ จัดทำบันทึกรายการและการ อ้างอิงทางกฎหมาย	แผนอบรม, สไลด์, แบบสอบถามประเมินผล , Attendance Sheet	บุคลากรทุกระดับ ได้รับการอบรม มี หลักฐานชัดเจน และ สามารถปฏิบัติได้จริง
6.10 การ ตรวจสอบและ ติดตามภายใน	ตรวจสอบว่าบันทึกรายการและ ฐานทางกฎหมายถูกใช้และ ปฏิบัติจริง	Internal Audit Report, Compliance Checklist, Audit Log	มีรายงานตรวจสอบ และข้อเสนอแนะ พร้อมหลักฐานการ ปฏิบัติจริง

การจัดทำเอกสารตามเกณฑ์

6.1.1 องค์กรมีการทบทวนแผนผังข้อมูลหรือมีการจัดทำแผนผังข้อมูลเพื่อทำความเข้าใจการไหลเวียน ของข้อมูลส่วนบุคคลในองค์กร

สิ่งที่ต้องทำ: มีการจัดทำแผนผังข้อมูลที่ชัดเจนและมีประสิทธิภาพ

หลักฐาน: แผนผังข้อมูล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

แผนผังข้อมูลส่วนบุคคล (Data Flow Diagram - DFD)

1. จุดประสงค์

เพื่อแสดงการไหลเวียนของข้อมูลส่วนบุคคลภายในองค์กร ตั้งแต่การเก็บรวบรวม การใช้ การจัดเก็บ
การส่งต่อ ไปจนถึงการลบหรือทำลายข้อมูล

2. ประเภทข้อมูลส่วนบุคคลที่เกี่ยวข้อง

- ข้อมูลลูกค้า (ชื่อ, เบอร์โทร, อีเมล, ที่อยู่)
- ข้อมูลพนักงาน (ประวัติส่วนตัว, ประวัติการทำงาน, หมายเลขบัญชีธนาคาร)
- ข้อมูลคู่สัญญา (ชื่อผู้ประกอบการ, ที่อยู่บริษัท, เลขประจำตัวผู้เสียภาษี)

แผนผังข้อมูลส่วนบุคคล: ระดับองค์กร (Data Flow Overview)

[เจ้าของข้อมูล]



[ช่องทางรับข้อมูล] -- (แบบฟอร์ม เว็บไซต์ แอปฯ E-mail)



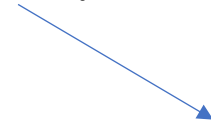
[ฝ่ายที่รับผิดชอบการเก็บข้อมูล]



[ระบบจัดเก็บข้อมูล]



[ฝ่ายที่ใช้ข้อมูล] [การส่งข้อมูลออกภายนอก]
(เช่น Cloud Outsource)



[การเก็บรักษาข้อมูล]



[การลบ / ทำลาย / คืนข้อมูล]

ตัวอย่างแบบเป็นขั้นตอน (พร้อมคำอธิบาย)

ลำดับ	กระบวนการ	หน่วยงาน/ระบบ	คำอธิบาย
1	การเก็บข้อมูล	ฝ่ายขาย / แบบฟอร์มสมัคร / เว็บไซต์	ลูกค้าให้ข้อมูลติดต่อเมื่อสมัครใช้บริการ
2	การจัดเก็บ	ระบบ CRM / ฐานข้อมูล HR	ข้อมูลถูกเก็บในฐานข้อมูลที่มีการควบคุมการเข้าถึง
3	การใช้ข้อมูล	ฝ่ายการตลาด / ฝ่ายบัญชี	ใช้ส่งโปรโมชั่น หรือออกใบเสร็จ / จ่ายเงินเดือน
4	การส่งต่อ	บ.รับช่วงประมวลผล / ระบบ Cloud	ใช้เก็บข้อมูลบน Cloud หรือให้ Third Party วิเคราะห์ข้อมูล
5	การทำลาย	IT / ฝ่ายกฎหมาย	เมื่อครบกำหนดตาม retention policy จะลบหรือทำลาย

เอกสารแนบ

- ไฟล์แผนผังข้อมูล (PDF หรือ PNG ที่สร้างจากโปรแกรม เช่น Lucid chart, Draw.io, PowerPoint หรือ Visio)
- รายชื่อระบบที่จัดเก็บข้อมูล
- นโยบายการเก็บรักษาและลบข้อมูล

6.1.2 แผนผังข้อมูลมีความถูกต้องเป็นปัจจุบัน และมีการมอบหมายให้มีผู้รับผิดชอบในการทบทวนเพื่อให้ข้อมูลเป็นปัจจุบันและถูกต้องอยู่เสมอ

สิ่งที่ต้องทำ: มีการมอบหมายให้มีผู้รับผิดชอบในการทบทวนแผนผังข้อมูล และมีรอบระยะเวลาการทบทวนที่ชัดเจน ข้อมูลถูกต้องและเป็นปัจจุบัน

หลักฐาน: หลักฐานการแต่งตั้งผู้รับผิดชอบในการจัดทำแผนผังข้อมูลในองค์กรและในแต่ละแผนก

สภาพบังคับ: กฎหมายไม่ได้กำหนด

คำสั่งแต่งตั้งผู้รับผิดชอบในการทบทวนแผนผังข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อแต่งตั้งผู้รับผิดชอบหลักในการจัดทำและทบทวนแผนผังข้อมูลส่วนบุคคลขององค์กรให้ถูกต้อง และเป็นปัจจุบัน รวมถึงกำหนดระยะเวลาการทบทวนที่ชัดเจน

2. รายละเอียดคำสั่งแต่งตั้ง

คำสั่งที่: 001/2567

เรื่อง: แต่งตั้งผู้รับผิดชอบในการจัดทำและทบทวนแผนผังข้อมูลส่วนบุคคลขององค์กร

ด้วยองค์กรตระหนักถึงความสำคัญของความถูกต้อง ครบถ้วน และเป็นปัจจุบันของแผนผังข้อมูลส่วนบุคคล ซึ่งถือเป็นองค์ประกอบพื้นฐานในการควบคุมความเสี่ยงและดำเนินการให้เป็นไปตามแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล

จึงแต่งตั้งบุคลากรเพื่อทำหน้าที่ดังนี้

(1) ผู้รับผิดชอบหลักขององค์กร

ชื่อ-สกุล: นายสมชาย ตั้งใจดี

ตำแหน่ง: หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ (IT)

หน้าที่

- รวบรวมแผนผังข้อมูลจากแต่ละหน่วยงาน
- ตรวจสอบความถูกต้องและการเชื่อมโยงข้อมูล
- จัดทำแผนผังภาพรวมองค์กร
- ประสานงานกับ DPO (Data Protection Officer)

(2) ผู้รับผิดชอบแต่ละหน่วยงาน

หน่วยงาน	ชื่อ-สกุล	ตำแหน่ง	หน้าที่
ฝ่ายบุคคล	นางสาวพรทิพย์ ใจงาม	หัวหน้า HR	จัดทำแผนผังข้อมูลพนักงาน
ฝ่ายขาย/ การตลาด	นายธนกฤต แสงทอง	หัวหน้าฝ่ายขาย	จัดทำแผนผังข้อมูลลูกค้า
ฝ่ายบัญชี	นางสาวชลธิชา เงินดี	นักบัญชีอาวุโส	จัดทำแผนผังข้อมูลการเงินและการจ่ายเงิน
ฝ่าย IT	นายวีรยุทธ เก่งจริง	เจ้าหน้าที่ระบบ	จัดทำแผนผังโครงสร้างการจัดเก็บและระบบรักษาความปลอดภัยของข้อมูล

3. รอบระยะเวลาการทบทวนแผนผังข้อมูล

การทบทวนแผนผังข้อมูลจะดำเนินการตามรอบดังนี้

ความถี่: ทุก 6 เดือน

รอบทบทวนถัดไป: กรกฎาคม 2567 และ มกราคม 2568

กรณีทบทวนเพิ่มเติม

- มีการเปลี่ยนระบบ IT / การจัดเก็บข้อมูล
- มีการเปลี่ยนนโยบายหรือกระบวนการสำคัญในงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- มีเหตุการณ์ด้านความปลอดภัยข้อมูล (เช่น ข้อมูลรั่วไหล)

4. การบันทึกผลการทบทวน

- ผู้รับผิดชอบแต่ละฝ่ายจะต้องจัดทำ **รายงานทบทวน** โดยระบุว่า
- มีการเปลี่ยนแปลงในกระบวนการจัดเก็บ/ใช้ข้อมูลหรือไม่
- แผนผังข้อมูลยังถูกต้องหรือมีจุดที่ต้องปรับปรุง
- แนบแผนผังฉบับปรับปรุง (ถ้ามี)
- รายงานส่งให้ DPO ภายในวันที่ 25 ของเดือนที่ครบรอบ

5. ลงนามคำสั่ง

ออกคำสั่ง ณ วันที่ 1 มิถุนายน พ.ศ. 2567

ลงนามโดย

.....

(นางศรินทิพย์ บริหารดี)

ผู้อำนวยการองค์กร

6.1.3 มีการตรวจสอบหรือกับส่วนงานอื่น ๆ ในองค์กรที่เกี่ยวข้อง เพื่อให้มั่นใจว่าแผนผังข้อมูลที่จัดทำมีความถูกต้อง และมีความสอดคล้องกันในเชิงกระบวนการกับส่วนงานอื่น (อาจใช้วิธีการตรวจสอบโดยคำถามหรือแบบสำรวจ)

สิ่งที่ต้องทำ: มีการตรวจสอบหรือกับหน่วยงานที่เกี่ยวข้องอย่างครบถ้วน

หลักฐาน: แบบสำรวจหรือคำถามการสอบถามข้อมูลเพื่อจัดทำแผนผังข้อมูลขององค์กร

สภาพบังคับ: กฎหมายไม่ได้กำหนด

แบบสอบถาม/แบบสำรวจการสอบถามข้อมูลเพื่อจัดทำแผนผังข้อมูลขององค์กร

วัตถุประสงค์:

เพื่อรวบรวมข้อมูลจากหน่วยงานภายในองค์กร เพื่อจัดทำหรือทบทวนแผนผังข้อมูลส่วนบุคคลให้มีความถูกต้อง ครบถ้วน และสอดคล้องกันในเชิงกระบวนการ

กลุ่มเป้าหมาย: หัวหน้าหรือผู้รับผิดชอบในแต่ละหน่วยงานที่มีการเก็บ ใช้ หรือประมวลผลข้อมูลส่วนบุคคล

แบบสอบถามการตรวจสอบข้อมูลส่วนบุคคลภายในหน่วยงาน

(เพื่อประกอบการจัดทำแผนผังข้อมูลส่วนบุคคลขององค์กร)

ข้อมูลเบื้องต้น

ชื่อหน่วยงาน: _____

ผู้ตอบแบบสอบถาม: _____

ตำแหน่ง: _____

วันที่ตอบ: _____

ตอนที่ 1: แหล่งที่มาของข้อมูลส่วนบุคคล

คำถาม	รายละเอียดคำตอบ
1. หน่วยงานของท่านเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งใดบ้าง?	☐ ลูกค้าโดยตรง ☐ เว็บไซต์ ☐ แบบฟอร์มกระดาษ ☐ บุคคลภายนอก ☐ ระบบภายในองค์กร
2. ประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวมคืออะไร?	_____ _____ _____ _____
3. มีข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรือไม่? (เช่น ข้อมูลสุขภาพ ศาสนา)	☐ มี โปรดระบุ: _____ ☐ ไม่มี

ตอนที่ 2: การใช้และเปิดเผยข้อมูล

คำถาม	รายละเอียดคำตอบ
4. ข้อมูลถูกนำไปใช้ในกิจกรรมใดบ้างในหน่วยงาน?	_____ _____ _____ _____
5. หน่วยงานของท่านมีการส่งต่อหรือแบ่งปันข้อมูลกับหน่วยงานภายในอื่นหรือไม่?	☐ มี โปรดระบุหน่วยงาน: _____ ☐ ไม่มี

6. หน่วยงานมีการส่งข้อมูลไปยังภายนอกองค์กรหรือไม่?

☐ มี โปรดระบุผู้รับ: _____ ☐ ไม่มี

ตอนที่ 3: การจัดเก็บและความปลอดภัยของข้อมูล

คำถาม	รายละเอียดคำตอบ
7. หน่วยงานเก็บข้อมูลส่วนบุคคลไว้ที่ใด?	☐ ฐานข้อมูลกลางองค์กร ☐ เซิร์ฟเวอร์แยกภายใน ☐ บน Cloud ☐ แฟ้มเอกสาร
8. มีมาตรการควบคุมสิทธิการเข้าถึงข้อมูลหรือไม่?	☐ มี ☐ ไม่มี โปรดอธิบาย: _____
9. หน่วยงานมีการกำหนดระยะเวลาเก็บรักษาข้อมูลหรือไม่?	☐ มี โปรดระบุระยะเวลา: _____ ☐ ไม่มี

ตอนที่ 4: ความสอดคล้องกับหน่วยงานอื่น

คำถาม	รายละเอียดคำตอบ
10. หน่วยงานของท่านเห็นว่าข้อมูลที่จัดทำแผนผังสอดคล้องกับกระบวนการของหน่วยงานอื่นหรือไม่?	☐ สอดคล้อง ☐ ไม่แน่ใจ ☐ ควรปรับปรุง
11. มีข้อเสนอแนะเพิ่มเติมเกี่ยวกับการจัดทำแผนผังข้อมูลหรือไม่?	_____ _____ _____

ลายเซ็นรับรอง

ลงชื่อ: _____

(ผู้ให้ข้อมูล)

วันที่: ____ / ____ / ____

แนบเพิ่มเติม

- แบบฟอร์มนี้ควรเก็บไว้เป็น **หลักฐานประกอบการทบทวนแผนผังข้อมูล** และแนบไว้กับเอกสารเวียนภายในองค์กร

เพื่อแสดงหลักฐานว่าองค์กรมีการทบทวน บันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities - ROPA) อย่างสม่ำเสมอ และเพื่อให้แน่ใจว่า ข้อมูลส่วนบุคคลที่เก็บรวบรวมมีเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมายขององค์กร ตามหลัก Data Minimization ภายใต้ มาตรา 22 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3. ขอบเขตของเอกสาร

เอกสารนี้ใช้กับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลในทุกหน่วยงานขององค์กร และทุกระบบที่เกี่ยวข้องกับการเก็บ ใช้ เปิดเผย หรือโอนข้อมูลส่วนบุคคล

4. หลักการที่ใช้ในการทบทวน

การทบทวนรายการบันทึกข้อมูลจะพิจารณาจากหลักการดังต่อไปนี้:

เกณฑ์	รายละเอียด
วัตถุประสงค์ของการประมวลผล	ตรวจสอบว่ายังคงสอดคล้องกับวัตถุประสงค์ที่กำหนดไว้หรือไม่
ประเภทของข้อมูล	ตรวจสอบว่ามีข้อมูลใดที่เกินความจำเป็นและสามารถยกเลิกการจัดเก็บได้หรือไม่
ระยะเวลาเก็บรักษา	มีข้อมูลใดที่พ้นระยะเวลาการเก็บรักษาแล้วหรือไม่
สิทธิของเจ้าของข้อมูล	ตรวจสอบว่าการเก็บข้อมูลเป็นไปตามสิทธิของเจ้าของข้อมูลหรือไม่

5. ความถี่ในการทบทวน

ทบทวนอย่างน้อย ปีละ 1 ครั้ง โดย DPO (Data Protection Officer) หรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

ในกรณีที่มีการเปลี่ยนแปลงวัตถุประสงค์การประมวลผลหรือระบบที่ใช้ จะมีการทบทวนเพิ่มเติมทันที

6. ขั้นตอนในการทบทวน

รวบรวมรายการกิจกรรมการประมวลผลข้อมูล (ROPA) ปัจจุบัน

วิเคราะห์ข้อมูลที่เกี่ยวข้องกับวัตถุประสงค์ที่ชอบด้วยกฎหมายหรือไม่

ทำเครื่องหมายรายการข้อมูลนี้อาจเกินความจำเป็น

จัดประชุมคณะกรรมการ DPO เพื่อพิจารณาข้อมูลที่ไม่จำเป็น

ปรับปรุงเอกสาร ROPA และแจ้งหน่วยงานที่เกี่ยวข้อง

7. ตัวอย่างผลการทบทวน (แนบได้เป็นหลักฐาน)

วันที่ ทบทวน	หน่วยงาน	ข้อมูลพบว่าเกินเกินจำเป็น	แนวทางแก้ไข

1 มิ.ย. 2567	แผนทรัพยากรบุคคล	บันทึกใบสมัครงานของผู้สมัครที่ไม่ผ่านการคัดเลือกเกิน 2 ปี	กำหนดลบอัตโนมัติภายใน 1 ปี
1 มิ.ย. 2567	แผนการตลาด	รายชื่อลูกค้าเก่าที่ไม่ตอบสนองต่อการตลาดเกิน 3 ปี	นำข้อมูลออกจากระบบ CRM

8. มาตรการรองรับ

- กำหนดใน Policy และ คู่มือปฏิบัติของเจ้าหน้าที่
- จัดอบรมผู้เกี่ยวข้องเกี่ยวกับหลักการ Data Minimization
- บูรณาการในระบบจัดการข้อมูล เช่น กำหนดการลบข้อมูลอัตโนมัติ

9. อ้างอิงทางกฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- มาตรา 22: การเก็บรวบรวมต้องจำกัดเท่าที่จำเป็นตามวัตถุประสงค์ที่ได้แจ้งไว้
- มาตรา 39 วรรคหนึ่ง: ผู้ควบคุมข้อมูลต้องจัดให้มีและเก็บรักษาบันทึกรายการ

โทษทางปกครอง หากไม่ปฏิบัติตาม มาตรา 39 วรรคหนึ่ง: ปรับไม่เกิน 3 ล้านบาท

10. ผู้จัดทำ

นาย/นาง.....

ตำแหน่ง: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

วันที่จัดทำ:

6.2.3 มีการทบทวนบันทึกการอย่างสม่ำเสมอให้มีความสอดคล้องกับนโยบายและแนวปฏิบัติขององค์กร เพื่อให้มั่นใจว่าบันทึกการมีความถูกต้องและเป็นปัจจุบัน รวมถึงมีการมอบหมายอย่างชัดเจนว่าบุคคลใดเป็นผู้รับผิดชอบทำหน้าที่ทบทวนบันทึกการดังกล่าว

สิ่งที่ต้องทำ: มีการทบทวนบันทึกการ และมอบหมายบุคคลที่มีหน้าที่รับผิดชอบให้ชัดเจน

หลักฐาน: แผนการทบทวนบันทึกการขององค์กร

หลักฐานการแต่งตั้งผู้รับผิดชอบในการจัดทำบันทึกการขององค์กรและในแต่ละแผนก

สภาพบังคับ: กฎหมายไม่ได้กำหนด

แผนการทบทวนบันทึกการประมวลผลข้อมูลส่วนบุคคล และการแต่งตั้งผู้รับผิดชอบ

1. ชื่อเอกสาร

แผนการทบทวนและมอบหมายหน้าที่ในการดูแลบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA)

2. ความมุ่งหมายของเอกสาร

เพื่อกำหนดแนวทางในการทบทวนรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลให้สอดคล้องกับ นโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร และเพื่อมอบหมายผู้รับผิดชอบในแต่ละหน่วยงานอย่างชัดเจน เพื่อให้ข้อมูลมีความ ถูกต้อง ครบถ้วน และเป็นปัจจุบัน

3. ขอบเขตการใช้

ใช้บังคับกับทุกหน่วยงานภายในองค์กรที่มีการเก็บ ใช้ เปิดเผย หรือโอนข้อมูลส่วนบุคคล ทั้งในรูปแบบอิเล็กทรอนิกส์และเอกสาร

4. แนวทางการทบทวน

การทบทวนบันทึกการ (Record of Processing Activities – ROPA) จะครอบคลุมเนื้อหา ดังนี้

รายการ	จุดที่ต้องทบทวน
วัตถุประสงค์ในการประมวลผล	ยังสอดคล้องกับการดำเนินงานหรือไม่
ประเภทข้อมูลส่วนบุคคล	ยังจำเป็นหรือมีการเปลี่ยนแปลงหรือไม่
ระยะเวลาเก็บรักษา	สอดคล้องกับนโยบาย retention หรือไม่
ผู้ควบคุมและผู้ประมวลผลข้อมูล	มีการเปลี่ยนแปลงหรือเพิ่มเติมหรือไม่
กลุ่มเป้าหมายของข้อมูล	มีการเปลี่ยนแปลงหรือขยายกลุ่มหรือไม่

5. ตารางแผนการทบทวน

หน่วยงาน	ความถี่ในการทบทวน	ผู้รับผิดชอบ	เครื่องมือ/ระบบที่ใช้
ฝ่ายบุคคล	ทุก 6 เดือน	น.ส. สีนันญา การบุญ	ระบบ HRMS + แบบฟอร์ม ROPA
ฝ่ายขายและการตลาด	ทุก 6 เดือน	นายพงศกร สุนทรโชติ	ระบบ HRM

ฝ่ายเทคโนโลยีสารสนเทศ	ทุก 6 เดือน	นายณัฐวุฒิ อินทร์ประเสริฐ	ระบบ IT Asset & DB
DPO (ศูนย์รวม)	ทุก 6 เดือน	น.ส. มาลี รัตนคุณ (DPO)	เอกสารสรุป ROPA ส่วนกลาง

6. การแต่งตั้งผู้รับผิดชอบ

คำสั่งแต่งตั้งผู้รับผิดชอบในการดูแลและทบทวนบันทึกการรายการ

องค์กรได้ออกคำสั่งแต่งตั้งอย่างเป็นทางการลงวันที่ .../.../.... ระบุชัดเจนว่า

แต่งตั้งผู้รับผิดชอบประจำหน่วยงานในการจัดทำและทบทวนบันทึกการรายการข้อมูลส่วนบุคคลให้สอดคล้องกับนโยบายองค์กร พร้อมรายงานต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ทุก 6 เดือน

ตัวอย่างคำสั่งแนบท้าย

- เอกสาร คำสั่งที่ 04/2567 เรื่องการแต่งตั้งผู้รับผิดชอบดูแลบันทึกการรายการข้อมูล
- เอกสาร แบบฟอร์มรายงานการทบทวน ROPA รอบ 1/2567

7. การติดตามผล

- DPO จะรวบรวมผลการทบทวนและรายงานต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
- มีการประชุมสรุปผลการทบทวนทุก 6 เดือน พร้อมข้อเสนอแนะเพื่อปรับปรุงรายการ

8. เอกสารแนบ (หลักฐาน)

- ตารางทบทวนบันทึกการรายการ (ตัวอย่างจริง)
- แบบฟอร์มทบทวน ROPA (Template)
- หนังสือแต่งตั้งผู้รับผิดชอบในแต่ละหน่วยงาน (ไฟล์แนบ)

9. ผู้จัดทำ

นาย/นาง.....

ตำแหน่ง: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

วันที่จัดทำ:

การทำเอกสารเหมือนรายการ 6.2.1 บันทึกการรายการถูกจัดทำในรูปแบบหนังสือหรือ อิเล็กทรอนิกส์ หรือ อาจทำตามตัวอย่างนี้

ชื่อองค์กร: บริษัท ABC จำกัด

หัวข้อ: บันทึกการรายการข้อมูลส่วนบุคคล

รูปแบบ: อิเล็กทรอนิกส์ (Excel / Google Sheets / ระบบจัดการฐานข้อมูล)

วันที่จัดทำ: 1 มิถุนายน 2568

ผู้รับผิดชอบ: ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO)

ลำดับ	ข้อมูลส่วนบุคคลที่เก็บรวบรวม	วัตถุประสงค์ของการเก็บรวบรวม	ผู้ควบคุมข้อมูล	ระยะเวลาการเก็บรักษา	สิทธิและวิธีการเข้าถึง	การใช้หรือเปิดเผยข้อมูล (มาตรา 27 วรรค 3)	การปฏิเสธคำขอ / คัดค้าน	มาตรการรักษาความมั่นคงปลอดภัย
1	ชื่อ-นามสกุล, เบอร์โทรศัพท์, ที่อยู่	เพื่อการติดต่อและจัดส่งสินค้า	ฝ่ายลูกค้าสัมพันธ์	5 ปี หลังเลิกใช้บริการ	เจ้าของข้อมูลมีสิทธิขอแก้ไขหรือลบข้อมูลผ่านทางอีเมล	ไม่มีการเปิดเผยข้อมูลแก่บุคคลภายนอก	ไม่มี	การเข้ารหัสข้อมูล, จำกัดสิทธิ์เข้าถึงข้อมูล
2	ข้อมูลบัตรเครดิต	เพื่อชำระเงินและยืนยันตัวตน	ฝ่ายบัญชี	2 ปี ตามนโยบายการเงิน	เจ้าของข้อมูลสามารถขอดูข้อมูลได้ที่ฝ่ายบัญชี	เปิดเผยต่อธนาคารตามข้อตกลง	ไม่มี	ระบบเข้ารหัส SSL และการเก็บข้อมูลในเซิร์ฟเวอร์ปลอดภัย

6.2.2 มีการทบทวนบันทึกการอย่างสม่ำเสมอว่าเป็นไปตามหลักการเก็บรวบรวมเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายขององค์กร (Data Minimization)

สิ่งที่ต้องทำ: มีการทบทวนบันทึกการอย่างสม่ำเสมอและเป็นไปตามหลักการ Data Minimization

หลักฐาน: หลักฐานการจัดทำบันทึกการตามหลักการ Data Minimization เช่น แนวปฏิบัติขององค์กร

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22
โทษทางปกครอง ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 39 วรรคหนึ่ง กำหนดโทษปรับทางปกครอง
ไม่เกิน 3 ล้านบาท

รายงานทบทวนบันทึกการข้อมูลส่วนบุคคล ตามหลัก Data Minimization

ชื่อองค์กร: บริษัท ABC จำกัด

หัวข้อ: รายงานทบทวนบันทึกการข้อมูลส่วนบุคคล

วันที่ทบทวน: 30 พฤษภาคม 2568

ผู้รับผิดชอบ: ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO)

รอบเวลาการทบทวน: ทุก 6 เดือน

1. วัตถุประสงค์ของการทบทวน

- เพื่อให้มั่นใจว่าการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นไปตามหลัก Data Minimization คือ
- เก็บเฉพาะข้อมูลที่จำเป็นเท่านั้น
- เก็บเพื่อวัตถุประสงค์ที่ชัดเจนและถูกต้องตามกฎหมาย
- ไม่เก็บข้อมูลที่เกินความจำเป็น

2. ขอบเขตการทบทวน

- ตรวจสอบรายการข้อมูลส่วนบุคคลที่จัดเก็บในบันทึก
- วิเคราะห์ความสอดคล้องของข้อมูลที่เก็บกับวัตถุประสงค์ที่ระบุ
- ตรวจสอบข้อมูลที่อาจเกินความจำเป็นหรือไม่ได้ใช้ประโยชน์
- ประเมินมาตรการปรับปรุงหรือลบข้อมูลที่ไม่จำเป็น

3. ผลการทบทวน

ลำดับ	ประเภทข้อมูลส่วนบุคคล	วัตถุประสงค์	ความจำเป็นในการเก็บข้อมูล	ข้อเสนอแนะ / การดำเนินการ
1	ชื่อ-นามสกุล เบอร์โทรศัพท์	ติดต่อและจัดส่งสินค้า	จำเป็น	คงไว้
2	ข้อมูลบัตรเครดิต	ชำระเงิน	จำเป็น	คงไว้
3	ข้อมูลที่อยู่อีเมลที่ไม่ได้ใช้งานนานเกิน 1 ปี	การติดต่อ	ไม่จำเป็น	เสนอให้ลบข้อมูลที่ไม่ได้ใช้งาน
4	ข้อมูลสถิติการเข้าชมเว็บไซต์แบบละเอียด	วิเคราะห์พฤติกรรม	เกินความจำเป็น	เสนอปรับลดรายละเอียดข้อมูลให้เหมาะสม

4. แนวปฏิบัติองค์กรในการทบทวนบันทึกข้อมูลส่วนบุคคล

- ทบทวนและอัปเดตรายการข้อมูลส่วนบุคคลทุก 6 เดือน

- ให้ความรู้และอบรมพนักงานเกี่ยวกับ Data Minimization
- มีขั้นตอนในการลบหรือปรับลดข้อมูลที่ไม่จำเป็นทันทีหลังการทบทวน
- บันทึกผลการทบทวนและนำเสนอผู้บริหารเพื่อติดตามผลอย่างต่อเนื่อง

6.2.3 มีการทบทวนบันทึกการอย่างสม่ำเสมอให้มีความสอดคล้องกับนโยบายและแนวปฏิบัติขององค์กร เพื่อให้มั่นใจว่าบันทึกการมีความถูกต้องและเป็นปัจจุบัน รวมถึงมีการมอบหมายอย่างชัดเจนว่าบุคคลใดเป็นผู้รับผิดชอบทำหน้าที่ทบทวนบันทึกการดังกล่าว

สิ่งที่ต้องทำ: มีการทบทวนบันทึกการ และมอบหมายบุคคลที่มีหน้าที่รับผิดชอบให้ชัดเจน

หลักฐาน: แผนการทบทวนบันทึกการขององค์กร

หลักฐานการแต่งตั้งผู้รับผิดชอบในการจัดทำบันทึกการขององค์กรและในแต่ละแผนก

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การทบทวนบันทึกการและการมอบหมายผู้รับผิดชอบอย่างชัดเจน

1. แผนการทบทวนบันทึกการข้อมูลส่วนบุคคล

รอบการ ทบทวน	กิจกรรม	ผู้รับผิดชอบ	ช่องทางการ รายงาน	หมายเหตุ
ทุก 6 เดือน	ทบทวนความถูกต้องและ ความสอดคล้องของบันทึก การกับนโยบายองค์กร และแนวปฏิบัติ	ฝ่ายคุ้มครอง ข้อมูลส่วนบุคคล (DPO)	รายงานต่อ ผู้บริหารสูงสุด	ปรับปรุงและ แก้ไขรายการตาม ความเหมาะสม
รายไตร มาส	ตรวจสอบและติดตามการ ปฏิบัติตามข้อกำหนดของแต่ละ แผนก	หัวหน้าแต่ละ แผนก	รายงานต่อฝ่าย คุ้มครองข้อมูล ส่วนบุคคล	แจ้งแก้ไขหากพบ ข้อมูลไม่ถูกต้อง

2. ตัวอย่างหนังสือแต่งตั้งผู้รับผิดชอบ

บริษัท ABC จำกัด

หนังสือแต่งตั้งผู้รับผิดชอบการจัดทำและทบทวนบันทึกการข้อมูลส่วนบุคคล

ตามที่บริษัทฯ ได้กำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลและมาตรการบริหารจัดการข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามกฎหมายและแนวปฏิบัติที่ดี ทางบริษัทฯ จึงแต่งตั้งบุคคลดังต่อไปนี้ให้เป็นผู้รับผิดชอบดำเนินการจัดทำและทบทวนบันทึกการข้อมูลส่วนบุคคลในหน่วยงานของตน

นายสมชาย ใจดี

ตำแหน่ง: ผู้จัดการฝ่ายทรัพยากรบุคคล

หน้าที่: รับผิดชอบบันทึกการข้อมูลส่วนบุคคลของพนักงาน และทบทวนความถูกต้องของข้อมูล

นางสาวสายรุ้ง แสงจันทร์

ตำแหน่ง: ผู้จัดการฝ่ายลูกค้าสัมพันธ์

หน้าที่: รับผิดชอบบันทึกการข้อมูลลูกค้า และทบทวนข้อมูลให้เป็นปัจจุบัน

นายวัฒนา แก้วใส

ตำแหน่ง: เจ้าหน้าที่ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO)

หน้าที่: ดูแลการจัดทำและทบทวนบันทึกการโดยรวมของบริษัทฯ และรายงานต่อผู้บริหาร

ให้มีผลตั้งแต่วันที่ 1 มิถุนายน 2568 เป็นต้นไป

ลงชื่อ

(กรรมการผู้จัดการ)

วันที่

6.3.1 บันทึกการมีรายการอย่างน้อยตามที่กำหนดไว้ในมาตรา 39 ดังต่อไปนี้

- (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- (3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- (5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิ์เข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- (6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม
- (7) การปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด (หากมี)
- (8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

สิ่งที่ต้องทำ: จัดทำบันทึกการมีรายการที่บันทึกครบถ้วนตามรายการขั้นต่ำที่กฎหมายกำหนด

หลักฐาน: บันทึกการมีรายการขององค์กร

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39

โทษปรับทางปกครอง มาตรา 82 ในกรณีที่ไม่ปฏิบัติตามมาตรา 39 วรรคหนึ่ง กำหนดโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

บันทึกการมีรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) ในรูปแบบอิเล็กทรอนิกส์

ลำดับ	ข้อมูลส่วนบุคคลที่เก็บรวบรวม	วัตถุประสงค์ของการเก็บรวบรวม	ผู้ควบคุมข้อมูล	ระยะเวลาการเก็บรักษา	สิทธิและวิธีการเข้าถึง	การใช้หรือเปิดเผยข้อมูล (มาตรา 27 วรรค 3)	การปฏิเสธคำขอ / คัดค้าน	มาตรการรักษาความมั่นคงปลอดภัย
1	ชื่อ-นามสกุล, เบอร์โทรศัพท์, ที่อยู่	เพื่อการติดต่อ และจัดส่งสินค้า	ฝ่ายลูกค้าสัมพันธ์	5 ปี หลังเลิกใช้บริการ	เจ้าของข้อมูลมีสิทธิขอแก้ไขหรือลบข้อมูลผ่านทางอีเมล	ไม่มีการเปิดเผยข้อมูลแก่บุคคลภายนอก	ไม่มี	การเข้ารหัสข้อมูล, จำกัดสิทธิ์เข้าถึงข้อมูล
2	ข้อมูลบัตรเครดิต	เพื่อชำระเงินและยืนยันตัวตน	ฝ่ายบัญชี	2 ปี ตามนโยบายการเงิน	เจ้าของข้อมูลสามารถขอข้อมูลได้ที่ฝ่ายบัญชี	เปิดเผยต่อธนาคารตามข้อตกลง	ไม่มี	ระบบเข้ารหัส SSL และการเก็บข้อมูลในเซิร์ฟเวอร์ปลอดภัย
3	ประวัติการเข้าใช้งานระบบ	เพื่อวิเคราะห์และปรับปรุงบริการ	ฝ่ายไอที	1 ปี หลังบันทึกข้อมูล	เจ้าของข้อมูลสามารถขอและลบข้อมูลได้ตามคำขอ	ไม่มีการเปิดเผยข้อมูล	มีการปฏิเสธคำขอบางรายการ	การจำกัดการเข้าถึงข้อมูลโดยพนักงานที่ได้รับอนุญาต

6.3.2 กรณีที่องค์กรมีผู้ประมวลผลข้อมูลส่วนบุคคล องค์กรต้องกำกับให้ผู้ประมวลผลข้อมูลส่วนบุคคลนั้น จัดทำบันทึกการรายการในส่วนที่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งให้แก่องค์กร ทั้งนี้ บันทึกการรายการดังกล่าวต้องมีรายการที่บันทึกอย่างน้อยตามที่กฎหมายกำหนด

สิ่งที่ต้องทำ: มีเอกสารหรือหลักฐานแสดงถึงการกำกับให้ผู้ประมวลผลข้อมูลส่วนบุคคลของตนจัดทำบันทึกการรายการตามที่กฎหมายกำหนด

หลักฐาน: บันทึกการรายการของผู้ประมวลผลข้อมูลส่วนบุคคล
เอกสารหรือหลักฐานที่แสดงถึงการที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำบันทึกการรายการ

สภาพบังคับ: คู่มือหรือข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 (3)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกการรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565
โทษปรับทางปกครอง มาตรา 86 ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 40 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

บันทึกการของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor Records of Processing Activities - ROPA)

ลำดับ	ข้อมูลส่วนบุคคลที่ประมวลผล	วัตถุประสงค์ของการประมวลผล	ผู้ควบคุมข้อมูลที่ให้คำสั่ง	ระยะเวลาการเก็บรักษาข้อมูล	สิทธิและวิธีการเข้าถึงข้อมูล	การใช้หรือเปิดเผยข้อมูลตามคำสั่งของผู้ควบคุมข้อมูล	มาตรการรักษาความมั่นคงปลอดภัย
1	ชื่อ-นามสกุล, ข้อมูลการชำระเงิน	จัดการการชำระเงินตามคำสั่งของลูกค้า	บริษัท ABC จำกัด (ผู้ควบคุมข้อมูล)	3 ปี หลังสิ้นสุดการให้บริการ	การเข้าถึงข้อมูลได้โดยผู้ควบคุมข้อมูลและเจ้าหน้าที่ที่ได้รับอนุญาต	ไม่มีการเปิดเผยข้อมูลแก่บุคคลภายนอก	ระบบเข้ารหัสข้อมูล SSL และการตรวจสอบสิทธิ์เข้าใช้งาน
2	ที่อยู่จัดส่ง, เบอร์โทรศัพท์	จัดส่งสินค้าและบริการตามคำสั่ง	บริษัท ABC จำกัด (ผู้ควบคุมข้อมูล)	5 ปี ตามระยะเวลาการเก็บรักษาของผู้ควบคุมข้อมูล	เจ้าของข้อมูลสามารถติดต่อผู้ควบคุมข้อมูลเพื่อแก้ไขข้อมูล	ไม่มีการเปิดเผยข้อมูล	จำกัดสิทธิ์เข้าถึงข้อมูลตามบทบาท

2. เอกสารกำกับและสั่งการให้ผู้ประมวลผลข้อมูลจัดทำบันทึกการ

หนังสือแจ้งกำกับการจัดทำบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

บริษัท ABC จำกัด

วันที่: 1 มิถุนายน 2568

เรื่อง: การกำกับให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำบันทึกการตามกฎหมาย PDPA

เรียน: ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ตามที่บริษัท ABC จำกัด เป็นผู้ควบคุมข้อมูลส่วนบุคคล และได้ว่าจ้างท่านเป็นผู้ประมวลผลข้อมูลส่วนบุคคล บริษัทฯ ขอแจ้งให้ท่านจัดทำบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่ท่านดำเนินการตามคำสั่งของบริษัทฯ โดยบันทึกการดังกล่าวต้องมีรายการที่บันทึกอย่างน้อยตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 กำหนด

ทั้งนี้ บริษัทฯ ขอให้ท่านส่งมอบบันทึกการดังกล่าวแก่บริษัทฯ อย่างสม่ำเสมอ เพื่อเป็นหลักฐานในการปฏิบัติตามกฎหมายและเพื่อการตรวจสอบขอขอบคุณในการให้ความร่วมมือ

ลงชื่อ.....

(ผู้มีอำนาจลงนาม)

ตำแหน่ง: ผู้จัดการฝ่ายกฎหมายและคุ้มครองข้อมูลส่วนบุคคล

6.4.1 บันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลมีการเชื่อมโยงไปยังเอกสารหรือข้อมูลต่าง ๆ ที่เกี่ยวข้องกับกิจกรรมนั้น เช่น

- (1) บันทึกความยินยอม
- (2) ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
- (3) ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล
- (4) สถานที่เก็บทางอิเล็กทรอนิกส์ และ/หรือทางกายภาพของข้อมูลส่วนบุคคล
- (5) รายงานการจัดทำผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA Report)
- (6) การบันทึกเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- (7) นโยบายหรือแนวปฏิบัติเกี่ยวกับระยะเวลาการจัดเก็บข้อมูลและการลบหรือทำลายข้อมูล

สิ่งที่ต้องทำ: บันทึกการมีการเชื่อมโยงไปยังกิจกรรมหรือเอกสารที่เกี่ยวข้องอย่างครบถ้วน

หลักฐาน: บันทึกการที่แสดงการเชื่อมโยงไปยังกิจกรรมหรือ เอกสารอื่นที่เกี่ยวข้อง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

บันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล พร้อมการเชื่อมโยงเอกสารที่เกี่ยวข้อง

ลำดับ	กิจกรรมการประมวลผลข้อมูลส่วนบุคคล	เอกสารที่เชื่อมโยง	สถานที่เก็บเอกสาร (อิเล็กทรอนิกส์ / กายภาพ)	หมายเหตุ
1	การเก็บรวบรวมข้อมูลลูกค้าเพื่อวัตถุประสงค์ติดต่อและจัดส่งสินค้า	- บันทึกความยินยอมลูกค้า (Consent Form)	Google Drive / ตู้เอกสารฝ่ายลูกค้าสัมพันธ์	บันทึกความยินยอมเก็บไว้อย่างชัดเจน
2	การประมวลผลข้อมูลบัตรเครดิตเพื่อชำระเงิน	- ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) - รายงาน DPI	ระบบจัดเก็บเอกสารภายใน (Intranet) / ตู้เอกสารฝ่ายบัญชี	รายงาน DPIA ผ่านการอนุมัติแล้ว
3	การแบ่งปันข้อมูลกับพันธมิตรธุรกิจ	- ข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement)	ระบบบริหารจัดการสัญญา (Contract Management System)	สัญญามีการต่ออายุและตรวจสอบทุกปี
4	การจัดเก็บข้อมูลลูกค้า	- นโยบายการเก็บรักษาข้อมูลและการลบข้อมูล	SharePoint / ตู้เอกสารฝ่าย IT	นโยบายสอดคล้องกับ PDPA และ GDPR
5	การตรวจสอบเหตุการณ์ละเมิดข้อมูล	- บันทึกเหตุการณ์ละเมิดข้อมูล (Data Break Log)	ระบบแจ้งเตือนความปลอดภัย (Security Incident System)	รายงานถูกส่งให้คณะกรรมการ PDPA แล้ว

คำอธิบายเพิ่มเติม

- **บันทึกความยินยอมลูกค้า (Consent Form):** เอกสารยินยอมที่ลูกค้าเซ็นรับทราบการเก็บและใช้ข้อมูลส่วนบุคคล
- **ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement):** สัญญาที่ระบุหน้าที่และความรับผิดชอบของผู้ประมวลผลข้อมูล
- **ข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement):** เอกสารที่ระบุเงื่อนไขการแบ่งปันข้อมูลกับบุคคลภายนอก
- **รายงาน DPIA (Data Protection Impact Assessment):** รายงานประเมินผลกระทบด้านการคุ้มครองข้อมูล เพื่อประเมินความเสี่ยงและมาตรการรักษาความปลอดภัย

- บันทึกเหตุการณ์ละเมิดข้อมูล (Data Breach Log): รายงานเหตุการณ์ที่มีการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น พร้อมมาตรการแก้ไข
- นโยบายการเก็บรักษาข้อมูลและการลบข้อมูล: เอกสารกำหนดระยะเวลาการเก็บรักษาข้อมูล และวิธีการลบหรือทำลายข้อมูลอย่างปลอดภัย

6.5.1 องค์การกำหนดฐานทางกฎหมาย (Lawful Basis) ที่เหมาะสมและสอดคล้องกับวัตถุประสงค์ สิ่งที่ต้องทำ: มีการดำเนินการครบถ้วน

หลักฐาน: นโยบายหรือแนวปฏิบัติขององค์กรที่เกี่ยวข้องกับการ พิจารณาฐานทางกฎหมาย

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 และ 26

โทษปรับทางปกครอง มาตรา 83 ในกรณี ที่ไม่ปฏิบัติตามมาตรา 24 กำหนดโทษปรับ ทางปกครองไม่เกิน 3 ล้านบาท

โทษปรับทางปกครอง มาตรา 84 ในกรณี ที่ไม่ปฏิบัติตามมาตรา 26 กำหนดโทษปรับ ทางปกครองไม่เกิน 5 ล้านบาท

นโยบายและแนวปฏิบัติการกำหนดฐานทางกฎหมาย (Lawful Basis) ในการประมวลผลข้อมูลส่วนบุคคล

บทนำ

องค์กรตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งกำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการตามฐานทางกฎหมายที่เหมาะสมและถูกต้องตามมาตรา 24 และมาตรา 26 เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล รวมถึงลดความเสี่ยงด้านกฎหมายที่อาจเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล เพื่อให้การประมวลผลข้อมูลส่วนบุคคลขององค์กรเป็นไปตามกฎหมายและมีความโปร่งใส องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติฉบับนี้ขึ้นเพื่อกำหนดหลักเกณฑ์ วิธีการ และความรับผิดชอบในการกำหนดฐานทางกฎหมายที่เหมาะสมในการประมวลผลข้อมูลส่วนบุคคลทุกประเภท

วัตถุประสงค์

- เพื่อกำหนดหลักเกณฑ์และแนวทางในการเลือกฐานทางกฎหมายที่เหมาะสมสำหรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลในองค์กร
- เพื่อส่งเสริมให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้อง โปร่งใส และสอดคล้องกับ PDPA
- เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล และรักษาความน่าเชื่อถือขององค์กร

- เพื่อสร้างมาตรฐานในการจัดทำเอกสารหลักฐานและบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) ที่ชัดเจน

ขอบเขต

นโยบายนี้ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลทุกประเภท ไม่ว่าจะเป็นข้อมูลทั่วไปหรือข้อมูลส่วนบุคคลพิเศษ (Special Category Data) โดยใช้หลักการกำหนดฐานทางกฎหมายตามมาตรา 24 และ 26 ของ PDPA โดยมีผลบังคับใช้กับ

- ผู้ควบคุมข้อมูล (Data Controller) ทุกหน่วยงานและฝ่ายที่เกี่ยวข้อง
- ผู้ประมวลผลข้อมูล (Data Processor) ที่ได้รับมอบหมายจากองค์กร
- พนักงานหรือบุคลากรที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลทุกระดับ

คำจำกัดความ

- **ข้อมูลส่วนบุคคล (Personal Data)** หมายถึง ข้อมูลใด ๆ ที่สามารถระบุตัวบุคคลได้
- **ฐานทางกฎหมาย (Lawful Basis)** หมายถึง เหตุผลทางกฎหมายที่ถูกต้องตาม PDPA ในการประมวลผลข้อมูลส่วนบุคคล
- **เจ้าของข้อมูล (Data Subject)** หมายถึง บุคคลที่ข้อมูลส่วนบุคคลของเขาถูกประมวลผล
- **ผู้ควบคุมข้อมูล (Data Controller)** หมายถึง บุคคลหรือนิติบุคคลที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูล
- **ผู้ประมวลผลข้อมูล (Data Processor)** หมายถึง บุคคลหรือนิติบุคคลที่ทำหน้าที่ประมวลผลข้อมูลในนามของผู้ควบคุมข้อมูล

กฎหมายที่เกี่ยวข้อง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

- มาตรา 24 และ 26 ของ PDPA ที่ระบุฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล
- มาตรา 83 และ 84 ที่กำหนดโทษปรับทางปกครองในกรณีไม่ปฏิบัติตามฐานทางกฎหมาย

หลักเกณฑ์การกำหนดฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล เพื่อให้การประมวลผลข้อมูลเป็นไปอย่างถูกต้องตามกฎหมายและมีความชัดเจน องค์กรกำหนดหลักเกณฑ์และแนวทางในการเลือกฐานทางกฎหมายไว้ดังนี้

1. ฐานความยินยอม (Consent)

การประมวลผลข้อมูลต้องได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูล ความยินยอมต้องเป็นไปโดยสมัครใจ มีข้อมูลครบถ้วน และเข้าใจได้ง่าย เจ้าของข้อมูลมีสิทธิถอนความยินยอมได้ทุกเมื่อ โดยไม่ส่งผลกระทบต่อความถูกต้องตามกฎหมายของการประมวลผลก่อนถอน การขอความยินยอมต้องจัดเก็บ

เป็นหลักฐานและสามารถตรวจสอบได้ เหมาะสำหรับกิจกรรมที่ไม่มีฐานทางกฎหมายรองรับ หรือใช้ในกรณีที่เป็นข้อมูลส่วนบุคคลพิเศษ

2. ฐานสัญญา (Contractual Necessity)

การประมวลผลข้อมูลเป็นไปเพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญา ข้อมูลที่ประมวลผลต้องเกี่ยวข้องและจำเป็นต่อการทำสัญญานั้น เช่น การจัดส่งสินค้า ชำระเงิน ไม่สามารถใช้ฐานนี้ได้ในกรณีที่ไม่มีสัญญาหรือหน้าที่ตามกฎหมายรองรับ

3. ฐานหน้าที่ตามกฎหมาย (Legal Obligation)

การประมวลผลข้อมูลจำเป็นเพื่อให้ผู้ควบคุมข้อมูลปฏิบัติตามหน้าที่ตามกฎหมายหรือข้อบังคับของรัฐ

เช่น การรายงานข้อมูลต่อหน่วยงานรัฐ การเก็บข้อมูลตามกฎหมายภาษีหรือแรงงาน ต้องระบุชัดเจนว่าเป็นการปฏิบัติตามกฎหมายฉบับใด

4. ฐานความสนใจที่ชอบด้วยกฎหมาย (Legitimate Interests)

- การประมวลผลเพื่อผลประโยชน์ที่ชอบด้วยกฎหมายขององค์กรหรือบุคคลที่สาม โดยไม่ละเมิดสิทธิของเจ้าของข้อมูล
- ต้องมีการประเมินผลกระทบต่อเจ้าของข้อมูลและทำสมดุลระหว่างผลประโยชน์ขององค์กรกับสิทธิของเจ้าของข้อมูล
- เหมาะสำหรับกิจกรรมที่องค์กรมีความจำเป็นต้องดำเนินการ เช่น การบริหารจัดการลูกค้า การวิเคราะห์ข้อมูลเพื่อปรับปรุงบริการ

5. ฐานป้องกันชีวิต (Vital Interests)

การประมวลผลจำเป็นเพื่อปกป้องชีวิตหรือความปลอดภัยของเจ้าของข้อมูลหรือบุคคลอื่น มักใช้ในกรณีฉุกเฉิน เช่น การรักษาพยาบาล

6. ฐานเพื่อประโยชน์สาธารณะ (Public Interest)

การประมวลผลที่จำเป็นเพื่อการปฏิบัติหน้าที่ของหน่วยงานรัฐหรือเพื่อประโยชน์สาธารณะ ต้องเป็นไปตามข้อกำหนดของกฎหมายหรือระเบียบที่เกี่ยวข้อง

7. ฐานสำหรับข้อมูลส่วนบุคคลพิเศษ (Special Category Data)

การประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษ เช่น ข้อมูลสุขภาพ เชื้อชาติ ศาสนา ต้องมีฐานทางกฎหมายเฉพาะตามมาตรา 26

- ต้องมีมาตรการคุ้มครองและความปลอดภัยสูงกว่า
- ต้องระบุฐานและเหตุผลที่ชัดเจน พร้อมบันทึกในเอกสารประกอบ

แนวทางปฏิบัติในการกำหนดฐานทางกฎหมาย

- **การวิเคราะห์กิจกรรมการประมวลผลข้อมูล**

ก่อนดำเนินการประมวลผล ต้องวิเคราะห์วัตถุประสงค์และลักษณะข้อมูล เพื่อเลือกฐานทางกฎหมายที่เหมาะสมและสอดคล้องกับข้อมูลกฎหมาย

- **การจัดทำเอกสารและบันทึกฐานทางกฎหมาย**

ทุกกิจกรรมการประมวลผลต้องบันทึกฐานทางกฎหมายที่ใช้ในบันทึกการกิจกรรมการประมวลผลข้อมูล (ROPA) รวมถึงเอกสารประกอบ เช่น แบบฟอร์มขอความยินยอม ข้อตกลงทางสัญญา รายงานผลประเมินความเสี่ยง

- **การสื่อสารกับเจ้าของข้อมูล**

แจ้งให้เจ้าของข้อมูลทราบฐานทางกฎหมายและวัตถุประสงค์ของการประมวลผลข้อมูลผ่านนโยบายความเป็นส่วนตัวหรือประกาศแจ้งข้อมูลส่วนบุคคล

- **การทบทวนฐานทางกฎหมายอย่างสม่ำเสมอ**

ทบทวนและปรับปรุงฐานทางกฎหมายในเอกสารและบันทึกอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีกฎหมายหรือเงื่อนไขใหม่เข้ามา

- **การอบรมและสร้างความตระหนักรู้**

ฝึกอบรมพนักงานและผู้เกี่ยวข้องให้เข้าใจและปฏิบัติตามนโยบายและแนวทางนี้อย่างเคร่งครัด

ความรับผิดชอบ

- ฝ่ายบริหาร รับผิดชอบอนุมัติและสนับสนุนนโยบายนี้ รวมถึงจัดสรรทรัพยากรที่เหมาะสม

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) รับผิดชอบให้คำปรึกษา แนะนำ และตรวจสอบการปฏิบัติตามนโยบาย

- ผู้ควบคุมข้อมูล ตรวจสอบให้

- แนใจว่ากิจกรรมการประมวลผลข้อมูลในหน่วยงานอยู่ภายใต้นโยบายนี้

- พนักงานและบุคลากร ปฏิบัติตามนโยบายและแจ้งข้อมูลหรือปัญหาที่เกี่ยวข้องกับการประมวลผลข้อมูลทันที

ตัวอย่างกรณีศึกษาและการประยุกต์ใช้ฐานทางกฎหมาย

- **กรณีที่ 1: การเก็บข้อมูลลูกค้าสำหรับการจัดส่งสินค้า**

ฐานทางกฎหมาย: สัญญา (Contractual Necessity)

เหตุผล: ข้อมูลชื่อ ที่อยู่ และเบอร์โทรศัพท์ใช้เพื่อจัดส่งสินค้าให้ลูกค้า

การปฏิบัติ: ระบุฐานนี้ในนโยบายความเป็นส่วนตัวและบันทึกใน ROPA

- **กรณีที่ 2: การทำแบบสำรวจความคิดเห็นเพื่อปรับปรุงบริการ**

ฐานทางกฎหมาย: ความยินยอม (Consent)

เหตุผล: การทำแบบสำรวจต้องได้รับความยินยอมชัดแจ้งจากเจ้าของข้อมูล

การปฏิบัติ: จัดทำแบบฟอร์มขอความยินยอมและบันทึกเอกสารไว้

– **กรณีที่ 3: การรายงานข้อมูลลูกจ้างต่อหน่วยงานภาครัฐ**

ฐานทางกฎหมาย: หน้าที่ตามกฎหมาย (Legal Obligation)

เหตุผล: กฎหมายกำหนดให้รายงานข้อมูลเพื่อจ่ายภาษีและประกันสังคม

การปฏิบัติ: ระบุฐานในเอกสารและแจ้งให้พนักงานทราบ

บทสรุป

การกำหนดฐานทางกฎหมายที่เหมาะสมเป็นหัวใจสำคัญของการปฏิบัติตาม PDPA เพื่อสร้างความมั่นใจว่าองค์กรจะดำเนินการประมวลผลข้อมูลส่วนบุคคลอย่างถูกต้อง โปร่งใส และเคารพสิทธิของเจ้าของข้อมูล นโยบายและแนวปฏิบัตินี้จะช่วยให้องค์กรสามารถป้องกันความเสี่ยงและรับมือกับข้อร้องเรียนหรือการตรวจสอบจากหน่วยงานกำกับดูแลได้อย่างมีประสิทธิภาพ องค์กรจึงขอให้ทุกหน่วยงานและบุคลากรที่เกี่ยวข้องนำแนวทางนี้ไปปฏิบัติอย่างเคร่งครัด และพร้อมรับฟังข้อเสนอแนะเพื่อพัฒนานโยบายให้สอดคล้องกับกฎหมายและบริบทที่เปลี่ยนแปลงอย่างต่อเนื่อง

6.5.2 หากองค์กรมีการประมวลผลข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 (Sensitive Data) องค์กรได้กำหนดฐานทางกฎหมายตามที่กำหนดไว้ในมาตรา 26 อย่างสอดคล้องและเหมาะสม และบันทึกฐานทางกฎหมายดังกล่าวในบันทึกการรายการ

สิ่งที่ต้องทำ: มีการดำเนินการครบถ้วน

หลักฐาน: บันทึกการรายการเหตุผลการเลือกฐานทางกฎหมายตามมาตรา 26

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26

โทษปรับทางปกครอง มาตรา 84 ในกรณีที่ไม่ปฏิบัติตามมาตรา 26 กำหนดโทษปรับ ทางปกครองไม่เกิน 5 ล้านบาท

การประมวลผลข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26

ข้อกำหนด

หากองค์กรมีการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) ตามที่ระบุไว้ใน **มาตรา 26** ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) องค์กรต้องดำเนินการดังนี้

- กำหนดฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลอ่อนไหวอย่างสอดคล้องและเหมาะสมตามที่กฎหมายกำหนด
- บันทึกฐานทางกฎหมายดังกล่าวไว้ในบันทึกการรายการ (Record of Processing Activities - ROPA)

สิ่งที่ต้องปฏิบัติ

- ดำเนินการกำหนดฐานทางกฎหมายสำหรับการประมวลผลข้อมูลส่วนบุคคลอ่อนไหวตามข้อกำหนดของมาตรา 26 ให้ครบถ้วน

- บันทึกเหตุการณ์เลือกฐานทางกฎหมายไว้ในบันทึกการไต่สวน เพื่อเป็นหลักฐานแสดงความโปร่งใสและการปฏิบัติตามกฎหมาย

หลักฐานประกอบการตรวจสอบ

บันทึกการไต่สวนเหตุการณ์เลือกฐานทางกฎหมายตามมาตรา 26 อย่างครบถ้วนและสมบูรณ์

สภาพบังคับและบทลงโทษ

- การปฏิบัติที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอ่อนไหวต้องเป็นไปตาม **มาตรา 26** ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- หากไม่ปฏิบัติตามมาตราดังกล่าว องค์กรอาจถูกลงโทษปรับทางปกครองตาม **มาตรา 84** โดยมีโทษปรับสูงสุดไม่เกิน 5,000,000 บาท

6.5.3 ในกรณีที่เป็นการประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรม องค์กรได้พิจารณาความจำเป็นและกำหนดมาตรการต่าง ๆ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องแล้ว

สิ่งที่ต้องทำ: มีการดำเนินการครบถ้วน

หลักฐาน: นโยบายหรือแนวปฏิบัติขององค์กรที่เกี่ยวกับการเก็บ รวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรคสาม
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมที่มีได้กระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566
โทษทางปกครอง มาตรา 84 ในกรณีที่ไม่ปฏิบัติตามมาตรา 26 กำหนดโทษปรับทางปกครองไม่เกิน 5 ล้านบาท

เรื่อง: นโยบายและแนวปฏิบัติในการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม

1. หลักการทั่วไป

องค์กรมีความตระหนักถึงความละเอียดอ่อนและความเสี่ยงของข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม จึงได้กำหนดนโยบายและมาตรการที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรคสาม และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566 ว่าด้วยหลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองข้อมูลดังกล่าว

2. ขอบเขตของข้อมูลเกี่ยวกับประวัติอาชญากรรม

ข้อมูลที่เกี่ยวข้อง ได้แก่:

- ประวัติการถูกดำเนินคดีอาญา
- คำพิพากษาของศาล
- รายงานจากสำนักงานตำรวจแห่งชาติหรือหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย

3. วัตถุประสงค์ในการประมวลผล

องค์กรดำเนินการเก็บรวบรวมและประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรมโดยมีวัตถุประสงค์ที่ชัดเจนและจำกัด เช่น:

- เพื่อคัดเลือกบุคลากรในตำแหน่งที่มีความเสี่ยงสูง (เช่น งานเกี่ยวข้องกับเด็ก ผู้สูงอายุ หรือ ทรัพย์สิน)
- เพื่อประเมินความเสี่ยงในงานรักษาความปลอดภัย
- เพื่อปฏิบัติตามกฎหมายหรือข้อบังคับเฉพาะด้าน

4. ฐานทางกฎหมาย

การประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรมกระทำภายใต้เงื่อนไขต่อไปนี้:
ได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูล และ/หรือเป็นการจำเป็นตามกฎหมายที่เกี่ยวข้องกับหน้าที่ขององค์กรในด้านแรงงาน ความมั่นคง หรือการรักษาความปลอดภัย

5. การประเมินความจำเป็นและสัดส่วน (Necessity & Proportionality)

- ก่อนดำเนินการเก็บข้อมูล องค์กรจะประเมิน:
- ความจำเป็นของการใช้ข้อมูล
- ผลกระทบต่อเจ้าของข้อมูล
- ทางเลือกที่นุ่มนวลหรือไม่รุกล้ำสิทธิมากเกินไป

6. มาตรการคุ้มครองข้อมูล

องค์กรได้กำหนดมาตรการเฉพาะสำหรับการจัดเก็บและประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรม ดังนี้:

(1) การจำกัดการเข้าถึง

ข้อมูลจะถูกเข้ารหัส (encryption) และจัดเก็บในระบบที่มีสิทธิ์การเข้าถึงเฉพาะบุคคลตามตำแหน่งหน้าที่

(2) การเก็บรักษา

- ข้อมูลจะถูกจัดเก็บแยกต่างหากจากข้อมูลทั่วไป
- มีระยะเวลาเก็บข้อมูลชัดเจนตามวัตถุประสงค์ และจะถูกลบทิ้งเมื่อสิ้นสุดความจำเป็น

(3) การบันทึกการเข้าถึงและการใช้ข้อมูล

- มีระบบบันทึก log ทุกครั้งที่มีการเข้าถึงหรือใช้ข้อมูล
- ผู้ดูแลระบบและผู้ควบคุมข้อมูลต้องผ่านการอบรมด้านจริยธรรมและความปลอดภัย

(4) การตรวจสอบภายใน

- มีแผนตรวจสอบและทบทวนนโยบายนี้ทุก 12 เดือน
- การละเมิดหรือการใช้ข้อมูลโดยมิชอบจะถูกดำเนินการทางวินัยทันที

7. การแจ้งเจ้าของข้อมูล

มีการแจ้งรายละเอียดการเก็บข้อมูลอย่างโปร่งใส รวมถึงสิทธิในการคัดค้านการประมวลผลหรือขอลบข้อมูล

8. การจัดทำบันทึกการกิจกรรมการประมวลผล (ROPA)

องค์กรมีการจัดทำ บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล สำหรับข้อมูลประวัติอาชญากรรม โดยระบุ:

- วัตถุประสงค์ของการประมวลผล
- ฐานทางกฎหมายที่ใช้
- หมวดหมู่ของข้อมูล
- ระยะเวลาที่เก็บรักษา
- รายละเอียดของมาตรการรักษาความมั่นคงปลอดภัย
- การเปิดเผยหรือถ่ายโอนข้อมูล

สรุป

องค์กรได้ดำเนินการตามข้อกำหนดของกฎหมายอย่างครบถ้วน โดยมีการกำหนดนโยบาย แนวปฏิบัติ และมาตรการคุ้มครองข้อมูลเกี่ยวกับประวัติอาชญากรรมอย่างเหมาะสม เพื่อป้องกันการละเมิดสิทธิของเจ้าของข้อมูล และสร้างความเชื่อมั่นในการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นระบบ

6.5.4 ในการประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรม หน่วยงานได้พิจารณา

- (1) ความจำเป็นตามกฎหมาย
- (2) มาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม
- (3) ระยะเวลาการจัดเก็บ การลบหรือทำลาย รวมถึงวิธีการตามที่กฎหมายกำหนด
- (4) การบันทึกวันที่ดำเนินการ
- (5) บุคคลที่ได้รับมอบหมายให้ประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรม

สิ่งที่ต้องทำ: มีการดำเนินการครบถ้วน

หลักฐาน: นโยบายหรือแนวปฏิบัติขององค์กรที่เกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 วรรคสาม
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์เกี่ยวกับมาตรการคุ้มครองข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมที่มีได้กระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย พ.ศ. 2566
โทษทางปกครอง มาตรา 84 ในกรณีที่ไม่ปฏิบัติตามมาตรา 26 กำหนดโทษปรับทางปกครองไม่เกิน 5 ล้านบาท

แนวปฏิบัติในการพิจารณาและควบคุมการประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรม

1. ความจำเป็นตามกฎหมาย

องค์กรประเมินและยืนยันว่า การประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรมมีความจำเป็นตามกฎหมายและภารกิจขององค์กร โดยเฉพาะกรณีต่อไปนี้

- เป็นไปตามข้อกำหนดของกฎหมายเฉพาะ (เช่น กฎหมายแรงงาน กฎหมายด้านความปลอดภัย)
- จำเป็นเพื่อประโยชน์สาธารณะ หรือความมั่นคงปลอดภัยขององค์กรและสังคม
- จำเป็นสำหรับการคัดเลือกบุคคลเพื่อปฏิบัติหน้าที่ที่อ่อนไหว เช่น เจ้าหน้าที่รักษาความปลอดภัย, พนักงานดูแลเด็ก, ผู้ดูแลผู้สูงอายุ
- การประมวลผลจะกระทำเฉพาะเมื่อไม่มีวิธีการอื่นที่น้อยกว่าซึ่งสามารถบรรลุวัตถุประสงค์เดียวกันได้

2. มาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม

องค์กรได้กำหนดมาตรการความมั่นคงปลอดภัยทางเทคนิคและองค์กรสำหรับการจัดเก็บและเข้าถึงข้อมูลประวัติอาชญากรรม ดังนี้

- ระบบจัดเก็บแยกเฉพาะ สำหรับข้อมูลที่เกี่ยวข้องกับประวัติอาชญากรรม โดยไม่รวมกับข้อมูลส่วนบุคคลทั่วไป
- การเข้ารหัสข้อมูล (Data Encryption) ทั้งในขณะจัดเก็บและขณะส่งผ่านเครือข่าย
- การจำกัดสิทธิ์การเข้าถึง เฉพาะบุคลากรที่ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น
- การบันทึก log file ทุกครั้งที่มีการเข้าถึง แก้ไข หรือใช้ข้อมูลดังกล่าว
- การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยข้อมูล อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

3. ระยะเวลาการจัดเก็บ การลบหรือทำลาย และวิธีการ

องค์กรกำหนดแนวทางชัดเจนในการจัดเก็บ ลบ หรือทำลายข้อมูล ดังนี้:

ระยะเวลาการจัดเก็บ

- เก็บรักษาไว้เฉพาะระยะเวลาที่จำเป็นต่อวัตถุประสงค์ เช่น ไม่เกิน 1 ปีหลังเสร็จสิ้นกระบวนการคัดเลือกพนักงาน
- กรณีต้องเก็บนานกว่านั้น ต้องมีเหตุผลรองรับและมีการประเมินความจำเป็นอย่างสม่ำเสมอ
- การลบหรือทำลาย:
- ใช้วิธีการทำลายที่ปลอดภัย เช่น การลบแบบปลอดภัย (secure delete) หรือการทำลายเอกสารโดยเครื่องทำลายเอกสารมาตรฐาน
- มีการบันทึกการทำลายข้อมูลทุกครั้ง โดยระบุผู้ดำเนินการ วันที่ และวิธีการ

4. การบันทึกวันที่ดำเนินการ

ทุกกระบวนการที่เกี่ยวข้องกับการประมวลผลข้อมูลประวัติอาชญากรรมจะมีการบันทึกวันที่ดำเนินการไว้อย่างเป็นระบบ เช่น

- วันที่ได้รับข้อมูล
- วันที่มีการใช้ข้อมูลเพื่อประกอบการพิจารณา
- วันที่ลบ/ทำลายข้อมูล
- วันที่มีการประเมินความจำเป็นหรือความเหมาะสมในการเก็บข้อมูล

ข้อมูลเหล่านี้จะถูกบันทึกในระบบจัดการข้อมูลส่วนบุคคล หรือในแบบฟอร์มการควบคุมภายใน (Data Processing Log)

5. บุคคลที่ได้รับมอบหมายให้ประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรม

องค์กรได้กำหนดขั้นตอนและเงื่อนไขการมอบหมายอย่างเคร่งครัด

แต่งตั้ง เจ้าหน้าที่ที่ได้รับมอบหมายโดยเฉพาะ ในการเข้าถึงและประมวลผลข้อมูลประวัติ

อาชญากรรม

ผู้ได้รับมอบหมายต้องผ่านการอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล

มี หนังสือแต่งตั้งเป็นทางการ และมีการตรวจสอบประวัติอาชญากรรมของบุคคลนั้นก่อนการมอบหมาย การเข้าถึงข้อมูลจะต้องกระทำในพื้นที่เฉพาะ หรือผ่านระบบที่มีการบันทึก log การใช้งานเท่านั้น

ภาคผนวกแนบประกอบ (ตัวอย่างเอกสารภายในองค์กร)

- นโยบายการจัดเก็บและใช้ข้อมูลประวัติอาชญากรรม (Criminal Data Handling Policy)
ระบุรายละเอียดเกี่ยวกับกระบวนการ ความจำเป็น มาตรการคุ้มครอง และการควบคุมการเข้าถึง
- แบบฟอร์มบันทึกกิจกรรมการประมวลผลข้อมูล (Criminal Data Processing Log Sheet)
ใช้บันทึกการเข้าถึง การใช้ การลบข้อมูล และบุคคลที่เกี่ยวข้อง
- บันทึกการทำลายข้อมูลประวัติอาชญากรรม (Destruction Record)
ระบุวันที่ทำลาย ผู้ดำเนินการ วิธีการ และเหตุผลประกอบ
- บัญชีรายชื่อผู้มีสิทธิ์เข้าถึงข้อมูล (Access Control List)
อัปเดตเป็นรายไตรมาส และผ่านความเห็นชอบจากผู้ควบคุมข้อมูล (Data Controller)

สรุป

องค์กรได้ดำเนินการตามองค์ประกอบ 5 ประการที่กฎหมายกำหนดไว้อย่างครบถ้วน โดยมี แนวนโยบายและแนวปฏิบัติชัดเจนเพื่อคุ้มครองข้อมูลประวัติอาชญากรรม ไม่ให้ถูกนำไปใช้ในทางที่รุกราน สิทธิหรือผิดวัตถุประสงค์

6.5.5 องค์การกำหนดฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลก่อนเริ่มกิจกรรมการประมวลผล

สิ่งที่ต้องทำ: มีการพิจารณากำหนดฐานทางกฎหมายก่อนการประมวลผลครบถ้วน

หลักฐาน: หลักฐานการพิจารณาและกำหนดฐานทางกฎหมาย

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21, 24, 26

โทษทางปกครอง มาตรา 83 ในกรณีที่ไม่ปฏิบัติตามมาตรา 21, 24 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

โทษทางปกครอง มาตรา 84 ในกรณีที่ไม่ปฏิบัติตามมาตรา 26 กำหนดโทษปรับทางปกครองไม่เกิน 5 ล้านบาท

เอกสารหลักฐานการพิจารณาและกำหนดฐานทางกฎหมาย (Lawful Basis Assessment Record)

หน่วยงาน: _____

กิจกรรมการประมวลผล: _____

วันที่พิจารณา: ____ / ____ / ____

ผู้รับผิดชอบ: _____

1. รายละเอียดกิจกรรมการประมวลผล

ประเภทของข้อมูล

- ข้อมูลส่วนบุคคลทั่วไป
- ข้อมูลส่วนบุคคลอ่อนไหว (ตามมาตรา 26)

วัตถุประสงค์ในการประมวลผล

อธิบายให้ชัดเจน เช่น การจ้างงาน การให้บริการ การดำเนินการตามสัญญา ฯลฯ

ตัวอย่าง: เพื่อประเมินคุณสมบัติของพนักงานก่อนการจ้างงาน

2. การประเมินฐานทางกฎหมาย

2.1 ฐานทางกฎหมายที่เลือกใช้ (ตามมาตรา 24 หรือ 26)

โปรดเลือกอย่างน้อยหนึ่งข้อ

1. ความยินยอมของเจ้าของข้อมูล
2. จำเป็นเพื่อการปฏิบัติตามสัญญา
3. จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายขององค์กร
4. จำเป็นเพื่อการปฏิบัติตามกฎหมาย
5. จำเป็นเพื่อประโยชน์สาธารณะ
6. จำเป็นเพื่อการคุ้มครองชีวิต

2.2 เหตุผลในการเลือกฐานทางกฎหมาย

ตัวอย่าง การเก็บข้อมูลบัตรประชาชนเพื่อยืนยันตัวตนลูกค้าถูกพิจารณาใช้ฐาน "จำเป็นเพื่อการปฏิบัติตามกฎหมาย" เนื่องจากข้อกำหนดของหน่วยงานกำกับดูแล

3. การประมวลผลข้อมูลอ่อนไหว

- ข้อมูลอ่อนไหว

ถ้ามี: โปรดระบุฐานตามมาตรา 26 (เฉพาะกิจกรรมที่เกี่ยวข้อง).....

ตัวอย่าง: ได้รับความยินยอมอย่างชัดแจ้ง / จำเป็นเพื่อการจ้างงาน / มีกฎหมายรองรับ ฯลฯ

4. การทบทวนความเหมาะสม

- การประเมินความสอดคล้องกับวัตถุประสงค์ ☒ ใช่ / ☐ ไม่ใช่
- การพิจารณาผลกระทบต่อเจ้าของข้อมูล ☒ ดำเนินการแล้ว / ☐ ยังไม่ดำเนินการ

- ความสมดุลระหว่างสิทธิของเจ้าของข้อมูลกับผลประโยชน์ขององค์กร ☒ ดำเนินการแล้ว / ☐ ยังไม่ดำเนินการ

5. สรุปและข้อเสนอแนะ

ตัวอย่าง ฐานที่ใช้เหมาะสมกับกิจกรรม และไม่ส่งผลกระทบต่อสิทธิของเจ้าของข้อมูลอย่างไม่เหมาะสม ควรมีการทบทวนทุก 12 เดือน

6. การลงนามรับรอง

ผู้พิจารณา:

(ชื่อ-สกุล) _____

(ตำแหน่ง) _____

(วันที่) ____ / ____ / ____

(ลายเซ็น) _____

ความเห็นของผู้ควบคุมข้อมูล (Data Controller):

☐ อนุมัติ ☐ ขอให้ปรับปรุงเพิ่มเติม ☐ ไม่อนุมัติ

(ลายเซ็น) _____

(วันที่) ____ / ____ / ____

หมายเหตุ:

- เอกสารนี้ควรถูกแนบไว้กับบันทึกการกิจกรรมการประมวลผล (Record of Processing Activities – ROPA)
- เอกสารควรถูกจัดเก็บอย่างปลอดภัย และพร้อมแสดงต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเมื่อมีการตรวจสอบ

6.5.6 องค์กรมีการบันทึกเหตุผลและวิธีการในการกำหนดหรือเลือกฐานทางกฎหมายที่เหมาะสม

สิ่งที่ต้องทำ: มีการบันทึกเหตุผลและวิธีการในการกำหนดหรือเลือกฐานทางกฎหมาย ครบถ้วน

หลักฐาน: บันทึกการเหตุผลการเลือกฐานทางกฎหมายตามมาตรา 24 และ/หรือมาตรา 26

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารบันทึกเหตุผลการเลือกฐานทางกฎหมาย (Legal Basis Justification Record)

ชื่อหน่วยงาน: _____

กิจกรรมการประมวลผล: _____

ผู้รับผิดชอบ: _____

วันที่บันทึก: ____ / ____ / ____

1. ลักษณะของข้อมูลที่เกี่ยวข้อง

โปรดเลือกประเภทข้อมูลที่ใช้ในกิจกรรมนี้

1. ข้อมูลส่วนบุคคลทั่วไป
2. ข้อมูลส่วนบุคคลอ่อนไหว (มาตรา 26)
3. ข้อมูลเกี่ยวกับประวัติอาชญากรรม

2. วัตถุประสงค์ของการประมวลผล

ระบุวัตถุประสงค์ของกิจกรรมการประมวลผล เช่น การให้บริการ, การจ้างงาน, การปฏิบัติตามกฎหมาย ฯลฯ

ตัวอย่าง: เพื่อดำเนินการยืนยันตัวตนลูกค้าก่อนให้บริการตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน

3. ฐานทางกฎหมายที่พิจารณา (มาตรา 24/26)

เลือกฐานทางกฎหมายที่ใช้งาน

- (1) ความยินยอมของเจ้าของข้อมูล
- (2) จำเป็นเพื่อการปฏิบัติตามสัญญา
- (3) จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายขององค์กร
- (4) จำเป็นเพื่อการปฏิบัติตามกฎหมาย
- (5) จำเป็นเพื่อประโยชน์สาธารณะ
- (6) จำเป็นเพื่อการคุ้มครองชีวิต

ถ้ามีข้อมูลอ่อนไหวหรือประวัติอาชญากรรม

- ใช้ความยินยอมอย่างชัดแจ้ง
- มีข้อยกเว้นตามกฎหมายเฉพาะ (เช่น กฎหมายแรงงาน, กฎหมายอาญา ฯลฯ)

4. เหตุผลในการเลือกฐานทางกฎหมาย

โปรดอธิบายเหตุผลว่าทำไมจึงเลือกใช้ฐานนี้

ตัวอย่าง: เนื่องจากมีข้อบังคับจากหน่วยงานกำกับให้ต้องตรวจสอบชื่อผู้รับบริการในรายชื่อบุคคลต้องห้ามฐาน “จำเป็นเพื่อปฏิบัติตามกฎหมาย” จึงมีความเหมาะสม

5. วิธีการประเมินและกำหนดฐาน

โปรตะระบุขั้นตอนหรือการพิจารณา เช่น

- ตรวจสอบความจำเป็นของกิจกรรม
- วิเคราะห์ความเหมาะสมตามมาตรา 24
- ตรวจสอบมีข้อยกเว้นตามมาตรา 26 หรือไม่
- ตรวจสอบมีทางเลือกอื่นที่ละเมิดสิทธิน้อยกว่าหรือไม่

ตัวอย่าง: มีการหารือภายในฝ่ายกฎหมายและฝ่ายนโยบายเพื่อกำหนดฐานทางกฎหมายร่วมกัน โดยพิจารณาจากความจำเป็น ความคุ้มค่า และความสอดคล้องกับข้อมูล

6. ความเห็นเพิ่มเติม (ถ้ามี)

เช่น ข้อเสนอแนะให้ทบทวนทุก 12 เดือน / แนวทางการแจ้งเจ้าของข้อมูล

7. การอนุมัติ

ลงชื่อผู้บันทึก

(ชื่อ-สกุล) _____

(ตำแหน่ง) _____

(วันที่) ____ / ____ / ____

ลงชื่อผู้ควบคุมข้อมูล (Data Controller)

(ชื่อ-สกุล) _____

(ตำแหน่ง) _____

☐ อนุมัติ ☐ ขอปรับปรุงเพิ่มเติม

(วันที่) ____ / ____ / ____

แนบ:

- สำเนาแบบแจ้งเจ้าของข้อมูล (Privacy Notice)
- แบบฟอร์มประเมินผลกระทบ (DPIA) (ถ้ามี)
- แผนการลบข้อมูลตามกำหนดเวลา

6.6 การแจ้งวัตถุประสงค์และฐานทางกฎหมายให้ผู้ที่เกี่ยวข้องรับทราบ : Lawful basis transparency

6.6.1 องค์กรแจ้งฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 24 และมาตรา 26 ในประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Privacy Notice)

สิ่งที่ต้องทำ: มีการดำเนินการครบถ้วน

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคลระบุฐานทางกฎหมาย

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (2)

แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โทษทางปกครอง มาตรา 82 ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 23 กำหนดโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

ประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)

ชื่อองค์กร: _____

วันที่มีผลบังคับใช้: ____ / ____ / ____

เวอร์ชัน: V1.0

ผู้ควบคุมข้อมูลส่วนบุคคล: _____

1. วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

องค์กรเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์ดังต่อไปนี้:

ชื่อเอกสาร	วัตถุประสงค์ในการประมวลผล	ประเภทข้อมูลที่เกี่ยวข้อง	ฐานทางกฎหมาย (มาตรา 24)	กรณีข้อมูลอ่อนไหว/ ประวัติอาชญากรรม (มาตรา 26)
ใบสมัคร	การสมัครงาน และสรรหาบุคลากร	ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ-สกุล, เบอร์ติดต่อ	จำเป็นเพื่อดำเนินการตามคำขอของเจ้าของข้อมูล ก่อนเข้าทำสัญญา	หากเก็บใบรับรองประวัติอาชญากรรม: ใช้ความยินยอมโดยชัดแจ้ง

บันทึกประวัติการให้บริการ	การให้บริการลูกค้า	ข้อมูลติดต่อ, ประวัติการใช้บริการ	จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายขององค์กร	ไม่มี
บัตรประชาชน	การปฏิบัติตามข้อกำหนดทางกฎหมาย	หมายเลขบัตรประชาชน, เอกสารภาษี	จำเป็นเพื่อปฏิบัติตามกฎหมาย	ไม่มี
กล้อง CCTV	การตรวจสอบความปลอดภัย	ภาพจากกล้องวงจรปิด (CCTV)	จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย	ไม่มี

2. ฐานทางกฎหมายในการประมวลผลข้อมูล (Legal Basis)

องค์กรพิจารณาและกำหนดฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลตาม มาตรา 24 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้แก่:

- 1) ได้รับความยินยอม จากเจ้าของข้อมูล (เฉพาะกรณีที่จำเป็นและไม่มีฐานอื่นรองรับ)
- 2) เพื่อปฏิบัติตามสัญญา หรือคำร้องขอของเจ้าของข้อมูล
- 3) เพื่อประโยชน์โดยชอบด้วยกฎหมาย ขององค์กร
- 4) เพื่อปฏิบัติตามกฎหมาย
- 5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต/ร่างกาย
- 6) เพื่อประโยชน์สาธารณะ/ภารกิจรัฐ

ในกรณีที่มีการเก็บรวบรวมและใช้ ข้อมูลส่วนบุคคลอ่อนไหวหรือข้อมูลเกี่ยวกับประวัติ

อาชญากรรม องค์กรจะพิจารณาฐานทางกฎหมายตาม มาตรา 26 โดย:

อาศัย ความยินยอมอย่างชัดแจ้ง ของเจ้าของข้อมูล

หรือมี ข้อยกเว้นตามกฎหมายเฉพาะ เช่น กฎหมายแรงงาน, กฎหมายว่าด้วยความมั่นคง

3. สิทธิของเจ้าของข้อมูล

เจ้าของข้อมูลมีสิทธิตามกฎหมาย เช่น ขอเข้าถึง แก้ไข คัดค้าน ลบ ขอระงับการใช้ หรือเพิกถอนความยินยอม ตามเงื่อนไขที่กำหนดไว้ในกฎหมาย

4. การติดต่อสอบถาม

หน่วยงาน/เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ชื่อ: _____

อีเมล: _____

โทรศัพท์: _____

5. การปรับปรุงประกาศ

องค์กรขอสงวนสิทธิ์ในการปรับปรุงประกาศฉบับนี้ โดยจะแจ้งให้ทราบผ่านช่องทางที่เหมาะสม

6.6.2 ในกรณีที่มีความจำเป็นตามกฎหมาย หรือมีการเปลี่ยนแปลงวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล องค์กรได้แจ้งการเปลี่ยนแปลงดังกล่าวให้เจ้าของข้อมูลส่วนบุคคลทราบ และบันทึกฐานทางกฎหมายนั้นลงในบันทึกรายการ

สิ่งที่ต้องทำ: มีการแจ้งและบันทึกฐานทางกฎหมายใหม่ลงในบันทึกรายการ

หลักฐาน: หลักฐานการบันทึกฐานทางกฎหมายที่เปลี่ยนแปลงลงในบันทึกรายการ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21, 23, 39

โทษทางปกครอง มาตรา 83 ในกรณีที่ไม่ปฏิบัติตามมาตรา 21 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

โทษทางปกครอง มาตรา 82 ในกรณีที่ไม่ปฏิบัติตามมาตรา 23, มาตรา 39 กำหนดโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

เอกสารหลักฐานการแจ้งและบันทึกการเปลี่ยนแปลงฐานทางกฎหมาย

(Legal Basis Update Record & Notification Log)

ชื่อองค์กร: _____

หน่วยงาน: _____

ผู้ควบคุมข้อมูลส่วนบุคคล: _____

วันที่จัดทำ: ____ / ____ / ____

ส่วนที่ 1: รายการแจ้งการเปลี่ยนแปลงวัตถุประสงค์และฐานทางกฎหมาย

ลำดับ	รายการ ข้อมูลส่วน บุคคลที่ เกี่ยวข้อง	วัตถุประสงค์ เดิม	วัตถุประสงค์ ใหม่	ฐานทาง กฎหมาย เดิม	ฐานทาง กฎหมาย ใหม่	วันที่ เปลี่ยนแปลง	แจ้ง เจ้าของ ข้อมูล แล้ว

1	ข้อมูลประวัติพนักงาน	เพื่อการบริหารงานบุคคล	เพื่อจัดทำแผนการเกษียณและส่งเสริมสุขภาพ	ม.24(3) (ประโยชน์โดยชอบ)	ม.24(1) (ยินยอม)	01/05/2568	แจ้งทางอีเมล
2	ข้อมูลกล้องวงจรปิด (CCTV)	เพื่อความปลอดภัย	ใช้ในการประเมินประสิทธิภาพการทำงาน	ม.24(3)	ม.24(1)	10/05/2568	แจ้งผ่านประกาศ

ส่วนที่ 2: รายละเอียดการแจ้งเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างข้อความแจ้ง (สามารถใช้ประกาศ/จดหมาย/อีเมล)

เรื่อง: แจ้งเปลี่ยนแปลงวัตถุประสงค์และฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

เรียน ท่านเจ้าของข้อมูลส่วนบุคคล

องค์กรมีความจำเป็นต้องเปลี่ยนแปลงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลของท่าน โดยมีรายละเอียดดังนี้

- **ข้อมูลที่เกี่ยวข้อง:** ข้อมูลประวัติพนักงาน
- **วัตถุประสงค์ใหม่:** เพื่อจัดทำแผนส่งเสริมสุขภาพพนักงาน
- **ฐานทางกฎหมาย:** ขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

ทั้งนี้ ท่านสามารถเพิกถอนความยินยอมได้ตลอดเวลาโดยไม่กระทบสิทธิพื้นฐานอื่นใดของท่าน

ขอแสดงความนับถือ

ฝ่ายคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 3: เอกสารแนบ

- แบบฟอร์มความยินยอม (Consent Form) [แนบ]
- บันทึกการกิจกรรมการประมวลผล (Updated Processing Record) [แนบ]
- สำเนาประกาศ/อีเมลแจ้งเจ้าของข้อมูล [แนบ]

ส่วนที่ 4: ผู้รับผิดชอบ

ผู้บันทึก: _____

ตำแหน่ง: _____

วันที่บันทึก: ____ / ____ / ____

6.6.3 ประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Privacy Notice) อยู่ในรูปแบบที่เข้าถึงได้ โดยง่ายและอ่านเข้าใจง่าย

สิ่งที่ต้องทำ: ประกาศการคุ้มครองข้อมูลส่วนบุคคลเข้าถึงได้ง่าย และเข้าใจง่าย

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคลระบุฐานทางกฎหมาย

สภาพบังคับ: แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูล บุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)

ขององค์กร [ชื่อองค์กร]

ประกาศนี้จัดทำขึ้นเพื่อแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ วิธีการ และสิทธิของท่าน ในการคุ้มครองข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. ข้อมูลที่เราเก็บรวบรวม

เราจะเก็บรวบรวมเฉพาะข้อมูลที่จำเป็น ดังนี้

- ชื่อ-นามสกุล
- หมายเลขบัตรประชาชน
- ที่อยู่ / อีเมล / เบอร์โทร
- ข้อมูลด้านการทำงาน (ตำแหน่ง, ประวัติการเข้า-ออกงาน)
- ข้อมูลภาพจากกล้องวงจรปิด (CCTV)
- ข้อมูลสุขภาพหรืออาชญากรรม (หากจำเป็น โดยอาศัยฐานตามมาตรา 26)

2. วัตถุประสงค์ในการประมวลผลข้อมูล

ข้อมูลของท่านจะถูกใช้เพื่อวัตถุประสงค์ดังต่อไปนี้

วัตถุประสงค์	ฐานทางกฎหมาย
การบริหารจัดการพนักงาน	มาตรา 24 (3) – ประโยชน์โดยชอบด้วยกฎหมาย
การให้บริการแก่ลูกค้า	มาตรา 24 (1) – การยินยอม
การปฏิบัติตามกฎหมายภาษี / แรงงาน	มาตรา 24 (6) – การปฏิบัติตามกฎหมาย

การรักษาความปลอดภัย (CCTV)	มาตรา 24 (3) – ประโยชน์โดยชอบ
การประมวลผลข้อมูลอ่อนไหว เช่น ประวัติอาชญากรรม	มาตรา 26 (1) (2) – กรณีจำเป็นตามกฎหมาย หรือได้รับความยินยอมโดยชัดแจ้ง

3. การเปิดเผยข้อมูลแก่บุคคลภายนอก

เราอาจเปิดเผยข้อมูลแก่หน่วยงานราชการ กองทุนประกันสังคม ธนาคาร หรือบริษัทคู่สัญญา ตามความจำเป็น และอาศัยฐานทางกฎหมายที่เหมาะสม

4. ระยะเวลาในการเก็บรักษา

ข้อมูลของท่านจะถูกเก็บไว้ไม่เกินระยะเวลาที่จำเป็นตามวัตถุประสงค์ และ/หรือข้อกำหนดทางกฎหมาย

5. สิทธิของท่านในฐานะเจ้าของข้อมูล

ท่านมีสิทธิขอเข้าถึง แก้ไข ลบ ขอร้องการประมวลผล หรือเพิกถอนความยินยอม ได้ตลอดเวลา โดยติดต่อผ่านช่องทางด้านล่าง

6. ช่องทางการติดต่อ

หากมีคำถามเพิ่มเติมหรือต้องการใช้สิทธิของเจ้าของข้อมูล กรุณาติดต่อ:

ฝ่ายคุ้มครองข้อมูลส่วนบุคคล
 โทร: 0xxx-xxx-xxx
 อีเมล: dpo@[domain].com
 เว็บไซต์: www.องค์กร.com/privacy

ลักษณะการเข้าถึง:

- ประกาศนี้สามารถดาวน์โหลดจากเว็บไซต์ขององค์กร
- ติดประกาศที่บริเวณทางเข้าหลักของสำนักงาน
- แจกแจงในแบบฟอร์มความยินยอม (Consent Form) ทุกครั้งก่อนเก็บข้อมูล

6.7 ความยินยอมมีเงื่อนไขสอดคล้องกับมาตรา 19

6.7.1 ความยินยอมสอดคล้องกับหลักเกณฑ์ตามมาตรา 19 ดังนี้

1. ทำโดยชัดแจ้งเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์
2. ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3. การขอความยินยมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่าย และเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่ายและไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว
 4. คำนี้หมายถึงถึงที่สุดถึงความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ต้องไม่มีการเลือกมาให้ก่อน (do not use pre-ticked boxes)
 5. การเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอม
 6. เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้ โดยจะต้องถอนความยินยอมได้ง่าย เช่นเดียวกับการให้ความยินยอม
 7. การถอนความยินยอมต้องไม่กระทบต่อการประมวลผลข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้ว
 8. หากการถอนความยินยอมกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด องค์กรต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ
- สิ่งที่ต้องทำ: การขอความยินยอมสอดคล้องกับหลักเกณฑ์ตามที่กฎหมายกำหนดครบถ้วน หลักฐาน: แบบฟอร์มขอความยินยอมขององค์กร
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 โทษทางปกครอง มาตรา 82 ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 19 กำหนดโทษปรับทาง ปกครองไม่เกิน 1 ล้านบาท

แบบฟอร์มขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคล

(Personal Data Consent Form)

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่บังคับใช้: [xx/xx/xxxx]

1. ข้อมูลที่เก็บรวบรวม

องค์กรมีความประสงค์จะเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน ดังนี้

- ชื่อ-นามสกุล
- หมายเลขบัตรประชาชน / หนังสือเดินทาง
- เบอร์ติดต่อ / อีเมล
- ข้อมูลสุขภาพ (ถ้ามี)
- ข้อมูลการใช้งานเว็บไซต์ / ก่อร่างวงจรปิด ฯลฯ

2. วัตถุประสงค์ของการประมวลผลข้อมูล

ข้อมูลของท่านจะถูกนำไปใช้เพื่อ

- การให้บริการตามที่ท่านร้องขอ

- การติดต่อกลับ / ส่งข้อมูลข่าวสาร
- การจัดกิจกรรมส่งเสริมการขาย / ประชาสัมพันธ์
- การวิเคราะห์พฤติกรรมการใช้งาน (เว็บไซต์, แอปพลิเคชัน)

3. ฐานทางกฎหมาย

เราขอความยินยอมจากท่านในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ข้างต้นตามมาตรา 19 แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4. ข้อตกลงและสิทธิของท่าน

- ความยินยอมนี้เป็น **การสมัครใจ** โดยไม่มีผลกระทบต่อการรับบริการหลัก
- ท่านสามารถ **ถอนความยินยอมเมื่อใดก็ได้** โดยติดต่อที่ [email / เว็บไซต์ / แบบฟอร์มออนไลน์]
- การถอนความยินยอมจะไม่กระทบต่อการประมวลผลที่ได้ดำเนินการโดยอาศัยความยินยอมก่อนหน้านี้ หากมีผลกระทบใด ๆ จากการถอนความยินยอม เราจะแจ้งให้ท่านทราบล่วงหน้าอย่างชัดเจน

5. การเลือกให้ความยินยอม

โปรดแสดงความยินยอมโดยทำเครื่องหมาย ☒ ข้างล่างนี้ (ไม่ได้เลือกมาให้ล่วงหน้า)

(☒) ข้าพเจ้ายินยอมให้ [ชื่อบริษัท] เก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลของข้าพเจ้าตามวัตถุประสงค์ที่ระบุไว้

(☐) ข้าพเจ้าไม่ยินยอม

6. ช่องทางติดต่อเพื่อถอนความยินยอม

หากท่านประสงค์จะถอนความยินยอม กรุณาติดต่อ:

ฝ่ายคุ้มครองข้อมูลส่วนบุคคล

โทร: 0xxx-xxx-xxx

อีเมล: dpo@[domain].com

เว็บไซต์: [www.\[องค์กร \].com/withdraw-consent](http://www.[องค์กร].com/withdraw-consent)

7. ลายเซ็นผู้ให้ความยินยอม

ลงชื่อ:

ชื่อ-นามสกุล (พิมพ์):

วันที่:

สรุปความสอดคล้องตามมาตรา 19

เกณฑ์	การปฏิบัติ
ข้อ 1	แบบฟอร์มทำเป็นลายลักษณ์อักษร / ระบบออนไลน์ได้
ข้อ 2	แจ้งวัตถุประสงค์อย่างชัดเจน
ข้อ 3	แบบฟอร์มแยกจากเงื่อนไขอื่น อ่านง่าย ไม่หลอกลวง
ข้อ 4	ไม่มีการเลือกมาให้ก่อน (ไม่ pre-tick)
ข้อ 5	ไม่มีเงื่อนไขให้ยินยอมจึงจะรับบริการได้
ข้อ 6	ถอนยินยอมง่าย (ผ่านเว็บไซต์/อีเมล)
ข้อ 7	แจ้งว่าจะไม่กระทบกับการประมวลผลที่ผ่านมา
ข้อ 8	หากกระทบ จะมีการแจ้งให้ทราบ

6.7.2 มีการบันทึกวัตถุประสงค์ของการขอความยินยอมและสามารถตรวจสอบการให้ความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้ รวมถึงจัดให้มีวิธีการในการเพิกถอนความยินยอมได้ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอ

สิ่งที่ต้องทำ: มีการบันทึกและสามารถตรวจสอบการให้ความยินยอมได้ โดยวิธีการเพิกถอนความยินยอมในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอ

หลักฐาน: บันทึกการยินยอมของเจ้าของข้อมูลส่วนบุคคล
รายชื่อผู้ที่เกี่ยวข้องและแผนผัง (flowchart) การดำเนินการที่เกี่ยวกับการจัดการความยินยอม

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19
แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ทางปกครอง มาตรา 82 ในกรณีที่ปฏิบัติตามมาตรา 19 กำหนดโทษปรับทางปกครองไม่เกิน 1 ล้านบาท

รายงานการจัดการความยินยอมของเจ้าของข้อมูลส่วนบุคคล

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่ปรับปรุงล่าสุด: [xx/xx/xxxx]

ส่วนที่ 1: รายการการบันทึกความยินยอมของเจ้าของข้อมูลส่วนบุคคล

รูปแบบการเก็บข้อมูล

องค์กรได้จัดเก็บรายการความยินยอมของเจ้าของข้อมูลส่วนบุคคลในรูปแบบ [ระบุ: ฐานข้อมูลอิเล็กทรอนิกส์ / เอกสารกระดาษ / ระบบ CRM / ระบบ consent management system (CMS)] โดยมีข้อมูลอย่างน้อยดังนี้:

- ชื่อ-นามสกุลเจ้าของข้อมูล
- วันที่ให้ความยินยอม
- วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล
- ช่องทางที่ให้ความยินยอม (เช่น ผ่านเว็บไซต์ / แบบฟอร์ม / แอปพลิเคชัน)
- สถานะปัจจุบัน (ยินยอม / ถอนยินยอม)
-

ตัวอย่างรายการ (จำลอง)

ลำดับ	ชื่อ-นามสกุล	วันที่ให้ความ ยินยอม	วัตถุประสงค์	ช่องทาง	สถานะ
001	นายสมชาย ใจดี	01/05/2567	การตลาดผ่านอีเมล	เว็บไซต์	ยินยอม
002	น.ส. กานต์วี จันทร์เพ็ญ	15/05/256	วิเคราะห์พฤติกรรมการใช้ งาน	แอปพลิเคชัน	ถอน ยินยอม

ส่วนที่ 2: การตรวจสอบการให้ความยินยอม

เจ้าหน้าที่ที่ได้รับมอบหมายสามารถเข้าถึงระบบบันทึกความยินยอมได้เพื่อ

- ตรวจสอบวัตถุประสงค์การประมวลผลที่ได้รับคามยินยอม
- ตรวจสอบสถานะการให้หรือถอนความยินยอมย้อนหลังได้อย่างน้อย 1 ปี
- ออกเอกสารรับรองหรือหลักฐานความยินยอมเมื่อเจ้าของข้อมูลร้องขอ

ส่วนที่ 3: วิธีการในการถอนความยินยอม

องค์กรจัดให้มี วิธีการถอนความยินยอมที่สะดวกและโปร่งใส ดังนี้

- ผ่านแบบฟอร์มออนไลน์ที่เว็บไซต์ขององค์กร
- ส่งคำขอผ่านอีเมลถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ยื่นคำร้องโดยตรง ณ จุดให้บริการขององค์กร
- โทรศัพท์ติดต่อฝ่ายลูกค้าสัมพันธ์ / DPO

เมื่อได้รับคำร้องถอนความยินยอม

- เจ้าหน้าที่จะดำเนินการตรวจสอบตัวตนภายใน 3 วันทำการ
- ระบบจะอัปเดตสถานะเป็น “ถอนยินยอม” ภายใน 7 วัน
- หากมีผลกระทบจากการถอนยินยอม จะมีการแจ้งให้ทราบเป็นลายลักษณ์อักษร

ส่วนที่ 4: รายชื่อผู้ที่เกี่ยวข้องในการจัดการความยินยอม

ชื่อ-ตำแหน่ง	หน้าที่
นาย A (DPO)	ดูแลการจัดเก็บและถอนความยินยอม
นางสาว B (ฝ่ายกฎหมาย)	ตรวจสอบความถูกต้องของวัตถุประสงค์
นาย C (ฝ่าย IT)	ดูแลระบบจัดเก็บข้อมูลยินยอม
เจ้าหน้าที่ประจำเคาน์เตอร์บริการ	รับคำร้องถอนความยินยอมจากผู้ใช้บริการ

ส่วนที่ 5: แผนผังการดำเนินการ (Flowchart ข้อความ)

ขั้นตอนการจัดการความยินยอม

1. เจ้าของข้อมูลได้รับแบบฟอร์มขอความยินยอม
2. อ่านรายละเอียดและตัดสินใจให้ความยินยอมหรือปฏิเสธ
3. ระบบบันทึกข้อมูลในฐานข้อมูลความยินยอม
4. หากถอนความยินยอม
5. เจ้าของข้อมูลยื่นคำขอผ่านช่องทางที่กำหนด
6. เจ้าหน้าที่ตรวจสอบและปรับสถานะในระบบ
7. แจ้งผลให้เจ้าของข้อมูลทราบ

6.7.3 องค์กรมีตัวอย่างที่ใช้ในการขอความยินยอม และวิธีการให้ความยินยอมเพื่อให้เจ้าของข้อมูลส่วนบุคคลเข้าใจเงื่อนไขและวิธีการขอความยินยอม

สิ่งที่ต้องทำ: มีตัวอย่าง และแสดงวิธีการให้ความยินยอมเพื่อให้เจ้าของข้อมูลส่วนบุคคลเข้าใจ

หลักฐาน: ตัวอย่างแบบฟอร์มขอความยินยอมขององค์กรที่ให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงได้

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ตัวอย่างแบบฟอร์มขอความยินยอมและคำแนะนำการให้ความยินยอม

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่: [xx/xx/xxxx]

ส่วนที่ 1: คำชี้แจงก่อนขอความยินยอม

เพื่อให้ท่านเข้าใจและสามารถตัดสินใจให้ความยินยอมอย่างชัดเจน กรุณาอ่านรายละเอียดด้านล่างนี้อย่างละเอียดก่อนลงชื่อ:

- วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน คือ [ระบุวัตถุประสงค์ เช่น การส่งข่าวสาร โปรโมชั่น การวิเคราะห์ข้อมูล ฯลฯ]
- ท่านมีสิทธิที่จะไม่ให้ความยินยอม โดยไม่มีผลกระทบต่อการใช้บริการหลักขององค์กร
- ท่านสามารถถอนความยินยอมได้ทุกเมื่อ โดยใช้วิธีการถอนความยินยอมที่ระบุไว้ท้ายเอกสารนี้
- การให้ความยินยอมครั้งนี้เป็นไปอย่างสมัครใจ โดยท่านสามารถอ่านรายละเอียดเพิ่มเติมในประกาศคุ้มครองข้อมูลส่วนบุคคลของเราได้ที่ [ระบุ URL หรือสถานที่เข้าถึง]

ส่วนที่ 2: แบบฟอร์มขอความยินยอม

โปรดเลือกและทำเครื่องหมายในช่องที่ตรงกับความสมัครใจของท่าน

- [] ข้าพเจ้าให้ความยินยอมให้องค์กรเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของข้าพเจ้าตามวัตถุประสงค์ข้างต้น
- [] ข้าพเจ้าไม่ให้ความยินยอม

ชื่อ-นามสกุล:

วันที่:

ลายมือชื่อ:

ส่วนที่ 3: วิธีการให้ความยินยอม

- ท่านสามารถให้ความยินยอมโดยการติ๊กเลือกในแบบฟอร์มนี้
- หากเป็นการให้ความยินยอมผ่านระบบอิเล็กทรอนิกส์ ท่านจะต้องคลิก “ยอมรับ” หรือปุ่มที่แสดงความยินยอม โดยแบบฟอร์มจะแยกส่วนจากข้อความอื่นอย่างชัดเจน
- ภาษาที่ใช้ในแบบฟอร์มเป็นภาษาที่อ่านง่าย ไม่ซับซ้อน และไม่มีข้อความที่หลอกลวง
- ท่านต้องไม่มีการถูกบังคับหรือถูกตั้งค่าเลือกไว้ล่วงหน้า (ไม่มี pre-ticked box)
- หากมีคำถามเพิ่มเติม สามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขององค์กรได้ที่ [ระบุช่องทางติดต่อ]
-

ส่วนที่ 4: วิธีการถอนความยินยอม

ท่านสามารถถอนความยินยอมได้โดยทำตามช่องทางดังนี้

1. กรอกแบบฟอร์มถอนความยินยอมออนไลน์ที่ [ระบุ URL]
2. ส่งคำขอเป็นลายลักษณ์อักษรทางอีเมลที่ [ระบุอีเมล]
3. ติดต่อเจ้าหน้าที่ ณ จุดบริการขององค์กร
4. โทรศัพท์ที่หมายเลข [ระบุเบอร์โทรศัพท์]
5. เมื่อได้รับคำขอถอนความยินยอมแล้ว องค์กรจะดำเนินการอัปเดตสถานะให้ภายใน 7 วันทำการ และแจ้งผลให้ท่านทราบ

6.8.1 องค์กรมีกระบวนการในการทบทวนความยินยอมเพื่อตรวจสอบว่าวัตถุประสงค์ของการประมวลผลตามความยินยอมที่ได้รับมายังเหมาะสมอยู่

สิ่งที่ต้องทำ: มีกระบวนการทบทวนความยินยอมที่ครบถ้วน

หลักฐาน: นโยบายหรือแนวปฏิบัติ และกระบวนการในการทบทวนความยินยอมที่ได้รับมาขององค์กร

สภาพบังคับ: กฎหมายไม่ได้กำหนด

นโยบายและแนวปฏิบัติในการทบทวนความยินยอม

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่: [xx/xx/xxxx]

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและกระบวนการในการทบทวนความยินยอมที่ได้รับจากเจ้าของข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าวัตถุประสงค์ของการประมวลผลข้อมูลยังคงเหมาะสมและสอดคล้องกับความต้องการและกฎหมายที่เกี่ยวข้อง

2. ขอบเขต

นโยบายนี้ครอบคลุมความยินยอมทั้งหมดที่ได้รับจากเจ้าของข้อมูลส่วนบุคคลในทุกกิจกรรมการประมวลผลข้อมูลขององค์กร

3. แนวปฏิบัติในการทบทวนความยินยอม

3.1 การกำหนดช่วงเวลาทบทวน

- ความยินยอมจะได้รับการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือตามความเหมาะสมของลักษณะข้อมูลและวัตถุประสงค์การประมวลผล
- หากมีการเปลี่ยนแปลงวัตถุประสงค์การประมวลผลหรือข้อกำหนดที่เกี่ยวข้อง จะต้องทำการทบทวนและแจ้งเจ้าของข้อมูลโดยทันที

3.2 กระบวนการทบทวน

- ตรวจสอบรายการความยินยอมที่มีอยู่ในระบบ
- ประเมินว่าวัตถุประสงค์การใช้ข้อมูลยังคงชัดเจน ถูกต้อง และเหมาะสม
- แจ้งเจ้าของข้อมูลส่วนบุคคลหากพบความจำเป็นในการปรับเปลี่ยนวัตถุประสงค์ หรือหากต้องขอความยินยอมใหม่
- จัดทำรายงานการทบทวนความยินยอมเพื่อบันทึกผลการตรวจสอบและดำเนินการที่เกี่ยวข้อง

3.3 การสื่อสารและอบรม

ฝ่ายที่เกี่ยวข้องจะได้รับการอบรมเกี่ยวกับกระบวนการทบทวนความยินยอม มีการสื่อสารให้เจ้าของข้อมูลส่วนบุคคลรับทราบถึงสิทธิและการทบทวนความยินยอมอย่างชัดเจน

4. เอกสารและหลักฐาน

- บันทึกรายการความยินยอมของเจ้าของข้อมูลส่วนบุคคล
- รายงานการทบทวนความยินยอมตามช่วงเวลาที่กำหนด
- เอกสารแจ้งการเปลี่ยนแปลงวัตถุประสงค์และคำขอความยินยอมใหม่ (ถ้ามี)

5. ความรับผิดชอบ

- ฝ่ายบริหารข้อมูลส่วนบุคคลรับผิดชอบในการจัดการและดูแลกระบวนการทบทวนความยินยอม
- ฝ่าย IT สนับสนุนระบบบันทึกและตรวจสอบข้อมูลความยินยอม

6.8.2 องค์กรมีการกำหนดช่วงเวลาที่เหมาะสม (at Appropriate Intervals) ในการขอความยินยอมอีกครั้ง เพื่อใช้ในการทบทวนความยินยอมว่ายังมีเงื่อนไขสอดคล้องกับกฎหมายและวัตถุประสงค์เดิมอยู่

(อย่างน้อยควรมีการทบทวนทุก ๆ สองปี)

สิ่งที่ต้องทำ: มีการกำหนดช่วงเวลาที่เหมาะสมอย่างน้อยทุก ๆ สองปี

หลักฐาน: นโยบายหรือแนวปฏิบัติ และกระบวนการในการทบทวนความยินยอมที่ได้รับมาขององค์กร

สภาพบังคับ: กฎหมายไม่ได้กำหนด

นโยบายและแนวปฏิบัติในการกำหนดช่วงเวลาทบทวนความยินยอม

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่: [xx/xx/xxxx]

1. วัตถุประสงค์

เพื่อกำหนดช่วงเวลาที่เหมาะสมในการขอความยินยอมซ้ำจากเจ้าของข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าการประมวลผลข้อมูลส่วนบุคคลยังคงสอดคล้องกับกฎหมายและวัตถุประสงค์เดิม

2. ขอบเขต

นโยบายนี้ครอบคลุมความยินยอมที่ได้รับจากเจ้าของข้อมูลส่วนบุคคลในทุกกรณีที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3. แนวปฏิบัติในการกำหนดช่วงเวลาทบทวน

3.1 กำหนดช่วงเวลาทบทวน

กำหนดให้มีการทบทวนความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอย่างน้อยทุก ๆ สองปี ในกรณีที่มีการเปลี่ยนแปลงสำคัญในวัตถุประสงค์ของการประมวลผล หรือข้อกำหนดที่เกี่ยวข้อง ให้ทำการทบทวนและขอความยินยอมใหม่ทันที

3.2 การดำเนินการทบทวน

ตรวจสอบฐานข้อมูลความยินยอม เพื่อระบุข้อมูลที่ครบกำหนดทบทวนในแต่ละช่วงเวลา จัดทำการแจ้งเตือนเจ้าของข้อมูลให้ทราบถึงการทบทวนและขอความยินยอมใหม่ในเวลาที่เหมาะสม บันทึกผลการทบทวนและความยินยอมใหม่อย่างเป็นระบบ

3.3 การสื่อสารและความโปร่งใส

- แจ้งให้เจ้าของข้อมูลรับทราบถึงสิทธิและวิธีการในการให้และถอนความยินยอมอย่างชัดเจน
- จัดให้มีช่องทางในการติดต่อสอบถามข้อมูลเพิ่มเติมเกี่ยวกับการขอความยินยอมและการทบทวน

4. เอกสารและหลักฐาน

- นโยบายและแนวปฏิบัติในการกำหนดช่วงเวลาทบทวนความยินยอม
- รายงานหรือบันทึกการทบทวนความยินยอมตามช่วงเวลาที่กำหนด
- เอกสารแจ้งเตือนและตอบรับจากเจ้าของข้อมูลส่วนบุคคล

5. ความรับผิดชอบ

- ฝ่ายบริหารข้อมูลส่วนบุคคลรับผิดชอบในการกำหนดและดำเนินการทบทวนความยินยอมตามช่วงเวลาที่เหมาะสม
- ฝ่าย IT สนับสนุนระบบบันทึกและแจ้งเตือนการทบทวนความยินยอม

6.8.3 องค์กรจัดให้มีเครื่องมือในการควบคุมหรือกำหนดความเป็นส่วนตัวโดยเจ้าของข้อมูลส่วนบุคคล (privacy dashboards) เพื่อใช้ในการจัดการความยินยอมด้วยตัวเอง เช่น การให้หรือเพิกถอนความยินยอม

สิ่งที่ต้องทำ: มีเครื่องมือจัดการความยินยอมให้เจ้าของข้อมูลส่วนบุคคลกำหนดความเป็นส่วนตัวด้วยตนเอง

หลักฐาน: เครื่องมือในการควบคุมหรือกำหนดความเป็นส่วนตัวโดยเจ้าของข้อมูลส่วนบุคคล เช่น privacy dashboard

สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานและคำชี้แจงเกี่ยวกับเครื่องมือ Privacy Dashboard

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่: [xx/xx/xxxx]

1. วัตถุประสงค์

เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงและจัดการความยินยอม รวมถึงความเป็นส่วนตัวของตนเองได้อย่างสะดวก รวดเร็ว และโปร่งใส ผ่านเครื่องมือออนไลน์ที่องค์กรจัดทำขึ้น

2. รายละเอียดเครื่องมือ Privacy Dashboard

2.1 คุณสมบัติหลัก

- เจ้าของข้อมูลสามารถดูข้อมูลส่วนบุคคลที่องค์กรเก็บรวบรวม
- สามารถตรวจสอบฐานข้อมูลความยินยอมที่ได้ให้ไว้กับองค์กร
- มีฟังก์ชันให้เจ้าของข้อมูลยินยอมใหม่ (opt-in) หรือเพิกถอนความยินยอม (opt-out) ได้ด้วยตนเอง
- แจ้งเตือนเจ้าของข้อมูลเมื่อมีการเปลี่ยนแปลงนโยบายความเป็นส่วนตัวหรือขอความยินยอมใหม่
- ระบบสามารถบันทึกและแสดงประวัติการให้และถอนความยินยอมอย่างเป็นระบบ
- มีช่องทางติดต่อฝ่ายข้อมูลส่วนบุคคลเพื่อสอบถามหรือร้องเรียน

2.2 การเข้าถึง

- ผ่านเว็บไซต์หลักขององค์กร หรือแอปพลิเคชันที่รองรับ
- มีการยืนยันตัวตนเจ้าของข้อมูลอย่างปลอดภัยก่อนเข้าสู่ระบบ

3. กระบวนการใช้งาน

3.1 การเข้าสู่ระบบ

เจ้าของข้อมูลใช้บัญชีที่ได้รับจากองค์กร หรือระบบยืนยันตัวตนผ่าน OTP รหัสผ่าน หรือระบบยืนยันตัวตนสองขั้นตอน (2FA)

3.2 การจัดการความยินยอม

เจ้าของข้อมูลเลือกรายการข้อมูลที่ให้ความยินยอมไว้

- เจ้าของข้อมูลสามารถเปลี่ยนแปลงสถานะความยินยอมได้ตามต้องการ
- ระบบบันทึกข้อมูลการเปลี่ยนแปลงและแสดงสถานะล่าสุดให้เจ้าของข้อมูลตรวจสอบ

4. หลักฐานประกอบ

- คู่มือการใช้งาน Privacy Dashboard สำหรับเจ้าของข้อมูล
- ตัวอย่างหน้าจอระบบ Privacy Dashboard (แสดงในรูปแบบเอกสาร)
- รายงานการบันทึกและตรวจสอบความยินยอมของเจ้าของข้อมูล
- รายงานการแจ้งเตือนและการตอบรับจากเจ้าของข้อมูล

5. ความรับผิดชอบ

- ฝ่ายเทคโนโลยีสารสนเทศ รับผิดชอบการพัฒนาและดูแลระบบ Privacy Dashboard

- ฝ่ายบริหารข้อมูลส่วนบุคคล รับผิดชอบการจัดทำนโยบายและตรวจสอบการใช้งานเครื่องมือให้เป็นไปตามข้อกำหนด

6.9 องค์การมีระบบในการตรวจสอบอายุและความสามารถของผู้เยาว์ และมีมาตรการในการตรวจสอบว่าได้รับความยินยอมจากบุคคลที่มีอำนาจกระทำการแทนผู้เยาว์ (Risk-based age checks and parental/guardian consent) ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะตามกฎหมายว่าการขอความยินยอมนั้นต้องปฏิบัติตามเงื่อนไขของมาตรา 20

6.9.1 องค์การมีการตรวจสอบอายุของผู้เยาว์ โดยกำหนดวิธีการที่เหมาะสมสำหรับการตรวจสอบ เพื่อขอความยินยอมจากผู้เยาว์ตามกฎหมาย

สิ่งที่ต้องทำ: มีระบบและวิธีการตรวจสอบอายุของผู้เยาว์อย่างชัดเจน

หลักฐาน: ระบบหรือขั้นตอนการดำเนินงานในการตรวจสอบอายุของผู้เยาว์

สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานและคำชี้แจงระบบการตรวจสอบอายุของผู้เยาว์

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่: [xx/xx/xxxx]

1. วัตถุประสงค์

เพื่อกำหนดและจัดให้มีระบบในการตรวจสอบอายุของเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เยาว์ เพื่อให้การขอความยินยอมเป็นไปอย่างถูกต้องตามกฎหมายและสอดคล้องกับมาตรา 20 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ระบบและวิธีการตรวจสอบอายุ

2.1 วิธีการตรวจสอบอายุที่ใช้ในองค์กร

- การขอสำเนาบัตรประจำตัวประชาชน หรือเอกสารแสดงตัวตนที่มีวันเดือนปีเกิด
- การยืนยันวันเกิดผ่านระบบอิเล็กทรอนิกส์ เช่น การกรอกวันเดือนปีเกิดในแบบฟอร์มออนไลน์ พร้อมตรวจสอบความสมเหตุสมผล (Age Gate)
- การใช้ระบบตรวจสอบอายุอัตโนมัติที่เชื่อมต่อกับฐานข้อมูลภายนอก (ถ้ามี) เพื่อยืนยันข้อมูล
- การขอรับรองจากผู้ปกครองหรือผู้มีอำนาจกระทำการแทนผู้เยาว์ เพื่อยืนยันความถูกต้อง

2.2 แนวทางปฏิบัติ

- เจ้าหน้าที่จะต้องตรวจสอบและยืนยันอายุเจ้าของข้อมูลก่อนดำเนินการขอความยินยอม
- หากพบว่าเจ้าของข้อมูลเป็นผู้เยาว์ จะต้องดำเนินการขอความยินยอมจากผู้ปกครองหรือผู้มีอำนาจตามกฎหมาย
- มีการบันทึกผลการตรวจสอบอายุและการขอความยินยอมไว้เป็นหลักฐาน
- ระบบจะมีการแจ้งเตือนเมื่ออายุของเจ้าของข้อมูลใกล้จะเปลี่ยนสถานะ (เช่น จากผู้เยาว์เป็นผู้ใหญ่) เพื่อทบทวนความยินยอมใหม่

3. กระบวนการดำเนินงาน

3.1 ขั้นตอนการตรวจสอบอายุ

- เจ้าของข้อมูลกรอกวันเดือนปีเกิดผ่านแบบฟอร์มหรือช่องทางออนไลน์
- เจ้าหน้าที่ตรวจสอบเอกสารประกอบการยืนยันอายุ (ถ้ามี)
- หากเป็นผู้เยาว์ เจ้าหน้าที่แจ้งให้ผู้ปกครองหรือผู้มีอำนาจดำเนินการให้ความยินยอม
- บันทึกผลการตรวจสอบและเก็บรักษาเอกสารหรือข้อมูลประกอบ

3.2 การจัดการความยินยอมของผู้เยาว์

- มีแบบฟอร์มขอความยินยอมเฉพาะสำหรับผู้เยาว์และผู้ปกครอง
- ระบบจัดเก็บและตรวจสอบความถูกต้องของความยินยอมจากผู้มีอำนาจแทนผู้เยาว์

4. หลักฐานประกอบ

- เอกสารแสดงขั้นตอนและระบบตรวจสอบอายุเจ้าของข้อมูลผู้เยาว์

- ตัวอย่างแบบฟอร์มขอความยินยอมของผู้เยาว์และผู้ปกครอง
- รายงานบันทึกผลการตรวจสอบอายุและความยินยอม
- นโยบายภายในเกี่ยวกับการจัดการข้อมูลผู้เยาว์และการขอความยินยอม

5. ความรับผิดชอบ

- ฝ่ายบริหารข้อมูลส่วนบุคคลรับผิดชอบจัดทำและควบคุมระบบตรวจสอบอายุ
- ฝ่ายเทคโนโลยีสารสนเทศสนับสนุนระบบการยืนยันอายุผ่านช่องทางออนไลน์
- เจ้าหน้าที่ประสานงานติดตามและจัดเก็บหลักฐานความยินยอม

6.9.2 องค์กรมีมาตรการที่เหมาะสมในการตรวจสอบว่าบุคคลดังกล่าวสามารถให้ความยินยอมด้วยตนเองได้ ในกรณีที่ไม่ได้ต้องมีมาตรการที่เหมาะสมในการได้รับความยินยอมจากผู้ใช้อำนาจปกครอง แล้วแต่กรณี

สิ่งที่ต้องทำ: มีมาตรการในการตรวจสอบที่มีประสิทธิภาพและเหมาะสม

หลักฐาน: นโยบายหรือแนวปฏิบัติ และกระบวนการในการขอความยินยอมจากผู้ใช้อำนาจปกครอง
ปกครอง แล้วแต่กรณี

สภาพบังคับ: แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ.
คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

นโยบายและแนวปฏิบัติในการตรวจสอบความสามารถและการขอความยินยอมจากผู้ใช้อำนาจปกครอง

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่: [xx/xx/xxxx]

1. วัตถุประสงค์

เพื่อกำหนดมาตรการและกระบวนการตรวจสอบความสามารถของเจ้าของข้อมูลผู้เยาว์ในการให้ความยินยอมด้วยตนเอง และในกรณีที่ไม่สามารถให้ความยินยอมได้ ให้มีมาตรการในการขอความยินยอมจากผู้ใช้อำนาจปกครองตามกฎหมายและแนวทางของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. มาตรการตรวจสอบความสามารถในการให้ความยินยอม

2.1 การประเมินความสามารถของเจ้าของข้อมูลผู้เยาว์

- ใช้แบบสอบถามหรือการสัมภาษณ์เพื่อประเมินความเข้าใจของผู้เยาว์เกี่ยวกับวัตถุประสงค์และผลกระทบของการให้ความยินยอม
- พิจารณาอายุ ความรู้ ความเข้าใจ และสติปัญญาของผู้เยาว์ เพื่อประเมินว่าผู้เยาว์มีความสามารถในการให้ความยินยอมด้วยตนเองหรือไม่
- หากประเมินแล้วว่าผู้เยาว์มีความสามารถ ให้ดำเนินการขอความยินยอมโดยตรงจากผู้เยาว์
- หากผู้เยาว์ไม่มีความสามารถ ให้ดำเนินการขอความยินยอมจากผู้ใช้อำนาจปกครองแทน

2.2 กรณีที่ต้องขอความยินยอมจากผู้ใช้อำนาจปกครอง

- กำหนดขั้นตอนและแบบฟอร์มขอความยินยอมจากผู้ปกครองหรือผู้ใช้อำนาจตามกฎหมาย
- มีการยืนยันตัวตนของผู้ใช้อำนาจปกครอง เช่น สำเนาบัตรประชาชน หรือเอกสารแสดงสิทธิในการปกครอง
- บันทึกและเก็บรักษาความยินยอมจากผู้ใช้อำนาจปกครองไว้อย่างเป็นระบบ
- แจ้งให้ผู้ปกครองทราบสิทธิในการเพิกถอนความยินยอมได้ตามกฎหมาย

3. กระบวนการดำเนินงาน

3.1 ขั้นตอนการตรวจสอบและขอความยินยอม

- เจ้าของข้อมูลผู้เยาว์กรอกข้อมูลเบื้องต้นและตอบแบบประเมินความสามารถ
- เจ้าหน้าที่ประเมินความสามารถตามเกณฑ์ที่กำหนด
- หากประเมินว่าผู้เยาว์สามารถให้ความยินยอมได้ ให้ดำเนินการขอความยินยอมโดยตรง
- หากไม่สามารถให้ความยินยอมได้ ให้ดำเนินการขอความยินยอมจากผู้ใช้อำนาจปกครอง พร้อมยืนยันเอกสารสิทธิในการปกครอง
- บันทึกผลการประเมินและการขอความยินยอมลงในระบบฐานข้อมูลขององค์กร

4. หลักฐานประกอบ

- นโยบายและแนวปฏิบัติการตรวจสอบความสามารถและขอความยินยอมจากผู้ใช้อำนาจปกครอง
- แบบฟอร์มประเมินความสามารถของผู้เยาว์
- แบบฟอร์มขอความยินยอมจากผู้ใช้อำนาจปกครอง

- รายงานการประเมินและบันทึกผลความยินยอมจากผู้เยาว์และผู้ใช้อำนาจปกครอง

5. ความรับผิดชอบ

- ฝ่ายบริหารข้อมูลส่วนบุคคลรับผิดชอบจัดทำและควบคุมการดำเนินงานตามนโยบายนี้
- เจ้าหน้าที่ประสานงานตรวจสอบและประเมินความสามารถของเจ้าของข้อมูลผู้เยาว์
- ฝ่ายเทคโนโลยีสารสนเทศสนับสนุนระบบบันทึกและจัดเก็บข้อมูลความยินยอม

6.9.3 ในกรณีที่ให้บริการออนไลน์กับผู้เยาว์ องค์กรมีมาตรการในการประเมินความเสี่ยงเพื่อใช้ในการตรวจสอบอายุของผู้เยาว์ให้สอดคล้องกับระดับความเสี่ยงที่อาจเกิดขึ้นกับสิทธิและเสรีภาพของผู้เยาว์
 สิ่งที่ต้องทำ: มีการประเมินความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ และมีการพิจารณาตามแต่ละช่วงอายุ

หลักฐาน: รายงานการประเมินความเสี่ยงกรณีการให้บริการออนไลน์กับผู้เยาว์

สภาพบังคับ: แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

รายงานการประเมินความเสี่ยงกรณีการให้บริการออนไลน์กับผู้เยาว์

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่: [xx/xx/xxxx]

1. บทนำ

รายงานฉบับนี้จัดทำขึ้นเพื่อประเมินความเสี่ยงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ที่ใช้บริการออนไลน์ขององค์กร และเพื่อกำหนดมาตรการตรวจสอบอายุผู้เยาว์ให้เหมาะสมกับระดับความเสี่ยงตามช่วงอายุ เพื่อปกป้องสิทธิและเสรีภาพของผู้เยาว์ตามแนวทาง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ขอบเขตของการประเมิน

- การให้บริการออนไลน์ทุกประเภทที่มีการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์
- การตรวจสอบอายุและการขอความยินยอมจากผู้เยาว์หรือผู้ใช้อำนาจปกครอง
- การวิเคราะห์ความเสี่ยงในแต่ละช่วงอายุของผู้เยาว์ (เช่น ต่ำกว่า 13 ปี, 13-15 ปี, 16-18 ปี)

3. การประเมินความเสี่ยง

ช่วงอายุผู้เยาว์	ความเสี่ยงด้านสิทธิและเสรีภาพ	มาตรการตรวจสอบอายุและความเสี่ยงที่ดำเนินการ
ต่ำกว่า 13 ปี	ความเสี่ยงสูง เนื่องจากผู้เยาว์อายุน้อย อาจไม่เข้าใจผลกระทบ	- ตรวจสอบเอกสารยืนยันอายุจากผู้ปกครอง- ขอความยินยอมจากผู้ปกครองเท่านั้น- จำกัดการเข้าถึงข้อมูลหรือฟีเจอร์บางอย่าง
13-15 ปี	ความเสี่ยงปานกลาง มีความสามารถในการให้ความยินยอมบางส่วน	- ประเมินความสามารถในการให้ความยินยอมโดยตรงจากผู้เยาว์- ขอความยินยอมจากผู้ปกครองร่วมด้วยตามกรณี
16-18 ปี	ความเสี่ยงต่ำ ผู้เยาว์มีความสามารถในการให้ความยินยอมมากขึ้น	- ขอความยินยอมจากผู้เยาว์โดยตรง- มีมาตรการตรวจสอบอายุเพิ่มเติมเมื่อจำเป็น

4. มาตรการที่นำมาใช้

ระบบตรวจสอบอายุออนไลน์ เช่น การกรอกวันเดือนปีเกิดและการยืนยันตัวตนเบื้องต้น

- การใช้ระบบยืนยันตัวตนของผู้ปกครองในกรณีผู้เยาว์อายุต่ำกว่าเกณฑ์กำหนด
- การกำหนดนโยบายจำกัดการเข้าถึงข้อมูลหรือบริการที่ไม่เหมาะสมกับผู้เยาว์ในแต่ละช่วงอายุ
- การทบทวนและอัปเดตมาตรการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ

6.9.4 ในกรณีที่เป็นการขอความยินยอมจากผู้เยาว์หรือบุคคลไร้ความสามารถหรือเสมือนไร้ความสามารถ องค์กรมีมาตรการตรวจสอบที่เหมาะสมว่าบุคคลที่ให้ความยินยอมแทนเป็นผู้มีอำนาจกระทำการแทนเจ้าของข้อมูลส่วนบุคคลอย่างแท้จริง

สิ่งที่ต้องทำ: มีมาตรการในการตรวจสอบผู้มีอำนาจกระทำการแทน และมีขั้นตอนการขอเอกสารประกอบการพิจารณาที่ชัดเจน

หลักฐาน: แนวปฏิบัติหรือกลไกในการตรวจสอบสถานะผู้ให้ความยินยอมแทนเจ้าของข้อมูลส่วนบุคคล

สภาพบังคับ: แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

แนวปฏิบัติและกลไกในการตรวจสอบสถานะผู้ให้ความยินยอมแทนเจ้าของข้อมูลส่วนบุคคล

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่: [xx/xx/xxxx]

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการตรวจสอบว่าผู้ให้ความยินยอมแทนเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นผู้เยาว์ บุคคลไร้ความสามารถ หรือเสมือนไร้ความสามารถ เป็นผู้มีอำนาจกระทำการแทนอย่างถูกต้องตามกฎหมายและระเบียบที่เกี่ยวข้อง

2. ขอบเขต

แนวปฏิบัตินี้ครอบคลุมการขอความยินยอมในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมด้วยตนเองได้ และต้องมีผู้แทนที่มีอำนาจในการให้ความยินยอมแทน

3. มาตรการและขั้นตอนในการตรวจสอบผู้มีอำนาจให้ความยินยอมแทน

3.1 การยืนยันตัวตนของผู้ให้ความยินยอมแทน

- ตรวจสอบบัตรประจำตัวประชาชนหรือเอกสารราชการที่แสดงตัวตน
- ตรวจสอบความเกี่ยวข้องทางกฎหมาย เช่น บัตรผู้ปกครอง สูติบัตร หรือเอกสารแต่งตั้งผู้อนุบาล

3.2 การขอเอกสารประกอบการพิจารณา

- เอกสารแสดงความสัมพันธ์ เช่น สูติบัตรของผู้เยาว์, เอกสารรับรองความเป็นบิดา มารดา หรือผู้อนุบาล
- หนังสือมอบอำนาจ หรือคำสั่งศาลในกรณีผู้อนุบาลหรือผู้ดูแลตามกฎหมาย
- เอกสารทางการแพทย์หรือคำพิพากษาที่แสดงสถานะไร้ความสามารถหรือเสมือนไร้ความสามารถ

3.3 การบันทึกและเก็บรักษาข้อมูล

- บันทึกข้อมูลผู้ให้ความยินยอมแทนในระบบจัดการข้อมูล
- เก็บรักษาเอกสารประกอบการตรวจสอบอย่างปลอดภัยและเป็นความลับ

3.4 การตรวจสอบซ้ำ

ทบทวนและตรวจสอบความถูกต้องของเอกสารและสถานะของผู้ให้ความยินยอมแทนอย่างสม่ำเสมอ

กำหนดช่วงเวลาการตรวจสอบซ้ำตามนโยบายองค์กร (เช่น ทุก 1 ปี หรือเมื่อมีการเปลี่ยนแปลงข้อมูล)

4. ความรับผิดชอบ

- ฝ่ายบริหารจัดการข้อมูลส่วนบุคคลรับผิดชอบในการตรวจสอบและบันทึกข้อมูล
- ฝ่ายกฎหมายและความปลอดภัยข้อมูลสนับสนุนการตรวจสอบเอกสารและให้คำปรึกษาทางกฎหมาย
- แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

6.10 ในกรณีที่องค์กรใช้ฐานทางกฎหมายตามมาตรา 24 (5) สำหรับกรณีที่เป็นกรจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายขององค์กร (Legitimate Interest) องค์กรมีการจัดการประเมินผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Legitimate Interest Assessment: LIA) ก่อนเริ่มการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

6.10.1 มีการจัดการประเมินผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล เพื่อใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest Assessment: LIA)

สิ่งที่ต้องทำ: มีการดำเนินการครบถ้วน

หลักฐาน: เอกสารการประเมิน Legitimate Interest Assessment (LIA)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การประเมินผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Legitimate Interest Assessment: LIA)

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0 / วันที่: [xx/xx/xxxx]

1. วัตถุประสงค์

เพื่อประเมินและวิเคราะห์ผลกระทบที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลจากการใช้ฐานทางกฎหมายตามมาตรา 24 (5) เพื่อประโยชน์โดยชอบด้วยกฎหมายขององค์กร

2. ขอบเขต

การประเมินนี้ครอบคลุมกิจกรรมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยอาศัยฐาน Legitimate Interest ตามมาตรา 24 (5)

3. ขั้นตอนการประเมิน Legitimate Interest Assessment (LIA)

3.1 ระบุประโยชน์โดยชอบด้วยกฎหมายขององค์กร

- กำหนดวัตถุประสงค์และประโยชน์ที่องค์กรต้องการได้รับจากการประมวลผลข้อมูลส่วนบุคคล
- ระบุฐานกฎหมายที่เกี่ยวข้องกับการใช้ Legitimate Interest

3.2 ประเมินความจำเป็นและความเหมาะสม

- ตรวจสอบว่าการประมวลผลข้อมูลนั้นจำเป็นและเหมาะสมกับวัตถุประสงค์ที่ตั้งไว้หรือไม่
- พิจารณาวិธีการประมวลผลและปริมาณข้อมูลที่ใช้ให้เหมาะสมและไม่เกินความจำเป็น

3.3 ประเมินผลกระทบต่อเจ้าของข้อมูล

- วิเคราะห์ความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูล เช่น ผลกระทบต่อความเป็นส่วนตัว ส่วนตัว ความปลอดภัย และความเสี่ยงในการถูกละเมิดข้อมูล
- พิจารณามาตรการลดผลกระทบที่เหมาะสมเพื่อป้องกันหรือบรรเทาความเสี่ยง

3.4 จัดทำรายงานสรุปผลการประเมิน

- รายงานผลการประเมิน พร้อมข้อเสนอแนะและมาตรการควบคุม
- ระบุผู้รับผิดชอบและแผนการติดตามผลการดำเนินงาน

4. ความรับผิดชอบ

- ฝ่ายบริหารความเสี่ยงและคุ้มครองข้อมูลส่วนบุคคลรับผิดชอบดำเนินการประเมินและรายงาน
- ฝ่ายกฎหมายสนับสนุนคำปรึกษาด้านกฎหมายและตรวจสอบความถูกต้อง

5. เอกสารแนบ

- แบบฟอร์ม Legitimate Interest Assessment (LIA)
- รายงานผลการประเมินผลกระทบและแผนการบริหารความเสี่ยง

6. ข้อกำหนดตามกฎหมายที่เกี่ยวข้อง

- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (5)
- แนวทางปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลและการประเมินผลกระทบ

6.10.2 LIA มีการชั่งผลประโยชน์ตามหลักความได้สัดส่วน เพื่อให้มั่นใจว่าประโยชน์โดยชอบด้วยกฎหมายขององค์กรมีความเหมาะสมเมื่อเทียบกับสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยมีแนวทางการประเมินดังนี้

1. ไม่ใช่ข้อมูลในลักษณะที่เป็นการก้าวล่วงความเป็นส่วนตัวส่วนตัวเกินสมควร หรือในลักษณะที่ก่อให้เกิดความเสียหาย เว้นแต่มีเหตุผลและความจำเป็นตามกฎหมาย
2. มีการปกป้องผลประโยชน์หรือส่วนได้เสียของบุคคลที่เป็นกลุ่มเปราะบาง เช่น ผู้เยาว์ หรือผู้พิการ อย่างเหมาะสม
3. มีการกำหนดมาตรการที่เหมาะสมในการลดผลกระทบเชิงลบที่อาจเกิดขึ้น
4. เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอระงับหรือให้ยุติการประมวลผลดังกล่าว เว้นแต่จะมีข้อยกเว้นตามกฎหมาย

สิ่งที่ต้องทำ: มีการพิจารณาตามแนวทางการประเมินครบถ้วน

หลักฐาน: เอกสารการประเมิน Legitimate Interest Assessment (LIA)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานการประเมินผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Legitimate Interest Assessment: LIA)

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.1 / วันที่: [xx/xx/xxxx]

1. วัตถุประสงค์

เพื่อชี้แจงน้ำหนักและประเมินผลประโยชน์โดยชอบด้วยกฎหมายขององค์กรเทียบกับสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ตามหลักความได้สัดส่วน (Proportionality) และพิจารณามาตรการปกป้องกลุ่มเปราะบางและการลดผลกระทบเชิงลบ

2. แนวทางการประเมินผลการชี้แจงน้ำหนักผลประโยชน์

2.1 การหลีกเลี่ยงการใช้ข้อมูลเกินสมควร

- ประเมินว่าการใช้ข้อมูลไม่เป็นการละเมิดความเป็นส่วนตัวเกินความจำเป็น
- ตรวจสอบว่าการใช้ข้อมูลไม่ก่อให้เกิดความเสียหายหรือผลกระทบเชิงลบโดยไม่จำเป็น

2.2 การปกป้องกลุ่มเปราะบาง

- ระบุว่าข้อมูลของกลุ่มเปราะบาง เช่น ผู้เยาว์ ผู้พิการ หรือกลุ่มอื่น ๆ ที่อาจได้รับผลกระทบพิเศษหรือไม่
- กำหนดมาตรการป้องกันและดูแลสิทธิของกลุ่มเปราะบางอย่างเหมาะสม เช่น การขอความยินยอมจากผู้ปกครอง หรือการจำกัดการเข้าถึงข้อมูล

2.3 มาตรการลดผลกระทบเชิงลบ

- กำหนดมาตรการเชิงเทคนิคและองค์กร เช่น การเข้ารหัสข้อมูล การจำกัดการเข้าถึง หรือการกำหนดระยะเวลาการเก็บรักษาข้อมูล
- มีการติดตามและประเมินมาตรการอย่างสม่ำเสมอ

2.4 สิทธิของเจ้าของข้อมูลส่วนบุคคล

- แจ้งสิทธิของเจ้าของข้อมูลในการขอระงับหรือยุติการประมวลผลข้อมูล
- กำหนดขั้นตอนการรับเรื่องและดำเนินการตามคำขอของเจ้าของข้อมูลตามกฎหมายและข้อยกเว้นที่เกี่ยวข้อง

3. สรุปผลการชี้แจงน้ำหนักผลประโยชน์

- ประโยชน์โดยชอบด้วยกฎหมายขององค์กร: [ระบุรายละเอียด]
- ผลกระทบต่อเจ้าของข้อมูล: [วิเคราะห์ผลกระทบ]
- มาตรการที่ดำเนินการ: [ระบุมาตรการลดผลกระทบ]
- ความเหมาะสมและความได้สัดส่วน: [ข้อสรุป]

4. ความรับผิดชอบ

- ฝ่ายบริหารความเสี่ยงและคุ้มครองข้อมูลส่วนบุคคล รับผิดชอบจัดทำและติดตามการประเมิน

- ฝ่ายกฎหมายร่วมตรวจสอบความถูกต้องและสอดคล้องกับกฎหมาย

5. เอกสารแนบ

- แบบฟอร์มการประเมิน LIA ที่มีรายละเอียดการชั่งน้ำหนักผลประโยชน์
- บันทึกการประชุมหรือความคิดเห็นจากผู้เกี่ยวข้อง

6. ข้อกำหนดตามกฎหมายที่เกี่ยวข้อง

- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (5)
- แนวทางปฏิบัติและมาตรฐานสากลด้านการประเมินผลกระทบ

6.10.3 มีการจัดทำเป็นเอกสาร LIA เพื่อให้สามารถตรวจสอบได้ถึงการใช้นโยบายการประเมินและการตัดสินใจ

- สิ่งที่ต้องทำ: มีการจัดทำเอกสารเพื่อการตรวจสอบ และบันทึกแนวทางการประเมิน หรือการตัดสินใจ
ชัดเจน
- หลักฐาน: เอกสารรายงานการประเมินผลประโยชน์โดยชอบด้วยกฎหมาย Legitimate Interest
Assessment (LIA)
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานการประเมินผลประโยชน์โดยชอบด้วยกฎหมาย(Legitimate Interest Assessment (LIA) Report)

องค์กร: [ชื่อองค์กร]

เวอร์ชัน: 1.0

วันที่: [xx/xx/xxxx]

ผู้จัดทำ: [ชื่อผู้รับผิดชอบ]

1. บทนำ

- ระบุวัตถุประสงค์ของการทำ LIA และขอบเขตของการประเมิน
- อธิบายกรอบแนวทางการประเมินผลประโยชน์โดยชอบด้วยกฎหมายเทียบกับสิทธิและเสรีภาพของเจ้าของข้อมูล

2. ขั้นตอนการประเมิน

- ระบุขั้นตอนการดำเนินการประเมิน รวมถึงวิธีการเก็บรวบรวมข้อมูลและการวิเคราะห์
- บันทึกแนวทางการชั่งน้ำหนักผลประโยชน์และการพิจารณาปัจจัยต่าง ๆ

3. การตัดสินใจ

- สรุปผลการประเมินและการตัดสินใจว่าการใช้ข้อมูลเป็นไปอย่างเหมาะสมและสอดคล้องกับหลักความได้สัดส่วน (proportionality)
- ระบุเหตุผลประกอบการตัดสินใจอย่างละเอียด

4. เอกสารแนบและหลักฐาน

- แนบเอกสารสนับสนุน เช่น บันทึกการประชุม รายงานการวิเคราะห์ความเสี่ยง
- บันทึกการตรวจสอบหรือการอนุมัติจากผู้มีอำนาจ

5. ความรับผิดชอบและการทบทวน

- ระบุผู้รับผิดชอบในการจัดทำและทบทวน LIA
- กำหนดรอบระยะเวลาการทบทวนเอกสารและการอัปเดต

6. ลงชื่อรับรอง

- ลายมือชื่อผู้จัดทำและผู้อนุมัติ พร้อมวันที่

หมายเหตุ: เอกสารนี้สามารถใช้เป็นหลักฐานแสดงให้เห็นถึงกระบวนการและแนวทางการประเมิน รวมทั้งการตัดสินใจที่ชัดเจนและตรวจสอบได้ในองค์กร

6.10.4 มีการจัดทำเป็นเอกสาร LIA เพื่อให้สามารถตรวจสอบได้ถึงการใช้นโยบายการประเมินและการตัดสินใจ

สิ่งที่ต้องทำ: มีการจัดทำ LIA ก่อนเริ่ม

- หลักฐาน: นโยบายหรือแนวปฏิบัติและกระบวนการเกี่ยวกับการประเมิน Legitimate Interest Assessment (LIA) รายงานการประชุม
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

นโยบายและแนวปฏิบัติการประเมินผลประโยชน์โดยชอบด้วยกฎหมาย

(Legitimate Interest Assessment: LIA)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและกระบวนการในการดำเนินการประเมินผลประโยชน์โดยชอบด้วยกฎหมาย ก่อนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าการดำเนินการเป็นไปตามหลักความ ได้สัดส่วนและคุ้มครองสิทธิของเจ้าของข้อมูล

2. ขอบเขต

ครอบคลุมการประเมินทุกกรณีที่ต้องใช้ฐานทางกฎหมายตามมาตรา 24 (5) พ.ร.บ. คุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562

3. กระบวนการดำเนินการ

- ระบุวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล
- วิเคราะห์และชั่งน้ำหนักผลประโยชน์ขององค์กรเทียบกับผลกระทบต่อเจ้าของข้อมูล
- พิจารณาผลกระทบต่อกลุ่มเปราะบาง เช่น ผู้เยาว์ ผู้พิการ
- กำหนดมาตรการลดผลกระทบเชิงลบที่อาจเกิดขึ้น
- บันทึกผลการประเมินและการตัดสินใจในรายงาน LIA ก่อนเริ่มดำเนินการ
- จัดเก็บเอกสารประเมินและรายงานไว้สำหรับตรวจสอบภายในและภายนอก

4. ความรับผิดชอบ

ระบุผู้รับผิดชอบในการจัดทำและทบทวน LIA พร้อมกำหนดช่วงเวลาทบทวนอย่างสม่ำเสมอ ตัวอย่างรายงานการประชุมการพิจารณา Legitimate Interest Assessment (LIA)

วันที่: [วัน/เดือน/ปี]

เวลา: [เวลา]

สถานที่: [สถานที่]

ผู้เข้าร่วม: [รายชื่อผู้เข้าร่วม]

วาระการประชุม

- พิจารณาการใช้ฐานทางกฎหมาย Legitimate Interest
- รายงานผลการประเมิน LIA
- ตัดสินใจและกำหนดมาตรการเพิ่มเติม (ถ้ามี)

สรุปการประชุม

- อธิบายการวิเคราะห์และชั่งน้ำหนักผลประโยชน์ขององค์กรเทียบกับสิทธิและเสรีภาพของเจ้าของ ข้อมูล
- รับรองว่าได้พิจารณาผลกระทบต่อกลุ่มเปราะบางและกำหนดมาตรการลดผลกระทบแล้ว
- ตกลงให้ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลตาม LIA ที่จัดทำไว้
- กำหนดผู้รับผิดชอบติดตามและทบทวน LIA ในอนาคต

ลายเซ็น: _____

[ชื่อผู้จัดทำ]

[ชื่อผู้อนุมัติ]

6.10.5 มีการทบทวน LIA อย่างสม่ำเสมอ โดยเฉพาะในกรณีที่มีความเปลี่ยนแปลงเกี่ยวกับกิจกรรมการประมวลผลที่อาจกระทบต่อผลการประเมิน

สิ่งที่ต้องทำ: มีการทบทวน LIA อย่างสม่ำเสมอ

หลักฐาน: หลักฐานการทบทวนการประเมิน LIA

สภาพบังคับ: กฎหมายไม่ได้กำหนด

หลักฐานการทบทวนการประเมิน Legitimate Interest Assessment (LIA)

1. รายงานการทบทวน LIA

- รายงานสรุปผลการทบทวน LIA ที่แสดงวันที่ทบทวน ผู้ทบทวน และสาเหตุการทบทวน (เช่น มีการเปลี่ยนแปลงกิจกรรมการประมวลผล)
- รายละเอียดการวิเคราะห์ผลกระทบที่อาจเปลี่ยนแปลงจากการทบทวน
- ข้อเสนอแนะหรือมาตรการแก้ไข (ถ้ามี)

2. บันทึกการประชุมทบทวน LIA

- รายงานหรือบันทึกการประชุมที่มีการพิจารณาและอนุมัติผลการทบทวน LIA
- ลายเซ็นของผู้มีอำนาจรับรอง

3. เอกสารแนวปฏิบัติการทบทวน LIA

- นโยบายหรือคู่มือภายในที่กำหนดช่วงเวลาการทบทวน LIA (เช่น ทุก 1-2 ปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ)
- ขั้นตอนการแจ้งเตือนและติดตามการทบทวน

4. ตัวอย่างเอกสารอ้างอิง

- ไฟล์รายงานทบทวน LIA ที่มีการแก้ไขล่าสุด
- อีเมลหรือเอกสารที่แสดงการติดตามการทบทวน

บทที่ 8

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DPA และ DSA)

การจัดทำและบริหารข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) และข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement: DSA) ถือเป็นกลไกสำคัญในการสร้างความมั่นใจว่าการจัดการข้อมูลส่วนบุคคลขององค์กรเป็นไปอย่างปลอดภัย ถูกต้อง และสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) รวมถึงมาตรฐานสากลอื่น ๆ ที่เกี่ยวข้อง การทำข้อตกลงเหล่านี้ช่วยกำหนดขอบเขต หน้าที่ และความรับผิดชอบของทุกฝ่ายที่เกี่ยวข้องกับการประมวลผลหรือแบ่งปันข้อมูลส่วนบุคคล ซึ่งเป็นองค์ประกอบสำคัญของหลักการความรับผิดชอบ (Accountability) และการปฏิบัติตามข้อกำหนดทางกฎหมาย ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) เป็นเอกสารที่จัดทำขึ้นระหว่างเจ้าของข้อมูลหรือผู้ควบคุมข้อมูล (Data Controller) กับผู้ประมวลผลข้อมูล (Data Processor) เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ประมวลผลในการจัดเก็บ ใช้ และปกป้องข้อมูลส่วนบุคคลอย่างถูกต้องตามวัตถุประสงค์ที่กำหนด รวมถึงระบุข้อกำหนดด้านความปลอดภัย การจัดการความเสี่ยง การแจ้งเหตุละเมิดข้อมูล และการสนับสนุนการใช้สิทธิของเจ้าของข้อมูล DPA ยังช่วยให้ผู้ควบคุมข้อมูลสามารถตรวจสอบและติดตามการปฏิบัติตาม PDPA ของผู้ประมวลผลได้อย่างชัดเจน ลดความเสี่ยงจากการละเมิดข้อมูลและข้อกำหนดทางกฎหมาย

ในขณะที่ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA) จะมุ่งเน้นไปที่การแลกเปลี่ยนหรือส่งต่อข้อมูลระหว่างหน่วยงาน องค์กร หรือภาคส่วนต่าง ๆ โดยกำหนดวัตถุประสงค์ของการแบ่งปัน ขอบเขตของข้อมูล วิธีการจัดการและปกป้องข้อมูล เงื่อนไขในการเข้าถึง การเก็บรักษา ระยะเวลาการใช้ และข้อจำกัดในการเปิดเผยต่อบุคคลภายนอก DSA จึงเป็นเครื่องมือสำคัญในการป้องกันความสับสนหรือความเสี่ยงจากการใช้ข้อมูลผิดวัตถุประสงค์ และช่วยให้การแบ่งปันข้อมูลเป็นไปอย่างโปร่งใส ตรวจสอบได้ และปฏิบัติตาม PDPA อย่างครบถ้วน

การจัดทำ DPA และ DSA อย่างรัดกุมยังเกี่ยวข้องกับกระบวนการทบทวนเอกสาร การปรับปรุงข้อตกลงตามกฎหมายใหม่หรือแนวทางสากล และการอบรมบุคลากรที่เกี่ยวข้อง เพื่อให้แน่ใจว่าทุกฝ่ายเข้าใจบทบาท หน้าที่ และความรับผิดชอบของตนอย่างชัดเจน การทำบันทึกและจัดเก็บหลักฐานของข้อตกลงเหล่านี้จึงเป็นสิ่งสำคัญสำหรับการตรวจสอบภายในและภายนอกองค์กร

โดยรวมแล้ว การบริหาร DPA และ DSA อย่างมีประสิทธิภาพไม่เพียงแต่ช่วยให้การประมวลผลและแบ่งปันข้อมูลส่วนบุคคลเป็นไปอย่างปลอดภัย ถูกต้อง และสอดคล้องกับกฎหมาย แต่ยังสร้างความเชื่อมั่นแก่เจ้าของข้อมูลและผู้มีส่วนได้ส่วนเสีย ทำให้องค์กรสามารถปฏิบัติงานด้านข้อมูลส่วนบุคคลได้อย่างมั่นคง ยั่งยืน และเป็นไปตามมาตรฐานความเป็นส่วนตัวระดับสากล

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้ คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
1. การกำหนด ขอบเขตและ วัตถุประสงค์ (Scope & Purpose)	ระบุขอบเขตการประมวลผล/ แบ่งปันข้อมูล และ วัตถุประสงค์ที่ชัดเจน	ข้อตกลง DPA/DSA (Data Processing / Sharing Agreement), เอกสารแนบ หรือประกาศขอบเขต (Annexes / Scope Documents)	ครอบคลุมทุก ข้อมูลและ กระบวนการ ใช้ งานจริงและ ตรวจสอบได้
2. การระบุบทบาท และความรับผิดชอบ (Roles & Responsibilities)	กำหนดบทบาทของผู้ควบคุม ข้อมูล (Data Controller), ผู้ ประมวลผลข้อมูล (Data Processor) และผู้แบ่งปัน ข้อมูล (Data Sharing Entity)	แผนผังองค์กร (Organization Chart), ตารางบทบาท (Role Matrix), ข้อตกลง DPA/DSA	ระบุบทบาท ชัดเจน สอดคล้องกับ PDPA และแนว ปฏิบัติ
3. การระบุฐานทาง กฎหมาย (Legal Basis)	ระบุฐานทางกฎหมายของการ ประมวลผล/แบ่งปันข้อมูล เช่น ความยินยอม, ข้อผูกพัน ตามสัญญา, ความจำเป็นตามกฎหมาย	บันทึกฐานทางกฎหมาย (Legal Basis Register), ข้อกำหนดใน DPA/DSA (Clause), บันทึกคำชี้แจง (Memo)	ครบถ้วนและ สอดคล้องกับ วัตถุประสงค์ ของการ ประมวลผล/ แบ่งปัน
4. การจำกัดการใช้ และการเปิดเผย ข้อมูล (Use & Disclosure Restrictions)	กำหนดให้ข้อมูลถูกใช้ตาม วัตถุประสงค์ที่ตกลงและห้าม เปิดเผยบุคคลภายนอกโดย ไม่ได้รับอนุญาต	ข้อกำหนดใน DPA/DSA (Clause), ข้อตกลงไม่เปิดเผย ข้อมูล (Non-Disclosure Agreement – NDA), นโยบายภายในองค์กร (Policy)	ครบถ้วนและ สามารถ ตรวจสอบได้ จริง

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้ คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
5. การจัดการความปลอดภัยของข้อมูล (Security Measures)	กำหนดมาตรการรักษาความปลอดภัย การเข้ารหัส (Encryption), การควบคุมการเข้าถึง (Access Control) และมาตรการป้องกันการละเมิดข้อมูล	เอกสารแนบด้านความปลอดภัย (Security Annex), นโยบายความปลอดภัย (Policy), รายการตรวจสอบ (Checklist), รายงานตรวจสอบ (Audit Report)	มีข้อกำหนดครบถ้วน ครอบคลุมทุกประเภทข้อมูล
6. การแจ้งเหตุละเมิดข้อมูล (Data Breach Notification)	ระบุขั้นตอน วิธีการ และระยะเวลาในการแจ้งเหตุละเมิดข้อมูล	เอกสารขั้นตอนตอบสนองเหตุละเมิด (Incident Response Procedure), บันทึกการแจ้งเหตุละเมิด (Breach Notification Log)	ขั้นตอนชัดเจน ตรวจสอบได้ และสอดคล้องกับ PDPA
7. การสนับสนุนการใช้สิทธิของเจ้าของข้อมูล (Support for Data Subject Rights)	ระบุหน้าที่ของผู้ประมวลผล/ผู้แบ่งปันในการสนับสนุนเจ้าของข้อมูล เช่น การเข้าถึง แก้ไข ลบ	SOP / คู่มือปฏิบัติ (Standard Operating Procedure), บันทึกคำขอสิทธิ (Record of Data Subject Request), ข้อตกลง DPA/DSA (Clause)	ครบถ้วนและตรวจสอบได้จริง
8. การจัดทำบันทึกและรายงาน (Record-Keeping & Reporting)	จัดเก็บบันทึกการประมวลผล/แบ่งปันข้อมูลและจัดทำรายงานสำหรับตรวจสอบ Compliance	บันทึกการประมวลผล (Processing Log), บันทึกการแบ่งปันข้อมูล (Sharing Log), รายงานการปฏิบัติตามกฎหมาย (Compliance Report)	มีระบบจัดเก็บและรายงานครบถ้วน ตรวจสอบย้อนหลังได้
9. การทบทวนและปรับปรุงข้อตกลง (Review & Update)	ทบทวนและปรับปรุง DPA/DSA อย่างต่อเนื่องตามกฎหมายใหม่ แนวทางสากล หรือการเปลี่ยนแปลงในกระบวนการ	บันทึกเวอร์ชันเอกสาร (Version Control), บันทึกการประชุม (Meeting Minutes), บันทึกการแก้ไข (Memo)	มีหลักฐานปรับปรุงต่อเนื่อง แสดงการอัปเดตตามกฎหมายหรือแนวทางใหม่

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
10. การอบรมและสร้างความตระหนักรู้ (Training & Awareness)	อบรมบุคลากรเกี่ยวกับบทบาท หน้าที่ และแนวทางปฏิบัติตาม DPA/DSA	แผนอบรม (Training Plan), สไลด์นำเสนอ (Presentation Slides), รายชื่อผู้เข้าร่วม (Attendance Sheet), แบบสอบถามประเมินผล (Evaluation Form)	บุคลากรทุกระดับได้รับการอบรม มีหลักฐานชัดเจน และสามารถปฏิบัติได้จริง
11. การตรวจสอบภายใน (Internal Audit)	ตรวจสอบว่าการปฏิบัติตาม DPA/DSA ถูกนำไปใช้จริง และสอดคล้องกับ PDPA	รายงานตรวจสอบภายใน (Internal Audit Report), แบบฟอร์มตรวจสอบ Compliance (Compliance Checklist), บันทึกการตรวจสอบ (Audit Log)	มีรายงานตรวจสอบ พร้อมข้อเสนอแนะและหลักฐานการปฏิบัติจริง
12. การเชื่อมโยงกับการบริหารความเสี่ยง (Risk Management Linkage)	ผูกโยง DPA/DSA กับระบบบริหารความเสี่ยงองค์กร เพื่อประเมินและจัดการความเสี่ยงด้านข้อมูล	ทะเบียนความเสี่ยง (Risk Register), รายงานประเมินความเสี่ยง (Risk Assessment Report), รายงานตรวจสอบย้อนหลัง (Audit Trail)	มีหลักฐานเชื่อมโยงความเสี่ยงและติดตามอย่างต่อเนื่อง
13. การจัดการผู้ประมวลผล/ผู้แบ่งปันย่อย (Sub - processor/Sub - entity Management)	กำหนดเงื่อนไขการใช้ผู้ประมวลผล/ผู้แบ่งปันย่อยให้สอดคล้องกับ DPA/DSA	รายชื่อผู้ประมวลผล/ผู้แบ่งปันย่อย (Sub-processor List), ข้อตกลงย่อย (Sub-agreements), บันทึกการอนุมัติ (Approval Records)	ระบุครบถ้วน มีหลักฐานการอนุมัติ และตรวจสอบการปฏิบัติได้จริง
14. การกำหนดบทลงโทษ/ข้อวินัย (Sanctions & Disciplinary Measures)	ระบุผลทางกฎหมายหรือข้อวินัยสำหรับการละเมิด DPA/DSA	ข้อกำหนดใน DPA/DSA (Clause), นโยบายการลงโทษ (Policy on Sanctions), บันทึกการลงโทษ (Disciplinary Records)	ระบุครบถ้วน ใช้บังคับได้จริง และตรวจสอบย้อนหลังได้

การจัดทำเอกสารตามเกณฑ์มาตรฐาน

7.1 องค์กรมีนโยบายและแนวปฏิบัติเพื่อกำกับการแบ่งปันข้อมูลส่วนบุคคลอย่างเหมาะสม (Data Sharing Policies and Procedures)

7.1.1 องค์กรมีการฝึกอบรมพนักงานทุกคนที่เกี่ยวข้องกับการแบ่งปันข้อมูลส่วนบุคคลอย่างเพียงพอและเหมาะสม และมีการสร้างความตระหนักถึงความรับผิดชอบของพนักงานต่อหน้าที่ดังกล่าว รวมถึงมีการทบทวนการฝึกอบรมนี้อย่างเหมาะสม (Refresher Training)

สิ่งที่ต้องทำ: การอบรมพนักงานที่เกี่ยวข้องกับการแบ่งปันข้อมูลส่วนบุคคลอย่างเพียงพอ และมีการทบทวนการอบรมอย่างเหมาะสม

หลักฐาน: หลักฐานในการฝึกอบรมพนักงาน เช่น รายชื่อผู้เข้าร่วมอบรม ผลทดสอบการฝึกอบรม หลักฐานการทบทวนการฝึกอบรมพนักงาน เช่น รายชื่อผู้เข้าร่วมอบรม ผลทดสอบการฝึกอบรม

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (7)

โทษทางปกครอง: มาตรา 86 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

หลักการฝึกอบรมและทบทวนการฝึกอบรมพนักงานเกี่ยวกับการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing)

1. รายชื่อผู้เข้าร่วมอบรม

- รายชื่อพนักงานที่เข้ารับการฝึกอบรม พร้อมระบุวันที่และหัวข้อการอบรม
- ลายเซ็นหรือการยืนยันการเข้าร่วมอบรมของพนักงานแต่ละคน

2. ผลทดสอบหลังการอบรม

- เอกสารแสดงผลการทดสอบความรู้หรือแบบประเมินหลังการอบรม (ถ้ามี)
- สรุปผลคะแนน หรือข้อมูลแสดงความเข้าใจของพนักงานต่อเนื้อหาที่อบรม

3. รายงานสรุปการอบรม

- รายงานหรือบันทึกการอบรมที่ระบุวัตถุประสงค์ เนื้อหา ผู้บรรยาย และผลการอบรม
- เอกสารประกอบการอบรม เช่น สไลด์, คู่มือ, วิดีโอที่ใช้ในการฝึกอบรม

4. หลักฐานการทบทวนการฝึกอบรม (Refresher Training)

- รายชื่อและวันที่ของการอบรมทบทวน (refresh) สำหรับพนักงานเดิม
- ผลการประเมินหรือทดสอบหลังอบรมทบทวน
- รายงานหรือบันทึกการทบทวนที่ระบุว่ามีการปรับปรุงเนื้อหาเพื่อความเหมาะสมตามสถานการณ์ปัจจุบัน

5. นโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการแบ่งปันข้อมูลส่วนบุคคล

- เอกสารนโยบายองค์กรเกี่ยวกับการแบ่งปันข้อมูลส่วนบุคคลที่ระบุความรับผิดชอบของพนักงาน
- แนวทางปฏิบัติที่พนักงานต้องปฏิบัติตาม เพื่อรักษาความมั่นคงและความเป็นส่วนตัวของข้อมูล

6. บันทึกการติดตามและตรวจสอบ

- เอกสารแสดงการติดตามความคืบหน้าการอบรมและการทบทวนอย่างสม่ำเสมอ
- รายงานการประเมินความรู้และความตระหนักของพนักงานในแต่ละรอบการอบรม

7.1.2 องค์กรมีการประเมินความเสี่ยงในการแบ่งปันข้อมูลส่วนบุคคลผ่าน DPIA หรือมีการประเมินรูปแบบอื่น เพื่อประเมินความถูกต้องตามกฎหมาย ประโยชน์ และความเสี่ยงของการแบ่งปันหรือการเปิดเผยข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: มีการประเมินครบถ้วน

หลักฐาน: หลักฐานการทำการประเมินความเสี่ยงในการแบ่งปันข้อมูลส่วนบุคคล เช่น DPIA

สภาพบังคับ: กฎหมายไม่ได้กำหนด

หลักฐานการประเมินความเสี่ยงในการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Risk Assessment)

1. รายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูล (Data Protection Impact Assessment: DPIA)

- เอกสารรายงาน DPIA ที่แสดงรายละเอียดการประเมินความเสี่ยงของการแบ่งปันข้อมูล
- วัตถุประสงค์ประสงค์ของการแบ่งปันข้อมูล ขอบเขตของข้อมูลที่แบ่งปัน และผู้เกี่ยวข้อง
- การวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นกับสิทธิและเสรีภาพของเจ้าของข้อมูล
- มาตรการบรรเทาความเสี่ยงที่นำมาใช้เพื่อปกป้องข้อมูลส่วนบุคคล

2. เอกสารการประเมินความเสี่ยงในรูปแบบอื่น (ถ้ามี)

- แบบฟอร์มหรือรายงานการวิเคราะห์ความเสี่ยง (Risk Assessment) ที่จัดทำสำหรับการแบ่งปันข้อมูล
- รายงานการตรวจสอบความสอดคล้องทางกฎหมายและข้อกำหนดที่เกี่ยวข้อง
- บันทึกการพิจารณาและอนุมัติจากผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง

3. กระบวนการและนโยบายที่เกี่ยวข้อง

- นโยบายหรือแนวปฏิบัติที่ระบุวิธีการประเมินความเสี่ยงก่อนการแบ่งปันข้อมูล
- คู่มือหรือเอกสารแนะนำสำหรับผู้ปฏิบัติงานในการทำ DPIA หรือประเมินความเสี่ยง

4. บันทึกการประชุมหรือการตัดสินใจ

- รายงานหรือบันทึกการประชุมที่แสดงการทบทวนผลการประเมินความเสี่ยง
- เอกสารแสดงการตัดสินใจดำเนินการแบ่งปันข้อมูลโดยพิจารณาจากผลการประเมิน

ตัวอย่างรายงาน DPIA (Data Protection Impact Assessment) สำหรับการแบ่งปันข้อมูลส่วนบุคคล

1. ข้อมูลทั่วไป

ชื่อกิจกรรม: การแบ่งปันข้อมูลส่วนบุคคลกับหน่วยงานพันธมิตร

วันที่จัดทำรายงาน: 1 มิถุนายน 2568

ผู้รับผิดชอบ: ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

วัตถุประสงค์ของการแบ่งปันข้อมูล: เพื่อปรับปรุงการให้บริการและประสานงานกับหน่วยงานพันธมิตร

2. ข้อมูลส่วนบุคคลที่แบ่งปัน

- รายละเอียดข้อมูล: ชื่อ-นามสกุล, เบอร์โทรศัพท์, อีเมล, ข้อมูลการให้บริการ
- จำนวนข้อมูล: ข้อมูลของลูกค้า 1,000 คน

3. การประเมินความเสี่ยง

ความเสี่ยงที่อาจเกิดขึ้น	ผลกระทบที่อาจเกิดขึ้น	ความรุนแรง (สูง/กลาง/ต่ำ)	มาตรการบรรเทาความเสี่ยง
ข้อมูลรั่วไหลระหว่างการส่งข้อมูล	เจ้าของข้อมูลเสียหายทางชื่อเสียงและความเป็นส่วนตัว	สูง	ใช้การเข้ารหัสข้อมูลระหว่างส่งข้อมูล (Encryption)
การใช้ข้อมูลโดยไม่ได้รับอนุญาต	การละเมิดสิทธิส่วนบุคคล	สูง	ทำสัญญาความลับกับหน่วยงานพันธมิตรและตรวจสอบสิทธิ์เข้าถึง
การจัดเก็บข้อมูลไม่ปลอดภัย	ข้อมูลถูกโจรกรรมหรือเข้าถึงโดยไม่ได้รับอนุญาต	กลาง	จัดเก็บข้อมูลในระบบที่มีระบบรักษาความปลอดภัยสูง

4. สรุปและข้อเสนอแนะ

- การแบ่งปันข้อมูลเป็นไปตามวัตถุประสงค์ที่ชัดเจน
- ได้ดำเนินการมาตรการรักษาความปลอดภัยที่เหมาะสมและเพียงพอ
- แนะนำให้มีการทบทวนการประเมินนี้ทุก 6 เดือน หรือเมื่อมีกระบวนการเปลี่ยนแปลง

5. ลายเซ็นผู้รับผิดชอบ

ผู้จัดทำ: _____

วันที่: _____

ผู้อนุมัติ: _____

วันที่: _____

หมายเลข	หัวข้อประเมิน	รายละเอียด / คำถาม	คะแนน ความ รุนแรง (1-5)	คะแนน ความ น่าจะเป็น (1-5)	คะแนน รวม (คูณ)	มาตรการที่มีอยู่ / ข้อเสนอแนะ
1	ประเภทของข้อมูลที่แบ่งปัน	ข้อมูลส่วนบุคคลชนิดใดบ้างที่จะแบ่งปัน				
2	วิธีการแบ่งปันข้อมูล	ใช้วิธีการอะไร (เช่น อีเมล, แชร์รหัส, FTP, ปลอดภัย)				
3	ความเสี่ยงด้านความปลอดภัย	มีความเสี่ยงด้านความปลอดภัยอะไรบ้าง				
4	ผลกระทบต่อเจ้าของข้อมูล	หากข้อมูลรั่วไหลจะมีผลกระทบอย่างไร				
5	มาตรการควบคุมความเสี่ยง	มีมาตรการใดในการป้องกันความเสี่ยง				
6	การกำกับดูแลและตรวจสอบ	มีระบบตรวจสอบการปฏิบัติตามมาตรการหรือไม่				
7	การขอความยินยอม	ได้รับความยินยอมจากเจ้าของข้อมูลหรือไม่				

คำอธิบายคะแนน

ความรุนแรง: 1 = ต่ำสุด, 5 = สูงสุด

ความน่าจะเป็น: 1 = ไม่ค่อยเกิดขึ้น, 5 = เกิดขึ้นบ่อย

7.1.3 องค์กรมีการจัดทำเอกสารเพื่อบันทึกการตัดสินใจ (document all sharing decisions) เพื่อวัตถุประสงค์ในการตรวจสอบและกำกับ และองค์กรมีการสอบทานอย่างสม่ำเสมอ

สิ่งที่ต้องทำ: มีการจัดทำเอกสารเพื่อบันทึกการตัดสินใจ โดยผู้บริหารระดับสูง DPO หรือพนักงานที่มีส่วนเกี่ยวข้องขององค์กรครบถ้วน

หลักฐาน: หลักฐานการสอบทานการตัดสินใจแบ่งปันข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารบันทึกการตัดสินใจแบ่งปันข้อมูลส่วนบุคคล

องค์กร: _____

วันที่: _____

ผู้บันทึก: _____

ตำแหน่ง: _____

1. รายละเอียดการแบ่งปันข้อมูลส่วนบุคคล

วัตถุประสงค์ของการแบ่งปันข้อมูล:

ประเภทข้อมูลส่วนบุคคลที่จะแบ่งปัน:

หน่วยงาน/บุคคลที่จะได้รับข้อมูล:

2. การประเมินความเสี่ยงและข้อกังวล

ความเสี่ยงที่เกี่ยวข้อง:

มาตรการที่ใช้ในการควบคุมและลดความเสี่ยง:

3. การตัดสินใจแบ่งปันข้อมูล

การตัดสินใจ

() อนุมัติให้แบ่งปันข้อมูล

() ไม่อนุมัติให้แบ่งปันข้อมูล

() อนุมัติภายใต้เงื่อนไข (โปรดระบุ) _____

เหตุผลในการตัดสินใจ

4. ผู้มีอำนาจตัดสินใจลงนาม

ชื่อ-นามสกุล	ตำแหน่ง	ลายเซ็น	วันที่
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

หลักฐานการสอบทานการตัดสินใจแบ่งปันข้อมูลส่วนบุคคล

วันที่สอบทาน: _____

ผู้สอบทาน: _____

ตำแหน่ง: _____

รายละเอียดการสอบทาน

ข้อมูลที่สอบทาน:

ผลการสอบทาน:

() ผ่านตามเกณฑ์

() พบข้อบกพร่อง (โปรดระบุ) _____

ข้อเสนอแนะ/มาตรการปรับปรุง:

ลายเซ็นผู้สอบทาน

(ชื่อ-นามสกุล)

วันที่ _____

7.1.3 องค์กรมีการจัดทำเอกสารเพื่อบันทึกการตัดสินใจ (document all sharing decisions) เพื่อวัตถุประสงค์ในการตรวจสอบและกำกับ และองค์กรมีการสอบทานอย่างสม่ำเสมอ

สิ่งที่ต้องทำ: มีการจัดทำเอกสารเพื่อบันทึกการตัดสินใจ โดยผู้บริหารระดับสูง DPO หรือพนักงานที่มีส่วนเกี่ยวข้องกับองค์กรครบถ้วน

หลักฐาน: หลักฐานการสอบทานการตัดสินใจแบ่งปันข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารบันทึกการตัดสินใจแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Decision Log)

องค์กร: _____

วันที่บันทึก: _____

ผู้บันทึก: _____

ตำแหน่ง: _____

1. รายละเอียดการแบ่งปันข้อมูล

วัตถุประสงค์ของการแบ่งปันข้อมูล:

ประเภทข้อมูลส่วนบุคคลที่แบ่งปัน:

ผู้รับข้อมูล (หน่วยงาน/บุคคลภายนอก):

2. การประเมินและการตัดสินใจ

การประเมินความเสี่ยงหรือการตรวจสอบที่ดำเนินการ:

ผลการตัดสินใจแบ่งปันข้อมูล:

() อนุมัติ

() ไม่อนุมัติ

() อนุมัติภายใต้เงื่อนไข (โปรดระบุ) _____

เหตุผลประกอบการตัดสินใจ:

3. การลงนามรับรอง

ชื่อผู้ลงนาม	ตำแหน่ง	ลายเซ็น	วันที่
_____	_____	_____	_____
_____	_____	_____	_____

ตัวอย่างหลักฐานการสอบทานการตัดสินใจแบ่งปันข้อมูลส่วนบุคคล (Review Record)

วันที่สอบทาน: _____

ผู้สอบทาน: _____

ตำแหน่ง: _____

รายละเอียดการสอบทาน

ข้อมูลหรือรายการที่สอบทาน:

ผลการสอบทาน:

() ผ่าน

() มีข้อบกพร่อง (โปรดระบุ) _____

ข้อเสนอแนะและมาตรการปรับปรุง (ถ้ามี):

ลายเซ็นผู้สอบทาน

(ชื่อ-นามสกุล)

วันที่ ____

7.1.4 องค์กรมีนโยบาย แนวปฏิบัติ และคำแนะนำที่ชัดเจนเกี่ยวกับการแบ่งปันข้อมูลส่วนบุคคลอย่างเหมาะสม รวมถึงการระบุผู้มีอำนาจในการตัดสินใจเกี่ยวกับการแบ่งปันข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการแบ่งปันอย่างเป็นระบบ (systematic data sharing) หรือการเปิดเผยเพียงครั้งเดียว (one-off disclosures)

สิ่งที่ต้องทำ: มีนโยบายและแนวปฏิบัติเกี่ยวกับการแบ่งปันข้อมูลส่วนบุคคล ทั้งกรณีการแบ่งปันอย่างเป็นระบบ (systematic data sharing) และการเปิดเผยเพียงครั้งเดียว (one-off disclosures)

หลักฐาน: นโยบายและแนวปฏิบัติเกี่ยวกับการแบ่งปันข้อมูลส่วนบุคคล กรณีการแบ่งปันอย่างเป็นระบบ (systematic data sharing) และการเปิดเผยเพียงครั้งเดียว (one-off disclosures)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

นโยบายและแนวปฏิบัติในการแบ่งปันข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและหลักเกณฑ์ในการแบ่งปันข้อมูลส่วนบุคคลขององค์กรอย่างเหมาะสม ปลอดภัย และสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

2. ขอบเขต

- นโยบายนี้ครอบคลุมการแบ่งปันข้อมูลส่วนบุคคลทั้งในรูปแบบ
- การแบ่งปันข้อมูลอย่างเป็นระบบ (Systematic Data Sharing)
- การเปิดเผยข้อมูลเพียงครั้งเดียว (One-off Disclosures)

3. คำนิยาม

- การแบ่งปันข้อมูลอย่างเป็นระบบ หมายถึง การแบ่งปันข้อมูลส่วนบุคคลที่เกิดขึ้นอย่างต่อเนื่อง มีระบบและกระบวนการที่ชัดเจน เช่น การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภายในองค์กรหรือหน่วยงานพันธมิตร
- การเปิดเผยข้อมูลเพียงครั้งเดียว หมายถึง การแบ่งปันข้อมูลส่วนบุคคลที่เกิดขึ้นเป็นครั้งคราว หรือเป็นกรณีพิเศษ ไม่มีการทำซ้ำในระยะยาว

4. แนวปฏิบัติในการแบ่งปันข้อมูลส่วนบุคคล

4.1 การแบ่งปันข้อมูลอย่างเป็นระบบ

- ต้องมีข้อตกลงหรือสัญญาที่ชัดเจนระหว่างผู้ควบคุมข้อมูลและผู้รับข้อมูล
- กำหนดขอบเขตข้อมูลที่จะถูกแบ่งปันอย่างชัดเจนและจำกัดไว้เฉพาะข้อมูลที่จำเป็น
- มีมาตรการรักษาความปลอดภัยของข้อมูลในทุกขั้นตอน
- มีการตรวจสอบและทบทวนการแบ่งปันข้อมูลเป็นระยะอย่างสม่ำเสมอ
- มีการจัดทำบันทึกการแบ่งปันข้อมูล (Data Sharing Logs) สำหรับตรวจสอบย้อนหลัง

4.2 การเปิดเผยข้อมูลเพียงครั้งเดียว

- ต้องมีการประเมินความจำเป็นและความเหมาะสมก่อนเปิดเผยข้อมูล
- การเปิดเผยต้องได้รับความยินยอมจากเจ้าของข้อมูล หรือมีเหตุผลตามกฎหมายที่ชัดเจน
- มีการบันทึกเหตุผลและรายละเอียดของการเปิดเผยข้อมูลในเอกสารที่สามารถตรวจสอบได้
- ผู้มีอำนาจในการตัดสินใจการเปิดเผยข้อมูลต้องเป็นผู้ที่ได้รับมอบหมายอย่างชัดเจน เช่น DPO หรือผู้บริหารระดับสูง

5. ผู้มีอำนาจในการตัดสินใจ

- กำหนดให้ **เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)** และ/หรือ **ผู้บริหารระดับสูง** มีอำนาจและความรับผิดชอบในการตัดสินใจเกี่ยวกับการแบ่งปันข้อมูลส่วนบุคคลทั้งในกรณีแบ่งปันอย่างเป็นระบบและการเปิดเผยเพียงครั้งเดียว
- ผู้มีอำนาจต้องตรวจสอบให้แน่ใจว่าการแบ่งปันข้อมูลเป็นไปตามนโยบายนี้และกฎหมายที่เกี่ยวข้อง

6. การฝึกอบรมและสร้างความตระหนัก

องค์กรจัดให้มีการฝึกอบรมและสร้างความตระหนักแก่พนักงานเกี่ยวกับนโยบายนี้และความรับผิดชอบในการแบ่งปันข้อมูลส่วนบุคคลอย่างเหมาะสม

7. การทบทวนนโยบาย

นโยบายนี้จะได้รับการทบทวนและปรับปรุงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกี่ยวกับกฎหมายหรือกระบวนการแบ่งปันข้อมูล

7.2 ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreements) องค์กรมีการทบทวนข้อตกลงการแบ่งปันข้อมูลกับหน่วยงานที่มีการแบ่งปันข้อมูลส่วนบุคคลเป็นประจำ

7.2.1 มีการจัดทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคลกับหน่วยงานที่เกี่ยวข้องกับการแบ่งปันข้อมูลส่วนบุคคลขององค์กร และผู้บริหารระดับสูงลงนามในข้อตกลงนั้น

สิ่งที่ต้องทำ: มีการจัดทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคลครบถ้วนทุกหน่วยงาน

หลักฐาน: ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล ลงนามโดยผู้บริหารระดับสูงในองค์กร สภาพบังคับ: กฎหมายไม่ได้กำหนด

ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement – DSA)

1. คู่สัญญา

- หน่วยงานผู้ควบคุมข้อมูล: [ชื่อหน่วยงานขององค์กร]
- หน่วยงานผู้รับข้อมูล: [ชื่อหน่วยงานที่เกี่ยวข้อง]

2. วัตถุประสงค์ของการแบ่งปันข้อมูล

เพื่อแบ่งปันข้อมูลส่วนบุคคลที่จำเป็นต่อการปฏิบัติหน้าที่ร่วมกันอย่างถูกต้องตามกฎหมาย และปกป้องข้อมูลส่วนบุคคลของเจ้าของข้อมูล

3. ข้อมูลที่แบ่งปัน

รายละเอียดประเภทและขอบเขตของข้อมูลส่วนบุคคลที่จะแบ่งปัน เช่น ชื่อ-นามสกุล, เบอร์โทรศัพท์, ข้อมูลสุขภาพ ฯลฯ

4. ขอบเขตการใช้ข้อมูล

หน่วยงานผู้รับข้อมูลจะใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่ระบุในข้อตกลงนี้เท่านั้น และไม่อนุญาตให้เปิดเผยแก่บุคคลภายนอกโดยไม่ได้รับอนุญาต

5. การรักษาความปลอดภัยของข้อมูล

ทั้งสองฝ่ายต้องปฏิบัติตามมาตรการรักษาความปลอดภัยเพื่อป้องกันข้อมูลส่วนบุคคลจากการเข้าถึง ใช้ หรือเปิดเผยโดยไม่ได้รับอนุญาต

6. ระยะเวลาของข้อตกลง

ระบุระยะเวลาที่ข้อตกลงมีผลบังคับใช้ เช่น ตั้งแต่วันที่ xx/xx/xxxx ถึงวันที่ xx/xx/xxxx หรือจนกว่าจะมีการยกเลิกข้อตกลง

7. การทบทวนและยกเลิกข้อตกลง

ทั้งสองฝ่ายจะทบทวนข้อตกลงอย่างน้อยปีละครั้ง และสามารถยกเลิกข้อตกลงได้โดยแจ้งเป็นลายลักษณ์อักษรล่วงหน้าไม่น้อยกว่า 30 วัน

8. การลงนามรับรอง

เพื่อเป็นการรับรองและผูกพันตามข้อตกลงนี้

ฝ่าย	ชื่อผู้ลงนาม	ตำแหน่ง	ลายมือชื่อ	วันที่ลงนาม
หน่วยงานผู้ควบคุมข้อมูล	[ชื่อผู้บริหารระดับสูง]	[ตำแหน่ง]		/.../.....
หน่วยงานผู้รับข้อมูล	[ชื่อผู้บริหารระดับสูง]	[ตำแหน่ง]		/.../.....

แนวทางการใช้หลักฐาน

- เก็บรักษาข้อตกลงฉบับนี้ไว้ในรูปแบบเอกสารหรือไฟล์ดิจิทัล
- มีการจัดทำทะเบียนข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement Register) เพื่อบันทึกสถานะและวันที่ทบทวน
- จัดเตรียมเอกสารทบทวนข้อตกลงเป็นประจำตามข้อกำหนดในนโยบายองค์กร

7.2.2 ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement: DSA) มีรายละเอียดอย่างน้อย ดังนี้

- (1) บทบาทของฝ่ายต่าง ๆ ที่เกี่ยวข้องกับการแบ่งปันข้อมูลส่วนบุคคล
- (2) วัตถุประสงค์ของการแบ่งปันข้อมูลส่วนบุคคล
- (3) การแสดงทิศทางการไหลเวียนของข้อมูล และการประมวลผลข้อมูลส่วนบุคคลที่จะเกิดขึ้นในแต่ละขั้นตอน
- (4) การกำหนดมาตรฐานต่าง ๆ ที่เกี่ยวข้องกับการส่งหรือโอนข้อมูลส่วนบุคคล (โดยกำหนดค่าเริ่มต้นให้มีความเป็นส่วนตัวสูงสำหรับผู้เยาว์หรือกลุ่มเปราะบาง)

สิ่งที่ต้องทำ: มีรายละเอียดครบถ้วน

หลักฐาน: ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคลขององค์กร

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสาร Data Sharing Agreement (DSA)

Data Sharing Agreement (DSA)

ระหว่าง

บริษัท ABC จำกัด และ บริษัท XYZ จำกัด

1. บทนำ

ข้อตกลงฉบับนี้ทำขึ้นระหว่างบริษัท ABC จำกัด (“ผู้แบ่งปันข้อมูล”) และบริษัท XYZ จำกัด (“ผู้รับข้อมูล”) เพื่อกำหนดเงื่อนไขการแบ่งปันและการใช้ข้อมูลส่วนบุคคลอย่างเหมาะสมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. บทบาทของฝ่ายต่าง ๆ

ฝ่าย	บทบาทและหน้าที่หลัก
บริษัท ABC จำกัด	รวบรวมและแบ่งปันข้อมูลส่วนบุคคลของลูกค้า เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ เพื่อใช้ในการวิเคราะห์และพัฒนาบริการ
บริษัท XYZ จำกัด	รับข้อมูลจาก ABC เพื่อวิเคราะห์พฤติกรรมลูกค้าและส่งรายงานผลให้ ABC เพื่อใช้ในการปรับปรุงบริการ

3. วัตถุประสงค์การแบ่งปันข้อมูล

- เพื่อวิเคราะห์พฤติกรรมการซื้อสินค้าและบริการของลูกค้า
- เพื่อพัฒนาปรับปรุงบริการและการตลาดให้เหมาะสมกับกลุ่มเป้าหมาย
- เพื่อประมวลผลข้อมูลในเชิงสถิติโดยไม่ระบุตัวบุคคล (anonymous data) เพื่อวางแผนธุรกิจ

4. ข้อมูลที่แบ่งปัน

- ข้อมูลส่วนบุคคล เช่น ชื่อ, ที่อยู่, เบอร์โทรศัพท์, อายุ, เพศ
- ข้อมูลการทำธุรกรรม เช่น ประวัติการสั่งซื้อ, ความถี่การใช้บริการ
- ข้อมูลพฤติกรรมการใช้งาน เช่น เวลาการเข้าชมเว็บไซต์, ประเภทสินค้าโปรด

5. การไหลเวียนของข้อมูล (Data Flow)

แผนภาพ Data Flow Diagram (DFD)



คำอธิบายแผนภาพ

- บริษัท ABC รวบรวมข้อมูลลูกค้า
- ส่งข้อมูลอย่างปลอดภัยด้วยระบบเข้ารหัสไปยังบริษัท XYZ
- บริษัท XYZ วิเคราะห์ข้อมูลและส่งรายงานกลับให้ ABC

6. มาตรฐานความปลอดภัยข้อมูล

- ใช้การเข้ารหัสข้อมูลระหว่างการส่งข้อมูล (AES-256)
- กำหนดสิทธิ์เข้าถึงข้อมูลตามบทบาทหน้าที่
- บันทึกการเข้าถึงและการใช้ข้อมูลอย่างละเอียด
- มีมาตรการจัดการกรณีข้อมูลรั่วไหล

7. สิทธิของเจ้าของข้อมูล

- เจ้าของข้อมูลมีสิทธิขอเข้าถึง แก้ไข หรือลบข้อมูลของตน
- มีสิทธิขอระงับการใช้ข้อมูลในกรณีที่เห็นว่ามีความเสี่ยงหรือไม่เหมาะสม
- บริษัททั้งสองฝ่ายจะร่วมกันดำเนินการตามคำขอของเจ้าของข้อมูลโดยเร็ว

8. การบันทึกและตรวจสอบ

- มีการจัดทำเอกสารบันทึกการแบ่งปันและใช้ข้อมูลอย่างชัดเจน

- ผู้บริหารระดับสูงและ DPO รับผิดชอบในการตรวจสอบและทบทวนข้อตกลงนี้อย่างน้อยปีละ 1 ครั้ง
- มีการจัดทำรายงานสรุปผลการใช้ข้อมูลเพื่อตรวจสอบความถูกต้อง

9. การยกเลิกข้อตกลง

ข้อตกลงนี้สามารถยกเลิกได้ด้วยการแจ้งเป็นลายลักษณ์อักษรล่วงหน้าไม่น้อยกว่า 30 วัน
เมื่อยกเลิก ข้อมูลส่วนบุคคลที่ได้รับจะต้องถูกลบทิ้งหรือส่งคืนโดยทันที

10. การแก้ไขข้อตกลง

- การแก้ไขข้อตกลงต้องได้รับความเห็นชอบจากทั้งสองฝ่าย
- การแก้ไขจะมีผลบังคับใช้เมื่อได้รับการลงนามยอมรับแล้วเท่านั้น

11. กฎหมายและข้อบังคับที่เกี่ยวข้อง

- การดำเนินการทั้งหมดจะต้องเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ปฏิบัติตามแนวทางและประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ลงชื่อผู้แทนบริษัท

บริษัท ABC จำกัด	บริษัท XYZ จำกัด
นายสมชาย ใจดี (กรรมการผู้จัดการ)	นางสาวพรทิพย์ สวัสดิ์ (กรรมการผู้จัดการ)
วันที่: 15 มิถุนายน 2568	วันที่: 15 มิถุนายน 2568

แบบฟอร์มบันทึกการตัดสินใจแบ่งปันข้อมูล (Document All Sharing Decisions)

วันที่	รายละเอียดการแบ่งปันข้อมูล	ผู้อนุมัติ	หมายเหตุ
2025-06-01	แบ่งปันข้อมูลลูกค้าแก่บริษัท XYZ	นายสมชาย ใจดี	ข้อมูลเข้ารหัสตามมาตรฐาน
2025-06-15	อัปเดตขอบเขตข้อมูลที่แบ่งปัน	นางสาวพรทิพย์	เพิ่มข้อมูลพฤติกรรมใช้งาน

7.2.3 หากมีความจำเป็น ควรมีขั้นตอนและคำแนะนำที่ครอบคลุมการดำเนินงานประจำวันของแต่ละองค์กร (day-to-day operations support) เพื่อจะสนับสนุนการดำเนินงานตาม DSA

สิ่งที่ต้องทำ: มีคู่มือการดำเนินงานของพนักงานครบถ้วน

หลักฐาน: คู่มือการดำเนินงานของพนักงาน

สภาพบังคับ: กฎหมายไม่ได้กำหนด

คู่มือการดำเนินงานประจำวันของพนักงาน” เพื่อสนับสนุนการดำเนินงานตามข้อตกลงการแบ่งปัน
ข้อมูลส่วนบุคคล (DSA)
สำหรับการแบ่งปันข้อมูลส่วนบุคคลระหว่างหน่วยงาน ตามข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล
(DSA)

หน่วยงาน: [ชื่อองค์กรของคุณ]

ฉบับที่: 1 | วันที่บังคับใช้: 1 กรกฎาคม 2568

1. จุดประสงค์ของคู่มือ

คู่มือนี้จัดทำขึ้นเพื่อสนับสนุนให้พนักงานสามารถปฏิบัติงานเกี่ยวกับการแบ่งปันข้อมูลส่วนบุคคลตามข้อตกลง DSA ได้อย่างถูกต้อง ปลอดภัย และสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

2. ขอบเขตการใช้งาน

- พนักงานทุกคนที่มีหน้าที่เกี่ยวข้องกับ:
- การเตรียมข้อมูลเพื่อแบ่งปัน
- การส่งหรือรับข้อมูลส่วนบุคคล
- การตรวจสอบความถูกต้องของข้อมูล
- การรายงานเหตุการณ์การละเมิดข้อมูล (ถ้ามี)

3. ขั้นตอนการดำเนินงานประจำวัน

3.1 เตรียมข้อมูล

- ตรวจสอบว่าข้อมูลที่จะแบ่งปันตรงกับขอบเขตที่กำหนดไว้ใน DSA
- ทำการลบข้อมูลส่วนบุคคลที่ไม่จำเป็น (data minimisation)
- ตรวจสอบความถูกต้องและความทันสมัยของข้อมูล

3.2 ตรวจสอบสิทธิ์ของผู้รับ

- ยืนยันตัวบุคคลหรือหน่วยงานผู้รับข้อมูลว่าเป็นผู้มีสิทธิ์
- ตรวจสอบขอบเขตสิทธิ์ในการเข้าถึงข้อมูล (access control)

3.3 การเข้ารหัสและการส่งข้อมูล

- เข้ารหัสข้อมูลด้วยมาตรฐาน AES-256 หรือใช้ Secure File Transfer Protocol (SFTP)
- ส่งข้อมูลผ่านช่องทางที่ปลอดภัย (encrypted email หรือ VPN)

3.4 บันทึกการแบ่งปันข้อมูล

- กรอกแบบฟอร์ม “บันทึกการแบ่งปันข้อมูล” ทุกครั้ง (แนบตัวอย่างท้ายเอกสาร)
- ส่งสำเนาการบันทึกให้ DPO (Data Protection Officer)

3.5 การรับข้อมูล

- ตรวจสอบว่าข้อมูลที่ได้รับตรงตาม DSA
- ยืนยันว่าไม่ได้รับข้อมูลเกินกว่าที่กำหนด
- ดำเนินการจัดเก็บในระบบที่มีความปลอดภัย

3.6 การรายงานเหตุการณ์

- หากพบว่าการส่งข้อมูลผิด หรือข้อมูลรั่วไหล ให้แจ้ง DPO ภายใน 24 ชั่วโมง
- กรอกแบบฟอร์ม “รายงานเหตุการณ์การละเมิดข้อมูล”

4. ตัวอย่างแบบฟอร์มที่ใช้ประจำวัน

แบบฟอร์ม: บันทึกการแบ่งปันข้อมูล

วันที่ แบ่งปัน	หน่วยงาน ผู้รับ	ชนิดของข้อมูล	วัตถุประสงค์	วิธีส่ง ข้อมูล	ผู้รับผิดชอบ	หมายเหตุ
3 ก.ค. 6	กรม สุขภาพจิต	ข้อมูลผู้ป่วย (ไม่ ระบุตัวตน)	วิเคราะห์นโยบาย สุขภาพ	SFTP	นาย ก.	-

5. คำแนะนำสำคัญ

- ห้ามใช้ข้อมูลเพื่อวัตถุประสงค์อื่นนอกจากที่ระบุไว้ใน DSA
- ห้ามเก็บข้อมูลไว้ในอุปกรณ์ส่วนตัวหรือระบบที่ไม่ได้รับอนุญาต
- ห้ามส่งต่อข้อมูลให้บุคคลที่สามนอกเหนือจากผู้มีอำนาจตาม DSA

6. ช่องทางการติดต่อ DPO

หากมีข้อสงสัยหรือเหตุการณ์ผิดปกติ โปรดติดต่อ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ชื่อ: [ชื่อ DPO]

โทร: [เบอร์โทร]

อีเมล: [อีเมล DPO]

7. การทบทวนคู่มือ

คู่มือฉบับนี้จะถูกทบทวนทุก 12 เดือน หรือเมื่อมีการเปลี่ยนแปลงใน DSA หรือกฎหมายที่เกี่ยวข้อง

7.2.4 หากองค์กรทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controller) องค์กรควรกำหนดหน้าที่และความรับผิดชอบภายใต้ DSA อย่างเหมาะสม และควรแจ้งรายละเอียดและวัตถุประสงค์ต่าง ๆ ที่เกี่ยวข้องกับการดำเนินการตาม DSA ที่มีลักษณะเป็น Joint Controller ให้เจ้าของข้อมูลส่วนบุคคลรับทราบอย่างเหมาะสมผ่าน Privacy Notice

สิ่งที่ต้องทำ: มีการแจ้งผ่าน Privacy Notice ครบถ้วน

หลักฐาน: ประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กรแสดงการดำเนินการตามข้อตกลงแบ่งปันข้อมูลส่วนบุคคล กรณีองค์กรเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice) ขององค์กรที่ทำหน้าที่เป็น ผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controller)

กรณีองค์กรทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controller)

องค์กร: [ชื่อองค์กรของคุณ]

วันที่มีผลบังคับใช้: 1 กรกฎาคม 2568

1. บทนำ

[ชื่อองค์กรของคุณ] (“องค์กร”) ให้ความสำคัญต่อการคุ้มครองข้อมูลส่วนบุคคลของท่าน และดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“PDPA”) โดยในบางกรณี องค์กรได้มีข้อตกลงการแบ่งปันข้อมูลส่วนบุคคลร่วมกับหน่วยงานอื่น ซึ่งทำให้มีสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controller)” ภายใต้กฎหมาย

2. ขอบเขตของความเป็นผู้ควบคุมร่วม (Joint Controller)

องค์กรมีการร่วมดำเนินการกับ [เช่น กรมสุขภาพจิต / สำนักงานสถิติแห่งชาติ ฯลฯ] เพื่อประมวลผลข้อมูลส่วนบุคคลในลักษณะต่อไปนี้:

- เก็บรวบรวมข้อมูลจากหลายแหล่งข้อมูลของหน่วยงานร่วม
- ใช้ข้อมูลเพื่อวิเคราะห์/วิจัยร่วมกันในโครงการ [ชื่อโครงการ/กิจกรรม]
- ตัดสินใจร่วมกันเกี่ยวกับวิธีการและวัตถุประสงค์ของการประมวลผลข้อมูล

โดยองค์กรและหน่วยงานที่เกี่ยวข้องได้ทำข้อตกลงร่วมกันผ่าน “ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA)” ที่กำหนดบทบาท หน้าที่ และความรับผิดชอบอย่างชัดเจน

3. วัตถุประสงค์ของการประมวลผลข้อมูลร่วม

ข้อมูลของท่านอาจถูกใช้ร่วมกันระหว่างหน่วยงานควบคุมข้อมูลร่วมเพื่อวัตถุประสงค์ดังต่อไปนี้

- การวางแผนนโยบายสาธารณสุข
- การให้บริการทางสังคมแก่กลุ่มเปราะบาง
- การศึกษาวิจัยเพื่อพัฒนาบริการสาธารณะ

4. ประเภทของข้อมูลที่ประมวลผล

- ข้อมูลที่ถูกแบ่งปันและประมวลผลรวมอาจรวมถึง:
- ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ-นามสกุล วันเกิด เลขบัตรประชาชน
- ข้อมูลอ่อนไหว เช่น ข้อมูลสุขภาพ (จะได้รับความยินยอมก่อน เว้นแต่มีเหตุยกเว้นตามกฎหมาย)

5. สิทธิของเจ้าของข้อมูล

ท่านมีสิทธิต่าง ๆ ตามที่กฎหมายกำหนด ได้แก่

- ขอเข้าถึงหรือขอสำเนาข้อมูลของท่าน
- ขอให้แก้ไขข้อมูลให้ถูกต้อง
- ขอให้ระงับการใช้ข้อมูลหรือคัดค้านการประมวลผล
- ขอให้ลบข้อมูล (ในกรณีที่ใช้สิทธิได้)
- ท่านสามารถใช้สิทธิโดยติดต่อ DPO ขององค์กรตามช่องทางด้านล่าง

6. การจัดเก็บและการรักษาความมั่นคงปลอดภัย

- ข้อมูลจะถูกเก็บรักษาอย่างปลอดภัยในระบบที่ได้รับการออกแบบตามมาตรฐาน ISO/IEC 27001
- องค์กรและหน่วยงานร่วมได้ตกลงวิธีการป้องกันข้อมูลใน DSA

7. ช่องทางติดต่อ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ชื่อ: [ชื่อ DPO]

โทร: [เบอร์โทร DPO]

อีเมล: [อีเมล DPO]

8. การปรับปรุงประกาศ

- องค์กรอาจปรับปรุงประกาศฉบับนี้เป็นระยะ โดยจะประกาศเวอร์ชันล่าสุดที่ [URL เว็บไซต์ขององค์กร]
- จัดทำให้คุณดาวน์โหลดได้โดยตรงครับ

7.2.5 องค์กรมีการทบทวนและตรวจสอบการดำเนินการตาม DSA อย่างสม่ำเสมอ เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่แบ่งปันยังคงมีความถูกต้องและเป็นปัจจุบัน และเพื่อตรวจสอบว่า DSA ยังคงครอบคลุมชุดข้อมูลที่ถูกต้องหรือไม่

สิ่งที่ต้องทำ: มีกระบวนการตรวจสอบอย่างสม่ำเสมอ

หลักฐาน: กระบวนการขององค์กรในการตรวจสอบการดำเนินการ ตาม DSA

สภาพบังคับ: กฎหมายไม่ได้กำหนด

กระบวนการตรวจสอบและทบทวนการดำเนินการตามข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement – DSA)

หน่วยงาน: [ชื่อองค์กรของคุณ]

ผู้รับผิดชอบหลัก: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO), ฝ่ายนิติการ, และฝ่ายสารสนเทศ

เวอร์ชันล่าสุด: 1.0

วันที่มีผลบังคับใช้: [วัน/เดือน/ปี]

1. วัตถุประสงค์

เพื่อให้แน่ใจว่าการแบ่งปันข้อมูลส่วนบุคคลตาม DSA เป็นไปตามเงื่อนไขที่ตกลงไว้ มีความถูกต้อง เป็นปัจจุบัน และสอดคล้องกับหลักการของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตลอดจนเพื่อการปรับปรุง ข้อตกลง DSA ให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลง

2. ขอบเขต

กระบวนการนี้ครอบคลุมการตรวจสอบทุกโครงการหรือทุกหน่วยงานที่มีการแบ่งปันข้อมูลตาม DSA ที่มีผลบังคับใช้ระหว่างองค์กรกับคู่สัญญา หรือองค์กรที่ควบคุมร่วม

3. ความถี่ในการตรวจสอบ

อย่างน้อยปีละ 1 ครั้งหรือเมื่อมีเหตุเปลี่ยนแปลง เช่น การเพิ่มชุดข้อมูลใหม่ การเปลี่ยนระบบไอที หรือเปลี่ยนวัตถุประสงค์ของการแบ่งปันข้อมูล

4. ขั้นตอนการตรวจสอบ

ขั้นตอน	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา
1. ตรวจสอบชุดข้อมูล	ตรวจสอบว่าข้อมูลที่แบ่งปันตาม DSA ยังคงมีความจำเป็น ถูกต้อง และเป็นปัจจุบัน	DPO / ฝ่ายสารสนเทศ	1 สัปดาห์
2. ตรวจสอบความสอดคล้อง	ตรวจสอบว่า DSA ครอบคลุมข้อมูลที่แบ่งปันทั้งหมดหรือไม่ และสอดคล้องกับการใช้งานจริง	ฝ่ายกฎหมาย / DPO	1 สัปดาห์
3. ประเมินความเสี่ยง	ประเมินความเสี่ยงใหม่ (หากมีการเปลี่ยนแปลงระบบหรือผู้ให้บริการ)	DPO / ฝ่ายความปลอดภัย	1 สัปดาห์
4. ออกรายงานผล	จัดทำรายงานผลการตรวจสอบ เสนอผู้บริหาร และคู่สัญญา (หากเกี่ยวข้อง)	DPO	3 วัน

5. ปรับปรุง DSA	ดำเนินการปรับปรุง DSA หากจำเป็น	ฝ่ายกฎหมาย / คู่สัญญา	ตาม กระบวนการ อนุมัติ

5. แบบฟอร์ม / เอกสารประกอบ

- แบบฟอร์มตรวจสอบความครบถ้วนของ DSA
- แบบประเมินความเสี่ยงข้อมูลส่วนบุคคล
- รายงานผลการตรวจสอบประจำปี
- บันทึกการสื่อสารกับคู่สัญญา
- บันทึกการทบทวนความสอดคล้องกับ Privacy Notice

6. การรายงานและติดตามผล

- DPO จะจัดทำรายงานประจำปีส่งให้ผู้บริหารสูงสุด
- ผลการตรวจสอบจะถูกรวบรวมไว้เป็นเอกสารประกอบการต่ออายุหรือแก้ไข DSA
- หากพบการละเมิดหรือการใช้ข้อมูลผิดวัตถุประสงค์ จะดำเนินการแจ้งเตือนคู่สัญญา และรายงานหน่วยงานกำกับหากจำเป็น

7. ตัวอย่างเหตุการณ์ที่ควรตรวจสอบ DSA ก่อนถึงรอบประจำปี

- การเปลี่ยนแปลงระบบการจัดเก็บ/ส่งต่อข้อมูล
- การรวมระบบกับพันธมิตรใหม่
- การเปิดเผยข้อมูลกับหน่วยงานที่ยังไม่มีข้อตกลงร่วม
- การร้องเรียนจากเจ้าของข้อมูลหรือหน่วยงานกำกับดูแล

หมายเหตุ: เอกสารนี้ควรแนบรวมกับ DSA และใช้เป็นเอกสารอ้างอิงหากหน่วยงานกำกับต้องการตรวจสอบความพร้อมด้านการบริหารจัดการข้อมูลส่วนบุคคล

ลำดับ	หัวข้อประเมิน	รายละเอียด	ตรวจพบ (✓ / ✗)	หมายเหตุ
แบบฟอร์มตรวจสอบความครบถ้วนของข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA Checklist) ชื่อองค์กร: ชื่อหน่วยงาน/ฝ่ายที่เกี่ยวข้อง: ชื่อผู้ประเมิน: วันที่ตรวจสอบ:/...../.....				

1	ข้อตกลงมีลายเซ็นของผู้บริหารระดับสูงหรือไม่	ตรวจสอบว่าเอกสาร DSA ได้รับอนุมัติและลงนามแล้ว		
2	มีระบุวัตถุประสงค์ของการแบ่งปันข้อมูลอย่างชัดเจนหรือไม่	เช่น เพื่อการให้บริการ, การตรวจสอบ, ฯลฯ		
3	มีการระบุบทบาทของแต่ละฝ่ายใน DSA หรือไม่	เช่น Data Controller, Data processor		
4	มีแผนผังแสดงทิศทางการไหลของข้อมูล (Data Flow) หรือไม่	แนบแผนผัง Data Flow Diagram ไว้ใน DSA		
	มีรายละเอียดเกี่ยวกับมาตรฐานความปลอดภัยในการส่งข้อมูลหรือไม่	เช่น การเข้ารหัส การควบคุมการเข้าถึง		
6	มีการระบุการป้องกันข้อมูลของผู้เยาว์หรือกลุ่มเปราะบางหรือไม่	เช่น default privacy limited access		
7	มีแนบ Privacy Notice ที่ชี้แจงสิทธิของเจ้าของข้อมูลหรือไม่	โดยเฉพาะในกรณี Join Controller		
8	มีคู่มือการดำเนินงาน (SOP) สำหรับเจ้าหน้าที่หรือไม่	ใช้อำนาจการแบ่งปันข้อมูลประจำวัน		
9	มีการทบทวน DSA ล่าสุดเมื่อใด	ระบุวันที่ทบทวนครั้งสุดท้าย		
10	มีแผน/ขั้นตอนสำหรับการตรวจสอบซ้ำทุกปีหรือไม่	เพื่อให้ข้อมูลเป็นปัจจุบัน		

สรุปผล

- ผ่านการตรวจสอบ ()
- มีข้อเสนอแนะเพื่อปรับปรุง ()
- ต้องแก้ไขก่อนใช้งาน ()

ผู้ประเมิน:

ลงชื่อ:

ตำแหน่ง:

ตัวอย่างรายงานผลการตรวจสอบการดำเนินการตาม DSA

ชื่อรายงาน: รายงานผลการตรวจสอบการดำเนินการตามข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA)

หน่วยงาน: แผนกคุ้มครองข้อมูลส่วนบุคคล, ฝ่ายนิติการ, [ชื่อองค์กร]

รอบการตรวจสอบ: ปีงบประมาณ 2567

วันที่จัดทำรายงาน: 30 กันยายน 2567

1. สรุปภาพรวม

ในปีงบประมาณ 2567 องค์กรได้ทำการตรวจสอบข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement: DSA) ทั้งหมด 5 ฉบับ ซึ่งมีผลบังคับใช้กับหน่วยงานภายในและภายนอกองค์กร โดยมุ่งเน้นตรวจสอบด้านความถูกต้อง ความครบถ้วน และความสอดคล้องตามแนวทาง PDPA

2. ผลการตรวจสอบแบบจำแนก

ลำดับ	คู่สัญญา	ชื่อ DSA	ผลการตรวจสอบ	ข้อสังเกต
1	โรงพยาบาล A	DSA_2566_Hospital_A	ผ่าน	มีระบุ flow ของข้อมูลชัดเจน
2	บริษัทประกัน B	DSA_2566_InsuranceB	ต้องปรับปรุง	ไม่มี Privacy Notice แนบ
3	สำนักงานสถิติแห่งชาติ	DSA_2566_ISO	ผ่าน	ครอบคลุมทุกประเด็น
4	บริษัทเทคโนโลยี C	DSA_2566_Tech_C	ต้องปรับปรุง	ไม่มีข้อมูลผู้ควบคุมร่วม
5	กรมควบคุมโรค	DSA_2566_DDC	ผ่าน	มีการเข้ารหัสตามมาตรฐาน ISO 27001

3. สรุปข้อเสนอแนะ

- ควรเพิ่มเติม Privacy Notice ให้ครบถ้วนในทุกกรณีที่เกี่ยวข้องกับ Joint Controller
- ควรแนบ คู่มือ SOP ประจำวัน สำหรับเจ้าหน้าที่ใน DSA ฉบับที่ไม่มี
- ปรับปรุง แผนผัง Data Flow ให้แสดงผลการประมวลผลอย่างละเอียดมากขึ้น
- จัดให้มีการ ติดตามการแก้ไข ภายใน 30 วันหลังส่งรายงานฉบับนี้

4. แนบเอกสาร

- Checklist การตรวจสอบแต่ละ DSA
- แบบฟอร์มข้อเสนอแนะและแผนแก้ไข (Corrective Action Plan)
- สำเนา DSA (เฉพาะที่อนุญาตให้ตรวจสอบ)
- สำเนา Privacy Notice (ถ้ามี)

ลงชื่อ:

(นายสมพงษ์ ข้อมูลดี)

ตำแหน่ง: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

วันที่: 30 กันยายน 2567

7.2.6 องค์กรจัดทำบันทึกกลางของ DSA ทั้งหมดขององค์กร (central log of the current DSA) เพื่อการควบคุมและตรวจสอบ

สิ่งที่ต้องทำ: มีการจัดทำบันทึกกลางของ DSA ทั้งหมดขององค์กร

หลักฐาน: บันทึกกลางของ DSA ทั้งหมดขององค์กร

สภาพบังคับ: กฎหมายไม่ได้กำหนด

บันทึกกลางของข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Central Log of Data Sharing Agreements)

ชื่อองค์กร: [ชื่อองค์กรของคุณ]

หน่วยงานรับผิดชอบในการจัดเก็บและดูแลบันทึกนี้: [เช่น ฝ่ายกฎหมาย / ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO)]

ผู้รับผิดชอบหลัก: [ชื่อ - ตำแหน่ง]

วันที่ปรับปรุงล่าสุด: 30 กันยายน 2567

ตารางบันทึก DSA ทั้งหมดขององค์กร

ลำดับ	ชื่อ DSA	หน่วยงานคู่สัญญา	วัตถุประสงค์	วันที่ลงนาม	วันที่หมดอายุ	ประเภทข้อมูลที่แบ่งปัน	บทบาทขององค์กร	หมายเหตุ
1	DSA_2566_Hospital_A	โรงพยาบาล A	การอ้างอิงข้อมูลผู้ป่วยระหว่างรพ.	01/01/2566	31/12/2568	ชื่อ, หมายเลขบัตร, ผลการวินิจฉัย	Data Controller	มีการเข้ารหัสข้อมูล

2	DSA_2566_Insurance_B	บริษัท ประกัน B	ประเมิน ความเสี่ยง สุขภาพเพื่อ ทำประกัน	15/02/25 66	14/02/25 67	ข้อมูล สุขภาพ, ประวัติ แพทย์	Joint Controller	อยู่ ระหว่าง แก้ไข Privacy Notice
3	DSA_2566_NS O	สำนักงาน สถิติ แห่งชาติ	ส่งข้อมูล เพื่อสถิติ ระดับชาติ	01/02/25 66	01/04/25 71	ข้อมูลนิร นาม, อายุ, เพศ	Data Controller	-
4	DSA_2567_Ed uPlatform	แพลตฟอร์ม การเรียนรู้ ออนไลน์	การสมัคร ใช้งาน LMS และ วิเคราะห์ ผล	20/06/25 67	19/06/25	อีเมล, ชื่อผู้ใช้, คะแนน	Data Processor	กำหนด ค่าความ เป็น ส่วนตัว ขั้นสูง
5	DSA_2567_Te ch_C	บริษัท เทคโนโลยี C	การพัฒนา AI วิเคราะห์ เสียง สนทนา	01/07/25 67	01/07/25 69	เสียง, ข้อความ , อารมณ์	Joint Controller	มี Data Flow Diagram แนบ

คำอธิบายการใช้ตาราง

ชื่อข้อตกลง: ใช้รูปแบบรหัส เช่น “ข้อตกลง_ปี_ชื่อองค์กร” เพื่อค้นหาได้สะดวก

บทบาทขององค์กร:

- “ผู้ควบคุมข้อมูลส่วนบุคคล” (Data Controller) หมายถึง องค์กรเป็นผู้ตัดสินใจเรื่องวัตถุประสงค์และวิธีการประมวลผลข้อมูล
- “ผู้ควบคุมข้อมูลร่วม” (Joint Controller) หมายถึง องค์กรร่วมกับอีกฝ่ายตัดสินใจวัตถุประสงค์และวิธีการ
- “ผู้ประมวลผลข้อมูล” (Data Processor) หมายถึง องค์กรทำตามคำสั่งของอีกฝ่ายหนึ่ง

หมายเหตุ: ระบุสถานะเอกสาร เช่น อยู่ระหว่างปรับปรุง, แนบไฟล์เพิ่มเติม, กำหนดค่าความเป็นส่วนตัว ฯลฯ
เอกสารแนบ (ควรเก็บในระบบหรือโฟลเดอร์ที่มีสิทธิ์เข้าถึงเฉพาะ)

เอกสารต่อไปนี้ควรถูกจัดเก็บไว้ร่วมกับบันทึกกลาง (ในระบบไฟล์หรือระบบจัดเก็บเอกสารขององค์กร):

- ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคลในรูปแบบ PDF ที่ลงนามแล้ว
- ประกาศความเป็นส่วนตัว (Privacy Notice) ที่เกี่ยวข้องกับแต่ละ DSA
- แผนภาพการไหลของข้อมูล (Data Flow Diagram)

- รายงานผลการตรวจสอบประจำปี (ตามข้อ 7.2.5)
- แบบฟอร์มตรวจสอบและเช็ค리스트ที่เกี่ยวข้องกับ DSA

สรุป

- บันทึกกลางฉบับนี้ควรมีการ อัปเดตทันทีเมื่อมีข้อตกลงใหม่, มีการแก้ไข, หรือเมื่อหมดอายุ
- เอกสารนี้ควรถูกจัดเก็บใน ระบบที่มีความปลอดภัย และมีการควบคุมสิทธิ์การเข้าถึงอย่างเหมาะสม
- องค์กรสามารถใช้เป็นหลักฐานยืนยันการปฏิบัติตามแนวทาง PDPA หรือการตรวจสอบภายใน/ภายนอกได้อย่างเหมาะสม

แบบฟอร์มตรวจสอบการดำเนินการตามข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (DSA)

ชื่อหน่วยงาน:

ผู้ตรวจสอบ:

ตำแหน่ง:

วันที่ตรวจสอบ:

รอบการตรวจสอบ: ☐ รายเดือน ☐ รายไตรมาส ☐ รายครึ่งปี ☐ รายปี

ส่วนที่ 1: การตรวจสอบความครบถ้วนของข้อตกลง (DSA Checklist)

รายการตรวจสอบ	รายละเอียด	สถานะ	หมายเหตุ
1. มีสำเนา DSA ที่ลงนามเก็บไว้ อย่างเป็นระบบ	เอกสารต้องมี ลายเซ็นทั้งสองฝ่าย	☐ ผ่าน ☐ ไม่ผ่าน	
2. DSA ระบุวัตถุประสงค์ของการ แบ่งปันข้อมูลอย่างชัดเจน	เช่น เพื่อวิเคราะห์, ให้บริการ, ฯลฯ	☐ ผ่าน ☐ ไม่ผ่าน	
3. มีระยะเวลาการแบ่งปันข้อมูล ที่ชัดเจน	มีการกำหนดวัน เริ่มต้น-สิ้นสุด	☐ ผ่าน ☐ ไม่ผ่าน	
4. ระบุบทบาทชัดเจน (Controller / Joint Controller / Processor)	ตรวจสอบกับ ประกาศ Privacy Notice	☐ ผ่าน ☐ ไม่ผ่าน	

5. มีการระบุประเภทข้อมูลที่แบ่งปัน (Personal / Sensitive)	และมีการกำหนด มาตรการป้องกัน	☐ ผ่าน ☐ ไม่ผ่าน	
6. มีขั้นตอนลบ/คืน/หยุดแบ่งปันเมื่อ DSA สิ้นสุด	เพื่อความปลอดภัย ของข้อมูล	☐ ผ่าน ☐ ไม่ผ่าน	

ส่วนที่ 2: การตรวจสอบความถูกต้องและเป็นปัจจุบันของข้อมูล

รายการตรวจสอบ	รายละเอียด	สถานะ	หมายเหตุ
1. ตรวจสอบว่าข้อมูลที่แบ่งปันยังเป็นข้อมูลล่าสุด	โดยเทียบกับ ฐานข้อมูลหลักของ องค์กร	☐ ผ่าน ☐ ไม่ผ่าน	
2. มีการทบทวนว่าชุดข้อมูล ยังสอดคล้องกับวัตถุประสงค์ เดิม	☐ ใช่ ☐ ไม่ใช่	☐ ผ่าน ☐ ไม่ผ่าน	
3. มีหลักฐานการทบทวน เช่น บันทึกประชุม / รายงาน / อีเมล	☐ มี ☐ ไม่มี	☐ ผ่าน ☐ ไม่ผ่าน	
4. พบปัญหาหรือความ คลาดเคลื่อนในรอบก่อนหน้า	☐ พบ ☐ ไม่พบ	☐ ดำเนินการแล้ว ☐ ยังไม่ดำเนินการ	

รายงานผลการตรวจสอบ (Summary Report)

ข้อค้นพบสำคัญ

.....

ประเด็นที่ต้องปรับปรุง/แก้ไขเพิ่มเติม

.....

ข้อเสนอแนะจากผู้ตรวจสอบ

.....

การดำเนินการถัดไป:

- แจ้งหัวหน้างาน/กรรมการข้อมูล
- ทบทวน DSA ร่วมกับคู่สัญญา
- แก้ไขประกาศความเป็นส่วนตัว (Privacy Notice)
- อื่น ๆ

ลายมือชื่อผู้ตรวจสอบ

ลงชื่อ:

วันที่:

7.3 การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ (Cross-border Personal Data Transfer)
องค์กรมีขั้นตอนการดำเนินงานเพื่อให้แน่ใจว่าการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศได้
ดำเนินการอย่างถูกต้องและเหมาะสม

7.3.1 กรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ ประเทศปลายทางหรือองค์กรระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy) ตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด

สิ่งที่ต้องทำ: มีการตรวจสอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์กรระหว่างประเทศที่รับข้อมูลส่วนบุคคล ตามหลักเกณฑ์ที่ประกาศกำหนด และมีเอกสารสนับสนุน

หลักฐาน: รายงานแสดงว่าองค์กรได้มีการตรวจสอบว่าประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและเป็นไปตามที่กฎหมายกำหนด

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566

ในกรณีที่มิได้ปฏิบัติตามมาตรา 28 โทษทางอาญา มาตรา 79 กำหนดโทษทางอาญา จำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

กรณีเป็นข้อมูลตาม มาตรา 26 โทษทางปกครอง มาตรา 83 กำหนดโทษปรับทางปกครอง ไม่เกิน 3 ล้านบาท

รายงานการจัดทำมาตรการคุ้มครองที่เหมาะสม (Appropriate Safeguards) สำหรับการโอนข้อมูลไปยังประเทศที่ไม่มี Adequacy

ชื่อเอกสาร: รายงานการประเมินมาตรการคุ้มครองที่เหมาะสมในการส่งข้อมูลส่วนบุคคลไปยังประเทศปลายทาง

หน่วยงานผู้จัดทำ: ฝ่ายกฎหมายและการคุ้มครองข้อมูลส่วนบุคคล (DPO Office)

วันที่จัดทำ: [ระบุวันที่]

1. วัตถุประสงค์

เพื่อแสดงว่าองค์กรได้ปฏิบัติตาม มาตรา 28 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยจัดทำมาตรการคุ้มครองที่เหมาะสม สำหรับการโอนข้อมูลส่วนบุคคลไปยังประเทศที่ยังไม่มีประกาศว่าเป็นประเทศที่มีความเพียงพอ (Adequacy)

2. ประเทศปลายทางที่อยู่ในการประเมิน

ลำดับ	ประเทศปลายทาง	มี Adequacy ตามประกาศหรือไม่	แนวทางดำเนินการ
1	จีน	ไม่มี Adequacy	ใช้ Appropriate Safeguard
2	อินเดีย	ไม่มี Adequacy	ใช้ Appropriate Safeguards
3	สหรัฐอาหรับเอมิเรตส์ (UAE)	ไม่มี Adequacy	ใช้ Appropriate Safeguards
4	พม่า	ไม่มี Adequacy	ใช้ Appropriate Safeguards
5	ลาว	ไม่มี Adequacy	ใช้ Appropriate Safeguards

3. ลักษณะข้อมูลและวัตถุประสงค์ของการโอน

- ประเภทของข้อมูล: ข้อมูลบุคคลพื้นฐาน, ข้อมูลการทำงาน, ข้อมูลลูกค้า

- วัตถุประสงค์: การประมวลผลระบบสนับสนุนด้านไอที, การวิเคราะห์ทางธุรกิจ, การจัดทำบัญชีเงินเดือน, บริการสนับสนุนลูกค้า
- ผู้รับข้อมูล: บริษัทในเครือ, บริษัทคู่สัญญา, ผู้ให้บริการคลาวด์หรือ outsourcing ในประเทศปลายทาง

4. มาตรการคุ้มครองที่เหมาะสมที่ดำเนินการ (Appropriate Safeguards)

4.1 ข้อตกลงตามมาตรฐาน (Standard Contractual Clauses: SCCs)

- ได้จัดทำสัญญาถ่ายโอนข้อมูลระหว่างประเทศซึ่งมีเงื่อนไขขั้นต่ำตามที่กฎหมายไทยกำหนด
- ข้อสัญญาระบุสิทธิของเจ้าของข้อมูลอย่างชัดเจน เช่น การเข้าถึง แก้ไข ถอนความยินยอม
- กำหนดหน้าที่ของผู้รับข้อมูลให้ดำเนินการตามมาตรฐานความมั่นคงปลอดภัย

4.2 การประเมินผลกระทบจากบริบทของประเทศปลายทาง (Transfer Impact Assessment)

- ประเมินความเสี่ยงจากกฎหมายของประเทศปลายทาง
- ตรวจสอบว่ามีการบังคับใช้หรือแทรกแซงโดยหน่วยงานรัฐในทางที่อาจละเมิดสิทธิของเจ้าของข้อมูลหรือไม่

4.3 มาตรการทางเทคนิคและองค์กร

- การเข้ารหัสข้อมูลแบบ End-to-End
- จำกัดสิทธิ์การเข้าถึงข้อมูลตามระดับหน้าที่งาน
- จัดให้มีการฝึกอบรมพนักงานในประเทศปลายทางเกี่ยวกับข้อกำหนดด้าน PDPA
- การจัดทำบันทึกกิจกรรมการเข้าถึงและการประมวลผลข้อมูล

5. เอกสารสนับสนุน

- แบบฟอร์ม Transfer Impact Assessment (TIA)
- สำเนาสัญญา SCCs หรือสัญญาคุ้มครองข้อมูล (Data Transfer Agreement)
- รายงานความมั่นคงปลอดภัยของระบบปลายทาง
- บันทึกการตรวจสอบภายในหรือ audit report
- บันทึกการฝึกอบรมผู้รับข้อมูลในประเทศปลายทาง

6. ข้อเสนอแนะในการติดตามและทบทวน

- มีการทบทวนความเหมาะสมของมาตรการทุก 12 เดือน หรือเมื่อมีการเปลี่ยนแปลงประเทศปลายทาง/ผู้รับข้อมูล
- หากพบว่าประเทศปลายทางได้รับการรับรองความเพียงพอ (Adequacy) ในอนาคต จะปรับขั้นตอนตามข้อยกเว้นในกฎหมาย
- องค์กรมีระบบให้เจ้าของข้อมูลสามารถร้องเรียนหรือตรวจสอบสิทธิได้โดยสะดวก

7. ผู้รับผิดชอบ

นางสาวจิราพร รัตนพงศ์

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

โทร: [ระบุเบอร์]

อีเมล: [ระบุอีเมล]

รายละเอียดการประเมินการโอนข้อมูลส่วนบุคคลไปยังประเทศที่ไม่มี Adequacy

ลำดับ	ประเทศปลายทาง	ชื่อองค์กร/ผู้รับข้อมูล	ประเภทข้อมูลที่โอน	วัตถุประสงค์ของการโอน	มาตรการที่ใช้	มี SCCs หรือไม่	มี TIA หรือไม่	ความถี่ในการตรวจสอบ	หมายเหตุ
1	สหรัฐอเมริกา	Amazon Web Services (AWS)	ข้อมูลลูกค้า ชื่อ อีเมล ประวัติการใช้งาน	จัดเก็บและประมวลผลข้อมูลบนคลาวด์	SCCs, TIA, การเข้ารหัส	✓	✓	ทุก 12 เดือน	มี SOC 2 Report ล่าสุด
2	สิงคโปร์	บริษัทในเครือขององค์กร	ข้อมูลพนักงาน	บริหารจัดการทรัพยากรบุคคล	SCCs, TIA, Policy Sharing	✓	✓	ทุก 6 เดือน	มี ISO/IEC 27001
3	จีน	ผู้ให้บริการจัดเก็บข้อมูลสำรอง	ข้อมูลระบบไอทีบางส่วน	สำรองข้อมูลแบบ offsite	SCCs, การเข้ารหัส, จำกัดการเข้าถึง	✓	✓	ทุก 12 เดือน	ตรวจสอบการควบคุมสิทธิ์
4	อินเดีย	บริษัท outsourcing ด้าน IT support	ข้อมูลคำร้องขอบริการของลูกค้า	บริการสนับสนุนลูกค้าระหว่างประเทศ	SCCs, TIA, NDA พนักงาน	✓	✓	ทุก 6 เดือน	มีข้อสัญญาควบคุมภายนอก
5	UAE	ผู้ให้บริการระบบ CRM	ข้อมูลผู้สมัครงาน	ระบบจัดการผู้สมัคร	SCCs, การเข้ารหัส, Audit logs	✓	✓	ทุก 12 เดือน	ดำเนินการเฉพาะใน server ที่กำหนด
6	พม่า	พนักงานท้องถิ่นในสำนักงานสาขา	ข้อมูล HR และสัญญาจ้าง	การจ้างงานในพื้นที่	SCCs, TIA, ควบคุมสิทธิ์	✓	✓	ทุก 6 เดือน	มีการอบรมภายใน
7	ลาว	คู่สัญญาด้านการจัดกิจกรรม	ข้อมูลลูกค้าผู้ลงทะเบียน	การจัดกิจกรรมและส่งของรางวัล	SCCs, NDA, ลาย	✓	✓	ทุก 12 เดือน	เป็นกิจกรรมตามระยะเวลา

					ลักษณะ อักษร				

หมายเหตุเพิ่มเติม:

- SCCs (Standard Contractual Clauses): ข้อสัญญาที่มีเงื่อนไขตามที่ประกาศคณะกรรมการฯ กำหนด
- TIA (Transfer Impact Assessment): การประเมินความเสี่ยงจากบริบทของประเทศปลายทาง
- NDA: ข้อตกลงรักษาความลับระหว่างบุคคลหรือองค์กร

7.3.2 กรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ การส่งหรือโอนดังกล่าวมีความสอดคล้องกับข้อกำหนดของกฎหมายในกรณีอื่น ๆ ตามที่กำหนดในมาตรา 28 หรือมาตรา 29 และมีฐานทางกฎหมายที่เหมาะสมในการส่งหรือโอน

สิ่งที่ต้องทำ: มีการตรวจสอบความสอดคล้องและฐานทางกฎหมายครบถ้วน และมีเอกสารสนับสนุน

หลักฐาน: รายงานแสดงว่าองค์กรได้มีการตรวจสอบว่าประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและเป็นไปตามที่กฎหมายกำหนด

Binding Corporate Rules (BCRs)

มาตรการที่เหมาะสมในการโอนข้อมูล เช่น MCCs, SCCs

หลักฐานในการพิจารณาฐานทางกฎหมายในการโอนข้อมูลไปต่างประเทศ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28, 29

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566

รายงานการตรวจสอบความสอดคล้องและฐานทางกฎหมายในการส่งหรือโอนข้อมูลส่วนบุคคลไป
ต่างประเทศ

ตามมาตรา 28 และ 29 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หน่วยงานผู้จัดทำ: คณะทำงานคุ้มครองข้อมูลส่วนบุคคล (Data Protection Compliance Team)

วันที่จัดทำ: [ระบุวันที่]

ผู้รับผิดชอบหลัก: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

1. วัตถุประสงค์ของรายงาน

เพื่อแสดงว่าองค์กรได้ดำเนินการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยสอดคล้องกับกฎหมายและหลักเกณฑ์ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 28 และมาตรา 29 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีฐานทางกฎหมายที่เหมาะสม ครบถ้วน และมีเอกสารสนับสนุนประกอบ

2. ขอบเขตการโอนข้อมูล

รายการ	รายละเอียด
ประเภทข้อมูล	ข้อมูลลูกค้า ข้อมูลพนักงาน ข้อมูลการใช้งานระบบ
วัตถุประสงค์	การให้บริการผ่านระบบคลาวด์ การบริหาร HR ระหว่างประเทศ การวิเคราะห์ข้อมูล
ผู้รับข้อมูล	บริษัทในเครือ, คู่สัญญา, ผู้ให้บริการภายนอกในต่างประเทศ
ประเทศปลายทาง	สหรัฐอเมริกา, สิงคโปร์, จีน, อินเดีย, UAE, พม่า, ลาว

3. การตรวจสอบฐานทางกฎหมายและมาตรการที่ใช้

3.1 การใช้มาตรา 28:

กรณีประเทศปลายทาง **ไม่มี Adequacy** องค์กรได้ดำเนินการตามทางเลือกที่กำหนดไว้ใน มาตรา 28 (2) ได้แก่:

ทางเลือกตามมาตรา 28	การปฏิบัติขององค์กร	เอกสารสนับสนุน
มีสัญญาหรือข้อผูกพันตามหลักเกณฑ์ (SCCs MCCs)	ดำเนินการแล้ว	สำเนา SCCs พร้อมข้อกำหนดขั้นต่ำตามประกาศปี 2566

มี BCRs (Binding Corporate Rules)	สำหรับบริษัทในเครือ	นโยบาย BCRs ภายในองค์กร
มีมาตรการคุ้มครองที่เหมาะสมอื่น ๆ	มี Transfer Impact Assessment (TIA), การเข้ารหัส, NDA	เอกสาร TIA และรายงาน audit ความมั่นคงปลอดภัย

3.2 การใช้มาตรา 29

กรณีจำเป็นต้องโอนข้อมูลโดยไม่มีมาตรการตามมาตรา 28 องค์กรพิจารณาใช้ข้อยกเว้นตามมาตรา 29 ซึ่งรวมถึง

ฐานทางกฎหมาย (มาตรา 29)	ตัวอย่างการใช้งาน	เอกสารสนับสนุน
ได้รับความยินยอมโดยชัดแจ้ง	กรณีสมัครเข้าร่วมกิจกรรมต่างประเทศ	แบบฟอร์มยินยอม (Elicit Consent Form)
จำเป็นเพื่อปฏิบัติตามสัญญา	การใช้บริการจัดส่งสินค้าระหว่างประเทศ	สำเนาสัญญาและเงื่อนไขบริการ
จำเป็นเพื่อประโยชน์โดยชอบธรรม	การสำรองข้อมูลเพื่อความมั่นคงทางระบบ	บันทึกการวิเคราะห์ legitimate Interest
จำเป็นเพื่อการดำเนินคดี	กรณีร้องเรียนข้อพิพาทกับผู้ให้บริการนอกประเทศ	หนังสือแจ้งเหตุและคำร้องทางกฎหมาย

4. ตารางสรุปการประเมินความสอดคล้อง

ประเทศปลายทาง	มี Adequacy หรือไม่	ใช้มาตราใด	มาตรการที่ใช้	เอกสารแนบ
สหรัฐอเมริกา	ไม่มี Adequacy	ม.28(2)(ข)	SCCs, TIA, NDA	SCC2024-00-v3.docx, TIA Report
สิงคโปร์	ไม่มี Adequacy	ม.28(2)(ค)	BCRs, Internal Rules	BCR-GroupPolicy.pdf
จีน	ไม่มี Adequacy	ม.28(2)(ข) + ม.29(1)	SCCs + ยินยอม	Consent_China.docx

อินเดีย	ไม่มี Adequacy	ม.28(2)(ง)	TIA, Audit Report, NDA	TIA-India.xlsx
UA	ไม่มี Adequacy	ม.29(2)	Legitimate Interest + SCCs	LegalBasisNote-UAE.pdf
พม่า	ไม่มี Adequacy	ม.28(2)(ข)	SCCs, Policy Sharing	SCCs-Myanmar.docx
ลาว	ไม่มี Adequacy	ม.29(2)	Consent + Audit Logs	ConsentForm_Laos.doc

5. เอกสารแนบที่ใช้เป็นหลักฐาน

- สำเนาสัญญา Standard Contractual Clauses (SCCs)
- นโยบาย Binding Corporate Rules (BCRs)
- แบบฟอร์มการยินยอมโดยชัดแจ้ง (Explicit Consent Forms)
- รายงาน Transfer Impact Assessment (TIA)
- บันทึกการวิเคราะห์ Legitimate Interest
- รายงานการตรวจสอบระบบความมั่นคงปลอดภัย (Audit Log)

6. ข้อเสนอแนะและแนวทางการปรับปรุง

- จัดทบทวนฐานทางกฎหมายและมาตรการทุก 12 เดือน
- ตรวจสอบสถานะ Adequacy ของประเทศปลายทางตามประกาศคณะกรรมการทุก 6 เดือน
- พัฒนาแบบฟอร์ม Legal Basis Checklist เพื่อใช้ก่อนการโอนข้อมูลทุกครั้ง

7. ผู้รับผิดชอบและช่องทางติดต่อ

นายกฤติน ทองจันทร์
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
 อีเมล: dpo@[ชื่องค์กร].co.th
 โทร: 02-xxx-xxxx ต่อ 123

7.4 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) องค์กรมีข้อปฏิบัติ/แนวปฏิบัติที่เหมาะสมเกี่ยวกับการดำเนินงานของผู้ประมวลผลข้อมูลส่วนบุคคล

7.4.1 องค์กรทำ DPA (Data Processing Agreement) กับผู้ประมวลผลข้อมูลส่วนบุคคลขององค์กรทุกราย

สิ่งที่ต้องทำ: มีการจัดทำ DPA (Data Processing Agreement) กับผู้ประมวลผลข้อมูลส่วนบุคคลครบถ้วนทุกราย

- หลักฐาน: รายชื่อของผู้ประมวลผลข้อมูลส่วนบุคคลขององค์กร ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 วรรคสาม ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 6 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 8 โทษทางปกครอง มาตรา 86 ในกรณีที่ไม่ปฏิบัติตาม มาตรา 40 กำหนดโทษปรับทางปกครอง ไม่เกิน 3 ล้านบาท

รายชื่อผู้ประมวลผลข้อมูลส่วนบุคคลขององค์กร

องค์กรได้ทำข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ทั้งหมดที่ได้รับมอบหมายให้ดำเนินการใดๆ แทนองค์กร ซึ่งรวมถึงการจัดเก็บ ประมวลผล วิเคราะห์ หรือถ่ายโอนข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

ลำดับ	ชื่อบริษัท	ประเภทบริการ	ประเภทข้อมูลที่ประมวลผล	หมายเหตุ
1	บริษัท ABC จำกัด	บริการคลาวด์ (Cloud Storage)	ข้อมูลลูกค้า, ข้อมูลบัญชี	ใช้ AWS Southeast
2	บริษัท XYZ จำกัด	บริการวิเคราะห์ข้อมูล	ข้อมูลการใช้งานระบบ, Log	มีการเข้าถึงข้อมูลโดยตรง
3	บริษัท 123 จำกัด	พัฒนาเว็บไซต์และ API	ข้อมูลแบบฟอร์ม, ข้อมูลผู้สมัคร	มี Sub-Processor
4	บริษัท DEF จำกัด	ระบบสำรองข้อมูล	ข้อมูลทั้งหมดแบบเข้ารหัส	ทำ Data Backup รายวัน
5	บริษัท GHI จำกัด	ระบบบัญชี HR	ข้อมูลเงินเดือน, รายชื่อพนักงาน	มีข้อมูลอ่อนไหวบางส่วน

2. รายละเอียดข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

ทุกบริษัทที่ระบุข้างต้นได้ทำสัญญาข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ซึ่งมีสาระสำคัญ ดังนี้

1. วัตถุประสงค์ของการประมวลผล

- 1.1. ระบุวัตถุประสงค์เฉพาะของแต่ละ Data Processor
- 1.2. ระบุลักษณะบริการที่ใช้และผลกระทบต่อเจ้าของข้อมูล

2. ประเภทและกลุ่มของข้อมูล

- 2.1. ประเภทข้อมูล: ข้อมูลส่วนบุคคลทั่วไป, ข้อมูลทางบัญชี, ข้อมูลอ่อนไหวบางประเภท
- 2.2. กลุ่มเจ้าของข้อมูล: ลูกค้า, พนักงาน, ผู้สมัครงาน, ผู้ใช้งานระบบ

3. ระยะเวลาการประมวลผล

- 3.1. เริ่มนับตั้งแต่วันที่ลงนามสัญญา จนถึงสิ้นสุดการให้บริการ

3.2. มีข้อกำหนดการลบหรือคืนข้อมูลหลังสิ้นสุดสัญญาภายใน 30 วัน

4. สิทธิและหน้าที่ของคู่สัญญา

- 4.1. ผู้ประมวลผลต้องปฏิบัติตามคำสั่งขององค์กร
- 4.2. ห้ามใช้ข้อมูลเพื่อประโยชน์อื่น
- 4.3. ต้องช่วยเหลือองค์กรในการปฏิบัติตามสิทธิของเจ้าของข้อมูล เช่น การขอลบข้อมูล

5. มาตรการรักษาความมั่นคงปลอดภัย

- 5.1. การเข้ารหัสข้อมูล (Encryption)
- 5.2. การควบคุมการเข้าถึง (Access Control)
- 5.3. การเก็บ Log การใช้งาน
- 5.4. การอบรมความรู้ด้านการคุ้มครองข้อมูลแก่พนักงาน

6. การแจ้งเหตุการณ์ละเมิดข้อมูล (Data Breach Notification)

- 6.1. แจ้งองค์กรภายใน 24 ชั่วโมงหลังพบเหตุ
- 6.2. ส่งรายงานผลการสอบสวนภายใน 72 ชั่วโมง
- 6.3. ประสานงานร่วมกันหากต้องแจ้งคณะกรรมการ

7. การใช้ผู้ประมวลผลย่อย (Sub-processor)

- 7.1. ต้องแจ้งองค์กรล่วงหน้าและได้รับความเห็นชอบเป็นลายลักษณ์อักษร
- 7.2. Sub-processor ต้องมี DPA กับผู้ประมวลผลหลักด้วย

8. การตรวจสอบและการประเมิน

- 8.1. องค์กรมีสิทธิในการขอตรวจสอบหรือทำ audit เพื่อประเมินความสอดคล้องของการปฏิบัติงาน
- 8.2. จัดให้มีการรายงานประจำปีเกี่ยวกับการประมวลผลข้อมูล

9. การรับผิดชอบทางกฎหมาย

- 9.1. ผู้ประมวลผลต้องรับผิดชอบหากเกิดการละเมิดจากความประมาทเลินเล่อ
- 9.2. มีข้อกำหนดค่าปรับกรณีผิดสัญญาหรือไม่แจ้งเหตุละเมิดข้อมูล

3. สถานะของข้อตกลง

- ข้อตกลง DPA ทั้งหมดมีผลบังคับใช้แล้ว ตั้งแต่ไตรมาสที่ 1 ปี 2567
- มีการจัดเก็บสำเนาสัญญาในระบบ DMS ขององค์กร พร้อมวันหมดอายุและวันต่ออายุสัญญา
- มีการทบทวนข้อตกลงปีละ 1 ครั้ง ตามนโยบาย Governance ขององค์กร

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement - DPA)

ระหว่าง

บริษัท [ชื่อองค์กร] (“ผู้ควบคุมข้อมูลส่วนบุคคล” หรือ “ผู้ว่าจ้าง”)

ที่อยู่: [ที่อยู่ขององค์กร]

และ

บริษัท [ชื่อผู้ประมวลผล] (“ผู้ประมวลผลข้อมูลส่วนบุคคล” หรือ “ผู้รับจ้าง”)

ที่อยู่: [ที่อยู่ของผู้ประมวลผล]

ลงวันที่: [วัน เดือน ปี]

ข้อ 1: ความหมายในข้อตกลงฉบับนี้

- “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาซึ่งสามารถระบุตัวตนได้
- “การประมวลผล” หมายถึง การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล เช่น การรวบรวม ใช้ เก็บ รักษาเปิดเผย ฯลฯ
- “PDPA” หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ข้อ 2: วัตถุประสงค์ของการประมวลผล

ผู้ประมวลผลตกลงที่จะประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูล เพื่อให้บริการ [ระบุลักษณะบริการ เช่น พัฒนาแอป, จัดเก็บคลาวด์, วิเคราะห์ข้อมูล ฯลฯ] ภายใต้ขอบเขตของข้อตกลงฉบับนี้เท่านั้น

ข้อ 3: ประเภทข้อมูลและเจ้าของข้อมูล

- ผู้ประมวลผลอาจเข้าถึงหรือจัดการข้อมูลดังต่อไปนี้:
- ข้อมูลทั่วไป: ชื่อ, เบอร์โทร, อีเมล
- ข้อมูลที่มีความอ่อนไหว: [หากมี เช่น สุขภาพ ความพิการ ฯลฯ]
- กลุ่มเจ้าของข้อมูล: ลูกค้า พนักงาน ผู้ใช้งานระบบ ฯลฯ

ข้อ 4: ระยะเวลาของการประมวลผล

- การประมวลผลจะดำเนินการระหว่าง:
- วันที่เริ่มต้นสัญญา: [ระบุ]
- จนถึง: [ระบุวันสิ้นสุด หรือ “สิ้นสุดการให้บริการ”]

ข้อ 5: หน้าที่ของผู้ประมวลผล

ผู้ประมวลผลตกลงจะ

- ประมวลผลข้อมูลเฉพาะตามคำสั่งของผู้ควบคุมเท่านั้น
- ไม่ใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่น
- ดำเนินมาตรการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม เช่น การเข้ารหัส การควบคุมการเข้าถึง
- แจ้งเหตุการละเมิดข้อมูลต่อผู้ควบคุมภายใน 24 ชั่วโมง และส่งรายงานภายใน 72 ชั่วโมง
- ลบหรือส่งคืนข้อมูลเมื่อสิ้นสุดการให้บริการ
- ไม่โอนข้อมูลให้ Sub-processor โดยไม่ได้รับอนุญาตล่วงหน้า

ข้อ 6: สิทธิของผู้ควบคุมข้อมูล

- ผู้ควบคุมมีสิทธิ
- ตรวจสอบและประเมินมาตรการของผู้ประมวลผลได้ตามสมควร
- ขอรับรายงานประจำปีเกี่ยวกับการประมวลผล
- เรียกร้องให้ผู้ประมวลผลลบ แก้ไข หรือจำกัดการประมวลผลข้อมูลตามคำขอของเจ้าของข้อมูล

ข้อ 7: การใช้ผู้ประมวลผลย่อย (Sub-processor)

ผู้ประมวลผลจะไม่มอบหมายหรือโอนหน้าที่ให้แก่ Sub-processor เว้นแต่ได้รับความเห็นชอบเป็นลายลักษณ์อักษรจากผู้ควบคุม และจะต้องทำ DPA กับ Sub-processor ที่มีเนื้อหาสาระเช่นเดียวกับฉบับนี้

ข้อ 8: ความรับผิดชอบและการชดเชยค่าเสียหาย

ผู้ประมวลผลต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการละเมิดข้อตกลงนี้ โดยเฉพาะในกรณีที่เกิดจากการละเลย หรือการไม่ปฏิบัติตามกฎหมาย PDPA

ข้อ 9: การสิ้นสุดข้อตกลง

เมื่อสิ้นสุดการให้บริการ

- ผู้ประมวลผลจะต้องลบหรือส่งคืนข้อมูลทั้งหมดภายใน 30 วัน
- ต้องจัดส่งเอกสารรับรองว่าไม่มีการเก็บข้อมูลใด ๆ ไว้

ข้อ 10: กฎหมายที่ใช้บังคับ

ข้อตกลงนี้อยู่ภายใต้บังคับของกฎหมายไทย โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายอื่นที่เกี่ยวข้อง

ลงนามโดย

ผู้ควบคุมข้อมูลส่วนบุคคล

ลงชื่อ: _____

ชื่อ-สกุล:

ตำแหน่ง:

วันที่:

ผู้ประมวลผลข้อมูลส่วนบุคคล

ลงชื่อ: _____

ชื่อ-สกุล:

ตำแหน่ง:

วันที่:

7.4.2 DPA ประกอบด้วยเงื่อนไขอย่างน้อยตามที่กำหนดใน มาตรา 40 ได้แก่

1. ดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งเท่านั้น
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
3. แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
4. จัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
5. สิ่งที่ต้องทำ: มีการจัดทำ DPA (Data Processing Agreement) และประกอบเงื่อนไขตามที่กำหนดในกฎหมายฉบับอื่น

หลักฐาน: ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 วรรคแรก
โทษทางปกครอง มาตรา 86 ในกรณีที่ฝ่าฝืนปฏิบัติตาม มาตรา 40 กำหนดโทษปรับทางปกครอง ไม่เกิน 3 ล้านบาท

เงื่อนไขใน DPA ตามมาตรา 40

ข้อกำหนดเงื่อนไขสำคัญใน DPA (Data Processing Agreement)

1. ดำเนินการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมเท่านั้น
ผู้ประมวลผลต้องประมวลผลข้อมูลตามคำสั่งที่ได้รับเท่านั้น ไม่ใช้ข้อมูลในทางอื่นหรือเพื่อประโยชน์ส่วนตัว
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
ผู้ประมวลผลต้องมีมาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม เช่น
 1. การควบคุมการเข้าถึงข้อมูล
 2. การเข้ารหัสข้อมูล
 3. การสำรองข้อมูลและกู้คืนข้อมูล
 4. การป้องกันการโจมตีทางไซเบอร์

3. แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

กรณีเกิดเหตุละเมิดข้อมูล (Data Breach) ผู้ประมวลผลต้องแจ้งผู้ควบคุมข้อมูลทันทีโดยไม่มีความล่าช้า และรายงานรายละเอียดเหตุการณ์อย่างครบถ้วน

4. จัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลต้องจัดทำและเก็บบันทึกเกี่ยวกับการประมวลผล เช่น

1. ประเภทข้อมูลที่ประมวลผล
2. วัตถุประสงค์ของการประมวลผล
3. วันที่และระยะเวลาการเก็บรักษาข้อมูล
4. รายชื่อผู้ที่เข้าถึงข้อมูล

ตัวอย่างเนื้อหาเงื่อนไขใน DPA ที่ครอบคลุมมาตรา 40

ข้อ X: ข้อกำหนดการประมวลผลข้อมูลส่วนบุคคล

- ผู้ประมวลผลตกลงที่จะดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลเท่านั้น และห้ามใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่น
- ผู้ประมวลผลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันข้อมูลส่วนบุคคลจากการเข้าถึง ใช้ หรือเปิดเผยโดยไม่ได้รับอนุญาต รวมถึงมาตรการทางเทคนิคและองค์กร
- หากเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ผู้ประมวลผลจะต้องแจ้งผู้ควบคุมข้อมูลโดยทันที และให้ข้อมูลที่จำเป็นเพื่อให้ผู้ควบคุมสามารถดำเนินการตามกฎหมายได้อย่างถูกต้อง
- ผู้ประมวลผลจะต้องจัดทำและเก็บรักษาบันทึกการเกี่ยวกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการให้บริการตามข้อตกลงนี้ และจะเปิดเผยบันทึกดังกล่าวแก่ผู้ควบคุมข้อมูลเมื่อได้รับคำขอ

หลักฐานที่จัดเตรียมไว้

- ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ที่มีเนื้อหาครอบคลุมเงื่อนไขข้างต้น
- รายชื่อผู้ประมวลผลข้อมูลส่วนบุคคลที่องค์กรทำ DPA ด้วย
- ตัวอย่างบันทึกการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities - ROPA) ของผู้ประมวลผล

ตัวอย่างข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement - DPA) ฉบับสมบูรณ์ ที่เพิ่มรายละเอียดตามมาตรา 40 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฉบับนี้จัดทำขึ้นระหว่าง

(1) ผู้ควบคุมข้อมูลส่วนบุคคล: [ชื่อองค์กร]

ที่อยู่: [ที่อยู่]

(ต่อไปนี้จะเรียกว่า “ผู้ควบคุมข้อมูล”)

และ

(2) ผู้ประมวลผลข้อมูลส่วนบุคคล: [ชื่อผู้ประมวลผล]

ที่อยู่: [ที่อยู่]

(ต่อไปนี้จะเรียกว่า “ผู้ประมวลผล”)

เพื่อกำหนดข้อตกลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูล โดยมีรายละเอียดและเงื่อนไขดังต่อไปนี้

ข้อ 1 วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลจะดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูลเพื่อวัตถุประสงค์ [ระบุวัตถุประสงค์การประมวลผล] เท่านั้น

ข้อ 2 คำสั่งการประมวลผล

ผู้ประมวลผลตกลงที่จะดำเนินการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลเท่านั้น โดยไม่ใช่ข้อมูลในทางอื่นใดที่มีได้รับอนุญาตเป็นลายลักษณ์อักษร

ข้อ 3 ข้อมูลส่วนบุคคลและกิจกรรมการประมวลผล

3.1 ประเภทข้อมูลส่วนบุคคลที่ประมวลผล ได้แก่ [ระบุประเภทข้อมูล เช่น ข้อมูลส่วนบุคคลทั่วไป ข้อมูลสุขภาพ ฯลฯ]

3.2 กิจกรรมการประมวลผลที่ดำเนินการ เช่น การจัดเก็บ การบันทึก การใช้ การเปิดเผย การลบ ฯลฯ

3.3 ระยะเวลาการประมวลผล: [ระบุระยะเวลาที่จะเก็บข้อมูล]

ข้อ 4 มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ผู้ประมวลผลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันข้อมูลส่วนบุคคลจากการเข้าถึง การเปิดเผย การเปลี่ยนแปลง หรือการทำลายที่ไม่ได้รับอนุญาต รวมถึงแต่ไม่จำกัดเพียง

- การควบคุมการเข้าถึงข้อมูล (Access Control)
- การเข้ารหัสข้อมูล (Encryption)
- การสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Disaster Recovery)
- การตรวจสอบและบันทึกกิจกรรม (Audit Logs)
- การอบรมและให้ความรู้แก่พนักงานเกี่ยวกับความมั่นคงปลอดภัยข้อมูล

ข้อ 5 การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Data Breach)

ผู้ประมวลผลต้องแจ้งให้ผู้ควบคุมข้อมูลทราบโดยทันทีหากมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคลเกิดขึ้น โดยไม่เกิน [ระบุจำนวนชั่วโมง/วัน เช่น 24 ชั่วโมง] หลังจากทราบเหตุการณ์ และต้องให้ข้อมูลรายละเอียดเกี่ยวกับเหตุการณ์ รวมถึงมาตรการแก้ไขที่ได้ดำเนินการ

ข้อ 6 การจัดทำและเก็บรักษาบันทึกการประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลต้องจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการให้บริการตามข้อตกลงนี้อย่างครบถ้วน และต้องพร้อมเปิดเผยบันทึกดังกล่าวแก่ผู้ควบคุมข้อมูลหรือต่อหน่วยงานที่มีอำนาจตามกฎหมายเมื่อได้รับคำขอ

ข้อ 7 การใช้ผู้ประมวลผลข้อมูลย่อย (Sub-processor)

7.1 ผู้ประมวลผลจะไม่ใช้ผู้ประมวลผลข้อมูลย่อยโดยไม่ได้รับความยินยอมล่วงหน้าจากผู้ควบคุมข้อมูลเป็นลายลักษณ์อักษร

7.2 ผู้ประมวลผลต้องทำให้มั่นใจว่าผู้ประมวลผลข้อมูลย่อยปฏิบัติตามข้อกำหนดเดียวกับที่ระบุในข้อตกลงนี้

ข้อ 8 สิทธิของเจ้าของข้อมูลส่วนบุคคล

ผู้ประมวลผลจะช่วยสนับสนุนผู้ควบคุมข้อมูลในการตอบสนองต่อคำขอของเจ้าของข้อมูลตามสิทธิที่กำหนดไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น สิทธิขอเข้าถึงข้อมูล สิทธิขอลบข้อมูล และสิทธิคัดค้านการประมวลผล

ข้อ 9 การคืนหรือทำลายข้อมูลส่วนบุคคล

เมื่อสิ้นสุดการให้บริการหรือเมื่อผู้ควบคุมข้อมูลร้องขอ ผู้ประมวลผลต้องคืนข้อมูลส่วนบุคคลทั้งหมดให้แก่ผู้ควบคุมข้อมูลหรือทำลายข้อมูลดังกล่าวตามคำสั่งของผู้ควบคุมข้อมูลโดยทันที ยกเว้นมีข้อกำหนดทางกฎหมายที่อนุญาตให้เก็บรักษาข้อมูลต่อ

ข้อ 10 การตรวจสอบและการทบทวน

ผู้ควบคุมข้อมูลมีสิทธิในการตรวจสอบหรือมอบหมายบุคคลที่เชื่อถือได้เข้าตรวจสอบการปฏิบัติตามข้อตกลงนี้ของผู้ประมวลผล รวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัย

ข้อ 11 ความรับผิดชอบและการชดเชยค่าเสียหาย

ผู้ประมวลผลต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการละเมิดข้อกำหนดตามข้อตกลงนี้ และต้องชดเชยค่าเสียหายแก่ผู้ควบคุมข้อมูลตามที่กฎหมายกำหนด

ข้อ 12 กฎหมายที่ใช้บังคับและเขตอำนาจศาล

ข้อตกลงนี้อยู่ภายใต้บังคับของกฎหมาย [ระบุประเทศ เช่น กฎหมายไทย] และคู่สัญญาตกลงที่จะอยู่ภายใต้เขตอำนาจศาลของ [ระบุศาล เช่น ศาลไทย]

ลงชื่อผู้ควบคุมข้อมูล

.....

ชื่อ:

ตำแหน่ง:

วันที่:

ลงชื่อผู้ประมวลผลข้อมูล

.....

ชื่อ:

ตำแหน่ง:

วันที่:

7.4.3 ในกรณีที่องค์กรใช้ผู้ประมวลผลข้อมูลส่วนบุคคล องค์กรได้ประเมินความเสี่ยงที่เกี่ยวข้องและมีการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม

สิ่งที่ต้องทำ: มีการประเมินความเสี่ยงและมีการบริหารจัดการความเสี่ยง

หลักฐาน: แบบประเมินและผลการประเมินความเสี่ยง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

แบบประเมินความเสี่ยงและผลการประเมินความเสี่ยงในการใช้ผู้ประมวลผลข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการใช้ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ให้เป็นไปอย่างเหมาะสมและสอดคล้องกับนโยบายความมั่นคงปลอดภัยข้อมูลขององค์กร

2. ขอบเขตการประเมิน

- ผู้ประมวลผลข้อมูลส่วนบุคคลทั้งหมดที่องค์กรให้บริการ
- กิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่ได้รับมอบหมาย

3. ขั้นตอนการประเมินความเสี่ยง

ขั้นตอน	รายละเอียด	หมายเหตุ
3.1 ระบุผู้ประมวลผลข้อมูล	ระบุรายชื่อและรายละเอียดผู้ประมวลผลข้อมูล	[ชื่อบริษัท, ที่อยู่, ขอบเขตงาน]
3.2 ประเมินความเสี่ยงด้านความมั่นคงปลอดภัย	ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของผู้ประมวลผล เช่น การเข้ารหัสข้อมูล การควบคุมการเข้าถึง	ให้คะแนน 1-5 หรือระดับต่ำ/กลาง/สูง
3.3 ประเมินความเสี่ยงด้านการละเมิดข้อมูล	ตรวจสอบประวัติการละเมิดข้อมูล (ถ้ามี) และวิธีการแจ้งเหตุ	รายละเอียดเหตุการณ์ที่ผ่านมา
3.4 ประเมินความเสี่ยงด้านการปฏิบัติตามกฎหมาย	ตรวจสอบว่าผู้ประมวลผลมี DPA ครบถ้วนและปฏิบัติตามกฎหมาย PDPA	มี/ไม่มี
3.5 ประเมินความเสี่ยงอื่นๆ	เช่น ความเสี่ยงทางเทคนิค ความเสี่ยงจากบุคลากร ฯลฯ	รายละเอียด

4. ผลการประเมินความเสี่ยงและการบริหารจัดการ

ความเสี่ยงที่พบ	ระดับความเสี่ยง	มาตรการบริหารจัดการ	ผู้รับผิดชอบ	กำหนดเวลา
ตัวอย่าง: มาตรการรักษาความมั่นคงปลอดภัยไม่เพียงพอ	สูง	ขอให้ผู้ประมวลผลปรับปรุงระบบเข้ารหัสข้อมูลภายใน 30 วัน	ฝ่าย IT	30 วัน
ตัวอย่าง: ไม่มีประวัติละเมิดข้อมูล	ต่ำ	เฝ้าระวังตามปกติ	ฝ่ายความมั่นคงข้อมูล	ต่อเนื่อง

5. สรุปและขอเสนอแนะ

สรุปผลการประเมินโดยรวม พร้อมข้อเสนอแนะเพื่อปรับปรุงและลดความเสี่ยง

6. ลงชื่อผู้ประเมินและอนุมัติ

ผู้ประเมิน: _____

วันที่: _____

ผู้อนุมัติ: _____

วันที่: _____

7.4.3 ในกรณีที่ต้องใช้ผู้ประมวลผลข้อมูลส่วนบุคคล องค์กรได้ประเมินความเสี่ยงที่เกี่ยวข้องและมีการบริหารจัดการความเสี่ยงนั้นอย่างเหมาะสม

สิ่งที่ต้องทำ: มีการประเมินความเสี่ยงและมีการบริหารจัดการความเสี่ยง

หลักฐาน: แบบประเมินและผลการประเมินความเสี่ยง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

แบบประเมินความเสี่ยงและผลการประเมินความเสี่ยงในการใช้ผู้ประมวลผลข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อประเมินและบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการใช้ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ให้เป็นไปอย่างเหมาะสมและสอดคล้องกับนโยบายความมั่นคงปลอดภัยข้อมูลขององค์กร

2. ขอบเขตการประเมิน

- ผู้ประมวลผลข้อมูลส่วนบุคคลทั้งหมดที่องค์กรให้บริการ
- กิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่ได้รับมอบหมาย

3. ขั้นตอนการประเมินความเสี่ยง

ขั้นตอน	รายละเอียด	หมายเหตุ
3.1 ระบุผู้ประมวลผลข้อมูล	ระบุรายชื่อและรายละเอียดผู้ประมวลผลข้อมูล	[ชื่อบริษัท, ที่อยู่, ขอบเขตงาน]
3.2 ประเมินความเสี่ยงด้านความมั่นคงปลอดภัย	ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของผู้ประมวลผล เช่น การเข้ารหัสข้อมูล การควบคุมการเข้าถึง	ให้คะแนน 1-5 หรือ ระดับต่ำ/กลาง/สูง
3.3 ประเมินความเสี่ยงด้านการละเมิดข้อมูล	ตรวจสอบประวัติการละเมิดข้อมูล (ถ้ามี) และวิธีการแจ้งเหตุ	รายละเอียดเหตุการณ์ที่ผ่านมา

3.4 ประเมินความเสี่ยงด้านการปฏิบัติตามกฎหมาย	ตรวจสอบว่าผู้ประมวลผลมี DPA ครบถ้วนและปฏิบัติตามกฎหมาย PDPA	มี/ไม่มี
3.5 ประเมินความเสี่ยงอื่น ๆ	เช่น ความเสี่ยงทางเทคนิค ความเสี่ยงจากบุคลากร ฯลฯ	รายละเอียด

4. ผลการประเมินความเสี่ยงและการบริหารจัดการ

ความเสี่ยงที่พบ	ระดับความเสี่ยง	มาตรการบริหารจัดการ	ผู้รับผิดชอบ	กำหนดเวลา
ตัวอย่าง: มาตรการรักษาความมั่นคงปลอดภัยไม่เพียงพอ	สูง	ขอให้ผู้ประมวลผลปรับปรุงระบบเข้ารหัสข้อมูลภายใน 30 วัน	ฝ่าย IT	30 วัน
ตัวอย่าง: ไม่มีประวัติละเมิดข้อมูล	ต่ำ	เฝ้าระวังตามปกติ	ฝ่ายความมั่นคงข้อมูล	ต่อเนื่อง

5. สรุปและขอเสนอแนะ

สรุปผลการประเมินโดยรวม พร้อมขอเสนอแนะเพื่อปรับปรุงและลดความเสี่ยง

6. ลงชื่อผู้ประเมินและอนุมัติ

ผู้ประเมิน: _____

วันที่: _____

ผู้อนุมัติ: _____

วันที่: _____

7.4.4 DPA ลงนามโดยผู้บริหารระดับสูงขององค์กร หรือเป็นกรณีให้ผู้บริหารในระดับการจัดการที่เหมาะสม (Appropriate Level of Management) มีอำนาจลงนามแทน องค์กรมีนโยบายหรือแนวปฏิบัติที่ชัดเจนในการมอบหมาย โดยพิจารณาให้ได้สัดส่วนกับมูลค่าและความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดใน DPA

สิ่งที่ต้องทำ: มีนโยบายหรือแนวปฏิบัติที่ชัดเจนในการมอบหมายผู้รับผิดชอบลงนาม และมีการพิจารณาถึงสัดส่วนกับมูลค่าและความเสี่ยงอย่างเหมาะสม

หลักฐาน: ขั้นตอนและผู้รับผิดชอบในการอนุมัติลงนาม DPA ขององค์กร

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ขั้นตอนและนโยบายการมอบหมายผู้มีอำนาจลงนามในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA Signing Authority Policy)

1. วัตถุประสงค์

เพื่อกำหนดนโยบายและขั้นตอนการมอบหมายผู้มีอำนาจลงนามในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) ให้เหมาะสมกับมูลค่าและความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคล รวมทั้งรับประกันการอนุมัติอย่างถูกต้องตามระดับการบริหารที่เหมาะสม

2. ขอบเขต

นโยบายนี้ครอบคลุมการมอบหมายผู้มีอำนาจลงนามใน DPA ขององค์กรสำหรับผู้ประมวลผลข้อมูลส่วนบุคคลทุกราย

3. นโยบายการมอบหมายผู้มีอำนาจลงนาม

- ผู้มีอำนาจลงนาม DPA ได้แก่ ผู้บริหารระดับสูง (เช่น กรรมการผู้จัดการ, CEO, COO) หรือผู้บริหารระดับกลางที่ได้รับมอบหมายอย่างเป็นทางการตามลำดับชั้นบริหาร
- การมอบหมายจะต้องสอดคล้องกับมูลค่าและความเสี่ยงของการประมวลผลข้อมูล เช่น การประมวลผลข้อมูลที่มีมูลค่าสูงหรือเสี่ยงสูงต้องให้ผู้บริหารระดับสูงลงนามโดยตรง
- กรณีมูลค่าและความเสี่ยงต่ำ สามารถมอบหมายให้ผู้บริหารระดับการจัดการที่เหมาะสม เช่น ผู้จัดการฝ่าย หรือหัวหน้าหน่วยงานที่รับผิดชอบ ลงนามแทนได้
- ต้องมีการจัดทำบันทึกการมอบหมายผู้มีอำนาจลงนามอย่างเป็นทางการ และมีการทบทวนอย่างน้อยปีละครั้ง

4. ขั้นตอนการอนุมัติและลงนาม DPA

ขั้นตอน	รายละเอียด	ผู้รับผิดชอบ
4.1 การจัดเตรียม DPA	ฝ่ายกฎหมายหรือฝ่ายบริหารความเสี่ยงจัดทำ DPA ตามข้อกำหนดและตรวจสอบเบื้องต้น	ฝ่ายกฎหมาย/ความเสี่ยง
4.2 การประเมินมูลค่าและความเสี่ยง	ประเมินมูลค่าและระดับความเสี่ยงของการประมวลผลข้อมูลที่จะทำตาม DPA	ฝ่ายบริหารความเสี่ยง/IT
4.3 การกำหนดผู้มีอำนาจลงนาม	อ้างอิงนโยบายมอบหมายผู้มีอำนาจลงนามตามมูลค่าและความเสี่ยง	ฝ่ายบริหารสูงสุด

4.4 การอนุมัติ DPA	ส่ง DPA ให้ผู้มีอำนาจลงนามตามที่กำหนดลงนาม	ผู้บริหารระดับสูงหรือระดับการจัดการที่มอบหมาย
4.5 การจัดเก็บและบันทึก	จัดเก็บเอกสาร DPA พร้อมสำเนาและบันทึกผู้ลงนามในระบบเอกสารขององค์กร	ฝ่ายบริหารเอกสาร/IT

5. ตัวอย่างโครงสร้างผู้มีอำนาจลงนามตามมูลค่าและความเสี่ยง

มูลค่าการประมวลผลข้อมูล	ระดับความเสี่ยง	ผู้มีอำนาจลงนาม
สูง (ข้อมูลสำคัญ/จำนวนมาก)	สูง	CEO หรือกรรมการผู้จัดการ
ปานกลาง	ปานกลาง	รองผู้จัดการทั่วไป / ผู้จัดการฝ่ายที่รับผิดชอบ
ต่ำ (ข้อมูลทั่วไป/น้อย)	ต่ำ	หัวหน้าหน่วยงานที่เกี่ยวข้อง

6. การตรวจสอบและทบทวน

- ฝ่ายบริหารความเสี่ยงและฝ่ายกฎหมายจะร่วมกันทบทวนการมอบหมายผู้มีอำนาจลงนามทุกปี
- ปรับปรุงนโยบายตามความเหมาะสมกับสภาพแวดล้อมทางธุรกิจและความเสี่ยงใหม่ ๆ ที่เกิดขึ้น

7. ลงชื่อรับรองนโยบาย

ผู้จัดทำ: _____

วันที่: _____

ผู้อนุมัติ: _____

วันที่: _____

7.4.5 องค์กรจัดทำบันทึกกลางของ DPA (Central Log of the Current DPA) ทั้งหมดขององค์กร เพื่อการควบคุม ตรวจสอบ และทบทวนเมื่อเงื่อนไขการประมวลผลเปลี่ยนแปลง

สิ่งที่ต้องทำ: มีการจัดทำบันทึกกลางของ DPA ทั้งหมดขององค์กร

หลักฐาน: บันทึกกลางของ DPA ทั้งหมดขององค์กร

สภาพบังคับ: กฎหมายไม่ได้กำหนด

หลักฐานการจัดทำข้อตกลงเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคลช่วง (Sub-Processor Agreement)

1. วัตถุประสงค์

เพื่อกำหนดเงื่อนไขที่ชัดเจนในการใช้ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง (Sub-Processor) โดยผู้ประมวลผลข้อมูลหลักต้องได้รับอนุญาตจากองค์กร และมีการทำข้อตกลงเพื่อให้ผู้ประมวลผลข้อมูลช่วงรับผิดชอบตามเงื่อนไขเดียวกับผู้ประมวลผลข้อมูลหลัก

2. ขอบเขต

ครอบคลุมข้อตกลงระหว่างองค์กร, ผู้ประมวลผลข้อมูลหลัก, และผู้ประมวลผลข้อมูลช่วงทุกกรณี

3. เนื้อหาข้อตกลงเกี่ยวกับผู้ประมวลผลข้อมูลช่วง (Sub-Processor)

- **การอนุญาต:** ผู้ประมวลผลข้อมูลหลักต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากองค์กรก่อนการใช้ผู้ประมวลผลข้อมูลช่วง
- **ข้อตกลง:** ผู้ประมวลผลข้อมูลหลักต้องทำข้อตกลงเป็นลายลักษณ์อักษรกับผู้ประมวลผลข้อมูลช่วงโดยมีเงื่อนไขที่ไม่ต่ำกว่าข้อตกลงที่ทำกับองค์กร
- **ความรับผิดชอบ:** ผู้ประมวลผลข้อมูลหลักต้องรับผิดชอบต่อการกระทำหรือความผิดพลาดของผู้ประมวลผลข้อมูลช่วงเสมือนเป็นความรับผิดชอบของตนเอง
- **มาตรการรักษาความปลอดภัย:** ผู้ประมวลผลข้อมูลช่วงต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมและสอดคล้องกับที่กำหนดในข้อตกลงหลัก
- **การแจ้งเหตุละเมิด:** ผู้ประมวลผลข้อมูลช่วงต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อผู้ประมวลผลข้อมูลหลักทันทีที่ทราบ
- **การตรวจสอบ:** ผู้ประมวลผลข้อมูลหลักมีสิทธิ์ในการตรวจสอบหรือขอข้อมูลเพื่อยืนยันการปฏิบัติตามข้อตกลงจากผู้ประมวลผลข้อมูลช่วง

4. ตัวอย่างหลักฐาน

4.1 ข้อตกลงระหว่างผู้ประมวลผลข้อมูลหลักและผู้ประมวลผลข้อมูลช่วง

ข้อกำหนด	รายละเอียด
การอนุญาต	ผู้ประมวลผลข้อมูลหลักได้รับอนุญาตเป็นลายลักษณ์อักษรจากองค์กรก่อนเริ่มใช้ผู้ประมวลผลช่วง
ข้อตกลง	ทำสัญญาโดยมีเงื่อนไขเดียวกับ DPA ที่ทำกับองค์กร
ความรับผิดชอบ	ผู้ประมวลผลข้อมูลหลักรับผิดชอบความเสียหายที่เกิดจากผู้ประมวลผลช่วง

มาตรการรักษาความปลอดภัย	ระบุให้ผู้ประมวลผลช่วงต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
การแจ้งเหตุละเมิด	ผู้ประมวลผลช่วงแจ้งเหตุละเมิดทันทีและรายงานต่อผู้ประมวลผลหลัก
การตรวจสอบ	ผู้ประมวลผลหลักมีสิทธิ์ตรวจสอบผู้ประมวลผลช่วง

4.2 ตัวอย่างการอนุญาตให้ผู้ประมวลผลข้อมูลช่วง

หนังสืออนุญาตจากองค์กรมายังผู้ประมวลผลข้อมูลหลักอนุญาตให้ผู้ประมวลผลข้อมูลช่วงรายงานหรือบันทึกการอนุญาตให้ผู้ประมวลผลข้อมูลช่วงที่ได้รับการอนุมัติ

5. ลงชื่อผู้รับผิดชอบ

ผู้รับผิดชอบจัดทำข้อตกลง: _____

วันที่: _____

ผู้อนุมัติ: _____

วันที่: _____

บันทึกกลางข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Central Log of Data Processing Agreements)

1. วัตถุประสงค์

เพื่อจัดเก็บและบริหารจัดการข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) ทั้งหมดขององค์กรในที่เดียวอย่างเป็นระบบ เพื่อให้ง่ายต่อการควบคุม ตรวจสอบ และทบทวนเมื่อมีการเปลี่ยนแปลงเงื่อนไขการประมวลผลข้อมูล

2. ขอบเขต

ครอบคลุมข้อตกลง DPA ของผู้ประมวลผลข้อมูลส่วนบุคคลทุกรายที่องค์กรได้ทำสัญญาด้วย

3. เนื้อหาของบันทึกกลาง DPA

หมายเลข ที่	ชื่อผู้ ประมวลผล ข้อมูล	วันที่ทำ ข้อตกลง	ระยะเวลา สัญญา	ผู้มี อำนาจ ลงนาม	รายละเอียด มาตรการ ความมั่นคง	สถานะ (ใช้งาน/ หมดอายุ)	หมายเหตุ
001	บริษัท เอ็ก เซลเลนท์ จำกัด	10 ม.ค. 2565	1 ปี	CEO	มีมาตรการ เข้ารหัส ข้อมูล	ใช้งาน	ต่อสัญญา 10 ม.ค. 2566

002	บริษัท ดาต้าเซฟ จำกัด	15 ก.พ. 2566	2 ปี	ผู้จัดการ ฝ่าย IT	มีระบบแจ้ง เตือนเหตุ ละเมิด	ใช้งาน	กำลัง ตรวจสอบ ความเสี่ยง

4. ขั้นตอนการดูแลบันทึกกลาง

- ฝ่ายบริหารความเสี่ยงและฝ่ายกฎหมายรับผิดชอบในการจัดเก็บและอัปเดตบันทึกกลางนี้อย่างสม่ำเสมอ
- ตรวจสอบสถานะ DPA ทุกไตรมาสเพื่อให้แน่ใจว่าเงื่อนไขและสัญญายังคงเป็นปัจจุบัน
- แจ้งเตือนก่อนหมดอายุหรือเปลี่ยนแปลงเงื่อนไขอย่างน้อย 30 วัน
- บันทึกนี้เป็นเอกสารกลางที่ใช้ในการอ้างอิงในการตรวจสอบภายในและภายนอก

5. ตัวอย่างบันทึกการอัปเดต

วันที่อัปเดต	รายการที่อัปเดต	ผู้ดำเนินการ	หมายเหตุ
1 เม.ย. 258	ต่อสัญญา DPA บริษัท เอ็กเซลเลนซ์ จำกัด	ฝ่าย กฎหมาย	สัญญาใหม่ 1 ปี
10 เม.ย. 2568	ปรับปรุงมาตรการความมั่นคง บริษัท ดาต้าเซฟ จำกัด	ฝ่าย IT	เพิ่มระบบ 2FA

6. ลงชื่อผู้รับผิดชอบการจัดทำและดูแลบันทึกกลาง

ผู้รับผิดชอบ: _____

วันที่: _____

ผู้อนุมัติ: _____

วันที่: _____

7.4.6 ทบทวน DPA (Data Processing Agreement) อย่างสม่ำเสมอเพื่อให้มีความถูกต้องเป็นปัจจุบัน สอดคล้องกับการดำเนินงานที่แท้จริง

สิ่งที่ต้องทำ: มีการทบทวน DPA อย่างสม่ำเสมอ

หลักฐาน: หลักฐานการทบทวนข้อตกลงและความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลอย่างสม่ำเสมอ เช่น รายงานการประชุมที่เกี่ยวข้อง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

หลักฐานการทบทวนข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

(Data Processing Agreement Review)

1. วัตถุประสงค์

เพื่อให้ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) มีความถูกต้องและสอดคล้องกับการดำเนินงานจริงขององค์กรและผู้ประมวลผลข้อมูลส่วนบุคคลอย่างต่อเนื่อง

2. ขอบเขต

ครอบคลุม DPA ทุกฝ่ายที่องค์กรได้ทำไว้กับผู้ประมวลผลข้อมูลส่วนบุคคล

3. ขั้นตอนการทบทวน DPA

- กำหนดระยะเวลาในการทบทวน DPA อย่างน้อยปีละ 1 ครั้ง หรือเมื่อต้องมีการเปลี่ยนแปลงเงื่อนไขหรือขอบเขตของการประมวลผลข้อมูล
- ตรวจสอบความสอดคล้องของเนื้อหาใน DPA กับการปฏิบัติจริงของผู้ประมวลผล
- บันทึกข้อสรุป ผลการทบทวน และคำแนะนำที่เกี่ยวข้อง
- แจ้งผู้บริหารและฝ่ายที่เกี่ยวข้องเพื่อรับทราบและอนุมัติ
- ดำเนินการแก้ไขหรือปรับปรุงข้อตกลงตามที่จำเป็น

4. ตัวอย่างหลักฐานการทบทวน DPA

4.1 รายงานการประชุมทบทวน DPA

วันที่ประชุม	หัวข้อ	รายชื่อผู้เข้าร่วม	สรุปผลการทบทวน	การดำเนินการต่อ
20 มี.ค. 2568	ทบทวน DPA บริษัท เอ็กเซลเลนซ์ จำกัด	ฝ่ายกฎหมาย, ฝ่าย IT, ฝ่ายบริหารความเสี่ยง	DPA ยังเหมาะสม แต่เพิ่มข้อกำหนดเรื่องการแจ้งเหตุละเมิดข้อมูลภายใน 24 ชม.	แจ้งผู้ประมวลผลปรับปรุง DPA

4.2 แบบฟอร์มบันทึกผลการทบทวน

ชื่อผู้ประมวลผลข้อมูล	วันที่ทำ DPA	วันที่ทบทวนล่าสุด	ผลการทบทวน	หมายเหตุ
บริษัท ดาต้าเซฟ จำกัด	15 ก.พ. 2566	1 เม.ย. 2568	สอดคล้องและครบถ้วน	-

5. ลงชื่อผู้รับผิดชอบทบทวนและอนุมัติ

ผู้รับผิดชอบทบทวน: _____

วันที่: _____

ผู้อนุมัติ: _____

วันที่: _____

7.4.7 มีข้อตกลงที่ชัดเจนเกี่ยวกับเงื่อนไขการใช้ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง (sub-processor) ว่าต้องดำเนินการอย่างไร เช่น ต้องได้รับอนุญาตก่อน ต้องมีการทำข้อตกลงระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลช่วง เพื่อให้ต้องรับผิดชอบต่อองค์กร เป็นต้น

สิ่งที่ต้องทำ: มีข้อตกลงเกี่ยวกับเงื่อนไขการใช้ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงที่ชัดเจน

หลักฐาน: ข้อตกลงระหว่างผู้ประมวลผลข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

สัญญาการประมวลผลข้อมูลส่วนบุคคล

นายจ้าง: _____

ฝ่าย/แผนก _____

ลูกจ้าง: _____

วันที่: _____

สัญญาการประมวลผลข้อมูลส่วนบุคคล

เขียนที่ _____

สัญญาทำขึ้นเมื่อวันที่ _____

ระหว่าง

สัญญาฉบับนี้ทำขึ้นระหว่างบริษัท_____ จำกัด สำนักงานตั้งอยู่_____	
_____ โดย_____ ตำแหน่ง_____	
_____ ผู้รับมอบอำนาจ ซึ่งต่อไปในสัญญานี้จะเรียกว่า “ผู้ควบคุมข้อมูลส่วนบุคคล” ฝ่ายหนึ่ง	
กับ_____ บุตรประจำตัวประชาชน หรือหนังสือเดินทางเลขที่_____	
_____ อยู่บ้านเลขที่_____ หมู่_____ ตำบล_____	
_____ อำเภอ_____ จังหวัด_____	
_____ โทรศัพท์_____ อีเมล_____ ชื่อที่ใช้ในไลน์_____	
_____ ไลน์ไอดี_____ ซึ่งต่อไปนี้จะเรียกว่า “ผู้ประมวลผลข้อมูลส่วนบุคคล” อีกฝ่ายหนึ่ง	
โดยที่ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล โดยมีข้อกำหนดและขอบเขตดังนี้	
วัตถุประสงค์	
1. ผู้ควบคุมข้อมูลส่วนบุคคล ตกลงให้ผู้ประมวลผลจัดทำ การประมวลผลข้อมูลส่วนบุคคล ตามรายการที่แนบท้ายสัญญานี้ หมายเลข..... โดยให้ผู้ประมวลผลดำเนินการ_____	

2. การประมวลผลข้อมูลส่วนบุคคลตามคำสั่ง	
ผู้ประมวลผลตกลงที่จะดำเนินการประมวลผลข้อมูลตามคำสั่งของผู้ควบคุมข้อมูลตามข้อ ๑. ข้างต้น โดยตกลงที่จะดำเนินการตามคำสั่งอย่างเคร่งครัด และตกลงจะรักษาความมั่นคงปลอดภัยตามมาตรฐานที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดและบังคับใช้	
3. นิยามของข้อมูลส่วนบุคคล	
ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ	
4. เงื่อนไขการประมวลผลข้อมูลส่วนบุคคล	
การประมวลผลตามสัญญานี้ ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงที่จะประมวลผลข้อมูลส่วนบุคคลภายใต้เงื่อนไขดังต่อไปนี้	
4.1 ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงประมวลผลข้อมูลส่วนบุคคลตามคำสั่งที่ระบุเอาไว้ในข้อ 1. เท่านั้น	
4.2 ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงจะไม่เปิดเผยข้อมูลส่วนบุคคลแก่บุคคลอื่น เว้นแต่จะเป็นการเปิดเผยแก่พนักงาน หรือลูกจ้าง หรือบุคคลใด ๆ ซึ่งปฏิบัติงานตามคำสั่งของผู้ประมวลผลข้อมูลส่วนบุคคล โดยผู้ประมวลผลตกลงที่จะกำกับการปฏิบัติงานของบุคคลดังกล่าวให้การดำเนินงานเป็นไปตามวัตถุประสงค์ ตลอดจนการมีมาตรการรักษาความมั่นคงปลอดภัย และมาตรการต่าง ๆ ที่กฎหมายที่เกี่ยวข้องกำหนด	

4.3 ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องไม่ทำการคัดลอก ทำซ้ำซึ่งข้อมูลส่วนบุคคล เว้นแต่การทำซ้ำนั้นเป็นส่วนหนึ่งของการทำตามคำสั่ง หรือเพื่อให้บรรลุผลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล

4.4 หากผู้ประมวลผลข้อมูลส่วนบุคคลมีการเปลี่ยนแปลงกิจการ หรือเปลี่ยนตัวนิติบุคคลไม่ว่าด้วยเหตุใด ๆ อันส่งผลให้มีการเปลี่ยนแปลงตัวคู่สัญญา ผู้ประมวลผลข้อมูลส่วนบุคคลสัญญาว่าจะแจ้งให้ผู้ควบคุมข้อมูลทราบในทันที หากกิจการใหม่นั้นไม่มีมาตรการตามที่กำหนดเอาไว้ หรือมีแต่ต่ำกว่าที่ตกลงกันไว้ในสัญญานี้ และ/หรือที่กฎหมายกำหนดให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลผิดสัญญา

5. การรักษาความมั่นคงปลอดภัย

5.1 ผู้ประมวลผลตกลงว่ามีการดำเนินการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด รายละเอียดปรากฏตามเอกสารที่เกี่ยวข้องกับการดำเนินการตามกฎหมาย เอกสารแนบท้ายหมายเลข

5.2 ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงว่าจะดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยและเข้ารหัสซึ่งความลับของข้อมูลส่วนบุคคล ทั้งมาตรการรักษาความมั่นคงปลอดภัยทางด้านการบริหาร ทางด้านกายภาพ ทางด้านเทคนิค หรือมาตรการอื่นซึ่งจะมีขึ้นในภายภาคหน้า ทั้งนี้ ตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะประกาศกำหนด และ/หรือตามความก้าวหน้าทางเทคโนโลยี

หากไม่มีการดำเนินการที่เหมาะสมจนกระทั่งมีการละเมิด หรือกระทำการอันไม่ชอบด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นที่เกี่ยวข้องอันทำให้ข้อมูลส่วนบุคคลเกิดการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงรับผิดชอบความเสียหายที่เกิดขึ้น

6. สิทธิของเจ้าของข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงว่าจะปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด รวมถึงการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบว่าการร้องขอเกี่ยวกับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

7. การแจ้งเตือน

7.1 กรณีมีการละเมิดข้อมูลส่วนบุคคลไม่ว่าด้วยวิธีการใด ๆ หรือเหตุใด ๆ ผู้ประมวลผลต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบในทันที ทั้งนี้ ไม่เกิน 24 ชั่วโมงนับแต่รับทราบถึงเหตุละเมิด

7.2 ผู้ประมวลผลต้องดำเนินการจัดทำมาตรการที่สมควรเพื่อแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคลด้วยมาตรการที่เหมาะสมในทันที โดยแจ้งให้ทราบในรายละเอียดต่าง ๆ ดังนี้

- แจ้งรายละเอียดของลักษณะ และผลที่เกิด หรืออาจเกิดขึ้นของการละเมิด รวมถึงข้อมูลอื่นที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล
- มาตรการที่ผู้ประมวลผลใช้เพื่อลดผลกระทบ และเยียวยาผลของการละเมิด
- ประเภทของข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลซึ่งถูกละเมิด

7.3 ผู้ประมวลผลตกลงจะเป็นผู้ชดใช้ความเสียหาย และเยียวยาความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล รวมถึงการรับผิดชอบตามกฎหมายไม่ว่าจะเป็นทางแพ่ง อาญา หรือทางปกครอง

7.4 ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการตามมาตรการที่สมควรและมีมาตรฐานไม่ต่ำกว่าที่กฎหมายกำหนดเพื่อให้ทราบถึงสาเหตุของการละเมิด และป้องกันมิให้เกิดการละเมิดซ้ำ

8. การลบ หรือทำลายข้อมูล

8.1 ผู้ประมวลผลข้อมูลส่วนบุคคลสัญญาว่าจะปฏิบัติตามนโยบายการลบข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคลตามเอกสารแนบท้ายสัญญาฉบับนี้ หมายเลข.....

8.2 ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงว่าจะส่งคืนข้อมูลส่วนบุคคลให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลภายใน 5 วัน นับแต่วันที่สัญญาสิ้นสุดลง หรือมีการส่งมอบงานงวดสุดท้าย หรือนับแต่วันที่.....

8.3 ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงว่าจะลบข้อมูลส่วนบุคคลหลังจากการยกเลิกข้อตกลงการประมวลผลข้อมูลส่วนบุคคล หรือลบเมื่อการดำเนินการประมวลผลเสร็จสิ้นบรรลุผลแล้วภายใน 5 วัน

อนึ่ง “การลบ” หมายถึง การทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกจากระบบ และไม่อาจกู้คืนได้ไม่ว่าบุคคลใด ๆ และไม่ว่าในเวลาใด ๆ

8.4 ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงว่าจะทำลายข้อมูลส่วนบุคคล

9. การเปิดเผย ส่งต่อ หรือโอนข้อมูลส่วนบุคคล

ประมวลผลข้อมูลส่วนบุคคลตกลงว่าจะไม่โอนข้อมูลส่วนบุคคล หรือเปิดเผยข้อมูลส่วนบุคคล หรือส่งต่อข้อมูลส่วนบุคคล หรือกระทำโดยประการใด ๆ ให้ผู้ไม่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลไม่ว่าด้วยวิธีการใด ๆ เว้นแต่จะได้รับความยินยอมจากผู้ควบคุมข้อมูลส่วนบุคคลโดยชัดแจ้ง

ข้อตกลงฉบับนี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกัน ทั้งสองฝ่ายได้อ่านและเข้าใจข้อความในข้อตกลงโดยละเอียดแล้ว จึงได้ลงลายมือชื่อพร้อมประทับตรา (ถ้ามี) ไว้เป็นสำคัญ ต่อหน้าพยานและต่างเก็บรักษาไว้ฝ่ายละหนึ่งฉบับ

สัญญานี้เป็นความลับ

เอกสารฉบับนี้เป็นการลงลายมือชื่ออิเล็กทรอนิกส์ที่จัดทำ และเก็บในฐานข้อมูลอิเล็กทรอนิกส์ของพนักงานของบริษัท ซึ่งได้ยืนยันตัวบุคคลของผู้ทำสัญญาทั้งสองฝ่ายอย่างถูกต้องแล้ว โดยบุคคลที่ไม่มีสิทธิไม่สามารถเข้าถึงระบบฐานข้อมูลนี้ได้

ลงชื่อ.....บริษัท
(.....)

กรรมการผู้จัดการ

พยาน

ประทับตราสำคัญของบริษัท

.....พยาน

(.....)

ลงชื่อ.....พนักงาน
(.....)

ลงชื่อ.....

(.....)

ลงชื่อ.....

เอกสารแนบท้ายสัญญา

เอกสารจากฝ่ายผู้ควบคุมข้อมูลส่วนบุคคล ได้แก่

คำสั่งให้ประมวลผล และวัตถุประสงค์ เอกสารแนบท้าย หมายเลข 1.

คำสั่ง

1. -----

2. -----

วัตถุประสงค์

1. -----

2. -----

ประเภทข้อมูลส่วนบุคคล

ข้อมูลทั่วไป ได้แก่

1. -----

2. -----

ข้อมูลอ่อนไหว

1. -----

2. -----

เอกสารจากฝ่ายประมวลผล ได้แก่

- นโยบายการลบข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล
- เอกสารแนบท้าย หมายเลข.....
- เอกสารที่เกี่ยวกับการการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

- เอกสารแนบท้ายหมายเลข.....เช่น นโยบายการคุ้มครองข้อมูลส่วนบุคคล ระเบียบหรือแนวปฏิบัติหรือข้อบังคับให้พนักงานหรือลูกจ้างปฏิบัติตามกฎหมายและมาตรการการคุ้มครองข้อมูลส่วนบุคคล มาตรการการรักษาความมั่นคงปลอดภัย บันทึกการกิจกรรมข้อมูลส่วนบุคคล (Ropa) เป็นต้น

หลักฐาน: ข้อตกลงการใช้ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง (Agreement on the Use of Sub-Processor)

1. คู่สัญญา

1.1 ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor): _____

1.2 ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง (Sub-Processor): _____

2. วัตถุประสงค์

เพื่อกำหนดขอบเขต เงื่อนไข และความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลช่วง ในการประมวลผลข้อมูลส่วนบุคคลแทนผู้ประมวลผลข้อมูลส่วนบุคคล ภายใต้คำสั่งและข้อตกลงที่ทำไว้กับผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

3. เงื่อนไขสำคัญ

3.1 การแต่งตั้ง: ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงจะปฏิบัติงานเฉพาะตามคำสั่งเป็นลายลักษณ์อักษรของผู้ประมวลผลข้อมูลส่วนบุคคล

3.2 การอนุญาต: ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลส่วนบุคคล ผ่านผู้ประมวลผลข้อมูลส่วนบุคคล ก่อนเริ่มดำเนินการ

3.3 สัญญาผูกพัน: ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงต้องลงนามในข้อตกลงนี้ เพื่อรับผิดชอบตามมาตรฐานที่เทียบเท่ากับผู้ประมวลผลข้อมูลส่วนบุคคล

3.4 ความลับและความมั่นคงปลอดภัย: ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงต้องดำเนินการด้านความมั่นคงปลอดภัยของข้อมูล และรักษาความลับตามที่กฎหมายกำหนด

3.5 ความรับผิด: ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการฝ่าฝืนข้อตกลง หรือการละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล

3.6 การสิ้นสุดสัญญา: เมื่อสัญญาสิ้นสุด ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงต้องลบหรือส่งคืนข้อมูลส่วนบุคคลทั้งหมดให้แก่ผู้ประมวลผลข้อมูลส่วนบุคคลตามที่กำหนด

4. เอกสารแนบท้าย สำเนาการอนุญาตจากผู้ควบคุมข้อมูลส่วนบุคคล รายการข้อมูลส่วนบุคคลที่ประมวลผล รายละเอียดมาตรการรักษาความมั่นคงปลอดภัยของผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

5. การลงนาม ลงนาม ณ วันที่ _____

ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor) (ลงนาม)

ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง (Sub-Processor) (ลงนาม)

7.5 เงื่อนไขข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Controller – Data Processor Contract Requirements) ภายใต้ DPA (Data Processing Agreement) มีเงื่อนไขครบถ้วนตามที่กฎหมายกำหนด

7.5.1 DPA (Data Processing Agreement) ควรระบุเงื่อนไขให้ครบถ้วนตามข้อ 7.4.2 และรวมถึงควรระบุเงื่อนไขดังต่อไปนี้

1. การปฏิบัติตามคำแนะนำของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่กฎหมายกำหนดให้ดำเนินการโดยไม่มีคำสั่งดังกล่าว.
2. บุคคลที่ประมวลผลข้อมูลส่วนบุคคลในนามของผู้รับจ้าง (พนักงาน/ลูกจ้าง) อยู่ภายใต้หน้าที่ในการรักษาความลับ.
3. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องช่วยองค์กรตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล.
4. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องยอมรับการตรวจสอบ (Audits and Inspections) โดยผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลภายนอกที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมาย

สิ่งที่ต้องทำ: มีเงื่อนไขตามที่กำหนดครบถ้วน

หลักฐาน: ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

หลักฐานการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

ตามข้อ 7.5.1

1. วัตถุประสงค์

เพื่อยืนยันว่าองค์กรได้จัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) ระหว่างองค์กร (ผู้ควบคุมข้อมูลส่วนบุคคล) กับผู้ประมวลผลข้อมูลส่วนบุคคล โดยมีเงื่อนไขครบถ้วนตามที่กฎหมายกำหนดในข้อ 7.4.2 และเงื่อนไขเพิ่มเติมในข้อ 7.5.1 อย่างครบถ้วน

2. เงื่อนไขหลักใน DPA ที่ครบถ้วนและสำคัญ

- ผู้ประมวลผลข้อมูลต้องดำเนินการตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่กฎหมายกำหนดให้ดำเนินการโดยไม่มีคำสั่งดังกล่าว

- บุคลากรของผู้ประมวลผลข้อมูล (พนักงาน ลูกจ้าง หรือบุคคลที่เกี่ยวข้อง) ต้องอยู่ภายใต้หน้าที่รักษาความลับและมีความรับผิดชอบต่อข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูลต้องช่วยองค์กรในการตอบสนองคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น การขอเข้าถึง การแก้ไข หรือการลบข้อมูล
- ผู้ประมวลผลข้อมูลต้องยอมรับการตรวจสอบ (Audit) และการตรวจสอบภายใน (Inspection) โดยผู้ควบคุมข้อมูล หรือบุคคลที่ได้รับมอบหมาย
- รวมถึงเงื่อนไขตามมาตรา 40 ในข้อ 7.4.2 เช่น การรักษาความมั่นคงปลอดภัย, การแจ้งเหตุละเมิดข้อมูล, การเก็บบันทึกรายการการประมวลผลข้อมูล

3. ตัวอย่างหลักฐาน

3.1 ตัวอย่างสาระสำคัญใน DPA

เงื่อนไข	รายละเอียด
การปฏิบัติตามคำสั่ง	ผู้ประมวลผลข้อมูลดำเนินการตามคำสั่งของผู้ควบคุมข้อมูลเท่านั้น
การรักษาความลับ	พนักงานผู้เกี่ยวข้องต้องรักษาความลับของข้อมูลส่วนบุคคล
ช่วยตอบสนองคำขอใช้สิทธิ	ผู้ประมวลผลข้อมูลต้องช่วยสนับสนุนองค์กรในการตอบคำขอของเจ้าของข้อมูล
การตรวจสอบ	ยอมรับการตรวจสอบและตรวจสอบภายในตามที่ผู้ควบคุมข้อมูลกำหนด
มาตรการรักษาความมั่นคงปลอดภัย	มีมาตรการรักษาความปลอดภัยข้อมูลที่เหมาะสม
การแจ้งเหตุละเมิด	แจ้งเหตุละเมิดข้อมูลโดยทันทีเมื่อเกิดเหตุ

3.2 ตัวอย่างบันทึกหรือรายงานที่เป็นหลักฐาน

- สัญญา DPA ที่ลงนามระหว่างองค์กรกับผู้ประมวลผลข้อมูลส่วนบุคคล
- รายงานผลการตรวจสอบการปฏิบัติตามข้อตกลงของผู้ประมวลผลข้อมูล
- รายงานการประชุมหรือบันทึกการทบทวน DPA
- รายงานการตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูล

4. สรุป

องค์กรมีการจัดทำและทบทวนข้อตกลงการประมวลผลข้อมูลส่วนบุคคลที่ระบุเงื่อนไขครบถ้วนตามข้อกำหนดทั้งมาตรา 40 และเงื่อนไขเพิ่มเติมในข้อ 7.5.1 เพื่อให้มั่นใจว่าการดำเนินการของผู้ประมวลผลข้อมูลเป็นไปอย่างถูกต้องและปลอดภัย

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement - DPA)

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

ระหว่าง

[ชื่อองค์กรผู้ควบคุมข้อมูลส่วนบุคคล] (ต่อไปนี้จะเรียกว่า "ผู้ควบคุมข้อมูล")

กับ

[ชื่อองค์กรผู้ประมวลผลข้อมูลส่วนบุคคล] (ต่อไปนี้จะเรียกว่า "ผู้ประมวลผลข้อมูล")

1. ขอบเขตของการประมวลผลข้อมูล

ผู้ประมวลผลข้อมูลจะดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูลและเฉพาะในขอบเขตตามคำสั่งที่ได้รับเท่านั้น

2. การรักษาความลับ

บุคลากรของผู้ประมวลผลข้อมูลที่เข้าถึงข้อมูลส่วนบุคคลต้องอยู่ภายใต้ข้อผูกพันรักษาความลับและห้ามเปิดเผยข้อมูลใด ๆ นอกเหนือจากที่ได้รับอนุญาตตามข้อตกลงนี้

3. มาตรการรักษาความมั่นคงปลอดภัย

ผู้ประมวลผลข้อมูลต้องจัดให้มีมาตรการทางเทคนิคและองค์กรที่เหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การเปิดเผย การเปลี่ยนแปลง หรือการทำลายข้อมูลโดยไม่ได้รับอนุญาต

4. การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลจะต้องแจ้งให้ผู้ควบคุมข้อมูลทราบโดยทันทีที่ทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลตามข้อตกลงนี้

5. การเก็บบันทึกกิจกรรมการประมวลผล

ผู้ประมวลผลข้อมูลต้องจัดทำและเก็บรักษายกยันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง และต้องสามารถนำเสนอเพื่อการตรวจสอบตามคำขอของผู้ควบคุมข้อมูล

6. การช่วยตอบสนองคำขอของเจ้าของข้อมูล

ผู้ประมวลผลข้อมูลต้องช่วยผู้ควบคุมข้อมูลในการตอบสนองคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น คำขอเข้าถึง แก้ไข หรือลบข้อมูล

7. การตรวจสอบและตรวจประเมิน

ผู้ควบคุมข้อมูลหรือผู้ที่ได้รับมอบหมาย มีสิทธิในการตรวจสอบ (audit) และตรวจประเมินการปฏิบัติตามข้อตกลงของผู้ประมวลผลข้อมูล

8. การใช้ผู้ประมวลผลข้อมูลช่วง (Sub-processor)

ผู้ประมวลผลข้อมูลต้องได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ควบคุมข้อมูลก่อนที่จะมอบหมายงานประมวลผลข้อมูลให้ผู้ประมวลผลข้อมูลช่วง และต้องทำข้อตกลงที่มีข้อผูกพันเทียบเท่า

ลงชื่อ

ผู้ควบคุมข้อมูล

วันที่

ลงชื่อ

ผู้ประมวลผลข้อมูล

วันที่

รายงานการตรวจสอบการปฏิบัติตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

ระหว่าง [ชื่อองค์กรผู้ควบคุมข้อมูล] กับ [ชื่อองค์กรผู้ประมวลผลข้อมูล]

วันที่ตรวจสอบ: [วันที่]

1. วัตถุประสงค์

เพื่อประเมินและตรวจสอบการปฏิบัติตามข้อตกลง DPA ที่ได้ทำไว้กับผู้ประมวลผลข้อมูล เพื่อให้มั่นใจว่าผู้ประมวลผลข้อมูลปฏิบัติตามข้อกำหนดด้านความปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

2. ขอบเขตการตรวจสอบ

- ตรวจสอบเงื่อนไขตามข้อ 1 ถึง 8 ของ DPA
- ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยที่นำมาใช้จริง
- ตรวจสอบการแจ้งเหตุละเมิดข้อมูล (ถ้ามี)
- ตรวจสอบการจัดทำบันทึกการกิจกรรมการประมวลผล
- ตรวจสอบการตอบสนองคำขอใช้สิทธิของเจ้าของข้อมูล
- ตรวจสอบการใช้ผู้ประมวลผลข้อมูลช่วง (Sub-processor)

3. ผลการตรวจสอบ

หัวข้อ	ผลการปฏิบัติ	หมายเหตุ

ปฏิบัติตามคำสั่งผู้ควบคุมข้อมูล	ผ่าน	การประมวลผลเป็นไปตามคำสั่งทุกประการ
การรักษาความลับ	ผ่าน	มีการลงนาม NDA กับพนักงาน
มาตรการรักษาความมั่นคงปลอดภัย	ผ่าน	ใช้มาตรการเข้ารหัสข้อมูลและระบบป้องกันการเข้าถึง
การแจ้งเหตุละเมิดข้อมูล	ไม่มี เหตุการณ์	-
การเก็บบันทึกรายการกิจกรรม	ผ่าน	มีการจัดเก็บบันทึกตามที่กำหนด
การช่วยตอบสนองคำขอใช้สิทธิ	ผ่าน	ดำเนินการตามคำขอเจ้าของข้อมูลอย่างเหมาะสม
การตรวจสอบและตรวจประเมิน	ผ่าน	ยินยอมให้มีการตรวจสอบจากผู้ควบคุมข้อมูล
การใช้ผู้ประมวลผลข้อมูลช่วง	ผ่าน	ได้รับอนุญาตและมีสัญญากับผู้ประมวลผลข้อมูลช่วง

4. สรุป

ผู้ประมวลผลข้อมูล [ชื่อองค์กร] ปฏิบัติตามข้อตกลง DPA อย่างเคร่งครัดและครบถ้วน ไม่มีข้อบกพร่องที่สำคัญในการปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคล

ลงชื่อผู้ตรวจสอบ

วันที่

7.5.2 DPA (Data Processing Agreement) กำหนดมาตรการด้านความมั่นคงปลอดภัยทั้งในเชิงองค์กรและเชิงเทคนิคที่ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มี เช่น การเข้ารหัส การแบ่งข้อมูล และการกักกันระบบ เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยมิชอบ

สิ่งที่ต้องทำ: มีการกำหนดมาตรการด้านความมั่นคงปลอดภัยใน DPA

หลักฐาน: ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 วรรคสาม
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 6
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 8

โทษทางปกครอง: มาตรา 86 ในกรณีที่ไม่ปฏิบัติตาม มาตรา 40 กำหนดโทษปรับทางปกครอง ไม่เกิน 3 ล้านบาท

ตัวอย่างเนื้อหามาตรการด้านความมั่นคงปลอดภัยในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

1. มาตรการด้านองค์กร (Organizational Security Measures)

1.1 นโยบายและแนวปฏิบัติด้านความปลอดภัยข้อมูลส่วนบุคคล

องค์กรต้องจัดทำนโยบายความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่ครอบคลุมทุกขั้นตอนของการประมวลผลข้อมูล ตั้งแต่การเก็บรวบรวม การใช้ การเปิดเผย การจัดเก็บ การถ่ายโอน ไปจนถึงการทำลายข้อมูล โดยนโยบายนี้จะต้องระบุความรับผิดชอบของพนักงานทุกระดับ รวมถึงผู้บริหารระดับสูงให้ชัดเจน โดยต้องประกาศให้พนักงานรับทราบและปฏิบัติตามอย่างเคร่งครัด นโยบายนี้ต้องได้รับการทบทวนและปรับปรุงอย่างสม่ำเสมอ (อย่างน้อยปีละครั้ง) เพื่อให้สอดคล้องกับการเปลี่ยนแปลงทางกฎหมาย เทคโนโลยี และความเสี่ยงใหม่ ๆ ที่เกิดขึ้น ต้องมีแนวทางปฏิบัติที่ชัดเจนในกรณีที่เกิดเหตุละเมิดข้อมูล หรือเหตุการณ์ด้านความปลอดภัย เช่น การแจ้งเตือน การสอบสวน การแก้ไข และการรายงานต่อหน่วยงานที่เกี่ยวข้อง

1.2 การกำหนดบทบาทและความรับผิดชอบ (Roles and Responsibilities)

องค์กรต้องกำหนดบทบาทและความรับผิดชอบที่ชัดเจนสำหรับผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ทั้งในส่วนของผู้ควบคุมข้อมูล (Data Controller) และผู้ประมวลผลข้อมูล (Data Processor)

แต่งตั้งเจ้าหน้าที่รับผิดชอบความปลอดภัยข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หรือเจ้าหน้าที่ที่รับผิดชอบเฉพาะทางด้านความมั่นคงปลอดภัยข้อมูล โดยเจ้าหน้าที่นี้ต้องมีความรู้ความสามารถเพียงพอในการปฏิบัติงาน

กำหนดขอบเขตหน้าที่ของพนักงานแต่ละคนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลให้ชัดเจน รวมถึงจำกัดการเข้าถึงข้อมูลตามความจำเป็น (need-to-know basis)

1.3 การฝึกอบรมและสร้างความตระหนักรู้ด้านความปลอดภัย (Training and Awareness)

ผู้ประมวลผลข้อมูลต้องดำเนินการฝึกอบรมพนักงานและผู้เกี่ยวข้องเรื่องการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยข้อมูลอย่างสม่ำเสมอ

จัดทำโปรแกรมอบรมสำหรับพนักงานใหม่ก่อนเริ่มงาน และอบรมซ้ำเป็นระยะ เพื่อสร้างความตระหนักรู้เกี่ยวกับความสำคัญของข้อมูลส่วนบุคคลและวิธีการป้องกันความเสี่ยง

ประเมินผลการอบรมและความเข้าใจของพนักงาน เช่น ผ่านแบบทดสอบหรือการประเมินผลด้านความปลอดภัย

ส่งเสริมวัฒนธรรมองค์กรที่ให้ความสำคัญกับความปลอดภัยข้อมูล และสนับสนุนให้พนักงานรายงานปัญหาและข้อผิดพลาดโดยไม่มีความกลัวผลกระทบ

1.4 การจัดการความเสี่ยงและการประเมินผล (Risk Management and Assessment)

- ผู้ประมวลผลข้อมูลต้องจัดให้มีการประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลอย่างสม่ำเสมอ เพื่อระบุจุดอ่อนหรือช่องโหว่ในระบบและกระบวนการประมวลผลข้อมูล

- การประเมินความเสี่ยงนี้ควรรวมถึงการวิเคราะห์ภัยคุกคาม ความเสี่ยงจากบุคคลภายในและภายนอก รวมทั้งผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูล
- วางแผนบริหารจัดการความเสี่ยงอย่างเหมาะสม เช่น การป้องกัน การตรวจจับ การตอบสนอง และการกู้คืนระบบ
- บันทึกผลการประเมินและแผนการแก้ไข เพื่อเป็นหลักฐานในการตรวจสอบภายในและภายนอก

1.5 การตรวจสอบและควบคุมภายใน (Internal Audit and Control)

- ต้องมีการตรวจสอบมาตรการความปลอดภัยและการปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยบุคคลหรือหน่วยงานที่มีความเป็นอิสระ
- การตรวจสอบนี้รวมถึงการประเมินการปฏิบัติตามข้อกำหนดทางกฎหมายและข้อกำหนดใน DPA ต้องมีรายงานผลการตรวจสอบ พร้อมคำแนะนำในการปรับปรุงแก้ไข และติดตามการดำเนินการแก้ไขตามคำแนะนำ
- ส่งเสริมการตรวจสอบร่วมกับผู้ควบคุมข้อมูล (Data Controller) ตามสิทธิในการตรวจสอบที่ระบุใน DPA

1.6 การจัดการเหตุการณ์ละเมิดข้อมูล (Incident Management)

- ผู้ประมวลผลข้อมูลต้องมีขั้นตอนที่ชัดเจนในการตรวจจับ จัดการ และรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- การแจ้งเหตุการณ์ต้องทำอย่างรวดเร็วและเป็นไปตามระยะเวลาที่กฎหมายกำหนด (เช่น ภายใน 72 ชั่วโมงใน GDPR หรือทันทีที่ได้รับทราบในกฎหมายไทย)
- การวางแผนรับมือเหตุการณ์ (Incident Response Plan) ต้องระบุวิธีการตรวจสอบต้นเหตุ การลดผลกระทบ และการป้องกันไม่ให้เกิดซ้ำ
- ต้องเก็บรักษาเอกสารและหลักฐานที่เกี่ยวข้องกับเหตุการณ์เพื่อใช้เป็นหลักฐานและปรับปรุงกระบวนการ

2. มาตรการด้านเทคนิค (Technical Security Measures)

2.1 การเข้ารหัสข้อมูล (Data Encryption)

การเข้ารหัสเป็นมาตรการหลักในการปกป้องข้อมูลส่วนบุคคลจากการเข้าถึงโดยไม่ได้รับอนุญาต โดยผู้ประมวลผลข้อมูลต้องใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมกับประเภทข้อมูลและช่องทางการสื่อสาร ข้อมูลที่ถูกเก็บรักษา (Data at Rest) ต้องถูกเข้ารหัสด้วยมาตรฐานที่ได้รับการยอมรับ เช่น AES-256 ข้อมูลที่ถูกส่งผ่านเครือข่าย (Data in Transit) ต้องถูกเข้ารหัสด้วยโปรโตคอลที่ปลอดภัย เช่น TLS 1.2 หรือสูงกว่า

กุญแจเข้ารหัสต้องถูกจัดการอย่างปลอดภัย มีการเปลี่ยนแปลงและเก็บรักษาอย่างเหมาะสม

2.2 การแฝงข้อมูล (Data Masking / Pseudonymisation)

เพื่อจำกัดการเปิดเผยข้อมูลที่สามารถระบุตัวตนได้ ผู้ประมวลผลข้อมูลควรนำเทคนิคการแฝงข้อมูลมาใช้ในระบบ เช่น

การลบหรือแทนที่ข้อมูลส่วนบุคคลด้วยค่าที่ไม่สามารถระบุเจ้าของได้โดยตรง (Pseudonymisation)

การลดความละเอียดของข้อมูล หรือการเปลี่ยนแปลงบางส่วนของข้อมูลเพื่อป้องกันการระบุตัวตน

2.3 การจัดการสิทธิ์การเข้าถึง (Access Control)

ต้องมีการควบคุมการเข้าถึงข้อมูลและระบบอย่างเข้มงวด โดยกำหนดสิทธิ์ตามบทบาทหน้าที่และความจำเป็นในการปฏิบัติงาน (Role-Based Access Control)

- การใช้รหัสผ่านที่มีความซับซ้อนและนโยบายการเปลี่ยนรหัสผ่านเป็นประจำ
- การใช้ระบบยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication: MFA) โดยเฉพาะสำหรับการเข้าถึงระบบที่มีข้อมูลสำคัญ
- การบันทึกและติดตามการเข้าถึงข้อมูลและระบบ (Access Logs) เพื่อใช้ในการตรวจสอบย้อนหลัง

2.4 การสำรองข้อมูลและแผนการกู้คืน (Backup and Disaster Recovery)

ผู้ประมวลผลข้อมูลต้องมีระบบสำรองข้อมูลที่เหมาะสมและแผนการกู้คืนระบบในกรณีเกิดเหตุการณ์ไม่คาดคิด เช่น ไฟดับ ไฟไหม้ หรือภัยคุกคามทางไซเบอร์

- ต้องสำรองข้อมูลอย่างสม่ำเสมอและเก็บในสถานที่ปลอดภัยที่แยกจากระบบหลัก
- ต้องทดสอบแผนการกู้คืนระบบอย่างน้อยปีละครั้ง เพื่อประเมินความพร้อมและความสามารถในการกลับมาทำงานได้รวดเร็ว
- มีมาตรการในการป้องกันข้อมูลสำรองจากการถูกแก้ไข หรือลบโดยไม่ได้รับอนุญาต

2.5 ระบบป้องกันมัลแวร์และการโจมตีทางไซเบอร์ (Anti-Malware and Cybersecurity)

- ผู้ประมวลผลข้อมูลต้องติดตั้งระบบป้องกันไวรัส มัลแวร์ และระบบป้องกันภัยคุกคามทางไซเบอร์ที่ทันสมัย
- ต้องอัปเดตฐานข้อมูลไวรัสและแพตช์ระบบอย่างสม่ำเสมอ
- มีระบบตรวจจับและตอบสนองต่อภัยคุกคาม เช่น ระบบตรวจสอบพฤติกรรมที่ผิดปกติ (Intrusion Detection Systems IDS)
- การจำกัดการติดตั้งซอฟต์แวร์และโปรแกรมที่ไม่ผ่านการอนุมัติ

2.6 การตรวจสอบและบันทึกกิจกรรม (Monitoring and Logging)

- การเก็บบันทึกกิจกรรมต่าง ๆ ในระบบช่วยในการตรวจสอบและวิเคราะห์เหตุการณ์ความปลอดภัย
- การบันทึกการเข้าใช้งาน การเปลี่ยนแปลงข้อมูล และเหตุการณ์ผิดปกติอย่างละเอียด
- การเก็บบันทึกต้องเก็บไว้ในที่ปลอดภัย และสามารถตรวจสอบย้อนหลังได้
- ต้องมีการวิเคราะห์และติดตามบันทึกเพื่อหาสัญญาณของการละเมิดหรือการโจมตี

3. มาตรการด้านกายภาพ (Physical Security Measures)

3.1 การควบคุมการเข้าถึงสถานที่ (Physical Access Control)

- ผู้ประมวลผลข้อมูลต้องมีมาตรการควบคุมการเข้าถึงสถานที่ที่ใช้จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลอย่างเข้มงวด

- ใช้ระบบควบคุมการเข้าออก เช่น บัตรประจำตัว บัตรแม่เหล็ก หรือระบบสแกนลายนิ้วมือ
- จำกัดการเข้าถึงแก่บุคลากรที่มีหน้าที่เท่านั้น
- จัดให้มีเจ้าหน้าที่รักษาความปลอดภัยตรวจตราและดูแลสถานที่อย่างต่อเนื่อง

3.2 การป้องกันอุปกรณ์และสื่อบันทึกข้อมูล (Equipment and Media Protection)

- อุปกรณ์และสื่อบันทึกข้อมูลที่มีข้อมูลส่วนบุคคลต้องได้รับการป้องกันจากการสูญหาย ถูกขโมย หรือเสียหาย
- จัดเก็บอุปกรณ์ในห้องที่มีการควบคุมอุณหภูมิและความชื้นอย่างเหมาะสม
- การใช้ตู้เซฟหรือล็อกอุปกรณ์และสื่อบันทึกข้อมูลที่มีความสำคัญ
- กำหนดนโยบายการกำจัดอุปกรณ์และสื่อบันทึกข้อมูลที่ไม่ใช้งานแล้วอย่างปลอดภัย เช่น การทำลายฮาร์ดดิสก์

3.3 การป้องกันภัยธรรมชาติและเหตุการณ์ฉุกเฉิน (Protection Against Natural Disasters and Emergencies)

- ต้องมีมาตรการเพื่อป้องกันภัยธรรมชาติ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว รวมถึงแผนการรับมือเหตุการณ์ฉุกเฉิน
- ติดตั้งระบบตรวจจับและแจ้งเตือนภัย เช่น ระบบตรวจจับควัน ระบบดับเพลิงอัตโนมัติ
- วางแผนอพยพและฝึกซ้อมสถานการณ์ฉุกเฉินกับพนักงานเป็นประจำ
- มีการวางแผนสำรองสถานที่ทำงานและระบบเพื่อให้สามารถดำเนินธุรกิจต่อเนื่องได้

สรุป

การกำหนดมาตรการด้านความมั่นคงปลอดภัยใน DPA ต้องครอบคลุมทั้งมาตรการองค์กร เทคนิค และกายภาพ เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลได้รับการปกป้องอย่างครบถ้วน มีประสิทธิภาพ และเป็นไปตามข้อกำหนดกฎหมายที่เกี่ยวข้อง

7.5.3 มีการกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคลในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (notification of personal data breaches) ตามหลักเกณฑ์ที่กฎหมายกำหนด

สิ่งที่ต้องทำ: มีข้อกำหนดตามกฎหมายครบถ้วน

หลักฐาน: ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 8
 โทษทางปกครอง: มาตรา 83, 86 ในกรณีที่ไม่ปฏิบัติตาม มาตรา 37, 40 กำหนดโทษปรับทางปกครอง ไม่เกิน 3 ล้านบาท

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement – DPA) “หน้าที่ของผู้ประมวลผลข้อมูลในการช่วยเหลือผู้ควบคุมข้อมูลในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล”

ตัวอย่างเนื้อหาข้อกำหนดใน DPA (ข้อ 7.5.3)

ข้อ X: การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลและความช่วยเหลือระหว่างผู้ประมวลผลข้อมูลกับผู้ควบคุมข้อมูล

ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงและยอมรับว่า

1.1 ในกรณีที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Personal Data Breach) ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะ การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การสูญหายของข้อมูล การเข้าถึงข้อมูลโดยมิชอบ หรือการทำลายข้อมูลโดยไม่ตั้งใจ ผู้ประมวลผลข้อมูลต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบทันทีและโดยเร็วที่สุด เมื่อทราบเหตุการณ์นั้น โดยไม่เกิน 72 ชั่วโมงหลังจากทราบเหตุการณ์

1.2 การแจ้งเหตุละเมิดข้อมูลต้องมีรายละเอียดที่เพียงพอเพื่อให้ผู้ควบคุมข้อมูลสามารถประเมินความเสี่ยงและดำเนินการตามข้อกำหนดของกฎหมายได้ เช่น ลักษณะของเหตุการณ์ ผลกระทบที่อาจเกิดขึ้น ข้อมูลที่ได้รับผลกระทบ มาตรการที่ดำเนินการเพื่อบรรเทาผลกระทบ และมาตรการที่เสนอให้ดำเนินการเพิ่มเติม

ผู้ประมวลผลข้อมูลต้องช่วยเหลือและสนับสนุนผู้ควบคุมข้อมูลในการดำเนินการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อหน่วยงานที่มีอำนาจและเจ้าของข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้อง

2.1 การช่วยเหลือดังกล่าวรวมถึงการให้ข้อมูล การร่วมวิเคราะห์เหตุการณ์ การให้คำแนะนำ และการดำเนินการอื่น ๆ ที่จำเป็นเพื่อให้การแจ้งเหตุเป็นไปอย่างถูกต้องและทันเวลา

2.2 ผู้ประมวลผลข้อมูลต้องจัดให้มีขั้นตอนภายในและระบบที่ช่วยให้สามารถตรวจจับและรายงานเหตุการณ์ละเมิดข้อมูลได้อย่างมีประสิทธิภาพและรวดเร็ว

ผู้ประมวลผลข้อมูลต้องเก็บบันทึกเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น รวมถึงการแจ้งเหตุและมาตรการที่ได้ดำเนินการ เพื่อให้สามารถตรวจสอบและนำเสนอต่อผู้ควบคุมข้อมูลหรือหน่วยงานที่เกี่ยวข้องได้ตามความเหมาะสม

การไม่ปฏิบัติตามข้อกำหนดในข้อนี้ถือเป็นการละเมิดสัญญา และผู้ประมวลผลข้อมูลต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น รวมถึงโทษทางปกครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้อง

7.5.4 DPA มีข้อกำหนดเพื่อให้แน่ใจว่าผู้ประมวลผลข้อมูลส่วนบุคคลจะลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคลทั้งหมดไปยังผู้ควบคุมข้อมูลส่วนบุคคลเมื่อสิ้นสุดสัญญา ผู้ประมวลผลข้อมูลส่วนบุคคลต้องลบหรือทำลายข้อมูลส่วนบุคคลที่มีอยู่ด้วย เว้นแต่กฎหมายกำหนดให้มีการจัดเก็บ

สิ่งที่ต้องทำ: มีข้อกำหนดครบถ้วนและชัดเจน

หลักฐาน: ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 วรรคหนึ่ง และวรรคสาม โทษทางปกครอง มาตรา 86 ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 40 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ข้อกำหนดใน DPA ที่สอดคล้องกับการจัดการข้อมูลส่วนบุคคลเมื่อสิ้นสุดสัญญา (Data Retention, Return, and Deletion)

ข้อ X: การลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคลเมื่อสิ้นสุดสัญญา

เมื่อสิ้นสุดระยะเวลาของสัญญาหรือคำสั่งที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล หรือเมื่อตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการอย่างใดอย่างหนึ่งดังต่อไปนี้โดยทันทีและครบถ้วน:

1.1 ลบหรือทำลายข้อมูลส่วนบุคคลทั้งหมดที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลในรูปแบบดิจิทัลและเอกสารที่เกี่ยวข้อง

1.2 ส่งคืนข้อมูลส่วนบุคคลทั้งหมดกลับให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล โดยไม่มีการเก็บสำเนาใดๆ เว้นแต่มีข้อตกลงเป็นลายลักษณ์อักษรที่อนุญาตให้เก็บข้อมูลไว้ชั่วคราวเพื่อวัตถุประสงค์เฉพาะและจำกัด

- กรณีที่กฎหมายหรือระเบียบข้อบังคับที่เกี่ยวข้องกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องเก็บรักษาข้อมูลส่วนบุคคลไว้ ผู้ประมวลผลข้อมูลต้องแจ้งให้ผู้ควบคุมข้อมูลทราบถึงข้อจำกัดดังกล่าว รวมถึงระยะเวลาที่ต้องเก็บข้อมูลและมาตรการรักษาความมั่นคงปลอดภัยระหว่างเก็บรักษา
- ผู้ประมวลผลข้อมูลต้องจัดทำรายงานการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคลและส่งให้ผู้ควบคุมข้อมูลส่วนบุคคลเพื่อเป็นหลักฐาน โดยระบุวันที่ เวลา และขั้นตอนที่ดำเนินการ
- ผู้ประมวลผลข้อมูลต้องมั่นใจว่าการลบหรือทำลายข้อมูลเป็นไปตามมาตรฐานความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลถูกกู้คืนหรือใช้งานโดยไม่ได้รับอนุญาต เช่น การลบข้อมูลอย่างถาวร การทำลายเอกสารในรูปแบบกระดาษด้วยวิธีการบดทำลายหรือเผา
- หากมีข้อพิพาทหรือข้อสงสัยเกี่ยวกับการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลต้องร่วมมือกับผู้ควบคุมข้อมูลส่วนบุคคลอย่างเต็มที่เพื่อแก้ไขปัญหาหรือข้อสงสัยนั้น
- การไม่ปฏิบัติตามข้อกำหนดในข้อนี้ถือเป็นการละเมิดสัญญา และผู้ประมวลผลข้อมูลต้องรับผิดชอบต่อความเสียหายหรือบทลงโทษตามกฎหมายที่เกี่ยวข้อง

7.6 การตรวจสอบผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor Due Diligence)

องค์กรดำเนินการตรวจสอบสถานะผู้ประมวลผลฯ เพื่อให้มั่นใจว่าผู้ประมวลผลข้อมูลส่วนบุคคลจะใช้มาตรการเชิงเทคนิคและมาตรการเชิงองค์กรที่เหมาะสมในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามข้อกำหนดของกฎหมาย

หลักการตรวจสอบสถานะผู้ประมวลผลข้อมูลส่วนบุคคลในกระบวนการจัดซื้อจัดจ้าง

1. แนวปฏิบัติการตรวจสอบสถานะผู้ประมวลผลข้อมูลส่วนบุคคล (Due Diligence Guideline for Data Processors)

วัตถุประสงค์

เพื่อกำหนดขั้นตอนและวิธีการตรวจสอบสถานะของผู้ประมวลผลข้อมูลส่วนบุคคลก่อนการทำสัญญาจ้าง เพื่อให้มั่นใจว่าผู้ประมวลผลจะใช้มาตรการเชิงเทคนิคและเชิงองค์กรที่เหมาะสม ปฏิบัติตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรฐานความมั่นคงปลอดภัยข้อมูลที่เกี่ยวข้อง

ขอบเขต

การตรวจสอบนี้จะครอบคลุมผู้ประมวลผลข้อมูลส่วนบุคคลทุกประเภท โดยเฉพาะอย่างยิ่งผู้ที่ประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง เช่น ข้อมูลส่วนบุคคลที่ละเอียดอ่อน ข้อมูลสุขภาพ หรือข้อมูลที่เกี่ยวข้องกับความมั่นคงขององค์กร

ขั้นตอนการตรวจสอบสถานะ

1.1 การประเมินความเสี่ยง (Risk Assessment)

- ระบุประเภทข้อมูลส่วนบุคคลที่จะถูกประมวลผล
- ประเมินความเสี่ยงของข้อมูลที่ได้รับจากผู้ประมวลผล เช่น ความเป็นไปได้ในการถูกละเมิดข้อมูล ผลกระทบต่อเจ้าของข้อมูล
- กำหนดระดับความเสี่ยง (ต่ำ ปานกลาง สูง) ตามเกณฑ์ที่กำหนดภายในองค์กร

1.2 การตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของผู้ประมวลผล (Security Measures Review)

- ตรวจสอบนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของผู้ประมวลผล

- ตรวจสอบการรับรองมาตรฐานความปลอดภัย เช่น ISO/IEC 27001, SOC 2 หรือมาตรฐานที่เกี่ยวข้อง
- ตรวจสอบวิธีการควบคุมการเข้าถึงข้อมูล (Access Control) การเข้ารหัสข้อมูล (Encryption) และมาตรการกู้คืนข้อมูล (Disaster Recovery)

1.3 การตรวจสอบนโยบายการจัดการข้อมูลส่วนบุคคล

- ตรวจสอบนโยบายความเป็นส่วนตัวและการปฏิบัติตามกฎหมายของผู้ประมวลผล
- ตรวจสอบการอบรมพนักงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- ตรวจสอบการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Data Breach Management)

1.4 การตรวจสอบประวัติการดำเนินงานและความน่าเชื่อถือ

- ตรวจสอบประวัติการให้บริการและรีวิวจากลูกค้ารายอื่น
- ตรวจสอบประวัติการละเมิดข้อมูลหรือเหตุการณ์ผิดพลาดที่เกี่ยวข้อง
- พิจารณาความสามารถในการตอบสนองต่อข้อร้องเรียนและคำขอใช้สิทธิของเจ้าของข้อมูล

การตัดสินใจและอนุมัติ

- กำหนดเกณฑ์ผ่าน/ไม่ผ่านการตรวจสอบตามระดับความเสี่ยง
- รายงานผลการประเมินต่อคณะกรรมการหรือผู้บริหารที่เกี่ยวข้อง
- บันทึกและจัดเก็บเอกสารการตรวจสอบเพื่อใช้ในการติดตามและทบทวนภายหลัง

2. ตัวอย่างแบบฟอร์มตรวจสอบสถานะผู้ประมวลผลข้อมูลส่วนบุคคล (Due Diligence Checklist)

หมวดหมู่	รายการตรวจสอบ	ผลการตรวจสอบ (ผ่าน/ไม่ผ่าน)	หมายเหตุ
ประเภทและขอบเขตของข้อมูล	ระบุประเภทข้อมูลและผู้ประมวลผลจะเข้าถึงและประมวลผล		
มาตรการรักษาความมั่นคงปลอดภัย	มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม		ตรวจสอบมาตรฐาน ISO/IEC 27001
การควบคุมการเข้าถึงข้อมูล	มีระบบควบคุมการเข้าถึงที่ชัดเจนและเข้มงวด		
การเข้ารหัสข้อมูล	ใช้การเข้ารหัสข้อมูลระหว่างส่งและจัดเก็บข้อมูล		
การจัดการเหตุการณ์ละเมิดข้อมูล	มีขั้นตอนแจ้งเตือนและแก้ไขเหตุการณ์ละเมิดข้อมูล		

การอบรมพนักงาน	มีการอบรมพนักงานเกี่ยวกับการ คุ้มครองข้อมูลส่วนบุคคล		
ประวัติการ ดำเนินงาน	ไม่มีประวัติการละเมิดข้อมูลหรือ ข้อร้องเรียนรุนแรง		

3. ตัวอย่างรายงานผลการตรวจสอบสถานะผู้ประมวลผลข้อมูลส่วนบุคคล

ชื่อผู้ประมวลผลข้อมูล: บริษัท เอ็กเซล ซอฟต์ จำกัด

วันที่ตรวจสอบ: 25 เมษายน 2568

ผู้ตรวจสอบ: ฝ่ายบริหารความเสี่ยงและการปฏิบัติตามกฎหมาย

สรุปผลการตรวจสอบ

บริษัท เอ็กเซล ซอฟต์ จำกัด ได้ผ่านกระบวนการตรวจสอบสถานะตามระดับความเสี่ยงที่กำหนดไว้ โดยมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และมีการปฏิบัติตามข้อกำหนดของกฎหมาย PDPA อย่างครบถ้วน รวมถึงมีระบบจัดการเหตุการณ์ละเมิดข้อมูลที่มีประสิทธิภาพและพนักงานได้รับการอบรมอย่างต่อเนื่อง

ข้อเสนอแนะ

- ควรเสริมสร้างมาตรการเข้ารหัสข้อมูลในขั้นตอนการจัดเก็บข้อมูลเพิ่มเติม
- ควรจัดทำแผนทดสอบการกู้คืนข้อมูลเป็นประจำทุกปี

7.6.2 มีกระบวนการตรวจสอบสถานะรวมถึงมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล เช่น การเยี่ยมชมไซต์/สถานที่ หรือการทดสอบระบบ เป็นต้น และบันทึกรายงานผลการตรวจสอบเพื่อพิจารณาคัดเลือกผู้ประมวลผลข้อมูลส่วนบุคคลต่อไป

สิ่งที่ต้องทำ: มีกระบวนการตรวจสอบสถานะและความมั่นคงปลอดภัยของข้อมูล รวมถึงมีบันทึกรายงานผลการตรวจสอบ

หลักฐาน: หลักฐานการบันทึกข้อมูลจากการตรวจสอบด้านความมั่นคงปลอดภัยของข้อมูลและผลการพิจารณาขององค์กร

สภาพบังคับ: กฎหมายไม่ได้กำหนด

หลักฐานการตรวจสอบสถานะและมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลผู้ประมวลผลข้อมูลส่วนบุคคล

1. แนวปฏิบัติการตรวจสอบสถานะและมาตรการรักษาความมั่นคงปลอดภัย (Security and Compliance Due Diligence Procedure)

วัตถุประสงค์

เพื่อกำหนดกระบวนการตรวจสอบสถานะของผู้ประมวลผลข้อมูลส่วนบุคคลโดยรวมถึงการประเมินมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในเชิงลึก เช่น การเยี่ยมชมสถานที่ การทดสอบระบบ เพื่อให้มั่นใจว่าผู้ประมวลผลมีความพร้อมและมีมาตรการที่เหมาะสมในการปกป้องข้อมูล

ขั้นตอนการตรวจสอบ

1.1 การเยี่ยมชมไซต์ (Site Visit)

- กำหนดแผนการเยี่ยมชมสำนักงานหรือศูนย์ข้อมูลของผู้ประมวลผล
- ตรวจสอบการตั้งค่าและการควบคุมทางกายภาพ เช่น ระบบควบคุมการเข้าออก (Access Control), กล้องวงจรปิด, ระบบป้องกันอัคคีภัย
- ตรวจสอบกระบวนการจัดการอุปกรณ์และสภาพแวดล้อมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

1.2 การทดสอบระบบ (System Testing)

- ทดสอบมาตรการทางเทคนิค เช่น การเข้ารหัสข้อมูล, การควบคุมการเข้าถึงระบบ, ระบบสำรองข้อมูลและกู้คืนข้อมูล
- ทดสอบการป้องกันภัยคุกคาม เช่น การจำลองโจมตีทางไซเบอร์ (penetration testing) หรือ vulnerability assessment
- ประเมินความสามารถในการตรวจจับและตอบสนองต่อเหตุการณ์ความปลอดภัย (Security Incident Response)

1.3 การสัมภาษณ์และประเมินบุคลากร

- สัมภาษณ์ผู้ดูแลระบบและเจ้าหน้าที่ที่เกี่ยวข้องเพื่อประเมินความเข้าใจและการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัย
- ตรวจสอบการอบรมและการรับรู้เรื่อง PDPA และนโยบายความมั่นคงปลอดภัยข้อมูล

1.4 การบันทึกรายงานผลการตรวจสอบ

- จัดทำรายงานสรุปผลการเยี่ยมชมและทดสอบระบบ
- ระบุข้อสังเกต ข้อบกพร่อง และข้อเสนอแนะเพื่อการปรับปรุง
- จัดเก็บรายงานในระบบบริหารจัดการเอกสารขององค์กร เพื่อใช้ประกอบการตัดสินใจคัดเลือกและติดตามผู้ประมวลผล

2. ตัวอย่างแบบฟอร์มรายงานการตรวจสอบสถานะและความมั่นคงปลอดภัยของข้อมูล (Security Audit Report Template)

รายการตรวจสอบ	ผลการตรวจสอบ	หมายเหตุ/ข้อเสนอแนะ
ระบบควบคุมการเข้าออกสถานที่	ผ่าน	กล้องวงจรปิดทำงานดี ไม่มีช่องโหว่

การเข้ารหัสข้อมูล	ผ่าน	ใช้ AES-256 ในการเข้ารหัสข้อมูล
ระบบสำรองข้อมูลและกู้คืนข้อมูล	ผ่าน	มีการทดสอบกู้คืนข้อมูลเป็นประจำทุก 6 เดือน
การตอบสนองต่อเหตุการณ์	ผ่าน	มีแผนการแจ้งเตือนและตอบสนองเหตุการณ์อย่างชัดเจน
การอบรมบุคลากร	ผ่าน	พนักงานได้รับการอบรมเรื่อง PDPA ทุกปี

3. ตัวอย่างรายงานสรุปผลการตรวจสอบ

ชื่อผู้ประมวลผลข้อมูล: บริษัท ซอฟต์แวร์ ดีไซน์ จำกัด

วันที่ตรวจสอบ: 10 พฤษภาคม 2568

ผู้ตรวจสอบ: ฝ่ายรักษาความมั่นคงปลอดภัยสารสนเทศ

สรุปผลการตรวจสอบ

บริษัทฯ มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมทั้งทางกายภาพและเทคนิค ระบบควบคุมการเข้าออกเป็นไปตามมาตรฐาน ไม่มีช่องโหว่สำคัญที่พบจากการทดสอบระบบ และพนักงานมีความรู้ความเข้าใจในมาตรการคุ้มครองข้อมูลส่วนบุคคลตาม PDPA อย่างดี

ข้อเสนอแนะ

- เสริมระบบตรวจสอบการเข้าถึงระบบฐานข้อมูลแบบเรียลไทม์ (real-time monitoring)
- เพิ่มความถี่ในการทดสอบ penetration testing เป็นทุก 6 เดือน

7.6.3 มีกระบวนการตรวจสอบด้านอื่น ๆ ที่เกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อให้มั่นใจว่าผู้ประมวลผลข้อมูลส่วนบุคคลมีศักยภาพที่จะปกป้องและคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลได้

สิ่งที่ต้องทำ: มีการตรวจสอบคุณสมบัติด้านอื่น ๆ เพิ่มเติม รวมถึงมีหลักฐานหรือเอกสารสนับสนุนที่แสดงถึงคุณสมบัติอย่างชัดเจน

หลักฐาน: หลักฐานการตรวจสอบผู้ประมวลผลข้อมูลส่วนบุคคลด้านอื่น ๆ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

หลักฐานการตรวจสอบคุณสมบัติด้านอื่น ๆ ของผู้ประมวลผลข้อมูลส่วนบุคคล

1. แนวปฏิบัติการตรวจสอบคุณสมบัติด้านอื่น ๆ (Additional Due Diligence Procedure)

วัตถุประสงค์

เพื่อประเมินและตรวจสอบคุณสมบัติและความสามารถของผู้ประมวลผลข้อมูลในด้านอื่น ๆ ที่มีความเกี่ยวข้องและส่งผลต่อการปกป้องข้อมูลส่วนบุคคล เช่น ความน่าเชื่อถือ ความสามารถทางเทคนิค ความยั่งยืนทางธุรกิจ และการปฏิบัติตามกฎระเบียบที่เกี่ยวข้อง

ขอบเขตการตรวจสอบ

- ความน่าเชื่อถือขององค์กร เช่น การมีประวัติการดำเนินงานที่ดี ไม่มีประวัติการละเมิดข้อมูล
- การมีมาตรฐานหรือใบรับรองที่เกี่ยวข้อง เช่น ISO 27001, CSA STAR, SOC 2
- ความสามารถทางเทคนิค เช่น บุคลากรที่มีทักษะเฉพาะทาง การใช้เทคโนโลยีที่ทันสมัย
- ความมั่นคงทางการเงิน เพื่อความยั่งยืนในการดำเนินงาน
- การปฏิบัติตามกฎหมายและข้อบังคับอื่น ๆ ที่เกี่ยวข้อง
- ความสามารถในการให้บริการสนับสนุนและตอบสนองต่อเหตุการณ์ฉุกเฉิน

ขั้นตอนการตรวจสอบ

1.1 การตรวจสอบประวัติและความน่าเชื่อถือ

- ตรวจสอบประวัติการดำเนินงานและประวัติการละเมิดข้อมูล (ถ้ามี)
- ตรวจสอบข้อมูลในฐานข้อมูลข่าวสารหรือรายงานสถานะทางธุรกิจ

1.2 การตรวจสอบใบรับรองและมาตรฐานความปลอดภัย

- ขอสำเนาใบรับรองความปลอดภัยหรือมาตรฐานที่เกี่ยวข้อง
- ตรวจสอบความถูกต้องและสถานะของใบรับรอง

1.3 การประเมินความสามารถทางเทคนิค

- ตรวจสอบข้อมูลบุคลากรหลัก เช่น ประสบการณ์และคุณสมบัติของทีมงานด้านความปลอดภัยและเทคโนโลยี
- ตรวจสอบโครงสร้างพื้นฐานเทคโนโลยีและเครื่องมือที่ใช้

1.4 การประเมินความมั่นคงทางการเงิน

- ตรวจสอบรายงานทางการเงินล่าสุด เช่น งบการเงิน รายงานการตรวจสอบบัญชี
- ประเมินความเสี่ยงด้านการเงินที่อาจส่งผลกระทบต่อความต่อเนื่องของการให้บริการ

1.5 การตรวจสอบการปฏิบัติตามกฎหมายและข้อบังคับ

- ตรวจสอบนโยบายและกระบวนการที่เกี่ยวข้องกับการปฏิบัติตามกฎหมาย เช่น PDPA, GDPR
- ตรวจสอบการอบรมและการรับรู้ของพนักงานเกี่ยวกับข้อกฎหมาย

1.6 การประเมินความพร้อมในการสนับสนุนและตอบสนองเหตุการณ์

- ตรวจสอบแผนการตอบสนองเหตุการณ์และการกู้คืนระบบ (Incident Response Plan & Disaster Recovery Plan)
- ประเมินความรวดเร็วและประสิทธิภาพของการสนับสนุนลูกค้า

2. ตัวอย่างแบบฟอร์มรายงานการตรวจสอบคุณสมบัติด้านอื่น ๆ

รายการตรวจสอบ	ผลการตรวจสอบ	หมายเหตุ/ข้อเสนอแนะ
ประวัติและความน่าเชื่อถือ	ผ่าน	ไม่มีประวัติการละเมิดข้อมูล
ใบรับรองมาตรฐานความปลอดภัย	ผ่าน	มีใบรับรอง ISO 27001 และ SOC 2
ความสามารถทางเทคนิค	ผ่าน	ทีมงานมีประสบการณ์และเครื่องมือครบครัน
ความมั่นคงทางการเงิน	ผ่าน	งบการเงินแสดงผลประกอบการดี
การปฏิบัติตามกฎหมายและข้อบังคับ	ผ่าน	มีนโยบายและอบรมพนักงานอย่างต่อเนื่อง
ความพร้อมในการตอบสนองเหตุการณ์	ผ่าน	มีแผนฉุกเฉินและการกู้คืนระบบครบถ้วน

3. ตัวอย่างรายงานสรุปผลการตรวจสอบ

ชื่อผู้ประมวลผลข้อมูล: บริษัท ดาต้า เซอร์วิส จำกัด

วันที่ตรวจสอบ: 15 มิถุนายน 2568

ผู้ตรวจสอบ: ฝ่ายบริหารความเสี่ยงและควบคุมภายใน

สรุปผลการตรวจสอบ

จากการตรวจสอบข้อมูลและเอกสารสนับสนุน พบว่าผู้ประมวลผลข้อมูลฯ มีคุณสมบัติและศักยภาพในด้านต่าง ๆ ที่เหมาะสม ทั้งในเรื่องความน่าเชื่อถือ การมีมาตรฐานความปลอดภัยระดับสากล ความสามารถทางเทคนิค รวมถึงความมั่นคงทางการเงินและการปฏิบัติตามกฎหมายที่เกี่ยวข้อง

ข้อเสนอแนะ

- ควรติดตามสถานะใบรับรองมาตรฐานและการอบรมพนักงานอย่างสม่ำเสมอ
- แนะนำให้มีการทบทวนประวัติการดำเนินงานและประเมินความเสี่ยงใหม่ทุก 12 เดือน

7.7 การตรวจสอบการปฏิบัติตามสัญญา (Data Processor Compliance Reviews)

องค์กรตรวจสอบการปฏิบัติตามสัญญาของผู้ประมวลผลข้อมูลส่วนบุคคล

7.7.1 DPA มีข้อกำหนดที่อนุญาตให้องค์กรดำเนินการตรวจสอบ (Right to Audit) เพื่อยืนยันว่าผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามข้อกำหนดและเงื่อนไขตามสัญญาทั้งหมด

สิ่งที่ต้องทำ: มีข้อกำหนดที่ครอบคลุมถึงการที่องค์กรสามารถมอบหมายให้บุคคลอื่นเข้าตรวจสอบได้ด้วย

หลักฐาน: ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement – DPA) ที่สอดคล้องกับข้อกำหนดให้มีสิทธิการตรวจสอบ (Right to Audit)

ตัวอย่างข้อความในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

ข้อ X. สิทธิในการตรวจสอบและการมอบหมาย (Right to Audit and Delegation)

- ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงให้องค์กร (ผู้ควบคุมข้อมูลส่วนบุคคล) มีสิทธิในการดำเนินการตรวจสอบ (Audit) เพื่อยืนยันว่าผู้ประมวลผลได้ปฏิบัติตามข้อกำหนดและเงื่อนไขของข้อตกลงฉบับนี้อย่างครบถ้วนและถูกต้อง
- การตรวจสอบดังกล่าวสามารถดำเนินการโดยบุคคลหรือนิติบุคคลที่องค์กรมอบหมาย โดยผู้ประมวลผลข้อมูลต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ที่ได้รับมอบหมายดังกล่าวในการเข้าถึงเอกสาร ข้อมูล และสถานที่ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล
- การตรวจสอบจะดำเนินการโดยไม่ก่อให้เกิดผลกระทบต่อการดำเนินงานปกติของผู้ประมวลผลข้อมูลส่วนบุคคล และต้องมีการแจ้งล่วงหน้าเป็นลายลักษณ์อักษรไม่น้อยกว่า 15 วันทำการ
- ผู้ประมวลผลข้อมูลส่วนบุคคลต้องให้ข้อมูลและเอกสารที่เกี่ยวข้องทั้งหมดแก่ผู้ตรวจสอบ รวมทั้งต้องเปิดโอกาสให้มีการสัมภาษณ์เจ้าหน้าที่หรือบุคคลที่เกี่ยวข้อง เพื่อให้สามารถตรวจสอบได้อย่างครบถ้วนและมีประสิทธิภาพ

- หากพบว่าผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามข้อกำหนดตามข้อตกลงนี้ องค์กรมีสิทธิ์เรียกร้องให้ผู้ประมวลผลดำเนินการแก้ไข และสามารถพิจารณาใช้มาตรการตามสัญญา รวมถึงสิทธิ์ในการยุติการทำสัญญาได้ตามสมควร

หลักฐานที่องค์กรควรจัดเก็บ

- สำเนาข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA) ที่ระบุข้อความข้างต้น
- รายงานผลการตรวจสอบ (Audit Reports) ที่จัดทำตามสิทธิ์การตรวจสอบ
- เอกสารการแจ้งล่วงหน้าและบันทึกการดำเนินการตรวจสอบ
- รายงานผลการแก้ไขหรือติดตามหลังการตรวจสอบ

7.7.2 องค์กรดำเนินการตรวจสอบการปฏิบัติตามข้อกำหนดเป็นประจำตามระดับความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคล เพื่อทดสอบว่าผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามข้อตกลงใน DPA

สิ่งที่ต้องทำ: มีการตรวจสอบครบถ้วนเป็นประจำ

หลักฐาน: กระบวนการหรือกฎระเบียบภายในองค์กรที่เกี่ยวกับการตรวจสอบการปฏิบัติตามข้อกำหนด
หลักฐานในการดำเนินการตรวจสอบตามขั้นตอนหรือกระบวนการที่ได้กำหนดไว้

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การตรวจสอบการปฏิบัติตามข้อกำหนดของผู้ประมวลผลข้อมูลส่วนบุคคล(Compliance Review Process)อย่างสม่ำเสมอ โดยเน้นการทำตามระดับความเสี่ยง

1. นโยบายการตรวจสอบการปฏิบัติตาม DPA

องค์กรได้กำหนดนโยบายและแนวทางปฏิบัติสำหรับการตรวจสอบผู้ประมวลผลข้อมูลส่วนบุคคลอย่างสม่ำเสมอ โดยมีวัตถุประสงค์เพื่อยืนยันว่าผู้ประมวลผลข้อมูลได้ดำเนินการตามข้อกำหนดใน Data Processing Agreement (DPA) อย่างครบถ้วนและถูกต้อง รวมทั้งเป็นการบริหารความเสี่ยงด้านข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ

2. ระดับความเสี่ยงและวิธีการตรวจสอบ

องค์กรแบ่งระดับความเสี่ยงของผู้ประมวลผลข้อมูลตามประเภทของข้อมูลและลักษณะการประมวลผล เช่น

- **ความเสี่ยงสูง:** ข้อมูลสุขภาพ ข้อมูลการเงิน หรือข้อมูลส่วนบุคคลที่ละเอียดอ่อน
- **ความเสี่ยงปานกลาง:** ข้อมูลส่วนบุคคลทั่วไปที่ไม่ใช่ข้อมูลละเอียดอ่อน
- **ความเสี่ยงต่ำ:** ข้อมูลที่เปิดเผยมั่วสาธารณะ หรือข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล

- ความถี่ในการตรวจสอบจะพิจารณาตามระดับความเสี่ยงดังนี้
- ความเสี่ยงสูง: ตรวจสอบอย่างน้อยปีละ 1 ครั้ง
- ความเสี่ยงปานกลาง: ตรวจสอบอย่างน้อยทุก 2 ปี
- ความเสี่ยงต่ำ: ตรวจสอบตามความเหมาะสม เช่น ทุก 3 ปี หรือเมื่อต้องการ

3. กระบวนการตรวจสอบ

- กำหนดแผนการตรวจสอบประจำปี (Annual Audit Plan) โดยฝ่ายควบคุมข้อมูลหรือฝ่ายความมั่นคงปลอดภัยข้อมูล
- แจ้งให้ผู้ประมวลผลข้อมูลทราบล่วงหน้าก่อนเข้าตรวจสอบ
- ดำเนินการตรวจสอบตามแผน โดยอาจใช้วิธีตรวจเอกสาร เยี่ยมชมสถานที่ ทดสอบระบบ และสัมภาษณ์ผู้เกี่ยวข้อง
- บันทึกผลการตรวจสอบอย่างละเอียด และจัดทำรายงานผลการตรวจสอบ

4. การจัดทำรายงานและการติดตาม

- รายงานผลการตรวจสอบจะส่งให้ฝ่ายบริหารและผู้ควบคุมข้อมูล เพื่อประเมินผลและวางแผนแก้ไข
- หากพบประเด็นที่ไม่เป็นไปตามข้อกำหนด จะต้องกำหนดมาตรการแก้ไข พร้อมกำหนดกรอบเวลา และผู้รับผิดชอบติดตาม
- ดำเนินการติดตามผลการแก้ไข และบันทึกไว้เป็นหลักฐาน

5. เอกสารหลักฐานประกอบ

- นโยบายและแนวทางปฏิบัติการตรวจสอบผู้ประมวลผลข้อมูล
- แผนการตรวจสอบประจำปี (Annual Audit Plan)
- หนังสือแจ้งการตรวจสอบล่วงหน้า
- รายงานผลการตรวจสอบ (Audit Report)
- รายงานการติดตามผลการแก้ไข (Follow-up Report)

สภาพบังคับ

กฎหมายไม่ได้กำหนดเป็นข้อบังคับ แต่ถือเป็นแนวทางปฏิบัติที่ดีเพื่อบริหารความเสี่ยงและรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ

เอกสารหลักฐานการตรวจสอบการปฏิบัติตามข้อกำหนดของผู้ประมวลผลข้อมูลส่วนบุคคล

1. นโยบายการตรวจสอบผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor Compliance Review Policy)

วัตถุประสงค์

- เพื่อกำหนดแนวทางและขั้นตอนในการตรวจสอบการปฏิบัติตามสัญญาของผู้ประมวลผลข้อมูลส่วนบุคคล
- เพื่อให้มั่นใจว่าผู้ประมวลผลข้อมูลดำเนินการตามข้อกำหนดและมาตรฐานความมั่นคงปลอดภัยของข้อมูลอย่างเคร่งครัดและสม่ำเสมอ

ขอบเขต

นโยบายนี้ครอบคลุมการตรวจสอบผู้ประมวลผลข้อมูลส่วนบุคคลทุกแห่งที่องค์กรทำสัญญา

ประมวลผลข้อมูล

ข้อกำหนด

- การจัดกลุ่มผู้ประมวลผลข้อมูลตามระดับความเสี่ยงของข้อมูลที่ประมวลผล (สูง ปานกลาง ต่ำ)
- กำหนดความถี่และวิธีการตรวจสอบตามระดับความเสี่ยง
- จัดทำแผนตรวจสอบประจำปี (Annual Audit Plan) โดยฝ่ายควบคุมข้อมูลหรือฝ่ายความมั่นคงปลอดภัยข้อมูล
- ดำเนินการตรวจสอบโดยบุคลากรที่มีความรู้ความสามารถและเป็นกลาง
- รายงานผลการตรวจสอบพร้อมข้อเสนอแนะและแนวทางแก้ไข
- ติดตามผลการดำเนินการแก้ไขข้อบกพร่องอย่างต่อเนื่อง

ความถี่การตรวจสอบ

- ความเสี่ยงสูง: ตรวจสอบปีละอย่างน้อย 1 ครั้ง
- ความเสี่ยงปานกลาง: ตรวจสอบอย่างน้อยทุก 2 ปี
- ความเสี่ยงต่ำ: ตรวจสอบตามความเหมาะสม

2. แผนการตรวจสอบผู้ประมวลผลข้อมูล (Annual Audit Plan)

ลำดับ	ชื่อผู้ประมวลผล	ประเภทข้อมูล	ระดับความเสี่ยง	ความถี่ตรวจสอบ	กำหนดการตรวจสอบ (เดือน/ปี)	ผู้รับผิดชอบ
1	บริษัท เอ บี ซี	ข้อมูลสุขภาพ	สูง	ปีละ 1 ครั้ง	มิ.ย. 2568	ฝ่ายความมั่นคงปลอดภัยข้อมูล

2	บริษัท ดี อี เอฟ	ข้อมูล ทั่วไป	ปานกลาง	ทุก 2 ปี	ธ.ค. 2568	ฝ่ายควบคุม ข้อมูล
3	บริษัท จี เอช ไอ	ข้อมูลไม่ ละเอียด	ต่ำ	ตามความ เหมาะสม	เม.ย. 2569	ฝ่ายควบคุม ข้อมูล

3. แบบฟอร์มแจ้งการตรวจสอบล่วงหน้า (Audit Notification Letter)

เรียน ผู้บริหารบริษัท [ชื่อผู้ประมวลผลข้อมูล]

ตามที่องค์กรของเราได้ดำเนินการจัดทำแผนตรวจสอบผู้ประมวลผลข้อมูลส่วนบุคคลประจำปี เพื่อยืนยันว่าการดำเนินการตามสัญญาการประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้องและสอดคล้องกับข้อกำหนดของกฎหมาย รวมถึงมาตรฐานความมั่นคงปลอดภัยข้อมูล

ด้วยเหตุนี้ องค์กรขอแจ้งกำหนดการเข้าตรวจสอบระบบและกระบวนการประมวลผลข้อมูลของบริษัทท่านในวันที่ [วัน เดือน ปี] ณ สำนักงานของท่าน

จึงเรียนมาเพื่อโปรดให้ความร่วมมือและจัดเตรียมข้อมูลที่เกี่ยวข้อง เพื่อความสะดวกในการตรวจสอบ

ขอแสดงความนับถือ

[ชื่อผู้ส่ง]

[ตำแหน่ง]

[หน่วยงาน]

4. รายงานผลการตรวจสอบ (Audit Report Template)

รายงานการตรวจสอบการปฏิบัติตามข้อกำหนดของผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูล: [ชื่อบริษัท]

วันที่ตรวจสอบ: [วัน เดือน ปี]

ผู้ตรวจสอบ: [ชื่อผู้ตรวจสอบ]

ระดับความเสี่ยง: [สูง/ปานกลาง/ต่ำ]

ผลการตรวจสอบ

ข้อกำหนด	รายละเอียด	สถานะ (ผ่าน/ไม่ผ่าน)	หมายเหตุ
การปฏิบัติตาม DPA	ตรวจสอบการดำเนินงานตามข้อตกลง	ผ่าน	มีเอกสารยืนยันครบถ้วน

มาตรการความมั่นคงปลอดภัย	ตรวจสอบระบบความปลอดภัยและการเข้าถึงข้อมูล	ผ่าน	มีระบบเข้ารหัสและสำรองข้อมูล
การแจ้งเหตุข้อมูลรั่วไหล	ตรวจสอบกระบวนการแจ้งเหตุการณ์	ผ่าน	มีขั้นตอนชัดเจน
การฝึกอบรมบุคลากร	ตรวจสอบการฝึกอบรมด้านข้อมูลส่วนบุคคล	ผ่าน	มีบันทึกการอบรมล่าสุด
การจัดการเมื่อสิ้นสุดสัญญา	ตรวจสอบการลบ/ทำลายข้อมูล	ผ่าน	มีหลักฐานการทำลายข้อมูล

ข้อเสนอแนะ

- รายละเอียดข้อเสนอแนะและแนวทางปรับปรุง
- รายละเอียดข้อเสนอแนะเพิ่มเติม

สรุป

ผลการตรวจสอบโดยรวม [ผ่าน/ไม่ผ่าน] ข้อกำหนดตามสัญญา DPA

ผู้ตรวจสอบ: _____

วันที่: _____

5. รายงานการติดตามผลการแก้ไข (Follow-up Report)

เรื่อง: การติดตามผลการแก้ไขจากรายงานตรวจสอบผู้ประมวลผลข้อมูล

ผู้ประมวลผลข้อมูล: [ชื่อบริษัท]

วันที่ติดตามผล: [วัน เดือน ปี]

หมายเลขข้อบกพร่อง	รายละเอียดข้อบกพร่อง	มาตรการแก้ไขที่ดำเนินการ	สถานะ (เสร็จสมบูรณ์/ดำเนินการต่อ)	หมายเหตุ
1	ระบบเข้ารหัสยังไม่ครบถ้วน	ติดตั้งระบบเข้ารหัสครบถ้วนแล้ว	เสร็จสมบูรณ์	
2	เอกสารนโยบายไม่ครบถ้วน	จัดทำและแจกจ่ายเอกสารใหม่	ดำเนินการต่อ	คาดเสร็จภายในเดือนหน้า

ผู้ติดตามผล: _____

วันที่: _____

7.8 การให้บริการโดยบุคคลที่สาม (Third Party Products and Services)

องค์กรพิจารณา “การปกป้องข้อมูลด้วยการออกแบบ” (“Data Protection by Design”) เมื่อเลือกบริการและผลิตภัณฑ์ที่จะใช้ในกิจกรรมการประมวลผลข้อมูล

7.8.1 หากมีบุคคลที่สามจัดหาผลิตภัณฑ์หรือบริการเพื่อประมวลผลข้อมูลส่วนบุคคล องค์กรเลือกผู้ค้า (Supplier) ที่มีมาตรฐานในการปกป้องข้อมูลส่วนบุคคล โดยออกแบบผลิตภัณฑ์หรือบริการของตนโดยคำนึงถึงการปกป้องข้อมูลด้วยการออกแบบ (Privacy by Design)

สิ่งที่ต้องทำ: มีการตรวจสอบนโยบาย แนวปฏิบัติ หรือการดำเนินการของผู้ค้า และมีเอกสารสนับสนุน

หลักฐาน: แนวปฏิบัติหรือการดำเนินการขององค์กรในการตรวจสอบหลัก “การปกป้องข้อมูลด้วยการออกแบบ” (Data Protection by Design) ของผู้ค้า (Supplier)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เรื่อง “การให้บริการโดยบุคคลที่สาม (Third Party Products and Services)” ที่มุ่งเน้นการตรวจสอบ “Data Protection by Design” ของผู้ค้า (Supplier)

แนวปฏิบัติการตรวจสอบหลักการ “Data Protection by Design” สำหรับผู้ค้า (Supplier) ที่ให้บริการผลิตภัณฑ์หรือบริการเกี่ยวกับข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อให้แน่ใจว่าองค์กรเลือกใช้บริการและผลิตภัณฑ์จากบุคคลที่สามที่มีมาตรฐานการปกป้องข้อมูลส่วนบุคคลอย่างเคร่งครัด โดยพิจารณาและตรวจสอบว่าได้บูรณาการหลักการ “Data Protection by Design” ในการออกแบบผลิตภัณฑ์และบริการแล้ว

2. ขอบเขต

แนวปฏิบัตินี้ครอบคลุมการพิจารณา เลือก และตรวจสอบผู้ค้าผลิตภัณฑ์และบริการที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลทุกประเภทก่อนการทำสัญญาหรือสั่งซื้อ

3. ข้อกำหนดหลัก

3.1 การประเมินก่อนเลือกผู้ค้า (Pre-selection Assessment)

- รวบรวมข้อมูลนโยบายความเป็นส่วนตัว (Privacy Policy) และนโยบายการรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security Policy) ของผู้ค้า

- ตรวจสอบว่าผู้ค้ามีการบูรณาการหลักการ “Data Protection by Design” ในการออกแบบผลิตภัณฑ์และบริการ เช่น การจำกัดการเข้าถึงข้อมูล, การเข้ารหัสข้อมูล, การใช้เทคนิคการปกปิดข้อมูล (Data Masking), การจำกัดการเก็บข้อมูล (Data Minimization) เป็นต้น
- ขอเอกสารหรือแบบฟอร์มยืนยัน เช่น แบบสอบถามด้านความมั่นคงปลอดภัย (Security Questionnaire), รายงานการประเมินความปลอดภัย (Security Assessment Report), หรือการรับรองมาตรฐานที่เกี่ยวข้อง (เช่น ISO/IEC 27001)

3.2 การตรวจสอบและประเมินผล (Due Diligence)

- ตรวจสอบผลการประเมินด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวของผลิตภัณฑ์/บริการจากแหล่งที่เชื่อถือได้
- ประเมินความเสี่ยงที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์/บริการนั้นต่อข้อมูลส่วนบุคคลขององค์กร
- ตรวจสอบว่าผู้ค้าสนับสนุนการปฏิบัติตามข้อกำหนดด้านข้อมูลส่วนบุคคล เช่น การตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูล, การแจ้งเหตุข้อมูลรั่วไหล เป็นต้น

3.3 การกำหนดข้อกำหนดในสัญญา

- ระบุในสัญญาหรือข้อตกลงว่าผู้ค้าต้องปฏิบัติตามหลักการ “Data Protection by Design” และมาตรฐานความมั่นคงปลอดภัยที่องค์กรกำหนด
- กำหนดสิทธิขององค์กรในการตรวจสอบ (Right to Audit) และการติดตามประสิทธิภาพของมาตรการปกป้องข้อมูล

3.4 การติดตามและทบทวน (Ongoing Monitoring)

- ติดตามประสิทธิภาพการปกป้องข้อมูลของผู้ค้าอย่างสม่ำเสมอ เช่น ผ่านการรายงานความปลอดภัยประจำปี หรือการตรวจสอบแบบ Remote Audit
- ทบทวนและปรับปรุงแนวทางตามความเปลี่ยนแปลงของเทคโนโลยีและกฎหมาย

4. ตัวอย่างเอกสารแนบประกอบการตรวจสอบ

4.1 แบบฟอร์มประเมินผู้ค้า (Supplier Privacy & Security Assessment Questionnaire)

หัวข้อประเมิน	คำตอบ (ใช่/ไม่ใช่/ไม่ทราบ)	หมายเหตุเพิ่มเติม
มีการออกแบบผลิตภัณฑ์/บริการโดยคำนึงถึงความเป็นส่วนตัว?		
มีการเข้ารหัสข้อมูลส่วนบุคคลในระบบหรือไม่?		ระบุวิธีการเข้ารหัส (AES, TLS ฯลฯ)
มีมาตรการจำกัดการเข้าถึงข้อมูลตามสิทธิ์?		

มีนโยบายการเก็บรักษาข้อมูลและกำหนดระยะเวลาลบข้อมูล?		
มีขั้นตอนแจ้งเหตุการณ์ข้อมูลรั่วไหลหรือไม่?		ระบุช่องทางการแจ้งและระยะเวลา
มีมาตรฐานหรือการรับรองด้านความมั่นคงปลอดภัย (IS)		ระบุชื่อมาตรฐานและวันที่รับรอง

4.2 ตัวอย่างข้อกำหนดในสัญญา (Data Protection by Design Clause)

"ผู้ค้าให้ความยินยอมและตกลงว่าผลิตภัณฑ์และบริการที่จัดทำให้องค์กรจะถูกออกแบบและดำเนินการโดยคำนึงถึงหลักการ Data Protection by Design เพื่อปกป้องข้อมูลส่วนบุคคลขององค์กรให้มีความปลอดภัยสูงสุด และปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง รวมทั้งยินยอมให้องค์กรมีสิทธิในการตรวจสอบและประเมินการปฏิบัติงานเพื่อให้เป็นไปตามข้อตกลงนี้"

5. สรุป

แนวปฏิบัตินี้ช่วยให้องค์กรมั่นใจว่าการเลือกใช้ผลิตภัณฑ์และบริการจากบุคคลที่สามสอดคล้องกับหลักการ Data Protection by Design ลดความเสี่ยงด้านความมั่นคงปลอดภัยข้อมูล และช่วยสนับสนุนการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างครบถ้วน

7.9 วัตถุประสงค์ที่จำกัด (Purpose Limitation) องค์กรดำเนินการเชิงรุกเพื่อให้มั่นใจว่าการเปิดเผยหรือแบ่งปันข้อมูลส่วนบุคคลกับองค์กรอื่น (ผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลที่สาม) จะทำเพียงเท่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์สำหรับการโอนหรือเปิดเผยเท่านั้น

7.9.1 องค์กรมีแนวปฏิบัติหรือการดำเนินการว่า การแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคลกับองค์กรอื่นจะดำเนินการเท่าที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์สำหรับการโอนหรือเปิดเผยตามข้อตกลงที่ได้จัดทำเท่านั้น

สิ่งที่ต้องทำ: มีแนวปฏิบัติในการพิจารณาตามหลักการวัตถุประสงค์ที่จำกัด

หลักฐาน: แนวปฏิบัติหรือแนวทางที่องค์กรใช้ในการพิจารณาการจำกัดการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น ตามหลักวัตถุประสงค์ที่จำกัด

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 21, 22, 27 โทษทางปกครอง มาตรา 83 ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 21, มาตรา 22, มาตรา 27 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท กรณีเป็นข้อมูลส่วนบุคคลตามมาตรา 26 มีโทษทางปกครองตามมาตรา 84 ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 21, มาตรา 22, มาตรา 27 กำหนดโทษปรับทางปกครองไม่เกิน 5 ล้านบาท

แนวปฏิบัติการจำกัดวัตถุประสงค์ในการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคล (Purpose Limitation Policy)

1. วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติสำหรับการเปิดเผยหรือแบ่งปันข้อมูลส่วนบุคคลกับบุคคลหรือองค์กรภายนอก โดยเปิดเผยข้อมูลเท่าที่จำเป็นและเหมาะสมสำหรับวัตถุประสงค์ที่ได้ตกลงไว้ เพื่อป้องกันการนำข้อมูลไปใช้ในทางที่เกินขอบเขต และสอดคล้องกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ขอบเขต

แนวปฏิบัตินี้ครอบคลุมถึงการแบ่งปันข้อมูลส่วนบุคคลทุกรูปแบบ ทั้งกับผู้ประมวลผลข้อมูลภายนอก (Data Processor) และบุคคลที่สาม (Third Party) ไม่ว่าจะเป็นการแบ่งปันภายในประเทศหรือต่างประเทศ

3. แนวทางปฏิบัติ

3.1 การกำหนดวัตถุประสงค์ชัดเจน

- ต้องระบุวัตถุประสงค์ที่ชัดเจนและเหมาะสมสำหรับการเปิดเผยข้อมูลส่วนบุคคลในสัญญาหรือข้อตกลงร่วมกับผู้รับข้อมูล
- วัตถุประสงค์ต้องสอดคล้องกับขอบเขตการประมวลผลตามกฎหมายที่เกี่ยวข้อง

3.2 การจำกัดการเปิดเผยข้อมูล

- เปิดเผยข้อมูลเฉพาะข้อมูลที่จำเป็น (Data Minimization) เพื่อบรรลุวัตถุประสงค์นั้นเท่านั้น
- พิจารณาใช้เทคนิคการลดความเสี่ยง เช่น การทำข้อมูลเป็นนิรนาม (Anonymization) หรือการแฝงข้อมูล (Pseudonymization) เมื่อเป็นไปได้

3.3 การควบคุมการอนุมัติ

- กำหนดขั้นตอนการขออนุมัติเปิดเผยข้อมูล โดยผู้ขออนุมัติต้องเป็นเจ้าหน้าที่ที่ได้รับมอบหมาย และต้องระบุรายละเอียดข้อมูล วัตถุประสงค์ และผู้รับข้อมูลชัดเจน
- บันทึกการอนุมัติไว้เป็นหลักฐานทุกครั้ง

3.4 การตรวจสอบและติดตาม

- ตรวจสอบการเปิดเผยข้อมูลอย่างสม่ำเสมอเพื่อให้มั่นใจว่าการใช้ข้อมูลเป็นไปตามวัตถุประสงค์ที่กำหนดไว้
- ปรับปรุงแนวทางและขั้นตอนให้สอดคล้องกับกฎหมายและสถานการณ์ที่เปลี่ยนแปลง

4. แบบฟอร์มประกอบ

4.1 แบบฟอร์มขออนุมัติเปิดเผยข้อมูลส่วนบุคคล (Data Disclosure Approval Form)

รายละเอียด	ข้อมูล
วันที่ขออนุมัติ	[_____]
ชื่อผู้ขออนุมัติ	[_____]
ตำแหน่ง	[_____]
วัตถุประสงค์ในการเปิดเผยข้อมูล	[_____]
ประเภทและปริมาณข้อมูลที่จะเปิดเผย	[_____]
ผู้รับข้อมูล (องค์กร/บุคคล)	[_____]
ระยะเวลาที่ข้อมูลจะถูกใช้	[_____]
ข้อกำหนดการคุ้มครองข้อมูลที่ได้รับต้องปฏิบัติ	[_____]
การอนุมัติ (ชื่อ, ตำแหน่ง, ลายเซ็น)	[_____]
หมายเหตุเพิ่มเติม	[_____]

4.2 ตัวอย่างบันทึกการเปิดเผยข้อมูล (Data Disclosure Log)

วันที่เปิดเผย	ผู้เปิดเผยข้อมูล	ผู้รับข้อมูล	วัตถุประสงค์	รายละเอียดข้อมูล	หมายเหตุ

2025-06-01	นายสมชาย จันทร์แจ่ม	บริษัท ABC จำกัด	ตรวจสอบ ประวัติ	รายชื่อและเบอร์โทร	ไม่มี
2025-06-03	นางสาวลลิตา ทองดี	สำนักงาน กฎหมาย	ดำเนินคดี	ข้อมูลส่วนตัวเจ้าของ ข้อมูล	อยู่ใน สัญญา

5. การบังคับใช้และบทลงโทษ

- หากพบว่าการเปิดเผยข้อมูลเกินขอบเขตหรือไม่มีวัตถุประสงค์ที่ชัดเจน องค์กรจะดำเนินการตามมาตรการทางวินัย รวมถึงแจ้งผู้ควบคุมข้อมูลและเจ้าของข้อมูลตามที่กฎหมายกำหนด
- บุคลากรต้องปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด เพื่อป้องกันความเสียหายและบทลงโทษตามกฎหมาย พ.ศ. 2562 มาตรา 21, 22, 27 และบทลงโทษทางปกครองตามมาตรา 83, 84

6. ผู้รับผิดชอบ

ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO) และฝ่ายที่เกี่ยวข้องรับผิดชอบในการตรวจสอบและติดตามการปฏิบัติตามแนวทางนี้

ลงชื่ออนุมัติ

.....

(ชื่อผู้บริหาร)

ตำแหน่ง:

วันที่:

7.9.2 เมื่อมีการแบ่งปันหรือเปิดเผยข้อมูลส่วนบุคคล ข้อมูลนั้นจะถูกทำเป็นข้อมูลแฝง (Pseudonymized) หรือเปิดเผยน้อยที่สุดเท่าที่จำเป็น (Data Minimization) หรือทำให้เป็นข้อมูลนิรนามเมื่อทำได้ (Anonymization)

สิ่งที่ต้องทำ: มีการจัดทำเป็นข้อมูลแฝงหรือข้อมูลนิรนามก่อนการแบ่งปันข้อมูลส่วนบุคคล

หลักฐาน: หลักฐานการทำข้อมูลแฝงหรือข้อมูลนิรนามก่อนการแบ่งปันข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22 และ มาตรา 37 (1)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4

โทษทางปกครอง: มาตรา 83 ในกรณีที่未按ปฏิบัติตามมาตรา 22 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

แนวปฏิบัติการทำข้อมูลแฝงหรือข้อมูลนิรนามก่อนการแบ่งปันข้อมูลส่วนบุคคล

(Pseudonymization and Anonymization Policy)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและขั้นตอนในการจัดทำข้อมูลแฝง (Pseudonymization) หรือข้อมูลนิรนาม (Anonymization) ก่อนการแบ่งปันข้อมูลส่วนบุคคลให้กับบุคคลภายนอกหรือผู้ประมวลผลข้อมูลส่วนบุคคลอื่น ๆ โดยมีวัตถุประสงค์ลดความเสี่ยงในการละเมิดข้อมูลส่วนบุคคลและปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ขอบเขต

แนวปฏิบัตินี้ใช้กับการแบ่งปันข้อมูลส่วนบุคคลในทุกรูปแบบ ไม่ว่าจะเป็นการส่งข้อมูลผ่านระบบอิเล็กทรอนิกส์ เอกสาร หรือช่องทางอื่น ๆ โดยต้องจัดทำข้อมูลให้อยู่ในรูปแบบที่ปลอดภัยตามหลักการ Data Minimization, Pseudonymization หรือ Anonymization

3. แนวทางปฏิบัติ

3.1 การวิเคราะห์ข้อมูลก่อนแบ่งปัน

- ประเมินประเภทข้อมูลและความจำเป็นในการเปิดเผยข้อมูลส่วนบุคคลแต่ละรายการ
- กำหนดว่าข้อมูลใดจำเป็นต้องทำเป็นข้อมูลแฝงหรือข้อมูลนิรนามเพื่อป้องกันการระบุตัวบุคคล

3.2 การทำข้อมูลแฝง (Pseudonymization)

- ดำเนินการแทนที่ข้อมูลที่สามารถระบุตัวบุคคลได้ด้วยรหัสหรือข้อมูลแทนที่ (เช่น รหัสลูกค้า, หมายเลขประจำตัวเทียม)
- แยกกุญแจหรือข้อมูลที่ใช้แปลงข้อมูลแฝงออกจากชุดข้อมูลหลักและเก็บไว้อย่างปลอดภัย

3.3 การทำข้อมูลนิรนาม (Anonymization)

- ดำเนินการตัดหรือแก้ไขข้อมูลส่วนบุคคลที่อาจนำไปสู่การระบุตัวบุคคลออกอย่างสมบูรณ์ เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ เป็นต้น
- ทดสอบข้อมูลเพื่อยืนยันว่าข้อมูลดังกล่าวไม่สามารถย้อนกลับไประบุตัวบุคคลได้ (Irreversibility)

3.4 การบันทึกหลักฐานและเอกสาร

- จัดทำบันทึกการดำเนินการทำข้อมูลแฝงหรือข้อมูลนิรนามอย่างละเอียด พร้อมระบุวันที่ กระบวนการที่ใช้ และผู้ดำเนินการ
- เก็บรักษาหลักฐานในรูปแบบไฟล์อิเล็กทรอนิกส์หรือเอกสาร พร้อมให้ตรวจสอบได้เมื่อจำเป็น

3.5 การตรวจสอบและทบทวน

- ทบทวนแนวทางการทำข้อมูลแฝงและนิรนามอย่างสม่ำเสมอเพื่อให้สอดคล้องกับมาตรฐานและเทคโนโลยีล่าสุด
- ตรวจสอบว่าผู้รับข้อมูลได้รับเฉพาะข้อมูลที่ผ่านการแฝงหรือทำให้นิรนามแล้วเท่านั้น

4. ตัวอย่างหลักฐานประกอบ

4.1 แบบฟอร์มบันทึกการทำข้อมูลแฝง/นิรนาม (Pseudonymization/Anonymization Record Form)

รายละเอียด	ข้อมูล
วันที่ดำเนินการ	[_____]
ผู้ดำเนินการ	[_____]
ประเภทข้อมูลที่ทำกรแฝง/นิรนาม	[_____]
วิธีการทำข้อมูลแฝง/นิรนาม	[เช่น การแทนที่รหัส การตัดข้อมูลส่วนบุคคล]
ระบบหรือเครื่องมือที่ใช้	[_____]
วัตถุประสงค์การแบ่งปันข้อมูล	[_____]
ผู้รับข้อมูล	[_____]
หมายเหตุเพิ่มเติม	[_____]

4.2 ตัวอย่างรายงานการทำข้อมูลแฝง

วันที่: 1 มิถุนายน 2568

ผู้ดำเนินการ: นางสาวสุตารัตน์ จันทร์สว่าง

ข้อมูลที่ทำกรแฝง: หมายเลขประจำตัวประชาชน (แทนที่ด้วยรหัสลูกค้า 6 หลัก)

วิธีการ: ใช้ระบบฐานข้อมูลภายในทำการแทนที่ข้อมูลโดยอัตโนมัติและเก็บกุญแจแยกต่างหาก

วัตถุประสงค์: ส่งข้อมูลให้บริษัทที่ปรึกษาทางการตลาดเพื่อวิเคราะห์พฤติกรรมลูกค้า

ผู้รับข้อมูล: บริษัท Marketing Analytics จำกัด

หมายเหตุ: ข้อมูลที่ส่งออกไปไม่มีชื่อหรือข้อมูลระบุตัวบุคคลอื่นประกอบ

5. กฎหมายที่เกี่ยวข้องและบทลงโทษ

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22 และ มาตรา 37 (1)
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4
- โทษทางปกครองตามมาตรา 83 ในกรณีที่ไม่ปฏิบัติตามมาตรา 22 และมาตรา 37 ปรับไม่เกิน 3 ล้านบาท

6. ผู้รับผิดชอบ

- ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO) มีหน้าที่กำกับดูแลและตรวจสอบการดำเนินการตามแนวทางนี้
- ฝ่ายเทคโนโลยีสารสนเทศ (IT) ร่วมสนับสนุนการจัดทำข้อมูลแฝงหรือข้อมูลนิรนามตามข้อกำหนด

7. การบังคับใช้

แนวปฏิบัตินี้ถือเป็นข้อบังคับสำหรับบุคลากรทุกฝ่ายที่เกี่ยวข้องกับการจัดการและแบ่งปันข้อมูลส่วนบุคคล ผู้ไม่ปฏิบัติตามจะได้รับการพิจารณาดำเนินมาตรการทางวินัยตามนโยบายองค์กร

บทที่ 9

ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

ในยุคดิจิทัลปัจจุบัน การประมวลผลข้อมูลส่วนบุคคลกลายเป็นหัวใจสำคัญของการดำเนินงานทั้งภาครัฐและเอกชน ข้อมูลส่วนบุคคลไม่เพียงเกี่ยวข้องกับการบริหารจัดการธุรกิจหรือการให้บริการต่อประชาชนเท่านั้น แต่ยังมีสำคัญต่อการรักษาความน่าเชื่อถือ ความเป็นส่วนตัว และสิทธิของเจ้าของข้อมูลตามกฎหมาย PDPA (Personal Data Protection Act) การประเมินความเสี่ยงและผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลจึงเป็นเครื่องมือสำคัญที่ช่วยให้องค์กรสามารถระบุ จัดลำดับความสำคัญ และควบคุมความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคลได้อย่างมีระบบ การประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล (Data Protection Risk Assessment) คือกระบวนการวิเคราะห์และประเมินปัจจัยที่อาจก่อให้เกิดผลกระทบต่อความลับ ความถูกต้อง และความพร้อมของข้อมูล ซึ่งรวมถึงความเสี่ยงที่อาจเกิดจากการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่เหมาะสม ความบกพร่องของระบบเทคโนโลยี

สารสนเทศ และข้อจำกัดด้านการปฏิบัติตามกฎหมาย การประเมินความเสี่ยงดังกล่าวจะช่วยให้องค์กรสามารถวางมาตรการควบคุมและลดผลกระทบที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

นอกจากนี้ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment – DPIA) เป็นกระบวนการที่เน้นวิเคราะห์ผลกระทบเชิงลึกต่อสิทธิและเสรีภาพของเจ้าของข้อมูล โดยเฉพาะในกรณีที่มีการประมวลผลข้อมูลในลักษณะที่มีความเสี่ยงสูง เช่น การเก็บรวบรวมข้อมูลเชิงอ่อนไหว (Sensitive Data) การประมวลผลข้อมูลจำนวนมาก (Large-scale Processing) หรือการใช้เทคโนโลยีใหม่ ๆ เช่น การติดตามพฤติกรรมออนไลน์ การประเมินผลกระทบเหล่านี้ช่วยให้องค์กรระบุมาตรการป้องกันที่เหมาะสม เช่น การทำ pseudonymisation การเข้ารหัส การจำกัดการเข้าถึง และการกำหนดบทบาทความรับผิดชอบที่ชัดเจน

การผสมผสานระหว่างการประเมินความเสี่ยงทั่วไปและ DPIA ช่วยให้องค์กรสร้างระบบการจัดการข้อมูลส่วนบุคคลที่มีความมั่นคง ปลอดภัย และสอดคล้องกับข้อกำหนดทางกฎหมาย อีกทั้งยังเสริมสร้างความเชื่อมั่นให้กับเจ้าของข้อมูลว่าข้อมูลของตนได้รับการปกป้องอย่างเหมาะสม นอกจากนี้ การทบทวนและปรับปรุงผลการประเมินเป็นประจำ ยังช่วยให้องค์กรสามารถปรับตัวและตอบสนองต่อความเสี่ยงใหม่ ๆ ที่อาจเกิดขึ้นจากการเปลี่ยนแปลงทางเทคโนโลยีและกฎหมายได้อย่างทันการณ์

โดยสรุป ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลไม่เพียงเป็นเครื่องมือเชิงป้องกัน แต่ยังเป็นหลักประกันสำคัญที่ช่วยให้องค์กรดำเนินการประมวลผลข้อมูลส่วนบุคคลได้อย่างโปร่งใส ปลอดภัย และมีความรับผิดชอบต่อเจ้าของข้อมูลอย่างแท้จริง

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
1. การระบุและจำแนกความเสี่ยงด้านข้อมูลส่วนบุคคล	ระบุความเสี่ยงทุกประเภทที่อาจเกิดขึ้นกับข้อมูลส่วนบุคคล เช่น การเข้าถึงโดยไม่ได้รับ	รายการความเสี่ยง (Risk Register) ตารางจำแนกความเสี่ยง (Risk	ครอบคลุมทุกประเภทความเสี่ยง ระบุ

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้ คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
บุคคล (Identification & Classification of Risks)	อนุญาต การสูญหาย การ รั่วไหล การประมวลผลไม่ ถูกต้อง	Classification Table) รายงานวิเคราะห์เบื้องต้น	รายละเอียด ครบถ้วน สามารถ ตรวจสอบ ย้อนหลังได้
2. การประเมิน ความรุนแรงและ โอกาสเกิดความ เสี่ยง (Risk Assessment – Likelihood & Impact)	ประเมินระดับความรุนแรง (Impact) และโอกาสเกิดเหตุ (Likelihood) ของความเสี่ยง แต่ละรายการ	ตารางประเมินความเสี่ยง (Risk Assessment Matrix) รายงานวิเคราะห์ ความเสี่ยง (Risk Assessment Report)	ประเมินครบทุก ความเสี่ยง มี เกณฑ์ชัดเจนและ สอดคล้องกับ แนวทาง PDPA
3. การจัดลำดับ ความสำคัญของ ความเสี่ยง (Risk Prioritization)	จัดลำดับความสำคัญเพื่อ กำหนดมาตรการควบคุม โดย พิจารณาความรุนแรงและความ เป็นไปได้	ตารางจัดลำดับความเสี่ยง (Risk Ranking Table) Risk Heat Map	ครอบคลุมทุก ความเสี่ยงหลัก สามารถชี้แนะ มาตรการป้องกัน ได้ชัดเจน
4. การกำหนด มาตรการควบคุม และบรรเทาความ เสี่ยง (Risk Mitigation & Controls)	กำหนดมาตรการด้านเทคนิค และองค์กร เช่น การเข้ารหัส การควบคุมการเข้าถึง การ จำกัดสิทธิ การอบรมบุคลากร	รายงานมาตรการควบคุม (Control Measures Report) SOP Policy Evidence of Implementation	ครอบคลุมความ เสี่ยงทั้งหมด สามารถปฏิบัติจริง และตรวจสอบได้
5. การทำ Data Protection Impact Assessment (DPIA)	ประเมินผลกระทบเชิงลึกต่อ สิทธิและเสรีภาพของเจ้าของ ข้อมูล โดยเฉพาะกรณีความ เสี่ยงสูง เช่น การเก็บข้อมูล อ่อนไหว การประมวลผล จำนวนมาก	แบบฟอร์ม DPIA รายงาน DPIA Checklist DPIA	DPIA ครบถ้วน สอดคล้อง PDPA และบันทึกผลการ ประเมินครบทุก ขั้นตอน

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
6. การระบุผู้รับผิดชอบและบทบาท (Responsibility Assignment)	ระบุผู้รับผิดชอบในการจัดการความเสี่ยงและ DPIA เช่น DPO เจ้าหน้าที่ระบบ ฝ่ายกฎหมาย	ตารางบทบาทความรับผิดชอบ (Responsibility Matrix) Org Chart บันทึกมอบหมายงาน	ระบุครบทุกบทบาทและความรับผิดชอบ สามารถตรวจสอบการมอบหมายได้
7. การติดตามและทบทวนความเสี่ยง (Monitoring & Review)	ติดตามผลการจัดการความเสี่ยงและปรับปรุงตามการเปลี่ยนแปลงระบบ กฎหมาย หรือบริบทใหม่	บันทึกการติดตาม (Monitoring Log) รายงานทบทวนความเสี่ยง (Risk Review Report) Version Control	มีหลักฐานการติดตามต่อเนื่อง ทบทวนตามช่วงเวลาและเหตุการณ์สำคัญ
8. การรายงานความเสี่ยงต่อผู้บริหาร (Reporting to Management)	รายงานความเสี่ยงสำคัญ ผลกระทบ และมาตรการบรรเทาให้คณะผู้บริหารหรือคณะกรรมการความเสี่ยง	รายงานผู้บริหาร (Management Report) Presentation Meeting Minutes	รายงานครบถ้วน ชัดเจน สามารถใช้ตัดสินใจได้จริง
9. การบันทึกและจัดเก็บหลักฐาน (Record-Keeping & Evidence)	จัดเก็บเอกสารและหลักฐานการประเมินความเสี่ยง การปฏิบัติตามมาตรการ และ DPIA	Risk Register DPIA Report Audit Trail Evidence of Control Implementation	ครบถ้วน ตรวจสอบย้อนหลังได้ และสามารถใช้เป็นหลักฐาน PDPA
10. การฝึกอบรมและสร้างความตระหนักรู้เกี่ยวกับความเสี่ยง (Training & Awareness)	อบรมบุคลากรเกี่ยวกับการประเมินความเสี่ยง การจัดการ DPIA และบทบาทหน้าที่ของตน	แผนอบรม (Training Plan) สไลด์ (Presentation) รายชื่อผู้เข้าร่วม (Attendance Sheet) แบบสอบถามประเมินผล (Evaluation Form)	บุคลากรทุกระดับ ได้รับการอบรม มีหลักฐานชัดเจน และสามารถปฏิบัติได้จริง

หัวข้อย่อ	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
11. การตรวจสอบภายใน (Internal Audit / Compliance Check)	ตรวจสอบว่าการประเมินความเสี่ยงและ DPIA ถูกนำไปใช้จริง และสอดคล้อง PDPA	รายงานตรวจสอบภายใน (Internal Audit Report) Compliance Checklist Audit Log	มีรายงานตรวจสอบพร้อมข้อเสนอแนะ และหลักฐานการปฏิบัติจริง

การจัดทำเอกสารตามเกณฑ์

8.1.1 องค์กรมีกระบวนการที่จะช่วยให้พนักงานรายงานและยกระดับการปกป้องข้อมูล และสามารถแจ้งข้อกังวลและความเสี่ยงด้านการกำกับดูแลข้อมูลไปยังจุดศูนย์กลางหรือหน่วยงานกลางที่องค์กรกำหนด

สิ่งที่ต้องทำ: องค์กรมีกระบวนการหรือแนวปฏิบัติที่ช่วยให้พนักงานรายงานและยกระดับการปกป้องข้อมูล และสามารถแจ้งข้อกังวลและความเสี่ยงด้านการกำกับดูแลข้อมูลไปยังจุดศูนย์กลางหรือหน่วยงานกลางที่องค์กรกำหนด และมีเอกสารครบถ้วน

หลักฐาน: นโยบายภายในในการจัดให้มีมาตรการหรือช่องทางสำหรับการรายงานถึงข้อกังวลและความเสี่ยงด้านการกำกับดูแลข้อมูลส่วนบุคคลมายังศูนย์กลางหรือหน่วยงานกลางขององค์กร ประกาศช่องทางและวิธีการรายงานข้อกังวลและความเสี่ยงด้านการกำกับดูแลข้อมูลส่วนบุคคล รายงานข้อกังวลและความเสี่ยงด้านการกำกับดูแลข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3)

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการรายงานและยกระดับข้อกังวลด้านการกำกับดูแลข้อมูลส่วนบุคคล

(Policy on Reporting and Escalation of Data Governance Concerns)

1. วัตถุประสงค์

- นโยบายนี้จัดทำขึ้นเพื่อกำหนดกระบวนการและช่องทางในการรายงานข้อกังวล ข้อสงสัย หรือความเสี่ยงที่เกี่ยวข้องกับการคุ้มครองและการกำกับดูแลข้อมูลส่วนบุคคลภายในองค์กร โดยมีเป้าหมายเพื่อ

- เสริมสร้างความตระหนักรู้และการมีส่วนร่วมของพนักงานทุกระดับ
- สนับสนุนให้องค์กรสามารถตรวจพบและจัดการความเสี่ยงด้านข้อมูลได้อย่างทัน่วงที่
- สอดคล้องกับข้อกำหนดด้านกฎหมายและมาตรฐานที่เกี่ยวข้อง

2. ขอบเขต

- นโยบายนี้ครอบคลุมถึง
- พนักงานทุกคนในองค์กร (ประจำ/ชั่วคราว/สัญญาจ้าง)
- ผู้บริหารทุกระดับ
- หน่วยงานที่เกี่ยวข้องกับการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3. นโยบายหลัก

(1) องค์กรจัดให้มี **ช่องทางศูนย์กลาง (Central Channel)** สำหรับการรายงานข้อกังวลด้านข้อมูลส่วนบุคคล ได้แก่

- อีเมลกลางของหน่วยงานกำกับดูแลข้อมูล: **privacy@[ชื่อองค์กร].com**
- เบอร์โทรศัพท์สายตรงฝ่ายกำกับดูแลข้อมูล (Data Governance Hotline): **0-xxx-xxxx**
- กล่องรับแจ้ง (Data Concern Box) ภายในสำนักงาน
- ระบบออนไลน์ (Intranet Portal)

(2) พนักงานทุกคนมีสิทธิและหน้าที่ในการรายงานข้อกังวลหรือเหตุการณ์ที่อาจกระทบต่อการคุ้มครองข้อมูลส่วนบุคคล เช่น

- การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- การเก็บหรือใช้ข้อมูลเกินวัตถุประสงค์
- การขาดมาตรการควบคุมความปลอดภัย

(3) การรายงานสามารถทำได้ทั้ง **เปิดเผยชื่อ** หรือ **ไม่เปิดเผยชื่อ** โดยองค์กรรับประกันความลับของผู้รายงาน

(4) หน่วยงานกำกับดูแลข้อมูล (เช่น Data Protection Office / ฝ่ายกฎหมาย / คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) เป็นผู้รับผิดชอบตรวจสอบและดำเนินการตามกระบวนการแก้ไข/ป้องกัน

(5) องค์กรห้ามมิให้มีการตอบโต้ผู้รายงาน (Non-retaliation Policy)

4. กระบวนการรายงานและยกระดับ (Escalation Process)

- พนักงานรายงานข้อกังวล ผ่านช่องทางที่กำหนด
- หน่วยงานกลางรับเรื่อง → ลงทะเบียนและบันทึกเหตุการณ์
- ประเมินความเสี่ยงเบื้องต้น ว่าเป็นความเสี่ยงระดับต่ำ กลาง หรือสูง

- หากเป็นความเสียหายสูง → ยกระดับให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขององค์กร ภายใน 24 ชั่วโมง
- สรุปผลการตรวจสอบและการดำเนินการแก้ไข พร้อมรายงานต่อผู้บริหาร
- แจ้งผลการดำเนินงาน แก่ผู้รายงาน (ถ้าเปิดเผยตัวตน)

5. หลักฐานที่ต้องมี (Evidence Required)

- นโยบายนี้ (เป็นเอกสารภายในองค์กร)
- ประกาศช่องทางการรายงาน (เช่น บน Intranet / บอร์ดประกาศ / อีเมลประชาสัมพันธ์)
- แบบฟอร์มรายงานข้อกังวล (Data Concern Reporting Form)
- รายงานสรุปข้อกังวลและการแก้ไขปัญหา (Data Governance Concern Log & Report)

6. การทบทวนและปรับปรุง

นโยบายนี้ต้องมีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย มาตรฐาน หรือกระบวนการภายในองค์กร

นอกจากนี้ผู้เขียนเห็นว่าอาจรายงานข้อกังวล (Data Concern Reporting Form) และ Flowchart กระบวนการรายงาน เพื่อแนบเป็นหลักฐานเพิ่มเติมเพื่อความสมบูรณ์ได้ ซึ่งอาจดำเนินการตามตัวอย่างนี้

(1) แบบฟอร์มรายงานข้อกังวลด้านการกำกับดูแลข้อมูลส่วนบุคคล

Data Governance Concern Reporting Form

ข้อมูลผู้รายงาน

- ชื่อ-นามสกุล:
- แผนก/หน่วยงาน:
- เบอร์โทรศัพท์/อีเมล:
- (หากไม่ต้องการเปิดเผยตัวตน โปรดข้ามส่วนนี้)

ประเภทข้อกังวล (เลือกได้มากกว่า 1 ข้อ)

- การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- การเก็บหรือใช้ข้อมูลเกินวัตถุประสงค์
- การเปิดเผยข้อมูลโดยไม่ชอบ
- การขาดมาตรการควบคุมด้านความปลอดภัย

— อื่น ๆ (โปรดระบุ):

รายละเอียดเหตุการณ์

.....

วันที่เกิดเหตุการณ์

...../...../..... เวลา น.

เอกสาร/หลักฐานแนบ

— ไม่มี

— มี (โปรดระบุ):

ความเร่งด่วน (ผู้รายงานประเมิน)

— ปกติ

— เร่งด่วน

— อุกเหิน/เสี่ยงร้ายแรง

ข้อเสนอแนะ/ความคิดเห็นเพิ่มเติม

.....

Flowchart กระบวนการรายงาน

กระบวนการรายงานและยกระดับข้อกังวล

Data Governance Concern Reporting Process

ขั้นตอนที่ 1

พนักงานหรือผู้เกี่ยวข้องรายงานข้อกังวลผ่านช่องทางที่กำหนด

— Email: privacy@[ชื่อองค์กร].com

— Hotline: 0-xxx-xxxx

— Intranet Portal / แบบฟอร์ม

กล่องรับเรื่องร้องเรียน

ขั้นตอนที่ 2

- หน่วยงานกลาง (Data Governance Office หรือ DPO)
- รับเรื่อง → บันทึกใน Data Concern Log
- ตรวจสอบความครบถ้วนของข้อมูล

ขั้นตอนที่ 3

การประเมินเบื้องต้น

- ระดับต่ำ → แจ้งหน่วยงานที่เกี่ยวข้องแก้ไข
- ระดับกลาง → รายงานผู้บริหารสายงาน
- ระดับสูง/ฉุกเฉิน → ยกระดับต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 24 ชั่วโมง

ขั้นตอนที่ 4

- การดำเนินการแก้ไขและป้องกัน
- แต่งตั้งผู้รับผิดชอบ
- ตรวจสอบข้อเท็จจริง
- กำหนดมาตรการแก้ไข/ป้องกัน

ขั้นตอนที่ 5

- การรายงานผล
- จัดทำรายงานสรุป (Investigation Report)
- แจ้งผู้บริหาร
- แจ้งผลต่อผู้รายงาน (ถ้าเปิดเผยชื่อ)

ขั้นตอนที่ 6

- การจัดเก็บและทบทวน
- เก็บเอกสาร/รายงานไว้ในระบบอย่างปลอดภัย
- นำผลการดำเนินการเข้าสู่การทบทวนนโยบายประจำปี

8.1.2 องค์การระบุและจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลในทะเบียนจัดการความเสี่ยง (Risk Register) ที่เหมาะสม ซึ่งรวมถึงการเชื่อมโยงที่ชัดเจนระหว่างทะเบียนจัดการความเสี่ยง (Risk Register) ขององค์กรและแผนก/ส่วนงานต่าง ๆ และการประเมินความเสี่ยงของทรัพย์สินสารสนเทศ (Information Assets)

สิ่งที่ต้องทำ: องค์การมีการระบุและจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลในทะเบียนจัดการความเสี่ยงที่

เหมาะสม ซึ่งรวมถึงการเชื่อมโยงที่ชัดเจนระหว่างทะเบียนจัดการความเสี่ยง (Risk Register) ขององค์กรและแผนก/ส่วนงานต่าง ๆ และการประเมินความเสี่ยงของทรัพย์สินสารสนเทศ

หลักฐาน: นโยบายภายในสำหรับการจัดทำทะเบียนจัดการความเสี่ยงทั่วไป และทะเบียนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1. ทะเบียนจัดการความเสี่ยง (Risk Register) ทั่วไป
2. ทะเบียนจัดการความเสี่ยง (Risk Register) ของฝ่ายเทคโนโลยีสารสนเทศ
3. รายงานเหตุการณ์ด้านความเสี่ยงของข้อมูลส่วนบุคคล
4. รายงานผลการตรวจสอบทะเบียนจัดการความเสี่ยง (Risk Register) ทั่วไป
5. รายงานการตรวจสอบทะเบียนจัดการความเสี่ยง (Risk Register) ของฝ่ายเทคโนโลยีสารสนเทศ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3)

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

หลักฐานการระบุและจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลในทะเบียนจัดการความเสี่ยง (Risk Register)

1. นโยบายภายในสำหรับการจัดทำทะเบียนจัดการความเสี่ยง

องค์กรได้จัดทำนโยบายภายในเรื่อง “นโยบายการบริหารจัดการความเสี่ยง (Risk Management Policy)” ซึ่งครอบคลุมประเด็นสำคัญดังนี้

- กำหนดกรอบแนวทางและขอบเขตของการบริหารจัดการความเสี่ยงในองค์กร
- ระบุความรับผิดชอบของทุกแผนก/ส่วนงานในการระบุ วิเคราะห์ และรายงานความเสี่ยงที่เกี่ยวข้องกับกิจกรรมของตน
- เน้นความสำคัญของการเชื่อมโยงข้อมูลความเสี่ยงระหว่างทะเบียนจัดการความเสี่ยงระดับองค์กร และทะเบียนจัดการความเสี่ยงในแต่ละแผนก/ส่วนงาน รวมทั้งฝ่ายเทคโนโลยีสารสนเทศ
- มีแนวทางในการประเมินความเสี่ยงของทรัพย์สินสารสนเทศ (Information Assets) ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล
- กำหนดระยะเวลาการทบทวนและปรับปรุงทะเบียนจัดการความเสี่ยงเป็นระยะ
- ระบุขั้นตอนการรายงานและติดตามผลการจัดการความเสี่ยงต่อผู้บริหารระดับสูง

2. ทะเบียนจัดการความเสี่ยง (Risk Register)

2.1 ทะเบียนจัดการความเสี่ยงทั่วไปขององค์กร

- รายการความเสี่ยงในภาพรวมขององค์กร รวมทั้งความเสี่ยงด้านข้อมูลส่วนบุคคล
- มีคอลัมน์สำคัญ เช่น รหัสความเสี่ยง รายละเอียดความเสี่ยง แผนก/ส่วนงานที่รับผิดชอบ ความรุนแรง (Severity) ความน่าจะเป็น (Likelihood) ระดับความเสี่ยง (Risk Level) มาตรการควบคุม และสถานะปัจจุบัน
- เชื่อมโยงกับทะเบียนจัดการความเสี่ยงเฉพาะแผนกหรือส่วนงาน

2.2 ทะเบียนจัดการความเสี่ยงฝ่ายเทคโนโลยีสารสนเทศ

- เจาะจงความเสี่ยงที่เกี่ยวข้องกับระบบสารสนเทศและการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสี่ยงจากการโจมตีไซเบอร์ ความผิดพลาดของระบบ หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ระบุทรัพย์สินสารสนเทศสำคัญที่เกี่ยวข้อง พร้อมการประเมินความเสี่ยงและมาตรการป้องกัน
- มีการทบทวนและอัปเดตทะเบียนนี้อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์สำคัญ

3. รายงานเหตุการณ์ด้านความเสี่ยงของข้อมูลส่วนบุคคล

- เอกสารรายงานเหตุการณ์ความเสี่ยงที่เกิดขึ้นจริง หรือข้อสังเกตที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- รายละเอียดเหตุการณ์ วันที่เกิด รายงานผู้รับผิดชอบ และมาตรการที่นำมาใช้ในการแก้ไขและป้องกันไม่ให้เกิดซ้ำ
- รายงานเหล่านี้จะถูกรวบรวมและนำเข้าสู่กระบวนการบริหารความเสี่ยงขององค์กร

4. รายงานผลการตรวจสอบทะเบียนจัดการความเสี่ยง

4.1 รายงานตรวจสอบทะเบียนจัดการความเสี่ยงทั่วไป

- รายงานการตรวจสอบโดยฝ่ายตรวจสอบภายในหรือบุคคลที่ได้รับมอบหมาย
- ตรวจสอบความครบถ้วน ความสอดคล้องกับนโยบายภายใน และความเหมาะสมของการจัดการความเสี่ยง
- ระบุข้อเสนอแนะเพื่อปรับปรุงและแก้ไขในกรณีพบช่องว่าง

4.2 รายงานตรวจสอบทะเบียนจัดการความเสี่ยงฝ่ายเทคโนโลยีสารสนเทศ

- ตรวจสอบความสอดคล้องของทะเบียนกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศ
- ประเมินการจัดการความเสี่ยงที่เกี่ยวข้องกับการปกป้องข้อมูลส่วนบุคคลในระบบสารสนเทศ
- ให้คำแนะนำและข้อเสนอแนะสำหรับการเสริมสร้างมาตรการป้องกัน

หลักฐานการจัดการกระบวนการรายงานและยกระดับการปกป้องข้อมูลส่วนบุคคล

(Data Protection Reporting and Escalation Process)

1. นโยบายและแนวปฏิบัติภายในองค์กร

องค์กรได้จัดทำนโยบายภายในเรื่อง “นโยบายการรายงานข้อกังวลและความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล” ซึ่งระบุรายละเอียดดังนี้

- พนักงานทุกคนมีหน้าที่และความรับผิดชอบในการรายงานข้อกังวลหรือเหตุการณ์ที่อาจก่อให้เกิดความเสี่ยงต่อข้อมูลส่วนบุคคลที่องค์กรดูแล
- กำหนดช่องทางและวิธีการรายงานที่ชัดเจน เช่น ผ่านระบบแจ้งเหตุออนไลน์ อีเมล หรือสายด่วนภายในองค์กร
- การรายงานสามารถทำได้โดยไม่เปิดเผยชื่อ (Anonymous Reporting) เพื่อคุ้มครองผู้รายงาน
- กำหนดหน่วยงานกลางหรือจุดศูนย์กลางรับผิดชอบการรับเรื่องและดำเนินการประสานงาน ได้แก่ ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO)
- มีขั้นตอนการวิเคราะห์และประเมินความเสี่ยงที่ได้รับรายงาน พร้อมกำหนดแนวทางการแก้ไขหรือป้องกันอย่างเหมาะสม
- มีกระบวนการติดตามผลและรายงานความคืบหน้าให้ผู้ที่เกี่ยวข้องทราบอย่างสม่ำเสมอ

2. ประกาศช่องทางและวิธีการรายงานข้อกังวลและความเสี่ยงด้านข้อมูลส่วนบุคคล

องค์กรได้จัดทำเอกสารประกาศอย่างเป็นทางการเผยแพร่ให้พนักงานทราบผ่านช่องทางต่าง ๆ เช่น

- ประกาศในระบบอินทราเน็ตขององค์กร
- อีเมลแจ้งข่าวสารภายใน
- ป้ายประกาศในพื้นที่ทำงาน
- คู่มือพนักงาน

ตัวอย่างข้อความประกาศ:

“หากพนักงานพบเห็นหรือมีข้อกังวลเกี่ยวกับการปกป้องข้อมูลส่วนบุคคล หรือพบความเสี่ยงด้านการกำกับดูแลข้อมูลส่วนบุคคล สามารถรายงานได้ที่

ระบบแจ้งเหตุออนไลน์: [URL ของระบบ]

อีเมล: dpo@company.com

สายด่วนภายในหมายเลข: 1234

รายงานสามารถทำได้โดยไม่ต้องเปิดเผยชื่อเพื่อคุ้มครองความเป็นส่วนตัวของผู้รายงาน”

3. รายงานข้อกังวลและความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

องค์กรเก็บบันทึกการรายงานข้อกังวลและความเสี่ยงที่ได้รับไว้ในระบบบริหารจัดการความเสี่ยง (Risk Management System) หรือระบบจัดการข้อร้องเรียน โดยมีข้อมูลหลักดังนี้

วันที่ รายงาน	รายละเอียดข้อกังวล/ ความเสี่ยง	ผู้รายงาน (ถ้ามี)	หน่วยงาน รับผิดชอบ	สถานะการ ดำเนินการ	หมายเหตุ
12 มี.ค. 2568	พบการเข้าถึงข้อมูลโดย ไม่ได้รับอนุญาต	ไม่ระบุชื่อ	ฝ่าย IT Security	ดำเนินการ แก้ไขแล้ว	ปิดเคส
20 เม.ย. 2568	ข้อมูลส่วนบุคคลไม่ได้รับ การเข้ารหัสตามนโยบาย	คุณสมชาย	ฝ่าย DPO	อยู่ระหว่าง ตรวจสอบ	-

4. กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) และ (3)
- โทษทางปกครองตามมาตรา 83 ปรับไม่เกิน 3 ล้านบาทในกรณีไม่ปฏิบัติตามมาตรา 37

5. ผู้รับผิดชอบ

- ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO) รับผิดชอบรับและประสานงานการจัดการข้อกังวลและความเสี่ยง
- ฝ่ายทรัพยากรบุคคลและฝ่าย IT สนับสนุนการจัดทำช่องทางและมาตรการตามนโยบายนี้

เอกสาร นโยบายบริหารจัดการความเสี่ยง (Risk Management Policy) ตัวอย่างฟอร์ม ทะเบียนจัดการความเสี่ยง (Risk Register) และตัวอย่าง รายงานการตรวจสอบทะเบียนจัดการความเสี่ยง

ตัวอย่างเอกสารนโยบายบริหารจัดการความเสี่ยง (Risk Management Policy)

ชื่อเอกสาร: นโยบายบริหารจัดการความเสี่ยงองค์กร

เลขที่เอกสาร: RM-001/2568

วันที่บังคับใช้: 1 มิถุนายน 2568

จัดทำโดย: ฝ่ายบริหารความเสี่ยง

อนุมัติโดย: คณะกรรมการบริหารองค์กร

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและกรอบการบริหารจัดการความเสี่ยงในองค์กรอย่างเป็นระบบ เพื่อปกป้องข้อมูลส่วนบุคคลและทรัพย์สินสารสนเทศ ตลอดจนบริหารความเสี่ยงด้านอื่น ๆ ที่ส่งต่อการดำเนินงานอย่างมีประสิทธิภาพ

2. ขอบเขต

นโยบายนี้ครอบคลุมทุกแผนก/ส่วนงานในองค์กร รวมถึงการบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยของข้อมูล

3. ความรับผิดชอบ

- ผู้บริหารแต่ละแผนก/ส่วนงาน รับผิดชอบในการระบุ วิเคราะห์ และรายงานความเสี่ยงของหน่วยงานตนเอง
- ฝ่ายบริหารความเสี่ยง รับผิดชอบในการรวบรวมและจัดการทะเบียนจัดการความเสี่ยงระดับองค์กร
- ฝ่ายเทคโนโลยีสารสนเทศ รับผิดชอบบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับระบบสารสนเทศและข้อมูลส่วนบุคคล

4. แนวทางบริหารจัดการความเสี่ยง

- ระบุและประเมินความเสี่ยงที่มีผลกระทบต่อข้อมูลส่วนบุคคลและทรัพย์สินสารสนเทศ
- จัดทำและอัปเดตทะเบียนจัดการความเสี่ยง (Risk Register) ทั้งระดับองค์กรและระดับแผนก/ส่วนงานอย่างสม่ำเสมอ
- เชื่อมโยงทะเบียนจัดการความเสี่ยงในแต่ละแผนก/ส่วนงานเข้ากับทะเบียนระดับองค์กร
- กำหนดมาตรการควบคุมและบรรเทาความเสี่ยงที่เหมาะสม
- ทบทวนและรายงานสถานะความเสี่ยงต่อผู้บริหารระดับสูงอย่างน้อยปีละหนึ่งครั้ง

5. การรายงานและแจ้งเตือน

- พนักงานทุกคนมีหน้าที่รายงานเหตุการณ์หรือข้อกังวลด้านความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและความมั่นคงของข้อมูลไปยังฝ่ายบริหารความเสี่ยงหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- จัดให้มีช่องทางการแจ้งเตือนและรายงานที่ชัดเจนและเข้าถึงได้ง่าย

6. การตรวจสอบและทบทวน

- ฝ่ายตรวจสอบภายในจะทำการตรวจสอบกระบวนการบริหารจัดการความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง
- ผลการตรวจสอบและข้อเสนอแนะจะถูกนำไปใช้ปรับปรุงกระบวนการอย่างต่อเนื่อง

ตัวอย่างฟอร์มทะเบียนจัดการความเสี่ยง (Risk Register)

รหัสความเสี่ยง	รายละเอียดความเสี่ยง	แผนก/ส่วนงานรับผิดชอบ	ความรุนแรง (1-5)	ความน่าจะเป็น (1-5)	ระดับความเสี่ยง (คูณ)	มาตรการควบคุม	สถานะ	วันที่พบทวนล่าสุด	หมายเหตุ
RIS-001	การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต	ฝ่ายเทคโนโลยีสารสนเทศ	5	3	15	ใช้ระบบยืนยันตัวตนแบบสองขั้นตอน	กำลังดำเนินการ	10 พ.ค. 2568	ปรับปรุงระบบ MFA แล้ว
RIS-002	การเปิดเผยข้อมูลส่วนบุคคลเกินความจำเป็น	ฝ่ายบริหารข้อมูล	4		8	ตรวจสอบสิทธิ์การเข้าถึงข้อมูล	ดำเนินการแล้ว	10 พ.ค. 2568	ไม่มีเหตุการณ์ผิดปกติ

ตัวอย่างรายงานการตรวจสอบทะเบียนจัดการความเสี่ยง

ชื่อรายงาน: รายงานการตรวจสอบทะเบียนจัดการความเสี่ยงองค์กร

เลขที่: AUD-RM-002/2568

วันที่ตรวจสอบ: 15 พฤษภาคม 2568

ผู้ตรวจสอบ: ฝ่ายตรวจสอบภายใน

หน่วยงานที่ถูกรตรวจสอบ: ฝ่ายบริหารความเสี่ยง ฝ่ายเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์

เพื่อประเมินความสอดคล้องและประสิทธิผลของกระบวนการบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลและทรัพย์สินสารสนเทศตามนโยบายและข้อกำหนดภายในองค์กร

2. ขอบเขต

ตรวจสอบทะเบียนจัดการความเสี่ยงทั่วไปขององค์กรและทะเบียนจัดการความเสี่ยงของฝ่ายเทคโนโลยีสารสนเทศ

3. ผลการตรวจสอบ

รายการตรวจสอบ	ผลการตรวจสอบ	ข้อสังเกต/ข้อเสนอแนะ
ความครบถ้วนของทะเบียนจัดการความเสี่ยงทั่วไป	ครบถ้วนและอัปเดตเป็นประจำ	-
การเชื่อมโยงกับทะเบียนแผนก/ส่วนงานต่าง ๆ	มีการเชื่อมโยงและสอดคล้อง	แนะนำเพิ่มรายละเอียดการเชื่อมโยง
การประเมินความเสี่ยงของทรัพย์สินสารสนเทศ	มีการประเมินและจัดอันดับ	ควรเพิ่มความถี่การทบทวนในบางทรัพย์สิน
การรายงานและติดตามความเสี่ยง	มีรายงานต่อผู้บริหารตามระยะเวลา	-

4. สรุป

องค์กรมีระบบบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลที่เหมาะสมและมีประสิทธิภาพ โดยมีการอัปเดตทะเบียนความเสี่ยงและมาตรการควบคุมอย่างสม่ำเสมอ ควรปรับปรุงการเชื่อมโยงรายละเอียดในทะเบียนจัดการความเสี่ยงให้ชัดเจนมากขึ้น และเพิ่มความถี่การประเมินบางทรัพย์สินสารสนเทศ

8.1.2 องค์กรระบุและจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลในทะเบียนจัดการความเสี่ยง (Risk Register) ที่เหมาะสม ซึ่งรวมถึงการเชื่อมโยงที่ชัดเจนระหว่างทะเบียนจัดการความเสี่ยง (Risk Register) ขององค์กรและแผนก/ส่วนงานต่าง ๆ และการประเมินความเสี่ยงของทรัพย์สินสารสนเทศ (Information Assets)

- สิ่งที่ต้องทำ: องค์กรมีการระบุและจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลในทะเบียนจัดการความเสี่ยงที่เหมาะสม ซึ่งรวมถึงการเชื่อมโยงที่ชัดเจนระหว่างทะเบียนจัดการความเสี่ยง (Risk Register) ขององค์กรและแผนก/ส่วนงานต่าง ๆ และการประเมินความเสี่ยงของทรัพย์สินสารสนเทศ
- หลักฐาน: นโยบายภายในสำหรับการจัดทำทะเบียนจัดการความเสี่ยงทั่วไป และทะเบียนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
1. ทะเบียนจัดการความเสี่ยง (Risk Register) ทั่วไป
 2. ทะเบียนจัดการความเสี่ยง (Risk Register) ของฝ่ายเทคโนโลยีสารสนเทศ
 3. รายงานเหตุการณ์ด้านความเสี่ยงของข้อมูลส่วนบุคคล
 4. รายงานผลการตรวจสอบทะเบียนจัดการความเสี่ยง (Risk Register) ทั่วไป
 5. รายงานการตรวจสอบทะเบียนจัดการความเสี่ยง (Risk Register) ของฝ่ายเทคโนโลยีสารสนเทศ
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3)
โทษทางปกครอง ในกรณีที่ไม่มีปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การระบุและจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลในทะเบียนจัดการความเสี่ยง (Risk Register) พร้อมใช้เป็นหลักฐานประกอบการประเมินตาม PDPA

1. นโยบายภายในสำหรับการจัดทำทะเบียนจัดการความเสี่ยง (Risk Register)

ชื่อเอกสาร: นโยบายการบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล

สาระสำคัญ:

องค์กรกำหนดให้มีการจัดทำทะเบียนความเสี่ยงของทุกหน่วยงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล การจัดทำ Risk Register ต้องครอบคลุมประเด็นเกี่ยวกับความเสี่ยงจากการประมวลผลข้อมูล ความปลอดภัยของระบบ และความเสี่ยงต่อสิทธิของเจ้าของข้อมูล

มีการประสานงานกับฝ่ายเทคโนโลยีสารสนเทศ (IT) และฝ่ายกฎหมาย (Legal) เพื่อตรวจสอบความครอบคลุมของความเสี่ยง Risk Register ต้องได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง

2. ตัวอย่างทะเบียนจัดการความเสี่ยง (Risk Register) ทั่วไป

ลำดับ	ความเสี่ยง	หน่วยงาน รับผิดชอบ	ความ รุนแรง	ความ น่าจะเป็น	คะแนน รวม	มาตรการ ควบคุม	สถานะ
1	การเข้าถึง ข้อมูลโดย ไม่ได้รับ อนุญาต	IT	สูง	ปาน กลาง	สูง	ใช้ MFA จำกัด สิทธิการเข้าถึง	กำลัง ดำเนินการ
2	การส่งอีเมล ผิดผู้รับ	ฝ่ายบุคคล	ปาน กลาง	สูง	สูง	อบรมการส่ง อีเมลอย่าง ปลอดภัย	ดำเนินการ แล้ว

3. ทะเบียนจัดการความเสี่ยงของฝ่ายเทคโนโลยีสารสนเทศ

ครอบคลุมความเสี่ยงต่อ Information Assets เช่น เซิร์ฟเวอร์ ฐานข้อมูล อุปกรณ์เครือข่าย มีการแนบเอกสารการประเมินมูลค่าทรัพย์สิน (Asset Valuation) และผลกระทบจากการรั่วไหลของข้อมูล

4. รายงานเหตุการณ์ด้านความเสี่ยงของข้อมูลส่วนบุคคล

หัวข้อ: รายงานการละเมิดข้อมูลเมื่อเดือนเมษายน 2568

วันที่เกิดเหตุ: 20 เมษายน 2568

เหตุการณ์: พนักงานส่งไฟล์ข้อมูลลูกค้าไปยังบุคคลผิด

ประเภทข้อมูล: ข้อมูลติดต่อส่วนบุคคล

ผลกระทบ: แจ้งเตือนลูกค้า 50 ราย และรายงานต่อสำนักงานคุ้มครองข้อมูล

การจัดการ: ทบทวน Risk Register และเพิ่มความถี่ในการอบรมด้านความปลอดภัย

5. รายงานผลการตรวจสอบทะเบียนจัดการความเสี่ยง (องค์กรและฝ่าย IT)

หัวข้อ: รายงานผลการตรวจสอบทะเบียนความเสี่ยงประจำไตรมาส 2/2568

- การทบทวนความสอดคล้องระหว่าง Risk Register และสถานะการบริหารความเสี่ยงจริง
- การประเมินผลลัพธ์จากมาตรการควบคุมที่ใช้อยู่
- การเชื่อมโยงความเสี่ยงของแต่ละแผนกลับไปยัง Risk Register ส่วนกลาง
- มีข้อเสนอแนะเพิ่มเติมในการใช้ระบบอัตโนมัติช่วยแจ้งเตือนความเสี่ยงซ้ำซ้อน

8.1.3 หากองค์กรมีการระบุความเสี่ยงด้านข้อมูลส่วนบุคคล องค์กรมีแผนปฏิบัติการ รายงานความคืบหน้า และการพิจารณาบทเรียนที่ได้รับเพื่อหลีกเลี่ยงความเสี่ยงในอนาคต

สิ่งที่ต้องทำ: องค์กรมีการระบุความเสี่ยงด้านข้อมูลส่วนบุคคล มีแผนปฏิบัติการ มีการรายงานความคืบหน้า และมีการพิจารณาบทเรียนที่ได้รับเพื่อหลีกเลี่ยงความเสี่ยงในอนาคต

หลักฐาน: นโยบายการกำหนดแผนปฏิบัติการ รายงานความคืบหน้า และการพิจารณาบทเรียนที่ได้รับเพื่อหลีกเลี่ยงความเสี่ยงในอนาคต

รายงานผลการติดตามและประเมินผลการบริหารความเสี่ยง และบทเรียนที่ได้รับเพื่อหลีกเลี่ยงความเสี่ยงในอนาคต

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 5

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การ รายงานความคืบหน้า และการพิจารณาบทเรียนที่ได้รับจากความเสี่ยงด้านข้อมูลส่วนบุคคล พร้อมใช้เป็นเอกสารประกอบการตรวจประเมินตาม PDPA

1. นโยบายการกำหนดแผนปฏิบัติการ รายงานความคืบหน้า และการพิจารณาบทเรียนที่ได้รับ

ชื่อเอกสาร: นโยบายการจัดการและติดตามแผนปฏิบัติการความเสี่ยงด้านข้อมูลส่วนบุคคล

สาระสำคัญ:

- องค์กรกำหนดให้มีการจัดทำแผนปฏิบัติการ (Action Plan) ทันทีเมื่อมีการระบุความเสี่ยงด้านข้อมูลส่วนบุคคล
- มีการกำหนดระยะเวลา ความรับผิดชอบ และตัวชี้วัด (KPI) ในแต่ละแผน
- รายงานความคืบหน้า (Progress Report) ต้องจัดทำเป็นรายไตรมาส
- บทเรียนที่ได้รับ (Lessons Learned) จะต้องถูกวิเคราะห์และนำไปปรับปรุงแนวทางการดำเนินงาน รวมถึง Risk Register
- หน่วยงานเจ้าของความเสี่ยงต้องจัดประชุม Internal Risk Review เพื่อนำเสนอบทเรียนและแนวทางแก้ไขต่อคณะทำงานคุ้มครองข้อมูลส่วนบุคคล

2. แผนปฏิบัติการกรณีตัวอย่าง: ความเสี่ยงจากการส่งอีเมลผิดผู้รับ

ชื่อแผน: แผนปฏิบัติการลดความเสี่ยงจากความผิดพลาดในการส่งข้อมูลส่วนบุคคลผ่านอีเมล

วันที่เริ่มแผน: 1 เมษายน 2568

ความเสี่ยงที่พบ: พนักงานฝ่ายบริการลูกค้าส่งข้อมูลผิดผู้รับ

ผลกระทบ: มีการรั่วไหลของข้อมูลส่วนบุคคล (ชื่อ ที่อยู่ เบอร์โทร)

มาตรการ:

- จัดอบรมเพิ่มเติมเกี่ยวกับการส่งอีเมลและใช้ระบบ “Double Confirmation”
- ติดตั้งระบบเตือนก่อนส่งไฟล์แนบออกจากโดเมน
- ปรับแบบฟอร์มอัตโนมัติให้ลดการแนบไฟล์ที่ไม่จำเป็น
- ผู้รับผิดชอบ: หัวหน้าฝ่ายบริการลูกค้าและเจ้าหน้าที่ DPO
- ระยะเวลาดำเนินการ: 1 เม.ย. – 31 พ.ค. 2568

ตัวชี้วัด: ลดอัตราข้อผิดพลาดลงอย่างน้อย 80% ภายใน 2 เดือน

3. รายงานความคืบหน้า (Progress Report)

ชื่อรายงาน: รายงานความคืบหน้าในการดำเนินการตามแผนปฏิบัติการลดความเสี่ยงจากอีเมลผิดผู้รับ

ระยะเวลารายงาน: 1–30 เมษายน 2568

สถานะการดำเนินงาน: เสร็จสิ้นแล้ว 3 ใน 4 มาตรการ

ความสำเร็จ: พนักงาน 100% เข้าร่วมการอบรม

คำแนะนำเพิ่มเติมจาก DPO: ทบทวน Checklists การส่งอีเมลสำหรับพนักงานใหม่

ปัญหาที่พบ: การตั้งค่าระบบเตือนยังไม่เสถียร คาดว่าจะเสร็จสมบูรณ์ภายใน 15 พฤษภาคม

4. รายงานบทเรียนที่ได้รับ (Lessons Learned)

ชื่อเอกสาร: บทเรียนจากเหตุการณ์ความผิดพลาดในการส่งข้อมูลผ่านอีเมล

สาเหตุ: ขาดการตรวจสอบซ้ำก่อนกดส่ง (ไม่มีระบบเตือน/ขาดการอบรม)

แนวทางแก้ไขระยะยาว:

- รวม “มาตรฐานการส่งข้อมูล” เป็นส่วนหนึ่งของคู่มือ onboarding
- สร้างระบบแสดงแจ้งเตือนเมื่อแนบไฟล์ .xls/.pdf อัตโนมัติ
- ทบทวน Risk Register และเพิ่มรายการความเสี่ยงใหม่
- บทเรียนสำหรับหน่วยงานอื่น: ทุกหน่วยที่ส่งข้อมูลลูกค้าควรใช้ระบบเตือนก่อนส่งเช่นเดียวกัน
- การเปลี่ยนแปลงเชิงระบบ: เพิ่มเงื่อนไขระบบ email outbound gateway

สภาพบังคับตามกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37: ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการมาตรการที่เหมาะสมเพื่อป้องกันการรั่วไหลหรือเข้าถึงข้อมูลโดยไม่ชอบ
- ประกาศคณะกรรมการฯ พ.ศ. 2565 ข้อ 5: ให้มีการจัดทำแผน บันทึกรายการ และประเมินผลของมาตรการด้านความมั่นคงปลอดภัย
- โทษทางปกครอง: ปรับไม่เกิน 3 ล้านบาท หากละเลยการดำเนินการตามมาตรา 37

แผนปฏิบัติการ รายงานความคืบหน้า และบทเรียนที่ได้รับ เพื่อหลีกเลี่ยงความเสี่ยงด้านข้อมูลส่วนบุคคลในอนาคต

เอกสารหลักฐานตามข้อ 8.1.3: การบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล

1. นโยบายการบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล

ชื่อเอกสาร: นโยบายการบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล ฉบับที่ 1/2566

สาระสำคัญ:

- องค์กรกำหนดให้มีการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลอย่างสม่ำเสมอ (รายไตรมาส หรือ เมื่อมีเหตุการณ์สำคัญ)
- ทุกความเสี่ยงต้องได้รับการจัดทำแผนปฏิบัติการลดผลกระทบ (Mitigation Plan)
- หน่วยงาน Data Protection Office (DPO) หรือหน่วยงานกำกับดูแลข้อมูลมีหน้าที่ติดตามและสรุปผลความคืบหน้าเป็นรายเดือน
- องค์กรมีระบบ “บทเรียนจากเหตุการณ์” (Lessons Learned Register) เพื่อนำความรู้ไปใช้พัฒนาแนวทางป้องกันในอนาคต

2. ตัวอย่างทะเบียนระบุความเสี่ยง และแผนปฏิบัติการ (Risk & Mitigation Action Register)

ชื่อเอกสาร: ทะเบียนการบริหารความเสี่ยงด้านข้อมูลส่วนบุคคล ณ ไตรมาส 1/2567

ลำดับ	รายละเอียดความเสี่ยง	ระดับความเสี่ยง	แผนปฏิบัติการ	หน่วยงานรับผิดชอบ	กำหนดเสร็จ	สถานะ
1	การเข้าถึงฐานข้อมูลพนักงานโดยไม่มีการควบคุมที่เพียงพอ	สูง	ปรับสิทธิ์การเข้าถึงในระบบ HR	ฝ่าย IT / HR	มี.ค. 2567	เสร็จสมบูรณ์
2	ความล่าช้าในการแจ้งเหตุข้อมูลรั่วไหล	ปานกลาง	จัดทำแบบฟอร์มแจ้งเหตุเร่งด่วน	DPO / ฝ่ายกฎหมาย	เม.ย. 2567	ดำเนินการ

3. รายงานความคืบหน้าการดำเนินการตามแผนปฏิบัติการ

ชื่อเอกสาร: รายงานความคืบหน้าในการบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล ประจำไตรมาส 1/2567

สาระสำคัญ:

- สถานะการดำเนินการครบ 80% ของแผนที่กำหนดไว้
- มีเหตุการณ์ความเสี่ยงใหม่ 1 กรณี เพิ่มเข้าสู่ทะเบียน
- มีการฝึกอบรมเจ้าหน้าที่ใหม่เกี่ยวกับวิธีรายงานเหตุข้อมูลรั่วไหลจำนวน 25 คน

4. รายงานบทเรียนที่ได้รับ (Lessons Learned Report)

ชื่อเอกสาร: รายงานบทเรียนที่ได้รับจากการบริหารความเสี่ยงด้านข้อมูลส่วนบุคคล (Q1/2567)

ตัวอย่าง:

- เหตุการณ์: เจ้าหน้าที่ใหม่เข้าถึงข้อมูลพนักงานโดยไม่รู้ข้อจำกัด
- บทเรียน: ระบบยังไม่มีระบบแจ้งเตือนหรือ onboarding เรื่องสิทธิการเข้าถึง
- แนวทางปรับปรุง: เพิ่ม session onboarding เรื่องสิทธิข้อมูลในการอบรมพนักงานใหม่

5. แบบฟอร์มประกอบการติดตามและประเมินผล

- แบบฟอร์มติดตามแผนปฏิบัติการลดความเสี่ยง (Risk Mitigation Action Follow-up Form)
- แบบฟอร์มรายงานเหตุการณ์ความเสี่ยงด้านข้อมูลส่วนบุคคล (Data Incident Reporting Form)
- แบบฟอร์มประเมินผลหลังเหตุการณ์ (Post-Incident Evaluation Form)

8.1.4 นโยบายความเสี่ยงด้านข้อมูลส่วนบุคคลจัดทำเป็นเอกสารแยกต่างหากหรือเป็นส่วนหนึ่งของนโยบายความเสี่ยงระดับองค์กร และมีแนวปฏิบัติหรือขั้นตอนซึ่งกำหนดวิธีที่องค์กรและผู้ประมวลผลข้อมูลส่วนบุคคลขององค์กรจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล และมีวิธีที่องค์กรติดตามการปฏิบัติตามนโยบายความเสี่ยงด้านข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: องค์กรมีนโยบายความเสี่ยงด้านข้อมูลส่วนบุคคล แนวปฏิบัติหรือขั้นตอนกำหนดวิธีจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล และมีวิธีที่องค์กรติดตามการปฏิบัติตามนโยบายดังกล่าว

หลักฐาน: นโยบายความเสี่ยงด้านข้อมูลส่วนบุคคล

บันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA)

เอกสารรายการตรวจประเมินความเสี่ยงด้านความปลอดภัยในการบริหารจัดการข้อมูลส่วนบุคคล (Data Security Compliance Checklist: DSC Checklist)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารหลักฐานที่แสดงว่าองค์กรมีนโยบายความเสี่ยงด้านข้อมูลส่วนบุคคล พร้อมแนวปฏิบัติ วิธีการติดตาม และแบบฟอร์มประกอบ

1. นโยบายความเสี่ยงด้านข้อมูลส่วนบุคคล (Personal Data Risk Management Policy)

ชื่อเอกสาร: นโยบายการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล ฉบับที่ 1/2567

สาระสำคัญของเอกสาร:

จุดประสงค์: เพื่อระบุ ประเมิน และจัดการความเสี่ยงที่เกิดจากการประมวลผลข้อมูลส่วนบุคคล

ขอบเขต: ครอบคลุมทุกหน่วยงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

ความสัมพันธ์: นโยบายฉบับนี้เป็นภาคผนวกของนโยบายการจัดการความเสี่ยงระดับองค์กร

หน้าที่รับผิดชอบ:

- หน่วยงานเจ้าของระบบ/เจ้าของกระบวนการ

- DPO/คณะกรรมการคุ้มครองข้อมูล
- ฝ่ายตรวจสอบภายใน

วิธีติดตาม: ประเมินผลความเสี่ยงรายไตรมาส และตรวจสอบเอกสาร ROPA Checklist และการดำเนินการจริงทุก 6 เดือน

2. แนวปฏิบัติการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล (Personal Data Risk Procedures)

ชื่อเอกสาร: ขั้นตอนการระบุและจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล

เนื้อหา:

การระบุความเสี่ยง:

ระบุโดยใช้ Data Mapping และบันทึกลงใน ROPA

การประเมินความเสี่ยง:

- ใช้เกณฑ์ระดับความรุนแรง/ความน่าจะเป็น (เช่น Low/Medium/High)
- มีแบบฟอร์ม Risk Assessment Template

การจัดการความเสี่ยง:

- แผนลดความเสี่ยง (Risk Mitigation Plan)
- การมอบหมายผู้รับผิดชอบ

การติดตามผล:

- DPO ตรวจสอบร่วมกับฝ่ายตรวจสอบภายใน
- รายงานความคืบหน้าและปรับปรุงแผนทุกไตรมาส

3. บันทึกการของกิจกรรมการประมวลผล (Record of Processing Activities – ROPA)

ชื่อเอกสาร: ROPA – เวอร์ชันปรับปรุงล่าสุด ณ วันที่ 1 มิถุนายน 2567

ตัวอย่างข้อมูลในเอกสาร

ลำดับ	กระบวนการ	ประเภทข้อมูล	เจ้าของข้อมูล	ความเสี่ยงที่เกี่ยวข้อง	มาตรการลดความเสี่ยง
1	บันทึกข้อมูลพนักงาน	ข้อมูลระบุตัวตน	ฝ่าย HR	การเข้าถึงโดยไม่ได้รับอนุญาต	RBAC M A
2	การสมัครงานออนไลน์	ข้อมูลอ่อนไหว	ฝ่ายทรัพยากรบุคคล	การรั่วไหลจาก third-party	Encryption DPIA

4. รายการตรวจประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลส่วนบุคคล (Data Security Compliance Checklist – DSC Checklist)

ชื่อเอกสาร: แบบตรวจประเมินความปลอดภัยข้อมูลส่วนบุคคล ฉบับเดือนพฤษภาคม 2567

หมวดหมู่และตัวอย่างคำถาม:

หมวด: สิทธิการเข้าถึง

- มีการจำกัดสิทธิการเข้าถึงตามหน้าที่งานหรือไม่?
- ระบบมีการตรวจสอบประวัติการเข้าถึงหรือไม่?

หมวด: การส่งข้อมูล

- ข้อมูลส่วนบุคคลถูกเข้ารหัสขณะส่งหรือไม่?
- มีการบันทึก log การส่งข้อมูลหรือไม่?

หมวด: ผู้ประมวลผลข้อมูล (Data Processors)

- ผู้ประมวลผลมีสัญญา Data Processing Agreement หรือไม่?
- ผู้ประมวลผลมีรายงานการตรวจสอบมาตรฐานการด้านความปลอดภัยหรือไม่? *อยู่ระหว่างการดำเนินการ*

รวมคะแนน: 18/20 (ผ่านเกณฑ์)

5. วิธีติดตามการปฏิบัติตามนโยบาย

- มีการจัดประชุมความคืบหน้า (Risk Compliance Meeting) ทุกไตรมาส
- Audit Checkpoint โดยฝ่ายตรวจสอบภายใน ปีละ 1 ครั้ง
- จัดทำ “รายงานสรุปความเสี่ยงประจำปี” พร้อมบทเรียนที่ได้รับ

8.1.5 องค์กรมีขั้นตอนอย่างเป็นทางการ (Formal Procedures) ในการระบุ บันทึก และจัดการความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินสารสนเทศในทะเบียนควบคุมทรัพย์สินสารสนเทศ (An Information Asset Register)

สิ่งที่ต้องทำ: องค์กรมีขั้นตอนอย่างเป็นทางการในการระบุ บันทึก และจัดการความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินสารสนเทศในทะเบียนควบคุมทรัพย์สินสารสนเทศอย่างชัดเจนและครบถ้วน

หลักฐาน: นโยบายในการกำหนดขั้นตอนการระบุ บันทึก และจัดการความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินสารสนเทศในทะเบียนควบคุมทรัพย์สินสารสนเทศ ทะเบียนควบคุมทรัพย์สินสารสนเทศ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารหลักฐานอย่างละเอียด ซึ่งแสดงว่าองค์กรมี “ขั้นตอนอย่างเป็นทางการในการระบุ บันทึก และจัดการความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินสารสนเทศ” พร้อมตัวอย่างนโยบาย และทะเบียนควบคุมทรัพย์สินสารสนเทศที่สามารถนำไปใช้งานหรืออ้างอิงได้

หัวข้อ: องค์กรมีขั้นตอนอย่างเป็นทางการในการระบุ บันทึก และจัดการความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินสารสนเทศในทะเบียนควบคุมทรัพย์สินสารสนเทศ

1. นโยบายการจัดการทะเบียนควบคุมทรัพย์สินสารสนเทศ

ชื่อเอกสาร: นโยบายการควบคุมทรัพย์สินสารสนเทศ (Information Asset Management Policy)

สาระสำคัญ:

วัตถุประสงค์: เพื่อระบุ บันทึก และบริหารความเสี่ยงของทรัพย์สินสารสนเทศขององค์กรอย่างมีประสิทธิภาพ

ขอบเขต: ครอบคลุมทรัพย์สินทุกประเภท เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล เครือข่าย เอกสาร และข้อมูลส่วนบุคคล

นิยาม:

- **Information Asset:** ทรัพยากรที่มีมูลค่าเชิงสารสนเทศและต้องได้รับการคุ้มครอง
- **Asset Owner:** ผู้มีหน้าที่กำกับดูแลความปลอดภัยและการใช้งานของทรัพย์สิน
- **ความถี่ในการทบทวน:** อย่างน้อยปีละ 1 ครั้ง

ผู้รับผิดชอบ:

- เจ้าของทรัพย์สิน (Asset Owner)
- คณะกรรมการเทคโนโลยีสารสนเทศ
- DPO

2. ขั้นตอนในการระบุ บันทึก และจัดการความเสี่ยงของทรัพย์สินสารสนเทศ

ชื่อเอกสาร: ขั้นตอนการจัดทำทะเบียนควบคุมทรัพย์สินสารสนเทศ

สาระสำคัญ:

ขั้นตอนที่ 1: ระบุทรัพย์สิน

แยกตามหมวดหมู่

- ฮาร์ดแวร์ (เช่น Server PC Mobile)
- ซอฟต์แวร์ (เช่น ERP HRMS)
- ข้อมูล (Database Personal Data Files)
- บริการ Cloud/เครือข่าย

ขั้นตอนที่ 2: ประเมินมูลค่าและความเสี่ยง

- กำหนดความสำคัญ (Criticality)
- ประเมินความเสี่ยง:
- ความเป็นไปได้ (Likelihood)
- ผลกระทบ (Impact)
- ระดับความเสี่ยง (Low / Medium / High)

ขั้นตอนที่ 3: บันทึกในทะเบียนควบคุมทรัพย์สินสารสนเทศ

ใช้ฟอร์มที่มีช่องบันทึกผู้รับผิดชอบ มาตรการควบคุม และประวัติการตรวจสอบ

ขั้นตอนที่ 4: การจัดการและทบทวน

- ทบทวนรายการทรัพย์สินอย่างน้อยปีละ 1 ครั้ง
- หากมีเหตุการณ์ความเสี่ยง ต้องปรับปรุงทะเบียนทันที

3. ตัวอย่างทะเบียนควบคุมทรัพย์สินสารสนเทศ (Information Asset Register)

ชื่อเอกสาร: ทะเบียนควบคุมทรัพย์สินสารสนเทศ ประจำปี 2567

ลำดับ	ประเภททรัพย์สิน	รายละเอียด	เจ้าของทรัพย์สิน	ระดับความเสี่ยง	มาตรการควบคุม
1	ฐานข้อมูลพนักงาน	ฐานข้อมูลที่เก็บข้อมูลส่วนบุคคลของพนักงาน	HR Manager	สูง	Access Control Encryption
2	Server ERP	เซิร์ฟเวอร์ระบบ ERP ภายในองค์กร	IT Manager	กลาง	Firewall Physical Security
3	Google Workspace	บริการ Cloud ใช้งานอีเมล	DPO	กลาง	MFA Data Loss Prevention
4	แฟ้มเอกสารประวัติลูกค้า	ข้อมูลออฟไลน์ที่เก็บไว้ในตู้เซิร์ฟเวอร์	ผู้จัดการสาขา	สูง	CCTV ล็อค 2 ชั้น

4. แนวปฏิบัติเสริม (ตามมาตรฐาน ISO 27001 และ PDPA)

การจำแนกทรัพย์สิน (Asset Classification):

Confidential / Internal Use / Public

การมอบหมายความรับผิดชอบ (Ownership):

เจ้าของต้องรับผิดชอบการบำรุงรักษาและควบคุมความเสี่ยง

การจัดทำรายการสำรอง (Backup):

ข้อมูลสำคัญต้องมีการ Backup และเก็บไว้นอกสถานที่

การบันทึกเหตุการณ์ผิดปกติ (Security Incident Log):

ทุกเหตุการณ์ที่มีความเสี่ยงจะถูกบันทึกและวิเคราะห์

8.1.6 องค์กรมีมาตรการเพื่อลดความเสี่ยงที่ระบุในประเภทความเสี่ยง (Risk Categories) และองค์กรทดสอบมาตรการเหล่านี้เป็นประจำเพื่อให้แน่ใจว่ายังคงมีประสิทธิภาพ

สิ่งที่ต้องทำ: องค์กรมีมาตรการเพื่อลดความเสี่ยงที่ระบุในประเภทความเสี่ยง และมีการทดสอบประสิทธิภาพของมาตรการเป็นประจำ

หลักฐาน: นโยบายในการทดสอบมาตรการเพื่อลดความเสี่ยงที่ระบุในประเภทความเสี่ยง

รายงานผลการทดสอบมาตรการดังกล่าว

สภาพบังคับ: กฎหมายไม่ได้กำหนด

มาตรการเพื่อลดความเสี่ยงที่ระบุในประเภทความเสี่ยง (Risk Categories) และการทดสอบประสิทธิภาพของมาตรการเหล่านี้อย่างสม่ำเสมอ ซึ่งสามารถใช้เป็นหลักฐานเพื่อการตรวจประเมินตาม PDPA หรือกรอบควบคุมความเสี่ยงภายในองค์กร

หัวข้อ: องค์กรมีมาตรการเพื่อลดความเสี่ยงที่ระบุในประเภทความเสี่ยง และมีการทดสอบประสิทธิภาพของมาตรการอย่างสม่ำเสมอ

1. นโยบายการทดสอบมาตรการควบคุมความเสี่ยง (Policy on Risk Control Testing)

ชื่อเอกสาร: นโยบายการทดสอบและประเมินประสิทธิภาพของมาตรการควบคุมความเสี่ยงด้านข้อมูลส่วนบุคคล

วัตถุประสงค์:

- เพื่อกำหนดแนวทางในการทดสอบและตรวจสอบว่ามาตรการควบคุมที่ใช้งานอยู่มีประสิทธิภาพต่อเนื่อง
- สร้างความมั่นใจว่าองค์กรสามารถลดผลกระทบจากความเสี่ยงที่ระบุไว้ใน Risk Register ได้จริง

ขอบเขต:

ครอบคลุมมาตรการใน Risk Categories ดังนี้

- ความเสี่ยงด้านการเข้าถึงโดยไม่ได้รับอนุญาต
- ความเสี่ยงด้านการรั่วไหลของข้อมูล
- ความเสี่ยงจากความล้มเหลวของระบบเทคโนโลยี
- ความเสี่ยงด้านความผิดพลาดจากบุคลากร
- ความเสี่ยงด้านบุคคลภายนอกหรือผู้ให้บริการ (Third-party risk)

แนวปฏิบัติหลัก:

- กำหนดมาตรการควบคุมที่เฉพาะเจาะจง เช่น MFA DLP Access Logging การเข้ารหัส บันทึก log
- ทดสอบทุก 6 เดือน หรือตามระดับความเสี่ยงที่กำหนดไว้ในทะเบียน
- ใช้เทคนิคการทดสอบ เช่น Penetration Testing Simulation Test Table-top Exercise

บทบาทและความรับผิดชอบ:

- DPO และแผนก IT Security รับผิดชอบร่วมกัน
- ผู้จัดการแผนกประสานงานเพื่อจัดตารางทดสอบ

2. รายงานผลการทดสอบมาตรการลดความเสี่ยง (Risk Control Effectiveness Test Report)

ชื่อเอกสาร: รายงานการทดสอบมาตรการควบคุมความเสี่ยง – ครึ่งปีแรก พ.ศ. 2567

ตารางสรุปผลการทดสอบ (ตัวอย่าง)

ประเภทความเสี่ยง	มาตรการควบคุม	ผลการทดสอบ	สรุปผล	ข้อเสนอแนะ
การเข้าถึงโดยไม่ได้รับอนุญาต	MFA สำหรับระบบภายใน	ทดสอบผ่าน – ผู้ใช้ไม่สามารถข้าม MFA ได้	มีประสิทธิภาพ	ปรับปรุง UX เพื่อป้องกันหลีกเลี่ยงการใช้งานภายนอกระบบ
การรั่วไหลข้อมูล	การใช้ DLP บน Google Workspace	พบการแจ้งเตือนถูกส่งเมื่อมีความพยายามแนบไฟล์ข้อมูลส่วนบุคคล	มีประสิทธิภาพ	เพิ่มคำหลักใหม่สำหรับตรวจจับไฟล์สแกน PDF
ความเสี่ยงจากบุคลากร	การอบรม Awareness และ Phishing Simulation	89% ไม่คลิกลิงก์ปลอม	มีประสิทธิภาพ แต่ยังมีช่องโหว่	เพิ่มความถี่การฝึกอบรมต่อกลุ่มเสี่ยง
ความเสี่ยงจาก third-party	ตรวจสอบผู้ให้บริการผ่าน Vendor Risk Checklist	2 รายไม่ส่งแบบประเมินตามรอบ	ต้องติดตามเพิ่มเติม	แจ้งเตือนและพิจารณาจัดอบรมสำหรับ vendor

3. แนวทางในการปรับปรุงมาตรการหลังการทดสอบ

- หากผลการทดสอบพบจุดอ่อน ให้มี Action Plan ภายใน 30 วัน
- DPO จัดทำรายงานผลและข้อเสนอแนะเสนอต่อคณะกรรมการบริหารความเสี่ยง
- แผนปรับปรุงต้องเข้าสู่ทะเบียน Risk Register และจัดทำรายงานความคืบหน้า (ตามข้อ 8.1.3)

4. วิธีการติดตามและประเมินผลอย่างต่อเนื่อง

- มีการกำหนด KPI ว่ามาตรการควบคุมต้องมีประสิทธิภาพขั้นต่ำ 80%
- รายงานผลต่อที่ประชุมฝ่ายบริหารความเสี่ยงทุก 6 เดือน
- มีการเก็บ Log Audit Trail และบันทึกผลการทดสอบลงในระบบขององค์กร

8.2 องค์กรปกป้องข้อมูลโดยการออกแบบและกำหนดเป็นค่าเริ่มต้น (Data protection by design and by default) องค์กรใช้การปกป้องข้อมูลโดยการออกแบบและกำหนดเป็นค่าเริ่มต้นในการจัดการความเสี่ยง และกำหนดนโยบายและขั้นตอนให้มีการจัดทำ DPIA ตามความเหมาะสมและปัจจัยความเสี่ยง

8.2.1 องค์กรกำหนดให้มีการทำ DPIA ตั้งแต่เริ่มต้นของโครงการ ก่อนที่การประมวลผลข้อมูลส่วนบุคคลจะเริ่มต้น และ DPIA จะต้องดำเนินการควบคู่ไปกับกระบวนการวางแผนและการพัฒนา สิ่งที่ต้องทำ: องค์กรกำหนดให้มีการทำ DPIA ตั้งแต่ก่อนที่การประมวลผลข้อมูลส่วนบุคคลจะเริ่มต้น และมีการดำเนินการควบคู่ไปกับกระบวนการวางแผนและพัฒนา หลักฐาน: นโยบายการจัดทำการประเมินความเสี่ยงของโครงการ หนังสือรับรองรายงานผลการประเมินความเสี่ยง สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารหลักฐาน: รายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment - DPIA)

โครงการ: ระบบบริหารจัดการข้อมูลผู้รับบริการในหน่วยงานของรัฐ

หน่วยงานที่รับผิดชอบ: กองเทคโนโลยีสารสนเทศ สำนักนโยบายและแผน

1. บทนำ

เพื่อให้เป็นไปตามแนวทางการปกป้องข้อมูลโดยการออกแบบและการกำหนดเป็นค่าเริ่มต้น (Data Protection by Design and by Default) หน่วยงานได้จัดให้มีการจัดทำรายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ตั้งแต่ระยะเริ่มต้นของการออกแบบโครงการ และดำเนินการประเมินควบคู่ไปกับกระบวนการวางแผนและพัฒนาโครงการ เพื่อระบุ วิเคราะห์ และบริหารความเสี่ยงที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

2. วัตถุประสงค์ของโครงการ

วัตถุประสงค์ของการดำเนินโครงการนี้ คือการพัฒนาและปรับปรุงระบบฐานข้อมูลกลาง เพื่อรองรับการให้บริการประชาชน โดยมีการจัดเก็บข้อมูลส่วนบุคคล อาทิ ชื่อ-สกุล หมายเลขประจำตัวประชาชน ที่อยู่ ข้อมูลสุขภาพ และข้อมูลการขอรับบริการจากหน่วยงานของรัฐ

3. ลักษณะของข้อมูลที่เกี่ยวข้อง

- ข้อมูลประจำตัว (เช่น ชื่อ-นามสกุล หมายเลขบัตรประชาชน)
- ข้อมูลติดต่อ (เช่น ที่อยู่ หมายเลขโทรศัพท์ อีเมล)
- ข้อมูลอ่อนไหว (เช่น ข้อมูลสุขภาพ)
- ข้อมูลประวัติการรับบริการจากหน่วยงาน

4. การวิเคราะห์ผลกระทบ

การวิเคราะห์ได้ระบุถึงความเสี่ยงหลักที่อาจส่งผลกระทบต่อเจ้าของข้อมูล ดังนี้

ความเสี่ยง	ผลกระทบ	ความรุนแรง	ความน่าจะเป็น	มาตรการบรรเทา
การเข้าถึงโดยไม่ได้รับอนุญาต	เปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ	สูง	ปานกลาง	การใช้ระบบยืนยันตัวตน 2 ชั้น การเข้ารหัสข้อมูล
การจัดเก็บเกินระยะเวลาที่จำเป็น	ความเสี่ยงต่อการรั่วไหลในอนาคต	ปานกลาง	สูง	การกำหนดระยะเวลาการจัดเก็บและลบอัตโนมัติ
การส่งข้อมูลไปยังบุคคลภายนอก	สูญเสียการควบคุมข้อมูล	สูง	ต่ำ	การจัดทำสัญญาประมวลผลข้อมูล (Data Processing Agreement)

5. แนวทางการบูรณาการ DPIA เข้ากับกระบวนการวางแผน

หน่วยงานได้บูรณาการการประเมิน DPIA ไว้ในขั้นตอนต่อไปนี้:

- ระยะเริ่มต้น: วิเคราะห์ความจำเป็นในการเก็บข้อมูลส่วนบุคคล
- ระยะออกแบบ: การประเมินทางเลือกในการจัดเก็บข้อมูลให้น้อยที่สุดเท่าที่จำเป็น
- ระยะพัฒนา: ตรวจสอบระบบรักษาความมั่นคงปลอดภัยของข้อมูล
- ระยะทดลองใช้: ทบทวนและปรับปรุงตามข้อเสนอแนะจากการประเมินผลเบื้องต้น

6. สรุปและข้อเสนอแนะ

จากการประเมินพบว่า โครงการมีความเสี่ยงในระดับ “ปานกลางถึงสูง” จึงเสนอให้มีการดำเนินมาตรการบรรเทาความเสี่ยงเชิงรุกในทุกระยะ และมีการติดตามประเมินผลซ้ำเมื่อมีการเปลี่ยนแปลงวิธีการประมวลผลหรือจุดประสงค์ของการเก็บข้อมูล

ผู้จัดทำรายงาน:

นายณรงค์เดช อินทรวัฒน์

ตำแหน่ง: เจ้าหน้าที่วิเคราะห์นโยบายและแผนชำนาญการ

สังกัด: กองเทคโนโลยีสารสนเทศ

วัน/เดือน/ปี ที่จัดทำรายงาน: 4 มิถุนายน 2568

8.2.2 องค์กรอ้างอิง DPIA ในนโยบายและขั้นตอนการจัดการความเสี่ยง โครงการ และนโยบายการบริหารจัดการการเปลี่ยนแปลงทั้งหมด พร้อมทั้งเชื่อมโยงไปยังนโยบายและขั้นตอนตาม DPIA

สิ่งที่ต้องทำ: องค์กรมีการอ้างอิง DPIA ในนโยบายและขั้นตอนการจัดการความเสี่ยง โครงการ และนโยบายการบริหารจัดการการเปลี่ยนแปลงทั้งหมด พร้อมทั้งเชื่อมโยงไปยังนโยบายและขั้นตอนตาม DPIA รวมถึงมีเอกสารครบถ้วน

หลักฐาน: 1.นโยบายการนำการประเมินความเสี่ยงไปเชื่อมโยงในการจัดทำโครงการต่าง ๆ ภายในองค์กร
2.ทะเบียนจัดการความเสี่ยง
3.รายงานผลการประเมินความเสี่ยงจากบุคลากรที่เกี่ยวข้อง
4.หนังสือรับรองรายงานผลการประเมินความเสี่ยง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารหลักฐาน: นโยบายและขั้นตอนการเชื่อมโยงการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) กับกระบวนการบริหารความเสี่ยง โครงการ และการเปลี่ยนแปลงภายในองค์กร

ชื่อเอกสาร: นโยบายการเชื่อมโยงการประเมินความเสี่ยงจาก DPIA กับการดำเนินโครงการและการบริหารความเปลี่ยนแปลงภายในหน่วยงาน

หน่วยงาน: สำนักแผนงานและพัฒนาองค์กร

วัน/เดือน/ปี ที่จัดทำ: 4 มิถุนายน 2568

1. วัตถุประสงค์

เพื่อให้กระบวนการบริหารความเสี่ยงและการดำเนินโครงการต่าง ๆ ภายในหน่วยงานมีความสอดคล้องกับแนวทางการคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะการใช้การประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA) เป็นกลไกในการป้องกันความเสี่ยงและกำกับดูแลอย่างรัดกุม จึงได้จัดทำนโยบายฉบับนี้เพื่อกำหนดแนวทางและขั้นตอนที่ชัดเจนสำหรับการอ้างอิงและเชื่อมโยง DPIA เข้ากับระบบบริหารความเสี่ยงและการเปลี่ยนแปลงภายในองค์กร

2. ขอบเขตการบังคับใช้

นโยบายฉบับนี้มีผลบังคับใช้กับโครงการทั้งหมดของหน่วยงานที่มีการจัดเก็บ ใช้ เปิดเผย หรือโอนข้อมูลส่วนบุคคล ไม่ว่าจะดำเนินการโดยตรงโดยหน่วยงานหรือโดยผู้ประมวลผลภายนอก รวมถึงการเปลี่ยนแปลงระบบ เทคโนโลยี กระบวนการทำงาน หรือการจัดเก็บข้อมูลที่มีผลกระทบต่อเจ้าของข้อมูล

3. หลักการดำเนินงาน

1. โครงการหรือการเปลี่ยนแปลงใด ๆ ที่อาจมีผลต่อข้อมูลส่วนบุคคล ต้องดำเนินการประเมิน DPIA ในระยะต้นของการวางแผน
2. การประเมิน DPIA ต้องถูกอ้างอิงในทะเบียนบริหารความเสี่ยงประจำปี และแนบรายงานผลการประเมินไว้เป็นเอกสารประกอบ
3. การดำเนินโครงการใด ๆ ต้องแสดงหลักฐานว่าได้ตรวจสอบความเสี่ยงด้านข้อมูลส่วนบุคคลโดยใช้ DPIA ก่อนการอนุมัติแผน
4. การเปลี่ยนแปลงระบบงานหรือขั้นตอนการประมวลผลข้อมูลต้องมีการประเมินผลกระทบใหม่ (DPIA ฉบับปรับปรุง) หากเกิดความเสี่ยงใหม่ที่ไม่ได้ครอบคลุมใน DPIA เดิม
5. เอกสาร DPIA ที่จัดทำต้องเชื่อมโยงกับนโยบายและระเบียบภายใน เช่น ระเบียบการจัดการข้อมูลส่วนบุคคล ระเบียบการจัดซื้อจัดจ้าง และคู่มือการปฏิบัติงานของแต่ละแผน

4. เอกสารอ้างอิง

ทะเบียนบริหารความเสี่ยงประจำปี 2568

หมายเหตุ: มีระเบียบอ้างอิงโครงการที่ทำ DPIA ไว้อย่างครบถ้วน พร้อมระบุระดับความเสี่ยงที่ประเมินแล้ว
รายงานผลการประเมินความเสี่ยง

จัดทำโดยเจ้าหน้าที่ความมั่นคงสารสนเทศและฝ่ายกฎหมาย

หนังสือรับรองรายงานผลการประเมินความเสี่ยง

ลงนามโดยผู้อำนวยการฝ่ายบริหารองค์กร

คู่มือการดำเนินการตาม DPIA (เวอร์ชันปรับปรุง)

แนบไว้ในระบบงานภายใน (Intranet) พร้อม Link จากหน้าแผนโครงการและระบบติดตามความก้าวหน้า

5. สรุปข้อกำหนดตามนโยบาย

กระบวนการ	ต้องดำเนินการ	เอกสารที่เกี่ยวข้อง
การวางแผนโครงการใหม่	ทำ DPIA และอ้างอิงในแผน	แบบฟอร์มแผนโครงการ รายงาน DPIA
การเปลี่ยนแปลงระบบงาน	ตรวจสอบผลกระทบใหม่	รายงาน DPIA ฉบับปรับปรุง
การติดตามความเสี่ยง	ลงทะเบียนในระบบบริหารความเสี่ยง	ทะเบียนความเสี่ยงประจำปี
การรายงานผู้บริหาร	แนบสรุป DPIA ในรายงานประจำไตรมาส	หนังสือสรุปผลความเสี่ยง

6. ผู้รับผิดชอบและการติดตาม

หน่วยงานที่รับผิดชอบการดำเนินงานตามนโยบายนี้คือ:

- ฝ่ายบริหารความเสี่ยง

- ฝ่ายกฎหมาย
- ฝ่ายเทคโนโลยีสารสนเทศ
- ฝ่ายตรวจสอบภายในจะดำเนินการตรวจติดตามประจำปี เพื่อประเมินความครบถ้วนของการเชื่อมโยง DPIA เข้ากับโครงการและระบบงานต่าง ๆ

ลงชื่อ:

นายวรพจน์ ทศพร

หัวหน้ากลุ่มงานพัฒนาระบบและมาตรฐานองค์กร

ลงนามเมื่อ: 4 มิถุนายน 2568

8.2.3 องค์กรมีการคาดการณ์ถึงความเสี่ยงและเหตุการณ์ที่อาจรุกร้าความเป็นส่วนตัวก่อนที่จะเกิดขึ้น ในขั้นตอนการออกแบบเริ่มต้นของระบบ ผลิตภัณฑ์ หรือกระบวนการใด ๆ และตลอดทั้งระบบ องค์กรจะพิจารณาถึง

1. กิจกรรมการประมวลผลที่จะดำเนินการ
2. ความเสี่ยงที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของบุคคล
3. มาตรการที่เป็นไปได้เพื่อลดความเสี่ยงดังกล่าว
4. สิ่งที่ต้องทำ: องค์กรมีการคาดการณ์ถึงความเสี่ยงและเหตุการณ์ที่อาจรุกร้าความเป็นส่วนตัว ในขั้นตอนการออกแบบเริ่มต้นของระบบ ผลิตภัณฑ์ หรือกระบวนการใด ๆ และตลอดทั้งระบบ และองค์กรพิจารณาถึง
5. กิจกรรมการประมวลผลที่จะดำเนินการ
6. ความเสี่ยงที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของบุคคล
7. มาตรการที่เป็นไปได้เพื่อลดความเสี่ยงดังกล่าวอย่างครบถ้วน

หลักฐาน: นโยบายการประเมินความเสี่ยงของเหตุการณ์ที่อาจรุกร้าความเป็นส่วนตัว ในขั้นตอนการออกแบบเริ่มต้นของระบบ ผลิตภัณฑ์ หรือกระบวนการ
ทะเบียนจัดการความเสี่ยง
มาตรการเชิงรุกในการคุ้มครองข้อมูลส่วนบุคคลในทางป้องกัน (Proactive and Preventive)
แบบฟอร์มการประเมินความเสี่ยง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารหลักฐาน: นโยบายการคาดการณ์และประเมินความเสี่ยงด้านความเป็นส่วนตัวในขั้นตอนการออกแบบระบบ ผลิตภัณฑ์ และกระบวนการ (Privacy Risk Forecast and Prevention Policy)

**ชื่อเอกสาร: นโยบายการประเมินและคาดการณ์ความเสี่ยงที่อาจรุกร้าความเป็นส่วนตัวในระยะเริ่มต้น
ของโครงการ**

หน่วยงาน: ฝ่ายบริหารความเสี่ยงและการออกแบบระบบ

วันที่จัดทำ: 4 มิถุนายน 2568

1. วัตถุประสงค์

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดแนวทางในการพิจารณาและคาดการณ์ถึงความเสี่ยงที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลในช่วงเริ่มต้นของการออกแบบระบบงานผลิตภัณฑ์ และกระบวนการใหม่ รวมถึงตลอดวัฏจักรการพัฒนาและใช้งานระบบ โดยมีวัตถุประสงค์เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างปลอดภัย โปร่งใส และลดโอกาสเกิดการละเมิดความเป็นส่วนตัวอย่างมีประสิทธิภาพ

2. ขอบเขตการบังคับใช้

นโยบายฉบับนี้ใช้กับการพัฒนาและปรับปรุงระบบ เทคโนโลยี กระบวนการ หรือผลิตภัณฑ์ใด ๆ ภายในหน่วยงานที่มีความเกี่ยวข้องกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งโดยตรงและโดยอ้อม รวมถึงการว่าจ้างผู้ให้บริการภายนอกที่มีการเข้าถึงหรือจัดการข้อมูลส่วนบุคคล

3. แนวทางการดำเนินงาน

การคาดการณ์กิจกรรมการประมวลผลที่จะเกิดขึ้น

- ผู้พัฒนาระบบต้องจัดทำแบบฟอร์มระบุลักษณะของกิจกรรมการประมวลผลข้อมูล เช่น การเก็บข้อมูลจากผู้ใช้ การส่งต่อไปยังบุคคลภายนอก การวิเคราะห์ข้อมูล ฯลฯ
- แบบฟอร์มดังกล่าวต้องส่งให้ฝ่ายบริหารความเสี่ยงพิจารณาร่วมก่อนเริ่มกระบวนการพัฒนา

การระบุความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

- วิเคราะห์ว่าข้อมูลที่จัดเก็บมีลักษณะใด เป็นข้อมูลทั่วไปหรือข้อมูลอ่อนไหว
- พิจารณาผลกระทบที่อาจเกิดขึ้น เช่น การตีตราทางสังคม ความเสียหายต่อชื่อเสียง ความไม่ปลอดภัยทางกายภาพ หรือการเลือกปฏิบัติ

การกำหนดมาตรการป้องกันเชิงรุก (Proactive and Preventive Measures)

- รวมถึงการใช้การปกปิดตัวตน (Pseudonymisation) การเข้ารหัส (Encryption) การจำกัดการเข้าถึง (Access Control) การอบรมผู้เกี่ยวข้อง และการตั้งค่าเริ่มต้นที่ปลอดภัย (Default Privacy Settings)

4. เอกสารประกอบตามนโยบาย

ทะเบียนจัดการความเสี่ยงประจำโครงการ

มีการลงรายละเอียดของกิจกรรมการประมวลผลและผลกระทบที่คาดการณ์ไว้ในแต่ละโครงการพร้อมลำดับความเสี่ยง

มาตรการเชิงรุกในการป้องกันความเสี่ยง

ระบุมมาตรการเทคนิคและมาตรการองค์กร (Technical and Organizational Measures) ที่นำมาใช้ในระบบ เช่น การควบคุมสิทธิ์ของผู้ใช้งาน การแจ้งเตือนการรั่วไหลของข้อมูล

แบบฟอร์มการประเมินความเสี่ยง (Privacy Risk Assessment Form)

มีหัวข้อเกี่ยวกับลักษณะของกิจกรรมการประมวลผล ความอ่อนไหวของข้อมูล ระดับความน่าจะเป็นของเหตุการณ์รุกราน และระดับผลกระทบ

รายงานสรุปผลการวิเคราะห์ความเสี่ยง

จัดทำโดยฝ่ายเทคโนโลยีและฝ่ายกฎหมาย ก่อนการอนุมัติให้ดำเนินโครงการต่อไป

5. ขั้นตอนการประเมินความเสี่ยงล่วงหน้า

ขั้นตอน	รายละเอียด	ผู้รับผิดชอบ
1. แจ้งเริ่มต้นการออกแบบ	ทีมพัฒนาระบบแจ้งกิจกรรมประมวลผลที่คาดว่าจะเกิดขึ้น	หัวหน้าโครงการ
2. จัดทำแบบประเมินความเสี่ยง	กรอกแบบฟอร์ม Privacy Risk Assessment	ผู้พัฒนาระบบ + เจ้าหน้าที่คุ้มครองข้อมูล
3. วิเคราะห์และตรวจสอบร่วม	วิเคราะห์ผลกระทบและกำหนดมาตรการ	ฝ่ายบริหารความเสี่ยง
4. สรุปและเสนอผู้บริหาร	เสนอรายงานผลการคาดการณ์ความเสี่ยงเพื่ออนุมัติ	คณะกรรมการบริหารระบบ
5. ติดตามประเมินซ้ำหลังดำเนินการ	ทบทวนความเสี่ยงใหม่ (ถ้ามี)	ฝ่ายตรวจสอบภายใน

6. การติดตามและประเมินผล

หน่วยงานจะดำเนินการติดตามผลการประเมินล่วงหน้าเป็นประจำทุก 6 เดือน โดยเฉพาะโครงการที่มีลักษณะเปลี่ยนแปลงกระบวนการประมวลผลอย่างมีนัยสำคัญ โดยมีการจัดทำรายงานทบทวนความเสี่ยง และเสนอให้คณะกรรมการบริหารรับทราบ

ลงชื่อ

นางสาวจิราภรณ์ ศิริกุล

หัวหน้าฝ่ายบริหารความเสี่ยงและการออกแบบระบบ

ลงนามเมื่อ: 4 มิถุนายน 2568

8.3 นโยบายและขั้นตอน DPIA

องค์กรพิจารณาว่าจำเป็นต้องทำ DPIA หรือไม่ หรือจะเป็นแนวปฏิบัติที่ดีว่าควรทำ DPIA และองค์กรมีนโยบายและขั้นตอน DPIA ที่ชัดเจน

8.3.1 นโยบาย DPIA ควรรวมถึง

1. ขั้นตอนที่ชัดเจนในการตัดสินใจว่าต้องทำ DPIA หรือไม่
2. อะไรที่ DPIA ควรครอบคลุม
3. ใครจะเป็นผู้อนุมัติ
4. DPIA รวมเป็นส่วนหนึ่งของแผนการดำเนินการโดยรวมของโครงการนั้น ๆ

สิ่งที่ต้องทำ: องค์กรมีนโยบายการประเมินความเสี่ยงของข้อมูลส่วนบุคคล (DPIA) และมีรายละเอียดหรือขั้นตอนครบถ้วนตามที่กำหนด

หลักฐาน: นโยบายการประเมินความเสี่ยงของข้อมูลส่วนบุคคล
 รายงานการประเมินความเสี่ยงของข้อมูลส่วนบุคคล
 หนังสืออนุมัติรายงานการประเมินความเสี่ยงของข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

นโยบายการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA Policy)

คำประกาศนโยบาย

องค์กรตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และมุ่งมั่นปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และแนวทางสากลที่เกี่ยวข้อง เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างถูกต้อง โปร่งใส และปลอดภัย โดยได้กำหนดนโยบาย

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) เพื่อใช้เป็นกลไกสำคัญในการบริหารความเสี่ยงและคุ้มครองสิทธิของเจ้าของข้อมูล

1. วัตถุประสงค์

- 1.1 เพื่อกำหนดแนวทางปฏิบัติในการพิจารณาความจำเป็นในการจัดทำ DPIA
- 1.2 เพื่อระบุขอบเขตและสาระสำคัญของ DPIA ต้องครอบคลุม
- 1.3 เพื่อกำหนดบทบาทหน้าที่และผู้มีอำนาจอนุมัติ DPIA
- 1.4 เพื่อบูรณาการ DPIA เข้ากับกระบวนการดำเนินโครงการและการบริหารความเสี่ยงขององค์กร

2. ขั้นตอนการพิจารณาความจำเป็นในการทำ DPIA

- 2.1 ทุกโครงการ กิจกรรม หรือนโยบายใหม่ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ต้องได้รับการตรวจสอบเบื้องต้นเพื่อพิจารณาว่ามีความเสี่ยงสูงหรือไม่
- 2.2 เกณฑ์พิจารณาความเสี่ยงสูง ได้แก่
การประมวลผลข้อมูลส่วนบุคคลจำนวนมาก
การประมวลผลข้อมูลอ่อนไหว เช่น ข้อมูลสุขภาพ ความเชื่อ ศาสนา หรือข้อมูลชีวภาพ
การเฝ้าระวังหรือติดตามพฤติกรรมอย่างเป็นระบบ
การใช้เทคโนโลยีใหม่ที่มีผลกระทบต่อสิทธิของเจ้าของข้อมูล
การเชื่อมโยงข้อมูลจากหลายแหล่งจนสามารถระบุตัวบุคคลได้
- 2.3 หากเข้าข่าย ต้องจัดทำ DPIA โดยทันที หากไม่เข้าข่าย ต้องบันทึกเหตุผลเพื่อเก็บเป็นหลักฐาน

3. ขอบเขตและสาระสำคัญของ DPIA ต้องครอบคลุม

- 3.1 คำอธิบายเกี่ยวกับลักษณะ วัตถุประสงค์ และวิธีการประมวลผลข้อมูล
- 3.2 การประเมินความจำเป็นและความได้สัดส่วนของการประมวลผล
- 3.3 การวิเคราะห์และประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล
- 3.4 มาตรการทางเทคนิคและทางองค์กรเพื่อป้องกันและบรรเทาความเสี่ยง เช่น การเข้ารหัสข้อมูล การจำกัดสิทธิ์การเข้าถึง และการฝึกอบรมบุคลากร
- 3.5 ผลลัพธ์และข้อเสนอแนะในการลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

4. บทบาทหน้าที่และอำนาจการอนุมัติ

- 4.1 ผู้รับผิดชอบโครงการ (Project Owner/Manager): จัดทำ DPIA ตั้งแต่เริ่มต้น
- 4.2 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO): ตรวจสอบความครบถ้วนและให้คำแนะนำ
- 4.3 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขององค์กร หรือผู้บริหารสูงสุด: อนุมัติ DPIA ก่อนดำเนินโครงการ
- 4.4 หากยังมีความเสี่ยงสูงแม้มีมาตรการบรรเทา ต้องขอคำปรึกษาจากหน่วยงานกำกับดูแล (สคส.)

5. การบูรณาการ DPIA เข้ากับการดำเนินงาน

- 5.1 DPIA ต้องจัดทำและแล้วเสร็จก่อนการอนุมัติโครงการ
 - 5.2 ต้องมีการทบทวนและอัปเดต DPIA เมื่อมีการเปลี่ยนแปลงด้านเทคโนโลยีหรือวิธีการประมวลผล
 - 5.3 ต้องบันทึกและเก็บรักษาเอกสาร DPIA อย่างเป็นระบบ เพื่อสามารถแสดงต่อหน่วยงานกำกับดูแลได้
 - 5.4 ผลการประเมิน DPIA ต้องผนวกเข้ากับแผนการจัดการความเสี่ยงขององค์กร
- 6. ข้อกำหนดเพิ่มเติม**
- 6.1 DPIA เป็นส่วนหนึ่งของการปฏิบัติตามกฎหมายและมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล
 - 6.2 บุคลากรทุกระดับต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
 - 6.3 การละเมิดหรือฝ่าฝืนนโยบายนี้อาจถูกพิจารณาโทษทางวินัยหรือตามกฎหมาย

รายงานการประเมินความเสี่ยงของข้อมูลส่วนบุคคล (Personal Data Risk Assessment Report)

หน่วยงาน/โครงการ: ระบบบริหารจัดการนักศึกษาออนไลน์ (Online Student Management System)

วันที่จัดทำรายงาน: 3 กันยายน 2568

ผู้รับผิดชอบโครงการ: ฝ่ายเทคโนโลยีสารสนเทศและฝ่ายวิชาการ

ผู้ตรวจสอบ: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ผู้อนุมัติ: คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

1. บทนำ

การประเมินความเสี่ยงของข้อมูลส่วนบุคคลนี้ จัดทำขึ้นตามนโยบายการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA Policy) เพื่อระบุ วิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคลในโครงการ “ระบบบริหารจัดการนักศึกษาออนไลน์” และเพื่อกำหนดมาตรการควบคุมหรือบรรเทาความเสี่ยงให้สอดคล้องกับกฎหมาย PDPA และมาตรฐานสากล

2. วัตถุประสงค์ของโครงการ

จัดทำระบบออนไลน์เพื่อบริหารจัดการข้อมูลนักศึกษา

รองรับการลงทะเบียนเรียน การชำระเงิน การประเมินผลการเรียน และการให้บริการด้านวิชาการ
เพิ่มประสิทธิภาพการให้บริการ ลดการใช้เอกสาร และอำนวยความสะดวกแก่นักศึกษาและบุคลากร

3. ขอบเขตของการประเมิน

ประเภทข้อมูลที่ประมวลผล: ข้อมูลส่วนบุคคลทั่วไป (ชื่อ-สกุล รหัสนักศึกษา ที่อยู่ เบอร์โทรศัพท์ อีเมล)

ข้อมูลอ่อนไหว (ข้อมูลสุขภาพ กรณีขอความช่วยเหลือพิเศษ)

กลุ่มเจ้าของข้อมูล: นักศึกษา อาจารย์ และเจ้าหน้าที่

วิธีการประมวลผล: การเก็บ การจัดเก็บในระบบคลาวด์ การใช้ การเปิดเผยแก่หน่วยงานภายในและบางหน่วยงานภายนอก (เช่น สถาบันการเงิน)

4. การประเมินความเสี่ยง

ตารางการประเมินความเสี่ยงถูกจัดทำตามแนวทางมาตรฐาน โดยใช้เกณฑ์ประเมิน โอกาส (Likelihood) และ ผลกระทบ (Impact) และกำหนดระดับความเสี่ยง (ต่ำ/ปานกลาง/สูง)

ลำดับ	ความเสี่ยงที่ระบุ	รายละเอียด	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	มาตรการควบคุมที่มีอยู่	มาตรการเพิ่มเติมที่แนะนำ
1	การเข้าถึงโดยไม่ได้รับอนุญาต	บัญชีผู้ใช้ถูกแฮกหรือรหัสผ่านรั่วไหล	ปานกลาง	สูง	สูง	การใช้รหัสผ่านขั้นต่ำ 8 ตัวอักษร	ใช้การยืนยันตัวตนสองชั้น (2FA) การเข้ารหัสการสื่อสาร
2	การรั่วไหลของข้อมูลอ่อนไหว	ข้อมูลสุขภาพนักศึกษาเผยแพร่โดยไม่ตั้งใจ	ต่ำ	สูง	ปานกลาง	จำกัดสิทธิ์การเข้าถึงเฉพาะผู้มีหน้าที่	เพิ่มการเข้ารหัสข้อมูลที่จัดเก็บ และระบบตรวจจับการเข้าถึงผิดปกติ
3	การใช้ข้อมูลผิดวัตถุประสงค์	นำข้อมูลนักศึกษาไปใช้เพื่อการตลาดโดยไม่ได้รับความยินยอม	ต่ำ	สูง	ปานกลาง	มีนโยบายห้ามใช้ข้อมูลเกินวัตถุประสงค์	จัดอบรมพนักงาน และทำระบบ log เพื่อตรวจสอบการใช้งาน
4	ความเสี่ยงจากผู้ให้บริการภายนอก	ผู้ให้บริการระบบคลาวด์จัดเก็บข้อมูลในประเทศที่ไม่มีกฎหมาย	ต่ำ	สูง	ปานกลาง	สัญญาเงื่อนไขด้านการคุ้มครองข้อมูล	ตรวจสอบมาตรฐาน ISO/IEC 27001 และใช้การเข้ารหัสฝั่ง

	(Cloud Provider)	ผู้คุมครองข้อมูล					ลูกค้า (client-side encryption)

5. การประเมินมาตรการควบคุม

จากการประเมิน พบว่ามาตรการที่มีอยู่แล้วสามารถลดความเสี่ยงบางส่วนได้ แต่ยังมีความจำเป็นต้องเสริมสร้างมาตรการด้าน **เทคโนโลยี** (เช่น การเข้ารหัส 2FA IDS/IPS) และ **มาตรการเชิงองค์กร** (เช่น การอบรม การตรวจสอบภายใน การทบทวนนโยบายการเข้าถึงข้อมูล)

6. สรุปผลและข้อเสนอแนะ

การดำเนินโครงการ “ระบบบริหารจัดการนักศึกษาออนไลน์” สามารถดำเนินต่อไปได้ภายใต้เงื่อนไขว่าต้องจัดทำระบบการยืนยันตัวตนสองชั้น (2FA)

ต้องเข้ารหัสข้อมูลสุขภาพของนักศึกษาในฐานข้อมูลทั้งหมด

ต้องเพิ่มการอบรมบุคลากรเกี่ยวกับการใช้ข้อมูลตามวัตถุประสงค์

ต้องทบทวนสัญญากับผู้ให้บริการคลาวด์ และเลือกผู้ให้บริการที่มีมาตรฐานความปลอดภัยได้รับการรับรอง

ผลลัพธ์ของการประเมินนี้ จะถูกนำไปบันทึกและบูรณาการเข้ากับ **ทะเบียนการจัดการความเสี่ยงขององค์กร (Risk Register)** และรายงานต่อผู้บริหารระดับสูงเพื่ออนุมัติ

7. การอนุมัติ

ลงชื่อ

(ผู้รับผิดชอบโครงการ)

วันที่

ลงชื่อ

(เจ้าหน้าที่ผู้คุมครองข้อมูลส่วนบุคคล: DPO)

ลงชื่อ

(ผู้บริหาร/คณะกรรมการอนุมัติ)

วันที่

รายงานการประเมินความเสี่ยงของข้อมูลส่วนบุคคล (Personal Data Risk Assessment Report – Template)

หน่วยงาน/โครงการ:

วันที่จัดทำรายงาน:

ผู้รับผิดชอบโครงการ:

ผู้ตรวจสอบ: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ผู้อนุมัติ: คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขององค์กร / ผู้บริหารสูงสุด

1. บทนำ

รายงานฉบับนี้จัดทำขึ้นเพื่อระบุ วิเคราะห์ และประเมินความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคลในโครงการ รวมถึงเพื่อกำหนดมาตรการควบคุมและบรรเทาความเสี่ยงให้สอดคล้องกับนโยบายการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA Policy) และข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. วัตถุประสงค์ของโครงการ

.....

.....

.....

3. ขอบเขตของการประเมิน

ประเภทข้อมูลที่ประมวลผล:

กลุ่มเจ้าของข้อมูล:

วิธีการประมวลผล:

ระบบ/เทคโนโลยีที่ใช้:

4. การประเมินความเสี่ยง

คำแนะนำ: กรอกรข้อมูลความเสี่ยงที่อาจเกิดขึ้น มาตรการควบคุมที่มีอยู่ และมาตรการเพิ่มเติมที่แนะนำ

ลำดับ	ความเสี่ยงที่ระบุ	รายละเอียด	โอกาสเกิด (Likelihood 1-5)	ผลกระทบ (Impact 1-5)	ระดับความเสี่ยง (ต่ำ/ ปานกลาง/ สูง)	มาตรการควบคุมที่มีอยู่	มาตรการเพิ่มเติมที่แนะนำ
1							
2							

3							
4							

หมายเหตุการประเมินระดับความเสี่ยง:

โอกาสเกิด (Likelihood): 1 = น้อยมาก ... 5 = แน่จนเกิดขึ้น

ผลกระทบ (Impact): 1 = ผลกระทบน้อย ... 5 = ร้ายแรงต่อสิทธิหรือเสรีภาพของเจ้าของข้อมูล

ระดับความเสี่ยง: คำนวณจาก โอกาส x ผลกระทบ และแบ่งเป็น ต่ำ/ปานกลาง/สูง

5. สรุปผลและข้อเสนอแนะ

ผลการประเมินความเสี่ยงหลัก:

มาตรการบรรเทาที่ต้องดำเนินการ:

การติดตามและประเมินผล:

6. การอนุมัติ

ลงชื่อผู้รับผิดชอบโครงการ: วันที่:

ลงชื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO): วันที่:

ลงชื่อผู้อนุมัติ/คณะกรรมการ: วันที่:

7. หมายเหตุ

รายงานนี้ต้องถูกเก็บรักษาเป็นหลักฐานและทบทวนเมื่อมีการเปลี่ยนแปลงกระบวนการ เทคโนโลยี หรือโครงการ

การไม่ดำเนินการตามข้อเสนอแนะถือเป็นความเสี่ยงและต้องรายงานต่อผู้บริหาร

8.3.2 องค์กรมีเกณฑ์เพื่อตรวจสอบคัดกรอง (Screening Checklist) ว่าองค์กรต้องทำ DPIA หรือไม่ รวมถึงข้อควรพิจารณาที่เกี่ยวข้องทั้งหมดเกี่ยวกับขอบเขต ประสิทธิภาพ และลักษณะของการประมวลผลที่จะดำเนินการ

สิ่งที่ต้องทำ: องค์กรมีเกณฑ์เพื่อตรวจสอบคัดกรอง (Screening Checklist) ว่าองค์กรต้องทำ DPIA หรือไม่ รวมถึงข้อควรพิจารณาที่เกี่ยวข้องทั้งหมดเกี่ยวกับขอบเขต ประสิทธิภาพ และลักษณะของการประมวลผลที่จะดำเนินการ

หลักฐาน: นโยบายการประเมินความเสี่ยงของข้อมูลส่วนบุคคล
รายงานการประเมินความเสี่ยงของข้อมูลส่วนบุคคล

หนังสืออนุมัติรายงานการประเมินความเสี่ยงของข้อมูลส่วนบุคคล
สภาพบังคับ: กฎหมายไม่ได้กำหนด

**เอกสารหลักฐาน: นโยบายการคาดการณ์และประเมินความเสี่ยงด้านความเป็นส่วนตัวในขั้นตอนการ
ออกแบบระบบ ผลิตภัณฑ์ และกระบวนการ (Privacy Risk Forecast and Prevention Policy)**
**ชื่อเอกสาร: นโยบายการประเมินและคาดการณ์ความเสี่ยงที่อาจรุกร้าความเป็นส่วนตัวในระยะเริ่มต้นของ
โครงการ**

หน่วยงาน: ฝ่ายบริหารความเสี่ยงและการออกแบบระบบ

วันที่จัดทำ: 4 มิถุนายน 2568

1. วัตถุประสงค์

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดแนวทางในการพิจารณาและคาดการณ์ถึงความเสี่ยงที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลในช่วงเริ่มต้นของการออกแบบระบบงานผลิตภัณฑ์ และกระบวนการใหม่ รวมถึงตลอดวัฏจักรการพัฒนาและใช้งานระบบ โดยมีวัตถุประสงค์เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างปลอดภัย โปร่งใส และลดโอกาสเกิดการละเมิดความเป็นส่วนตัวอย่างมีประสิทธิภาพ

2. ขอบเขตการบังคับใช้

นโยบายฉบับนี้ใช้กับการพัฒนาและปรับปรุงระบบ เทคโนโลยี กระบวนการ หรือผลิตภัณฑ์ใด ๆ ภายในหน่วยงานที่มีความเกี่ยวข้องกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งโดยตรงและโดยอ้อม รวมถึงการว่าจ้างผู้ให้บริการภายนอกที่มีการเข้าถึงหรือจัดการข้อมูลส่วนบุคคล

3. แนวทางการดำเนินงาน

การคาดการณ์กิจกรรมการประมวลผลที่จะเกิดขึ้น

- ผู้พัฒนาระบบต้องจัดทำแบบฟอร์มระบุลักษณะของกิจกรรมการประมวลผลข้อมูล เช่น การเก็บข้อมูลจากผู้ใช้ การส่งต่อไปยังบุคคลภายนอก การวิเคราะห์ข้อมูล ฯลฯ
- แบบฟอร์มดังกล่าวต้องส่งให้ฝ่ายบริหารความเสี่ยงพิจารณาร่วมก่อนเริ่มกระบวนการพัฒนา

การระบุความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

- วิเคราะห์ว่าข้อมูลที่จัดเก็บมีลักษณะใด เป็นข้อมูลทั่วไปหรือข้อมูลอ่อนไหว
- พิจารณาผลกระทบที่อาจเกิดขึ้น เช่น การตีตราทางสังคม ความเสียหายต่อชื่อเสียง ความไม่ปลอดภัยทางกายภาพ หรือการเลือกปฏิบัติ

การกำหนดมาตรการป้องกันเชิงรุก (Proactive and Preventive Measures)

- รวมถึงการใช้การปกปิดตัวตน (Pseudonymisation) การเข้ารหัส (Encryption) การจำกัดการเข้าถึง (Access Control) การอบรมผู้เกี่ยวข้อง และการตั้งค่าเริ่มต้นที่ปลอดภัย (Default Privacy Settings)

4. เอกสารประกอบตามนโยบาย

ทะเบียนจัดการความเสี่ยงประจำโครงการ

มีการลงรายละเอียดของกิจกรรมการประมวลผลและผลกระทบที่คาดการณ์ไว้ในแต่ละโครงการ พร้อมลำดับความเสี่ยง

มาตรการเชิงรุกในการป้องกันความเสี่ยง

ระบุมาตรการเทคนิคและมาตรการองค์กร (Technical and Organizational Measures) ที่นำมาใช้ในระบบ เช่น การควบคุมสิทธิ์ของผู้ใช้งาน การแจ้งเตือนการรั่วไหลของข้อมูล

แบบฟอร์มการประเมินความเสี่ยง (Privacy Risk Assessment Form)

มีหัวข้อเกี่ยวกับลักษณะของกิจกรรมการประมวลผล ความอ่อนไหวของข้อมูล ระดับความน่าจะเป็นของเหตุการณ์รุกราน และระดับผลกระทบ

รายงานสรุปผลการวิเคราะห์ความเสี่ยง

จัดทำโดยฝ่ายเทคโนโลยีและฝ่ายกฎหมาย ก่อนการอนุมัติให้ดำเนินโครงการต่อไป

5. ขั้นตอนการประเมินความเสี่ยงล่วงหน้า

ขั้นตอน	รายละเอียด	ผู้รับผิดชอบ
1. แจ้งเริ่มต้นการออกแบบ	ทีมพัฒนาระบบแจ้งกิจกรรมประมวลผลที่คาดว่าจะเกิดขึ้น	หัวหน้าโครงการ
2. จัดทำแบบประเมินความเสี่ยง	กรอกแบบฟอร์ม Privacy Risk Assessment	ผู้พัฒนาระบบ + เจ้าหน้าที่คุ้มครองข้อมูล
3. วิเคราะห์และตรวจสอบรวม	วิเคราะห์ผลกระทบและกำหนดมาตรการ	ฝ่ายบริหารความเสี่ยง
4. สรุปและเสนอผู้บริหาร	เสนอรายงานผลการคาดการณ์ความเสี่ยงเพื่ออนุมัติ	คณะกรรมการบริหารระบบ
5. ติดตามประเมินซ้ำหลังดำเนินการ	ทบทวนความเสี่ยงใหม่ (ถ้ามี)	ฝ่ายตรวจสอบภายใน

6. การติดตามและประเมินผล

หน่วยงานจะดำเนินการติดตามผลการประเมินล่วงหน้าเป็นประจำทุก 6 เดือน โดยเฉพาะโครงการที่มีลักษณะเปลี่ยนแปลงกระบวนการประมวลผลอย่างมีนัยสำคัญ โดยมีการจัดทำรายงานทบทวนความเสี่ยง และเสนอให้คณะกรรมการบริหารรับทราบ

ลงชื่อ

นางสาวจิราภรณ์ ศิริกุล

หัวหน้าฝ่ายบริหารความเสี่ยงและการออกแบบระบบ

ลงนามเมื่อ: 4 มิถุนายน 2568

**8.3.3 หากเกณฑ์ตรวจสอบคัดกรองระบุว่างค์กรไม่จำเป็นต้อง ทำ DPIA องค์กรจะบันทึกเหตุผลเอาไว้
สิ่งที่ต้องทำ: องค์กรมีการบันทึกเหตุผล และมีนโยบายการตรวจสอบคัดกรอง (Screening Checklist)
รวมถึงมีรายงานผลการคัดกรองการประเมินความเสี่ยง**

หลักฐาน: นโยบายการตรวจสอบคัดกรองการดำเนินการประเมินความเสี่ยง

บันทึกเหตุผลการไม่ประเมินความเสี่ยง

รายงานผลการคัดกรองการประเมินความเสี่ยง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการตรวจสอบคัดกรองเพื่อพิจารณาความจำเป็นในการจัดทำ DPIA (DPIA Screening Policy)

ชื่อเอกสาร: นโยบายการตรวจสอบคัดกรองการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
(DPIA)

หน่วยงาน: คณะกรรมการกำกับการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

วันที่มีผลบังคับใช้: 4 มิถุนายน 2568

วัตถุประสงค์

นโยบายฉบับนี้มีวัตถุประสงค์เพื่อกำหนดเกณฑ์และกระบวนการคัดกรองโครงการหรือกิจกรรมใหม่ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล เพื่อพิจารณาว่ากิจกรรมใดจำเป็นต้องจัดทำ การประเมินผลกระทบ (DPIA) และกิจกรรมใดที่ไม่จำเป็นต้องดำเนินการ พร้อมการบันทึกเหตุผลไว้อย่างเป็นทางการเพื่อให้สามารถตรวจสอบย้อนหลังได้

ขอบเขต

นโยบายนี้ครอบคลุมกิจกรรมของทุกหน่วยงานภายในองค์กรที่มีการดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผย หรือประมวลผลข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลทั่วไปหรือข้อมูลอ่อนไหว

ขั้นตอนการคัดกรอง

ขั้นตอน	รายละเอียด	เอกสารที่เกี่ยวข้อง
1	ทีมงานกรอกแบบฟอร์ม DPIA Screening Checklist	DPIA Screening Checklist
2	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตรวจสอบและวิเคราะห์	รายงานผลการคัดกรอง (Screening Report)
3	หากไม่จำเป็นต้องทำ DPIA → บันทึกเหตุผลไว้ในแบบฟอร์มมาตรฐาน	บันทึกเหตุผลการไม่ทำ DPIA

เกณฑ์ตัวอย่างใน Checklist

- มีการประมวลผลข้อมูลอ่อนไหว (เช่น ข้อมูลสุขภาพ ชาติพันธุ์ ศาสนา)?
- มีการเฝ้าระวังบุคคลในพื้นที่สาธารณะ?
- มีการตัดสินใจอัตโนมัติที่ส่งผลกระทบอย่างมีนัยสำคัญต่อเจ้าของข้อมูล?
- โครงการมีผลกระทบในวงกว้าง (large scale) หรือไม่?

หากคำตอบ "ใช่" ในข้อใดข้อหนึ่ง → พิจารณาจัดทำ DPIA

หากคำตอบ "ไม่ใช่ทั้งหมด" → ไม่จำเป็นต้องจัดทำ DPIA แต่ต้อง บันทึกเหตุผล

2. แบบฟอร์มบันทึกเหตุผลกรณีไม่จำเป็นต้องทำ DPIA (Record of Non-DPIA Justification)

ชื่อโครงการ: ระบบลงทะเบียนอบรมออนไลน์ (e-Training Registration System)

วันที่ประเมิน: 2 พฤษภาคม 2568

ผู้ประเมิน: นางสาวชลธิชา เรืองรัตน์ (เจ้าหน้าที่ DPO)

ผลการคัดกรอง

- ไม่มีการประมวลผลข้อมูลอ่อนไหว
- ไม่มีการเฝ้าระวังบุคคลในพื้นที่สาธารณะ
- ไม่มีการตัดสินใจอัตโนมัติ
- ไม่มีผลกระทบในวงกว้าง

สรุปผล: ไม่เข้าเกณฑ์ที่ต้องจัดทำ DPIA

เหตุผล: โครงการมีเพียงการรวบรวมชื่อ-สกุล และอีเมลเพื่อส่งลิงก์การอบรม ไม่มีการนำข้อมูลไปใช้ต่อเพื่อวัตถุประสงค์อื่น ไม่มีความเสี่ยงที่ส่งผลกระทบต่อสิทธิของเจ้าของข้อมูลในระดับสูง

ลงชื่อ:

นางสาวชลธิชา เรืองรัตน์

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ลงวันที่: 2 พฤษภาคม 2568

3. รายงานผลการคัดกรองการประเมินความเสี่ยง (DPIA Screening Report)

สรุปรายเดือน: พฤษภาคม 2568

ลำดับ	ชื่อโครงการ	หน่วยงาน	ผลการคัดกรอง	เหตุผลไม่ทำ DPIA	ลงชื่อผู้รับรอง
1	ระบบอบรมออนไลน์	ฝ่าย HR	ไม่จำเป็น	ไม่ประมวลผลข้อมูลอ่อนไหว ไม่มีการตัดสินใจอัตโนมัติ	ชลธิชา เรืองรัตน์
2	ระบบติดตามพัสดุภายใน	ฝ่ายจัดซื้อ	ไม่จำเป็น	ไม่มีข้อมูลส่วนบุคคล	ปรัชญา ทิพย์วิไล

8.3.4 ขั้นตอนขององค์กรรวมถึงข้อกำหนดในการขอคำแนะนำจาก DPO และเจ้าหน้าที่อื่น ๆ ภายในองค์กรที่เกี่ยวข้องในการจัดทำ การประเมินความเสี่ยง

สิ่งที่ต้องทำ: องค์กรมีการขอคำแนะนำจาก DPO และเจ้าหน้าที่อื่น ๆ ภายในองค์กรที่เกี่ยวข้องในการจัดทำ การประเมินความเสี่ยง และมีเอกสารหลักฐานในการให้คำปรึกษาครบถ้วน

หลักฐาน: นโยบายการให้คำแนะนำในการจัดทำ การประเมินความเสี่ยง
ประกาศตารางนัดให้คำปรึกษาหรือช่องทางให้คำปรึกษา
คู่มือการให้คำปรึกษาด้านการประเมินความเสี่ยง
บันทึกการให้คำปรึกษาและข้อสังเกตเกี่ยวกับความเห็นหรือความเข้าใจของผู้เข้ารับคำปรึกษา

สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการให้คำแนะนำในการจัดทำ การประเมินความเสี่ยง

ชื่อเอกสาร: นโยบายการให้คำปรึกษาและสนับสนุนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA Consultation Policy)

หน่วยงานเจ้าของ: สำนักงานคุ้มครองข้อมูลส่วนบุคคลองค์กร

ประกาศใช้: 1 พฤษภาคม 2568

วัตถุประสงค์

เพื่อกำหนดขั้นตอน การมีส่วนร่วม และบทบาทหน้าที่ของเจ้าหน้าที่ DPO และหน่วยงานอื่นที่เกี่ยวข้อง ในการให้คำปรึกษา สนับสนุน และตรวจสอบการดำเนินการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลของแต่ละโครงการหรือระบบ

ขอบเขต

นโยบายนี้ครอบคลุมทุกหน่วยงานที่ต้องประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล ตั้งแต่ขั้นตอนเริ่มต้นของโครงการ จนถึงการอนุมัติดำเนินการ

บทบาทของ DPO

- ให้คำปรึกษาเบื้องต้นในการพิจารณาความจำเป็นของ DPIA
- ตรวจสอบแบบฟอร์ม DPIA ก่อนและหลังการประเมิน
- มีสิทธิให้ความเห็นเชิงเทคนิคและกฎหมาย
- บันทึกความเห็นหรือข้อเสนอแนะไว้ในแบบฟอร์มประเมิน

2. ประกาศช่องทางให้คำปรึกษาและตารางนัดหมาย

หัวข้อ: ตารางการเปิดให้คำปรึกษาด้าน DPIA และการประเมินความเสี่ยงข้อมูลส่วนบุคคล
วันที่ประกาศ: 30 เมษายน 2568

ช่องทางการติดต่อ

ช่องทาง	รายละเอียด
Email	dpo@or.anization.ac.th
Line/OA	@orgDPOsupport
ระบบจองนัด	ผ่าน Intranet > ระบบ DPO Booking
Walk-in	วันจันทร์ – ศุกร์ เวลา 13.00 – 16.00 น. ณ ห้อง 405 อาคารบริหารกลาง

3. คู่มือการให้คำปรึกษาด้านการประเมินความเสี่ยง

หัวข้อ: คู่มือการขอรับคำปรึกษาการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA Consultation Manual)

เนื้อหาหลัก:

- ขั้นตอนการขอคำปรึกษา (5 ขั้นตอน)

- เอกสารประกอบที่ต้องเตรียม เช่น DPIA Screening Form ร่างระบบ หรือแบบฟอร์มบันทึกความเสี่ยง
- วิธีการจูงใจ
- ข้อเสนอแนะในการเตรียมประเด็นคำถาม
- แนวทางปฏิบัติตามคำแนะนำ DPO
- แบบฟอร์ม “คำถาม – คำตอบ” สรุปหลังให้คำปรึกษา

5. บันทึกการให้คำปรึกษา (Consultation Log)

ชื่อผู้ขอคำปรึกษา: นายณัฐวุฒิ ศรีรักษา
โครงการ: ระบบลงทะเบียนกิจกรรมภายในองค์กร
วันที่ให้คำปรึกษา: 8 พฤษภาคม 2568

ผู้ให้คำปรึกษา: นางสาวปวีณา จันทร์เรือง (DPO)

ประเด็นที่ปรึกษา

- วิธีการออกแบบฟอร์ม DPIA
- การพิจารณาระดับความเสี่ยง
- แนวทางในการลดความเสี่ยงที่ตรวจพบ

ข้อเสนอแนะ

ปรับปรุงมาตรการ pseudonymisation

เพิ่ม banner แจ้งเจ้าของข้อมูลก่อนเริ่มเก็บข้อมูล

ความคิดเห็นของผู้รับคำปรึกษา

- “เข้าใจมากขึ้นเกี่ยวกับการวิเคราะห์ผลกระทบสิทธิของเจ้าของข้อมูล”
- “ได้รับแนวทางชัดเจนในการปรับปรุงระบบให้สอดคล้องกับกฎหมาย”

ลงชื่อ

ผู้ให้คำปรึกษา:

ผู้รับคำปรึกษา:

วันที่ลงนาม: 8 พฤษภาคม 2568

8.3.5 ขั้นตอนขององค์กรรวมถึงการปรึกษาหารือกับผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ตัวแทน และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้องตามความเหมาะสม

สิ่งที่ต้องทำ: องค์กรมีขั้นตอนที่รวมถึงการปรึกษาหารือกับผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ตัวแทน และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้องตามความเหมาะสม และมีเอกสารหลักฐานในการปรึกษาหารือครบถ้วน

หลักฐาน: นโยบายการให้คำแนะนำในการจัดการประเมินความเสี่ยง
ประกาศตารางนัดให้คำปรึกษาหรือช่องทางให้คำปรึกษา
คู่มือการให้คำปรึกษาด้านการประเมินความเสี่ยง
บันทึกการให้คำปรึกษาและข้อสังเกตเกี่ยวกับความเห็นหรือความเข้าใจของผู้เข้ารับคำปรึกษา

สภาพบังคับ: กฎหมายไม่ได้กำหนด

หัวข้อ: เอกสารหลักฐานการปรึกษาหารือกับผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล ตัวแทน และผู้มีส่วนได้ส่วนเสียอื่น ๆ

1. นโยบายการให้คำแนะนำในการจัดการประเมินความเสี่ยง (DPIA Consultation Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางและขอบเขตของการปรึกษาหารือระหว่างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) กับผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล ตัวแทน และผู้มีส่วนได้ส่วนเสียอื่น ๆ ก่อนและระหว่างกระบวนการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล

สาระสำคัญ

- ขั้นตอนและกรอบเวลาในการดำเนินการปรึกษาหารือ
- รายชื่อผู้มีส่วนเกี่ยวข้องที่ต้องเข้าร่วม
- วิธีการบันทึกความคิดเห็นและข้อเสนอแนะ
- แนวทางการตอบสนองต่อข้อเสนอแนะที่ได้รับ

2. ประกาศตารางนัดให้คำปรึกษาและช่องทางติดต่อ

หัวข้อ: กำหนดการให้คำปรึกษาและการมีส่วนร่วมของผู้เกี่ยวข้องในการจัดทำ DPIA

รายละเอียด

วัน-เวลา	ช่องทาง	รายละเอียด
ทุกวันอังคาร	Intranet – ระบบนัดหมาย DPO	สำหรับผู้ควบคุม/ประมวลผลข้อมูล
ทุกวันศุกร์	Microsoft Teams	สำหรับตัวแทนหรือผู้มีส่วนได้ส่วนเสียภายนอก
ตลอดเวลา	Email: dpo@organization.ac.th	สำหรับการส่งเอกสาร/ความคิดเห็น

3. คู่มือการให้คำปรึกษาด้านการประเมินความเสี่ยง

เนื้อหา

- วิธีการประสานงานเพื่อเข้ารับคำปรึกษา
- รายชื่อผู้เกี่ยวข้องที่ควรเข้าร่วมการหารือ
- รูปแบบการประชุม: Online/Offline/เอกสาร
- แบบฟอร์มการให้ข้อเสนอแนะ
- ขั้นตอนการจัดเก็บข้อเสนอแนะ และการสรุปผลเพื่อใช้ประกอบรายงาน DPIA

4. บันทึกการให้คำปรึกษา (Consultation Record)

ชื่อโครงการ: ระบบรับสมัครนักศึกษาออนไลน์

วันที่ให้คำปรึกษา: 6 พฤษภาคม 2568

ผู้เกี่ยวข้องที่เข้าร่วม

- ผู้ควบคุมข้อมูล: นายสมเกียรติ พิทักษ์สิทธิ์
- ผู้ประมวลผลข้อมูล: บริษัท ซอฟต์แวร์โปรเซส จำกัด
- ตัวแทนคณะกรรมการ IT: นางสาวจันทร์เพ็ญ มีทรัพย์
- เจ้าหน้าที่ DPO: น.ส.ปวีณา ศิริจันทร์

สาระสำคัญในการหารือ

- ความจำเป็นของการประมวลผลข้อมูลนักเรียน
- ขอบเขตการเข้าถึงข้อมูลของผู้ประมวลผล
- ความเห็นจากผู้ควบคุมเกี่ยวกับการเก็บ consent
- ข้อเสนอแนะให้จัดทำ Privacy Notice แบบย่อ
- DPO เสนอให้จัดทำ DPIA อย่างย่อ พร้อมแนบท้ายสัญญา

ผลการดำเนินการ

ข้อเสนอแนะทั้งหมดจะถูกรวมไว้ในรายงาน DPIA และนำเสนอต่อผู้บริหารเพื่อพิจารณาอนุมัติ

ลงชื่อ

ผู้จัดประชุม:

ผู้เข้าร่วม:

วันที่ลงนาม: 6 พฤษภาคม 2568

คู่มือการให้คำปรึกษาด้านการประเมินความเสี่ยง

1. วัตถุประสงค์ของคู่มือ

คู่มือฉบับนี้จัดทำขึ้นเพื่อเป็นแนวทางสำหรับการดำเนินงานเกี่ยวกับการให้คำปรึกษาด้านการประเมินความเสี่ยง (Data Protection Impact Assessment: DPIA) โดยเฉพาะการมีส่วนร่วมของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) และผู้มีส่วนเกี่ยวข้องภายในและภายนอกองค์กร เช่น ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ผู้ประมวลผลข้อมูล (Data Processor) ตัวแทนหน่วยงาน และผู้มีส่วนได้ส่วนเสียอื่น ๆ ตามความเหมาะสม โดยมุ่งเน้นให้เกิดกระบวนการทำงานที่มีประสิทธิภาพ โปร่งใส ตรวจสอบได้ และสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้อง

2. ขอบเขตของคู่มือ

คู่มือฉบับนี้ครอบคลุมแนวทาง ขั้นตอน รูปแบบ และวิธีการที่ใช้ในการให้คำปรึกษา ตั้งแต่เริ่มต้นกระบวนการวิเคราะห์โครงการ กระบวนการประเมินผลกระทบจากการประมวลผลข้อมูลส่วนบุคคล จนถึง การสรุปผลการประเมินเพื่อประกอบการตัดสินใจหรือดำเนินมาตรการที่จำเป็นต่อไป โดยใช้กรอบแนวคิดของการคาดการณ์ล่วงหน้า การป้องกันความเสี่ยงเชิงรุก และการมีส่วนร่วมของผู้เกี่ยวข้องอย่างเป็นระบบ

3. นิยามคำศัพท์

- **การประเมินความเสี่ยง (Risk Assessment):** การวิเคราะห์และประเมินผลกระทบที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูลจากการดำเนินกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- **DPIA:** เอกสารที่แสดงการประเมินความเสี่ยงจากกิจกรรมการประมวลผลข้อมูล พร้อมมาตรการลดผลกระทบดังกล่าว
- **DPO:** เจ้าหน้าที่ผู้ทำหน้าที่ให้คำแนะนำ ติดตาม ตรวจสอบ และประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคล
- **Stakeholders:** บุคคลหรือหน่วยงานที่ได้รับผลกระทบหรือมีบทบาทต่อกิจกรรมการประมวลผลข้อมูล เช่น เจ้าของข้อมูล หน่วยงานที่รับข้อมูล บุคคลภายนอก ฯลฯ

4. กระบวนการให้คำปรึกษา

4.1 การแจ้งความประสงค์ขอรับคำปรึกษา

ผู้ควบคุมข้อมูลหรือหน่วยงานเจ้าของโครงการต้องแจ้งความประสงค์ขอรับคำปรึกษาด้าน DPIA ผ่านระบบแบบฟอร์มหรือช่องทางที่กำหนด เช่น อีเมล ภายใน 15 วันก่อนเริ่มดำเนินการโครงการ โดยระบุข้อมูลเบื้องต้น เช่น วัตถุประสงค์ของโครงการ ประเภทข้อมูลที่ใช้ กลุ่มเป้าหมาย และระบบที่เกี่ยวข้อง

4.2 การจัดประชุมร่วมกับ DPO และผู้เกี่ยวข้อง

DPO จะประสานการจัดประชุมร่วมกับผู้มีส่วนเกี่ยวข้อง โดยกำหนดวัน เวลา และช่องทางการประชุมที่เหมาะสม โดยมีเป้าหมายหลักคือ

- ทำความเข้าใจโครงการและกิจกรรมการประมวลผล
- ประเมินระดับความเสี่ยงเบื้องต้น
- ระบุนผลกระทบที่อาจเกิดขึ้น
- เสนอแนวทางลดความเสี่ยงในเชิงนโยบายและเทคนิค

4.3 การเก็บรวบรวมข้อเสนอแนะและมุมมองจากผู้มีส่วนได้ส่วนเสีย

เพื่อให้กระบวนการประเมินมีความรอบด้าน องค์กรจะดำเนินการเชิญผู้มีส่วนได้ส่วนเสีย เช่น เจ้าของข้อมูล ตัวแทนหน่วยงานบริการสาธารณะ หรือภาคเอกชน มาร่วมแสดงความคิดเห็นในประเด็นต่อไปนี้:

- ความชัดเจนและความจำเป็นของการประมวลผล
- ความคุ้มค่าเทียบกับความเสี่ยง
- ความเป็นธรรมและการเข้าถึงข้อมูลของเจ้าของข้อมูล

5. แนวทางการจัดประชุมให้คำปรึกษา

5.1 การกำหนดวาระการประชุม

วาระหลักของการประชุมให้คำปรึกษาด้านความเสี่ยง ได้แก่

- สรุปภาพรวมของโครงการ
- รายละเอียดการประมวลผลข้อมูล
- การประเมินผลกระทบ
- มาตรการลดความเสี่ยง
- คำแนะนำจาก DPO
- คำถาม-คำตอบและข้อเสนอแนะ

5.2 เอกสารที่ใช้ในการประชุม

- แบบฟอร์ม DPIA
- แบบประเมินความเสี่ยงเบื้องต้น (Screening Checklist)
- เอกสารประกอบโครงการ เช่น โครงสร้างระบบ แผนผังการประมวลผลข้อมูล (Data Flow Diagram)
- คู่มือข้อพิจารณาด้านกฎหมาย

5.3 การจดบันทึกและติดตามผล

ผู้จัดประชุมจะต้องบันทึกข้อคิดเห็น ข้อเสนอแนะ และคำแนะนำจากผู้เข้าร่วม และสรุปผลการประชุมเป็นรายงานเพื่อจัดเก็บไว้เป็นหลักฐาน ประกอบการตัดสินใจในการดำเนินโครงการ

6. บทบาทหน้าที่ของผู้มีส่วนเกี่ยวข้อง

6.1 เจ้าหน้าที่ DPO

- ให้คำปรึกษาเชิงเทคนิคและกฎหมาย
- ประเมินความเสี่ยงจากมุมมองของการคุ้มครองข้อมูล
- เสนอแนะแนวทางการลดความเสี่ยง
- ตรวจสอบความครบถ้วนของรายงาน DPIA

6.2 ผู้ควบคุมข้อมูล

- ให้ข้อมูลเกี่ยวกับโครงการอย่างโปร่งใส
- เปิดรับข้อเสนอแนะจากผู้มีส่วนได้ส่วนเสีย
- พิจารณาปรับแนวทางการดำเนินการตามข้อเสนอแนะ

6.3 ผู้ประมวลผลข้อมูล / ตัวแทนหน่วยงาน

- ให้ข้อมูลทางเทคนิคเกี่ยวกับระบบหรือเทคโนโลยีที่ใช้
- สนับสนุนด้านวิธีการประมวลผล

6.4 เจ้าของข้อมูล / ผู้แทน

- มีสิทธิแสดงความคิดเห็นเกี่ยวกับการใช้ข้อมูลของตน
- เสนอแนะแนวทางที่เป็นประโยชน์ต่อการคุ้มครองสิทธิส่วนบุคคล

7. แบบฟอร์มและเครื่องมือที่ใช้ในการให้คำปรึกษา

- แบบฟอร์มขอรับคำปรึกษา
- แบบฟอร์มประเมินความเสี่ยงเบื้องต้น
- แบบสอบถามความคิดเห็นจาก Stakeholders
- แบบฟอร์มบันทึกการประชุมให้คำปรึกษา

8. แนวทางการจัดเก็บและเปิดเผยข้อมูล

ข้อมูลที่ได้จากการให้คำปรึกษาจะถูกจัดเก็บในระบบบริหารจัดการความเสี่ยงขององค์กร โดยจัดเป็นความลับระดับภายใน ยกเว้นในกรณีที่ต้องเปิดเผยต่อหน่วยงานกำกับดูแล หรือในกรณีที่เจ้าของข้อมูลร้องขอภายใต้สิทธิของตน

9. ข้อควรระวังและแนวทางแก้ไขปัญหา

- การให้คำปรึกษาควรดำเนินการโดยมีข้อมูลที่ชัดเจนและเพียงพอ
- หากเกิดความขัดแย้งด้านความคิดเห็น ควรใช้กลไกไกล่เกลี่ยร่วมกับฝ่ายนิติกร
- หากประเมินพบความเสี่ยงในระดับสูง ควรชะลอหรือปรับโครงการก่อนการอนุมัติขั้นสุดท้าย

10. การทบทวนและปรับปรุงคู่มือ

คู่มือฉบับนี้ จะได้รับการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมาย นโยบาย หรือระบบเทคโนโลยีที่เกี่ยวข้อง เพื่อให้แนวทางยังคงทันสมัยและสอดคล้องกับบริบทขององค์กร

8.3.6 การฝึกอบรมพนักงานรวมถึงความจำเป็นในการประเมินเพื่อทำ DPIA ในระยะแรกของแผนหรือโครงการใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และองค์กรมีการฝึกอบรมพนักงานในการจัดทำ DPIA

สิ่งที่ต้องทำ: มีการฝึกอบรมพนักงานรวมถึงความจำเป็นในการประเมินเพื่อทำ DPIA ในระยะแรกของแผนหรือโครงการใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และมีการให้ DPO ฝึกอบรมกับหน่วยงานภายนอกตามความเหมาะสม

หลักฐาน: นโยบายการฝึกอบรมพนักงานเพื่อการประเมินความเสี่ยงของข้อมูลส่วนบุคคล
 นโยบายการทดสอบความรู้และความเข้าใจของพนักงานด้านการประเมินความเสี่ยง
 ประกาศตารางนัดให้คำปรึกษาหรือช่องทางให้คำปรึกษา
 คู่มือการให้คำปรึกษาด้านการประเมินความเสี่ยง
 บันทึกการให้คำปรึกษาและข้อสังเกตเกี่ยวกับความเห็นหรือความเข้าใจของผู้เข้ารับคำปรึกษา
 นโยบายการกำหนดให้ DPO เข้าอบรมและอบรมพนักงานด้านการประเมินความเสี่ยงของข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการฝึกอบรมพนักงานเพื่อการประเมินความเสี่ยงของข้อมูลส่วนบุคคล

องค์กรมีนโยบายในการจัดฝึกอบรมให้แก่พนักงานทุกระดับเกี่ยวกับการประเมินผลกระทบด้านการคุ้มครองข้อมูล (Data Protection Impact Assessment – DPIA) โดยมุ่งเน้นที่การเข้าใจขั้นตอนและความสำคัญของการดำเนินการในระยะแรกของแผนงานหรือโครงการที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

1.1 การฝึกอบรมจะจัดขึ้นอย่างน้อยปีละ 1 ครั้ง

- 1.2 พนักงานใหม่ต้องเข้าร่วมอบรมภายใน 60 วันหลังเริ่มงาน
- 1.3 เนื้อหาฝึกอบรมรวมถึงพื้นฐาน PDPA แนวคิด DPIA วิธีการคัดกรองโครงการ และกรณีศึกษาจริง
- 1.4 การฝึกอบรมจัดในรูปแบบ On-site หรือ Online ตามความเหมาะสม
- 1.5 บันทึกการฝึกอบรมจัดเก็บไว้เพื่อใช้ในการตรวจสอบย้อนหลังได้อย่างน้อย 3 ปี

2. นโยบายการทดสอบความรู้และความเข้าใจของพนักงานด้านการประเมินความเสี่ยง

เพื่อให้มั่นใจว่าพนักงานมีความเข้าใจในประเด็นการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล องค์กรมีการจัดทดสอบหลังการฝึกอบรม ดังนี้:

- 2.1 ทดสอบความเข้าใจหลังการฝึกอบรมผ่านระบบอิเล็กทรอนิกส์
- 2.2 พนักงานต้องผ่านเกณฑ์ 70% ขึ้นไปจึงจะถือว่าอบรมผ่าน
- 2.3 กรณีไม่ผ่าน ต้องเข้าอบรมซ้ำหรือรับคำปรึกษาจาก DPO
- 2.4 ผลการทดสอบจะถูกรวบรวมในฐานข้อมูลฝึกอบรมพนักงาน
- 2.5 การทดสอบอัปเดตทุกปีตามกฎหมายหรือแนวปฏิบัติที่เปลี่ยนแปลง

3. ประกาศตารางนัดให้คำปรึกษาหรือช่องทางให้คำปรึกษา

- 3.1 องค์กรกำหนดตารางนัดหมายการให้คำปรึกษาด้าน DPIA โดยเจ้าหน้าที่ DPO จะเปิดให้ปรึกษาเดือนละ 1 ครั้ง หรือตามนัดหมายพิเศษ
- 3.2 ช่องทางให้คำปรึกษา ได้แก่
 - 3.2.1 Email กลางของ DPO
 - 3.2.2 Microsoft Teams / Zoom สำหรับการให้คำปรึกษาออนไลน์
 - 3.2.3 ระบบ Helpdesk ภายใน

- 3.3 การนัดหมายสามารถจองผ่านระบบ Intranet
- 3.4 ตารางและช่องทางประกาศในเว็บไซต์ภายในขององค์กร

4. คู่มือการให้คำปรึกษาด้านการประเมินความเสี่ยง

เนื้อหาครอบคลุม

- 4.1 ขั้นตอนการขอคำปรึกษา
- 4.2 การเตรียมข้อมูลโครงการก่อนขอคำปรึกษา
- 4.3 แบบฟอร์มคำปรึกษา
- 4.4 บทบาทของผู้ให้และผู้รับคำปรึกษา
- 4.5 ตัวอย่างข้อควรระวังในการทำ DPIA
- 4.6 แนวทางการปฏิบัติตามข้อเสนอแนะจาก DPO

(รายละเอียดอยู่ในเอกสาร "คู่มือการให้คำปรึกษาด้านการประเมินความเสี่ยง" ที่จัดทำไว้แล้ว)

5. บันทึกการให้คำปรึกษาและข้อสังเกตเกี่ยวกับความเห็นหรือความเข้าใจของผู้เข้ารับคำปรึกษา

- 5.1 แบบบันทึกประกอบด้วย
 - 5.1.1 ชื่อโครงการและเจ้าของโครงการ

5.1.2	วัน เวลา สถานที่ หรือช่องทางการให้คำปรึกษา
5.1.3	ประเด็นคำปรึกษาที่ได้รับ
5.1.4	ข้อเสนอแนะจาก DPO หรือเจ้าหน้าที่ผู้เกี่ยวข้อง
5.1.5	ความเห็นหรือข้อสงสัยของผู้เข้ารับคำปรึกษา
5.1.6	สถานะของการดำเนินการตามข้อเสนอแนะ
5.2	บันทึกทั้งหมดจัดเก็บในระบบเอกสารภายในองค์กรและสำรองข้อมูลไว้ทุกไตรมาส
5.3	องค์กรกำหนดให้หัวหน้าฝ่ายตรวจสอบคุณภาพพบทวนบันทึกคำปรึกษาเป็นรายไตรมาส
6.	นโยบายการกำหนดให้ DPO เข้าอบรมและอบรมพนักงานด้านการประเมินความเสี่ยงของข้อมูลส่วนบุคคล
6.1	DPO ต้องเข้ารับการอบรมจากแหล่งภายนอกที่ได้รับการรับรองไม่น้อยกว่าปีละ 1 ครั้ง
6.2	DPO มีหน้าที่จัดเตรียมหลักสูตรและคู่มือให้ความรู้กับพนักงาน
6.3	การฝึกอบรมภายในต้องได้รับการอนุมัติจากผู้บริหารฝ่ายนโยบาย
6.4	รายงานผลการอบรม DPO และแผนการอบรมต่อไปต้องส่งต่อฝ่ายทรัพยากรบุคคล
6.5	หากมีการปรับปรุงหลักเกณฑ์ของ PDPA หรือ DPIA จากภาครัฐ DPO ต้องเสนอแผนฝึกอบรมเพิ่มเติมภายใน 30 วัน

ใบลงทะเบียนเข้าร่วมการฝึกอบรม (ตัวอย่างกรอกข้อมูล)					
ลำดับ	ชื่อ-นามสกุล	ตำแหน่ง	แผนก/ฝ่าย	เบอร์โทร/อีเมล	ลายมือชื่อผู้เข้าอบรม
1	นายสมชาย ใจดี	เจ้าหน้าที่ IT	ฝ่ายเทคโนโลยีสารสนเทศ	somchai@example.com / 081-2345678	ลงชื่อ
2	นางสาว สมหญิง สมหวัง	เจ้าหน้าที่ฝ่ายกฎหมาย	ฝ่ายกฎหมาย	somying@example.com / 082-345-789	ลงชื่อ
3	นายวิทยา เกียรติคุณ	ผู้จัดการโครงการ	ฝ่ายบริหารโครงการ	witaya@example.com / 083-4567890	ลงชื่อ

4	นางสาวสุนิสา ศรีสุข	เจ้าหน้าที่ประเมินความเสี่ยง	ฝ่ายความปลอดภัยข้อมูล	sunisa@example.com / 084-5678901	ลงชื่อ
5	นายปกรณ์ สุขสวัสดิ์	เจ้าหน้าที่ DPO	ฝ่ายคุ้มครองข้อมูล	pakorn@example.com / 085-6789012	ลงชื่อ

แบบประเมินผลหลังการฝึกอบรม (ตัวอย่างกรอก)

ส่วนที่ 1: ความพึงพอใจ

รายการประเมิน	พอใจมาก (5)	พอใจ (4)	ปานกลาง (3)	น้อย (2)	ควรปรับปรุง (1)
1. วิทยากรมีความรู้ ความสามารถ	✓				
2. เนื้อหาตรงกับวัตถุประสงค์	✓				
3. ประโยชน์ที่ได้รับจากการอบรม	✓				
4. เอกสารประกอบการอบรม		✓			
5. วิธีการนำเสนอและกิจกรรมระหว่างอบรม	✓				

ส่วนที่ 2: ความเข้าใจ

ข้อ	คำถาม	เข้าใจดี	ไม่เข้าใจ
1	เข้าใจหลักการของ DPIA	✓	
2	รู้ขั้นตอนในการจัดทำ DPI	✓	
3	รู้ว่าเมื่อใดควรเริ่มทำ DPIA	✓	

ส่วนที่ 3: ข้อเสนอแนะเพิ่มเติม

- เพิ่มกรณีตัวอย่างเพื่อให้เข้าใจง่ายขึ้น
- ต้องการเวิร์กช็อปฝึกปฏิบัติเพิ่มเติม

Checklist การให้คำปรึกษา DPIA (กรอกตัวอย่างและตรวจสอบ)

รายการตรวจสอบ	มี/ครบ (✓)	ไม่มี/ไม่ครบ (✗)	หมายเหตุ
1. มีรายละเอียดโครงการครบถ้วน	✓		รายละเอียดครบถ้วนดี

2. ระบุวัตถุประสงค์การประมวลผลข้อมูล	✓		วัตถุประสงค์ชัดเจน
3. ระบุประเภทข้อมูลส่วนบุคคล	✓		ข้อมูลที่เกี่ยวข้องครบถ้วน
4. วิเคราะห์ผลกระทบต่อเจ้าของข้อมูลแล้ว	✓		มีการประเมินความเสี่ยงอย่างละเอียด
5. เสนอแนวทางลดความเสี่ยงเบื้องต้น	✓		มาตรการป้องกันที่แนะนำเหมาะสม
6. มีแบบฟอร์ม DPIA แบบมาพร้อมคำปรึกษา	✓		แบบฟอร์มตามมาตรฐาน
7. ได้รับข้อเสนอแนะจาก DPO	✓		ข้อเสนอแนะครบถ้วนและชัดเจน
8. ผู้รับคำปรึกษาทำความเข้าใจข้อเสนอแนะ	✓		ผู้ขอคำปรึกษาเข้าใจและยอมรับข้อเสนอแนะ

สรุปผลการให้คำปรึกษา

จากการให้คำปรึกษาโครงการนี้ พบว่าการจัดทำ DPIA มีความครบถ้วนและเหมาะสม สามารถดำเนินการได้ตามขั้นตอน มีการประเมินความเสี่ยงและมาตรการป้องกันที่เหมาะสม และผู้ขอคำปรึกษาเข้าใจถึงข้อเสนอแนะต่าง ๆ เป็นอย่างดี

ชื่อ-นามสกุล DPO: นายปกรณ์ สุขสวัสดิ์

ลายเซ็น: วันที่: 4 มิถุนายน 2568

8.3.7 องค์กร มอบหมายความรับผิดชอบในการจัดทำ DPIA ให้กับพนักงานที่มีอำนาจในโครงการ เช่น หัวหน้าโครงการ หรือผู้จัดการ เป็นต้น

สิ่งที่ต้องทำ: องค์กร มอบหมายความรับผิดชอบในการจัดทำ DPIA ให้กับพนักงานที่มีอำนาจในโครงการ และมีเอกสารสนับสนุนชัดเจน

หลักฐาน: นโยบายกำหนดบุคลากรที่เกี่ยวข้องกับการประเมินความเสี่ยง
นโยบายการกำหนดหน้าที่แก่พนักงานประจำโครงการในการจัดทำรายงานการประเมินความเสี่ยง
รายงานการประเมินความเสี่ยง

รายงานผลพิจารณารายงานการประเมินความเสี่ยง
สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายกำหนดบุคลากรที่เกี่ยวข้องกับการประเมินความเสี่ยงข้อมูลส่วนบุคคล

นโยบายการมอบหมายความรับผิดชอบในการจัดทำ การประเมินความเสี่ยงข้อมูลส่วนบุคคล (DPIA)

วัตถุประสงค์:

เพื่อกำหนดบทบาทหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องในการจัดทำ การประเมินความเสี่ยงข้อมูลส่วนบุคคล (DPIA) ให้ชัดเจนและมีประสิทธิภาพ เพื่อให้การประเมินความเสี่ยงเป็นไปตามมาตรฐานและข้อกำหนดขององค์กร

ขอบเขต:

นโยบายนี้ใช้กับพนักงานทุกคนที่ได้รับมอบหมายให้รับผิดชอบในโครงการหรือกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

บทบาทและความรับผิดชอบ:

- หัวหน้าโครงการ/ผู้จัดการโครงการ: รับผิดชอบในการจัดทำ DPIA สำหรับโครงการภายใต้ความดูแลของตน
- พนักงานที่ได้รับมอบหมาย: ปฏิบัติตามขั้นตอนการจัดทำ DPIA และรายงานผลการประเมินต่อผู้บังคับบัญชาและ DPO
- เจ้าหน้าที่ DPO: ให้คำปรึกษาและตรวจสอบความถูกต้องของการจัดทำ DPIA

การดำเนินการ

- หัวหน้าโครงการต้องกำหนดบุคลากรที่รับผิดชอบในการจัดทำ DPIA ก่อนเริ่มโครงการ
- จัดให้มีการฝึกอบรมและให้คำแนะนำเกี่ยวกับวิธีการประเมินความเสี่ยงข้อมูลส่วนบุคคล
- รายงานผลการประเมินความเสี่ยงต้องถูกจัดทำและส่งให้ DPO ตรวจสอบภายในระยะเวลาที่กำหนด

2. นโยบายการกำหนดหน้าที่แก่พนักงานประจำโครงการในการจัดทำรายงานการประเมินความเสี่ยง นโยบายการกำหนดหน้าที่ในการจัดทำรายงานการประเมินความเสี่ยงข้อมูลส่วนบุคคล (DPIA) สำหรับ พนักงานประจำโครงการ

วัตถุประสงค์:

เพื่อกำหนดหน้าที่ของพนักงานประจำโครงการในการจัดทำรายงาน DPIA อย่างเป็นระบบและ
ครอบคลุมความเสี่ยงที่อาจเกิดขึ้น

หน้าที่ของพนักงานประจำโครงการ:

- ศึกษาข้อมูลและรายละเอียดของโครงการที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- รวบรวมข้อมูลที่เป็นสำหรับการประเมินความเสี่ยง
- จัดทำรายงาน DPIA โดยใช้แบบฟอร์มที่องค์กรกำหนด
- ส่งรายงานให้ DPO หรือผู้มีอำนาจตรวจสอบและให้คำแนะนำ
- ดำเนินการแก้ไขและปรับปรุงตามข้อเสนอแนะที่ได้รับ

ขั้นตอนการรายงาน:

- จัดทำรายงาน DPIA เบื้องต้นและส่งให้หัวหน้าโครงการตรวจสอบ
- ส่งต่อให้ DPO ตรวจสอบและรับคำแนะนำ
- นำข้อเสนอแนะไปปรับปรุงรายงานและจัดเก็บเอกสารให้ครบถ้วน

3. ตัวอย่างรายงานการประเมินความเสี่ยงข้อมูลส่วนบุคคล (DPIA Report)

รายงานการประเมินความเสี่ยงข้อมูลส่วนบุคคล (DPIA)

ชื่อโครงการ: ระบบบริหารจัดการลูกค้า (CRM System)

หัวหน้าโครงการ: นายวิทยา เกียรติคุณ

ผู้จัดทำรายงาน: นางสาวสุนิสา ศรีสุข

วันที่จัดทำ: 1 มิถุนายน 2568

รายละเอียดโครงการ:

ระบบบริหารจัดการลูกค้าเพื่อเก็บรวบรวมและวิเคราะห์ข้อมูลลูกค้าเพื่อปรับปรุงบริการ

ข้อมูลส่วนบุคคลที่เกี่ยวข้อง:

ชื่อ ที่อยู่ เบอร์โทรศัพท์ ประวัติการสั่งซื้อ

การประเมินความเสี่ยง:

- ความเสี่ยงที่ 1: การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ระดับความเสี่ยง: สูง
- มาตรการป้องกัน: การเข้ารหัสข้อมูลและระบบล็อกอิน 2 ชั้น
- ความเสี่ยงที่ 2: การเก็บข้อมูลเกินความจำเป็น
- ระดับความเสี่ยง: ปานกลาง
- มาตรการป้องกัน: กำหนดขอบเขตข้อมูลที่จำเป็นอย่างชัดเจน

สรุปและข้อเสนอแนะ:

ระบบมีความปลอดภัยในระดับที่เหมาะสม แต่ควรมีการอบรมพนักงานเกี่ยวกับการจัดการข้อมูลเพิ่มเติม

4. รายงานผลพิจารณารายงานการประเมินความเสี่ยง

รายงานผลการพิจารณา DPIA

โครงการ: ระบบบริหารจัดการลูกค้า (CRM System)

ผู้พิจารณา: นายปรกรณ์ สุขสวัสดิ์ (DPO)

วันที่พิจารณา: 3 มิถุนายน 2568

ผลการพิจารณา:

รายงาน DPIA มีความครบถ้วนและเหมาะสมกับมาตรฐานองค์กร มีการวิเคราะห์ความเสี่ยงอย่างละเอียดและมีมาตรการควบคุมที่เหมาะสม ข้อเสนอแนะเพิ่มเติมได้ถูกแจ้งให้ทีมโครงการทราบเพื่อปรับปรุงต่อไป

ลงชื่อ:

(นายปรกรณ์ สุขสวัสดิ์)

วันที่: 3 มิถุนายน 2568

8.4.1 องค์กรมีเทมเพลต/แบบฟอร์มของ DPIA ที่เป็นมาตรฐาน มีโครงสร้างที่ชัดเจน (Well-Structured DPIA Template) และเป็นภาษาที่เข้าใจได้โดยง่าย

สิ่งที่ต้องทำ: องค์กรมีเทมเพลต/แบบฟอร์มของ DPIA ที่เป็นมาตรฐาน มีโครงสร้างที่ชัดเจน (Well-Structured DPIA Template) และเป็นภาษาที่เข้าใจได้โดยง่าย รวมถึงมีการสนับสนุนช่วยเหลือจาก DPO

หลักฐาน: นโยบายการจัดทำแบบฟอร์มการประเมินความเสี่ยง
แบบฟอร์มการประเมินความเสี่ยง
ประกาศตารางนัดให้คำปรึกษาหรือช่องทางให้คำปรึกษา

สภาพบังคับ: กฎหมายไม่ได้กำหนด

นโยบายการจัดทำแบบฟอร์มการประเมินความเสี่ยงข้อมูลส่วนบุคคล (DPIA)

วัตถุประสงค์

กำหนดแนวทางและมาตรฐานในการจัดทำแบบฟอร์มการประเมินความเสี่ยงข้อมูลส่วนบุคคล (DPIA) ที่มีโครงสร้างชัดเจน เข้าใจง่าย และใช้เป็นเครื่องมือในการประเมินความเสี่ยงอย่างเป็นระบบ

ขอบเขต

ใช้สำหรับทุกโครงการหรือกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในองค์กร

นโยบาย

- องค์กรจะจัดทำและใช้งานแบบฟอร์ม DPIA ที่ได้รับการออกแบบให้มีโครงสร้างชัดเจน และภาษาที่เข้าใจง่าย
- แบบฟอร์ม DPIA ต้องครอบคลุมข้อมูลที่จำเป็นทั้งหมดตามมาตรฐานสากลและแนวทางปฏิบัติที่ดี
- DPO จะทำหน้าที่ให้คำปรึกษาและสนับสนุนในการใช้งานแบบฟอร์ม DPIA เพื่อให้การประเมินความเสี่ยงเป็นไปอย่างถูกต้องและครบถ้วน
- องค์กรจะทบทวนและปรับปรุงแบบฟอร์ม DPIA อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับข้อกำหนดและความเปลี่ยนแปลงในสภาพแวดล้อมการทำงาน

ตัวอย่างแบบฟอร์มการประเมินความเสี่ยงข้อมูลส่วนบุคคล (DPIA)

1. ข้อมูลทั่วไปของโครงการ

ชื่อโครงการ: โครงการพัฒนาระบบลงทะเบียนผู้เข้าร่วมสัมมนาออนไลน์

ผู้รับผิดชอบโครงการ: นายสมชาย ใจดี

วันที่จัดทำ: 1 มิถุนายน 2568

2. วัตถุประสงค์ของการเก็บข้อมูลส่วนบุคคล

เพื่อรวบรวมข้อมูลผู้เข้าร่วมสัมมนาออนไลน์ ใช้สำหรับการจัดการการเข้าใช้งาน และส่งใบประกาศนียบัตรหลังจบสัมมนา

3. ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง

- ชื่อ-นามสกุล
- อีเมล
- เบอร์โทรศัพท์
- ข้อมูลบริษัท/องค์กร
- ประวัติการเข้าร่วมสัมมนาก่อนหน้า

4. การวิเคราะห์ความเสี่ยง

ความเสี่ยงที่อาจเกิดขึ้น	ระดับความเสี่ยง	มาตรการควบคุมและลดความเสี่ยง
ข้อมูลส่วนบุคคลรั่วไหลจากการโจมตีระบบ (Hacking)	สูง	ใช้ระบบรักษาความปลอดภัยระดับสูง (Firewall Encryption)
การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	ปานกลาง	กำหนดสิทธิ์การเข้าถึงเฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง
ข้อมูลถูกเก็บไว้นานเกินความจำเป็น	ต่ำ	กำหนดนโยบายการเก็บรักษาข้อมูลและลบข้อมูลที่ไม่จำเป็น
ความผิดพลาดจากการป้อนข้อมูลหรือการจัดการข้อมูล	ต่ำ	ฝึกอบรมพนักงานและตรวจสอบความถูกต้องของข้อมูลเป็นประจำ

5. การปรึกษาหารือกับ DPO หรือเจ้าหน้าที่ที่เกี่ยวข้อง

วันที่ปรึกษา: 5 มิถุนายน 2568

รายละเอียดข้อเสนอแนะ:

- แนะนำให้เพิ่มระบบยืนยันตัวตนสองขั้นตอน (2FA) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- กำหนดระยะเวลาการเก็บรักษาข้อมูลไม่เกิน 2 ปีหลังจบโครงการ
- จัดอบรมพนักงานเกี่ยวกับมาตรการความปลอดภัยข้อมูลและนโยบายคุ้มครองข้อมูลส่วนบุคคล

6. ข้อสรุปและข้อเสนอแนะ

- โครงการนี้มีความเสี่ยงที่สามารถบริหารจัดการได้ โดยการเพิ่มมาตรการความปลอดภัยตามคำแนะนำของ DPO และการทบทวนมาตรการอย่างสม่ำเสมอ
- แนะนำให้ดำเนินการตามแผนและกำหนดบทบาทความรับผิดชอบที่ชัดเจนในแต่ละส่วน

ลงชื่อผู้จัดทำ: นายสมชาย ใจดี

วันที่: 10 มิถุนายน 2568

8.4.2 DPIA มีรายละเอียดอย่างน้อยดังนี้

6. ลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผล
7. การประเมินความจำเป็น ความได้สัดส่วน และมาตรการการปฏิบัติตาม
8. การระบุและประเมินความเสี่ยงต่อเจ้าของข้อมูลส่วนบุคคล
9. มาตรการเพื่อลดความเสี่ยงเหล่านั้น
10. สิ่งที่ต้องทำ: องค์กรมีการจัดทำ DPIA และมีรายละเอียดครบถ้วน
11. หลักฐาน: นโยบายการประเมินความเสี่ยง
12. คู่มือการจัดทำรายงานการประเมินความเสี่ยงหรือแบบประเมินความเสี่ยง
13. รายงานการประเมินความเสี่ยงหรือแบบประเมินความเสี่ยง
14. สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการประเมินความเสี่ยง

วัตถุประสงค์

เพื่อกำหนดแนวทางและกรอบการดำเนินการในการประเมินความเสี่ยงเกี่ยวกับข้อมูลส่วนบุคคลอย่างครบถ้วน โดยมีเป้าหมายลดผลกระทบด้านความเป็นส่วนตัว และรักษาสีทธิของเจ้าของข้อมูล

ขอบเขต

นโยบายนี้ครอบคลุมการจัดทำรายงานการประเมินผลกระทบด้านความเป็นส่วนตัว (DPIA) สำหรับทุกโครงการหรือกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลทุกประเภท

แนวทางปฏิบัติ

- องค์กรต้องดำเนินการจัดทำ DPIA ก่อนเริ่มโครงการหรือการเปลี่ยนแปลงที่สำคัญในระบบหรือกระบวนการที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- DPIA ต้องครอบคลุมลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผล
- ต้องประเมินความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล
- ต้องระบุและประเมินความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลอย่างชัดเจน
- ต้องกำหนดมาตรการที่เหมาะสมเพื่อลดความเสี่ยงและตรวจสอบประสิทธิภาพของมาตรการนั้นอย่างสม่ำเสมอ
- ต้องปรึกษา DPO และผู้มีส่วนเกี่ยวข้องภายในองค์กรในทุกขั้นตอนการจัดทำ DPIA
- รายงาน DPIA ต้องจัดเก็บและดูแลรักษาเป็นเอกสารเพื่อการตรวจสอบภายในและการรายงานต่อหน่วยงานกำกับดูแล

2. คู่มือการจัดทำรายงานการประเมินความเสี่ยง (DPIA)

ส่วนที่ 1: ข้อมูลทั่วไปของโครงการ

- ชื่อโครงการ
- ผู้รับผิดชอบโครงการ
- วันที่เริ่มและวันที่จัดทำ DPIA
- วัตถุประสงค์ของการประมวลผลข้อมูล

ส่วนที่ 2: ลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผล

- รายละเอียดประเภทข้อมูลที่ประมวลผล
- ขอบเขตของการประมวลผลข้อมูล (ระบุหน่วยงานหรือระบบที่เกี่ยวข้อง)
- บริบทของโครงการ เช่น การใช้ข้อมูลกับผู้ร่วมโครงการ ภายนอกองค์กร ฯลฯ
- วัตถุประสงค์การประมวลผลข้อมูลที่ชัดเจน

ส่วนที่ 3: การประเมินความจำเป็นและความได้สัดส่วนของการประมวลผล

- เหตุผลที่จำเป็นต้องใช้ข้อมูลส่วนบุคคลในโครงการ
- การพิจารณาความเหมาะสมในการประมวลผลข้อมูลในแง่ของสิทธิและเสรีภาพของเจ้าของข้อมูล

ส่วนที่ 4: การระบุและประเมินความเสี่ยง

- ระบุความเสี่ยงที่อาจเกิดขึ้นต่อเจ้าของข้อมูล เช่น การรั่วไหล การเข้าถึงโดยไม่ได้รับอนุญาต การเก็บรักษาข้อมูลไม่ปลอดภัย ฯลฯ
- ประเมินระดับความรุนแรงของแต่ละความเสี่ยง (สูง/กลาง/ต่ำ)

ส่วนที่ 5: มาตรการเพื่อลดความเสี่ยง

- มาตรการด้านเทคนิค เช่น การเข้ารหัสข้อมูล การควบคุมการเข้าถึง
- มาตรการด้านการบริหาร เช่น การอบรมพนักงาน การจัดทำนโยบายภายใน
- การตรวจสอบและประเมินผลมาตรการที่นำมาใช้

ส่วนที่ 6: การสรุปผลและข้อเสนอแนะ

- สรุปความเสี่ยงโดยรวม
- ข้อเสนอแนะในการบริหารจัดการความเสี่ยง
- การติดตามผลและทบทวน DPIA

3. ตัวอย่างรายงานการประเมินความเสี่ยง (DPIA)

ชื่อโครงการ: ระบบลงทะเบียนพนักงานเข้าร่วมอบรมภายในองค์กร

ผู้รับผิดชอบ: นางสาวปรียา สายสว่าง

วันที่จัดทำ: 10 มิถุนายน 2568

1. ลักษณะ ขอบเขต บริบท และวัตถุประสงค์

ระบบนี้ถูกพัฒนาขึ้นเพื่อเก็บข้อมูลส่วนบุคคลของพนักงานที่เข้าร่วมอบรมภายในองค์กร เพื่อใช้ติดตามการอบรมและออกใบรับรองการอบรมให้กับพนักงาน ข้อมูลที่เก็บประกอบด้วย ชื่อ-นามสกุล เลขบัตรประชาชน อีเมล และข้อมูลการเข้าร่วมอบรม

2. การประเมินความจำเป็นและความได้สัดส่วน

ข้อมูลที่เก็บมีความจำเป็นต่อการบริหารจัดการอบรม และเพื่อประโยชน์ในการยืนยันตัวตนและติดตามผลการอบรม โดยมีการจำกัดการเข้าถึงข้อมูลเฉพาะเจ้าหน้าที่ฝ่ายทรัพยากรบุคคลที่เกี่ยวข้องเท่านั้น

3. การระบุและประเมินความเสี่ยง

ความเสี่ยง	ระดับความเสี่ยง	มาตรการลดความเสี่ยง
ข้อมูลรั่วไหลจากการโจมตีระบบ	สูง	ใช้ระบบป้องกันภัยคุกคามทางไซเบอร์ และเข้ารหัสข้อมูล
การเข้าถึงโดยไม่ได้รับอนุญาต	ปานกลาง	กำหนดสิทธิ์เข้าถึงและมีระบบล็อกการใช้งาน

การเก็บข้อมูลเกินความจำเป็น	ต่ำ	กำหนดระยะเวลาการเก็บข้อมูลตามนโยบายขององค์กร
4. มาตรการเพื่อลดความเสี่ยง – ใช้ระบบล็อกอินสองชั้น (2FA) – จัดอบรมพนักงานด้านความปลอดภัยข้อมูล – ตรวจสอบและทบทวนระบบเป็นประจำทุก 6 เดือน 5. สรุปและข้อเสนอแนะ โครงการนี้มีความเสี่ยงที่สามารถบริหารจัดการได้ด้วยมาตรการที่กำหนดไว้ แนะนำให้ดำเนินการทบทวนมาตรการอย่างสม่ำเสมอและอบรมพนักงานอย่างต่อเนื่อง		

8.4.3 DPIA กำหนดความสัมพันธ์และแสดงทิศทางการไหลเวียนของข้อมูลระหว่างผู้ควบคุมข้อมูลส่วนบุคคล

บุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคล และระบบอย่างชัดเจน

สิ่งที่ต้องทำ: องค์กรจัดทำ DPIA กำหนดความสัมพันธ์และแสดงทิศทางการไหลเวียนของข้อมูลระหว่างผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคล และระบบอย่างชัดเจน

หลักฐาน: นโยบายกำหนดความสัมพันธ์และการไหลเวียนของข้อมูลระหว่างผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคล
ทะเบียนจัดการความเสี่ยง
หนังสือรายงานความเสี่ยงที่จะก่อให้เกิดผลกระทบแก่เจ้าของข้อมูลส่วนบุคคล
หนังสือแจ้งความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายกำหนดความสัมพันธ์และการไหลเวียนของข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดแนวทางและกรอบการจัดการความสัมพันธ์ รวมถึงการไหลเวียนของข้อมูลส่วนบุคคล อย่างชัดเจนระหว่างผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคล และระบบที่เกี่ยวข้อง เพื่อให้การประมวลผลข้อมูลเป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคล และลดความเสี่ยงที่อาจเกิดขึ้นจากการจัดการข้อมูล

ขอบเขต

นโยบายนี้ครอบคลุมถึงการจัดการข้อมูลส่วนบุคคลทุกประเภทที่อยู่ภายใต้ความรับผิดชอบขององค์กร ตั้งแต่การเก็บรวบรวม การใช้ การเปิดเผยข้อมูล การถ่ายโอนข้อมูล ไปจนถึงการลบข้อมูล

แนวทางปฏิบัติ

- กำหนดบทบาทและหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลให้ชัดเจน
- จัดทำแผนผังหรือแผนภูมิแสดงทิศทางการไหลเวียนของข้อมูลระหว่างผู้เกี่ยวข้องทั้งหมด เพื่อให้เห็นภาพรวมการไหลของข้อมูลอย่างชัดเจน
- กำหนดมาตรการควบคุมการเข้าถึงข้อมูลในแต่ละจุดการไหลเวียน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- บันทึกและตรวจสอบการถ่ายโอนข้อมูลให้สามารถตรวจสอบย้อนหลังได้
- ให้ความรู้และอบรมพนักงานเกี่ยวกับความสัมพันธ์และการจัดการข้อมูลส่วนบุคคลอย่างถูกต้อง

2. ทะเบียนจัดการความเสี่ยง (Risk Management Register)

ลำดับ	รายการความเสี่ยง	ผู้รับผิดชอบ	ผลกระทบต่อเจ้าของข้อมูล	มาตรการควบคุม	สถานะการดำเนินการ
1	การส่งข้อมูลระหว่างหน่วยงานที่ไม่มีการเข้ารหัส	ฝ่าย IT	ข้อมูลรั่วไหล	ใช้การเข้ารหัสข้อมูลในการส่งข้อมูล	ดำเนินการแล้ว
2	การมอบหมายผู้ประมวลผลข้อมูลที่ไม่ผ่านการอบรม	ฝ่ายทรัพยากรบุคคล	การจัดการข้อมูลผิดพลาด	กำหนดเกณฑ์การอบรมและติดตามผลการอบรม	อยู่ระหว่างดำเนินการ
3	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตในระบบฐานข้อมูล	ฝ่ายระบบ	ข้อมูลถูกแก้ไขหรือลบโดยไม่ถูกต้อง	กำหนดสิทธิ์การเข้าถึงข้อมูลและตรวจสอบล็อก	ดำเนินการแล้ว

3. หนังสือรายงานความเสี่ยงที่จะก่อให้เกิดผลกระทบแก่เจ้าของข้อมูลส่วนบุคคล

เรื่อง รายงานความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคล

เรียน [ผู้บริหาร/หน่วยงานที่เกี่ยวข้อง]

ตามที่องค์กรได้ดำเนินการจัดทำรายงานการประเมินผลกระทบด้านความเป็นส่วนตัว (DPIA) สำหรับโครงการ [ชื่อโครงการ] พบว่ามีความเสี่ยงที่อาจส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในประเด็น ดังนี้:

- การถ่ายโอนข้อมูลระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลที่อาจไม่ได้รับการป้องกันที่เหมาะสม
- ความไม่ชัดเจนในการกำหนดบทบาทความรับผิดชอบของผู้เกี่ยวข้องทำให้เกิดความล่าช้าในการจัดการข้อมูล
- การขาดระบบบันทึกการไหลเวียนของข้อมูลที่สามารถตรวจสอบย้อนหลังได้

จึงขอให้พิจารณาและอนุมัติมาตรการลดความเสี่ยงตามข้อเสนอในรายงาน เพื่อให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างปลอดภัยและถูกต้องตามหลักกฎหมาย

ขอแสดงความนับถือ

[ชื่อผู้รายงาน]

[ตำแหน่ง]

[วันที่]

4. หนังสือแจ้งความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล

เรื่อง แจ้งความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล

เรียน [ผู้เกี่ยวข้อง]

ด้วยองค์กรได้พบความเสี่ยงที่อาจก่อให้เกิดการละเมิดข้อมูลส่วนบุคคลในโครงการ [ชื่อโครงการ] ซึ่งมีรายละเอียดดังนี้:

ความเสี่ยง: การส่งข้อมูลผ่านระบบที่ไม่มีการเข้ารหัส

ผลกระทบ: ข้อมูลอาจรั่วไหลไปยังบุคคลที่ไม่เกี่ยวข้อง

มาตรการที่ดำเนินการ: กำหนดให้มีการเข้ารหัสข้อมูลในทุกจุดที่มีการถ่ายโอนข้อมูล และอบรมพนักงานเกี่ยวกับการรักษาความปลอดภัยข้อมูล

จึงขอแจ้งให้หน่วยงานรับทราบเพื่อดำเนินการควบคุมและติดตามความเสี่ยงอย่างใกล้ชิด

ขอแสดงความนับถือ

[ชื่อผู้แจ้ง]

[ตำแหน่ง]

[วันที่]

8.4.4 DPIA ระบุมาตรการที่สามารถนำไปใช้เพื่อจำกัด บรรเทา หรือลดความเสี่ยงสูง

สิ่งที่ต้องทำ: องค์กรมีการจัดทำ DPIA และระบุมาตรการที่สามารถนำไปใช้เพื่อจำกัด บรรเทา หรือลด ความเสี่ยงสูง

หลักฐาน: นโยบายการจัดให้มีมาตรการจำกัด บรรเทา หรือ ลดความเสี่ยงสูงในการประเมินความเสี่ยง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการจัดให้มีมาตรการจำกัด บรรเทา หรือ ลดความเสี่ยงสูงในการประเมินความเสี่ยง

วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการที่ชัดเจนในการจำกัด บรรเทา หรือ ลดความเสี่ยงสูงที่อาจ เกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล โดยมุ่งเน้นการป้องกันและลดผลกระทบที่อาจเกิดกับเจ้าของ ข้อมูลส่วนบุคคลให้น้อยที่สุด

ขอบเขต

นโยบายนี้ครอบคลุมการประเมินและบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลในทุกโครงการ และกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลขององค์กร

แนวทางปฏิบัติ

- การระบุความเสี่ยงสูงที่ส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- การกำหนดมาตรการป้องกันความเสี่ยงที่เหมาะสมและมีประสิทธิภาพ เช่น การเข้ารหัสข้อมูล การ จำกัดการเข้าถึงข้อมูล การอบรมพนักงาน และการใช้เทคโนโลยีที่ปลอดภัย
- การติดตามและประเมินผลมาตรการที่นำมาใช้เป็นระยะ เพื่อให้มั่นใจว่าสามารถลดความเสี่ยงได้ อย่างมีประสิทธิภาพ
- การจัดทำรายงานสรุปมาตรการและผลการดำเนินงานเพื่อเสนอผู้บริหารและผู้เกี่ยวข้อง
- การปรับปรุงมาตรการตามผลการติดตามและการเปลี่ยนแปลงในสภาพแวดล้อมการประมวลผล ข้อมูล

8.4.5 องค์กรมีการบันทึกการดำเนินการตาม DPIA พร้อมด้วยการควบคุมโดยเอกสารที่เหมาะสม

(appropriate document controls) และมีการตรวจสอบเป็นระยะ ๆ เพื่อให้แน่ใจว่ากระบวนการนั้น เป็นข้อมูลล่าสุด

- สิ่งที่ต้องทำ: องค์กรมีการตรวจสอบการปฏิบัติตามรายงานการประเมินความเสี่ยง รวมถึงมีการบันทึกเป็นเอกสารอย่างชัดเจน และมีการตรวจสอบเป็นระยะ ๆ เพื่อให้แน่ใจว่ากระบวนการนั้นเป็นข้อมูลล่าสุด
- หลักฐาน: นโยบายการบันทึกการดำเนินการตามรายงานการประเมินความเสี่ยงและการตรวจสอบการประเมินความเสี่ยง
บันทึกการดำเนินการตามรายงานการประเมินความเสี่ยง
รายงานผลการตรวจสอบการปฏิบัติตามรายงานการประเมินความเสี่ยง
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

นโยบายการบันทึกการดำเนินการตามรายงานการประเมินความเสี่ยงและการตรวจสอบการประเมินความเสี่ยง

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบันทึกและควบคุมเอกสารการดำเนินการตามรายงานการประเมินความเสี่ยง (DPIA) รวมถึงการตรวจสอบและทบทวนข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่ากระบวนการและข้อมูลที่เกี่ยวข้องเป็นปัจจุบันและสอดคล้องกับข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล

ขอบเขต

นโยบายนี้ครอบคลุมการจัดการเอกสารและรายงานที่เกี่ยวข้องกับการประเมินความเสี่ยงและการดำเนินการตาม DPIA ในทุกหน่วยงานที่เกี่ยวข้อง

แนวทางปฏิบัติ

- จัดทำและบันทึกข้อมูลการดำเนินการตามรายงานการประเมินความเสี่ยงในระบบจัดเก็บเอกสารที่ปลอดภัยและสามารถติดตามตรวจสอบได้
- กำหนดผู้รับผิดชอบในการดูแลและควบคุมเอกสารที่เกี่ยวข้องกับ DPIA เพื่อให้มีการบันทึกและเก็บรักษาอย่างเหมาะสม
- กำหนดระยะเวลาการตรวจสอบและทบทวนรายงาน DPIA อย่างน้อยปีละ 1 ครั้ง หรือเมื่อต้องมีการเปลี่ยนแปลงกระบวนการประมวลผลข้อมูลส่วนบุคคล
- จัดทำรายงานผลการตรวจสอบการปฏิบัติตามรายงาน DPIA และจัดส่งให้ผู้บริหารและหน่วยงานที่เกี่ยวข้องเพื่อพิจารณาดำเนินการปรับปรุงแก้ไข
- บันทึกและจัดเก็บผลการตรวจสอบให้เป็นหลักฐานในการปฏิบัติงานและตรวจสอบภายหลัง

8.4.6 องค์การบันทึกคำแนะนำของ DPO และรายละเอียดการให้คำปรึกษาอื่น ๆ ของ DPO เกี่ยวกับ DPIA ดังกล่าว

- สิ่งที่ต้องทำ: องค์การมีนโยบายการจัดให้มีการให้คำแนะนำและรายละเอียดการให้คำปรึกษาอื่น ๆ และมีการปฏิบัติตามนโยบายดังกล่าว รวมถึงมีเอกสารครบถ้วน
- หลักฐาน: นโยบายการจัดให้มีการบันทึกคำแนะนำด้านการจัดทำรายงานการประเมินความเสี่ยงของ DPO
บันทึกการให้คำปรึกษาด้านการจัดทำการประเมินความเสี่ยงหรือแบบฟอร์มการประเมินความเสี่ยง
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการจัดให้มีการบันทึกคำแนะนำด้านการจัดทำรายงานการประเมินความเสี่ยงของ DPO

วัตถุประสงค์

เพื่อกำหนดแนวทางการให้คำแนะนำและการบันทึกรายละเอียดการให้คำปรึกษาของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เกี่ยวกับการจัดทำรายงานการประเมินความเสี่ยง (DPIA) ให้เป็นระบบและมีหลักฐานชัดเจน เพื่อสนับสนุนการปฏิบัติตามกฎหมายและนโยบายขององค์กร

ขอบเขต

นโยบายนี้ครอบคลุมการให้คำแนะนำและการบันทึกข้อมูลคำปรึกษาของ DPO ต่อหน่วยงานและบุคลากรที่เกี่ยวข้องกับการจัดทำ DPIA ทุกกรณี

แนวทางปฏิบัติ

- DPO จะต้องจัดให้มีการบันทึกรายละเอียดการให้คำปรึกษา เช่น วัน เวลา ผู้เข้ารับคำปรึกษา เนื้อหาของคำแนะนำและข้อสังเกตที่เกี่ยวข้องกับ DPIA
- บันทึกคำปรึกษาเหล่านี้จะถูกเก็บรักษาในระบบจัดเก็บเอกสารที่มีความปลอดภัย และสามารถเรียกดูได้เมื่อต้องการตรวจสอบ
- ผู้รับคำปรึกษาควรมีการลงชื่อรับทราบและยืนยันความเข้าใจในคำแนะนำของ DPO
- จัดทำรายงานสรุปคำแนะนำสำคัญที่เกี่ยวข้องกับการประเมินความเสี่ยงเพื่อนำเสนอต่อผู้บริหาร และใช้ประกอบการปรับปรุงกระบวนการ
- การให้คำปรึกษาจะต้องเป็นไปอย่างต่อเนื่องและครบถ้วน ตอบสนองความต้องการของหน่วยงานและโครงการที่เกี่ยวข้อง

นโยบายการจัดให้มีการบันทึกคำแนะนำด้านการจัดทำรายงานการประเมินความเสี่ยงของ DPO

วัตถุประสงค์

เพื่อกำหนดแนวทางการให้คำแนะนำและการบันทึกรายละเอียดการให้คำปรึกษาของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เกี่ยวกับการจัดทำรายงานการประเมินความเสี่ยง (DPIA) ให้เป็นระบบและมีหลักฐานชัดเจน เพื่อสนับสนุนการปฏิบัติตามกฎหมายและนโยบายองค์กร

ขอบเขต

ครอบคลุมการให้คำแนะนำและการบันทึกข้อมูลคำปรึกษาของ DPO ต่อหน่วยงานและบุคลากรที่เกี่ยวข้องกับการจัดทำ DPIA ทุกกรณี

แนวทางปฏิบัติ

- DPO ต้องจัดให้มีการบันทึกรายละเอียดการให้คำปรึกษา เช่น วัน เวลา ผู้เข้ารับคำปรึกษา เนื้อหา คำแนะนำและข้อสังเกตที่เกี่ยวข้องกับ DPIA
- บันทึกคำปรึกษาเก็บในระบบเอกสารที่ปลอดภัยและสามารถเรียกดูได้เมื่อจำเป็น
- ผู้เข้ารับคำปรึกษาควรลงชื่อรับทราบและยืนยันความเข้าใจในคำแนะนำ
- จัดทำรายงานสรุปคำแนะนำสำคัญเพื่อนำเสนอต่อผู้บริหารและใช้ปรับปรุงกระบวนการ
- คำปรึกษาต้องเป็นไปอย่างต่อเนื่องและครบถ้วน

แบบฟอร์มบันทึกการให้คำปรึกษาด้านการจัดทำการประเมินความเสี่ยง (DPIA Consultation Record Form) พร้อมข้อมูลสมมติ

รายละเอียด	ข้อมูลตัวอย่าง
วันที่ให้คำปรึกษา	3 มิถุนายน 2568
ชื่อผู้ให้คำปรึกษา (DPO)	นางสาวพิชญา ศรีสุข
ชื่อผู้เข้ารับคำปรึกษา	นายกิตติชัย นิลวงศ์
ตำแหน่ง	ผู้จัดการโครงการ
หน่วยงาน	ฝ่ายพัฒนาระบบสารสนเทศ
หัวข้อคำปรึกษา	การจัดทำ DPIA สำหรับโครงการพัฒนาระบบฐานข้อมูลลูกค้า
เนื้อหาคำแนะนำ	1. ให้ระบุลักษณะและขอบเขตการเก็บข้อมูลส่วนบุคคลอย่างชัดเจน 2. ประเมินความจำเป็นและความได้สัดส่วนในการประมวลผลข้อมูล 3. แนะนำมาตรการควบคุมความปลอดภัยข้อมูล เช่น การเข้ารหัสและการควบคุมสิทธิ์เข้าถึง 4. ให้บันทึกและติดตามผลการประเมินความเสี่ยงอย่างสม่ำเสมอ

ข้อสังเกตและคำถาม	ผู้เข้ารับคำปรึกษาสงสัยเรื่องการจัดเก็บข้อมูลจากบุคคลที่สามและการแจ้งให้เจ้าของข้อมูลทราบ	
การดำเนินการที่แนะนำ	จัดทำ DPIA โดยเพิ่มรายละเอียดการจัดเก็บข้อมูลจากบุคคลที่สามและวิธีการแจ้งเจ้าของข้อมูล พร้อมจัดประชุมชี้แจงกับทีมโครงการ	
ลงชื่อผู้ให้คำปรึกษา	(ลงชื่อ) นางสาวพิชญา ศรีสุข	
ลงชื่อผู้รับคำปรึกษา	(ลงชื่อ) นายกิตติชัย นิลวงศ์	

8.5 การลดหรือจัดการความเสี่ยงตามที่ DPIA ระบุ และการตรวจสอบพบทวน DPIA

องค์กรดำเนินการที่เหมาะสมและมีประสิทธิภาพเพื่อลดหรือจัดการความเสี่ยงใด ๆ ที่ DPIA ระบุ และองค์กรมีการตรวจสอบพบทวน DPIA ได้

8.5.1 องค์กรต้องไม่เริ่มการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงจนกว่าจะมีมาตรการบรรเทาผลกระทบตามที่กำหนดใน DPIA

สิ่งที่ต้องทำ: องค์กรเริ่มการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง เมื่อมีมาตรการบรรเทาผลกระทบตามที่กำหนดใน DPIA ชัดเจนและมีเอกสารสนับสนุนครบถ้วน

หลักฐาน: นโยบายการกำหนดเงื่อนไขการประมวลผลข้อมูลส่วนบุคคลหรือเริ่มโครงการ / กิจกรรม
รายงานการประเมินความเสี่ยง
เอกสารหรือหลักฐานแสดงการพิจารณามาตรการบรรเทาผลกระทบด้านการประมวลผลข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ตัวอย่างเอกสารหลักฐานตามข้อ 8.5.1 การลดหรือจัดการความเสี่ยงตาม DPIA

1. นโยบายการกำหนดเงื่อนไขการประมวลผลข้อมูลส่วนบุคคล หรือเริ่มโครงการ/กิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (Data Processing Initiation Policy)

วัตถุประสงค์

เพื่อกำหนดกรอบและแนวทางปฏิบัติสำหรับการเริ่มต้นการประมวลผลข้อมูลส่วนบุคคลที่อาจมีความเสี่ยงสูง โดยมุ่งเน้นการประเมินความเสี่ยงและกำหนดมาตรการบรรเทาผลกระทบก่อนเริ่มดำเนินการ เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรฐานที่เกี่ยวข้อง

ขอบเขต

นโยบายนี้ใช้บังคับกับทุกโครงการ กิจกรรม หรือระบบที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล โดยเฉพาะโครงการที่จัดอยู่ในกลุ่ม “ความเสี่ยงสูง” ซึ่งต้องได้รับการจัดทำรายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) และมีการกำหนดมาตรการบรรเทาความเสี่ยงอย่างชัดเจน

ข้อกำหนดและแนวทางปฏิบัติ

- ก่อนเริ่มโครงการหรือกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล องค์กรจะต้องจัดทำรายงาน DPIA และประเมินความเสี่ยงที่อาจเกิดขึ้นอย่างละเอียด
- ต้องกำหนดมาตรการบรรเทาผลกระทบที่เหมาะสม และมีการตรวจสอบความเพียงพอของมาตรการดังกล่าวโดยเจ้าหน้าที่ DPO (Data Protection Officer) และคณะกรรมการบริหารความเสี่ยง
- ห้ามเริ่มดำเนินการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงจนกว่าจะได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจตามนโยบาย
- มีการบันทึกและเก็บรักษาเอกสารทั้งหมดที่เกี่ยวข้องกับการประเมินความเสี่ยงและมาตรการบรรเทาผลกระทบไว้ในระบบจัดการเอกสารขององค์กร
- มีการทบทวนและปรับปรุงรายงาน DPIA อย่างสม่ำเสมอไม่น้อยกว่าปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในโครงการหรือการประมวลผลข้อมูลส่วนบุคคล
- ตัวอย่างข้อความนโยบาย
- องค์กรให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดให้ทุกโครงการที่มีการประมวลผลข้อมูลส่วนบุคคลต้องผ่านการประเมินความเสี่ยงและการจัดทำ DPIA เพื่อระบุความเสี่ยงและมาตรการบรรเทาความเสี่ยงก่อนเริ่มดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง องค์กรจะไม่อนุญาตให้เริ่มประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงหากยังไม่มีมาตรการบรรเทาผลกระทบที่ได้รับการอนุมัติอย่างเหมาะสม

การบังคับใช้และความรับผิดชอบ

- ฝ่ายบริหารความเสี่ยงและฝ่าย DPO มีหน้าที่ตรวจสอบความครบถ้วนและความเหมาะสมของ DPIA ก่อนอนุมัติโครงการ
- หัวหน้าโครงการต้องรับผิดชอบจัดทำ DPIA และนำเสนอมาตรการบรรเทาความเสี่ยงตามนโยบาย
- ฝ่ายตรวจสอบภายในและผู้บริหารระดับสูงต้องกำกับดูแลการปฏิบัติตามนโยบายอย่างเคร่งครัด

2. รายงานการประเมินความเสี่ยง (DPIA Report)

ส่วนที่ 1: บทนำ

ชื่อโครงการ: ระบบจัดการข้อมูลลูกค้าออนไลน์

วันที่จัดทำ: 15 พฤษภาคม 2568

ผู้จัดทำ: ฝ่ายพัฒนาระบบสารสนเทศ

ผู้ตรวจสอบ: DPO และฝ่ายบริหารความเสี่ยง

ส่วนที่ 2: ขอบเขตและวัตถุประสงค์

ขอบเขตของการประมวลผลข้อมูล ได้แก่ ข้อมูลส่วนบุคคลของลูกค้า เช่น ชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ ข้อมูลการชำระเงิน และประวัติการสั่งซื้อ

วัตถุประสงค์ของการประมวลผลเพื่อให้บริการจัดการบัญชีลูกค้าและติดตามคำสั่งซื้อ

ส่วนที่ 3: การประเมินความเสี่ยง

ระบุความเสี่ยงสำคัญที่อาจเกิดขึ้น เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล ความไม่ถูกต้องของข้อมูล หรือการถูกโจมตีจากภายนอก วิเคราะห์โอกาสและผลกระทบของความเสี่ยงเหล่านี้

ส่วนที่ 4: มาตรการบรรเทาความเสี่ยง

- การเข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะส่งผ่านระบบ
- ใช้ระบบ Multi-factor Authentication สำหรับการเข้าถึงระบบ
- มีการจัดอบรมพนักงานเรื่องการรักษาความปลอดภัยข้อมูลและความรับผิดชอบตาม PDPA
- ตรวจสอบและบันทึกการเข้าใช้ระบบอย่างสม่ำเสมอ โดยมีการทำ audit log

ส่วนที่ 5: การสรุปและคำแนะนำ

มาตรการบรรเทาความเสี่ยงที่แนะนำได้รับการประเมินว่าเหมาะสมและมีประสิทธิภาพ แนะนำให้ทบทวน DPIA ทุก 12 เดือน หรือเมื่อมีการเปลี่ยนแปลงสำคัญในระบบหรือมาตรการความปลอดภัย

3. หนังสืออนุมัติมาตรการบรรเทาผลกระทบ (Approval Letter for Risk Mitigation Measures)

วันที่: 25 พฤษภาคม 2568

จาก: คณะกรรมการบริหารความเสี่ยง

ถึง: ฝ่ายพัฒนาระบบสารสนเทศ

เรื่อง: อนุมัติการดำเนินการมาตรการบรรเทาผลกระทบสำหรับระบบจัดการข้อมูลลูกค้าออนไลน์

ตามที่ฝ่ายพัฒนาระบบสารสนเทศได้จัดทำรายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และนำเสนอรายละเอียดมาตรการบรรเทาความเสี่ยงที่เกี่ยวข้องกับโครงการระบบจัดการข้อมูลลูกค้าออนไลน์ คณะกรรมการบริหารความเสี่ยงพิจารณาแล้วเห็นว่ามาตรการบรรเทาผลกระทบดังกล่าวมีความเหมาะสมและเพียงพอที่จะลดความเสี่ยงด้านความปลอดภัยของข้อมูลส่วนบุคคลให้อยู่ในระดับที่ยอมรับได้

ดังนั้น คณะกรรมการบริหารความเสี่ยงอนุมัติให้ฝ่ายพัฒนาระบบสารสนเทศเริ่มดำเนินโครงการได้ตามแผนที่เสนอ พร้อมมีข้อกำหนดให้มีการทบทวนและตรวจสอบความปลอดภัยอย่างต่อเนื่อง

ลงชื่อ

(นายสมชาย ใจดี)

ประธานคณะกรรมการบริหารความเสี่ยง

4. รายงานการตรวจสอบและทบทวน DPIA

รายงานการตรวจสอบ DPIA ประจำปี 2568

วันที่ตรวจสอบ: 10 ธันวาคม 2568

ผู้ตรวจสอบ: ฝ่ายตรวจสอบภายใน

โครงการ: ระบบจัดการข้อมูลลูกค้าออนไลน์

ผลการตรวจสอบ:

- การดำเนินการตาม DPIA เป็นไปตามนโยบายและข้อกำหนด
- มีการบันทึกการอบรมพนักงานเกี่ยวกับการรักษาความปลอดภัยข้อมูลครบถ้วน
- ไม่มีเหตุการณ์รั่วไหลหรือละเมิดข้อมูลส่วนบุคคลในรอบปีที่ผ่านมา
- แนะนำให้ทบทวนและอัปเดตมาตรการด้านความปลอดภัยตามเทคโนโลยีและภัยคุกคามที่เปลี่ยนแปลง

สรุป:

องค์กรได้ปฏิบัติตามข้อกำหนดการลดความเสี่ยงและมีการตรวจสอบทบทวน DPIA อย่างมีประสิทธิภาพ

5. แนวทางการจัดเก็บและการควบคุมเอกสาร DPIA

- เอกสาร DPIA ทั้งหมดถูกจัดเก็บในระบบจัดการเอกสารขององค์กรในรูปแบบดิจิทัล มีการสำรองข้อมูลอย่างสม่ำเสมอ

- แนะนำให้ทบทวน DPIA ทุก 12 เดือน หรือเมื่อมีการเปลี่ยนแปลงสำคัญในระบบหรือมาตรการความปลอดภัย

3. หนังสืออนุมัติมาตรการบรรเทาผลกระทบ (Approval Letter for Risk Mitigation Measures)

วันที่: 25 พฤษภาคม 2568

จาก: คณะกรรมการบริหารความเสี่ยง

ถึง: ฝ่ายพัฒนาระบบสารสนเทศ

เรื่อง: อนุมัติการดำเนินมาตรการบรรเทาผลกระทบสำหรับระบบจัดการข้อมูลลูกค้าออนไลน์

ตามที่ฝ่ายพัฒนาระบบสารสนเทศได้จัดทำรายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และนำเสนอรายละเอียดมาตรการบรรเทาความเสี่ยงที่เกี่ยวข้องกับโครงการระบบจัดการข้อมูลลูกค้าออนไลน์ คณะกรรมการบริหารความเสี่ยงพิจารณาแล้วเห็นว่ามาตรการบรรเทาผลกระทบดังกล่าวมีความเหมาะสมและเพียงพอที่จะลดความเสี่ยงด้านความปลอดภัยของข้อมูลส่วนบุคคลให้อยู่ในระดับที่ยอมรับได้

ดังนั้น คณะกรรมการบริหารความเสี่ยงอนุมัติให้ฝ่ายพัฒนาระบบสารสนเทศเริ่มดำเนินโครงการได้ตามแผนที่เสนอ พร้อมมีข้อกำหนดให้มีการทบทวนและตรวจสอบความปลอดภัยอย่างต่อเนื่อง

ลงชื่อ

(นายสมชาย ใจดี)

ประธานคณะกรรมการบริหารความเสี่ยง

4. รายงานการตรวจสอบและทบทวน DPIA

รายงานการตรวจสอบ DPIA ประจำปี 2568

วันที่ตรวจสอบ: 10 ธันวาคม 2568

ผู้ตรวจสอบ: ฝ่ายตรวจสอบภายใน

โครงการ: ระบบจัดการข้อมูลลูกค้าออนไลน์

ผลการตรวจสอบ

- การดำเนินมาตรการตาม DPIA เป็นไปตามนโยบายและข้อกำหนด
- มีการบันทึกการอบรมพนักงานเกี่ยวกับการรักษาความปลอดภัยข้อมูลครบถ้วน
- ไม่มีเหตุการณ์รั่วไหลหรือละเมิดข้อมูลส่วนบุคคลในรอบปีที่ผ่านมา
- แนะนำให้ทบทวนและอัปเดตมาตรการด้านความปลอดภัยตามเทคโนโลยีและภัยคุกคามที่เปลี่ยนแปลง

สรุป

องค์กรได้ปฏิบัติตามข้อกำหนดการลดความเสี่ยงและมีการตรวจสอบทบทวน DPIA อย่างมีประสิทธิภาพ

5. แนวทางการจัดเก็บและการควบคุมเอกสาร DPIA

- เอกสาร DPIA ทั้งหมดถูกจัดเก็บในระบบจัดการเอกสารขององค์กรในรูปแบบดิจิทัล มีการสำรองข้อมูลอย่างสม่ำเสมอ
- มีการกำหนดสิทธิ์การเข้าถึงเอกสารเฉพาะบุคลากรที่เกี่ยวข้องเท่านั้น
- กำหนดให้มีการตรวจสอบและทบทวนเอกสารไม่น้อยกว่าปีละครั้ง
- เอกสารทั้งหมดมีการบันทึกเวอร์ชันและประวัติการแก้ไขอย่างชัดเจน

สรุป

เอกสารเหล่านี้แสดงให้เห็นว่าองค์กรได้ดำเนินการตามข้อ 8.5.1 ของการลดหรือจัดการความเสี่ยงที่เกิดจากการประมวลผลข้อมูลส่วนบุคคลอย่างครบถ้วนและเป็นระบบ ประกอบด้วยนโยบายที่ชัดเจน รายงานการประเมินความเสี่ยงและมาตรการบรรเทา รายงานอนุมัติจากผู้บริหาร รวมถึงการตรวจสอบและทบทวนอย่างต่อเนื่อง ทั้งหมดนี้ช่วยให้องค์กรมั่นใจได้ว่าการประมวลผลข้อมูลส่วนบุคคลดำเนินการอย่างปลอดภัยและสอดคล้องกับกฎหมาย

8.5.2 องค์กรมีการกำหนดเวลาสำหรับการทบทวน DPIA เป็นประจำ หรือเมื่อลักษณะ ขอบเขต บริบท หรือวัตถุประสงค์ของการประมวลผลเปลี่ยนแปลงไป

สิ่งที่ต้องทำ: องค์กรมีการกำหนดเวลาสำหรับการทบทวน DPIA และปฏิบัติตามอย่างเคร่งครัด หรือมีการทบทวนเมื่อลักษณะ ขอบเขต บริบท หรือวัตถุประสงค์ของการประมวลผลเปลี่ยนแปลงไป

หลักฐาน: นโยบายการทบทวนการปฏิบัติตามผลการประเมินความเสี่ยงและทะเบียนจัดการความเสี่ยง รายงานการปฏิบัติตามผลการประเมินความเสี่ยงและทะเบียนจัดการความเสี่ยง

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย
 ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) ข้อ 5
 โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การกำหนดเวลาสำหรับการทบทวน DPIA

1. ความสำคัญของการทบทวน DPIA เป็นประจำ

การจัดทำรายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) เป็นกระบวนการที่ช่วยให้องค์กรประเมินและจัดการความเสี่ยงจากการประมวลผลข้อมูลส่วนบุคคลอย่างรอบคอบ แต่เนื่องจากข้อมูลส่วนบุคคลและกระบวนการประมวลผลมีการเปลี่ยนแปลงอยู่เสมอ เช่น การปรับปรุงระบบ เทคโนโลยี หรือเปลี่ยนแปลงกฎหมายที่เกี่ยวข้อง ทำให้องค์กรต้องมีการทบทวน DPIA อย่างสม่ำเสมอ เพื่อให้มั่นใจว่ามาตรการควบคุมและการบริหารความเสี่ยงยังคงมีประสิทธิภาพและเหมาะสมกับสถานการณ์ปัจจุบัน

2. ข้อกำหนดตามกฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ระบุว่า ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมและสม่ำเสมอ รวมถึงการทบทวนและปรับปรุงมาตรการดังกล่าวให้ทันสมัย
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) ข้อ 5 กำหนดให้องค์กรจัดให้มีการทบทวนผลการประเมินความเสี่ยงและมาตรการรักษาความมั่นคงปลอดภัยอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในกระบวนการประมวลผลข้อมูล
- โทษทางปกครอง กรณีฝ่าฝืนปฏิบัติตามมาตรา 37 อาจถูกปรับไม่เกิน 3 ล้านบาท ซึ่งเป็นบทลงโทษที่รุนแรงและส่งผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

3. แนวทางการกำหนดเวลาทบทวน DPIA

3.1 การทบทวนตามรอบเวลาที่กำหนด

องค์กรควรกำหนดรอบเวลาการทบทวน DPIA อย่างชัดเจน เช่น ทุก 6 เดือน หรือทุก 12 เดือน ขึ้นอยู่กับระดับความเสี่ยงและลักษณะของการประมวลผลข้อมูล โดยรอบเวลานี้ควรถูกบันทึกไว้ในนโยบายความมั่นคงปลอดภัยข้อมูล หรือคู่มือบริหารความเสี่ยง

ตัวอย่างข้อความในนโยบาย:

"องค์กรจะดำเนินการทบทวนรายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) อย่างน้อยปีละหนึ่งครั้ง เพื่อให้มั่นใจว่ามาตรการรักษาความมั่นคงปลอดภัยและการจัดการความเสี่ยงมีความเหมาะสมและทันสมัยอยู่เสมอ"

3.2 การทบทวนเมื่อลักษณะ ขอบเขต บริบท หรือวัตถุประสงค์ของการประมวลผลเปลี่ยนแปลง

นอกจากการทบทวนตามรอบเวลาที่กำหนดแล้ว องค์กรต้องจัดให้มีการทบทวนทันทีเมื่อพบการเปลี่ยนแปลงที่สำคัญในกระบวนการประมวลผลข้อมูล เช่น

- มีการนำเทคโนโลยีใหม่เข้ามาใช้
- ข้อมูลส่วนบุคคลที่ประมวลผลเพิ่มขึ้นหรือเปลี่ยนประเภทข้อมูล
- เปลี่ยนแปลงผู้รับข้อมูลหรือผู้ประมวลผลข้อมูลภายนอก
- มีเหตุการณ์ด้านความปลอดภัย เช่น การละเมิดข้อมูล (data breach)
- เปลี่ยนแปลงกฎหมายหรือแนวทางปฏิบัติที่เกี่ยวข้อง

4. ตัวอย่างเอกสารหลักฐานและแนวทางปฏิบัติ

4.1 นโยบายการทบทวน DPIA (Policy for DPIA Review)

เนื้อหาหลัก:

- กำหนดรอบเวลาการทบทวน DPIA เป็นระยะ (เช่น 6 เดือน หรือ 12 เดือน)
- กำหนดเงื่อนไขการทบทวนเมื่อมีการเปลี่ยนแปลงในลักษณะ ขอบเขต บริบท หรือวัตถุประสงค์ของการประมวลผลข้อมูล
- ระบุผู้รับผิดชอบในการทบทวน เช่น DPO หรือฝ่ายบริหารความเสี่ยง
- กำหนดขั้นตอนการบันทึกผลการทบทวน และวิธีจัดเก็บเอกสาร

4.2 ทะเบียนจัดการความเสี่ยง (Risk Management Register)

- ทะเบียนนี้จะบันทึกรายละเอียดเกี่ยวกับ DPIA ที่ดำเนินการ รวมถึง
- วันที่เริ่มต้นและวันที่กำหนดทบทวนครั้งต่อไป
- สถานะการทบทวนล่าสุดและผลการทบทวน
- หมายเหตุเกี่ยวกับการเปลี่ยนแปลงที่อาจกระทบต่อความเสี่ยง
- รายชื่อผู้รับผิดชอบในการดำเนินการแก้ไขปรับปรุงมาตรการ

4.3 รายงานการทบทวน DPIA

- หลังการทบทวน DPIA ควรมีรายงานสรุปผลทบทวนอย่างเป็นทางการ ระบุ
- วันที่และเหตุผลที่ทำการทบทวน
- ผลการประเมินความเสี่ยงหลังทบทวน
- มาตรการใหม่หรือการปรับปรุงมาตรการที่แนะนำ
- ผู้รับผิดชอบดำเนินการและกำหนดเวลาติดตามผล

5. ตัวอย่างข้อความในนโยบายการทบทวน DPIA

Text Copy Edit

นโยบายการทบทวนรายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

1. องค์กรกำหนดให้มีการทบทวนรายงาน DPIA อย่างน้อยปีละหนึ่งครั้ง โดยมีเป้าหมายเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและความสอดคล้องกับกฎหมาย PDPA
2. นอกจากการทบทวนตามรอบเวลาที่กำหนด องค์กรจะดำเนินการทบทวนทันทีเมื่อพบการเปลี่ยนแปลงที่สำคัญในลักษณะ ขอบเขต บริบท หรือวัตถุประสงค์ของการประมวลผลข้อมูล
3. การทบทวนจะดำเนินการโดยเจ้าหน้าที่ DPO ร่วมกับฝ่ายบริหารความเสี่ยง และมีการจัดทำรายงานผลทบทวนอย่างเป็นทางการ
4. ผลการทบทวนและเอกสารที่เกี่ยวข้องจะถูกบันทึกและจัดเก็บในทะเบียนจัดการความเสี่ยงเพื่อการติดตามและตรวจสอบในอนาคต

6. สรุปและความสำคัญ

การทบทวน DPIA เป็นประจำ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เป็นกระบวนการที่ช่วยให้ องค์กรสามารถตอบสนองต่อภัยคุกคามและความเสี่ยงใหม่ ๆ ที่อาจเกิดขึ้นได้อย่างทันเวลา ช่วยป้องกันการละเมิดข้อมูลและความเสียหายทางกฎหมาย นอกจากนี้ ยังเป็นการสร้างความมั่นใจแก่ผู้เกี่ยวข้องและเจ้าของข้อมูลว่าข้อมูลส่วนบุคคลได้รับการปกป้องอย่างมีประสิทธิภาพและต่อเนื่อง

8.5.3 องค์กรมีขั้นตอนในการปรึกษาผู้เชี่ยวชาญ หากไม่สามารถลดความเสี่ยงที่เหลืออยู่ได้

- สิ่งที่ต้องทำ: องค์กรมีขั้นตอนในการปรึกษาผู้เชี่ยวชาญ หากไม่สามารถลดความเสี่ยงที่เหลืออยู่ได้ และมีเอกสารหลักฐานสนับสนุนครบถ้วน
- หลักฐาน: นโยบายกำหนดขั้นตอนในการปรึกษาผู้เชี่ยวชาญ
สัญญาจ้างผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคล
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

ขั้นตอนการปรึกษาผู้เชี่ยวชาญ กรณีไม่สามารถลดความเสี่ยงที่เหลืออยู่ได้

1. ความหมายและความสำคัญของการปรึกษาผู้เชี่ยวชาญ

ในกระบวนการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยเฉพาะการดำเนินการตาม DPIA องค์กรจะต้องดำเนินการมาตรการต่าง ๆ เพื่อระบุและลดความเสี่ยงให้เหลือน้อยที่สุด แต่ในบางกรณี อาจพบว่าความเสี่ยงที่เหลืออยู่ (residual risk) ไม่สามารถบรรเทาได้ด้วยมาตรการภายในองค์กรเพียงอย่างเดียว ซึ่งความเสี่ยงดังกล่าวอาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลได้

ดังนั้น การปรึกษาผู้เชี่ยวชาญภายนอก หรือที่มีความรู้เฉพาะทางในด้านคุ้มครองข้อมูลส่วนบุคคล จึงเป็นขั้นตอนสำคัญที่ช่วยให้องค์กรสามารถประเมินความเสี่ยงและแนวทางจัดการได้อย่างถูกต้องและเหมาะสม ลดโอกาสในการเกิดปัญหาทางกฎหมาย หรือการละเมิดข้อมูลส่วนบุคคลที่รุนแรง และยังเป็นเครื่องมือสำคัญในการเพิ่มความน่าเชื่อถือและความโปร่งใสขององค์กร

2. แนวทางปฏิบัติและขั้นตอนการปรึกษาผู้เชี่ยวชาญ

2.1 การประเมินสถานการณ์ที่ต้องปรึกษา

- องค์กรควรกำหนดเกณฑ์หรือสถานการณ์ที่แสดงว่าความเสี่ยงที่เหลืออยู่ไม่สามารถลดได้ด้วย มาตรการที่มีอยู่ เช่น
- ความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลที่มีผลกระทบรุนแรง (เช่น ข้อมูลประเภทพิเศษ หรือ ข้อมูลสุขภาพ)
- มาตรการบรรเทาความเสี่ยงที่ใช้อยู่ไม่ได้ผล หรือมีข้อจำกัดทางเทคนิคและงบประมาณ
- การเกิดเหตุการณ์ละเมิดข้อมูล (data breach) ซ้ำ ๆ หรือมีแนวโน้มสูง
- มีความซับซ้อนด้านเทคนิคหรือกฎหมายที่ต้องการความเห็นจากผู้เชี่ยวชาญ
- ความเสี่ยงที่มีผลต่อความเชื่อมั่นของผู้มีส่วนได้ส่วนเสียอย่างรุนแรง

2.2 ขั้นตอนการปรึกษา

- **แจ้งเหตุและรวบรวมข้อมูล**
เจ้าหน้าที่หรือทีมที่รับผิดชอบการบริหารความเสี่ยงทำรายงานสรุปสถานการณ์ ความเสี่ยงที่ไม่สามารถลดได้ และมาตรการที่ดำเนินการไปแล้ว
- **เลือกผู้เชี่ยวชาญที่เหมาะสม**
ผู้เชี่ยวชาญควรมีความรู้และประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล กฎหมาย PDPA หรือมาตรฐานความมั่นคงปลอดภัยข้อมูล (เช่น DPO ที่ได้รับการรับรอง ที่ปรึกษาด้านกฎหมาย หรือผู้เชี่ยวชาญด้าน IT Security)
- **ทำสัญญาหรือข้อตกลงการให้บริการ**
ระบุขอบเขตงาน ความลับข้อมูล และเงื่อนไขความรับผิดชอบ เพื่อความชัดเจนและป้องกันข้อพิพาท

- **ดำเนินการปรึกษาและรับคำแนะนำ**
องค์กรส่งข้อมูลและเอกสารที่เกี่ยวข้องให้ผู้เชี่ยวชาญพิจารณา พร้อมรับฟังคำแนะนำ แนวทางแก้ไข หรือมาตรการเสริมที่ควรดำเนินการ
- **จัดทำรายงานผลการปรึกษา**
จัดทำรายงานสรุปคำแนะนำและแผนการดำเนินการที่เสนอโดยผู้เชี่ยวชาญ พร้อมระบุผู้รับผิดชอบ และกำหนดเวลาในการดำเนินการ
- **ติดตามผลและทบทวน**
ดำเนินการตามคำแนะนำและติดตามประสิทธิผลอย่างต่อเนื่อง รวมถึงบันทึกการทบทวนผลการดำเนินงานในทะเบียนความเสี่ยงหรือระบบบริหารข้อมูลส่วนบุคคล

3. เอกสารหลักฐานที่ควรมี

3.1 นโยบายกำหนดขั้นตอนในการปรึกษาผู้เชี่ยวชาญ

- ระบุหลักเกณฑ์และกระบวนการที่องค์กรใช้ในการตัดสินใจว่าควรปรึกษาผู้เชี่ยวชาญเมื่อใด
- ระบุบทบาทหน้าที่ผู้รับผิดชอบในกระบวนการนี้
- กำหนดการจัดเก็บและการรักษาความลับของข้อมูลที่ส่งให้ผู้เชี่ยวชาญ
- แนวทางการจัดการกับคำแนะนำที่ได้รับ

3.2 สัญญาจ้างผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคล

- ขอบเขตของงานและบริการที่จัดหา
- ระยะเวลาการให้บริการ
- ข้อตกลงเกี่ยวกับการรักษาความลับและความปลอดภัยของข้อมูล
- เงื่อนไขการยกเลิกและความรับผิดชอบของแต่ละฝ่าย

3.3 รายงานการปรึกษาและคำแนะนำ

- รายงานสรุปสถานการณ์และปัญหาที่พบ
- คำแนะนำโดยละเอียดของผู้เชี่ยวชาญ
- แผนการดำเนินงานและมาตรการที่ควรนำไปใช้
- การตอบรับและแผนติดตามผลขององค์กร

ตัวอย่างข้อความในนโยบายการปรึกษาผู้เชี่ยวชาญ

นโยบายการปรึกษาผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคล

1. องค์กรจะดำเนินการปรึกษาผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่ไม่สามารถลดความเสี่ยงที่เหลืออยู่ได้ด้วยมาตรการภายในองค์กร
2. การปรึกษาจะดำเนินการโดยเจ้าหน้าที่ที่รับผิดชอบ พร้อมจัดเตรียมข้อมูลและเอกสารที่เกี่ยวข้อง เพื่อให้คำแนะนำเป็นไปอย่างครบถ้วน
3. ผู้เชี่ยวชาญต้องมีความเชี่ยวชาญในกฎหมาย PDPA และมาตรฐานความมั่นคงปลอดภัยข้อมูล

4. องค์กรจะจัดทำสัญญาจ้างผู้เชี่ยวชาญโดยระบุขอบเขตงาน เงื่อนไขการรักษาความลับ และข้อตกลงความรับผิดชอบ

รายงานผลการปรึกษาจะถูกบันทึกและนำไปใช้ในการปรับปรุงมาตรการคุ้มครองข้อมูลส่วนบุคคลขององค์กรอย่างต่อเนื่อง

5. ข้อดีและประโยชน์ของการปรึกษาผู้เชี่ยวชาญ

- ช่วยให้องค์กรมีมุมมองและความรู้เชิงลึกในประเด็นที่ซับซ้อน
- ลดความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการที่ไม่ถูกต้องหรือไม่ครบถ้วน
- เพิ่มความน่าเชื่อถือและสร้างความมั่นใจให้กับเจ้าของข้อมูลและหน่วยงานกำกับดูแล
- ลดโอกาสถูกปรับโทษหรือเกิดเหตุการณ์ละเมิดข้อมูลที่ร้ายแรง
- ช่วยพัฒนาศักยภาพและความรู้ของบุคลากรในองค์กร

6. สรุป

แม้ว่ากฎหมาย PDPA จะไม่ได้ระบุข้อบังคับชัดเจนเกี่ยวกับการปรึกษาผู้เชี่ยวชาญเมื่อมีความเสี่ยงที่เหลือนอยู่ แต่การมีขั้นตอนและนโยบายที่ชัดเจนในการดำเนินการเรื่องนี้ถือเป็นแนวทางปฏิบัติที่ดี (best practice) และเป็นปัจจัยสำคัญในการบริหารความเสี่ยงข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพและครบถ้วน องค์กรควรจัดเตรียมเอกสารและระบบการติดตามผลที่เหมาะสมเพื่อให้สามารถตรวจสอบและพัฒนาแนวทางป้องกันได้อย่างต่อเนื่อง

8.5.4 องค์กรบูรณาการผลลัพธ์จาก DPIA เข้ากับแผนงาน แผนปฏิบัติการโครงการ และบันทึกความเสี่ยงที่เกี่ยวข้อง รวมถึงทะเบียนจัดการความเสี่ยง

สิ่งที่ต้องทำ: องค์กรมีการบูรณาการผลลัพธ์จาก DPIA เข้ากับแผนงาน แผนปฏิบัติการโครงการ และบันทึกความเสี่ยงที่เกี่ยวข้อง รวมถึงทะเบียนจัดการความเสี่ยง และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการเผยแพร่รายงานการประเมินความเสี่ยง
รายงานการประเมินความเสี่ยง (ฉบับเผยแพร่ โดยปรากฏรายละเอียดเกี่ยวกับการพิจารณาผลกระทบด้านข้อมูลส่วนบุคคล)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การบูรณาการผลลัพธ์จาก DPIA เข้ากับแผนงาน แผนปฏิบัติการ และระบบบริหารความเสี่ยงขององค์กร

1. ความหมายและความสำคัญของการบูรณาการผลลัพธ์ DPIA

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) เป็นกระบวนการที่ช่วยให้องค์กรเข้าใจความเสี่ยงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในแต่ละโครงการหรือกิจกรรมอย่างละเอียด โดยผลลัพธ์ของ DPIA จะระบุความเสี่ยงที่มีต่อสิทธิและเสรีภาพของเจ้าของข้อมูล รวมถึงมาตรการที่องค์กรต้องดำเนินการเพื่อบรรเทาความเสี่ยงเหล่านั้น

การบูรณาการผลลัพธ์จาก DPIA เข้ากับแผนงานและแผนปฏิบัติการโครงการ เป็นสิ่งจำเป็นเพื่อให้แน่ใจว่า

- มาตรการป้องกันและลดความเสี่ยงถูกนำไปปฏิบัติอย่างจริงจังและมีระบบ
- การบริหารความเสี่ยงของข้อมูลส่วนบุคคลถูกจัดการควบคู่ไปกับความเสี่ยงขององค์กรโดยรวม
- ความเสี่ยงที่เกี่ยวข้องได้รับการติดตามและปรับปรุงอย่างต่อเนื่อง
- มีการบันทึกและรายงานความเสี่ยงอย่างโปร่งใสเพื่อการตรวจสอบและกำกับดูแล

2. แนวทางและขั้นตอนการบูรณาการผลลัพธ์ DPIA

2.1 การรวบรวมผลลัพธ์ DPIA

- หลังจากทำการประเมินผลกระทบข้อมูลส่วนบุคคลเสร็จสิ้น ผลลัพธ์ที่ได้จะประกอบด้วย:
- รายงานสรุปผลกระทบและความเสี่ยงที่ตรวจพบ
- มาตรการลดความเสี่ยงที่แนะนำและวิธีการนำไปใช้
- ข้อเสนอแนะในการปรับปรุงระบบงานหรือกระบวนการ
- ข้อมูลที่ใช้ประกอบการตัดสินใจ

2.2 การวางแผนบูรณาการผลลัพธ์

องค์กรควรมีการวางแผนเพื่อผนวกผลลัพธ์เหล่านี้เข้ากับแผนงานหรือแผนปฏิบัติการของแต่ละโครงการ เช่น

- กำหนดกิจกรรมหรือมาตรการความปลอดภัยข้อมูลในแผนงานโครงการ
- กำหนดความรับผิดชอบและแผนการติดตามผลการดำเนินงาน
- ระบุจุดที่ต้องมีการทบทวน DPIA ซ้ำในแผนงาน
- ผนวกข้อกำหนดด้านคุ้มครองข้อมูลลงในขั้นตอนการพัฒนาและดำเนินงาน

2.3 การบันทึกและติดตามความเสี่ยง

- นำผลลัพธ์ของ DPIA ไปบันทึกใน **ทะเบียนจัดการความเสี่ยง** เพื่อให้มีการติดตามและบริหารความเสี่ยงเป็นระบบ
- จัดทำรายงานสรุปความเสี่ยงและมาตรการที่บูรณาการในแผนงาน
- รายงานต่อผู้บริหารและเจ้าหน้าที่ที่เกี่ยวข้องเพื่อใช้ในการตัดสินใจและควบคุมดูแล
- กำหนดระยะเวลาทบทวนและปรับปรุงข้อมูลในทะเบียนความเสี่ยงตามสถานการณ์และผลการปฏิบัติจริง

3. ประโยชน์ของการบูรณาการผลลัพธ์ DPIA

- เพิ่มความสอดคล้องและประสิทธิภาพในการบริหารความเสี่ยงด้านข้อมูลส่วนบุคคล
- ทำให้มาตรการความปลอดภัยข้อมูลถูกนำไปใช้งานจริงในกิจกรรมและโครงการที่เกี่ยวข้อง
- ช่วยให้องค์กรสามารถตอบสนองความต้องการของหน่วยงานกำกับดูแลได้ดีขึ้น
- สร้างความเชื่อมั่นให้กับเจ้าของข้อมูลและผู้มีส่วนได้ส่วนเสีย
- ลดโอกาสการเกิดเหตุละเมิดข้อมูลและโทษปรับทางกฎหมาย
- สนับสนุนการบริหารจัดการความเสี่ยงโดยรวมอย่างมีระบบและเป็นระบบเดียวกันกับความเสี่ยงอื่น ๆ ขององค์กร

4. ตัวอย่างการบูรณาการในองค์กร

ตัวอย่างที่ 1: การพัฒนาระบบสารสนเทศ

- หลังจากทำ DPIA สำหรับระบบสารสนเทศใหม่ที่เก็บข้อมูลส่วนบุคคล ผลการประเมินพบว่าการเข้าถึงข้อมูลต้องมีการควบคุมสิทธิ์อย่างเข้มงวด
- มาตรการนี้ถูกบูรณาการลงในแผนปฏิบัติการของโครงการพัฒนาระบบ โดยมีการกำหนดให้มีการใช้ระบบยืนยันตัวตนแบบสองชั้น (2FA)
- ข้อมูลความเสี่ยงและมาตรการถูกบันทึกไว้ในทะเบียนจัดการความเสี่ยงขององค์กร
- มีการติดตามผลและรายงานผู้บริหารเป็นระยะ

ตัวอย่างที่ 2: การจัดกิจกรรมส่งเสริมการขาย

- DPIA สำหรับกิจกรรมส่งเสริมการขายที่เก็บข้อมูลลูกค้าระบุว่ามีความเสี่ยงด้านการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
- องค์กรบูรณาการข้อควรระวังและมาตรการลงในแผนงานกิจกรรม เช่น การกำหนดขั้นตอนจัดเก็บและทำลายข้อมูลอย่างปลอดภัย
- ความเสี่ยงและมาตรการถูกบันทึกและติดตามในทะเบียนความเสี่ยง

5. เอกสารหลักฐานที่ควรมี

- นโยบายการเผยแพร่รายงานการประเมินความเสี่ยง: ระบุขั้นตอนและความรับผิดชอบในการนำผล DPIA ไปใช้และเผยแพร่ในองค์กร

- รายงานการประเมินความเสี่ยง (DPIA report): ฉบับเต็มหรือฉบับสรุป ที่ระบุรายละเอียดผลกระทบและมาตรการ
- ทะเบียนจัดการความเสี่ยง: บันทึกความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล พร้อมสถานะและแผนการจัดการ
- แผนงานและแผนปฏิบัติการโครงการ: เอกสารแสดงแผนการดำเนินงานที่มีการบูรณาการผล DPIA

6. ข้อกฎหมายและแนวทางที่เกี่ยวข้อง

แม้ว่ากฎหมาย PDPA และประกาศที่เกี่ยวข้องจะไม่ได้กำหนดข้อบังคับเฉพาะสำหรับการบูรณาการผลลัพธ์ DPIA แต่การทำเช่นนี้ถือเป็นแนวทางปฏิบัติที่สอดคล้องกับหลักการบริหารความเสี่ยงและการคุ้มครองข้อมูลส่วนบุคคลในมาตรฐานสากล เช่น ISO/IEC 27001 และ GDPR

การบูรณาการผลลัพธ์ DPIA ยังช่วยให้องค์กรสามารถปฏิบัติตามมาตรา 37 ของ PDPA ซึ่งเกี่ยวกับการประเมินผลกระทบ และมาตรการรักษาความมั่นคงปลอดภัยที่กำหนดโดยประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

7. สรุป

การบูรณาการผลลัพธ์จาก DPIA เข้ากับแผนงานและทะเบียนจัดการความเสี่ยงขององค์กรเป็นกลไกที่ช่วยให้องค์กรบริหารจัดการความเสี่ยงข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ และสามารถตรวจสอบย้อนหลังได้อย่างโปร่งใส แม้จะไม่มีข้อกฎหมายบังคับ แต่ถือเป็นแนวปฏิบัติที่ดีและจำเป็นสำหรับองค์กรที่ต้องการปกป้องข้อมูลส่วนบุคคลอย่างเป็นระบบและยั่งยืน

ตัวอย่างแบบฟอร์มทะเบียนจัดการความเสี่ยง (Risk Register) สำหรับ DPIA

หมายเลขความเสี่ยง	ชื่อความเสี่ยง	รายละเอียดความเสี่ยง	ผลกระทบ	ความน่าจะเป็น	ระดับความรุนแรง (ผลกระทบ x ความน่าจะเป็น)	มาตรการควบคุม / แผนลดความเสี่ยง	ผู้รับผิดชอบ	สถานะการดำเนินการ	วันที่ทบทวนล่าสุด	หมายเหตุ
RR-001	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	ผู้ใช้ระบบอาจเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับสิทธิ์	ความเสียหายทางชื่อเสียง โทษปรับทางกฎหมาย	สูง	สูง	ใช้ระบบยืนยันตัวตนแบบสองชั้น (2FA) จำกัด	ฝ่าย IT Security	ดำเนินการแล้ว	01/06/2025	เพิ่มการตรวจสอบสิทธิ์ทุก 6 เดือน

						สิทธิ์การเข้าถึง				
RR-002	การรั่วไหลของข้อมูลผ่านช่องทางสื่อสาร	ข้อมูลถูกดักฟังหรือถูกเข้าถึงในขณะที่ส่งข้อมูล	ความเสียหายต่อเจ้าของข้อมูลและองค์กร	ปานกลาง	ปานกลาง	ใช้การเข้ารหัสข้อมูลทั้งในขณะพักและขณะส่ง	ฝ่ายพัฒนาโครงการ	อยู่ระหว่างดำเนินการ	01/06/2025	วางแผนทดสอบระบบเข้ารหัส
...	...	...	...	...	...	...	...	...	...	...

ร่างนโยบายการเผยแพร่รายงานการประเมินความเสี่ยงข้อมูลส่วนบุคคล (DPIA Report Dissemination Policy)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและขั้นตอนในการเผยแพร่และแบ่งปันรายงานการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) อย่างเหมาะสมภายในองค์กรและแก่ผู้มีส่วนได้ส่วนเสีย เพื่อสนับสนุนการบริหารความเสี่ยงข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพและเป็นไปตามข้อกำหนดทางกฎหมาย

2. ขอบเขต

นโยบายนี้ครอบคลุมการเผยแพร่รายงาน DPIA ของทุกโครงการหรือกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลภายในองค์กร

3. ความรับผิดชอบ

- **เจ้าของโครงการ** มีหน้าที่จัดทำและส่งมอบรายงาน DPIA
- **ผู้ควบคุมข้อมูลส่วนบุคคล (DPO)** มีหน้าที่ตรวจสอบความสมบูรณ์ของรายงานและดูแลกระบวนการเผยแพร่
- **ฝ่ายบริหารความเสี่ยง** รับผิดชอบในการบูรณาการข้อมูลความเสี่ยงจาก DPIA เข้ากับทะเบียนจัดการความเสี่ยงขององค์กร
- **ฝ่าย IT Security** รับผิดชอบการจัดเก็บและรักษาความลับของรายงาน DPIA

4. แนวทางการเผยแพร่

- รายงาน DPIA ต้องได้รับการอนุมัติจากผู้บริหารที่รับผิดชอบก่อนเผยแพร่
- การเผยแพร่รายงาน DPIA ควรทำในระดับที่เหมาะสมกับเนื้อหาและความลับของข้อมูลในรายงาน
- รายงานฉบับสมบูรณ์เก็บไว้ในระบบสารสนเทศขององค์กรที่มีการควบคุมการเข้าถึงอย่างเหมาะสม

- สรุปรายงานหรือข้อเสนอแนะที่สำคัญเผยแพร่ให้กับทีมโครงการและหน่วยงานที่เกี่ยวข้องโดยตรง
- หากมีการเผยแพร่ภายนอกองค์กร ต้องได้รับอนุมัติจากฝ่ายกฎหมายและผู้บริหารระดับสูง

5. การทบทวนและปรับปรุง

นโยบายนี้จะได้รับการทบทวนและปรับปรุงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงทางกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

6. เอกสารอ้างอิง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่องมาตรการรักษาความมั่นคงปลอดภัย พ.ศ. 2565

8.5.5 องค์กรมีขั้นตอนในการสื่อสารผลลัพธ์ของ DPIA ไปยังผู้มีส่วนได้ส่วนเสียที่เหมาะสม เช่น ผ่าน รายงานสรุปอย่างเป็นทางการ

สิ่งที่ต้องทำ: องค์กรมีขั้นตอนในการสื่อสารผลลัพธ์ของ DPIA ไปยังผู้มีส่วนได้ส่วนเสียที่เหมาะสม เช่น ผ่านรายงานสรุปอย่างเป็นทางการ และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการเผยแพร่รายงานการประเมินความเสี่ยง
รายงานการประเมินความเสี่ยง

สภาพบังคับ: กฎหมายไม่ได้กำหนด

องค์กรมีขั้นตอนในการสื่อสารผลลัพธ์ของ DPIA ไปยังผู้มีส่วนได้ส่วนเสียที่เหมาะสม เช่น ผ่าน รายงานสรุปอย่างเป็นทางการ

สิ่งที่ต้องทำ

องค์กรต้องจัดให้มีขั้นตอนและแนวทางปฏิบัติสำหรับการสื่อสารผลลัพธ์ของการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ไปยังผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องอย่างเหมาะสม โดยอาจใช้ช่องทางที่เหมาะสม เช่น

- การจัดทำ รายงานสรุปผล DPIA อย่างเป็นทางการ (DPIA Executive Summary Report) ซึ่งจะนำเสนอภาพรวมของการประเมินความเสี่ยงและมาตรการบรรเทาที่วางไว้

- การจัดประชุมหรือเวิร์กช็อปชี้แจงผลการประเมินและมาตรการควบคุมความเสี่ยง
- การส่งมอบรายงานฉบับเต็มแก่ผู้บริหารระดับสูง ฝ่ายกฎหมาย และหน่วยงานที่เกี่ยวข้อง
- การจัดเก็บข้อมูลผลลัพธ์ในระบบสารสนเทศขององค์กร พร้อมกำหนดสิทธิ์การเข้าถึงตามบทบาทหน้าที่
- ขั้นตอนนี้ต้องถูกบันทึกและปฏิบัติอย่างต่อเนื่อง เพื่อให้มั่นใจว่าผู้มีส่วนได้ส่วนเสียรับทราบและเข้าใจผลลัพธ์ รวมถึงมีส่วนร่วมในการดำเนินมาตรการจัดการความเสี่ยงที่เหมาะสมต่อไป

หลักฐานที่ต้องจัดเตรียม

- นโยบายการเผยแพร่รายงานการประเมินความเสี่ยง ที่ระบุขั้นตอน วิธีการ และความถี่ในการสื่อสารผล DPIA
- รายงานการประเมินความเสี่ยง (DPIA Report) ฉบับเต็มและฉบับสรุป
- บันทึกการประชุมหรือเวิร์กช็อป ที่แสดงการสื่อสารและการรับทราบของผู้มีส่วนได้ส่วนเสีย
- รายการรายชื่อผู้รับรายงานและการยืนยันการได้รับข้อมูล (Distribution list & Acknowledgement forms)
- เอกสารสนับสนุนอื่น ๆ เช่น อีเมลแจ้งผล รายงานการติดตามผล หรือเอกสารแจ้งเตือน

สภาพบังคับ

- กฎหมายไม่มีการกำหนดโดยตรงในส่วนนี้ แต่การสื่อสารอย่างมีประสิทธิภาพถือเป็นแนวปฏิบัติที่ดีในการบริหารความเสี่ยงข้อมูลส่วนบุคคล
- การมีขั้นตอนนี้ช่วยเสริมความโปร่งใสและเพิ่มความรับผิดชอบในองค์กร ซึ่งจะช่วยลดความเสี่ยงทางกฎหมายและชื่อเสียงในระยะยาว

ตัวอย่างแนวทางปฏิบัติและนโยบายการสื่อสารผลลัพธ์ DPIA

ตัวอย่างข้อความนโยบาย (Excerpt from DPIA Communication Policy)

นโยบายการสื่อสารผลการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA Communication Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการสื่อสารและเผยแพร่ผลการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลให้แก่ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องในองค์กร เพื่อให้เกิดความเข้าใจและความร่วมมือในการจัดการความเสี่ยงอย่างมีประสิทธิภาพ

ขอบเขต

นโยบายนี้ใช้บังคับกับทุกโครงการหรือกิจกรรมที่มีการประมวลผลข้อมูลส่วนบุคคลและผ่านกระบวนการ DPIA

แนวทางการสื่อสาร

- จัดทำรายงานสรุปผล DPIA ที่สื่อสารง่าย และมีข้อมูลสำคัญ เช่น ความเสี่ยงที่ประเมิน มาตรการบรรเทาความเสี่ยง ข้อเสนอแนะ และการดำเนินงานในอนาคต
- จัดส่งรายงานฉบับเต็มหรือรายงานสรุปให้กับผู้มีส่วนได้ส่วนเสียที่จำเป็น เช่น ฝ่ายบริหาร ฝ่ายกฎหมาย ฝ่าย IT Security และหน่วยงานที่รับผิดชอบโครงการ
- จัดประชุมชี้แจงและตอบคำถามเกี่ยวกับผลการประเมินกับผู้มีส่วนได้ส่วนเสีย
- เก็บรักษารายงานและหลักฐานการสื่อสารไว้ในระบบบริหารจัดการเอกสารขององค์กร

ความรับผิดชอบ

- DPO และเจ้าของโครงการรับผิดชอบจัดทำและเผยแพร่รายงาน DPIA
- ฝ่ายบริหารความเสี่ยงและฝ่ายสื่อสารองค์กรรับผิดชอบติดตามและประสานงานการสื่อสาร

1. ตัวอย่าง แบบฟอร์มรายงานสรุป DPIA (DPIA Executive Summary Report Template)

DPIA Executive Summary Report

โครงการ/กิจกรรม: พัฒนาระบบลงทะเบียนออนไลน์สำหรับงานสัมมนา

วันที่รายงาน: 1 มิถุนายน 2568

ผู้จัดทำรายงาน: นางสาวปริญญ์ ศรีทอง

หน่วยงานรับผิดชอบ: ฝ่ายเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์ของการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA Objective)

เพื่อประเมินความเสี่ยงด้านความเป็นส่วนตัวที่อาจเกิดขึ้นจากการพัฒนาระบบลงทะเบียนออนไลน์งานสัมมนา โดยเฉพาะข้อมูลส่วนบุคคลที่ต้องเก็บและจัดการ เช่น ชื่อ-นามสกุล เบอร์โทรศัพท์ อีเมล และข้อมูลที่เกี่ยวข้อง เพื่อกำหนดมาตรการบรรเทาความเสี่ยงและป้องกันการละเมิดข้อมูลส่วนบุคคล

2. ข้อมูลส่วนบุคคลที่เกี่ยวข้อง (Personal Data Involved)

- ข้อมูลส่วนบุคคลทั่วไป: ชื่อ-นามสกุล เพศ อายุ
- ข้อมูลติดต่อ: เบอร์โทรศัพท์มือถือ อีเมล
- ข้อมูลการลงทะเบียน: หน่วยงาน ตำแหน่งงาน ความสนใจ

3. รายละเอียดของการประมวลผล (Description of Processing Activities)

ระบบจะเก็บรวบรวมข้อมูลผ่านแบบฟอร์มออนไลน์จากผู้เข้าร่วมงานสัมมนา เพื่อใช้ในการจัดการลงทะเบียนและติดต่อประสานงาน ระบบจะจัดเก็บข้อมูลในฐานข้อมูลเซิร์ฟเวอร์ภายในองค์กร และมีการเข้าถึงข้อมูลโดยเจ้าหน้าที่ฝ่ายจัดงานเท่านั้น

4. การประเมินความเสี่ยง (Risk Assessment Summary)

ความเสี่ยง	ระดับความรุนแรง	ผลกระทบที่อาจเกิดขึ้น
การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	สูง	การรั่วไหลของข้อมูลส่วนบุคคล ส่งผลเสียต่อความเป็นส่วนตัวส่วนตัวของผู้ลงทะเบียนและชื่อเสียงองค์กร
การสูญหายของข้อมูล	กลาง	ข้อมูลสำคัญสูญหาย ส่งผลให้ไม่สามารถดำเนินงานได้ตามแผน
การใช้ข้อมูลในทางที่ผิด	สูง	ข้อมูลถูกนำไปใช้ในการตลาดโดยไม่ได้รับความยินยอม

5. มาตรการบรรเทาความเสี่ยง (Risk Mitigation Measures)

- กำหนดสิทธิ์เข้าถึงข้อมูลเฉพาะเจ้าหน้าที่ที่เกี่ยวข้อง
- ใช้ระบบเข้ารหัสข้อมูลทั้งในระหว่างการส่งและจัดเก็บ
- สำรองข้อมูลทุกวัน และเก็บรักษาในสถานที่ปลอดภัย
- จัดอบรมให้ความรู้แก่เจ้าหน้าที่เรื่อง PDPA และการรักษาความปลอดภัยข้อมูล
- จัดทำนโยบายการใช้ข้อมูลและขอความยินยอมจากผู้ลงทะเบียนก่อนเก็บข้อมูล

6. ข้อสรุปและขอเสนอแนะ (Conclusion and Recommendations)

หลังจากดำเนินการมาตรการบรรเทาความเสี่ยงแล้ว พบว่าความเสี่ยงที่เหลืออยู่มีระดับที่ยอมรับได้ โดยแนะนำให้ทบทวน DPIA อีกครั้งในกรณีที่มีการเปลี่ยนแปลงลักษณะการประมวลผลหรือเพิ่มประเภทข้อมูล นอกจากนี้ควรดำเนินการสื่อสารกับผู้มีส่วนได้ส่วนเสียเกี่ยวกับมาตรการรักษาความปลอดภัยข้อมูลอย่างต่อเนื่อง

7. การดำเนินการถัดไป (Next Steps)

- ทบทวนมาตรการรักษาความมั่นคงปลอดภัยข้อมูลทุก 6 เดือน
- จัดประชุมชี้แจงผลการประเมินความเสี่ยงแก่ผู้บริหารและฝ่ายงานที่เกี่ยวข้อง
- ติดตามและประเมินผลการบรรเทาความเสี่ยงในระหว่างดำเนินโครงการ

8. รายชื่อผู้รับรายงาน (Distribution List)

ชื่อ	ตำแหน่ง	หน่วยงาน	ลงชื่อรับทราบ	วันที่
นายสมชาย รุ่งเรือง	ผู้อำนวยการฝ่าย IT	ฝ่ายเทคโนโลยีฯ		1 มิ.ย. 68
นางสาวปรียา นุชศรีทอง	เจ้าหน้าที่ DPO	ฝ่ายเทคโนโลยีฯ		1 มิ.ย. 68
นายสุทธิพงษ์ พานทอง	หัวหน้าฝ่ายจัดงานสัมมนา	ฝ่ายบริหารงานทั่วไป		1 มิ.ย. 68

9. หมายเหตุ (Notes)

รายงานฉบับนี้จัดทำขึ้นเพื่อใช้ประกอบการบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลของโครงการพัฒนาระบบลงทะเบียนออนไลน์ และอาจปรับปรุงแก้ไขได้ตามสถานการณ์จริง

2. ตัวอย่าง แบบฟอร์มบันทึกการประชุมสื่อสารผลลัพธ์ DPIA (DPIA Communication Meeting Record Form)

โครงการ/กิจกรรม: พัฒนาระบบลงทะเบียนออนไลน์สำหรับงานสัมมนา

วันที่ประชุม: 5 มิถุนายน 2568

สถานที่: ห้องประชุมฝ่ายเทคโนโลยีสารสนเทศ

ผู้จัดประชุม: นางสาวปริญญ์ ศรีทอง (DPO)

ผู้เข้าร่วมประชุม

ชื่อ	ตำแหน่ง	หน่วยงาน	ลงชื่อ
นายสมชาย รุ่งเรือง	ผู้อำนวยการฝ่าย IT	ฝ่ายเทคโนโลยีฯ	
นางสาวปริญญ์ ศรีทอง	เจ้าหน้าที่ DPO	ฝ่ายเทคโนโลยีฯ	
นายสุทธิพงษ์ พานทอง	หัวหน้าฝ่ายจัดงานสัมมนา	ฝ่ายบริหารงานทั่วไป	
นางสาวกมลชนก สายทอง	เจ้าหน้าที่ฝ่ายรักษาความปลอดภัยข้อมูล	ฝ่ายเทคโนโลยีฯ	

1. วัตถุประสงค์ของการประชุม

- สื่อสารและชี้แจงผลการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลจากการพัฒนาระบบลงทะเบียนออนไลน์
- รับฟังข้อเสนอแนะและตอบคำถามเกี่ยวกับมาตรการบรรเทาความเสี่ยง
- วางแผนการติดตามผลและการประเมินซ้ำในอนาคต

2. เนื้อหาการประชุม

หัวข้อ	รายละเอียด	ผู้รับผิดชอบ	หมายเหตุ
สรุปผล DPIA	รายงานสรุปความเสี่ยงที่พบและมาตรการบรรเทา เช่น การเข้ารหัสข้อมูล การกำหนดสิทธิ์การเข้าถึง	นางสาวปริญญ์ ศรีทอง	-
ข้อเสนอแนะจากผู้เข้าร่วม	แนะนำให้เพิ่มการอบรมพนักงานอย่างต่อเนื่อง และเพิ่มระบบแจ้งเตือนเมื่อมีการเข้าถึงข้อมูลผิดปกติ	นายสมชาย รุ่งเรือง	จะดำเนินการเพิ่มเติม

ข้อซักถามและคำตอบ	มีคำถามเกี่ยวกับระยะเวลาการเก็บข้อมูลและวิธีการขอความยินยอม	นางสาวปริยานุช ศรีทอง	ตอบว่าตามนโยบายขององค์กร
กำหนดการติดตามผล	กำหนดให้ทบทวนมาตรการและ DPIA ทุก 6 เดือน หรือเมื่อลักษณะการประมวลผลเปลี่ยนแปลง	นางสาวปริยานุช ศรีทอง	จัดประชุมรอบถัดไป 5 ธ.ค. 2568

3. ข้อสรุปและข้อปฏิบัติ

- ผลการประเมินความเสี่ยงและมาตรการบรรเทาได้รับการยอมรับ
- จะดำเนินการเพิ่มการอบรมพนักงานและติดตั้งระบบแจ้งเตือน
- จะติดตามประเมินผลและทบทวน DPIA อย่างต่อเนื่องตามกำหนด

4. ลงชื่อรับรองการประชุม

ชื่อ	ตำแหน่ง	ลงชื่อ	วันที่
นายสมชาย รุ่งเรือง	ผู้อำนวยการฝ่าย IT		5 มิ.ย.

8.5.6 องค์กรเผยแพร่ผลการพิจารณา DPIA หากเป็นไปได้ โดยเปิดเผยตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และมีรูปแบบการเผยแพร่ที่เหมาะสม รวมถึงมีการลบรายละเอียดที่เกี่ยวกับข้อมูลความลับทางการค้าออกหากจำเป็น

สิ่งที่ต้องทำ: องค์กรมีการเผยแพร่ผลการพิจารณา DPIA หากเป็นไปได้ โดยเปิดเผยตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล รวมถึงมีการลบรายละเอียดที่เกี่ยวข้องกับข้อมูลความลับทางการค้าออกหากจำเป็น

หลักฐาน: นโยบายการเผยแพร่รายงานการประเมินความเสี่ยง รายงานการประเมินความเสี่ยง (ฉบับเผยแพร่ โดยปรากฏรายละเอียดเกี่ยวกับการพิจารณาผลกระทบด้านข้อมูลส่วนบุคคล)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การเผยแพร่ผลการพิจารณา DPIA (Data Protection Impact Assessment Disclosure)

สิ่งที่ต้องทำ

องค์กรต้องมีขั้นตอนและนโยบายที่ชัดเจนในการเผยแพร่ผลการพิจารณา DPIA ให้สาธารณะหรือผู้ที่เกี่ยวข้องได้รับทราบ ตามข้อกำหนดและข้อจำกัดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล และต้องมีมาตรการในการปกป้องข้อมูลที่เป็นความลับทางการค้า เช่น การลบหรือปกปิดข้อมูลที่สามารถทำให้เกิดความเสียหายต่อองค์กร หากมีความจำเป็น

รายละเอียดที่ควรครอบคลุมในขั้นตอนการเผยแพร่ผล DPIA ได้แก่:

- การกำหนดรูปแบบและช่องทางการเผยแพร่ผล DPIA ให้เหมาะสม เช่น ผ่านเว็บไซต์องค์กร รายงานประจำปี หรือรายงานความรับผิดชอบต่อสาธารณะ (CSR Report)
- การตรวจสอบให้มั่นใจว่าการเผยแพร่ข้อมูลเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและมาตรฐานความปลอดภัยข้อมูล
- การลบหรือปกปิดรายละเอียดที่เกี่ยวข้องกับความลับทางการค้า ข้อมูลที่มีความเสี่ยงสูง หรือข้อมูลนี้อาจละเมิดสิทธิของบุคคลใดบุคคลหนึ่ง
- การจัดเก็บหลักฐานการเผยแพร่ เช่น สำเนารายงานที่เผยแพร่ วันที่เวลาที่เผยแพร่ URL หรือเอกสารที่เผยแพร่

ตัวอย่างนโยบายการเผยแพร่รายงานการประเมินความเสี่ยง (DPIA Publication Policy)

นโยบายการเผยแพร่รายงาน DPIA

- องค์กรจะจัดทำรายงานการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA) สำหรับโครงการที่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง
- รายงาน DPIA ฉบับที่เหมาะสมจะได้รับการเผยแพร่ต่อสาธารณะในรูปแบบที่เหมาะสม เช่น ผ่านเว็บไซต์องค์กร เพื่อแสดงความโปร่งใสในการจัดการข้อมูลส่วนบุคคล
- รายงานเผยแพร่จะถูกปรับแต่งโดยลบข้อมูลที่ถือเป็นความลับทางการค้า หรือข้อมูลนี้อาจทำให้เกิดความเสียหายต่อองค์กร หรือบุคคลที่เกี่ยวข้อง
- การเผยแพร่จะดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจะต้องได้รับความเห็นชอบจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร
- องค์กรจะเก็บบันทึกหลักฐานการเผยแพร่รายงาน DPIA รวมถึงวันเวลาและช่องทางการเผยแพร่ เพื่อใช้ในการตรวจสอบและรายงานภายใน

ตัวอย่างรายงานการประเมินความเสี่ยง (ฉบับเผยแพร่)

รายงานการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA) โครงการพัฒนาระบบลงทะเบียนออนไลน์ (ฉบับเผยแพร่)

รายงานฉบับนี้ได้ถูกปรับแต่งเพื่อเผยแพร่สู่สาธารณะ โดยลบข้อมูลที่เกี่ยวข้องกับระบบรักษาความปลอดภัยภายในและข้อมูลความลับทางการค้า

- เนื้อหาที่เผยแพร่ประกอบด้วย: วัตถุประสงค์ของการประเมิน ข้อมูลส่วนบุคคลที่เกี่ยวข้อง ความเสี่ยงที่ประเมิน และมาตรการบรรเทาความเสี่ยงโดยรวม
- รายงานฉบับเต็มพร้อมข้อมูลละเอียดทางเทคนิคและความลับทางการค้าจะถูกเก็บรักษาในองค์กร และให้เฉพาะผู้ที่มีสิทธิ์เข้าถึงตามนโยบาย

ตัวอย่างขั้นตอนการเผยแพร่ผล DPIA

- จัดทำรายงาน DPIA ฉบับเผยแพร่ โดยคัดกรองข้อมูลที่เกี่ยวข้องกับความลับทางการค้าออก

- ขออนุมัติจากคณะกรรมการคุ้มครองข้อมูล เพื่อความเหมาะสมและถูกต้องของข้อมูลที่จะเผยแพร่
- เผยแพร่รายงานผ่านช่องทางที่เหมาะสม เช่น เว็บไซต์องค์กรหรือรายงานประจำปี
- จัดเก็บหลักฐานการเผยแพร่ เช่น Screenshot หน้าเว็บไซต์ ไฟล์ PDF ฉบับเผยแพร่ พร้อมบันทึกวันเวลาการเผยแพร่
- ติดตามและทบทวน การเผยแพร่เป็นระยะ ๆ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของกฎหมายและนโยบายองค์กร

รายงานการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA)

โครงการพัฒนาระบบลงทะเบียนออนไลน์

(ฉบับเผยแพร่)

1. บทนำ

องค์กรของเราตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และดำเนินการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (Data Protection Impact Assessment หรือ DPIA) สำหรับโครงการพัฒนาระบบลงทะเบียนออนไลน์ เพื่อให้มั่นใจว่าการประมวลผลข้อมูลส่วนบุคคลเป็นไปตามกฎหมายและมาตรฐานด้านความปลอดภัย

รายงานฉบับนี้จัดทำขึ้นเพื่อเผยแพร่สู่สาธารณะ โดยได้มีการคัดกรองข้อมูลที่เกี่ยวข้องกับความลับทางการค้า และข้อมูลที่สามารถละเมิดสิทธิของบุคคลใดบุคคลหนึ่งออก เพื่อความโปร่งใสและสร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสีย

2. วัตถุประสงค์ของ DPIA

เพื่อประเมินความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคลในโครงการพัฒนาระบบลงทะเบียนออนไลน์

เพื่อกำหนดมาตรการบรรเทาความเสี่ยงและป้องกันผลกระทบที่ไม่พึงประสงค์ต่อเจ้าของข้อมูล เพื่อสนับสนุนการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และข้อกำหนดอื่นที่เกี่ยวข้อง

3. ขอบเขตของโครงการและข้อมูลส่วนบุคคลที่ประมวลผล

- โครงการพัฒนาระบบลงทะเบียนออนไลน์ เป็นระบบสำหรับรับข้อมูลผู้ลงทะเบียน เพื่อใช้ในการจัดกิจกรรมขององค์กร
- ข้อมูลส่วนบุคคลที่เก็บรวบรวม ได้แก่ ชื่อ-นามสกุล เลขบัตรประชาชน เบอร์โทรศัพท์ ที่อยู่อีเมล และข้อมูลสุขภาพบางส่วน (สำหรับการจัดกิจกรรมที่เกี่ยวข้องกับสุขภาพ)

4. การประเมินความเสี่ยง

ความเสี่ยงที่อาจเกิดขึ้น	ผลกระทบ	ความน่าจะเป็น	ระดับความเสี่ยง	มาตรการบรรเทา
การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	ข้อมูลรั่วไหล สูญหาย	ปานกลาง	สูง	ใช้ระบบการเข้ารหัสข้อมูล และระบบควบคุมสิทธิ์เข้าถึง
การละเมิดความเป็นส่วนตัวของเจ้าของข้อมูล	สูญเสียความเชื่อมั่น	ต่ำ	ปานกลาง	ให้ความรู้พนักงานและมีนโยบายความเป็นส่วนตัวชัดเจน
การโจมตีทางไซเบอร์	ข้อมูลถูกทำลายหรือแก้ไข	ต่ำ	ปานกลาง	มีระบบ Firewall และการตรวจสอบช่องโหว่เป็นประจำ

5. มาตรการบรรเทาผลกระทบ

- การเข้ารหัสข้อมูลทั้งหมดทั้งในขณะเก็บและส่งผ่าน
- การกำหนดระดับการเข้าถึงข้อมูลตามหน้าที่ของผู้ใช้งาน
- การอบรมพนักงานเกี่ยวกับการปฏิบัติที่ดีในการคุ้มครองข้อมูลส่วนบุคคล
- การจัดทำแผนรับมือเหตุการณ์ข้อมูลรั่วไหล
- การตรวจสอบระบบความปลอดภัยอย่างสม่ำเสมอ

6. การเปิดเผยข้อมูลในรายงานฉบับนี้

เพื่อความโปร่งใส รายงานฉบับนี้ได้จัดทำขึ้นสำหรับเผยแพร่ต่อสาธารณะ โดยมีการลบหรือปกปิดข้อมูลที่เป็นความลับทางการค้าและข้อมูลที่สามารถส่งผลกระทบต่อองค์กร เช่น รายละเอียดทางเทคนิคของระบบรักษาความปลอดภัย ข้อมูลการตั้งค่าเซิร์ฟเวอร์ หรือแผนการปฏิบัติการภายในอื่นๆ

7. ช่องทางและรูปแบบการเผยแพร่

- รายงานนี้เผยแพร่ผ่านเว็บไซต์องค์กรในหน้าสิทธิและความเป็นส่วนตัว

- รายงานสามารถดาวน์โหลดได้ในรูปแบบไฟล์ PDF
- มีการอัปเดตและเผยแพร่รายงาน DPIA ฉบับใหม่ทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในโครงการ

8. บันทึกและหลักฐานการเผยแพร่

วันที่เผยแพร่: 15 เมษายน 2568

URL เผยแพร่: <https://www.organizationdomain.com/privacy/dpia-registration-system.pdf>

เอกสารฉบับเต็มถูกจัดเก็บในระบบภายในองค์กรและมีการควบคุมการเข้าถึงอย่างเข้มงวด

9. สรุป

โครงการพัฒนาระบบลงทะเบียนออนไลน์นี้ ได้ผ่านกระบวนการประเมินความเสี่ยงและจัดทำ DPIA อย่างครบถ้วน มีมาตรการบรรเทาความเสี่ยงที่เหมาะสม และเปิดเผยข้อมูลผลการประเมินในรูปแบบที่โปร่งใส ป้องกันการละเมิดข้อมูลส่วนบุคคล และสอดคล้องกับกฎหมายและแนวทางปฏิบัติที่ดีที่สุด

หากท่านต้องการสอบถามรายละเอียดเพิ่มเติม กรุณาติดต่อ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

อีเมล: dpo@organizationdomain.com

โทร: 02-123-4567

บทที่ 10

มาตรการรักษาความมั่นคงปลอดภัย (Data Security)

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Data Security) เป็นหัวใจสำคัญในการปกป้องสิทธิและเสรีภาพของเจ้าของข้อมูล รวมถึงการป้องกันความเสียหายที่อาจเกิดขึ้นต่อองค์กรเอง ทั้งจากการโจมตีทางไซเบอร์ การเข้าถึงโดยไม่ได้รับอนุญาต หรือการประมวลผลที่ไม่สอดคล้องกับกฎหมาย PDPA (Personal Data Protection Act) การจัดทำมาตรการรักษาความมั่นคงปลอดภัยจึงไม่เพียงเกี่ยวข้องกับเทคโนโลยีเท่านั้น แต่ครอบคลุมถึงการบริหารจัดการ การกำหนดบทบาทความรับผิดชอบ การสร้างวัฒนธรรมความปลอดภัย และการตรวจสอบความปลอดภ้ยอย่างต่อเนื่อง มาตรการรักษาความมั่นคงปลอดภัยข้อมูลสามารถแบ่งออกเป็นหลายระดับ ได้แก่ มาตรการทางเทคนิค (Technical Measures) เช่น การเข้ารหัสข้อมูล

(Encryption), การควบคุมการเข้าถึง (Access Control), การเฝ้าระวังระบบและการตรวจสอบความปลอดภัย (System Monitoring & Audit) และมาตรการทางองค์กร (Organizational Measures) เช่น การกำหนดนโยบายความปลอดภัย, การอบรมพนักงาน, การกำหนดบทลงโทษสำหรับการละเมิด และการวางแผนตอบสนองต่อเหตุการณ์ (Incident Response Plan) ความปลอดภัยของข้อมูลยังเกี่ยวข้องกับการจัดการวงจรชีวิตของข้อมูล (Data Lifecycle) ตั้งแต่การเก็บรวบรวม ใช้งาน การถ่ายโอน การเก็บรักษา จนถึงการลบหรือทำลายข้อมูล การประเมินความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Assessment) เป็นเครื่องมือสำคัญที่ช่วยให้องค์กรสามารถระบุจุดอ่อน วางมาตรการควบคุม และปรับปรุงระบบอย่างต่อเนื่อง นอกจากนี้ การบันทึกและจัดเก็บหลักฐานการปฏิบัติด้านความมั่นคงปลอดภัยยังช่วยให้สามารถตรวจสอบการปฏิบัติตาม PDPA ได้อย่างเป็นรูปธรรม

โดยสรุป การสร้างมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่มีประสิทธิภาพไม่เพียงช่วยป้องกันเหตุการณ์ละเมิดข้อมูล แต่ยังเป็นหลักประกันสำคัญที่เสริมสร้างความเชื่อมั่นให้กับเจ้าของข้อมูลและผู้มีส่วนเกี่ยวข้องว่าข้อมูลส่วนบุคคลได้รับการปกป้องอย่างเหมาะสม ครอบคลุมทุกขั้นตอน ตั้งแต่การจัดเก็บ ใช้งาน ไปจนถึงการลบหรือทำลายข้อมูลอย่างปลอดภัย

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
1. การเข้ารหัสข้อมูล (Data Encryption)	ใช้มาตรการเข้ารหัสข้อมูลทั้งในระหว่างการส่ง (Data in Transit) และเก็บรักษา (Data at Rest) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต	นโยบายการเข้ารหัส (Encryption Policy) รายงานการติดตั้งระบบเข้ารหัส Log การเข้าถึงข้อมูล	มีการเข้ารหัสข้อมูลทุกประเภท ข้อมูลสำคัญถูกป้องกันและตรวจสอบได้
2. การควบคุมการเข้าถึง (Access Control)	กำหนดสิทธิ์การเข้าถึงข้อมูลตามบทบาทหน้าที่ (Role-Based Access Control – RBAC) และตรวจสอบการเข้าถึงอย่างสม่ำเสมอ	ตารางสิทธิ์เข้าถึง (Access Rights Matrix) ระบบตรวจสอบการเข้าถึง (Access Logs), Policy การควบคุมสิทธิ์	มีการกำหนดสิทธิ์ชัดเจน ครอบคลุมทุกระบบ และสามารถตรวจสอบย้อนหลังได้
3. การเฝ้าระวังและตรวจสอบระบบ	ติดตั้งระบบตรวจสอบและบันทึกกิจกรรม	Log ระบบ (System Log) รายงานตรวจสอบ (Audit	มีการเฝ้าระวังต่อเนื่อง สามารถ

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้ คะแนน (เต็ม = สอดคล้องครบถ้วน)
(System Monitoring & Audit)	สำคัญ เช่น การเข้าถึง การแก้ไขข้อมูล และ การส่งออก	Report) Policy การ ตรวจสอบ	ระบุเหตุการณ์ ผิดปกติและติดตาม ได้จริง
4. การป้องกันภัย คุกคามและมัลแวร์ (Threat & Malware Protection)	ติดตั้งระบบป้องกัน ไวรัส มัลแวร์ และ Firewall รวมถึงอัปเดต ระบบอย่างสม่ำเสมอ	รายงานการติดตั้ง Antivirus/Firewall Log การ สแกนมัลแวร์ Policy การ ป้องกันภัย	ครอบคลุมทุกระบบ คอยอัปเดตและ ตรวจสอบสม่ำเสมอ
5. การสำรองและกู้คืน ข้อมูล (Backup & Recovery)	จัดทำระบบสำรอง ข้อมูล (Backup) และ แผนฟื้นฟูข้อมูล (Disaster Recovery Plan)	แผนสำรองข้อมูลและกู้คืน (Backup & Recovery Plan) รายงานการทดสอบการกู้คืน Log การสำรองข้อมูล	ข้อมูลสำคัญมีการ สำรองครบถ้วน ทดสอบฟื้นฟูได้จริง และสม่ำเสมอ
6. การจัดการ เหตุการณ์ละเมิดข้อมูล (Incident Response)	กำหนดขั้นตอนการ ตอบสนองต่อเหตุ ละเมิดข้อมูล (Data Breach) และแจ้ง เจ้าของข้อมูลและ หน่วยงานที่เกี่ยวข้อง	Incident Response Plan Log เหตุการณ์ละเมิด รายงานการแจ้งเหตุละเมิด	มีขั้นตอนชัดเจน ดำเนินการได้จริง และสามารถ ตรวจสอบย้อนหลัง ได้
7. การควบคุมอุปกรณ์ และสื่อบันทึกข้อมูล (Device & Media Control)	จัดการความปลอดภัย ของอุปกรณ์ คอมพิวเตอร์ สื่อบันทึก ข้อมูล และอุปกรณ์ พกพา	Policy การควบคุมอุปกรณ์ (Device Policy) Inventory อุปกรณ์, Log การเข้าถึงสื่อ บันทึก	ครอบคลุมทุก อุปกรณ์ ตรวจสอบ และป้องกันการสูญ หายหรือรั่วไหล
8. การบริหารจัดการ บัญชีผู้ใช้และรหัสผ่าน (User Account & Password Management)	กำหนดนโยบาย รหัสผ่าน การล็อกบัญชี เมื่อเกิดการพยายาม เข้าถึงผิดพลาด และ การรีเซ็ตรหัสผ่าน	Policy การจัดการบัญชีผู้ใช้ รายงานการตรวจสอบบัญชี Log การเปลี่ยนรหัสผ่าน	มีนโยบายรัดกุม บังคับใช้จริง และ ตรวจสอบย้อนหลัง ได้
9. การฝึกอบรมและ สร้างความตระหนัก	อบรมบุคลากรเกี่ยวกับ มาตรการรักษาความ	แผนอบรม (Training Plan) สไลด์นำเสนอ	บุคลากรทุกระดับ ได้รับการอบรม มี

หัวข้อย่อ	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้ คะแนน (เต็ม = สอดคล้องครบถ้วน)
ด้านความปลอดภัย (Security Training & Awareness)	มั่นคงปลอดภัย การ ป้องกัน phishing และ social engineering	(Presentation) รายชื่อ ผู้เข้าร่วม (Attendance Sheet) แบบสอบถาม ประเมินผล (Evaluation Form)	หลักฐานชัดเจน และสามารถปฏิบัติ ได้จริง
10. การตรวจสอบและ ประเมินความปลอดภัย ภายใน (Internal Security Audit / Assessment)	ตรวจสอบการปฏิบัติ ตามมาตรการรักษา ความมั่นคงปลอดภัย อย่างสม่ำเสมอ	รายงานตรวจสอบภายใน (Internal Security Audit Report) Compliance Checklist Log การแก้ไข ข้อบกพร่อง	มีรายงานตรวจสอบ ครบถ้วน พร้อม ข้อเสนอแนะและ หลักฐานการปฏิบัติ จริง
11. การเชื่อมโยง มาตรการความ ปลอดภัยกับความเสีย และ PDPA (Security & Risk Linkage)	ผูกโยงมาตรการความ ปลอดภัยกับการ ประเมินความเสี่ยงด้าน ข้อมูลและข้อกำหนด PDPA	Risk Register รายงาน เชื่อมโยงมาตรการ (Security- Risk Report) DPIA Record	ครอบคลุมทุกความ เสี่ยงหลัก สามารถ ตรวจสอบการ เชื่อมโยงและติดตาม ได้จริง
12. การปรับปรุงและ ทบทวนมาตรการ (Review & Update Security Measures)	ทบทวนมาตรการรักษา ความมั่นคงปลอดภัย อย่างต่อเนื่อง ปรับปรุง ตามเทคโนโลยีหรือ กฎหมายใหม่	Version Control Meeting Minutes Security Improvement Log	มีหลักฐานปรับปรุง ต่อเนื่อง แสดง การอัปเดตตาม มาตรฐานสากลและ กฎหมาย

การจัดทำเอกสารตามเกณฑ์

9.1 การสร้าง การค้นหา และการเข้าถึงรายการข้อมูล (Creating, Locating and Retrieving Records) องค์กรมีมาตรฐานขั้นต่ำสำหรับการสร้างบันทึก และกลไกที่มีประสิทธิภาพในการค้นหาและดึงข้อมูลเหล่านั้น

9.1.1 มีระบบ ตู้ บริเวณ หรือพื้นที่สำหรับจัดเก็บรายการข้อมูลต่าง ๆ มีการจัดทำบัญชีทรัพย์สินสารสนเทศสำหรับการจัดเก็บรายการข้อมูลเหล่านั้น

สิ่งที่ต้องทำ: มีระบบ ตู้ บริเวณ หรือพื้นที่สำหรับจัดเก็บรายการข้อมูลต่าง ๆ มีการจัดทำบัญชีทรัพย์สินสารสนเทศสำหรับการจัดเก็บรายการข้อมูลเหล่านั้น

หลักฐาน: นโยบายการจัดทำบัญชีทรัพย์สินสารสนเทศ
บัญชีทรัพย์สินสารสนเทศ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (4)

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

(1) นโยบายการจัดทำบัญชีทรัพย์สินสารสนเทศ

องค์กร: [ชื่อองค์กร]

เรื่อง: นโยบายการจัดทำบัญชีทรัพย์สินสารสนเทศ

ประกาศ ณ วันที่: 1 เมษายน พ.ศ. 2568

1. วัตถุประสงค์

เพื่อกำหนดแนวทางในการจัดทำบัญชีทรัพย์สินสารสนเทศขององค์กรอย่างเป็นระบบและปลอดภัย สอดคล้องกับมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ ควบคุมข้อมูลส่วนบุคคล

2. ขอบเขต

นโยบายฉบับนี้ครอบคลุมถึงข้อมูลส่วนบุคคลที่เก็บในรูปแบบเอกสารหรือดิจิทัลทุกประเภทที่อยู่ ภายใต้การควบคุมขององค์กร รวมถึงระบบจัดเก็บและเจ้าหน้าที่ที่มีหน้าที่ดูแลข้อมูล

3. นโยบาย

3.1 การกำหนดพื้นที่และวิธีจัดเก็บ

- องค์กรจัดให้มี **พื้นที่จัดเก็บข้อมูล** อย่างเป็นสัดส่วน เช่น ห้องเก็บเอกสาร ตู้ล็อกเกอร์ ตู้เหล็กที่มี การล็อก และระบบจัดเก็บข้อมูลอิเล็กทรอนิกส์ (เช่น ระบบ Cloud ที่มีการเข้ารหัส)
- พื้นที่จัดเก็บต้องมีระบบควบคุมการเข้าถึงอย่างเหมาะสม เช่น การใช้กุญแจ การใช้บัตรผ่าน หรือ รหัสผ่าน

3.2 การจัดทำบัญชีทรัพย์สินสารสนเทศ

หน่วยงานที่รับผิดชอบข้อมูลต้องจัดทำ **บัญชีทรัพย์สินสารสนเทศ** (Information Asset Register: IAR) ระบุข้อมูลประเภทต่าง ๆ เช่น

- ประเภทของข้อมูล
- ที่ตั้งหรือระบบที่จัดเก็บ
- เจ้าของข้อมูล (Data Owner)

- ความสำคัญหรือระดับความลับ
- รูปแบบการเข้าถึง
- บัญชีทรัพย์สินนี้ต้องได้รับการทบทวนและปรับปรุงอย่างน้อยปีละ 1 ครั้ง

3.3 ผู้รับผิดชอบ

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีหน้าที่กำกับดูแลการจัดทำบัญชีทรัพย์สินและความปลอดภัยของสถานที่จัดเก็บ
- ผู้บริหารหน่วยงานต้องรับรองความถูกต้องของบัญชีที่จัดทำขึ้น

4. การควบคุมและตรวจสอบ

มีการตรวจสอบการเข้าถึงพื้นที่จัดเก็บข้อมูลอย่างสม่ำเสมอ
การละเลยหรือไม่ปฏิบัติตามนโยบายนี้อาจนำไปสู่บทลงโทษทางวินัย และอาจถูกพิจารณาโทษทางปกครอง
ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ลงชื่อ

นาย..... (ผู้อำนวยการ)

[ชื่อองค์กร]

(2) ตัวอย่างบัญชีทรัพย์สินสารสนเทศ

ชื่อหน่วยงาน: กองเทคโนโลยีสารสนเทศ

วันที่จัดทำ: 1 เมษายน พ.ศ. 2568

ลำดับ	ประเภทข้อมูล	ระบบหรือพื้นที่จัดเก็บ	เจ้าของข้อมูล (Data Owner)	ระดับความลับ	วิธีเข้าถึงข้อมูล	หมายเหตุ
1	ข้อมูลพนักงาน	ระบบ HR Online	ผอ.กองบุคคล	ลับมาก	ชื่อผู้ใช้+รหัสผ่าน (2FA)	-
2	ข้อมูลลูกค้า	ห้องเก็บแฟ้ม ชั้น 4	ผอ.ฝ่ายขาย	ลับ	ตู้ล็อก มีรายชื่อผู้รับผิดชอบ	-
3	แบบฟอร์มคำขอ	ระบบเอกสารกลาง (DMS)	สำนักงานเลขานุการ	ปกติ	Login ด้วยอีเมลองค์กร	-

4	ข้อมูลสุขภาพ ผู้รับบริการ	ระบบ EMR (cloud)	ผอ.ฝ่ายบริการ ทางการแพทย์	ลับมาก	Login + OTP ผ่าน VPN	มีการ เข้ารหัส ข้อมูล

9.1.2 มีการเฝ้าระวังและคอยตรวจสอบข้อมูลที่เข้าออกจากระบบ ข้อมูลที่ขาดหาย หรือข้อมูลที่ไม่ถูกส่งกลับคืนมา

สิ่งที่ต้องทำ: มีการเฝ้าระวังและคอยตรวจสอบข้อมูลที่เข้าออกจากระบบ ข้อมูลที่ขาดหาย หรือข้อมูลที่ไม่ถูกส่งกลับคืนมา โดยมีเอกสารสนับสนุน

หลักฐาน: นโยบายการเฝ้าระวังและตรวจสอบข้อมูลส่วนบุคคล

บัญชีทรัพย์สินสารสนเทศ

รายงานการตรวจสอบการประมวลผลข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (4)

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

(1) นโยบายการเฝ้าระวังและตรวจสอบข้อมูลส่วนบุคคล

ชื่อองค์กร: [ชื่อองค์กร]

เรื่อง: นโยบายการเฝ้าระวังและตรวจสอบข้อมูลส่วนบุคคล

ประกาศ ณ วันที่: 1 เมษายน พ.ศ. 2568

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการเฝ้าระวัง ตรวจสอบ และติดตามข้อมูลที่เข้าออกจากระบบ รวมถึงการตรวจสอบเหตุการณ์ผิดปกติ เช่น ข้อมูลที่หาย หรือไม่ถูกส่งกลับคืนมา อันเป็นการป้องกันความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลส่วนบุคคลที่องค์กรรับผิดชอบ

2. ขอบเขต

นโยบายนี้ใช้กับข้อมูลส่วนบุคคลทั้งหมดที่องค์กรควบคุม ไม่ว่าจะจัดเก็บในรูปแบบเอกสารหรือระบบดิจิทัล ทั้งภายในและภายนอกองค์กร

3. นโยบายและแนวปฏิบัติ

3.1 การเฝ้าระวังข้อมูลที่เข้าและออกจากระบบ

- มีการติดตั้งระบบ Firewall, IDS/IPS (Intrusion Detection/Prevention Systems) และ DLP (Data Loss Prevention) เพื่อตรวจสอบและควบคุมข้อมูลที่เข้าและออก

- ระบบทำบันทึก Log ทุกกิจกรรม เช่น การดาวน์โหลด ส่งออก และอัปโหลดข้อมูล ผ่านระบบ SIEM

3.2 การตรวจสอบข้อมูลที่ขาดหายหรือไม่ถูกส่งคืน

- เจ้าหน้าที่ผู้รับผิดชอบแต่ละหน่วยงานจะต้องมีรายงานตรวจสอบความครบถ้วนของข้อมูล (Data Reconciliation Report)
- หากพบความผิดปกติ ต้องรายงานให้ DPO ภายใน 24 ชั่วโมง และดำเนินการแก้ไขภายใน 3 วันทำการ

3.3 การบันทึกและรายงาน

- ทุกการตรวจสอบต้องมี บันทึกเหตุการณ์ (Audit Trail)
- รายงานการประมวลผลข้อมูลต้องส่งให้คณะกรรมการ DPO อย่างน้อยไตรมาสละ 1 ครั้ง

4. การบังคับใช้และความรับผิดชอบ

- DPO เป็นผู้รับผิดชอบหลักในการกำกับดูแล ตรวจสอบ และรายงาน
- การละเมิดนโยบายนี้ อาจถูกลงโทษทางวินัย และอาจมีความผิดทางปกครองตาม มาตรา 37 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ลงชื่อ

นาย..... (ผู้อำนวยการ)

[ชื่อองค์กร]

(2) บัญชีทรัพย์สินสารสนเทศ (ฉบับเพิ่มเติมที่เน้นระบบเฝ้าระวัง)

ลำดับ	ระบบ/ทรัพย์สินสารสนเทศ	ข้อมูลที่จัดเก็บ	ระบบเฝ้าระวังข้อมูลเข้าออก	เจ้าของข้อมูล	หมายเหตุ
1	ระบบ HR Cloud	ข้อมูลพนักงาน	DLP, Firewall, Log Access	ผอ.กองบุคคล	มีรายงานการตรวจสอบรายเดือน
2	ระบบบัญชี EMR	ข้อมูลสุขภาพผู้ป่วย	SIEM, IPS	ผอ.ฝ่ายการแพทย์	ระบบแจ้งเตือนอัตโนมัติ
3	ระบบสารบรรณกลาง (DMS)	หนังสือราชการ	Audit Log + VPN	สำนักงานเลขานุการ	เข้าระบบด้วย 2FA

(3) ตัวอย่างรายงานการตรวจสอบการประมวลผลข้อมูลส่วนบุคคล

ชื่อรายงาน: รายงานการตรวจสอบข้อมูลที่เข้าออกระบบ และการติดตามข้อมูลที่ขาดหาย

หน่วยงาน: ฝ่ายเทคโนโลยีสารสนเทศ

ช่วงเวลา: 1 - 31 มีนาคม 2568

วันที่	ระบบที่ตรวจสอบ	เหตุการณ์ผิดปกติ	วิธีการตรวจสอบ	ผลการดำเนินการ
5 มี.ค.	ระบบ DMS	พบ Log ผิดปกติ: ดาวน์ โหลดแฟ้มขนาดใหญ่เวลา 03.00 น.	ตรวจสอบ Log / ยืนยันกับผู้ใช้	เป็นเจ้าหน้าที่ไอที ทำงาน ล่วงเวลา มีเอกสารยืนยัน
12 มี.ค.	ระบบ EMR	ข้อมูลไม่ถูก sync กลับจาก คลินิกภายนอก	ตรวจสอบระบบ VPN และ API	ระบบล่มชั่วคราว แก้ไข แล้วและส่งข้อมูลคืน สำเร็จ
25 มี.ค.	ระบบ HR Cloud	พบ Log ของ IP แปลกจาก ภายนอกพยายามเข้าระบบ	Firewall และ SIEM แจ้งเตือน	บล็อก IP และเพิ่ม whitelist ใหม่

ผู้จัดทำรายงาน

นายณัฐพล อินทรสุข

เจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศ

รับรองโดย

นางสาวกัญญชลา สุวรรณกิจ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ลงชื่อ

9.1.3 องค์กรมีนโยบายและแนวปฏิบัติเพื่อจัดเก็บ แยกหมวดหมู่ และทำดัชนี (index) สำหรับรายการข้อมูลส่วนบุคคลต่าง ๆ เพื่อสนับสนุนการบริหารข้อมูล การค้นหาข้อมูล และการทำลายข้อมูล

สิ่งที่ต้องทำ: องค์กรมีนโยบายหรือแนวปฏิบัติเพื่อจัดเก็บ แยกหมวดหมู่ และทำดัชนี (index) สำหรับรายการข้อมูลส่วนบุคคลต่าง ๆ เพื่อสนับสนุนการบริหารข้อมูล การค้นหาข้อมูล และการทำลายข้อมูล และมีเอกสารสนับสนุน

หลักฐาน: นโยบายและแนวปฏิบัติ (คู่มือ) เพื่อจัดเก็บ แยกหมวดหมู่ และทำดัชนี (index) สำหรับรายการข้อมูลส่วนบุคคล

คู่มือการจัดเก็บ แยกหมวดหมู่ และทำดัชนีข้อมูลส่วนบุคคล

ทะเบียนการประมวลผลข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยผู้
 ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)
 โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3
 ล้านบาท

(1) นโยบายและแนวปฏิบัติเพื่อจัดเก็บ แยกหมวดหมู่ และทำดัชนีข้อมูลส่วนบุคคล

ชื่อเอกสาร: นโยบายและแนวปฏิบัติในการจัดเก็บ แยกหมวดหมู่ และทำดัชนีข้อมูลส่วนบุคคล

ประกาศโดย: [ชื่อองค์กร]

ประกาศ ณ วันที่: 1 เมษายน พ.ศ. 2568

1. วัตถุประสงค์

เพื่อกำหนดหลักเกณฑ์ในการจัดเก็บ แยกหมวดหมู่ และจัดทำดัชนี (index) ของรายการข้อมูลส่วนบุคคลอย่างเป็นระบบ เพื่อสนับสนุนการบริหารจัดการข้อมูลที่มีประสิทธิภาพ และสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล

2. ขอบเขต

นโยบายนี้ครอบคลุมถึงข้อมูลส่วนบุคคลที่จัดเก็บในระบบสารสนเทศ และเอกสารที่เป็นรูปแบบกระดาษภายในองค์กรทุกหน่วยงาน

3. แนวปฏิบัติ

3.1 การจัดเก็บข้อมูล

- ข้อมูลส่วนบุคคลต้องจัดเก็บในพื้นที่ที่กำหนด มีระบบควบคุมการเข้าถึง
- สำหรับเอกสารกระดาษ ให้จัดเก็บในตู้ที่มีการล็อกและบันทึกผู้เข้าถึง

3.2 การแยกหมวดหมู่

- ข้อมูลต้องถูกแยกหมวดหมู่ตามประเภท เช่น:
- ข้อมูลบุคคลภายในองค์กร (เช่น ข้อมูลพนักงาน)
- ข้อมูลจากบุคคลภายนอก (เช่น ลูกค้า ผู้รับบริการ)
- ข้อมูลอ่อนไหว (Sensitive Data)

ใช้ระบบรหัสหมวดหมู่ เช่น EMP-001, CUS-001, SENS-001

3.3 การทำดัชนี (Index)

ทุกรายการข้อมูลจะต้องมีรหัสประจำรายการและดัชนีค้นหาในระบบหรือในสมุดทะเบียนระบบสารสนเทศจะต้องมีระบบค้นหา (Search Function) ที่สามารถเข้าถึงข้อมูลตามรหัสหมวดหมู่ได้อย่างรวดเร็ว

3.4 การบริหารจัดการข้อมูลเพื่อการค้นหาและทำลาย

ต้องมี คู่มือการค้นหาและจัดการข้อมูล เพื่อบริการผู้ใช้สิทธิของเจ้าของข้อมูล

ข้อมูลที่หมดอายุการจัดเก็บ ต้องดำเนินการลบหรือทำลายตามขั้นตอนที่กำหนด

4. ความรับผิดชอบ

- DPO เป็นผู้ควบคุมการใช้ดัชนีและกำกับการจัดหมวดหมู่ข้อมูล
- เจ้าหน้าที่สารสนเทศประจำหน่วยงานรับผิดชอบการจัดทำทะเบียนประมวลผลข้อมูลส่วนบุคคลให้ทันสมัย

(2) คู่มือการจัดเก็บ แยกหมวดหมู่ และทำดัชนีข้อมูลส่วนบุคคล

ชื่อเอกสาร: คู่มือการจัดเก็บ แยกหมวดหมู่ และทำดัชนีข้อมูลส่วนบุคคล

ประกาศโดย: งานบริหารจัดการข้อมูล / สำนักงาน DPO

โครงสร้างคู่มือ:

บทที่ 1: นิยามที่เกี่ยวข้อง

- ข้อมูลส่วนบุคคล / หมวดหมู่ข้อมูล / ดัชนี
- ข้อมูลที่ต้องควบคุมเป็นพิเศษ (Sensitive Data)

บทที่ 2: แนวทางปฏิบัติ

2.1 ขั้นตอนการจัดเก็บ

- ระบุประเภทของสื่อที่ใช้ (ดิจิทัล/กระดาษ)
- มาตรการการควบคุมการเข้าถึง (Access Control)

2.2 การแยกหมวดหมู่

- การจำแนกตามวัตถุประสงค์
- การกำหนดชื่อหมวดและรหัสเฉพาะ

2.3 การสร้างดัชนี

ตัวอย่างการจัดทำ index

รหัส	ชื่อข้อมูล	ประเภท	เจ้าของ	วันที่เก็บ	สถานที่จัดเก็บ
EMP001	ข้อมูลพนักงาน	บุคคลภายใน	แผนกบุคคล	1 ม.ค. 2567	Server HR

2.4 การทำลายข้อมูล

- ขั้นตอนการยืนยันสิ้นสุดการใช้
- แบบฟอร์มขอลบข้อมูล
- บันทึกการทำลายข้อมูล

(3) ตัวอย่างทะเบียนการประมวลผลข้อมูลส่วนบุคคล (RoPA)

ลำดับ	หมวดหมู่ข้อมูล	วัตถุประสงค์	ระบบที่ใช้ จัดเก็บ	เจ้าของข้อมูล	ระยะเวลาเก็บ รักษา
1	ข้อมูลพนักงาน (EMP)	บริหารงาน บุคคล	ระบบ HR Cloud	พนักงาน	10 ปี
2	ข้อมูลลูกค้า (CUS)	การให้บริการ	ระบบ CRM	ผู้รับบริการ	5 ปี
3	ข้อมูลอ่อนไหว (SENS)	ประกันสุขภาพ	ระบบ EMR	พนักงาน/ ผู้ป่วย	ตามข้อกำหนด

ผู้รับผิดชอบ

นายวรวิทย์ บุญธรรม

เจ้าหน้าที่จัดการข้อมูล (Data Steward)

9.1.4 มีการจัดทำดัชนี (index) สำหรับรายการข้อมูลที่จัดเก็บไว้นอกสถานที่ เพื่อให้สามารถเข้าถึงและติดตามข้อมูลได้อย่างถูกต้อง

สิ่งที่ต้องทำ: มีการจัดทำดัชนี (index) สำหรับรายการข้อมูลที่จัดเก็บไว้นอกสถานที่ เพื่อให้สามารถเข้าถึงและติดตามข้อมูลได้อย่างถูกต้อง และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการจัดทำดัชนี (index) สำหรับรายการข้อมูลส่วนบุคคลที่จัดเก็บไว้นอกสถานที่
ดัชนี (index) สำหรับรายการข้อมูลส่วนบุคคลที่จัดเก็บไว้นอกสถานที่

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

(1) นโยบายการจัดทำดัชนี (Index) สำหรับรายการข้อมูลส่วนบุคคลที่จัดเก็บไว้นอกสถานที่

ชื่อเอกสาร: นโยบายการจัดทำดัชนีข้อมูลส่วนบุคคลที่จัดเก็บนอกสถานที่

ประกาศโดย: [ชื่อองค์กร]

ประกาศ ณ วันที่: [ระบุวันที่]

1. วัตถุประสงค์

เพื่อกำหนดแนวทางในการติดตาม ควบคุม และค้นหาข้อมูลส่วนบุคคลที่มีการจัดเก็บไว้นอกสถานที่อย่างมีประสิทธิภาพ และสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

2. ขอบเขต

นโยบายนี้ครอบคลุมข้อมูลส่วนบุคคลทุกรูปแบบที่มีการจัดเก็บในสถานที่ที่อยู่นอกสำนักงานหลักขององค์กร เช่น:

- พื้นที่จัดเก็บเอกสารสำรอง
- ศูนย์ข้อมูลภายนอก (Data Center / Cloud Provider)
- ระบบที่อยู่ในความดูแลของผู้ประมวลผลข้อมูล (Processor)

3. นิยาม

- **ข้อมูลนอกสถานที่** หมายถึง ข้อมูลส่วนบุคคลที่ได้จัดเก็บในระบบหลักขององค์กร แต่ยังคงอยู่ภายใต้ความรับผิดชอบของผู้ควบคุมข้อมูล
- **Index** หมายถึง การบรรยายละเอียดข้อมูลที่จัดเก็บไว้แต่ละรายการอย่างมีระบบ เพื่อให้สามารถเข้าถึงและติดตามได้

4. แนวปฏิบัติ

4.1 การกำหนด Index

ต้องมีการจัดทำทะเบียน Index สำหรับข้อมูลทุกชุดที่จัดเก็บนอกสถานที่
รายละเอียดใน Index ประกอบด้วย:

- รหัสข้อมูล (Data Code)
- ชื่อข้อมูล
- ประเภทข้อมูล
- ผู้รับผิดชอบ
- สถานที่จัดเก็บ (เช่น Cloud, สาขา, ศูนย์จัดเก็บ)
- วันที่จัดเก็บ / วันที่สิ้นสุด
- สถานะการเข้าถึง
- ความถี่ในการสำรองข้อมูล

4.2 การตรวจสอบ

- DPO หรือเจ้าหน้าที่ข้อมูลต้องมีการตรวจสอบรายการ Index อย่างน้อยปีละ 1 ครั้ง
- ในกรณีพบว่ามีข้อมูลหมดอายุ ต้องดำเนินการลบหรือทำลายตามขั้นตอน

4.3 การรายงาน

ต้องจัดทำรายงานการติดตามข้อมูลนอกสถานที่เสนอผู้บริหารอย่างน้อยทุก 6 เดือน

(2) ตัวอย่าง Index สำหรับรายการข้อมูลส่วนบุคคลที่จัดเก็บนอกสถานที่

ลำดับ	รหัสข้อมูล	ชื่อข้อมูล	ประเภท	สถานที่จัดเก็บ	ผู้รับผิดชอบ	วันที่จัดเก็บ	วันที่หมดอายุ	หมายเหตุ
1	EXT001	ข้อมูลผู้ป่วยย้อนหลัง 10 ปี	Sensitive Data	บริษัท ABC Cloud Storage	ฝ่าย IT โรงพยาบาล	01/01/2566	01/01/2576	สัญญาจัดเก็บระยะยาว
2	EXT002	สำเนาบัตรประชาชนผู้สมัครงาน	Personal Data	สาขา พัทยา – ตู้เก็บเอกสาร	HR สาขา	15/03/2567	15/03/2570	ต้องลบทันทีหลังหมดอายุ
3	EXT003	ข้อมูลแบบสอบถามลูกค้า	Personal Data	Data Center จังหวัดชลบุรี	ฝ่ายการตลาด	01/08/2566	01/08/2569	จัดเก็บพร้อมระบบสำรอง
4	EXT004	ข้อมูลรายชื่อผู้บริจาค	Personal Data	ศูนย์รับบริจาค สาขา เชียงใหม่	แผนก CSR	01/10/2565	01/10/2568	-

หมายเหตุ

- ควรกำหนดเจ้าหน้าที่ประจำท้องถิ่นในแต่ละสาขาเป็น “ผู้ควบคุม Index” เพื่อความพร้อมในการตรวจสอบข้อมูลจริง
- กำหนดรหัสข้อมูลไม่ซ้ำกัน (Unique ID) เพื่อการอ้างอิงที่ง่าย

(3) เอกสารแนบอื่น ๆ ที่แนะนำ

- บันทึกส่งมอบ/บันทึกการจัดเก็บข้อมูลนอกสถานที่
- รายงานการตรวจสอบข้อมูลที่จัดเก็บนอกสถานที่
- สัญญาหรือข้อตกลงการให้บริการกับผู้ให้บริการจัดเก็บข้อมูล (ถ้ามี)

9.2 ความมั่นคงปลอดภัยสำหรับการส่งหรือโอนข้อมูล (Security for transfers) มีมาตรการด้านความมั่นคงปลอดภัยที่เหมาะสมเพื่อปกป้องข้อมูลระหว่างการส่งหรือโอนไปหรือรับมาจากองค์กรภายนอก

9.2.1 มีแนวปฏิบัติสำหรับการป้องกันการส่งหรือโอนข้อมูล ทั้งภายในและภายนอกองค์กร ไม่ว่าจะด้วยวิธีการส่งทางไปรษณีย์ ทางแฟกซ์ หรือวิธีการทางอิเล็กทรอนิกส์อื่น ๆ

สิ่งที่ต้องทำ: มีแนวปฏิบัติสำหรับการป้องกันการส่งหรือโอนข้อมูลทั้งภายในและภายนอกองค์กร ไม่ว่าจะด้วยวิธีการส่งทางไปรษณีย์ ทางแฟกซ์ หรือวิธีการทางอิเล็กทรอนิกส์อื่น ๆ และมีเอกสารสนับสนุน

หลักฐาน: นโยบายการกำหนดมาตรการด้านความมั่นคงปลอดภัยที่เหมาะสมเพื่อปกป้องข้อมูลระหว่างการส่งหรือโอนไปหรือรับมาจากองค์กรภายนอก
ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
ข้อตกลงการส่งหรือโอนข้อมูลส่วนบุคคล
บันทึกข้อตกลงรักษาความลับ

รายงานการตรวจสอบการปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคล
สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

โทษทางอาญา: กรณี Sensitive Data เป็นไปตามฐานความผิดเกี่ยวกับการฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 27

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท หรือ 5 ล้านบาท

(1) นโยบายการโอนและส่งข้อมูลส่วนบุคคลอย่างปลอดภัย

ชื่อเอกสาร: นโยบายการโอนและส่งข้อมูลส่วนบุคคลอย่างปลอดภัย

หน่วยงานที่รับผิดชอบ: [ชื่อหน่วยงานหรือองค์กร]

วันที่ประกาศใช้: [ระบุวันที่]

1. วัตถุประสงค์

เพื่อกำหนดแนวทางในการส่งหรือโอนข้อมูลส่วนบุคคลทั้งภายในและภายนอกองค์กรให้มีความมั่นคงปลอดภัย ป้องกันการรั่วไหลหรือเข้าถึงโดยไม่ได้รับอนุญาต

2. ขอบเขต

- นโยบายนี้ใช้กับวิธีการส่งหรือโอนข้อมูลทุกช่องทาง ได้แก่:
- การส่งทางไปรษณีย์ (เช่น เอกสารสำคัญ, แฟ้มข้อมูล)
- การส่งทางโทรสาร (แฟกซ์)
- การส่งผ่านอีเมล ระบบคลาวด์ หรือแพลตฟอร์มอิเล็กทรอนิกส์อื่น ๆ

3. แนวปฏิบัติ

3.1 การส่งข้อมูลภายในองค์กร

- ใช้ระบบภายในที่มีการยืนยันตัวตน เช่น Intranet หรือระบบ HRM/ERP ที่ปลอดภัย
- หลีกเลี่ยงการส่งข้อมูลผ่านช่องทางที่ไม่เข้ารหัส เช่น อีเมลทั่วไป
- หากใช้ Flash Drive หรือ External HDD ต้องเข้ารหัสข้อมูลก่อน

3.2 การส่งข้อมูลทางไปรษณีย์

- ต้องใส่เอกสารในซองปิดผนึกแน่นหนา พร้อมระบุ "เอกสารลับเฉพาะบุคคล"
- กำหนดผู้รับไว้ชัดเจน และส่งโดยวิธีลงทะเบียนหรือ EMS เท่านั้น
- บันทึกหมายเลขพัสดุและติดตามการส่งทุกครั้ง

3.3 การส่งทางแฟกซ์

- ยืนยันหมายเลขแฟกซ์กับผู้รับก่อนทุกครั้ง
- โทรแจ้งปลายทางก่อนและหลังการส่ง
- ห้ามส่งข้อมูล Sensitive ผ่านแฟกซ์ ยกเว้นได้รับอนุญาตเฉพาะกรณี

3.4 การส่งทางอีเมลหรือระบบอิเล็กทรอนิกส์

- ต้องใช้บัญชีอีเมลขององค์กรเท่านั้น
- แนบไฟล์ในรูปแบบที่เข้ารหัส (เช่น PDF with password) และแจ้งรหัสผ่านแยกต่างหาก
- ห้ามใช้ Gmail, Hotmail หรือบัญชีส่วนตัวในการส่งข้อมูลส่วนบุคคล
- หากใช้ Cloud (เช่น Google Drive, OneDrive) ต้องจำกัดสิทธิ์การเข้าถึงเฉพาะผู้ที่มีความจำเป็น

3.5 การโอนข้อมูลไปยังบุคคลภายนอก

- ต้องมี ข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement) หรือ ข้อตกลงการส่งหรือโอนข้อมูล ก่อนทุกครั้ง
- หากโอนข้อมูลข้ามประเทศ ต้องตรวจสอบว่าประเทศนั้นมีมาตรการคุ้มครองเพียงพอ หรือใช้ Standard Contractual Clauses
- ต้องมี บันทึกข้อตกลงรักษาความลับ (NDA) กับผู้รับข้อมูล

3.6 การติดตามและตรวจสอบ

- มีระบบ log การส่งข้อมูล และการตรวจสอบย้อนหลังได้

- หน่วยงาน DPO ต้องจัดทำรายงานการตรวจสอบการส่งหรือโอนข้อมูลอย่างน้อยปีละ 1 ครั้ง

(2) ตัวอย่างรายการ “หลักฐาน” ที่ใช้ในการประเมิน

นโยบายและแนวปฏิบัติ

- นโยบายการโอนและส่งข้อมูล (ตามตัวอย่างด้านบน)
- แนวทางการเข้ารหัสข้อมูลก่อนส่ง

เอกสารประกอบ/บันทึก

- บันทึกส่งเอกสารสำคัญ (พร้อมเลขพัสดุ EMS)
- Log การส่งอีเมลพร้อมรายงาน Audit Trail
- แบบฟอร์มคำขออนุญาตโอนข้อมูลส่วนบุคคล

ข้อตกลง Data Processing Agreement (DPA)

ข้อตกลงการส่งข้อมูลส่วนบุคคล (ระบุวัตถุประสงค์, ระยะเวลา, วิธีการส่ง, ความรับผิดชอบ)

บันทึกข้อตกลงรักษาความลับ (NDA) ระหว่างหน่วยงาน

รายงานการตรวจสอบ:

- รายงานการตรวจติดตามการโอนข้อมูลโดย DPO
- รายงานกรณีข้อมูลหลุดรั่ว (ถ้ามี) พร้อมแนวทางแก้ไข

แนวปฏิบัติสำหรับการป้องกันการส่งหรือโอนข้อมูลส่วนบุคคล ทั้งภายในและภายนอกองค์กร

การส่งข้อมูลภายในองค์กร

- 1.1 ผู้ส่งต้องตรวจสอบว่าผู้รับเป็นบุคคลภายในที่มีหน้าที่เกี่ยวข้องโดยตรงกับวัตถุประสงค์ของการใช้ข้อมูล
- 1.2 ต้องใช้ช่องทางการส่งข้อมูลที่มีความมั่นคงปลอดภัย เช่น ระบบอีเมลขององค์กรที่มีการเข้ารหัส การแชร์ผ่านระบบภายในองค์กรที่มีการควบคุมสิทธิ์
- 1.3 ห้ามใช้ช่องทางส่วนบุคคล เช่น อีเมลส่วนตัว หรือแอปพลิเคชันที่ไม่ได้รับอนุญาตจากองค์กร เช่น Line หรือ Messenger
- 1.4 หากจำเป็นต้องถ่ายโอนผ่านสื่อบันทึกข้อมูล เช่น USB Drive ต้องมีการเข้ารหัสไฟล์ก่อนทุกครั้ง และจัดเก็บในสื่อที่สามารถควบคุมการเข้าถึงได้
- 1.5 ควรจัดทำบันทึกการส่งข้อมูลภายใน เช่น แบบฟอร์มส่งงาน หรือระบบลงทะเบียนการโอนข้อมูล

การส่งข้อมูลทางไปรษณีย์

- 2.1 เอกสารต้องถูกบรรจุในซองที่ปิดผนึกแน่นหนา ปราศจากช่องให้มองเห็นเนื้อหา
 - 2.2 ระบุชื่อผู้รับและหน่วยงานอย่างชัดเจนบนหน้าซอง พร้อมข้อความ “เอกสารลับ” หรือ “เฉพาะผู้รับเท่านั้น”
 - 2.3 ใช้บริการไปรษณีย์ที่สามารถติดตามได้ เช่น EMS หรือบริการส่งเอกสารของบริษัทเอกชนที่มีระบบ Tracking
 - 2.4 จัดเก็บหมายเลขติดตามการส่งไว้เป็นหลักฐาน และจัดทำทะเบียนส่งเอกสารพร้อมวันที่และผู้ส่ง
- ### การส่งข้อมูลทางโทรสาร (Fax)
- 3.1 ตรวจสอบความถูกต้องของหมายเลขแฟกซ์กับผู้รับก่อนทุกครั้ง
 - 3.2 ติดต่อผู้รับทางโทรศัพท์เพื่อแจ้งก่อนการส่ง เพื่อให้ผู้รับอยู่ที่เครื่องแฟกซ์และเก็บข้อมูลทันที
 - 3.3 หลังส่งเสร็จ ให้โทรแจ้งผู้รับอีกครั้งเพื่อยืนยันการรับและขอให้ทำลายสำเนาหากได้รับผิดพลาด
 - 3.4 หลีกเลี่ยงการส่งข้อมูลที่มีความละเอียดอ่อนหรือข้อมูลอ่อนไหวผ่านแฟกซ์ หากจำเป็นต้องขออนุญาตเป็น

กรณีพิเศษจากผู้ควบคุมข้อมูล

การส่งข้อมูลทางอิเล็กทรอนิกส์ เช่น อีเมล หรือระบบคลาวด์

- 4.1 ต้องใช้บัญชีอีเมลองค์กรที่มีระบบยืนยันตัวตนแบบสองชั้น (2-Factor Authentication)
- 4.2 แนบไฟล์ข้อมูลในรูปแบบที่มีการเข้ารหัส เช่น PDF ที่มีรหัสผ่าน หรือ ZIP พร้อมรหัสผ่าน

- 4.3 ส่งรหัสผ่านสำหรับเปิดไฟล์แยกต่างหากจากช่องทางหลัก เช่น แฉทางโทรศัพท์ หรือแอปเข้ารหัสข้อความ
- 4.4 ห้ามแนบข้อมูลส่วนบุคคลในเนื้อหาของอีเมลโดยตรง ต้องอยู่ในเอกสารแนบเท่านั้น
- 4.5 หากส่งผ่านระบบคลาวด์ เช่น Google Drive หรือ Microsoft OneDrive ต้องตั้งค่าการเข้าถึงแบบจำกัดเฉพาะผู้รับ และกำหนดวันหมดอายุของลิงก์
- 4.6 ควรจัดทำ Log การส่งไฟล์หรือสร้างรายงานการเข้าถึงข้อมูล (access log) เพื่อใช้ในการติดตามกรณีเกิดเหตุผิดปกติ

การโอนข้อมูลให้กับบุคคลภายนอกหรือหน่วยงานภายนอก

- 5.1 ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนการโอน เว้นแต่มีฐานทางกฎหมายที่ชัดเจน
- 5.2 ต้องจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement – DPA) กับผู้รับข้อมูลก่อนเริ่มโอน
- 5.3 หากมีการโอนข้อมูลข้ามประเทศ ต้องตรวจสอบว่าประเทศปลายทางมีมาตรการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ หรือใช้สัญญามาตรฐาน (Standard Contractual Clauses – SCCs)
- 5.4 ต้องมีบันทึกข้อตกลงรักษาความลับ (Non-Disclosure Agreement – NDA) และระบุบทลงโทษหากมีการละเมิดข้อมูล
- 5.5 ควรมีการทดสอบระบบรักษาความปลอดภัยของผู้รับข้อมูล (เช่น การประเมินความเสี่ยง) ก่อนโอนข้อมูลจริง
- 5.6 ต้องจัดเก็บหลักฐานการโอน เช่น หนังสือส่งมอบเอกสาร รายงาน log การส่งผ่านระบบ พร้อมลงนามรับรองทั้งสองฝ่าย

การควบคุมภายหลังการโอนข้อมูล

- 6.1 ผู้ส่งข้อมูลต้องตรวจสอบว่าข้อมูลถูกใช้งานตามวัตถุประสงค์ที่แจ้งไว้
- 6.2 หากมีเหตุผิดปกติ เช่น การรั่วไหลข้อมูล หรือการเข้าถึงโดยไม่ได้รับอนุญาต ต้องแจ้งเจ้าของข้อมูล และหน่วยงานควบคุมข้อมูลภายในองค์กรทันที
- 6.3 หน่วยงาน DPO ต้องมีระบบติดตามการส่งหรือโอนข้อมูล และจัดทำรายงานตรวจสอบอย่างสม่ำเสมอ
- 6.4 การโอนข้อมูลซ้ำต้องได้รับการอนุมัติใหม่ทุกครั้ง ยกเว้นมีการระบุไว้ในข้อตกลงเดิมว่าอนุญาตให้โอนซ้ำได้ภายใต้เงื่อนไขเดิม

9.2.3 เมื่อต้องมีการส่งหรือโอนข้อมูลออกไปยังนอกสถานที่ วิธีการที่ใช้ในการส่งหรือโอนข้อมูลมีความปลอดภัย เช่น เลือกใช้เมสเซนเจอร์ที่มีความน่าเชื่อถือ ใช้การเข้ารหัสข้อมูล ใช้โปรโตคอลในการส่งหรือโอนข้อมูลที่มีความมั่นคงปลอดภัย หรือใช้ VPN เป็นต้น รวมทั้งมีการตรวจสอบว่าข้อมูลที่จัดส่งไปนั้นได้รับอย่างถูกต้อง

สิ่งที่ต้องทำ: เมื่อต้องมีการส่งหรือโอนข้อมูลออกไปยังนอกสถานที่ วิธีการที่ใช้ในการส่งหรือโอนข้อมูลมีความปลอดภัย เช่น เลือกใช้เมสเซนเจอร์ที่มีความน่าเชื่อถือ ใช้การเข้ารหัสข้อมูล ใช้โปรโตคอลในการส่งหรือโอนข้อมูลที่มีความมั่นคงปลอดภัย หรือใช้ VPN เป็นต้น รวมทั้งมีการตรวจสอบว่าข้อมูลที่จัดส่งไปนั้นได้รับอย่างถูกต้อง

หลักฐาน: นโยบายเพื่อรักษาความปลอดภัยด้านการโอนข้อมูลส่วนบุคคล

ทะเบียนการส่งหรือโอนข้อมูลส่วนบุคคล

หนังสือรับโอนข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

โทษทางอาญา กรณี Sensitive Data เป็นไปตามฐานความผิดเกี่ยวกับการฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 27

โทษทางปกครอง ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท หรือ 5 ล้านบาท

นโยบายเพื่อรักษาความปลอดภัยด้านการโอนข้อมูลส่วนบุคคล

(Personal Data Transfer Security Policy)

1) วัตถุประสงค์

กำหนดหลักการ มาตรการ และวิธีปฏิบัติที่ปลอดภัยในการส่งหรือโอนข้อมูลส่วนบุคคลออกไปยังนอกสถานที่/นอกเครือข่ายองค์กร (รวมถึงการโอนให้บุคคลภายนอก ผู้ประมวลผลข้อมูล และการโอนข้ามพรมแดน) เพื่อให้สอดคล้องกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act: PDPA) และมาตรฐานความมั่นคงปลอดภัยสารสนเทศขององค์กร

2) ขอบเขต

ครอบคลุมข้อมูลส่วนบุคคลทุกประเภทและทุกสื่อ (ดิจิทัล/กระดาษ/สื่อบันทึก), บุคลากรทุกกลุ่ม (พนักงาน ผู้รับจ้าง ที่ปรึกษา), ระบบแอปพลิเคชัน อุปกรณ์พกพา และผู้รับข้อมูลภายนอก รวมถึง ผู้ประมวลผล

ข้อมูลส่วนบุคคล (Data Processor: Processor) และ ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง (Sub-processor)

3) คำนิยาม

- ข้อมูลส่วนบุคคล (Personal Data): ข้อมูลที่ทำให้สามารถระบุตัวบุคคลได้โดยตรงหรือโดยอ้อม
- การโอนข้อมูล (Data Transfer): การส่ง เคลื่อนย้าย คัดลอก เปิดเผย หรือให้เข้าถึงข้อมูลไปยังนอกสถานที่/นอกเครือข่าย/บุคคลภายนอก
- ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller: Controller): บุคคลหรือนิติบุคคลที่มีอำนาจตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor: Processor): บุคคลหรือนิติบุคคลที่ประมวลผลข้อมูลตามคำสั่งของผู้ควบคุมข้อมูล
- ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง (Sub-processor): บุคคลหรือนิติบุคคลที่ผู้ประมวลผลข้อมูลว่าจ้างเพื่อดำเนินการแทน
- การเข้ารหัส (Encryption): วิธีการปกป้องข้อมูลด้วยการแปลงให้อยู่ในรูปที่ไม่สามารถอ่านได้ เว้นแต่จะมีรหัสกุญแจถอดรหัส
- การตรวจสอบความถูกต้องของการรับ (Delivery Verification): การยืนยันว่าผู้รับได้รับข้อมูลครบถ้วนและไม่ถูกเปลี่ยนแปลง เช่น การตรวจสอบค่า เช็คซัม (Checksum) ด้วยอัลกอริทึม SHA-256

4) หลักการทั่วไป

1. จำเป็นเท่านั้น (Data Minimization & Need-to-Know): ส่งเฉพาะข้อมูลที่เป็นไปตามวัตถุประสงค์และฐานกฎหมาย
2. การอนุมัติล่วงหน้า: การโอนข้อมูลที่จัดขึ้นเป็น “ลับ/ลับยิ่ง” หรือการโอนข้ามพรมแดน ต้องได้รับอนุมัติจากผู้บังคับบัญชาและ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)
3. การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA): ใช้เมื่อโอนข้อมูลผ่านช่องทางที่ต้องล็อกอิน เช่น โพรโทคอลการถ่ายโอนไฟล์แบบปลอดภัย (Secure File Transfer Protocol: SFTP) หรือ เครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)
4. การเข้ารหัสบังคับ (Mandatory Encryption): ขณะส่งต้องใช้ โพรโทคอลการรักษาความปลอดภัยระดับการส่งผ่าน (Transport Layer Security: TLS) เวอร์ชัน 1.2 ขึ้นไป, HTTPS, FTPS และเข้ารหัสไฟล์ด้วย มาตรฐานการเข้ารหัสขั้นสูง (Advanced Encryption Standard: AES) ขนาด 256 บิต

5. การบันทึกและตรวจสอบได้: ต้องบันทึกใน ทะเบียนการส่งหรือโอนข้อมูลส่วนบุคคล ระบุผู้ส่ง ผู้รับ วัตถุประสงค์ วันเวลา ช่องทาง และค่าแฮชไฟล์
6. การยืนยันการรับ: ผู้รับต้องออก หนังสือรับโอนข้อมูลส่วนบุคคล หรือมีระบบหลักฐานอัตโนมัติ
7. ข้อห้าม: ห้ามใช้แอปหรืออีเมลส่วนตัวที่ไม่ได้รับอนุญาต ห้ามส่งข้อมูลโดยไม่มีการเข้ารหัส ห้ามฝากไฟล์บนบริการสาธารณะที่ไม่ควบคุมสิทธิ์

5) การจัดชั้นข้อมูลและการควบคุมขั้นต่ำ

- ภายใน (Internal): ส่งผ่านอีเมลองค์กรที่เข้ารหัส TLS + กำกับสิทธิ์เข้าถึง
- ลับ (Confidential): เข้ารหัสไฟล์ AES-256 + ส่งผ่าน SFTP/HTTPS + MFA + ตรวจสอบเช็คซัม + หนังสือรับโอน
- ลับยิ่ง/อ่อนไหวพิเศษ (Highly Confidential / Sensitive Data) เช่น ข้อมูลสุขภาพ ชีวภาพเด็ก → ต้องเข้ารหัส AES-256 + ส่งผ่าน SFTP/MFT ผ่าน VPN + มีข้อตกลงไม่เปิดเผยข้อมูล (Non-Disclosure Agreement: NDA) + การอนุมัติจาก DPO + หนังสือรับโอนพร้อมลายเซ็นดิจิทัล

6) วิธีการโอนที่อนุญาตและเงื่อนไข

1. อิเล็กทรอนิกส์

- SFTP/FTPS/HTTPS (TLS $\geq$ 1.2): ต้องใช้บัญชีส่วนบุคคล + MFA + จำกัด IP
- อีเมลองค์กร: ใช้ได้เมื่อไฟล์เข้ารหัส AES-256 หรือใช้ S/MIME หรือ PGP
- พอร์ตถ่ายโอนไฟล์ (Managed File Transfer: MFT): ใช้ลิงก์แบบครั้งเดียว มีวันหมดอายุ และบันทึกการดาวน์โหลด
- API/ระบบต่อระบบ: ใช้ mTLS + OAuth 2.0/OIDC + จำกัดขอบเขต (Scope) + Rate Limiting

2. เมสเซนเจอร์/แชท

ใช้ได้เฉพาะแอปที่องค์กรอนุมัติ และต้องเปิด การเข้ารหัสแบบปลายทางถึงปลายทาง (End-to-End Encryption: E2EE) พร้อมเข้ารหัสไฟล์เพิ่ม

3. เครือข่ายส่วนตัวเสมือน (VPN)

สำหรับข้อมูลลับยิ่ง/อ่อนไหวพิเศษ ต้องใช้ VPN ขององค์กร (IPSec/OpenVPN/WireGuard) + MFA + นโยบายไม่แบ่งเส้นทาง (No Split Tunneling)

4. กายภาพ (Physical Media)

ใช้อุปกรณ์ที่เข้ารหัส เช่น USB/HDD ที่เข้ารหัสฮาร์ดแวร์ ใส่ช่องปัดฝุ่น และใช้ผู้ให้บริการขนส่งที่ตรวจสอบแล้ว

7) มาตรฐานการเข้ารหัสและการจัดการกุญแจ

- ไฟล์: ใช้ AES-256-GCM หรือเทียบเท่า
- การแลกเปลี่ยนกุญแจ (Key Exchange): ใช้ RSA-2048 หรือ ECC-256 ขึ้นไป
- การจัดการกุญแจ (Key Management System: KMS) หรือ โมดูลรักษาความปลอดภัยฮาร์ดแวร์ (Hardware Security Module: HSM) ต้องหมุนเวียนรหัสตามรอบ ห้ามแชร์ผ่านช่องทางเดียวกับไฟล์

8) การอนุมัติและเวิร์กโฟลว์ก่อนโอน

1. กรอกคำขอโอนและระบุฐานกฎหมาย
2. ตรวจสอบความจำเป็นและการลดข้อมูล (Data Minimization)
3. ประเมินผลกระทบด้านการคุ้มครองข้อมูล (Data Protection Impact Assessment: DPIA) หากเกี่ยวข้อง
4. ตรวจสอบข้อสัญญาและข้อตกลงการโอนข้ามพรมแดน
5. อนุมัติโดยผู้บังคับบัญชาและ DPO
6. บันทึกลงทะเบียนการโอน

9) การตรวจสอบความถูกต้องและการยืนยันการรับ

- สร้างค่าแฮช SHA-256 ก่อนส่ง
- หลังส่ง ผู้รับต้องตรวจสอบและยืนยันผล
- จัดทำ หนังสือรับโอนข้อมูลส่วนบุคคล
- หากใช้ MFT ให้เก็บ Log/Receipt เป็นหลักฐาน

10) การโอนข้ามพรมแดน

ต้องผ่านการอนุมัติจาก DPO/ฝ่ายกฎหมาย โดยต้องมี กลไกคุ้มครอง (Safeguards) ที่เหมาะสม เช่น สัญญามาตรฐาน (Standard Contractual Clauses: SCCs), ข้อตกลงภายในกลุ่ม (Binding Corporate Rules: BCRs) หรือมาตรการเสริมอื่น ๆ

11) การจัดเก็บหลังโอนและการลบอย่างปลอดภัย

- กำหนดระยะเวลาการเก็บข้อมูล
- เมื่อครบกำหนดให้ลบด้วยวิธีที่ปลอดภัย เช่น Crypto-Erase หรือ Secure Wipe
- บันทึกการลบเป็นหลักฐาน

12) เหตุการณ์ผิดปกติและการแจ้งเหตุ

- เมื่อพบความผิดปกติหรือสงสัยว่ามีการรั่วไหล ต้องรายงานไปยัง ศูนย์รักษาความปลอดภัยสารสนเทศ (Security Operations Center: SOC) และ DPO
- ประเมินการแจ้งต่อหน่วยงานกำกับดูแลและเจ้าของข้อมูลตามกฎหมาย

13) การอบรมและการบังคับใช้

- พนักงานที่เกี่ยวข้องต้องผ่านการอบรม
- การฝ่าฝืนมีมาตรการทางวินัยตามระเบียบองค์กร

ภาคผนวก A: เมทริกซ์วิธีโอนที่อนุญาต (สรุป)

ระดับข้อมูล	ช่องทางหลัก	การป้องกัน ขั้นต่ำ	การยืนยันการรับ
ภายใน (Internal)	อีเมลองค์กร/HTTPS (TLS $\geq$ 1.2)	TLS + การ จำกัดสิทธิ์	อีเมลตอบรับ/ ระบบ Log
ลับ (Confidential)	SFTP/MFT/HTTPS	AES-256 + MFA	เช็คซัม + หนังสือ รับโอน
ลับยิ่ง/อ่อนไหวพิเศษ (Highly Confidential/Sensitive)	SFTP/MFT ผ่าน VPN	AES-256 + MFA + VPN	เช็คซัม + ใบรับ พร้อมลายเซ็น ดิจิทัล

ทะเบียนการส่งหรือโอนข้อมูลส่วนบุคคล

(Personal Data Transfer Register)

คำแนะนำ: บันทึกทุกครั้งที่มีการส่ง/โอนข้อมูลไปยังนอกองค์กรหรือบุคคลภายนอก รวมถึงการโอนข้ามพรมแดน เก็บไว้ไม่น้อยกว่า 5 ปี

ตัวอย่างการบันทึก

Transfer ID	วันที่-เวลา โอน	หน่วยงาน ผู้ส่ง	ผู้ส่ง	ผู้รับ (องค์กร/อีเมล/ประเทศ)	วัตถุประสงค์/ฐานกฎหมาย	ประเภทข้อมูล/เจ้าของข้อมูล	ระดับอ่อนไหว	วิธีโอน/ช่องทาง	มาตรการเข้ารหัส	ชื่อไฟล์/ขนาด	SHA-256 Checksum	สัญญาอ้างอิง	การอนุมัติ	ผลการส่ง	ยืนยันการรับ (วัน-เวลา/ผู้ยืนยัน)	วิธีตรวจสอบ	เหตุการณ์ผิดปกติ	กำหนดลบ	การลบเสร็จ	หมายเหตุ
TR-2025-0001	03-09-2025 10:30	ฝ่ายลูกค้าสัมพันธ์	น.ส. กมล ...	ABC Ltd. / dpo@abc.com / สิงคโปร์	ปฏิบัติตามสัญญา (ให้บริการ)	ลูกค้า (ชื่อ/อีเมล)	ลับ	SFTP ผ่าน VPN	AES-256 + MFA	customer_080325.csv (5MB)	3f2a...9c	DPA-ABC-2025/01	ผู้จัดการ/ DPO	สำเร็จ	03-09-2025 11:05 / Mr. Tan	การตรวจสอบค่าเช็คซัม (Checksum)	ไม่มี	03-03-2026	05-03-2026 / secure wipe	-
TR-2025-0002	15-09-2025 14:20	ฝ่ายบุคคล	นาย สมชาย ...	XYZ Payroll Co. / hr@xyzpay.com / ไทย	ประมวลผลเงินเดือน (สัญญาจ้างแรงงาน)	พนักงาน (เลขบัญชี/เลขประกันสังคม)	อ่อนไหวพิเศษ	Email + ZIP- AES	ZIP- AES256 + Password	payrol_sep2025.zip (2MB)	5c7d...a2e	DPA-XYZ-2025/03	HR Manager	สำเร็จ	15-09-2025 14:45 / Ms. Kanya	การตรวจสอบลายเซ็นดิจิทัล (Digital Signature)	ไม่มี	15-09-2026	20-09-2026 / overwrite	-
TR-2025-0003	28-09-2025 09:15	ฝ่ายกฎหมาย	น.ส. วิภา ...	Law Firm DEF / secureportal.def.com / อังกฤษ	การโอนเพื่อพิจารณาคดี	คู่สัญญา (เอกสารสัญญา/ข้อมูลคดี)	ลับยิ่ง	MFT Portal	TLS 1.3 + MFA	contract_case987.pdf (12MB)	b9de...4fa	NDA-DEF-2025/07	CLO	สำเร็จ	28-09-2025 09:40 / Mr. Smith	การตรวจสอบระบบตอบรับอัตโนมัติ (System Receipt)	ไม่มี	28-09-2030	30-09-2030 / shredding	-

ตัวเลือกมาตรฐานและคำอธิบาย

วิธีโอน/ช่องทาง (Transfer Methods):

- SFTP (Secure File Transfer Protocol) = โพรโทคอลการถ่ายโอนไฟล์ที่เข้ารหัสและปลอดภัย
- FTPS (File Transfer Protocol Secure) = โพรโทคอลถ่ายโอนไฟล์ที่เพิ่มการเข้ารหัสด้วย TLS/SSL
- HTTPS Link (Hypertext Transfer Protocol Secure) = ลิงก์ดาวน์โหลดที่เข้ารหัสด้วย HTTPS
- Email (S/MIME: Secure/Multipurpose Internet Mail Extensions) = การส่งอีเมลเข้ารหัสและตรวจสอบลายเซ็น
- Email + ZIP-AES = การส่งไฟล์ ZIP ที่เข้ารหัสด้วยมาตรฐาน AES พร้อมส่งรหัสผ่านแยกช่องทาง
- MFT Portal (Managed File Transfer Portal) = ระบบกลางที่ใช้โอนย้ายไฟล์อย่างปลอดภัยและมีบันทึกติดตาม
- VPN (Virtual Private Network) = เครือข่ายส่วนตัวเสมือนที่เข้ารหัสการเชื่อมต่อ
- Physical Encrypted Media = การใช้สื่อกายภาพ (เช่น USB, HDD) ที่เข้ารหัสป้องกัน

ระดับอ่อนไหว (Sensitivity Level):

- ภายใน (Internal)
- ลับ (Confidential)
- ลับยิ่ง (Highly Confidential)
- อ่อนไหวพิเศษ (Special Sensitive Data – เช่น ข้อมูลสุขภาพ ชีวภาพ ความเชื่อ ฯลฯ)

ผลการส่ง (Transfer Result):

- สำเร็จ (Success)
- ล้มเหลว (Failed)
- ส่งซ้ำ (Resent)

วิธีตรวจสอบความถูกต้อง (Verification Methods):

- การตรวจสอบค่าเช็คซัม (Checksum) = การเปรียบเทียบค่ารหัสยืนยันไฟล์ เช่น SHA-256
- การตรวจสอบลายเซ็นดิจิทัล (Digital Signature) = ใช้กุญแจสาธารณะ/ส่วนตัวตรวจสอบความถูกต้องของไฟล์
- การตรวจสอบระบบตอบรับอัตโนมัติ (System Receipt) = ระบบแจ้งตอบรับเมื่อผู้รับได้รับไฟล์ครบถ้วน

หนังสือรับโอนข้อมูลส่วนบุคคล

(Personal Data Transfer Acknowledgement)

เลขที่หนังสือ:

วันที่:/...../.....

ระหว่าง

หน่วยงานผู้ส่งข้อมูล:

และ

หน่วยงานผู้รับข้อมูล:

1. วัตถุประสงค์ของหนังสือ

หนังสือฉบับนี้จัดทำขึ้นเพื่อยืนยันการโอนและการรับข้อมูลส่วนบุคคลระหว่างหน่วยงานผู้ส่งและหน่วยงานผู้รับ โดยมีวัตถุประสงค์เพื่อรับรองว่า:

1. ข้อมูลถูกส่งและรับอย่างครบถ้วน ถูกต้อง และปลอดภัย
2. ผู้รับข้อมูลมีพันธกรณีในการปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายและสัญญาที่เกี่ยวข้อง
3. มีหลักฐานยืนยันการส่งและรับข้อมูลเพื่อใช้ตรวจสอบภายหลัง

2. รายละเอียดการโอน

(ก) ข้อมูลที่โอน

- ฐานข้อมูลนักศึกษา (ไฟล์ Excel จำนวน 1 ไฟล์)
- สัญญาจ้างบุคลากร (PDF จำนวน 15 ไฟล์)
- รายงานประจำปี (Word จำนวน 1 ไฟล์)
- สำเนาบัตรประจำตัวพนักงาน (ไฟล์ภาพจำนวน 10 ไฟล์)
- บัญชีเงินเดือน (ไฟล์ Excel จำนวน 1 ไฟล์)

(ข) วิธีการโอน

ผ่านระบบเครือข่ายส่วนตัวเสมือน (VPN – *Virtual Private Network*: ระบบเชื่อมต่อเครือข่ายแบบเข้ารหัสที่สร้าง “อุโมงค์เสมือน” เพื่อป้องกันการดักฟังและแก้ไขข้อมูล) พร้อมมาตรการเข้ารหัส (AES-256 – *Advanced Encryption Standard*: มาตรฐานการเข้ารหัสข้อมูลระดับสูงที่ใช้ความยาวกุญแจ 256 บิต)

- (ค) การตรวจสอบความถูกต้อง
- ตรวจสอบ *Checksum* (รหัสตรวจสอบไฟล์ ซึ่งคำนวณจากอัลกอริทึม เช่น SHA-256 หากไฟล์เปลี่ยนไปแม้เพียงเล็กน้อย ค่า *Checksum* จะเปลี่ยนทันที) ผลการตรวจสอบพบว่าตรงกันกับต้นฉบับ
- (ง) เอกสาร/สัญญาอ้างอิง
- สัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement – DPA)
 - ข้อตกลงไม่เปิดเผยข้อมูล (Non-Disclosure Agreement – NDA)
 - ข้อกำหนดการโอนข้อมูลข้ามพรมแดน (Cross-Border Data Transfer Agreement)

3. รายการไฟล์ที่ได้รับ (ตัวอย่าง)

ลำดับ	ชื่อไฟล์ / คำอธิบาย	ขนาด โดยประมาณ	ค่า SHA-256 (Checksum)	จำนวน ระเบียน	หมายเหตุ
1	student_db_2025.xlsx (ฐานข้อมูลนักศึกษา)	5 MB	f1a3b4d...c9e	2,000 รายการ	–
2	employment_contracts.pdf (สัญญาจ้าง)	12 MB	9d8e2f7...a32	15 ไฟล์	–
3	annual_report_2024.docx (รายงานประจำปี)	3 MB	c3a6d2b...1fe	1 ไฟล์	–
4	staff_id_images.zip (สำเนา บัตรพนักงาน)	20 MB	e8f4a7c...d76	10 ไฟล์	บีบอัด ZIP เข้ารหัส AES
5	payroll_2025.xlsx (บัญชี เงินเดือน)	8 MB	a91f2b5...ee4	500 รายการ	ข้อมูล อ่อนไหว สูง

4. คำรับรองและข้อผูกพันของผู้รับข้อมูล

ผู้รับข้อมูลขอรับรองและตกลงผูกพันตามรายละเอียดต่อไปนี้:

1. การเก็บรักษา (Data Security)

จะเก็บรักษาข้อมูลที่ได้รับโดยใช้มาตรการรักษาความมั่นคงปลอดภัยทั้งทางเทคนิคและทางองค์กร เช่น การเข้ารหัส การควบคุมสิทธิ์เข้าถึง การบันทึกเหตุการณ์ (logging) และการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2. การใช้ข้อมูล (Purpose Limitation)

จะใช้ข้อมูลส่วนบุคคลเฉพาะตามวัตถุประสงค์ที่ตกลงและตามฐานกฎหมายที่เกี่ยวข้อง ไม่ใช่เพื่อประโยชน์อื่นใด

3. การเปิดเผยต่อบุคคลที่สาม (Non-Disclosure)

จะไม่เปิดเผยหรือโอนข้อมูลต่อบุคคลที่สาม เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานผู้ส่ง หรือมีหน้าที่ตามกฎหมายที่ต้องเปิดเผย

4. การรายงานเหตุการณ์ (Incident Reporting)

หากเกิดเหตุข้อมูลรั่วไหล สูญหาย ถูกแก้ไข หรือถูกเข้าถึงโดยไม่ชอบ จะรายงานต่อหน่วยงานผู้ส่ง และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO – *Data Protection Officer*) โดยไม่ชักช้า พร้อมมาตรการแก้ไข

5. สิทธิการตรวจสอบ (Audit Rights)

ยอมรับให้หน่วยงานผู้ส่งหรือผู้ได้รับมอบหมายเข้าตรวจสอบกระบวนการจัดการข้อมูลเพื่อยืนยันการปฏิบัติตามข้อตกลง

6. การลบหรือทำลายข้อมูล (Data Deletion/Destruction)

เมื่อสิ้นสุดระยะเวลาการเก็บรักษาหรือการใช้ จะดำเนินการลบหรือทำลายข้อมูลด้วยวิธีการที่ปลอดภัย เช่น *Secure Wipe* หรือ *Cryptographic Erasure* และจัดทำรายงานยืนยันการลบ/ทำลาย

7. ความรับผิด (Liability)

หากผู้รับข้อมูลฝ่าฝืนหรือทำให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือผู้ส่ง จะต้องรับผิดชอบต่อความเสียหาย ค่าปรับ ค่าชดเชย และค่าใช้จ่ายที่เกี่ยวข้อง

5. การลงนาม

ลงชื่อ ผู้รับข้อมูล

ตำแหน่ง

วันที่

ลงชื่อ ผู้ส่งข้อมูล

ตำแหน่ง

วันที่

หมายเหตุคำศัพท์เฉพาะ

- **Checksum (เช็กซัม):** รหัสตรวจสอบความถูกต้องของไฟล์เพื่อยืนยันว่าไม่ถูกแก้ไขหรือเสียหายระหว่างการโอน

- **Encryption (การเข้ารหัส):** การทำให้ข้อมูลอยู่ในรูปแบบที่ผู้อื่นไม่สามารถเข้าใจได้ เว้นแต่มีรหัสถอด
- **VPN (Virtual Private Network / เครือข่ายส่วนตัวเสมือน):** ระบบสร้างอุโมงค์เสมือนเพื่อเชื่อมต่อข้อมูลอย่างปลอดภัย ป้องกันการดักฟัง
- **AES-256:** มาตรฐานการเข้ารหัสข้อมูลที่ใช้ความยาวกุญแจ 256 บิต มีความปลอดภัยสูง
- **DPO (Data Protection Officer / เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล):** ผู้ที่องค์กรแต่งตั้งให้กำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล

9.2.4 มีการจัดทำข้อตกลงกับหน่วยงานภายนอกเพื่อใช้ในการควบคุมการส่งหรือโอนข้อมูลทางธุรกิจ (ซึ่งรวมถึงข้อมูลส่วนบุคคล) ระหว่างองค์กรกับหน่วยงานภายนอก

สิ่งที่ต้องทำ: การจัดทำข้อตกลงกับหน่วยงานภายนอกเพื่อใช้ในการควบคุมการส่งหรือโอนข้อมูลทางธุรกิจ (ซึ่งรวมถึงข้อมูลส่วนบุคคล) ระหว่างองค์กรกับหน่วยงานภายนอก และมีเอกสารสนับสนุนครบถ้วน

หลักฐาน: นโยบายการจัดทำข้อตกลงกับหน่วยงานภายนอก
ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล
ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) (2), 40 วรรคสาม

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)

โทษทางอาญา กรณี Sensitive Data เป็นไปตามฐานความผิดเกี่ยวกับการฝ่าฝืนหรือไม่
ปฏิบัติตามมาตรา 27

โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3
ล้านบาท หรือ 5 ล้านบาท

1. นโยบายการลดการส่งหรือโอนข้อมูลส่วนบุคคลออกไปยังภายนอกองค์กร

วัตถุประสงค์

เพื่อควบคุมและลดการส่งหรือโอนข้อมูลส่วนบุคคลออกไปยังหน่วยงานภายนอกอย่างไม่จำเป็น
โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูลและสิทธิของเจ้าของข้อมูล

แนวนโยบาย

- 1.1 ข้อมูลส่วนบุคคลจะต้องไม่ถูกส่งหรือโอนออกไปยังภายนอกองค์กร เว้นแต่มีเหตุผลที่ชอบด้วยกฎหมาย
และมีความจำเป็นต่อการกิจของหน่วยงาน
- 1.2 หน่วยงานต้องพิจารณาทางเลือกอื่นก่อน เช่น การประมวลผลข้อมูลภายใน การไม่ใช่ข้อมูลระบุตัว
บุคคลโดยตรง (pseudonymisation) หรือการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ (anonymisation)
- 1.3 การโอนข้อมูลต้องได้รับการอนุมัติจากเจ้าหน้าที่ควบคุมข้อมูล (DPO หรือผู้ได้รับมอบหมาย) และมีการ
จัดเก็บบันทึกทุกครั้ง
- 1.4 กรณีจำเป็นต้องโอนข้อมูล จะต้องใช้มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามความเสี่ยงของ
ข้อมูล

2. นโยบายการรักษาความมั่นคงปลอดภัยของการส่งหรือโอนข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมด้านเทคนิคและองค์กรในการส่งหรือโอนข้อมูลส่วนบุคคลให้เป็นไป
อย่างมั่นคงปลอดภัยตามข้อกำหนดของกฎหมาย

แนวนโยบาย

- 2.1 การส่งหรือโอนข้อมูลจะต้องใช้ช่องทางที่มีการเข้ารหัส (encryption) และตรวจสอบสิทธิ์ก่อนเข้าถึง
(authentication)
- 2.2 ห้ามส่งข้อมูลผ่านอีเมลหรือระบบข้อความส่วนตัวที่ไม่มีระบบควบคุม เช่น Gmail ส่วนบุคคล หรือ
Line
- 2.3 ระบบหรือช่องทางการโอนจะต้องสามารถจัดเก็บ log และมีระบบ audit trail สำหรับการตรวจสอบ
ย้อนหลัง

2.4 ข้อมูลที่โอนต้องมีการจัดทำบันทึกการโอนทุกครั้ง เช่น แบบฟอร์มโอนข้อมูล รายงาน log การเข้าถึงไฟล์

3. บันทึกการส่งหรือโอนข้อมูลส่วนบุคคล (ตัวอย่าง)

ชื่อไฟล์: บันทึกการโอนข้อมูล_ฝ่ายทรัพยากรบุคคล_01/2567.docx

ลำดับ	วันที่	ผู้ส่ง	ผู้รับ	จุดประสงค์	ประเภทข้อมูล	ช่องทางการส่ง	มีการเข้ารหัสหรือไม่	หมายเหตุ
1	4/5/2567	นายก	บริษัท X	ส่งข้อมูลประวัติพนักงานไปยังประกันสังคม	ข้อมูลระบุตัวบุคคล	SFTP	มี	ใช้รหัสผ่านแยก
2	10/5/2567	น.ส. ข	บริษัทที่ปรึกษา Y	ส่งแบบสอบถาม DPO	ข้อมูลไม่ระบุตัวบุคคล	อีเมลองค์กร	มี	PDF เข้ารหัส

4. ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)

หัวข้อสำคัญใน DPA

- 4.1 วัตถุประสงค์ของการประมวลผล
- 4.2 ขอบเขตและประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- 4.3 หน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล
- 4.4 ระยะเวลาการจัดเก็บข้อมูล
- 4.5 มาตรการความปลอดภัยที่ต้องดำเนินการ
- 4.6 การแจ้งเหตุละเมิดข้อมูลภายในระยะเวลาที่กำหนด
- 4.7 การลบหรือคืนข้อมูลเมื่อสิ้นสุดสัญญา

5. ข้อตกลงการส่งหรือโอนข้อมูลส่วนบุคคล

หัวข้อสำคัญ

- 5.1 กำหนดขอบเขตของข้อมูลที่จะโอน
- 5.2 วัตถุประสงค์ในการโอน
- 5.3 ช่องทางที่ใช้ในการโอน และการรักษาความปลอดภัยระหว่างการโอน
- 5.4 การควบคุมการเข้าถึงจากฝั่งผู้รับข้อมูล
- 5.5 ห้ามนำข้อมูลไปใช้เพื่อวัตถุประสงค์อื่นโดยไม่ได้รับอนุญาต

6. บันทึกข้อตกลงรักษาความลับ (NDA)

สาระสำคัญ

- 6.1 คู่สัญญาต้องเก็บรักษาข้อมูลส่วนบุคคลที่ได้รับไว้เป็นความลับและไม่เปิดเผยแก่บุคคลอื่น
- 6.2 ห้ามใช้ข้อมูลเพื่อวัตถุประสงค์อื่นที่ไม่เกี่ยวข้องกับสัญญาหลัก
- 6.3 ระยะเวลาที่ข้อมูลมีผลบังคับใช้ แม้ภายหลังจากสิ้นสุดความสัมพันธ์ทางสัญญา

7. รายงานการตรวจสอบการปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคล

องค์ประกอบของรายงาน

- 7.1 รายงานรายการโอนข้อมูลย้อนหลัง 6 เดือน พร้อมผู้รับและวัตถุประสงค์
- 7.2 ผลการตรวจสอบระบบรักษาความปลอดภัย (เช่น การเข้ารหัส ช่องทางการส่ง การเก็บ log)
- 7.3 รายการข้อเสนอแนะจากฝ่ายควบคุมข้อมูลหรือผู้ตรวจสอบภายใน
- 7.4 แผนการปรับปรุงหรือแก้ไขกระบวนการที่ยังมีความเสี่ยง

8. แบบฟอร์มบันทึกการส่งหรือโอนข้อมูลส่วนบุคคล (แนบท้าย)

ชื่อแบบฟอร์ม: FM-DATA-TRANSFER-01

วัตถุประสงค์: ใช้สำหรับบันทึกการส่งหรือโอนข้อมูลส่วนบุคคลแต่ละครั้ง

วันที่ โอน	ผู้ส่ง ข้อมูล	หน่วยงาน ผู้รับ	จุดประสงค์	ประเภท ข้อมูล	ช่องทาง	เข้ารหัส/ไม่ เข้ารหัส	ผู้อนุมัติ	หมายเหตุ

หมายเหตุ: ให้หน่วยงานกรอกข้อมูลให้ครบถ้วนทุกครั้งที่มีการส่งหรือโอนข้อมูล และจัดเก็บแบบฟอร์มไว้ในระบบเอกสารอย่างเป็นทางการ

9.3.1 มีการทบทวนคุณภาพของรายการข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องเหมาะสม และไม่จัดเก็บไว้เกินกว่าความจำเป็น

สิ่งที่ต้องทำ: มีการทบทวนคุณภาพของรายการข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องเหมาะสม และไม่จัดเก็บไว้เกินกว่าความจำเป็น

หลักฐาน: นโยบายการทบทวนข้อมูลส่วนบุคคล
นโยบายการทำให้ข้อมูลสมบูรณ์ ถูกต้อง และเป็นปัจจุบัน

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4), ข้อ 5

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

1. นโยบายการทบทวนข้อมูลส่วนบุคคล

1.1 วัตถุประสงค์

เพื่อกำหนดแนวทางในการทบทวนรายการข้อมูลส่วนบุคคลที่หน่วยงานจัดเก็บไว้ ให้นั่นใจว่าข้อมูลมีความถูกต้อง เป็นปัจจุบัน และไม่มีการเก็บรักษาข้อมูลที่เกินความจำเป็นตามวัตถุประสงค์ที่ระบุไว้

1.2 ขอบเขตการบังคับใช้

นโยบายนี้ใช้บังคับกับข้อมูลส่วนบุคคลที่อยู่ภายใต้การดูแลของทุกหน่วยงานภายในองค์กร ทั้งที่จัดเก็บในรูปแบบอิเล็กทรอนิกส์และเอกสาร

1.3 แนวทางปฏิบัติ

ผู้รับผิดชอบข้อมูลต้องจัดทำแผนการทบทวนข้อมูลส่วนบุคคลเป็นประจำอย่างน้อยปีละ 1 ครั้ง

- การทบทวนจะต้องพิจารณาประเด็นต่อไปนี้:
- ความครบถ้วนของข้อมูล
- ถูกต้องของข้อมูล
- ความเหมาะสมของข้อมูลกับวัตถุประสงค์
- ระยะเวลาในการจัดเก็บข้อมูล (ยังคงมีเหตุผลในการจัดเก็บหรือไม่)

หากพบว่าข้อมูลมีความล้าสมัยหรือไม่จำเป็น ต้องดำเนินการแก้ไขหรือลบออกตามกระบวนการที่กำหนด ทุกการทบทวนต้องมีบันทึกผลการตรวจสอบ และเสนอรายงานต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

- 1.4 เอกสารประกอบและแบบฟอร์ม

- แบบฟอร์มตรวจสอบรายการข้อมูลส่วนบุคคล
- ตารางการกำหนดรอบการทบทวนข้อมูล
- รายงานผลการทบทวนข้อมูลส่วนบุคคล (รายครึ่งปี)

2. นโยบายการทำให้ข้อมูลสมบูรณ์ ถูกต้อง และเป็นปัจจุบัน

2.1 วัตถุประสงค์

เพื่อกำหนดกระบวนการให้แน่ใจว่าข้อมูลส่วนบุคคลที่หน่วยงานจัดเก็บ มีความสมบูรณ์ ถูกต้อง และได้รับการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ ตามหลักการคุ้มครองข้อมูลส่วนบุคคล

2.2 แนวทางปฏิบัติ

- ก่อนการจัดเก็บข้อมูลส่วนบุคคล ต้องมีการตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูลจากแหล่งที่มาหลายช่องทางหากเป็นไปได้
- ให้ผู้เจ้าของข้อมูลมีช่องทางในการตรวจสอบ แก้ไข หรือร้องขอให้ปรับปรุงข้อมูลส่วนบุคคลของตนเอง เช่น ผ่านระบบออนไลน์หรือแบบฟอร์มเฉพาะ
- กำหนดช่วงเวลาการทบทวนข้อมูลตามประเภทของข้อมูล เช่น
 1. ข้อมูลติดต่อ: ทบทวนทุก 6 เดือน
 2. ข้อมูลสุขภาพหรือข้อมูลที่เปลี่ยนแปลงได้รวดเร็ว: ทบทวนทุก 3 เดือน
 3. ข้อมูลประวัติการจ้างงาน: ทบทวนปีละ 1 ครั้ง
- มีระบบแจ้งเตือนเจ้าหน้าที่ที่ดูแลข้อมูลเมื่อถึงรอบการตรวจสอบข้อมูล
- กำหนดความรับผิดชอบของแต่ละฝ่ายในการดำเนินการตรวจสอบและปรับปรุงข้อมูลให้ชัดเจน
- กำหนดให้มีการเก็บบันทึกการปรับปรุงข้อมูลทุกครั้ง โดยระบุวัน เวลา ผู้ดำเนินการ และรายละเอียดการเปลี่ยนแปลง

2.3 ช่องทางสนับสนุน

- แบบฟอร์มขอแก้ไขข้อมูลส่วนบุคคล
- ระบบแจ้งเตือนอัตโนมัติ (เช่น ผ่าน email / dashboard ระบบข้อมูล)
- ช่องทางติดต่อเจ้าหน้าที่คุ้มครองข้อมูล (DPO) สำหรับสอบถามหรือร้องเรียน

2.4 การกำกับติดตาม

- หน่วยงานที่เกี่ยวข้องจะจัดทำรายงานสรุปผลการปรับปรุงข้อมูลอย่างน้อยทุก 6 เดือน
- DPO จะทำการสุ่มตรวจการบันทึกข้อมูลที่ปรับปรุงแล้ว เพื่อประเมินประสิทธิภาพของกระบวนการที่ไม่ดำเนินการตามรอบเวลาที่กำหนด จะต้องรายงานเหตุผลต่อผู้บริหารโดยตรง

9.3.2 มีการสร้างความตระหนักให้แก่ผู้ที่เกี่ยวข้องกับประเด็นปัญหาด้านคุณภาพของข้อมูล ซึ่งรวมถึงการตรวจสอบคุณภาพของข้อมูลอย่างสม่ำเสมอ

สิ่งที่ต้องทำ: มีการสร้างความตระหนักให้แก่ผู้ที่เกี่ยวข้องเกี่ยวกับประเด็นปัญหาด้านคุณภาพข้อมูล ซึ่งรวมถึงการตรวจสอบคุณภาพของข้อมูลอย่างสม่ำเสมอ และมีเอกสารครบถ้วน

- หลักฐาน: นโยบายการฝึกอบรมและการทดสอบผู้ที่เกี่ยวข้องเกี่ยวกับประเด็นปัญหาด้านคุณภาพของข้อมูลส่วนบุคคล
- หลักเกณฑ์การฝึกอบรมด้านคุณภาพของข้อมูลส่วนบุคคล
- แบบทดสอบความรู้ด้านคุณภาพของข้อมูลส่วนบุคคล
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (4) (7)
- โทษทางปกครอง: ในกรณีที่ไม่มีปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

1. นโยบายการฝึกอบรมและการทดสอบผู้ที่เกี่ยวข้องเกี่ยวกับประเด็นปัญหาด้านคุณภาพของข้อมูลส่วนบุคคล

1.1 วัตถุประสงค์

เพื่อสร้างความตระหนักรู้และความเข้าใจที่ถูกต้องเกี่ยวกับคุณภาพของข้อมูลส่วนบุคคลแก่บุคลากรทุกระดับที่เกี่ยวข้องกับการจัดเก็บ ใช้ หรือประมวลผลข้อมูลส่วนบุคคล โดยมุ่งเน้นให้บุคลากรตระหนักถึงผลกระทบของข้อมูลที่ผิดพลาด หรือข้อมูลที่ไม่สมบูรณ์ต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล รวมถึงกระตุ้นให้มีการปฏิบัติตามมาตรฐานและกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด

1.2 ขอบเขตการบังคับใช้

นโยบายนี้มีผลบังคับใช้กับบุคลากรทุกคนในองค์กรที่มีหน้าที่และความรับผิดชอบเกี่ยวข้องกับข้อมูลส่วนบุคคล ตั้งแต่ระดับผู้บริหาร ฝ่ายบริหารงานบุคคล ฝ่ายไอที เจ้าหน้าที่ประมวลผลข้อมูล และผู้ที่เกี่ยวข้องอื่น ๆ รวมถึงผู้ที่ได้รับมอบหมายให้ดำเนินงานเกี่ยวกับข้อมูลส่วนบุคคล

1.3 แนวทางการฝึกอบรมและทดสอบ

ความถี่ในการฝึกอบรม

- ฝึกอบรมเบื้องต้นสำหรับพนักงานใหม่ภายใน 30 วันหลังเข้าทำงาน
- ฝึกอบรมทบทวนอย่างน้อยปีละ 1 ครั้ง เพื่ออัปเดตความรู้และทบทวนมาตรการรักษาคุณภาพข้อมูล

เนื้อหาหลักสูตร

- ความสำคัญของข้อมูลส่วนบุคคลและคุณภาพของข้อมูล
- ความเสี่ยงและผลกระทบจากข้อมูลที่ผิดพลาดหรือไม่สมบูรณ์
- วิธีการตรวจสอบและทบทวนคุณภาพข้อมูลอย่างสม่ำเสมอ
- กฎหมายและข้อกำหนดที่เกี่ยวข้อง เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

- บทลงโทษกรณีไม่ปฏิบัติตามกฎหมาย

รูปแบบการฝึกอบรม

- การบรรยาย/สัมมนาในห้องเรียนหรือออนไลน์
- การฝึกอบรมเชิงปฏิบัติการ
- การแจกเอกสาร คู่มือ และสื่อการเรียนรู้เพิ่มเติม

การทดสอบวัดผล

- จัดทำแบบทดสอบก่อนและหลังการอบรมเพื่อวัดระดับความรู้
- บันทึกและเก็บรักษาผลการทดสอบเพื่อเป็นหลักฐาน

การรายงานและติดตามผล

- จัดทำรายงานผลการฝึกอบรมและผลทดสอบเสนอผู้บริหารและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- วิเคราะห์และปรับปรุงหลักสูตรตามข้อเสนอแนะและผลการประเมิน

1.4 ความรับผิดชอบ

- ผู้บริหารต้องสนับสนุนทรัพยากรและส่งเสริมการฝึกอบรมอย่างต่อเนื่อง
- ฝ่ายทรัพยากรบุคคลรับผิดชอบประสานงานและจัดทำแผนฝึกอบรม
- ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO) รับผิดชอบการจัดทำเนื้อหาและมาตรฐานการฝึกอบรม
- บุคลากรต้องเข้ารับการฝึกอบรมตามกำหนด และผ่านการทดสอบวัดผล

1.5 การอ้างอิงกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (4) และ (7)

2. หลักเกณฑ์การฝึกอบรมด้านคุณภาพของข้อมูลส่วนบุคคล

2.1 ผู้มีสิทธิ์และหน้าที่เข้ารับการฝึกอบรม

- บุคลากรใหม่ที่เกี่ยวข้องกับการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล
- เจ้าหน้าที่ฝ่ายไอทีที่ดูแลระบบฐานข้อมูลและระบบสารสนเทศ
- เจ้าหน้าที่ฝ่ายบริหารงานบุคคลที่ต้องใช้ข้อมูลส่วนบุคคลในกระบวนการบริหาร
- หัวหน้างานและผู้บริหารที่มีหน้าที่กำกับดูแลงานข้อมูลส่วนบุคคล
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

2.2 ประเภทของการฝึกอบรม

- **ฝึกอบรมเบื้องต้น (Orientation Training)**
เน้นให้ความรู้พื้นฐานเกี่ยวกับข้อมูลส่วนบุคคล คุณภาพของข้อมูล และกฎหมายที่เกี่ยวข้อง
- **ฝึกอบรมทบทวน (Refresher Training)**
เพื่ออัปเดตข้อมูลใหม่ ๆ และทบทวนความรู้เดิมอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
- **ฝึกอบรมเชิงลึกเฉพาะกรณี (Specialized Training)**
สำหรับผู้ที่มีบทบาทเฉพาะ เช่น การตรวจสอบคุณภาพข้อมูล หรือการจัดการเหตุการณ์ข้อมูลรั่วไหล

2.3 เนื้อหาสำคัญของการฝึกอบรม

- ความหมายและความสำคัญของคุณภาพข้อมูลส่วนบุคคล
- ปัญหาที่เกิดจากข้อมูลที่ไม่ถูกต้อง หรือไม่สมบูรณ์
- มาตรฐานและแนวทางปฏิบัติในการทบทวนและตรวจสอบคุณภาพข้อมูล
- ความรับผิดชอบและบทบาทของแต่ละฝ่าย
- กระบวนการและวิธีการจัดเก็บข้อมูลให้ถูกต้องเหมาะสม
- กฎหมายและข้อกำหนดที่เกี่ยวข้อง (เช่น มาตรา 37 ของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล)
- บทลงโทษทางปกครองและทางอาญา
- กรณีศึกษาหรือแบบฝึกหัดจำลองสถานการณ์

2.4 วิธีการฝึกอบรม

- บรรยายโดยผู้เชี่ยวชาญด้านกฎหมายและข้อมูลส่วนบุคคล
- กิจกรรมกลุ่มเพื่อฝึกการวิเคราะห์และแก้ไขปัญหาข้อมูล
- การนำเสนอกรณีศึกษาจริงหรือจำลอง
- แบบทดสอบวัดความรู้ก่อนและหลังอบรม
- แจกคู่มือและสื่อการเรียนรู้เพิ่มเติม เช่น อินโฟกราฟิก วิดีโอสั้น

2.5 การวัดผลและการติดตามผล

- จัดเก็บบันทึกการเข้าร่วมอบรมและผลการทดสอบทั้งหมด
- ประเมินความพึงพอใจและความเข้าใจจากผู้เข้าร่วมอบรม
- รายงานผลให้ผู้บริหารและหน่วยงานที่เกี่ยวข้อง
- ปรับปรุงเนื้อหาและวิธีการอบรมตามข้อเสนอแนะและผลการประเมิน

2.6 การปฏิบัติตามกฎหมายและข้อบังคับ

- ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามมาตรการที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ต้องมีหลักฐานชัดเจนของการฝึกอบรมและผลการทดสอบเพื่อใช้ในการตรวจสอบและรายงาน

- การไม่ปฏิบัติตามมาตรา 37 อาจมีบทลงโทษทางปกครองสูงสุดถึง 3 ล้านบาท

แบบทดสอบความรู้ด้านคุณภาพของข้อมูลส่วนบุคคล (ตัวอย่าง 5 ข้อ)

3.1 ตัวอย่างแบบทดสอบ (เลือกตอบเพียงข้อเดียวที่ถูกต้อง)

1. ข้อใดคือสาเหตุของปัญหาด้านคุณภาพของข้อมูลที่พบบ่อยที่สุด

- (ก) การมีรหัสผ่านที่อ่อนแอ
- (ข) การจัดเก็บข้อมูลเกินความจำเป็น
- (ค) การกรอกข้อมูลผิดหรือไม่ครบถ้วน
- (ง) การไม่มีการขอความยินยอมก่อนเก็บข้อมูล

2. ข้อใดเป็นผลจากข้อมูลส่วนบุคคลที่ไม่ถูกต้อง

- (ก) การปฏิเสธให้บริการโดยไม่ถูกต้อง
- (ข) การเพิ่มความปลอดภัยของระบบ
- (ค) การขอความยินยอมอย่างถูกต้อง
- (ง) การประมวลผลข้อมูลได้เร็วขึ้น

3. วิธีใดต่อไปนี้สามารถช่วยตรวจสอบคุณภาพของข้อมูลได้

- (ก) ใช้ AI ประมวลผลข้อมูลทุกวัน
- (ข) ลบข้อมูลเก่าทุก 3 เดือน
- (ค) ตรวจสอบความครบถ้วนและถูกต้องของข้อมูลตามรอบที่กำหนด
- (ง) อัปเดตข้อมูลขึ้นระบบคลาวด์

4. การฝึกอบรมด้านคุณภาพของข้อมูลควรดำเนินการอย่างน้อยกี่ครั้งต่อปี

- (ก) เดือนละครั้ง
- (ข) ทุกครั้งที่มีการอัปเดตข้อมูล
- (ค) ปีละ 1 ครั้ง
- (ง) เฉพาะพนักงานใหม่เท่านั้น

5. บทลงโทษสูงสุดทางปกครองตามมาตรา 37 กรณีไม่ปฏิบัติตามมาตรการที่กฎหมายกำหนดคืออะไร

- (ก) ปรับไม่เกิน 3 แสนบาท
- (ข) ปรับไม่เกิน 3 ล้านบาท
- (ค) จำคุกไม่เกิน 2 ปี
- (ง) ปรับและจำคุกพร้อมกัน

9.3.3 มีการลบหรือทำลายข้อมูลส่วนบุคคลเป็นระยะ ๆ เพื่อไม่ให้มีการจัดเก็บข้อมูลไว้เกินกว่าระยะเวลาที่กำหนด

สิ่งที่ต้องทำ: มีการลบหรือทำลายข้อมูลส่วนบุคคลเป็นระยะ ๆ อย่างสม่ำเสมอ เพื่อไม่ให้มีการจัดเก็บข้อมูลไว้เกินกว่าระยะเวลาที่กำหนด

หลักฐาน: นโยบายและกระบวนการเกี่ยวกับวิธีการจำกัดการเก็บรวบรวมข้อมูลส่วนบุคคลที่ไม่พึงประสงค์

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567 ข้อ 6, ข้อ 9

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายและกระบวนการเกี่ยวกับวิธีการจำกัดการเก็บรวบรวมข้อมูลส่วนบุคคลที่ไม่พึงประสงค์

1.นโยบายการจัดการและจำกัดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

1.1 กำหนดวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลให้ชัดเจน และผูกติดกับระยะเวลาการเก็บรักษาข้อมูลตามความเหมาะสมและความจำเป็นในการดำเนินงานขององค์กร

1.2 ระบุประเภทข้อมูลส่วนบุคคลแต่ละประเภท พร้อมกำหนดระยะเวลาที่เหมาะสมสำหรับการเก็บรักษา เช่น ข้อมูลพนักงานเก็บไว้จนกว่าจะสิ้นสุดการจ้างงาน + 5 ปี ข้อมูลลูกค้าเก็บไว้ไม่เกิน 3 ปีหลังสิ้นสุดสัญญา เป็นต้น

1.3 กำหนดข้อยกเว้นสำหรับข้อมูลที่ต้องเก็บรักษานานกว่าปกติ เช่น กรณีข้อกำหนดทางกฎหมาย หรือข้อผูกพันกับหน่วยงานภายนอก

1.4 ระบุผู้รับผิดชอบหลักและรองในแต่ละฝ่ายหรือหน่วยงานในการติดตาม ดูแล และบริหารจัดการการเก็บรักษาข้อมูลให้เป็นไปตามนโยบาย

2.กระบวนการตรวจสอบและทบทวนข้อมูลส่วนบุคคลเพื่อจำกัดระยะเวลาการเก็บรักษา

2.1 จัดทำตารางตรวจสอบข้อมูลส่วนบุคคลที่มีอยู่ในระบบต่าง ๆ แยกตามประเภทข้อมูลและระยะเวลาที่กำหนดไว้ในนโยบาย

2.2 ดำเนินการตรวจสอบข้อมูลที่ครบกำหนดลบหรือทำลายเป็นระยะ ๆ อย่างน้อยทุก 3 เดือน หรือภายในระยะเวลาที่เหมาะสมตามลักษณะข้อมูล

2.3 บันทึกรายงานผลการตรวจสอบทุกครั้ง เพื่อเป็นหลักฐานและใช้สำหรับการตรวจสอบภายใน (Internal Audit)

2.4 หากพบข้อมูลที่ยังถูกเก็บรักษาเกินระยะเวลาที่กำหนด ต้องดำเนินการลบหรือทำลายข้อมูลทันทีและรายงานผลให้ผู้บริหารทราบ

3.วิธีการลบหรือทำลายข้อมูลส่วนบุคคลอย่างปลอดภัยและเป็นระบบ

3.1 สำหรับข้อมูลดิจิทัล ใช้เทคโนโลยีการลบข้อมูลอย่างถาวร (Data Erasure) ที่สามารถยืนยันการลบข้อมูลได้ เช่น การเขียนทับข้อมูลหลายรอบ (Overwriting) หรือการใช้ซอฟต์แวร์ลบข้อมูลตามมาตรฐานสากล

3.2 สำหรับเอกสารหรือข้อมูลในรูปแบบกระดาษ ดำเนินการทำลายด้วยวิธีการที่เหมาะสม เช่น การทำลายด้วยเครื่องทำลายเอกสาร (Shredder) หรือเผาเผาในที่ปลอดภัย เพื่อป้องกันการถูกขโมยหรือเข้าถึงโดยไม่ได้รับอนุญาต

3.3 กำหนดแนวทางการทำลายอุปกรณ์จัดเก็บข้อมูลที่ไม่ได้ใช้งาน เช่น ฮาร์ดไดรฟ์ แฟลชไดรฟ์ หรือสื่อบันทึกข้อมูลอื่น ๆ

3.4 จัดทำบันทึกการทำลายข้อมูลที่มีรายละเอียด ได้แก่ วันที่ทำลาย, ประเภทข้อมูล, จำนวน, วิธีการทำลาย, ผู้ดำเนินการ และผู้อนุมัติ เพื่อใช้เป็นหลักฐานทางกฎหมายและการตรวจสอบ

4.การกำหนดมาตรการป้องกันการเก็บข้อมูลเกินความจำเป็น

4.1 กำหนดนโยบายไม่เก็บข้อมูลเกินกว่าที่จำเป็นตามวัตถุประสงค์ที่ระบุไว้ในแต่ละกรณี

4.2 มีระบบควบคุมการเข้าถึงและตรวจสอบการเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อป้องกันการเก็บข้อมูลซ้ำซ้อน หรือข้อมูลที่ไม่มีความจำเป็น

4.3 จัดทำคู่มือหรือแนวทางปฏิบัติแก่ผู้ปฏิบัติงานเกี่ยวกับการจำกัดประเภทและระยะเวลาการเก็บข้อมูล

4.4 ทบทวนและปรับปรุงนโยบายอย่างสม่ำเสมอเพื่อให้สอดคล้องกับกฎหมายใหม่ ๆ หรือการเปลี่ยนแปลงขององค์กร

5.การฝึกอบรมและสร้างความตระหนักเกี่ยวกับการจำกัดระยะเวลาการเก็บข้อมูล

5.1 จัดอบรมให้ความรู้แก่บุคลากรทุกฝ่ายที่เกี่ยวข้องกับการจัดเก็บและจัดการข้อมูลส่วนบุคคล เรื่องความสำคัญของการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อครบกำหนด

5.2 จัดกิจกรรมส่งเสริมความรู้ เช่น สื่อประชาสัมพันธ์ เอกสารแจก หรือเวิร์กช็อป เพื่อให้เกิดความเข้าใจและตระหนักในเรื่องการจัดการข้อมูลส่วนบุคคลอย่างเหมาะสม

5.3 ประเมินผลการอบรมและความเข้าใจของบุคลากรอย่างสม่ำเสมอ เช่น แบบทดสอบ หรือการประเมินภาคปฏิบัติ เพื่อให้มั่นใจว่าบุคลากรสามารถปฏิบัติตามนโยบายได้อย่างถูกต้อง

6. การตรวจสอบและรายงานการปฏิบัติตามนโยบาย

6.1 จัดให้มีการตรวจสอบภายใน (Internal Audit) เกี่ยวกับการปฏิบัติตามนโยบายและกระบวนการลบหรือทำลายข้อมูลอย่างสม่ำเสมอ

6.2 จัดทำรายงานผลการตรวจสอบพร้อมข้อเสนอแนะ เพื่อให้ผู้บริหารสามารถติดตามและแก้ไขปัญหาได้ทันทั่วทั้งที่

6.3 ส่งรายงานการตรวจสอบให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อใช้ในการประเมินความเสี่ยงและปรับปรุงระบบการจัดการข้อมูล

6.4 มีช่องทางให้พนักงานหรือบุคคลภายนอกแจ้งเบาะแสหรือรายงานกรณีพบข้อมูลที่ถูกระบุรักษาเกินกำหนดเพื่อดำเนินการแก้ไขทันที

9.4 กำหนดระยะเวลาการจัดเก็บข้อมูล (Retention schedule)

มีกำหนดระยะเวลาการจัดเก็บข้อมูลที่เหมาะสมสำหรับข้อมูลส่วนบุคคลทุกประเภทและมีการทบทวนอย่างสม่ำเสมอ

9.4.1 มีการกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลตามความต้องการทางธุรกิจ ซึ่งรวมถึงให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และหลักการที่เกี่ยวข้อง

สิ่งที่ต้องทำ: มีการกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลตามความต้องการทางธุรกิจ สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และหลักการที่เกี่ยวข้อง

หลักฐาน: นโยบายระยะเวลาการจัดเก็บข้อมูลและการเก็บรักษาข้อมูลส่วนบุคคล
รายงานตรวจสอบการจัดเก็บและการเก็บรักษาข้อมูลส่วนบุคคล
หนังสือแจ้งการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22 มาตรา 37 (1) (3)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 22 มาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

เอกสารหลักฐานการกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลตามความต้องการทางธุรกิจ
สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และหลักการที่เกี่ยวข้อง

1. บทนำ

การจัดเก็บข้อมูลส่วนบุคคลเป็นกิจกรรมที่องค์กรทุกแห่งต้องดำเนินการอย่างรอบคอบเพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และข้อกำหนดของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งระเบียบข้อบังคับที่เกี่ยวข้อง เพื่อป้องกันการละเมิดสิทธิของเจ้าของข้อมูล และลดความเสี่ยงด้านความปลอดภัยของข้อมูล

หนึ่งในหลักการสำคัญคือการกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลให้เหมาะสมกับวัตถุประสงค์และความต้องการทางธุรกิจ โดยไม่เก็บข้อมูลไว้นานเกินความจำเป็นเพื่อประโยชน์ในการบริหารจัดการและการปฏิบัติตามกฎหมาย นโยบายและกระบวนการเกี่ยวกับการกำหนดและทบทวนระยะเวลาการเก็บข้อมูลจึงเป็นเครื่องมือสำคัญที่ช่วยให้องค์กรสามารถบริหารข้อมูลได้อย่างมีประสิทธิภาพและสอดคล้องตามมาตรฐาน

2. แนวทางและขั้นตอนการกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคล

2.1 การวิเคราะห์ประเภทข้อมูลและวัตถุประสงค์การเก็บรวบรวม

- รวบรวมข้อมูลประเภทต่าง ๆ ที่องค์กรเก็บ เช่น ข้อมูลพนักงาน ลูกค้า คู่ค้า ข้อมูลทางการแพทย์ หรือข้อมูลทางการเงิน
- กำหนดวัตถุประสงค์ของการเก็บข้อมูล เช่น การจ้างงาน การให้บริการ การชำระเงิน หรือการปฏิบัติตามกฎหมาย
- ประเมินระยะเวลาที่จำเป็นในการเก็บข้อมูลเพื่อวัตถุประสงค์นั้น ๆ

2.2 การพิจารณาข้อกำหนดทางกฎหมายและระเบียบ

- ตรวจสอบข้อกำหนดกฎหมาย เช่น PDPA, กฎหมายแรงงาน, กฎหมายภาษี, กฎหมายอื่น ๆ ที่เกี่ยวข้อง
- ตรวจสอบระเบียบและแนวทางปฏิบัติจากหน่วยงานกำกับดูแลที่เกี่ยวข้อง
- ประเมินข้อจำกัดทางกฎหมายว่าระยะเวลาเก็บข้อมูลขั้นต่ำและสูงสุดเป็นอย่างไร

2.3 การกำหนดระยะเวลาการเก็บข้อมูลตามความต้องการทางธุรกิจและข้อกำหนด

- รวมข้อมูลจากข้อ 2.1 และ 2.2 เพื่อกำหนดช่วงเวลาที่เหมาะสม
- กำหนดระยะเวลาการเก็บแต่ละประเภทข้อมูลในเอกสารนโยบายให้ชัดเจน
- ระบุขั้นตอนการขออนุมัติหรือขยายเวลาการเก็บข้อมูลในกรณีจำเป็น

2.4 การทบทวนและปรับปรุงระยะเวลาการเก็บข้อมูลอย่างสม่ำเสมอ

- จัดให้มีการทบทวนระยะเวลาการเก็บข้อมูลอย่างน้อยปีละหนึ่งครั้ง
- ติดตามการเปลี่ยนแปลงกฎหมายหรือข้อบังคับที่อาจส่งผลกระทบต่อระยะเวลาเก็บข้อมูล
- บันทึกผลการทบทวนและแก้ไขนโยบายตามความเหมาะสม

3. การจัดทำนโยบายระยะเวลาการจัดเก็บข้อมูลและเก็บรักษาข้อมูลส่วนบุคคล

3.1 โครงสร้างและเนื้อหาของนโยบาย

- วัตถุประสงค์ของนโยบาย
- ขอบเขตการใช้บังคับ
- นิยามและคำศัพท์ที่เกี่ยวข้อง
- การกำหนดประเภทข้อมูลส่วนบุคคลที่องค์กรเก็บรักษา
- ระยะเวลาการเก็บข้อมูลสำหรับแต่ละประเภทข้อมูล พร้อมเหตุผลประกอบ
- ขั้นตอนและวิธีการในการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคลเมื่อครบกำหนด
- ความรับผิดชอบของหน่วยงานและบุคลากรในการปฏิบัติตามนโยบาย
- การทบทวนและปรับปรุงนโยบาย

3.2 ตัวอย่างส่วนหนึ่งของนโยบายระยะเวลาการจัดเก็บข้อมูล

ตัวอย่างนโยบายระยะเวลาการจัดเก็บข้อมูล

ข้อมูลพนักงาน : เก็บไว้ตามกฎหมายแรงงานไม่น้อยกว่า 5 ปีหลังจากสิ้นสุดการจ้างงาน

ข้อมูลลูกค้า : เก็บไว้ตามวัตถุประสงค์ในการให้บริการ และไม่นานเกิน 7 ปี หลังจากสิ้นสุดการให้บริการ

ข้อมูลทางการเงิน : เก็บไว้ตามกฎหมายภาษีไม่น้อยกว่า 10 ปี

ข้อมูลทางการแพทย์ : เก็บไว้ตามกฎหมายว่าด้วยวิชาชีพและการแพทย์ไม่น้อยกว่า 10 ปี

การลบหรือทำลายข้อมูลจะต้องดำเนินการทันทีเมื่อครบกำหนด เว้นแต่มีข้อกฎหมายหรือข้อบังคับให้เก็บไว้ต่อ

3.3 การสื่อสารและอบรมนโยบาย

- จัดฝึกอบรมและสร้างความตระหนักให้กับพนักงานและผู้เกี่ยวข้อง
- ประกาศและเผยแพร่ภายในช่องทางภายในองค์กร
- มีเอกสารคู่มือหรือ FAQ เพื่อช่วยการเข้าใจและปฏิบัติตามนโยบาย

4. การดำเนินการตรวจสอบและรายงานผลการจัดเก็บและเก็บรักษาข้อมูล

4.1 การจัดทำรายงานตรวจสอบ

- รายงานสรุปประเภทข้อมูลและระยะเวลาที่จัดเก็บ
- รายงานความสอดคล้องกับนโยบายและข้อกำหนดทางกฎหมาย
- รายงานผลการลบหรือทำลายข้อมูลตามกำหนด

4.2 ตัวอย่างเนื้อหาารายงานตรวจสอบ

ตัวอย่างรายงานตรวจสอบการจัดเก็บข้อมูลส่วนบุคคล (สรุป)

วันที่ตรวจสอบ : 1 เมษายน 2568

ผู้ตรวจสอบ : ฝ่ายบริหารความเสี่ยงข้อมูล

ข้อมูลที่ตรวจสอบ : ข้อมูลพนักงาน, ข้อมูลลูกค้า, ข้อมูลทางการเงิน

สรุปผล :

ข้อมูลพนักงานทั้งหมด 1,200 รายการ มี 15 รายการเกินระยะเวลาที่กำหนด 6 เดือน ซึ่งอยู่ระหว่างดำเนินการลบ

ข้อมูลลูกค้าจัดเก็บสอดคล้องกับนโยบาย

ข้อมูลทางการเงินจัดเก็บครบถ้วนตามข้อกำหนด

ข้อเสนอแนะ : เร่งดำเนินการลบข้อมูลที่เก็บเกินกำหนด และทบทวนระบบจัดเก็บข้อมูลให้มีการแจ้งเตือนก่อนครบกำหนด

4.3 การเก็บรักษารายงานและการใช้เป็นหลักฐาน

- รายงานต้องถูกเก็บรักษาอย่างน้อย 5 ปี
- ใช้รายงานเป็นหลักฐานในการตรวจสอบภายในและการตรวจประเมินจากหน่วยงานภายนอก

5. การจัดทำหนังสือแจ้งการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคล

5.1 เนื้อหาในหนังสือแจ้ง

- รายละเอียดข้อมูลส่วนบุคคลที่ถูกลบ ทำลาย หรือส่งคืน
- วันที่ดำเนินการและวิธีการดำเนินการ
- เหตุผลการดำเนินการตามนโยบายและกฎหมาย
- รายชื่อผู้อนุมัติและผู้ดำเนินการ

5.2 ตัวอย่างหนังสือแจ้ง

หนังสือแจ้งการลบข้อมูลส่วนบุคคล

เลขที่หนังสือ : 001/2568

วันที่ : 15 เมษายน 2568

เรียน : เจ้าของข้อมูลส่วนบุคคล / ผู้เกี่ยวข้อง

ด้วยตามนโยบายการจัดเก็บข้อมูลส่วนบุคคลของบริษัทฯ และข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บริษัทฯ ได้ดำเนินการลบข้อมูลส่วนบุคคลของท่าน ดังรายละเอียดดังนี้

ประเภทข้อมูล : ข้อมูลลูกค้า (ประวัติการสั่งซื้อ)

วันที่เก็บข้อมูล : 1 มกราคม 2558 – 31 ธันวาคม 2561

วันที่ดำเนินการลบ : 15 เมษายน 2568

วิธีการลบ : การลบข้อมูลถาวรจากระบบฐานข้อมูลและสำเนาเอกสารที่เกี่ยวข้อง

หากท่านมีข้อสงสัย กรุณาติดต่อ ฝ่ายบริหารข้อมูลส่วนบุคคล บริษัทฯ โทร. 02-xxxxxxx

ลงชื่อ

(นางสาว สมหญิง ใจดี)

ผู้จัดการฝ่ายบริหารข้อมูลส่วนบุคคล

5.3 การเก็บรักษาเอกสารแจ้ง

- เก็บเอกสารในระบบเอกสารขององค์กรอย่างปลอดภัย
- เก็บไว้ไม่น้อยกว่า 5 ปีเพื่อรองรับการตรวจสอบ

6. สรุปและข้อเสนอแนะ

การกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลที่เหมาะสม เป็นเรื่องจำเป็นเพื่อรักษาสิทธิของเจ้าของข้อมูลและปฏิบัติตามกฎหมายอย่างครบถ้วน องค์กรควรจัดทำนโยบายที่ชัดเจน มีขั้นตอนปฏิบัติที่เป็นรูปธรรม และมีระบบติดตามตรวจสอบอย่างสม่ำเสมอ เพื่อป้องกันความเสี่ยงและสนับสนุนการบริหารข้อมูลอย่างมืออาชีพ

การสร้างวัฒนธรรมตระหนักและฝึกอบรมบุคลากรที่เกี่ยวข้องให้เข้าใจและปฏิบัติตามนโยบายเป็นสิ่งสำคัญ นอกจากนี้ การเก็บรักษาหลักฐานต่าง ๆ เช่น รายงานตรวจสอบและหนังสือแจ้งการลบ ทำลายข้อมูล ต้องดำเนินการอย่างรัดกุมเพื่อใช้เป็นเครื่องมือในการพิสูจน์ความถูกต้องในการบริหารจัดการข้อมูล

เช็คลิสต์การลบข้อมูลส่วนบุคคล

1. ระบุข้อมูลที่จะลบ

- ☐ ตรวจสอบประเภทข้อมูลส่วนบุคคลที่ครบกำหนดต้องลบ (personal data, special category data)
- ☐ ระบุแหล่งที่เก็บข้อมูล เช่น ระบบฐานข้อมูล, ไฟล์เอกสาร, ระบบอีเมล, เอกสารกระดาษ
- ☐ ตรวจสอบว่าข้อมูลดังกล่าวเป็นข้อมูลซ้ำหรือเชื่อมโยงกับระบบอื่นหรือไม่

2. ตรวจสอบสิทธิและภาระผูกพันทางกฎหมาย

- ☐ ตรวจสอบข้อกฎหมายหรือข้อบังคับที่กำหนดระยะเวลาเก็บข้อมูลขั้นต่ำ (เช่น กฎหมายภาษี, กฎหมายแรงงาน)
- ☐ ตรวจสอบคำขอลบข้อมูลจากเจ้าของข้อมูล (Data Subject Access Request - DSAR)
- ☐ ประเมินว่ามีข้อยกเว้นหรือเหตุผลในการเก็บข้อมูลต่อไป (เช่น คดีความ, สัญญาที่ยังไม่สิ้นสุด)

3. วางแผนและกำหนดวิธีการลบ

- ☐ เลือกวิธีการลบที่เหมาะสม เช่น ลบถาวร (permanent deletion), การทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ (anonymization/pseudonymization)

☐ กำหนดขั้นตอนการลบในระบบ IT และระบบเอกสาร

☐ กำหนดผู้รับผิดชอบในการดำเนินการลบ

☐ กำหนดกำหนดเวลาที่ต้องดำเนินการลบ

4. ดำเนินการลบข้อมูล

☐ ดำเนินการลบข้อมูลตามขั้นตอนที่กำหนด

☐ ตรวจสอบว่าข้อมูลถูกลบหรือทำลายอย่างสมบูรณ์ในทุกระบบ

☐ สำรองข้อมูล (backup) ที่เกี่ยวข้องได้รับการลบหรือลบตามนโยบาย

5. ยืนยันและบันทึกผลการลบ

☐ จัดทำเอกสารยืนยันการลบข้อมูล (Data Deletion Confirmation)

☐ บันทึกรายละเอียดการลบ เช่น วัน เวลา วิธีการ และผู้ดำเนินการ

☐ จัดเก็บเอกสารยืนยันการลบอย่างปลอดภัยเพื่อใช้เป็นหลักฐานในการตรวจสอบภายหลัง

6. แจ้งผู้เกี่ยวข้อง (ถ้ามี)

☐ แจ้งเจ้าของข้อมูลว่าข้อมูลได้ถูกลบตามคำขอ (ถ้ามีคำขอ)

☐ แจ้งหน่วยงานหรือฝ่ายที่เกี่ยวข้องภายในองค์กร

7. ทบทวนและปรับปรุงกระบวนการ

☐ ทบทวนผลการลบข้อมูลเป็นระยะ ๆ เพื่อประเมินประสิทธิภาพ

☐ ปรับปรุงนโยบายและขั้นตอนการลบข้อมูลตามข้อเสนอแนะหรือการเปลี่ยนแปลงกฎหมาย

☐ จัดอบรมและสร้างความตระหนักในทีมงานที่เกี่ยวข้อง

8. ตรวจสอบและประเมินความเสี่ยง

☐ ตรวจสอบว่าการลบข้อมูลไม่ได้ส่งผลกระทบต่อ การดำเนินธุรกิจหรือการปฏิบัติตามกฎหมายอื่น ๆ

☐ ประเมินความเสี่ยงที่อาจเกิดจากการลบข้อมูล เช่น การสูญหายของข้อมูลสำคัญ

9.4.2 มีเอกสารหรือข้อมูลเพื่อระบุระยะเวลาสำหรับการจำหน่ายออกเพื่อลบหรือทำลายข้อมูลทั้งหมด ระยะเวลาการจัดเก็บ

สิ่งที่ต้องทำ: มีเอกสารหรือข้อมูลเพื่อระบุระยะเวลาสำหรับการจำหน่ายออกเพื่อลบหรือทำลายข้อมูลทั้งหมดระยะเวลาการจัดเก็บครบทุกประเภทข้อมูล

หลักฐาน: นโยบายการควบคุมระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล
ทะเบียนการประมวลผลข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22 มาตรา 37 (1) (3)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 22 มาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

1. นโยบายการควบคุมระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล

1.1 วัตถุประสงค์ของนโยบาย

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดแนวทางและระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลในองค์กร เพื่อให้สอดคล้องกับข้อกำหนดและข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล รวมถึงเพื่อป้องกันการจัดเก็บข้อมูลเกินความจำเป็นหรือเก็บไว้นานเกินกำหนด

1.2 ขอบเขต

นโยบายนี้ครอบคลุมข้อมูลส่วนบุคคลทุกประเภทที่องค์กรเก็บรวบรวมและประมวลผล ไม่ว่าจะเป็นข้อมูลในรูปแบบอิเล็กทรอนิกส์หรือเอกสารกระดาษ

1.3 การกำหนดระยะเวลาการเก็บข้อมูล

- ระยะเวลาการเก็บข้อมูลจะถูกกำหนดโดยพิจารณาจากความจำเป็นทางธุรกิจ ข้อกำหนด ข้อบังคับ และหลักการคุ้มครองข้อมูลส่วนบุคคล
- ระยะเวลานี้จะถูกระบุอย่างชัดเจนในทะเบียนการประมวลผลข้อมูลส่วนบุคคล และจะได้รับการทบทวนอย่างสม่ำเสมอเพื่อให้ทันสมัยและเหมาะสม

1.4 กระบวนการจำหน่ายข้อมูล

- เมื่อข้อมูลครบกำหนดระยะเวลาการเก็บรักษา ข้อมูลดังกล่าวจะต้องถูกจำหน่ายออกโดยการลบหรือทำลายอย่างปลอดภัย
- การจำหน่ายออกต้องดำเนินการโดยบุคลากรที่ได้รับมอบหมาย และต้องมีการบันทึกหลักฐานทุกขั้นตอน
- ในกรณีที่มีข้อจำกัดทางกฎหมายหรือสัญญา ข้อมูลอาจต้องถูกเก็บต่อจนกว่าจะครบเงื่อนไขดังกล่าว

1.5 ความรับผิดชอบ

- ผู้ควบคุมข้อมูลมีหน้าที่กำหนดและควบคุมการดำเนินการตามนโยบายนี้
- ผู้ปฏิบัติงานทุกคนต้องปฏิบัติตามนโยบายและรายงานปัญหาหรือข้อผิดพลาดที่เกี่ยวข้อง

1.6 การฝึกอบรมและสร้างความตระหนัก

จัดให้มีการฝึกอบรมและสื่อสารให้บุคลากรทุกคนรับทราบและเข้าใจนโยบายนี้อย่างต่อเนื่อง

2. ทะเบียนการประมวลผลข้อมูลส่วนบุคคล (Data Processing Register)

2.1 รายละเอียดข้อมูลในทะเบียน

- ประเภทข้อมูลส่วนบุคคลที่เก็บรวบรวม
- วัตถุประสงค์การเก็บข้อมูล
- ระยะเวลาการเก็บข้อมูลที่กำหนดไว้สำหรับแต่ละประเภทข้อมูล

- วิธีการเก็บรักษาและสถานที่เก็บข้อมูล
- บุคคลหรือฝ่ายที่รับผิดชอบในการดูแลข้อมูลแต่ละประเภท

2.2 การจัดทำและบำรุงรักษาทะเบียน

- ทะเบียนต้องได้รับการจัดทำขึ้นอย่างครบถ้วนและเป็นปัจจุบัน
- มีการตรวจสอบและทบทวนข้อมูลในทะเบียนเป็นประจำ (อย่างน้อยปีละหนึ่งครั้ง)
- บันทึกการเปลี่ยนแปลงหรือปรับปรุงระยะเวลาการเก็บข้อมูลที่เกิดขึ้นทุกครั้ง

2.3 การใช้ทะเบียนในการบริหารจัดการข้อมูล

- ใช้เป็นเครื่องมือในการตรวจสอบว่าข้อมูลใดครบกำหนดต้องลบหรือทำลาย
- สนับสนุนการวางแผนและดำเนินการจำหน่ายข้อมูลตามระยะเวลาที่กำหนด
- เป็นหลักฐานแสดงการปฏิบัติตามกฎหมายและข้อกำหนดด้านการคุ้มครองข้อมูล

3. ตัวอย่างการกำหนดระยะเวลาการจัดเก็บข้อมูลในทะเบียน

ประเภทข้อมูล	วัตถุประสงค์การเก็บข้อมูล	ระยะเวลาการเก็บรักษา	หมายเหตุ
ข้อมูลลูกค้า	การให้บริการและการจัดการบัญชี	5 ปี หลังจากสิ้นสุดสัญญา	ตามข้อกำหนดทางธุรกิจและภาษี
ข้อมูลพนักงาน	การบริหารทรัพยากรบุคคล	10 ปี หลังสิ้นสุดการทำงาน	ตามกฎหมายแรงงานและสวัสดิการ
ข้อมูลผู้สมัครงาน	การคัดเลือกและประเมินผล	1 ปี หลังจากสิ้นสุดกระบวนการ	เพื่อป้องกันการเก็บข้อมูลเกินความจำเป็น
ข้อมูลการเงินและบัญชี	การตรวจสอบภาษีและการเงิน	7 ปี ตามกฎหมายภาษี	ตามประกาศกรมสรรพากร
ข้อมูลสุขภาพ	การรักษาพยาบาลและประกันภัย	15 ปี ตามกฎหมายสุขภาพ	มีความละเอียดอ่อนสูง

4. สรุปข้อกำหนดและบทลงโทษตามกฎหมายที่เกี่ยวข้อง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22 และมาตรา 37 (1) (3) กำหนดให้องค์กรต้องกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล และต้องลบหรือทำลายข้อมูลเมื่อครบกำหนด

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) กำหนดมาตรการด้านความมั่นคงปลอดภัยในการจัดเก็บและจำหน่ายข้อมูล

หากไม่ปฏิบัติตาม มีโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

9.4.3 มีการมอบหมายหน้าที่ความรับผิดชอบเพื่อลบหรือทำลายข้อมูลตามระยะเวลาการทำลายที่กำหนดไว้ ให้มีการทบทวนการลบหรือทำลายข้อมูลนั้น

สิ่งที่ต้องทำ: มีการมอบหมายหน้าที่ความรับผิดชอบเพื่อลบหรือทำลายข้อมูลตามระยะเวลาที่กำหนดไว้ มีกระบวนการรวมถึงหลักฐานในการแจ้งให้บุคลากรดังกล่าวดำเนินการลบหรือทำลายชัดเจน

หลักฐาน: นโยบายการควบคุมระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล

ทะเบียนการประมวลผลข้อมูลส่วนบุคคล

หนังสือแจ้งการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) (3)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (6)

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

1. นโยบายการควบคุมระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล

1.1 วัตถุประสงค์

กำหนดแนวทางและหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องในการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อครบระยะเวลาที่กำหนดไว้ เพื่อให้การดำเนินการเป็นไปอย่างถูกต้อง โปร่งใส และเป็นไปตามกฎหมาย

1.2 การมอบหมายหน้าที่ความรับผิดชอบ

กำหนดบุคคลหรือหน่วยงานรับผิดชอบในการตรวจสอบข้อมูลที่ครบกำหนดการเก็บรักษา กำหนดบุคลากรหรือทีมงานที่มีหน้าที่ในการดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลอย่างปลอดภัย จัดทำระบบแจ้งเตือนเพื่อให้บุคลากรที่รับผิดชอบได้รับข้อมูลและดำเนินการตามระยะเวลาที่กำหนด

1.3 กระบวนการลบหรือทำลายข้อมูล

- ผู้รับผิดชอบจะต้องดำเนินการลบหรือทำลายข้อมูลตามที่ระบุในทะเบียนการประมวลผลข้อมูลส่วนบุคคล

- จัดทำบันทึกหรือเอกสารแจ้งการลบหรือทำลายข้อมูลทุกครั้ง โดยระบุประเภทข้อมูล วันที่ดำเนินการ และวิธีการลบ/ทำลาย
- ดำเนินการทบทวนและตรวจสอบประสิทธิภาพของกระบวนการลบหรือทำลายข้อมูลอย่างสม่ำเสมอ เพื่อป้องกันข้อผิดพลาดและข้อมูลรั่วไหล

1.4 การสื่อสารและฝึกอบรม

แจ้งให้บุคลากรที่เกี่ยวข้องทราบนโยบายและกระบวนการลบหรือทำลายข้อมูลอย่างชัดเจน จัดอบรมให้ความรู้เกี่ยวกับความสำคัญและขั้นตอนในการดำเนินการลบหรือทำลายข้อมูลตามกฎหมาย

2. ทะเบียนการประมวลผลข้อมูลส่วนบุคคล

2.1 บันทึกรายละเอียดข้อมูลและระยะเวลาการเก็บรักษา

- ระบุประเภทข้อมูลที่ต้องลบหรือทำลายพร้อมระยะเวลาที่กำหนด
- ระบุผู้รับผิดชอบในการดำเนินการลบหรือทำลายข้อมูล
- บันทึกวันที่ที่ข้อมูลครบกำหนดและวันที่ดำเนินการลบหรือทำลายจริง

2.2 การติดตามและทบทวน

- มีระบบตรวจสอบว่าการลบหรือทำลายข้อมูลเกิดขึ้นจริงตามเวลาที่กำหนด
- ตรวจสอบและทบทวนทะเบียนประมวลผลข้อมูลเป็นระยะอย่างน้อยปีละ 1 ครั้ง
- บันทึกผลการตรวจสอบและรายงานปัญหาหรือข้อผิดพลาดที่พบ

3. ตัวอย่างหนังสือแจ้งการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคล

เรื่อง แจ้งการลบ/ทำลายข้อมูลส่วนบุคคล

เรียน [ชื่อผู้รับผิดชอบ]

ตามที่ข้อมูลส่วนบุคคลประเภท [ระบุประเภทข้อมูล] ได้ครบกำหนดระยะเวลาการเก็บรักษาตามนโยบายขององค์กรและกฎหมายที่เกี่ยวข้อง จึงขอแจ้งให้ท่านดำเนินการลบ/ทำลายข้อมูลดังกล่าวภายในวันที่ [ระบุวันที่] โดยใช้วิธีการ [ระบุวิธีการลบหรือทำลาย เช่น การลบข้อมูลในระบบอย่างถาวร การทำลายเอกสารทางกายภาพ]

กรุณabanบันทึกและรายงานผลการดำเนินการมายังฝ่ายควบคุมข้อมูลส่วนบุคคลภายในวันที่ [ระบุวันที่] เพื่อเป็นหลักฐานการปฏิบัติตามข้อกำหนด

ขอแสดงความนับถือ

[ชื่อผู้ส่ง]

[ตำแหน่ง]

[หน่วยงาน]

[วันที่]

4. สรุปข้อกำหนดและบทลงโทษ

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) (3)
กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล รวมถึงการลบหรือทำลายข้อมูลเมื่อครบระยะเวลาที่กำหนด
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (6)
กำหนดมาตรการการรักษาความมั่นคงปลอดภัยและหน้าที่ของผู้รับผิดชอบในการปฏิบัติตามระเบียบการลบหรือทำลายข้อมูล
- บทลงโทษ
หากไม่ปฏิบัติตามมาตรการดังกล่าว จะมีโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

9.4.4 มีการทบทวนข้อมูลที่จัดเก็บไว้เพื่อระบุโอกาสในการลดการจัดเก็บข้อมูล (เช่น หากสามารถลบหรือทำลายได้ก็ให้ดำเนินการ) การแปลงข้อมูลให้เป็นข้อมูลแฝง (Pseudonymization) หรือการทำให้ข้อมูลเป็นนิรนาม (Anonymization)

สิ่งที่ต้องทำ: มีการทบทวนข้อมูลที่จัดเก็บไว้เพื่อระบุโอกาสในการลดการจัดเก็บข้อมูล (เช่น หากสามารถลบหรือทำลายได้ ก็ให้ดำเนินการ) การแปลงข้อมูลให้เป็นข้อมูลแฝง (Pseudonymization) หรือการทำให้ข้อมูลเป็นนิรนาม (Anonymization) และมีเอกสารประกอบครบถ้วน

หลักฐาน: นโยบายการควบคุมระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล
ทะเบียนการประมวลผลข้อมูลส่วนบุคคล
หนังสือแจ้งการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคล หรือแปลงข้อมูลส่วนบุคคลนั้นให้เป็นข้อมูลแฝง (Pseudonymization) หรือทำให้เป็นนิรนาม (Anonymization)

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22 มาตรา 37 (3)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4), ข้อ 5

โทษทางปกครอง: ในกรณีที่มิปฏิบัติตามมาตรา 22 มาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

1. นโยบายการควบคุมระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล (Data Retention and Minimization Policy)

1.1 วัตถุประสงค์

กำหนดแนวทางในการทบทวนข้อมูลส่วนบุคคลที่จัดเก็บไว้ เพื่อลดความเสี่ยงจากการเก็บข้อมูลเกินจำเป็น และป้องกันการละเมิดสิทธิส่วนบุคคล โดยมีการลบ ทำลาย หรือแปลงข้อมูลเพื่อความปลอดภัย

1.2 ขอบเขต

ครอบคลุมข้อมูลส่วนบุคคลทุกประเภทที่องค์กรเป็นผู้ควบคุมข้อมูล (Data Controller) รวมถึงข้อมูลที่อยู่ในรูปแบบดิจิทัลและกายภาพ

1.3 หลักการปฏิบัติ

- ทบทวนข้อมูลส่วนบุคคลที่จัดเก็บอย่างสม่ำเสมอ (อย่างน้อยปีละ 1 ครั้ง) เพื่อประเมินว่าข้อมูลใดควรลบหรือทำลาย
- ประเมินโอกาสในการลดการจัดเก็บข้อมูลผ่านวิธีการแปลงข้อมูลให้เป็นข้อมูลแฝง (Pseudonymization) หรือทำให้เป็นนิรนาม (Anonymization)
- ดำเนินการลบ ทำลาย หรือแปลงข้อมูลที่หมดความจำเป็นหรือที่สามารถลดความเสี่ยงได้ โดยต้องมีเอกสารบันทึกและรายงานชัดเจน

1.4 คำนิยามสำคัญ

- การแปลงข้อมูลให้เป็นข้อมูลแฝง (Pseudonymization): การแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบที่ไม่สามารถระบุตัวบุคคลได้โดยตรงโดยไม่ใช้ข้อมูลเพิ่มเติม
- การทำให้ข้อมูลเป็นนิรนาม (Anonymization): การปรับเปลี่ยนข้อมูลจนไม่สามารถระบุตัวบุคคลได้เลย ไม่ว่าจะใช้ข้อมูลเสริมใดๆ ก็ตาม

2. ทะเบียนการประมวลผลข้อมูลส่วนบุคคล (Data Processing Register)

2.1 รายละเอียดที่ต้องบันทึก

- ประเภทข้อมูลส่วนบุคคล
- ระยะเวลาที่จัดเก็บข้อมูลตามนโยบายและกฎหมาย
- การดำเนินการทบทวนข้อมูลในแต่ละรอบ
- วิธีการลบ ทำลาย หรือแปลงข้อมูลที่ใช้ (ระบุเป็น Pseudonymization หรือ Anonymization)
- วันที่ดำเนินการและผู้รับผิดชอบ

3. ตัวอย่างหนังสือแจ้งการลบ ทำลาย หรือแปลงข้อมูล

เรื่อง แจ้งการดำเนินการลบ/ทำลาย/แปลงข้อมูลส่วนบุคคล

เรียน [ชื่อผู้รับผิดชอบ]

ตามที่ข้อมูลส่วนบุคคลประเภท [ระบุประเภทข้อมูล] ที่อยู่ภายใต้ความรับผิดชอบของท่าน ได้ผ่านการทบทวนตามนโยบายควบคุมระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล และพบว่าข้อมูลดังกล่าว

1. ครบกำหนดระยะเวลาการเก็บรักษา และควรดำเนินการลบ/ทำลาย หรือ
2. มีความเหมาะสมในการแปลงเป็นข้อมูลแฝง (Pseudonymization) หรือทำให้เป็นนิรนาม (Anonymization)

จึงขอให้ท่านดำเนินการตามข้อกำหนดดังกล่าว ภายในวันที่ [ระบุวันที่] และจัดส่งรายงานผลการดำเนินการมายังฝ่ายควบคุมข้อมูลส่วนบุคคล เพื่อเป็นหลักฐานการปฏิบัติงาน

ขอแสดงความนับถือ

[ชื่อผู้ส่ง]

[ตำแหน่ง]

[หน่วยงาน]

[วันที่]

4. แนวทางการดำเนินการทบทวนและลดการจัดเก็บข้อมูล

4.1 ขั้นตอนการทบทวนข้อมูล

- รวบรวมข้อมูลที่จัดเก็บไว้ทั้งหมดในระบบและรูปแบบเอกสาร
- ตรวจสอบระยะเวลาที่ข้อมูลแต่ละชุดได้รับการจัดเก็บเทียบกับนโยบายและกฎหมาย
- ระบุข้อมูลที่ครบกำหนดหรือไม่จำเป็นต้องเก็บต่อไป

4.2 การลบหรือทำลายข้อมูล

- ดำเนินการลบหรือทำลายข้อมูลที่ไม่จำเป็นต้องเก็บไว้ เช่น การลบไฟล์ข้อมูลในระบบ การทำลายเอกสารทางกายภาพ
- บันทึกหลักฐานการลบหรือทำลายข้อมูล

4.3 การแปลงข้อมูลให้เป็นข้อมูลแฝง (Pseudonymization)

- ใช้เทคนิคการเข้ารหัสหรือแยกข้อมูลตัวระบุออกจากข้อมูลที่ใช้วิเคราะห์ เช่น การแทนที่ชื่อด้วยรหัส
- ข้อมูลที่ถูกแปลงยังสามารถนำไปใช้วิเคราะห์หรือประมวลผลได้โดยไม่ระบุตัวบุคคลได้โดยตรง

4.4 การทำให้ข้อมูลเป็นนิรนาม (Anonymization)

- กำจัดหรือลบข้อมูลที่สามารถระบุตัวบุคคลได้ทั้งหมด
- ข้อมูลนิรนามไม่สามารถเชื่อมโยงกลับไปยังตัวบุคคลได้อีก

5. สถาปัตยกรรมทางกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22, 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

9.5 การลบหรือทำลายข้อมูล (Destruction)

องค์กรกำหนดนโยบายการลบหรือทำลายข้อมูลไว้ในนโยบายที่เกี่ยวข้องอย่างเหมาะสมเพื่อป้องกันการเปิดเผยข้อมูลโดยไม่ชอบด้วยกฎหมาย ก่อน ระหว่าง หรือภายหลังการลบหรือทำลาย

9.5.1 สำหรับเอกสารที่เป็นกระดาษ มีการใช้ถังขยะที่ล็อกได้เพื่อจัดเก็บข้อมูลส่วนบุคคลไว้ ใช้การขอยให้เป็นชิ้นเล็ก ๆ ในการทำลายกระดาษ หรือใช้การเผาทิ้ง

สิ่งที่ต้องทำ: สำหรับเอกสารที่เป็นกระดาษ มีการใช้ถังขยะที่ล็อกได้เพื่อจัดเก็บข้อมูลส่วนบุคคลไว้ ใช้การขอยให้เป็นชิ้นเล็ก ๆ ในการทำลายกระดาษ หรือใช้การเผาทิ้ง

หลักฐาน: นโยบายการลบข้อมูลส่วนบุคคลที่เป็นกระดาษสถาปัตยกรรม: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) (3)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้
ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ.
2567 ข้อ 3, ข้อ 9

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายและแนวปฏิบัติในการลบหรือทำลายข้อมูลส่วนบุคคลที่เป็นเอกสารกระดาษ

1. วัตถุประสงค์

เพื่อกำหนดนโยบายและแนวปฏิบัติที่ชัดเจนเกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคลในรูปแบบเอกสารกระดาษอย่างปลอดภัย มีประสิทธิภาพ และเป็นมิตรกับสิ่งแวดล้อม ตลอดจนป้องกันการเข้าถึงหรือเปิดเผยข้อมูลโดยมิชอบ ซึ่งอาจก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือองค์กร

2. ขอบเขตการบังคับใช้

ใช้บังคับกับบุคลากรทุกระดับในหน่วยงาน/องค์กรที่เกี่ยวข้องกับการจัดเก็บ ใช้งาน หรือทำลายเอกสารที่มีข้อมูลส่วนบุคคลไม่ว่าโดยตรงหรือโดยอ้อม

3. นิยามคำศัพท์ที่เกี่ยวข้อง

3.1 **ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าโดยตรงหรือทางอ้อม

3.2 **การทำลายเอกสาร** หมายถึง การดำเนินการใด ๆ ที่ทำให้ข้อมูลไม่สามารถนำกลับมาใช้ใหม่ หรือไม่สามารถระบุตัวเจ้าของข้อมูลได้อีกต่อไป

3.3 **เจ้าหน้าที่ผู้รับผิดชอบ** หมายถึง พนักงานที่ได้รับมอบหมายในการดำเนินการทำลายข้อมูล และจัดเก็บหลักฐานการดำเนินการ

4. ขั้นตอนการทำลายข้อมูลส่วนบุคคลในรูปแบบกระดาษ

4.1 เอกสารที่มีข้อมูลส่วนบุคคลซึ่งไม่จำเป็นต้องใช้งานอีก ต้องแยกออกจากเอกสารทั่วไป และจัดเก็บไว้ในภาชนะเฉพาะ เช่น ถังขยะล็อกได้ (lockable bin) หรือกล่องที่มีระบบปิดผนึก

4.2 ก่อนทำลายเอกสาร ให้ผู้รับผิดชอบดำเนินการตรวจสอบและลงบันทึกเอกสารที่เตรียมจะทำลาย โดยระบุรายละเอียดที่จำเป็น เช่น วันที่ ชื่อผู้อนุมัติ ฯลฯ

4.3 การทำลายเอกสารสามารถดำเนินการได้ด้วยวิธีดังต่อไปนี้

4.3.1 **การใช้เครื่องทำลายเอกสารแบบละเอียด (Micro-Cut Shredder)** ซึ่งสามารถชอยเอกสารให้เป็นเส้นขนาดไม่เกิน 5 มิลลิเมตร และไม่สามารถนำกลับมาประกอบใหม่ได้

4.3.2 **การส่งต่อเอกสารไปยังผู้ให้บริการกำจัดเอกสารแบบปลอดภัย (Certified Destruction Vendor)** ซึ่งมีระบบควบคุมการทำลายตามมาตรฐาน ISO/IEC 21964 และมีใบรับรองการทำลาย (Certificate of Destruction)

4.4 ห้ามทำลายเอกสารด้วยการเผาเว้นแต่มีระบบควบคุมมลพิษที่ได้รับอนุญาตจากหน่วยงานสิ่งแวดล้อม

4.5 หลังการทำลาย ให้เจ้าหน้าที่จัดทำรายงานผลการทำลาย พร้อมลงนามรับรองโดยผู้ดำเนินการ และผู้ตรวจสอบ

5. ตารางบันทึกการทำลายเอกสารที่มีข้อมูลส่วนบุคคล

ลำดับ	วันที่ทำลาย	รายละเอียดเอกสาร	จำนวนหน้า	วิธีการทำลาย	ชื่อผู้ดำเนินการ	ชื่อผู้ตรวจสอบ	หมายเหตุ
1	05/06/2562	ใบสมัครงาน ปี 2562	120 หน้า	Micro-Cut Shredder	นายสมชาย ใจดี	นางสาว รัตนา มีสุข	ทำลายสำเร็จ
2	02/06/2562	แบบฟอร์ม ลูกค้าเก่า	200 หน้า	บริการกำจัดจาก บริษัท A	น.ส.กัญญา สายชล	นาย วิทยา ตรงธรรม	แนบใบรับรองแล้ว
...	...	...	...	...	...	...	...

6. การอบรมและควบคุมภายใน

6.1 องค์กรจะจัดการอบรมอย่างน้อยปีละ 1 ครั้ง เกี่ยวกับการจัดการเอกสารที่มีข้อมูลส่วนบุคคล และวิธีการทำลายข้อมูลอย่างถูกต้อง

6.2 ฝ่ายตรวจสอบภายในจะสุ่มตรวจการดำเนินการทำลายข้อมูลทุกไตรมาส และรายงานต่อผู้บริหารระดับสูง

7. อ้างอิงกฎหมายและประกาศที่เกี่ยวข้อง

7.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) และ (3)

7.2 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2), (4)

7.3 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ พ.ศ. 2567 ข้อ 3 และ ข้อ 9

8. บทกำหนดโทษกรณีไม่ปฏิบัติตาม

ผู้ควบคุมข้อมูลส่วนบุคคลที่ไม่ปฏิบัติตามมาตรา 37 อาจถูกลงโทษทางปกครองด้วยการปรับไม่เกิน 3,000,000 บาท

9. วันมีผลบังคับใช้

ตั้งแต่วันที่ เป็นต้นไป

10. ผู้รับผิดชอบในการดำเนินการ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือผู้ที่ได้รับมอบหมายโดยผู้ควบคุมข้อมูล

9.5.2 สำหรับข้อมูลที่อยู่บนอุปกรณ์ไฟฟ้าอิเล็กทรอนิกส์ มีการใช้วิธีการลบหรือทำลายที่มีความมั่นคงปลอดภัย หรือการทำลายสนามแม่เหล็กบนอุปกรณ์ดังกล่าว

สิ่งที่ต้องทำ: ข้อมูลที่อยู่บนอุปกรณ์ไฟฟ้าอิเล็กทรอนิกส์มีการใช้วิธีการลบหรือทำลายที่มีความมั่นคงปลอดภัย หรือการทำลายสนามแม่เหล็กบนอุปกรณ์ดังกล่าว

หลักฐาน: นโยบายการลบข้อมูลส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) (3)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567 ข้อ 3 วรรคสอง

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการลบหรือทำลายข้อมูลอิเล็กทรอนิกส์ พร้อมขั้นตอนการอนุมัติ

แบบฟอร์มลงนาม และการเชื่อมโยงกับมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27701:2019

วัตถุประสงค์

เพื่อกำหนดแนวทางการลบหรือทำลายข้อมูลส่วนบุคคลที่จัดเก็บอยู่ในรูปแบบอิเล็กทรอนิกส์อย่างปลอดภัย ไม่สามารถกู้คืนหรือเข้าถึงข้อมูลได้อีก ทั้งนี้เพื่อให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และมาตรฐานความมั่นคงปลอดภัยของสารสนเทศ

ขอบเขต

นโยบายนี้ครอบคลุมถึงข้อมูลส่วนบุคคลที่จัดเก็บหรือประมวลผลอยู่ในอุปกรณ์อิเล็กทรอนิกส์ทุกประเภท เช่น คอมพิวเตอร์ แล็ปท็อป เซิร์ฟเวอร์ ฮาร์ดดิสก์ USB แฟลชไดรฟ์ โทรศัพท์มือถือ กล้องวงจรปิด หรืออุปกรณ์ IoT อื่นใดที่อาจมีการจัดเก็บข้อมูลส่วนบุคคล

หลักการ

- (1) ข้อมูลส่วนบุคคลที่หมดความจำเป็นต้องใช้ตามวัตถุประสงค์หรือครบระยะเวลาการเก็บรักษา ต้องถูกลบหรือทำลายโดยวิธีที่มั่นคงปลอดภัย
- (2) การทำลายจะต้องดำเนินการโดยเจ้าหน้าที่ที่ได้รับมอบหมายหรือผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น
- (3) ต้องมีการขออนุมัติล่วงหน้าก่อนการทำลาย และจัดเก็บหลักฐานการดำเนินการทุกครั้ง
- (4) วิธีการลบหรือทำลายต้องสอดคล้องกับมาตรฐาน ISO/IEC 27001:2022 ข้อ A.8.10 และ ISO/IEC 27701:2019 ข้อ 7.4.6

วิธีการลบหรือทำลายข้อมูล

- (4.1) การลบข้อมูลแบบปลอดภัย (Secure Deletion) โดยใช้ซอฟต์แวร์ที่ได้มาตรฐาน เช่น DBAN, Blancco, Eraser หรือฟังก์ชัน overwrite ข้อมูลอย่างน้อย 3 รอบ
- (4.2) การทำลายข้อมูลด้วยวิธีการฟอร์แมตที่ไม่สามารถกู้คืนได้ เช่น Low-level format หรือ Secure Wipe
- (4.3) การทำลายอุปกรณ์จัดเก็บข้อมูล (Physical Destruction) เช่น การบด การทุบ การเจาะ หรือการใช้เครื่องทำลายฮาร์ดดิสก์โดยเฉพาะ
- (4.4) ไม่แนะนำให้ใช้วิธีการทำลายโดยการเผา เนื่องจากมีผลกระทบต่อสิ่งแวดล้อม

ขั้นตอนการอนุมัติการลบหรือทำลาย

- (5.1) หน่วยงานที่ต้องการลบหรือทำลายข้อมูล ยื่นคำขอโดยกรอกแบบฟอร์มอนุมัติ (แนบท้าย)
- (5.2) เจ้าหน้าที่ DPO หรือเจ้าหน้าที่รักษาความมั่นคงปลอดภัยของสารสนเทศพิจารณาคำขอ
- (5.3) ผู้อำนวยการฝ่ายหรือผู้บริหารระดับที่กำหนดอนุมัติคำขอ
- (5.4) เจ้าหน้าที่ดำเนินการลบหรือทำลายตามวิธีที่ได้รับอนุมัติ
- (5.5) บันทึกผลการดำเนินการลงในตารางบันทึก และแนบรายงานผลการลบหรือทำลายพร้อมลายมือชื่อของผู้รับผิดชอบ

ตารางบันทึกการลบหรือทำลายข้อมูล

ลำดับ	วันที่ดำเนินการ	รายละเอียดอุปกรณ์/ไฟล์	วิธีที่ใช้	ผู้ดำเนินการ	ผู้อนุมัติ	หมายเหตุ
1	15/01/2567	คอมพิวเตอร์ตั้งโต๊ะ (R-WS-001)	Secure Erase ด้วย DBAN	นายกิตติพงศ์ อินทร์ดี	น.ส.จาร์วรรณ พงษ์สุข	เครื่องเก่าหมดอายุการใช้งานแล้ว

2	28/02/2567	USB Flash Drive 1GB	ฟอร์แมตแบบ low-level	น.ส.สมฤดี ทองแท้	นายธีรชาติ คำงาม	พบข้อมูลพนักงานหมดความจำเป็นต้องใช้
3	10/03/2567	ฮาร์ดดิสก์สำรอง (Backup Server 01)	บดทำลายด้วยเครื่องทำลาย HDD	นายวีระพงษ์ จันทรีไส	น.ส.ณัฐชยา วัฒนโชติ	ตามรอบการหมุนเวียน 3 ปี
4	24/04/2567	กล้องวงจรปิด (ระบบ Analog DVR)	ลบไฟล์ภาพย้อนหลัง 90 วันโดยใช้ CMS	นายธนพนธ์ หอมจันทร์	นางสาวสุภาวดี เจริญสุข	ตามนโยบาย retention 90 วัน
5	05/06/2567	โทรศัพท์มือถือบริษัท (รุ่น iPhone 11)	Wipe ข้อมูลผ่านระบบ MDM (Intune)	นายกฤษณ์ คำใส	นายภาณุวัฒน์ ศิริพานิช	พนักงานลาออก ระบบถอนการควบคุมแล้ว

แบบฟอร์มอนุมัติการลบหรือทำลายข้อมูล (แนบท้าย)

คำขออนุมัติการลบหรือทำลายข้อมูลส่วนบุคคล (อิเล็กทรอนิกส์)

ชื่อผู้ยื่นคำขอ:

ตำแหน่ง:

หน่วยงาน:

รายละเอียดข้อมูลที่ต้องการลบหรือทำลาย:

.....

วิธีการที่เสนอใช้:

เหตุผลในการลบหรือทำลาย:

ลงชื่อผู้ขอ วันที่

ความเห็นของ DPO/เจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศ:

.....

ลงชื่อผู้อนุมัติ วันที่

การเชื่อมโยงกับกฎหมายและมาตรฐาน

- (8.1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) และ (3)
 (8.2) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย พ.ศ. 2565 ข้อ 4 (2) และ (4)
 (8.3) ประกาศคณะกรรมการฯ เรื่อง หลักเกณฑ์ในการลบหรือทำลายข้อมูล พ.ศ. 2567 ข้อ 3 วรรคสอง
 (8.4) มาตรฐาน ISO/IEC 27001:2022 - ข้อ A.8.10 (Disposal of media)
 (8.5) มาตรฐาน ISO/IEC 27701:2019 - ข้อ 7.4.6 (Secure disposal and erasure)

บทลงโทษกรณีไม่ปฏิบัติตาม

หากผู้ควบคุมข้อมูลไม่ปฏิบัติตามมาตรา 37 แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อาจได้รับโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

9.5.3 มีการส่งขยะที่มีข้อมูลความลับไปกำจัดนอกสถานที่โดยวิธีการที่มีความมั่นคงปลอดภัย

สิ่งที่ต้องทำ: มีการส่งขยะที่มีข้อมูลความลับไปกำจัดนอกสถานที่โดยวิธีการที่มีความมั่นคงปลอดภัย และมีหลักฐานสนับสนุน

หลักฐาน: นโยบายการลบข้อมูลส่วนบุคคลที่เป็นกระดาษ
 ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
 บันทึกข้อตกลงรักษาความลับ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) (3)
 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)
 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. 2567

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การส่งขยะที่มีข้อมูลความลับไปกำจัดนอกสถานที่โดยวิธีที่มีความมั่นคงปลอดภัย

1. วัตถุประสงค์

เพื่อให้การกำจัดข้อมูลความลับหรือข้อมูลส่วนบุคคลที่ไม่จำเป็นต้องใช้ต่อไปแล้วเป็นไปอย่างปลอดภัย ป้องกันการรั่วไหลจากการส่งข้อมูลหรือวัสดุออกนอกสถานที่ขององค์กร โดยเฉพาะข้อมูลในรูปแบบกระดาษหรือวัสดุอื่นที่อาจสามารถระบุข้อมูลส่วนบุคคลได้

2. แนวทางปฏิบัติ

(1) การคัดแยกและบรรจุ

เอกสารที่มีข้อมูลความลับหรือข้อมูลส่วนบุคคลจะต้องได้รับการคัดแยกออกจากขยะทั่วไป บรรจุในภาชนะที่ไม่โปร่งแสง มีฉลากกำกับ “ข้อมูลส่วนบุคคล/ข้อมูลลับ – รอทำลาย” ภาชนะดังกล่าวจะต้องสามารถล็อกได้ หรือควบคุมไม่ให้เข้าถึงโดยไม่ได้รับอนุญาต

(2) การจัดส่งไปยังผู้ให้บริการภายนอก

ต้องดำเนินการผ่าน ผู้ให้บริการที่มีการประเมินความเสี่ยงแล้ว และมีข้อตกลงในการประมวลผลข้อมูล (Data Processing Agreement: DPA) และข้อตกลงรักษาความลับ (Non-Disclosure Agreement: NDA)

ผู้ให้บริการต้องมีนโยบายหรือมาตรการด้านความมั่นคงปลอดภัย เช่น การใช้รถขนส่งที่ล็อกได้ การกำกับดูแลระหว่างขนส่ง

(3) การทำลายอย่างปลอดภัยโดยผู้รับจ้างภายนอก

- ต้องทำลายข้อมูลโดยวิธีการที่ไม่สามารถกู้คืนหรือระบุเจ้าของข้อมูลได้อีก เช่น การย่อยละเอียด (shredding แบบละเอียดระดับ DIN 66399 P-4 หรือสูงกว่า)
- ภายหลังการทำลาย ต้องได้รับใบรับรองการทำลาย (Certificate of Destruction)

3. เอกสารและหลักฐานที่ต้องจัดเก็บ

- สำเนาสัญญาจ้าง/ข้อตกลงการประมวลผลข้อมูล (DPA)
- บันทึกการส่งมอบเอกสารเพื่อทำลาย
- บันทึกการตรวจสอบสถานที่และกระบวนการของผู้ให้บริการ
- ใบรับรองการทำลาย (Certificate of Destruction)
- รายงานเหตุการณ์ (กรณีมีเหตุผิดปกติระหว่างขนส่ง)

4. การเชื่อมโยงกับ ISO/IEC 27001 และ ISO/IEC 27701

มาตรฐาน	หมายเลขข้อ	คำอธิบายการเชื่อมโยง
ISO/IEC 27001	A.8.3.2	การกำจัดสื่อข้อมูลอย่างปลอดภัย
ISO/IEC 27001	A.13.2.1	การจัดการกับข้อมูลที่ส่งผ่านบุคคลภายนอก
ISO/IEC 27701	7.4.6	การว่าจ้างผู้ให้บริการภายนอกเพื่อการประมวลผลข้อมูลส่วนบุคคล

ISO/IEC 27701	7.5.7	การลบหรือทำลายข้อมูลเมื่อหมดความจำเป็น

9.5.4 มีการจัดทำสัญญากับผู้ให้บริการภายนอกเพื่อลบหรือทำลายข้อมูลส่วนบุคคล ผู้ให้บริการได้มีการแสดงถึงมาตรฐานที่ใช้ในการลบหรือทำลายข้อมูล หรือมีใบรับรองเพื่อแสดงถึงมาตรฐานการลบหรือทำลาย

สิ่งที่ต้องทำ: มีการจัดทำสัญญากับผู้ให้บริการภายนอกเพื่อลบหรือทำลายข้อมูลส่วนบุคคล โดยผู้ให้บริการได้มีการแสดงถึงมาตรฐานที่ใช้ในการลบหรือทำลายข้อมูล หรือมีใบรับรองเพื่อแสดงถึงมาตรฐานการลบหรือทำลาย

หลักฐาน: นโยบายการลบข้อมูลส่วนบุคคลที่เป็นกระดาษ
นโยบายการลบข้อมูลส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์
ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
บันทึกข้อตกลงรักษาความลับ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37, 40 วรรคสาม

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การจัดทำสัญญากับผู้ให้บริการภายนอกเพื่อลบหรือทำลายข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อให้การว่าจ้างบุคคลภายนอก (third-party vendor) เพื่อลบหรือทำลายข้อมูลส่วนบุคคลเป็นไปตามกฎหมายและมาตรฐานความมั่นคงปลอดภัย โดยเฉพาะในกรณีที่องค์กรไม่มีขีดความสามารถหรือเทคโนโลยีภายในที่เพียงพอสำหรับการลบ/ทำลายข้อมูลอย่างปลอดภัยและตรวจสอบได้

2. แนวทางปฏิบัติ

(1) การเลือกผู้ให้บริการที่มีคุณสมบัติ

ผู้ให้บริการต้องมี ใบรับรองมาตรฐาน ที่เกี่ยวข้องกับการลบหรือทำลายข้อมูล เช่น

- ISO/IEC 27001 หรือ ISO/IEC 27040 (การรักษาความมั่นคงของข้อมูลในระบบ IT)
- ใบรับรอง NAID (National Association for Information Destruction)
- มาตรฐาน DIN 66399 สำหรับการทำลายเอกสาร

(2) การจัดทำข้อตกลงและสัญญา

ต้องมีการทำ ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)

ต้องมี บันทึกข้อตกลงรักษาความลับ (Non-Disclosure Agreement: NDA)

- ข้อตกลงต้องระบุอย่างชัดเจนถึง
- ชนิดของข้อมูลที่ถูกส่งให้ลบหรือทำลาย
- วิธีการลบ/ทำลายที่ใช้
- มาตรฐานหรือแนวปฏิบัติที่ผู้รับจ้างอ้างอิง
- การรับรองว่าไม่เก็บสำเนาข้อมูลใดไว้
- การออกใบรับรองการลบ/ทำลาย (Certificate of Data Destruction)

(3) การควบคุมและติดตามผล

- องค์กรต้องเก็บบันทึกการลบ/ทำลายทุกครั้ง

- มีสิทธิในการตรวจสอบ (audit) กระบวนการของผู้รับจ้าง
- ต้องมีช่องทางรายงานเหตุผิดปกติ (Data Incident)

3. ตัวอย่างประกอบ

ตัวอย่างมาตรฐาน/ใบรับรองจากผู้ให้บริการ

- ใบรับรอง ISO/IEC 27001:2022 – แสดงระบบการบริหารความมั่นคงปลอดภัยสารสนเทศ
- ใบรับรอง NAID AAA Certification – รับรองการทำลายข้อมูลตามมาตรฐานระดับสากล
- รายงานผลการ audit จากบริษัทอิสระว่าได้ดำเนินการทำลายข้อมูลตามมาตรฐาน DIN 66399 ระดับ P-4

4. แบบฟอร์มที่เกี่ยวข้อง

แบบฟอร์มบันทึกการทำสัญญากับผู้ให้บริการลบ/ทำลายข้อมูล

ชื่อฟอร์ม: แบบฟอร์มบันทึกการว่าจ้างและตรวจสอบคุณสมบัติผู้ให้บริการลบ/ทำลายข้อมูลส่วนบุคคล

ลำดับ	วันที่ทำสัญญา	ชื่อผู้ให้บริการ	มาตรฐาน/ใบรับรองที่อ้างอิง	ประเภทข้อมูล	DPA แนบ	NDA แนบ	ใบรับรอง ลบ/ ทำลาย	หมายเหตุ
1	12/04/2567	บริษัท ซี เคียวริตี้ พลัส จำกัด	ISO/IEC 27001, DIN 66399	เอกสาร HR / ฐานข้อมูล เก่า	✓	✓	รอส่ง ภายใน 7 วัน	Audit ปีละ 1 ครั้ง

5. หลักฐานประกอบ

- นโยบายการลบข้อมูลส่วนบุคคล (ทั้งในรูปแบบกระดาษและอิเล็กทรอนิกส์)
- ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)
- บันทึกข้อตกลงการรักษาความลับ (NDA)
- ใบรับรองมาตรฐานหรือรายงาน audit ล่าสุดของผู้ให้บริการ
- ใบรับรองการทำลายข้อมูล (Certificate of Data Destruction)

6. ข้อกำหนดทางกฎหมาย

กฎหมาย	รายละเอียดข้อกำหนด
มาตรา 37	ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการที่เหมาะสมในการลบหรือทำลายข้อมูล
มาตรา 40 วรรคสาม	หากมอบหมายให้ผู้อื่นประมวลผล ต้องมีข้อตกลงอย่างชัดเจน และต้องควบคุมให้ดำเนินการอย่างถูกต้องตามกฎหมาย

7. โทษหากไม่ปฏิบัติตาม

หากไม่จัดทำสัญญา หรือไม่เลือกผู้ให้บริการที่มีมาตรฐาน อาจถือเป็นการละเลยต่อหน้าที่ของผู้ควบคุมข้อมูล

ตามมาตรา 37 หากฝ่าฝืน อาจถูกปรับทางปกครอง ไม่เกิน 3 ล้านบาท

8. การเชื่อมโยงกับมาตรฐานสากล

มาตรฐาน	ข้อที่เกี่ยวข้อง	เนื้อหาที่เชื่อมโยง
ISO/IEC 27701	A.8.3.2	การลบหรือทำลายสื่อข้อมูลอย่างมั่นคงปลอดภัย
ISO/IEC 27701	7.2.6	การเลือกผู้ประมวลผลข้อมูลภายนอก (Processor) อย่างรัดกุม
ISO/IEC 27701	7.5.7	การควบคุมและจัดทำหลักฐานการลบ/ทำลายข้อมูล

9.5.5 มีการบันทึกไว้เป็นข้อมูลสำหรับอุปกรณ์หรือขยะที่มีข้อมูลความลับทั้งหมดที่ได้มีการส่งออกไปเพื่อกำจัดหรือทำลาย

สิ่งที่ต้องทำ: มีการบันทึกไว้เป็นข้อมูลสำหรับอุปกรณ์หรือขยะที่มีข้อมูลความลับทั้งหมดที่ได้มีการส่งออกไปเพื่อกำจัดหรือทำลาย และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการลบ กำจัด หรือทำลายข้อมูลส่วนบุคคลที่เป็นกระดาษ
นโยบายการลบ กำจัด หรือทำลายข้อมูลส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์
ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การบันทึกข้อมูลการส่งออกอุปกรณ์หรือขยะที่มีข้อมูลความลับเพื่อนำไปกำจัดหรือทำลาย

1. วัตถุประสงค์

เพื่อให้องค์กรสามารถ ติดตาม ตรวจสอบ และพิสูจน์ย้อนหลัง ได้ถึงการจัดการกับอุปกรณ์หรือสื่อที่มีข้อมูลส่วนบุคคลหรือข้อมูลลับที่ถูกนำไปกำจัดหรือลบ ทำลายอย่างถูกวิธี โดยไม่มีข้อมูลหลุดรอดหรือตกอยู่ในความครอบครองของบุคคลภายนอก

2. แนวทางปฏิบัติ

(1) การจัดทำ ทะเบียนการส่งออกอุปกรณ์/สื่อข้อมูลเพื่อนำไปกำจัด

- จัดทำทะเบียนประจำ หรือระบบบันทึกข้อมูลอิเล็กทรอนิกส์ที่บันทึกข้อมูลดังต่อไปนี้:
- ประเภทของอุปกรณ์/สื่อ (เช่น ฮาร์ดดิสก์, USB, เครื่องพิมพ์, กระดาษสำเนา)
- หมายเลขอุปกรณ์/Serial No. (ถ้ามี)

- รายละเอียดข้อมูลที่มีอยู่ในอุปกรณ์ (ข้อมูลส่วนบุคคล, ข้อมูลสุขภาพ, ข้อมูลทางบัญชี ฯลฯ)
- วิธีการกำจัด (ลบ/ทำลาย/รีไซเคิล)
- ชื่อบริษัท/หน่วยงานภายนอกที่รับกำจัด
- วันที่ส่งมอบ
- ผู้อนุมัติ และผู้ดำเนินการ

(2) การควบคุมการเข้าถึงอุปกรณ์ก่อนกำจัด

- จัดเก็บอุปกรณ์ที่รอการทำลายไว้ในพื้นที่ปลอดภัย (secure zone)
- จำกัดผู้เข้าถึง
- มีการล้างข้อมูลก่อน (data sanitization) ตามมาตรฐาน เช่น DoD 5220.22-M, NIST SP 800-88

(3) การจัดเก็บเอกสารหลักฐาน

- เอกสารการส่งมอบ (Delivery Form หรือ Work Order)
- ใบรับรองการลบ/ทำลายข้อมูล (Certificate of Destruction)
- ภาพถ่ายการดำเนินการ (ถ้ามี)
- สำเนาสัญญาหรือ MOU กับผู้ให้บริการภายนอก

3. แบบฟอร์มบันทึกการส่งออกอุปกรณ์เพื่อนำไปทำลาย

ชื่อฟอร์ม: ทะเบียนการส่งออกอุปกรณ์/ขยะที่มีข้อมูลส่วนบุคคล

ลำดับ	วันที่ส่งมอบ	ประเภทอุปกรณ์	หมายเลข	ข้อมูลที่เกี่ยวข้อง	วิธีการทำลาย	บริษัทที่รับทำลาย	ผู้อนุมัติ	เอกสารแนบ
1	20/06/2568	ฮาร์ดดิสก์ (HDD)	SN-DX10432	ฐานข้อมูลพนักงาน	ทำลายทางกายภาพ (shredding)	บจก. เอ็มเอสดาต้าดีสทรอย	น.ส. วาริสาระ	ใบรับรองการลบข้อมูล

4. ตัวอย่างเอกสารแนบที่ควรมี

- นโยบายการลบ กำจัด หรือทำลายข้อมูลส่วนบุคคล (ทั้งแบบกระดาษและอิเล็กทรอนิกส์)
- ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล กับผู้ให้บริการทำลายข้อมูล
- ใบรับรองการทำลาย (Certificate of Destruction)
- บันทึกการล้างข้อมูล (Data Sanitization Log)
- ภาพถ่ายหรือวิดีโอการทำลาย (ถ้าดำเนินการภายในองค์กร)

5. ข้อกำหนดทางกฎหมาย

กฎหมาย/ข้อบังคับ	ข้อความที่เกี่ยวข้อง
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37	ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการป้องกันไม่ให้ข้อมูลส่วนบุคคลรั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงในขั้นตอนของการกำจัดหรือทำลายข้อมูล
ประกาศคณะกรรมการฯ ปี 2565 ข้อ 4 (2)	ต้องมีมาตรการในการจัดเก็บ การใช้งาน และการส่งต่อข้อมูลอย่างปลอดภัย รวมถึงขั้นตอนทำลาย
ประกาศคณะกรรมการฯ ปี 2565 ข้อ 4 (4)	ต้องมีการบันทึกหลักฐานการลบหรือทำลายข้อมูลที่สามารถตรวจสอบย้อนหลังได้

6. โทษหากไม่ปฏิบัติตาม

- ไม่สามารถแสดงหลักฐานว่าได้ดำเนินการลบ/ทำลายข้อมูลตามกฎหมาย อาจเสี่ยงต่อ
- การรั่วไหลของข้อมูลส่วนบุคคล
- ความผิดตามมาตรา 37
- โทษทางปกครอง: ปรับไม่เกิน 3 ล้านบาท

7. การเชื่อมโยงกับมาตรฐาน ISO

มาตรฐาน	ข้อที่เกี่ยวข้อง	แนวปฏิบัติที่เชื่อมโยง
ISO/IEC 27701	A.8.3.2	การลบ/ทำลายข้อมูลจากสื่อจัดเก็บที่ไม่ใช้แล้ว
ISO/IEC 27701	7.4.7	การควบคุมการทำลายข้อมูลส่วนบุคคลหลังจากสิ้นสุดวัตถุประสงค์
NIST SP 800-88	บทที่ 2-3	แนวทางการลบข้อมูลจากสื่อเก็บข้อมูลทั้งแบบแม่เหล็กและอิเล็กทรอนิกส์

9.6 บัญชีทรัพย์สินสารสนเทศ (Information Asset Register)

องค์กรมีการจัดทำบัญชีทรัพย์สินสารสนเทศ ระบบและแอปพลิเคชันที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลภายในองค์กร

9.6.1 มีการจัดทำบัญชีทรัพย์สินสารสนเทศ โดยบัญชีดังกล่าวได้รวมถึงเจ้าของทรัพย์สิน สถานที่จัดเก็บทรัพย์สิน ระยะเวลาการจัดเก็บ และมาตรการความมั่นคงปลอดภัย (เพื่อป้องกันทรัพย์สิน)

- สิ่งที่ต้องทำ: มีการจัดทำบัญชีทรัพย์สินสารสนเทศ โดยบัญชีดังกล่าวได้รวมถึงเจ้าของทรัพย์สิน สถานที่จัดเก็บทรัพย์สิน ระยะเวลาการจัดเก็บ และมาตรการความมั่นคงปลอดภัย
- หลักฐาน: นโยบายการจัดทำบัญชีทรัพย์สินสารสนเทศ
บัญชีทรัพย์สินสารสนเทศ
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)
- โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

บัญชีทรัพย์สินสารสนเทศ (Information Asset Register)

9.6.1 การจัดทำบัญชีทรัพย์สินสารสนเทศ

1. วัตถุประสงค์

เพื่อให้องค์กรมีการจัดเก็บข้อมูลทรัพย์สินสารสนเทศ (Information Assets) ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลอย่างครบถ้วนและมีระบบ สามารถบริหารจัดการความเสี่ยง ป้องกันความเสียหายหรือการรั่วไหลของข้อมูล และสอดคล้องกับข้อกำหนดของกฎหมาย PDPA

2. แนวทางปฏิบัติ

(1) การจัดทำบัญชีทรัพย์สินสารสนเทศ

- จัดทำบัญชีทรัพย์สินสารสนเทศอย่างเป็นระบบ โดยมีข้อมูลหลักอย่างน้อยดังนี้:
- ชื่อทรัพย์สินสารสนเทศ (เช่น ระบบฐานข้อมูลลูกค้า, แอปพลิเคชัน CRM, เซิร์ฟเวอร์เก็บข้อมูล)
- ประเภททรัพย์สิน (ฮาร์ดแวร์, ซอฟต์แวร์, ข้อมูล, บุคลากร)
- เจ้าของทรัพย์สิน (Information Asset Owner) ผู้รับผิดชอบดูแลรักษา
- สถานที่จัดเก็บ (เช่น ห้องเซิร์ฟเวอร์, ศูนย์ข้อมูล, คลาวด์)
- ระยะเวลาการจัดเก็บ (Retention Period) ตามนโยบายองค์กรและกฎหมาย
- มาตรการความมั่นคงปลอดภัยที่นำมาใช้ (เช่น การเข้ารหัสข้อมูล, การสำรองข้อมูล, การควบคุมการเข้าถึง)
- สถานะของทรัพย์สิน (ใช้งาน/ไม่ใช้งาน/รอทำลาย)

(2) การกำหนดเจ้าของทรัพย์สิน

- กำหนดบุคคลหรือหน่วยงานที่รับผิดชอบในการดูแลรักษาทรัพย์สินสารสนเทศแต่ละรายการอย่างชัดเจน
- เจ้าของทรัพย์สินต้องประเมินความเสี่ยงและจัดทำมาตรการรักษาความมั่นคงปลอดภัย รวมถึงดูแลการใช้งานและอนุมัติการเข้าถึงข้อมูล

(3) การอัปเดตบัญชีทรัพย์สินสารสนเทศ

- บัญชีต้องได้รับการทบทวนและอัปเดตอย่างสม่ำเสมอ (อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงระบบ)
- มีการตรวจสอบและตรวจยืนยันข้อมูลความถูกต้องโดยเจ้าของทรัพย์สินสารสนเทศ

3. ตัวอย่างโครงสร้างบัญชีทรัพย์สินสารสนเทศ

หมายเลข	ชื่อทรัพย์สินสารสนเทศ	ประเภท	เจ้าของทรัพย์สิน	สถานที่จัดเก็บ	ระยะเวลาการจัดเก็บ	มาตรการความมั่นคงปลอดภัย	สถานะ

001	ระบบฐานข้อมูลลูกค้า CRM	ซอฟต์แวร์	นายสมชายใจดี	ศูนย์ข้อมูลหลัก	5 ปี	การเข้ารหัสข้อมูล, ระบบยืนยันตัวตนสองชั้น	ใช้งานอยู่
002	เซิร์ฟเวอร์จัดเก็บข้อมูลสำคัญ	ฮาร์ดแวร์	ฝ่ายไอที	ห้องเซิร์ฟเวอร์	ตลอดอายุการใช้งาน	การควบคุมการเข้าใช้งาน, สำรองข้อมูลรายวัน	ใช้งานอยู่
003	เอกสารประวัติพนักงาน	ข้อมูล	ฝ่ายบุคคล	ตู้เก็บเอกสารห้องบุคคล	10 ปี	การล็อกตู้, การเข้าถึงจำกัด	รอทำลาย

4. หลักฐานประกอบการจัดทำบัญชีทรัพย์สินสารสนเทศ

- นโยบายการจัดการบัญชีทรัพย์สินสารสนเทศ (Information Asset Management Policy)
- บัญชีทรัพย์สินสารสนเทศ (Information Asset Register) ฉบับล่าสุด
- รายงานการตรวจสอบและทบทวนบัญชีทรัพย์สินสารสนเทศ
- เอกสารแนวทางและมาตรการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ

5. ข้อกำหนดทางกฎหมายและข้อบังคับที่เกี่ยวข้อง

กฎหมาย/ประกาศ	ข้อความที่เกี่ยวข้อง
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37	กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล รวมถึงการบริหารจัดการทรัพย์สินสารสนเทศที่เกี่ยวข้อง
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ปี 2565 ข้อ (2), (4)	กำหนดมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลและให้มีการบันทึกและติดตามทรัพย์สินสารสนเทศอย่างมีประสิทธิภาพ

6. โทษทางปกครอง

ในกรณีที่มิปฏิบัติตามมาตรา 37 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 องค์กรอาจถูกปรับทางปกครองไม่เกิน 3 ล้านบาท

7. การเชื่อมโยงกับมาตรฐาน ISO

มาตรฐาน	ข้อที่เกี่ยวข้อง	แนวทางเชื่อมโยง

ISO/IEC 27001	A.8.1.1, A.8.1.2	จัดการและควบคุมทรัพย์สินสารสนเทศอย่างเป็นระบบ
ISO/IEC 27701	7.1.2	การบริหารจัดการทรัพย์สินส่วนบุคคลและการรักษาความปลอดภัย ของข้อมูลส่วนบุคคล

8. ตัวอย่างแบบฟอร์มบัญชีทรัพย์สินสารสนเทศ (Information Asset Register)

หมายเลข	ชื่อ ทรัพย์สิน สารสนเทศ	ประเภท	เจ้าของ ทรัพย์สิน	สถานที่ จัดเก็บ	ระยะเว ลาการ จัดเก็บ	มาตรการ รักษาความ มั่นคง ปลอดภัย	สถานะ	หมายเหตุ
001	ระบบ ฐานข้อมูล ลูกค้า (CRM system)	ซอฟต์แวร์	นาย สมชาย ใจดี (IT Manager)	ศูนย์ ข้อมูล หลัก อาคาร A ชั้น 3	5 ปี	เข้ารหัสข้อมูล (AES-256), ระบบยืนยัน ตัวตนสองชั้น (2FA), Firewall	ใช้ งาน อยู่	สำรอง ข้อมูล ราย วันที่ ศูนย์ ข้อมูล สำรอง
002	เซิร์ฟเวอร์ จัดเก็บ ข้อมูล สำคัญ	ฮาร์ดแวร์	ฝ่ายไอที	ห้อง เซิร์ฟเวอร์ อาคาร B ชั้น 1	ตลอด อายุการ ใช้งาน	ระบบควบคุม การเข้าถึงด้วย บัตรผ่าน, กล้องวงจรปิด, ระบบดับเพลิง อัตโนมัติ	ใช้ งาน อยู่	ตรวจสอบ ระบบ ความ ปลอดภัย ราย เดือน
003	เอกสาร ประวัติ พนักงาน	ข้อมูล เอกสาร	ฝ่าย บุคคล	ห้องเก็บ เอกสาร ฝ่าย บุคคล	10 ปี	ตู้ล็อกกุญแจ, จำกัดการเข้า ใช้งานเฉพาะ พนักงานฝ่าย บุคคล	รอ ทำลาย ย	จะ ทำลาย ตาม นโยบาย หลัง ครบ 10 ปี

004	แอปพลิเคชันจัดการเวลางานพนักงาน	ซอฟต์แวร์	ฝ่ายทรัพยากรบุคคล	คลาวด์ส่วนตัว AWS Region Asia Southeast	3 ปี	ระบบยืนยันตัวตน Multi-Factor Authentication, การเข้ารหัสข้อมูลระหว่างส่ง	ใช้งานอยู่	มีการทดสอบเจาะระบบ ทุก 6 เดือน
005	คอมพิวเตอร์แล็ปท็อปของพนักงาน	ฮาร์ดแวร์	ผู้ใช้งานแต่ละบุคคล	สำนักงาน ส่วนกลาง	4 ปี	การล็อกด้วยรหัสผ่าน, ระบบล็อกเครื่องอัตโนมัติเมื่อไม่ใช้งาน	ใช้งานอยู่	บันทึกประวัติการซ่อมบำรุง

หมายเหตุ

- ประเภททรัพย์สินสารสนเทศ เช่น ซอฟต์แวร์, ฮาร์ดแวร์, ข้อมูลเอกสาร
- เจ้าของทรัพย์สิน คือผู้รับผิดชอบในการดูแลและรักษาความมั่นคงปลอดภัยของทรัพย์สินนั้น
- สถานที่จัดเก็บ ต้องระบุชัดเจนเพื่อประเมินความเสี่ยงและควบคุมการเข้าถึง
- ระยะเวลาการจัดเก็บ กำหนดตามนโยบายองค์กรและข้อกำหนดที่เกี่ยวข้อง
- มาตรการรักษาความมั่นคงปลอดภัย ควรระบุรายละเอียดเช่น ระบบเข้ารหัส, การควบคุมการเข้าถึง, ระบบตรวจสอบความมั่นคงปลอดภัย เป็นต้น

สถานะ เช่น ใช้งานอยู่, รอทำลาย, ทำลายแล้ว

9.6.2 มีการทบทวนบัญชีทรัพย์สินสารสนเทศเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องและเป็นปัจจุบัน

สิ่งที่ต้องทำ: มีการทบทวนบัญชีทรัพย์สินสารสนเทศเป็นระยะ ๆ เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องและเป็นปัจจุบัน

หลักฐาน: นโยบายการทบทวนบัญชีทรัพย์สินสารสนเทศ

รายงานผลการตรวจสอบบัญชีทรัพย์สินสารสนเทศ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4), ข้อ 5

โทษทางปกครอง: ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การทบทวนบัญชีทรัพย์สินสารสนเทศเป็นระยะ ๆ

สิ่งที่ต้องทำ

องค์กรต้องดำเนินการทบทวนบัญชีทรัพย์สินสารสนเทศอย่างสม่ำเสมอเป็นระยะ ๆ ตามกำหนดที่เหมาะสม (อย่างน้อยปีละ 1 ครั้ง หรือบ่อยกว่านั้นตามความเหมาะสมขององค์กร) เพื่อให้มั่นใจได้ว่าข้อมูลในบัญชีมีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน โดยการทบทวนควรครอบคลุมการตรวจสอบข้อมูลเจ้าของทรัพย์สิน สถานที่จัดเก็บ ระยะเวลาการจัดเก็บ และมาตรการรักษาความมั่นคงปลอดภัยที่ใช้จริงในปัจจุบัน

นอกจากนี้ หากมีการเปลี่ยนแปลงทรัพย์สินสารสนเทศ เช่น มีการเพิ่ม ลด หรือเปลี่ยนแปลงระบบ แอปพลิเคชัน หรืออุปกรณ์ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ควรมีการอัปเดตบัญชีให้สอดคล้องทันที

หลักฐานประกอบการปฏิบัติ

- นโยบายการทบทวนบัญชีทรัพย์สินสารสนเทศ
- รายงานผลการตรวจสอบและทบทวนบัญชีทรัพย์สินสารสนเทศ
- รายงานการแก้ไขปรับปรุงบัญชีทรัพย์สินสารสนเทศ

สภาพบังคับทางกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2), (4) และ ข้อ 5

โทษทางปกครอง

กรณีไม่ปฏิบัติตามมาตรา 37 อาจถูกลงโทษปรับทางปกครองสูงสุดไม่เกิน 3 ล้านบาท

ตัวอย่างกระบวนการทบทวนบัญชีทรัพย์สินสารสนเทศ

ขั้นตอน	รายละเอียด	ผู้รับผิดชอบ	เอกสารประกอบ
1. กำหนดแผนการทบทวน	กำหนดช่วงเวลาการทบทวนบัญชีทรัพย์สินสารสนเทศประจำปี พร้อม	ฝ่าย IT Security / Data Protection Office (DPO)	แผนงานทบทวนบัญชีทรัพย์สินสารสนเทศประจำปี

	กำหนดความถี่การทบทวนเพิ่มเติมตามความจำเป็น		
2. รวบรวมข้อมูลปัจจุบัน	รวบรวมข้อมูลบัญชีทรัพย์สินสารสนเทศฉบับล่าสุด และข้อมูลการเปลี่ยนแปลงที่เกิดขึ้นในช่วงเวลาที่ผ่านมา	ฝ่าย IT / เจ้าของทรัพย์สิน	บัญชีทรัพย์สินสารสนเทศปัจจุบัน, รายงานเปลี่ยนแปลงทรัพย์สิน
3. ตรวจสอบความถูกต้อง	ตรวจสอบความครบถ้วนและความถูกต้องของข้อมูลในบัญชี เช่น ตรวจสอบเจ้าของทรัพย์สิน สถานที่จัดเก็บ มาตรการรักษาความมั่นคงปลอดภัย	ฝ่าย IT Security / DPO	รายงานผลการตรวจสอบบัญชีทรัพย์สินสารสนเทศ
4. แก้ไขและปรับปรุง	แก้ไขข้อมูลในบัญชีให้เป็นปัจจุบันตามผลการตรวจสอบ รวมถึงบันทึกการเปลี่ยนแปลง	ฝ่าย IT / เจ้าของทรัพย์สิน	บัญชีทรัพย์สินสารสนเทศฉบับปรับปรุง, บันทึกการเปลี่ยนแปลง
5. รายงานผลการทบทวน	จัดทำรายงานสรุปผลการทบทวนบัญชีทรัพย์สินสารสนเทศ พร้อมข้อเสนอแนะ (ถ้ามี) เพื่อเสนอผู้บริหารอนุมัติ	ฝ่าย IT Security / DPO	

รายงานผลการทบทวนบัญชีทรัพย์สินสารสนเทศ

ประจำปี พ.ศ. 2568

1. วัตถุประสงค์

เพื่อให้มั่นใจว่าบัญชีทรัพย์สินสารสนเทศขององค์กรมีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

2. ผลการทบทวน

- ตรวจสอบบัญชีทรัพย์สินสารสนเทศพบว่า ข้อมูลเจ้าของทรัพย์สินและสถานที่จัดเก็บครบถ้วน
- พบว่ามีการเพิ่มระบบฐานข้อมูลลูกค้าใหม่ 1 ระบบ จึงได้บันทึกเพิ่มในบัญชีแล้ว
- มีการเปลี่ยนแปลงมาตรการความมั่นคงปลอดภัยของเซิร์ฟเวอร์หลัก (เพิ่มระบบ Firewall ใหม่)
- มีการลบอุปกรณ์เก่าที่เลิกใช้งานออกจากบัญชีเรียบร้อยแล้ว

3. ข้อเสนอแนะ

- ควรเพิ่มความถี่การทบทวนบัญชีเป็นทุก 6 เดือน เนื่องจากการเปลี่ยนแปลงระบบสารสนเทศบ่อย
- ส่งเสริมให้เจ้าของทรัพย์สินสารสนเทศแจ้งการเปลี่ยนแปลงข้อมูลทุกครั้งทันที

4. สรุป

บัญชีทรัพย์สินสารสนเทศอยู่ในสถานะที่เหมาะสมและพร้อมใช้งานในการบริหารความเสี่ยงด้านข้อมูลส่วนบุคคล

ลงชื่อ

.....

(นายสมชาย ใจดี)

Data Protection Officer

วันที่ 1 มิถุนายน 2568

9.6.3 มีการประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในรายการบัญชีทรัพย์สินสารสนเทศ มีการดำเนินการตรวจสอบทางกายภาพ เพื่อให้มั่นใจว่าทรัพย์สินในบัญชีมีความถูกต้องและครบถ้วน

สิ่งที่ต้องทำ: มีการประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในรายการบัญชีทรัพย์สินสารสนเทศ มีการดำเนินการตรวจสอบทางกายภาพ เพื่อให้มั่นใจว่าทรัพย์สินในบัญชีมีความถูกต้องและครบถ้วน

หลักฐาน: การประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในบัญชีทรัพย์สินสารสนเทศ
รายงานการประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในบัญชีทรัพย์สินสารสนเทศ
รายงานความเห็นประกอบการพิจารณารายงานการประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในบัญชีทรัพย์สินสารสนเทศ
หนังสือการพิจารณาการประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในบัญชีทรัพย์สินสารสนเทศ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (4)

โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การประเมินความเสี่ยงและการตรวจสอบทางกายภาพบัญชีทรัพย์สินสารสนเทศ

สิ่งที่ต้องทำ

องค์กรต้องดำเนินการประเมินความเสี่ยงอย่างเป็นระบบสำหรับทรัพย์สินสารสนเทศที่อยู่ในบัญชีทรัพย์สินสารสนเทศ (Information Asset Register) โดยพิจารณาความเสี่ยงที่อาจเกิดขึ้น เช่น ความเสียหายจากภัยคุกคามทางกายภาพ ความลับรั่วไหล ความผิดพลาดของระบบ หรือภัยคุกคามทางไซเบอร์

นอกจากนี้ ต้องมีการตรวจสอบทางกายภาพอย่างสม่ำเสมอ เช่น การตรวจนับอุปกรณ์ การตรวจสอบสถานที่จัดเก็บเพื่อยืนยันว่าทรัพย์สินดังกล่าวมีอยู่จริงและอยู่ในสภาพที่ปลอดภัย เพื่อป้องกันการสูญหายหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

หลักฐานประกอบการปฏิบัติ

- นโยบายการประเมินความเสี่ยงสำหรับทรัพย์สินสารสนเทศ
- รายงานการประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในบัญชีทรัพย์สินสารสนเทศ
- รายงานความเห็นประกอบการพิจารณาผลการประเมินความเสี่ยง
- หนังสือสรุปผลการพิจารณาและอนุมัติรายงานการประเมินความเสี่ยง

สภาพบังคับทางกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2), (3), (4)

โทษทางปกครอง

หากไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองสูงสุดไม่เกิน 3 ล้านบาท

ขั้นตอน	รายละเอียด	ผู้รับผิดชอบ	เอกสารประกอบ
1. กำหนดกรอบและวิธีการประเมินความเสี่ยง	กำหนดแนวทางการประเมินความเสี่ยงโดยใช้เกณฑ์ความรุนแรงและโอกาสเกิดความเสี่ยง	ฝ่ายความมั่นคงปลอดภัยสารสนเทศ (IT Security) / DPO	นโยบายประเมินความเสี่ยง
2. รวบรวมข้อมูลทรัพย์สิน	ใช้บัญชีทรัพย์สินสารสนเทศที่จัดทำไว้ เพื่อกำหนดขอบเขตการประเมิน	ฝ่าย IT / เจ้าของทรัพย์สิน	บัญชีทรัพย์สินสารสนเทศ
3. ประเมินความเสี่ยง	วิเคราะห์ความเสี่ยงที่เกี่ยวข้องกับแต่ละทรัพย์สิน เช่น การถูกโจมตี, สูญหาย, เสียหาย	ฝ่าย IT Security / DPO	รายงานการประเมินความเสี่ยง

4. ตรวจสอบทาง กายภาพ	ดำเนินการตรวจนับและ ตรวจสอบสถานที่จัดเก็บ เช่น การตรวจนับอุปกรณ์ คอมพิวเตอร์ เซิร์ฟเวอร์ ฯลฯ	ฝ่าย IT / ฝ่ายบริหาร สถานที่	รายงานตรวจสอบทาง กายภาพ
5. รายงานและ พิจารณา	จัดทำรายงานสรุปผลการ ประเมินและตรวจสอบ พร้อม ข้อเสนอแนะส่งผู้บริหารพิจารณา	ฝ่าย IT Se urit / DPO	รายงานความเห็น ประกอบการพิจารณา , หนังสืออนุมัติ
6. ดำเนิน มาตรการลด ความเสี่ยง	ปรับปรุงมาตรการรักษาความ มั่นคงปลอดภัยตามผลการ ประเมิน	ฝ่าย IT Security / ฝ่ายบริหารความเสี่ยง	บันทึกการดำเนินการ

รายงานการประเมินความเสี่ยงสำหรับทรัพย์สินสารสนเทศ
ประจำปี พ.ศ. 2568

1. วัตถุประสงค์

เพื่อประเมินความเสี่ยงที่อาจเกิดขึ้นต่อทรัพย์สินสารสนเทศขององค์กร และตรวจสอบความถูกต้องของทรัพย์สินในบัญชีสารสนเทศ

2. วิธีการประเมิน

ใช้เกณฑ์การประเมินความรุนแรง (สูง กลาง ต่ำ) และโอกาสเกิดความเสี่ยง (บ่อย ปานกลาง น้อย) ในการวิเคราะห์

3. ผลการประเมิน

- พบว่าทรัพย์สินส่วนใหญ่มีความเสี่ยงในระดับต่ำถึงกลาง
- พบความเสี่ยงสูงในส่วนของเซิร์ฟเวอร์หลัก เนื่องจากตั้งอยู่ในห้องที่ไม่ได้ควบคุมการเข้าออกอย่างเข้มงวด
- ทรัพย์สินทั้งหมดได้รับการตรวจสอบทางกายภาพครบถ้วน ไม่มีทรัพย์สินสูญหาย

4. ข้อเสนอแนะ

- เพิ่มระบบควบคุมการเข้าออกห้องเซิร์ฟเวอร์ เช่น ติดตั้งระบบล็อกอิเล็กทรอนิกส์
- กำหนดตารางตรวจสอบทางกายภาพเพิ่มเป็นทุก 6 เดือน
- ให้เจ้าของทรัพย์สินรายงานการเปลี่ยนแปลงทรัพย์สินทุกครั้งที่เกิดขึ้น

5. สรุป

ทรัพย์สินสารสนเทศมีความถูกต้องครบถ้วนตามบัญชี และได้ดำเนินการประเมินความเสี่ยงเป็นประจำ เพื่อป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ลงชื่อ

.....

(นายสมชาย ใจดี)

Data Protection Officer

วันที่ 1 มิถุนายน 2568

9.7 ข้อกำหนดเกี่ยวกับการใช้ซอฟต์แวร์อย่างเหมาะสม (Rules for acceptable software use)
องค์กรมีการประเมิน บันทึกลง และนำข้อกำหนดเกี่ยวกับการใช้ซอฟต์แวร์อย่างเหมาะสมหรือเงื่อนไขการ
อนุญาตมาใช้บังคับกับระบบและแอปพลิเคชันที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล

9.7.1 ข้อกำหนดมีข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์อย่างเหมาะสม

สิ่งที่ต้องทำ: ข้อกำหนดมีข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์ และเหมาะสมกับผู้ใช้

หลักฐาน: มาตรการทางเทคนิคที่เพียงพอต่อการรับรองความปลอดภัยและปกป้องข้อมูลที่ประมวลผล
นโยบายความปลอดภัยเพื่อจำกัดในการคัดลอกข้อมูลโดยอุปกรณ์
ข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์

รายงานผลการตรวจสอบข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (5)

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ข้อกำหนดเกี่ยวกับการใช้ซอฟต์แวร์อย่างเหมาะสม (Rules for acceptable software use)

9.7.1 ข้อกำหนดมีข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์อย่างเหมาะสม

สิ่งที่ต้องทำ

องค์กรต้องกำหนดข้อกำหนดและข้อปฏิบัติที่ชัดเจนสำหรับการใช้ซอฟต์แวร์ในระบบและแอปพลิเคชันที่ใช้ประมวลผลข้อมูลส่วนบุคคล เพื่อให้การใช้งานซอฟต์แวร์เป็นไปอย่างเหมาะสม ปลอดภัย และสอดคล้องกับเงื่อนไขการอนุญาตของซอฟต์แวร์นั้น ๆ

ข้อกำหนดดังกล่าวควรครอบคลุมถึงการป้องกันการใช้ซอฟต์แวร์ผิดกฎหมาย การจำกัดการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต การควบคุมการคัดลอกข้อมูลโดยอุปกรณ์ภายนอก เช่น USB drive หรือ External HDD และการรักษาความมั่นคงปลอดภัยของข้อมูลที่ถูกระบุประมวลผล

หลักฐานประกอบการปฏิบัติ

- มาตรการทางเทคนิคที่เพียงพอเพื่อรับรองความปลอดภัยและปกป้องข้อมูลที่มีประมวลผล เช่น การใช้ระบบควบคุมการเข้าถึง การตรวจสอบการติดตั้งซอฟต์แวร์
- นโยบายความปลอดภัยที่จำกัดการคัดลอกหรือถ่ายโอนข้อมูลโดยอุปกรณ์พกพาหรืออุปกรณ์เชื่อมต่อภายนอก
- ข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์ที่สื่อสารถึงผู้ใช้งานในองค์กร
- รายงานผลการตรวจสอบข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์ เช่น รายงานตรวจสอบการใช้งานซอฟต์แวร์ผิดกฎหมาย หรือซอฟต์แวร์ที่ไม่ได้รับอนุญาต

สภาพบังคับทางกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2), (3), (5)

โทษทางปกครอง

หากไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองสูงสุดไม่เกิน 3 ล้านบาท

ตัวอย่างข้อกำหนดสำหรับการใช้ซอฟต์แวร์อย่างเหมาะสม

- **การติดตั้งซอฟต์แวร์**

ผู้ใช้งานต้องได้รับอนุญาตจากฝ่าย IT ก่อนติดตั้งซอฟต์แวร์ใด ๆ ในเครื่องคอมพิวเตอร์ที่ใช้ประมวลผลข้อมูลส่วนบุคคล

องค์กรจะจัดให้มีรายการซอฟต์แวร์ที่ได้รับอนุญาต (Approved Software List) เพื่อใช้ในงานเท่านั้น
- **การใช้ซอฟต์แวร์ลิขสิทธิ์**

ต้องใช้ซอฟต์แวร์ที่มีใบอนุญาตถูกต้องตามกฎหมายเท่านั้น ห้ามใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์

ฝ่าย IT จะทำการตรวจสอบและอัปเดตใบอนุญาตซอฟต์แวร์เป็นประจำ
- **การจำกัดการคัดลอกและถ่ายโอนข้อมูล**

ห้ามใช้ USB drive หรืออุปกรณ์จัดเก็บข้อมูลภายนอกในการคัดลอกข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

องค์กรจะใช้มาตรการทางเทคนิค เช่น การตั้งค่า Group Policy หรือ Software Restriction Policy เพื่อควบคุมการใช้อุปกรณ์เหล่านี้
- **การตรวจสอบการใช้งานซอฟต์แวร์**

มีการตรวจสอบและบันทึกการติดตั้งและใช้งานซอฟต์แวร์เพื่อป้องกันการติดตั้งซอฟต์แวร์ผิดกฎหมายหรือไม่เหมาะสม

รายงานการตรวจสอบจะถูกจัดทำและรายงานต่อผู้บริหารเป็นระยะ

รายงานผลการตรวจสอบข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์
ประจำปีงบประมาณที่ 2 ปี พ.ศ. 2568

1. วัตถุประสงค์

เพื่อประเมินการปฏิบัติตามข้อกำหนดการใช้ซอฟต์แวร์อย่างเหมาะสมและตรวจสอบการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต

2. ผลการตรวจสอบ

- พบว่าซอฟต์แวร์ที่ติดตั้งทั้งหมดเป็นซอฟต์แวร์ลิขสิทธิ์ที่ได้รับอนุญาต
- ไม่พบการใช้อุปกรณ์เก็บข้อมูลภายนอกที่ไม่ได้รับอนุญาตในการคัดลอกข้อมูลส่วนบุคคล
- มีการบังคับใช้นโยบายจำกัดการติดตั้งซอฟต์แวร์อย่างเคร่งครัด
- ระบบบันทึกการติดตั้งซอฟต์แวร์และการใช้งานทำงานได้ดี ไม่มีช่องโหว่ที่สำคัญ

3. ข้อเสนอแนะ

- ควรจัดฝึกอบรมเพิ่มเติมให้พนักงานเกี่ยวกับข้อกำหนดการใช้ซอฟต์แวร์
- ควรปรับปรุงนโยบายการใช้ซอฟต์แวร์ให้ครอบคลุมกรณีการใช้งานบนอุปกรณ์เคลื่อนที่ (Mobile Devices)

ลงชื่อ

.....

(นางสาวสาวิตรี สุขใจ)

เจ้าหน้าที่ฝ่าย IT Security

วันที่ 15 มิถุนายน 2568

9.7.2 ข้อปฏิบัติมีการกล่าวถึงหรือได้อธิบายถึงมาตรการหรือการจัดเตรียมด้านความมั่นคงปลอดภัย เพื่อป้องกันข้อมูลส่วนบุคคลที่อยู่ในระบบหรือแอปพลิเคชันนั้น

สิ่งที่ต้องทำ: มีข้อปฏิบัติที่มีการกล่าวถึงหรือได้อธิบายถึงมาตรการหรือการจัดเตรียมด้านความมั่นคงปลอดภัย เพื่อป้องกันข้อมูลส่วนบุคคลที่อยู่ในระบบหรือแอปพลิเคชันนั้น และขั้นตอนหรือมาตรการดังกล่าวได้รับการทบทวน หรือตรวจสอบโดยการตรวจสอบภายใน (Internal Audit) หรือการตรวจสอบจากภายนอก (External Audit)

หลักฐาน: นโยบายหรือข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (7)

โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

**ข้อปฏิบัติมีการกล่าวถึงหรือได้อธิบายถึงมาตรการหรือการจัดเตรียมด้านความมั่นคงปลอดภัย เพื่อ
ป้องกันข้อมูลส่วนบุคคลที่อยู่ในระบบหรือแอปพลิเคชันนั้น**

สิ่งที่ต้องทำ

องค์กรต้องมีข้อปฏิบัติหรือระเบียบข้อกำหนดที่อธิบายมาตรการความมั่นคงปลอดภัยที่ใช้ปกป้อง
ข้อมูลส่วนบุคคลในระบบหรือแอปพลิเคชันอย่างชัดเจน เช่น การใช้ระบบการเข้ารหัส (encryption) การ
ควบคุมการเข้าถึงด้วยรหัสผ่าน การจัดการสิทธิ์ผู้ใช้ (access control) หรือมาตรการรักษาความมั่นคง
ปลอดภัยอื่น ๆ ที่เหมาะสมกับความเสี่ยง

นอกจากนี้ ขั้นตอนหรือมาตรการเหล่านี้ต้องได้รับการทบทวน ตรวจสอบเป็นระยะผ่าน
กระบวนการตรวจสอบภายใน (Internal Audit) หรือการตรวจสอบจากผู้ตรวจสอบภายนอก (External
Audit) เพื่อให้มั่นใจว่ามาตรการเหล่านี้ยังมีประสิทธิภาพและสอดคล้องกับข้อกำหนดทางกฎหมาย

หลักฐานประกอบการปฏิบัติ

- นโยบายหรือข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์ที่ระบุมาตรการรักษาความมั่นคงปลอดภัยอย่าง
ชัดเจน
- รายงานผลการตรวจสอบภายใน (Internal Audit Report) หรือรายงานตรวจสอบจากภายนอก
(External Audit Report) ที่ครอบคลุมมาตรการความมั่นคงปลอดภัยของซอฟต์แวร์และระบบ
ประมวลผลข้อมูลส่วนบุคคล

สภาพบังคับทางกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้
ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2), (4), (7)

โทษทางปกครอง

หากไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองไม่เกิน 3 ล้านบาท

ตัวอย่างข้อปฏิบัติและมาตรการรักษาความมั่นคงปลอดภัยของซอฟต์แวร์

การควบคุมการเข้าถึงระบบ

- ระบบต้องรองรับการยืนยันตัวตนด้วยรหัสผ่านที่มีความซับซ้อนและมีการเปลี่ยนรหัสผ่านเป็นระยะ
- กำหนดสิทธิ์การเข้าถึงข้อมูลตามบทบาทหน้าที่ (Role-Based Access Control - RBAC)

การเข้ารหัสข้อมูล

- ข้อมูลส่วนบุคคลที่จัดเก็บในระบบหรือส่งผ่านเครือข่ายต้องมีการเข้ารหัสอย่างเหมาะสม (เช่น AES-256)
- ใช้โปรโตคอลที่ปลอดภัย เช่น HTTPS ในการส่งข้อมูลผ่านอินเทอร์เน็ต

การบันทึกและตรวจสอบกิจกรรมในระบบ (Logging & Monitoring)

- ระบบต้องบันทึกกิจกรรมสำคัญ เช่น การล็อกอิน การแก้ไขข้อมูล การดาวน์โหลดข้อมูล
- มีการตรวจสอบบันทึกเหล่านี้อย่างสม่ำเสมอเพื่อค้นหาพฤติกรรมผิดปกติ

การทบทวนและตรวจสอบมาตรการรักษาความมั่นคงปลอดภัย

- มีการจัดทำรายงานผลการตรวจสอบภายใน (Internal Audit) อย่างน้อยปีละหนึ่งครั้ง
- มีการตรวจสอบจากผู้ตรวจสอบภายนอก (External Audit) อย่างน้อยปีละครั้ง เพื่อประเมินประสิทธิภาพของมาตรการด้านความมั่นคงปลอดภัย

รายงานผลการตรวจสอบภายในระบบรักษาความมั่นคงปลอดภัยของซอฟต์แวร์

ประจำปีงบประมาณ พ.ศ. 2568

1. วัตถุประสงค์

เพื่อประเมินการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของซอฟต์แวร์ที่ใช้ประมวลผลข้อมูลส่วนบุคคล และตรวจสอบความเหมาะสมของมาตรการด้านความปลอดภัย

2. ผลการตรวจสอบ

- ระบบมีการใช้รหัสผ่านที่ซับซ้อนและมีการเปลี่ยนรหัสผ่านตามกำหนด
- มีการจัดการสิทธิ์การเข้าถึงข้อมูลอย่างเหมาะสมตามหน้าที่ของผู้ใช้
- ข้อมูลส่วนบุคคลมีการเข้ารหัสทั้งในที่เก็บและการส่งข้อมูลผ่านเครือข่าย
- มีการบันทึกกิจกรรมและตรวจสอบอย่างสม่ำเสมอ
- แนะนำให้เพิ่มการฝึกอบรมพนักงานเกี่ยวกับความปลอดภัยของข้อมูลเพิ่มเติม

3. ข้อเสนอแนะ

- ควรจัดให้มีการตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยจากภายนอกเพื่อเพิ่มความน่าเชื่อถือ
- ปรับปรุงนโยบายความปลอดภัยให้ครอบคลุมเทคโนโลยีใหม่ ๆ

ลงชื่อ

.....

(นายสมชาย ใจดี)

หัวหน้าฝ่ายตรวจสอบภายใน

วันที่ 10 มีนาคม 2568

ตัวอย่างนโยบายข้อปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยของซอฟต์แวร์ (Software Security Policy)

1. วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติและมาตรการรักษาความมั่นคงปลอดภัยของซอฟต์แวร์และระบบที่ใช้ประมวลผลข้อมูลส่วนบุคคล ให้มั่นใจได้ว่าข้อมูลส่วนบุคคลได้รับการปกป้องจากการเข้าถึง การแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาต

2. ขอบเขต

นโยบายนี้ครอบคลุมซอฟต์แวร์ ระบบ และแอปพลิเคชันที่ใช้ในการจัดเก็บ ประมวลผล และถ่ายโอนข้อมูลส่วนบุคคลภายในองค์กร

3. ข้อกำหนดและมาตรการ

3.1 การควบคุมการเข้าถึง

ผู้ใช้ทุกคนต้องมีบัญชีผู้ใช้ส่วนตัว และต้องใช้รหัสผ่านที่มีความซับซ้อน (อย่างน้อย 8 ตัวอักษร ประกอบด้วย ตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และสัญลักษณ์)

- รหัสผ่านต้องมีการเปลี่ยนทุก 90 วัน และไม่ควรรีใช้รหัสผ่านเดิมซ้ำ
- การอนุญาตเข้าถึงข้อมูลหรือฟังก์ชันของซอฟต์แวร์จะกำหนดตามหน้าที่และความจำเป็นของผู้ใช้ (Principle of Least Privilege)

3.2 การเข้ารหัสข้อมูล

- ข้อมูลส่วนบุคคลที่จัดเก็บในระบบต้องถูกเข้ารหัสด้วยมาตรฐานที่ได้รับการยอมรับ เช่น AES-256
- ข้อมูลที่ส่งผ่านเครือข่ายต้องใช้โปรโตคอลปลอดภัย เช่น HTTPS หรือ VPN

3.3 การบันทึกกิจกรรมและตรวจสอบ

- ระบบต้องมีการบันทึกกิจกรรมสำคัญ เช่น การเข้าสู่ระบบ การเปลี่ยนแปลงข้อมูล และการดาวน์โหลดข้อมูล
- มีการตรวจสอบบันทึกกิจกรรมอย่างสม่ำเสมอเพื่อค้นหาพฤติกรรมที่ผิดปกติหรือเสี่ยงต่อความปลอดภัย

3.4 การทบทวนและตรวจสอบความปลอดภัย

- มีการจัดให้มีการตรวจสอบภายใน (Internal Audit) อย่างน้อยปีละหนึ่งครั้ง เพื่อตรวจสอบประสิทธิภาพและการปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัย
- มีการจัดให้มีการตรวจสอบจากภายนอก (External Audit) อย่างน้อยปีละครั้ง

3.5 การอบรมและสร้างความตระหนัก

จัดอบรมพนักงานเกี่ยวกับนโยบายการใช้ซอฟต์แวร์อย่างปลอดภัยและการปกป้องข้อมูลส่วนบุคคลอย่างสม่ำเสมอ

4. การบังคับใช้

ผู้ที่ฝ่าฝืนนโยบายนี้จะได้รับการดำเนินการตามข้อกำหนดของกฎหมายและข้อบังคับขององค์กร

รายงานผลการตรวจสอบภายในระบบรักษาความมั่นคงปลอดภัยของซอฟต์แวร์
ประจำปีงบประมาณ พ.ศ. _____

1. ข้อมูลทั่วไป

- ชื่อหน่วยงาน: _____
- ชื่อผู้ตรวจสอบ: _____
- วันที่ตรวจสอบ: _____
- ช่วงเวลาที่ตรวจสอบ: _____

2. วัตถุประสงค์การตรวจสอบ

เพื่อประเมินการปฏิบัติตามนโยบายข้อปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยของซอฟต์แวร์ และตรวจสอบความเหมาะสมของมาตรการด้านความมั่นคงปลอดภัยของระบบและแอปพลิเคชันที่ใช้ประมวลผลข้อมูลส่วนบุคคล

3. ขอบเขตการตรวจสอบ

- ซอฟต์แวร์และระบบที่ตรวจสอบ: _____
- ประเภทข้อมูลส่วนบุคคลที่เกี่ยวข้อง: _____

4. ข้อค้นพบ (Findings)

4.1 การควบคุมการเข้าถึง

- ผลการตรวจสอบ: _____
- ข้อเสนอแนะ: _____

4.2 การเข้ารหัสข้อมูล

- ผลการตรวจสอบ: _____
- ข้อเสนอแนะ: _____

4.3 การบันทึกกิจกรรมและตรวจสอบ

- ผลการตรวจสอบ: _____
- ข้อเสนอแนะ: _____

4.4 การทบทวนและตรวจสอบมาตรการรักษาความปลอดภัย

- ผลการตรวจสอบ: _____
- ข้อเสนอแนะ: _____

5. ข้อเสนอแนะและข้อเสนอแนะ

- ใช้บริการผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศหรือผู้ตรวจสอบภายนอก (IT Audit) ในกรณีที่จำเป็น เพื่อให้การตรวจสอบมีความเป็นอิสระและมาตรฐาน
- พิจารณาและดำเนินการแก้ไขข้อบกพร่องหรือช่องโหว่ที่พบจากการตรวจสอบอย่างทันท่วงที
- มีการเก็บรักษาหลักฐานการตรวจสอบ เช่น รายงานผลการตรวจสอบ สัญญาบริการตรวจสอบ และหนังสือการพิจารณาผลการตรวจสอบ เพื่อใช้ประกอบการตรวจสอบและรับรองความถูกต้องตามกฎหมาย

หลักฐานประกอบ

- นโยบายการเฝ้าระวังให้มีการปฏิบัติตามข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์
- สัญญาบริการการตรวจสอบของผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศภายนอก (IT Audit)
- รายงานผลการตรวจสอบข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์
- หนังสือการพิจารณารายงานผลการตรวจสอบข้อปฏิบัติสำหรับการใช้ซอฟต์แวร์

สภาพบังคับ

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (7) และ ข้อ 5

โทษทางปกครอง

ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองสูงสุดไม่เกิน 3 ล้านบาท

9.8 การควบคุมการเข้าถึง (Access control)

องค์กรควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น และมีการทบทวนสิทธิในการเข้าถึงอย่างสม่ำเสมอ

9.8.1 มีนโยบายควบคุมการเข้าถึงข้อมูล นโยบายครอบคลุมถึงวิธีปฏิบัติในการใช้ข้อมูลการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย เช่น การใช้รหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับการพิสูจน์ตัวตนเพื่อเข้าระบบ

สิ่งที่ต้องทำ: มีนโยบายควบคุมการเข้าถึงข้อมูล นโยบายครอบคลุมถึงวิธีปฏิบัติในการใช้ข้อมูลการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย เช่น การใช้รหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับการพิสูจน์ตัวตนเพื่อเข้าระบบ

หลักฐาน: นโยบายควบคุมการเข้าถึงข้อมูลส่วนบุคคล
ทะเบียนการควบคุมการเข้าถึงข้อมูลส่วนบุคคล

มาตรการทางเทคนิคเพื่อจำกัดการเข้าถึงข้อมูลส่วนบุคคลตามทะเบียนของบุคลากรที่ได้รับอนุญาต

รายงานผลการตรวจสอบการเข้าถึงทะเบียนของบุคลากรที่ได้รับอนุญาต

หนังสือแจ้งเตือนเหตุการณ์รั่วไหลหรือความเสี่ยงที่เกิดขึ้นจากการเข้าถึงของบุคลากรที่ไม่ได้รับอนุญาต

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control Policy)

1. วัตถุประสงค์

เพื่อกำหนดหลักเกณฑ์และแนวทางการควบคุมการเข้าถึงข้อมูลส่วนบุคคลในองค์กร ให้มีความมั่นคงปลอดภัย ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และรักษาความลับ ความถูกต้อง และความสมบูรณ์ของข้อมูลส่วนบุคคล

2. ขอบเขต

นโยบายนี้ครอบคลุมการเข้าถึงข้อมูลส่วนบุคคลในทุกระบบ เทคโนโลยี แอปพลิเคชัน และอุปกรณ์ที่เกี่ยวข้องกับการเก็บรวบรวม ประมวลผล หรือจัดเก็บข้อมูลส่วนบุคคลขององค์กร

3. คำนิยาม

- **ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลที่ระบุหรือสามารถระบุตัวบุคคลได้ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- **ผู้ได้รับอนุญาต** หมายถึง บุคลากรหรือบุคคลที่องค์กรมอบหมายให้มีสิทธิ์เข้าถึงข้อมูลส่วนบุคคลตามบทบาทหน้าที่
- **การพิสูจน์ตัวตน (Authentication)** หมายถึง กระบวนการตรวจสอบและยืนยันตัวบุคคลก่อนให้สิทธิ์เข้าถึงระบบหรือข้อมูล

4. นโยบายหลัก

4.1 การควบคุมสิทธิ์การเข้าถึง

- ให้มีการกำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคลตามหลัก “สิทธิ์น้อยที่สุด” (Least Privilege Principle) โดยบุคคลจะได้รับสิทธิ์เพียงพอที่จำเป็นสำหรับการปฏิบัติงานเท่านั้น

- กำหนดบทบาทและระดับการเข้าถึง (Role-Based Access Control) อย่างชัดเจนและเป็นลายลักษณ์อักษร
- มีการจัดทำทะเบียนควบคุมสิทธิการเข้าถึงข้อมูลอย่างเป็นระบบและอัปเดตสม่ำเสมอ

4.2 การพิสูจน์ตัวตน

- ผู้ใช้ระบบต้องทำการพิสูจน์ตัวตนด้วยข้อมูลประจำตัวที่มีความมั่นคงปลอดภัย เช่น
- การใช้รหัสผ่านที่มีความซับซ้อน (ความยาวไม่น้อยกว่า 8 ตัวอักษร มีตัวอักษรใหญ่-เล็ก ตัวเลข และสัญลักษณ์)
- กำหนดให้เปลี่ยนรหัสผ่านเป็นระยะเวลาที่เหมาะสม (เช่น ทุก 90 วัน)
- ส่งเสริมการใช้ระบบยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)
- ห้ามมิให้ผู้ใดเปิดเผยหรือแลกเปลี่ยนข้อมูลการพิสูจน์ตัวตนกับบุคคลอื่น

4.3 การจำกัดการเข้าถึงและการตรวจสอบ

การเข้าถึงข้อมูลต้องถูกจำกัดผ่านมาตรการทางเทคนิค เช่น ระบบล็อกอิน การตั้งค่าเครือข่ายและไฟร์วอลล์ จัดให้มีระบบบันทึกและตรวจสอบการเข้าถึงข้อมูล (Access Log) เพื่อให้สามารถติดตามและตรวจสอบเหตุการณ์การเข้าถึงข้อมูลได้ ให้มีการทบทวนสิทธิการเข้าถึงข้อมูลอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงบทบาทหน้าที่

4.4 การเฝ้าระวังและจัดการเหตุการณ์

- มีระบบแจ้งเตือนเมื่อพบการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือมีพฤติกรรมที่ผิดปกติ
- กำหนดขั้นตอนในการตอบสนองและแก้ไขเหตุการณ์ รวมถึงการรายงานเหตุการณ์ต่อผู้บริหารและหน่วยงานที่เกี่ยวข้อง
- ฝึกอบรมบุคลากรให้ตระหนักถึงความสำคัญของการรักษาความลับและความมั่นคงของข้อมูล

5. การตรวจสอบและทบทวนนโยบาย

นโยบายนี้จะได้รับการตรวจสอบและทบทวนอย่างน้อยปีละหนึ่งครั้ง โดยฝ่ายความมั่นคงปลอดภัยสารสนเทศและฝ่ายตรวจสอบภายใน

ปรับปรุงนโยบายให้สอดคล้องกับกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

6. บทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้อาจทำให้เกิดความเสียหายแก่ข้อมูลส่วนบุคคล และองค์กรจะดำเนินการทางวินัย รวมถึงรับผิดชอบตามกฎหมายที่เกี่ยวข้อง เช่น การถูกปรับทางปกครองตามมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีโทษปรับไม่เกิน 3 ล้านบาท

7. ตัวอย่างแบบฟอร์มและเอกสารที่เกี่ยวข้อง

- แบบฟอร์มขอสิทธิเข้าถึงข้อมูลส่วนบุคคล
- ทะเบียนสิทธิการเข้าถึงข้อมูลส่วนบุคคล
- รายงานผลการตรวจสอบการเข้าถึงข้อมูล
- แบบฟอร์มรายงานเหตุการณ์รั่วไหลของข้อมูล (Data Breach Report)

1. แบบฟอร์มขอสิทธิเข้าถึงข้อมูลส่วนบุคคล (Access Request Form) — ตัวอย่าง

รายละเอียด	ข้อมูล / คำอธิบาย
ชื่อผู้ขอ	นายสมชาย ใจดี
ตำแหน่ง	เจ้าหน้าที่ไอที
แผนก/ฝ่าย	ฝ่ายเทคโนโลยีสารสนเทศ
เบอร์ติดต่อ	081-234-5678
อีเมล	somchai@example.com
วันที่ขอ	01 /06 /2025
ระบบ/ข้อมูลที่ต้องการเข้าถึง	ระบบฐานข้อมูลลูกค้า (CRM)
เหตุผลขอสิทธิ์เข้าถึงข้อมูล	เพื่อทำการบำรุงรักษาและแก้ไขปัญหาข้อมูล
ระดับการเข้าถึงที่ต้องการ (อ่าน, แก้ไข, ลบ ฯลฯ)	อ่านและแก้ไข
ระยะเวลาที่ต้องการสิทธิ์	1 เดือน
ลงชื่อผู้ขอ	สมชาย ใจดี
วันที่	01 / 06 / 2525

สำหรับเจ้าหน้าที่อนุมัติ

รายละเอียด	ข้อมูล / คำอธิบาย
ผลการพิจารณา (อนุมัติ / ไม่อนุมัติ)	อนุมัติ
เหตุผล	จำเป็นต่อการบำรุงรักษาระบบ
ระดับการเข้าถึงที่อนุมัติ	อ่านและแก้ไข
ระยะเวลาการให้สิทธิ์	1 เดือน
ลงชื่อผู้อนุมัติ	นางสาวรุ่งนภา สายทอง
วันที่	02/ 06 /2025

2. แบบฟอร์มทะเบียนสิทธิการเข้าถึงข้อมูลส่วนบุคคล (Access Rights Register) — ตัวอย่าง

ลำดับ	ชื่อ ผู้ใช้งาน	ตำแหน่ง	แผนก/ ฝ่าย	ระบบ/ ข้อมูลที่ เข้าถึง	ระดับ การ เข้าถึง	วันที่ได้รับ สิทธิ	วันที่สิทธิ หมดอายุ	สถานะ สิทธิ (ใช้ งาน/ ระงับ)	หมายเหตุ
1	นาย สมชาย ใจ ดี	เจ้าหน้าที่ ไอที	ฝ่าย เทคโนโลยี สารสนเทศ	ระบบ ฐานข้อมูล ลูกค้า (CRM)	อ่าน และ แก้ไข	02/06/2525	02/07/2525	ใช้งาน	-
2	นางสาว กนกวรรณ พูนสุข	เจ้าหน้าที่ ฝ่าย การตลาด	ฝ่าย การตลาด	ระบบ ฐานข้อมูล ลูกค้า (CRM)	อ่าน	15/05/2525	15/11/2525	ใช้งาน	ขอ สิทธิ ข้อมูล
3	นายปรีชา ประเสริฐ	ผู้จัดการ ฝ่าย บุคคล	ฝ่ายบุคคล	ระบบ ข้อมูล พนักงาน	อ่าน	01/01/2525	31/12/2525	ระงับ	พ้น สภาพ พนักงาน

3. แบบรายงานผลการตรวจสอบการเข้าถึงข้อมูล (Access Audit Report) — ตัวอย่าง

รายละเอียด	ข้อมูล / คำอธิบาย
ชื่อผู้ตรวจสอบ	นางสาวอรทัย สวัสดิ์ดี
วันที่ตรวจสอบ	31 /05 / 2525
ระบบ/ข้อมูลที่ตรวจสอบ	ระบบฐานข้อมูลลูกค้า (CRM)
วัตถุประสงค์การตรวจสอบ	ตรวจสอบสิทธิการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน
ขอบเขตการตรวจสอบ	สิทธิการเข้าถึงของผู้ใช้งาน 50 รายล่าสุด
ผลการตรวจสอบ	พบผู้ใช้งาน 3 รายที่มีสิทธิเกินกว่าความจำเป็น ต้องลดระดับสิทธิ
ข้อเสนอแนะและแนว ทางแก้ไข	แจ้งผู้ดูแลระบบลดสิทธิ และทบทวนสิทธิทุก 6 เดือน
สรุปภาพรวม	การควบคุมสิทธิเข้าถึงข้อมูลโดยรวมมีประสิทธิภาพแต่ต้องปรับปรุง บางส่วน
ลงชื่อผู้ตรวจสอบ	อรทัย สวัสดิ์ดี
วันที่	31 / 05 / 2525

4. แบบฟอร์มรายงานเหตุการณ์รั่วไหลของข้อมูล (Data Breach Report) — ตัวอย่าง	
รายละเอียด	ข้อมูล / คำอธิบาย
ชื่อผู้รายงาน	นายวสันต์ พิทักษ์ข้อมูล
ตำแหน่ง	เจ้าหน้าที่รักษาความปลอดภัยข้อมูล
แผนก/ฝ่าย	ฝ่ายความปลอดภัยสารสนเทศ
เบอร์ติดต่อ	089-876-0402
อีเมล	wasan@example.com
วันที่เกิดเหตุการณ์	28 / 05 / 2025
เวลาเกิดเหตุการณ์	14:30 น.
สถานที่เกิดเหตุ	เซิร์ฟเวอร์หลักบริษัท
ลักษณะเหตุการณ์	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากบุคคลภายนอก
ข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	ชื่อ-นามสกุล, เบอร์โทรศัพท์, อีเมลลูกค้า
จำนวนข้อมูลหรือจำนวนบุคคลที่ได้รับผลกระทบ	150 ราย
สาเหตุเบื้องต้นของเหตุการณ์	ระบบป้องกันรั่วไหล (Firewall) ถูกเจาะผ่านช่องโหว่
การดำเนินการเบื้องต้น	ปิดช่องโหว่และเปลี่ยนรหัสผ่านระบบทั้งหมด
ผู้รับผิดชอบติดตามแก้ไข	นางสาวรุ่งนภา สายทอง
วันที่รายงาน	29 / 05 / 2025
ลงชื่อผู้รายงาน	วสันต์ พิทักษ์ข้อมูล

9.8.2 มีแนวปฏิบัติเพื่อให้สิทธิการเข้าถึงระบบอย่างเป็นทางการ แนวปฏิบัตินี้ครอบคลุมถึงพนักงานประจำ พนักงานชั่วคราว และผู้ให้บริการภายนอก การให้สิทธิการเข้าถึงเป็นไปตามบทบาทและหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน

สิ่งที่ต้องทำ: มีแนวปฏิบัติเพื่อให้สิทธิการเข้าถึงระบบอย่างเป็นทางการ แนวปฏิบัตินี้ครอบคลุมถึงพนักงานประจำ พนักงานชั่วคราว และผู้ให้บริการภายนอก การให้สิทธิการเข้าถึงเป็นไปตามบทบาทและหน้าที่ความรับผิดชอบของผู้ปฏิบัติงาน

หลักฐาน: นโยบายควบคุมสิทธิการเข้าถึงข้อมูลส่วนบุคคลสารสนเทศ
ทะเบียนของบุคลากรที่ได้รับอนุญาตเข้าถึงเทคโนโลยีสารสนเทศ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
 ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)
 โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง
 ไม่เกิน 3 ล้านบาท

แนวปฏิบัติการให้สิทธิการเข้าถึงระบบ

1. วัตถุประสงค์

เพื่อกำหนดหลักเกณฑ์และวิธีการในการให้สิทธิการเข้าถึงระบบสารสนเทศและข้อมูลส่วนบุคคล
 ขององค์กรอย่างเป็นทางการและเหมาะสมตามบทบาทหน้าที่ความรับผิดชอบของบุคลากรทุกประเภท
 ได้แก่ พนักงานประจำ พนักงานชั่วคราว และผู้ให้บริการภายนอก

2. ขอบเขต

ครอบคลุมบุคลากรทุกประเภทที่มีความจำเป็นต้องเข้าถึงระบบสารสนเทศและข้อมูลส่วนบุคคล
 ขององค์กร ทั้งในรูปแบบการใช้งานภายในและการปฏิบัติงานร่วมกับองค์กร

3. คำนิยาม

- **พนักงานประจำ:** บุคลากรที่มีสัญญาจ้างงานประจำกับองค์กร
- **พนักงานชั่วคราว:** บุคลากรที่มีสัญญาจ้างชั่วคราว หรือเป็นผู้ช่วยงานระยะสั้น
- **ผู้ให้บริการภายนอก:** ผู้ให้บริการหรือที่ปรึกษาที่ได้รับการว่าจ้างจากองค์กรเพื่อปฏิบัติงานที่
 เกี่ยวข้องกับระบบสารสนเทศ

4. แนวปฏิบัติในการให้สิทธิการเข้าถึง

4.1 หลักการทั่วไป

- การให้สิทธิการเข้าถึงระบบสารสนเทศและข้อมูลส่วนบุคคลต้องเป็นไปตามบทบาท หน้าที่ความ
 รับผิดชอบ และความจำเป็นในการปฏิบัติงานเท่านั้น
- ไม่อนุญาตให้มีสิทธิเกินกว่าที่จำเป็น หรือใช้สิทธิเกินขอบเขตที่กำหนดไว้
- การให้สิทธิต้องมีการบันทึกและจัดทำทะเบียนสิทธิผู้ใช้อย่างชัดเจน

4.2 กระบวนการให้สิทธิ

ผู้ขอสิทธิต้องกรอกแบบฟอร์มขอสิทธิเข้าถึงข้อมูลส่วนบุคคลและระบบสารสนเทศ
 หัวหน้าฝ่าย/ผู้บังคับบัญชาต้องตรวจสอบและอนุมัติการให้สิทธิตามบทบาทหน้าที่ของผู้ขอ
 ฝ่ายไอทีหรือเจ้าหน้าที่ที่รับผิดชอบระบบจะดำเนินการให้สิทธิตามคำอนุมัติและบันทึกข้อมูลไว้ในทะเบียน
 สิทธิ

4.3 การให้สิทธิกับพนักงานแต่ละประเภท

- **พนักงานประจำ:** ให้สิทธิ์ตามตำแหน่งและบทบาทงานประจำที่ได้รับมอบหมาย
- **พนักงานชั่วคราว:** ให้สิทธิ์จำกัดตามระยะเวลาที่สัญญาจ้างกำหนด และตามหน้าที่ที่ได้รับมอบหมายเฉพาะงาน
- **ผู้ให้บริการภายนอก:** ให้สิทธิ์เฉพาะงานที่จำเป็นตามสัญญาการว่าจ้าง และต้องได้รับการกำกับดูแลอย่างเข้มงวด

4.4 การทบทวนสิทธิ์

- ทบทวนสิทธิ์การเข้าถึงทุก 6 เดือน หรือเมื่อมีการเปลี่ยนแปลงบทบาทหน้าที่ของผู้ใช้งาน
- ยกเลิกสิทธิ์ทันทีเมื่อพนักงานออกจากงานหรือสิ้นสุดสัญญา

5. การจัดเก็บทะเบียนสิทธิ์การเข้าถึง

- จัดทำและดูแลทะเบียนรายชื่อบุคลากรที่ได้รับสิทธิ์การเข้าถึงระบบและข้อมูลส่วนบุคคลอย่างเป็นระบบ
- ระบุข้อมูลดังนี้: ชื่อผู้ใช้งาน, ประเภทบุคลากร, บทบาทหน้าที่, ระบบที่เข้าถึง, ระดับสิทธิ์, วันที่ให้สิทธิ์, วันที่สิทธิ์หมดอายุ, สถานะสิทธิ์

6. ความรับผิดชอบ

- ผู้บังคับบัญชา: ตรวจสอบและอนุมัติสิทธิ์การเข้าถึงตามบทบาทหน้าที่
- ฝ่ายไอที: ให้สิทธิ์และบันทึกข้อมูลในทะเบียนสิทธิ์
- บุคลากรทุกคน: ปฏิบัติตามข้อกำหนดและไม่ใช้สิทธิ์เกินขอบเขต

7. เอกสารอ้างอิง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

ตัวอย่างแบบฟอร์มที่เกี่ยวข้อง

ตัวอย่าง: แบบฟอร์มขอสิทธิ์เข้าถึงระบบ (Access Request Form)

รายละเอียด	ข้อมูลตัวอย่าง
ชื่อผู้ขอ	นางสาวศิริพร แสงทอง
ประเภทบุคลากร	พนักงานชั่วคราว
ตำแหน่ง	เจ้าหน้าที่ช่วยเหลืองานบุคคล

ระบบที่ขอเข้าถึง	ระบบฐานข้อมูลพนักงาน	
ระดับสิทธิ์	อ่านข้อมูลเท่านั้น	
เหตุผล	ช่วยตรวจสอบข้อมูลพนักงานตามคำสั่งหัวหน้า	
ระยะเวลาที่ต้องการสิทธิ์	3 เดือน (01/06/2025 - 31/08/2025)	
ลงชื่อผู้ขอ	ศิริพร แสงทอง	
วันที่	01/06/2025	

9.8.3 มีการจำกัดและควบคุมการให้สิทธิการเข้าถึงในระดับสูง

สิ่งที่ต้องทำ: มีการจำกัดและควบคุมการให้สิทธิการเข้าถึงในระดับสูง

หลักฐาน: นโยบายจำกัดและควบคุมการให้สิทธิการเข้าถึงในระดับสูง

รายงานผลการตรวจสอบการเข้าถึงในระดับสูงตามทะเบียนของบุคลากรที่ได้รับอนุญาต

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

แนวปฏิบัติการจำกัดและควบคุมการให้สิทธิการเข้าถึงในระดับสูง

1. วัตถุประสงค์

เพื่อกำหนดมาตรการและขั้นตอนในการจำกัดและควบคุมสิทธิการเข้าถึงระบบและข้อมูลส่วนบุคคลในระดับสูง ซึ่งเป็นสิทธิ์ที่มีอำนาจมากกว่าระดับทั่วไป เช่น สิทธิ์ในการแก้ไขข้อมูลเชิงลึก หรือสิทธิ์ในการบริหารจัดการระบบ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และลดความเสี่ยงด้านความปลอดภัยของข้อมูล

2. ขอบเขต

ครอบคลุมผู้ใช้งานทุกประเภทที่ได้รับสิทธิ์ระดับสูง เช่น ผู้ดูแลระบบ (System Administrator), เจ้าหน้าที่ความปลอดภัยข้อมูล (Data Protection Officer), หรือบุคลากรที่ได้รับมอบหมายให้มีสิทธิ์บริหารจัดการระบบสารสนเทศ

3. หลักการและแนวทางปฏิบัติ

3.1 การกำหนดสิทธิ์ระดับสูง

- สิทธิ์ระดับสูงจะถูกกำหนดให้กับบุคลากรที่จำเป็นต้องใช้สิทธิ์นั้นเพื่อปฏิบัติงานตามบทบาทหน้าที่จริงเท่านั้น

- ต้องมีการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงหรือเจ้าหน้าที่ความปลอดภัยข้อมูล
- ห้ามมอบหมายสิทธิ์ระดับสูงโดยไม่มีเหตุผลชัดเจนหรือเกินความจำเป็น

3.2 การควบคุมการให้สิทธิ์

- การให้สิทธิ์ระดับสูงต้องมีการบันทึกข้อมูลอย่างละเอียด เช่น ชื่อผู้ได้รับสิทธิ์, ระดับสิทธิ์, ระบบหรือข้อมูลที่สามารถเข้าถึงได้, วันที่ให้สิทธิ์ และระยะเวลาที่มีสิทธิ์
- จำกัดการใช้งานสิทธิ์ระดับสูงให้อยู่ในช่วงเวลาที่กำหนด และต้องมีการยืนยันการใช้งานหากเป็นการเข้าถึงในเวลานอกเวลาทำการปกติ

3.3 การตรวจสอบและทบทวนสิทธิ์

- ดำเนินการตรวจสอบการใช้งานสิทธิ์ระดับสูงอย่างสม่ำเสมออย่างน้อยทุก 3 เดือน
- รายงานผลการตรวจสอบต้องมีการบันทึกและนำเสนอให้ผู้บริหารและเจ้าหน้าที่ความปลอดภัยข้อมูลพิจารณา
- ทบทวนสิทธิ์และปรับเปลี่ยนหรือยกเลิกทันทีเมื่อไม่จำเป็นต้องใช้สิทธิ์ระดับสูงอีกต่อไป

3.4 มาตรการด้านเทคนิคเสริม

- เปิดใช้ระบบล็อกการใช้งาน (Audit Logs) เพื่อบันทึกกิจกรรมของผู้ใช้สิทธิ์ระดับสูง
- ใช้ระบบการพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) สำหรับผู้ใช้สิทธิ์ระดับสูงเท่านั้น
- กำหนดนโยบายความปลอดภัยในการเปลี่ยนรหัสผ่านอย่างเข้มงวดสำหรับบัญชีผู้ใช้สิทธิ์ระดับสูง

4. ความรับผิดชอบ

- ผู้บริหารระดับสูง: อนุมัติและควบคุมการให้สิทธิ์ระดับสูง
- เจ้าหน้าที่ความปลอดภัยข้อมูล: กำกับดูแลและตรวจสอบการใช้งานสิทธิ์ระดับสูง
- ฝ่ายไอที: จัดการให้สิทธิ์ และดำเนินการบันทึกตรวจสอบกิจกรรมตามมาตรฐาน
- ผู้ได้รับสิทธิ์ระดับสูง: ปฏิบัติตามข้อกำหนดและรายงานเหตุผิดปกติทันที

5. เอกสารและหลักฐาน

- นโยบายจำกัดและควบคุมการให้สิทธิการเข้าถึงในระดับสูง (Access Control Policy for High-level Access)
- ทะเบียนผู้ได้รับสิทธิ์ระดับสูง (High-level Access Registry)
- รายงานผลการตรวจสอบการใช้งานสิทธิ์ระดับสูง (Audit Report)
- บันทึกการอนุมัติการให้สิทธิ์ระดับสูง (Authorization Records)

6. สภาพบังคับ

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

7. โทษทางปกครอง

ในกรณีไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองไม่เกิน 3 ล้านบาท

ตัวอย่างเอกสารและแบบฟอร์ม

ตัวอย่าง: ส่วนหนึ่งของ นโยบายจำกัดและควบคุมการให้สิทธิการเข้าถึงในระดับสูง

ข้อ 5: การอนุมัติสิทธิระดับสูง

สิทธิระดับสูงจะให้เฉพาะผู้ที่ได้รับอนุมัติจากผู้บริหารระดับสูงโดยเป็นลายลักษณ์อักษร โดยผู้ขอสิทธิต้องระบุเหตุผลความจำเป็นในการขอใช้งานอย่างชัดเจน

ตัวอย่าง: แบบฟอร์มขอสิทธิระดับสูง (High-level Access Request Form)

รายการ	ตัวอย่างข้อมูล
ชื่อผู้ขอ	นายสมชาย ใจดี
ตำแหน่ง	ผู้ดูแลระบบ (System Administrator)
ระบบที่ขอเข้าถึง	ระบบฐานข้อมูลลูกค้า (Customer Database)
ระดับสิทธิ์ที่ขอ	สิทธิ์แก้ไขและบริหารระบบ
เหตุผลขอสิทธิ	ต้องดูแลและแก้ไขปัญหาทางเทคนิคของระบบฐานข้อมูล
ระยะเวลาที่ต้องการสิทธิ	1 ปี (01/06/2025 - 31/05/2026)
ผู้อนุมัติ	นางสาวสุดารัตน์ ผู้จัดการฝ่ายไอที
ลงชื่อผู้ขอ	สมชาย ใจดี
ลงชื่อผู้อนุมัติ	สุดารัตน์
วันที่	01/06/2025

ตัวอย่าง: รายงานผลการตรวจสอบสิทธิระดับสูง (Audit Summary Report)

รายการ	รายละเอียด
ชื่อผู้ใช้งาน	นายสมชาย ใจดี
ระบบ	ระบบฐานข้อมูลลูกค้า

สิทธิ์ที่ใช้	แก้ไขข้อมูลและบริหารระบบ	
กิจกรรมที่ตรวจพบ	1) การเข้าสู่ระบบ เวลา 08:30 น. 2) แก้ไขข้อมูลลูกค้า 10 รายการ เวลา 09:00 น. 3) อัปเดตโครงสร้างฐานข้อมูล เวลา 10:00 น.	
ข้อสรุป	ไม่มีการใช้งานนอกเวลาทำการหรือกิจกรรมที่ผิดปกติ	
วันที่ตรวจสอบ	30/08/2025	

9.8.4 มีการเก็บล็อก (log) สำหรับการเข้าถึงระบบ

สิ่งที่ต้องทำ: มีการเก็บล็อกสำหรับการเข้าถึงระบบ

หลักฐาน: นโยบายควบคุมการเข้าถึงข้อมูลส่วนบุคคล

ทะเบียนการควบคุมการเข้าถึงข้อมูลส่วนบุคคล

มาตรการทางเทคนิคเพื่อจำกัดการเข้าถึงข้อมูลส่วนบุคคลตามทะเบียนของบุคลากรที่ได้รับอนุญาต

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

แนวปฏิบัติการเก็บล็อก (Log) สำหรับการเข้าถึงระบบ

1. วัตถุประสงค์

เพื่อกำหนดแนวทางในการบันทึกและเก็บรักษาข้อมูลล็อกการเข้าถึงระบบสารสนเทศ เพื่อใช้ในการตรวจสอบและติดตามกิจกรรมของผู้ใช้งาน ป้องกันและตรวจจับการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต หรือการกระทำที่ผิดปกติ

2. ขอบเขต

ครอบคลุมระบบสารสนเทศที่เกี่ยวข้องกับการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลขององค์กร รวมถึงระบบเครือข่าย ระบบฐานข้อมูล และระบบแอปพลิเคชันทุกประเภท

3. แนวทางการปฏิบัติ

3.1 การเก็บล็อก

ระบบต้องมีการบันทึกข้อมูลล็อกอย่างต่อเนื่องและครบถ้วน สำหรับทุกกิจกรรมที่เกี่ยวข้องกับการเข้าถึงข้อมูลส่วนบุคคล เช่น การเข้าสู่ระบบ การแก้ไขข้อมูล การดาวน์โหลด หรือการลบข้อมูล

ข้อมูลล็อกควรระบุอย่างน้อย ได้แก่

- รหัสผู้ใช้งาน (User ID)
- เวลาและวันที่ของกิจกรรม
- ประเภทของกิจกรรม (เช่น เข้าสู่ระบบ, แก้ไขข้อมูล)
- ระบบหรือข้อมูลที่เข้าถึง
- ที่อยู่ IP ของผู้ใช้งาน (ถ้ามี)
- ข้อมูลล็อกต้องเก็บรักษาในรูปแบบที่ไม่สามารถแก้ไขเปลี่ยนแปลงย้อนหลังได้ (Immutable Log) หรือมีระบบตรวจสอบความสมบูรณ์ของล็อก

3.2 การรักษาความปลอดภัยข้อมูลล็อก

- ข้อมูลล็อกต้องถูกเก็บไว้อย่างปลอดภัย มีการจำกัดสิทธิ์ในการเข้าถึงเฉพาะบุคลากรที่ได้รับอนุญาต
- ต้องมีมาตรการสำรองข้อมูลล็อกเพื่อป้องกันการสูญหาย

3.3 การตรวจสอบและวิเคราะห์ล็อก

- ดำเนินการตรวจสอบล็อกอย่างสม่ำเสมอเพื่อหากิจกรรมที่ผิดปกติหรือมีความเสี่ยงต่อความปลอดภัยของข้อมูล
- บันทึกผลการตรวจสอบและรายงานต่อเจ้าหน้าที่ความปลอดภัยข้อมูลและผู้บริหาร

3.4 การเก็บรักษาข้อมูลล็อก

- เก็บข้อมูลล็อกอย่างน้อยตามระยะเวลาที่กฎหมายหรือมาตรฐานองค์กรกำหนด เช่น อย่างน้อย 1 ปี หรือ 3 ปี
- หลังจากหมดระยะเวลาที่กำหนดให้ดำเนินการลบข้อมูลล็อกอย่างปลอดภัย

4. ความรับผิดชอบ

ฝ่ายไอที: จัดการระบบการเก็บล็อกและการสำรองข้อมูล

เจ้าหน้าที่ความปลอดภัยข้อมูล: ตรวจสอบและวิเคราะห์ล็อก รวมถึงรายงานผล

ผู้บริหาร: กำกับดูแลให้มีการดำเนินการตามนโยบายนี้อย่างเคร่งครัด

5. เอกสารและหลักฐาน

- นโยบายควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control Policy)
- ทะเบียนการควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control Registry)
- รายงานผลการตรวจสอบล็อก (Log Audit Report)
- บันทึกและมาตรการทางเทคนิคเพื่อจำกัดการเข้าถึงข้อมูลตามทะเบียน

6. สภาพบังคับ

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

7. โทษทางปกครอง

ในกรณีไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองไม่เกิน 3 ล้านบาท

ตัวอย่างเอกสารและแบบฟอร์ม

ตัวอย่าง: นโยบายควบคุมการเข้าถึงข้อมูลส่วนบุคคล (ส่วนเกี่ยวกับการเก็บล็อก)

ข้อ 7: การเก็บและบริหารจัดการล็อก (Logs)

ระบบสารสนเทศขององค์กรต้องเก็บล็อกกิจกรรมที่เกี่ยวข้องกับการเข้าถึงข้อมูลส่วนบุคคลอย่างครบถ้วนและปลอดภัย โดยต้องระบุรหัสผู้ใช้งาน เวลา กิจกรรม และระบบที่ถูกเข้าถึง ข้อมูลล็อกต้องถูกเก็บรักษาไม่ให้มีการแก้ไขย้อนหลังและต้องมีมาตรการจำกัดการเข้าถึงอย่างเหมาะสม

ตัวอย่าง: แบบฟอร์มบันทึกล็อกการเข้าถึงระบบ (Log Entry Sample)

หมายเลขบันทึก	วันที่และเวลา	รหัสผู้ใช้งาน	IP Address	กิจกรรม	ระบบที่เข้าถึง
0001	2025-06-01 08:30:00	user123	192.168.1.100	เข้าสู่ระบบ (Login)	ระบบฐานข้อมูลลูกค้า
0002	2025-06-01 09:15:23	user123	192.168.1.100	แก้ไขข้อมูลลูกค้า	ระบบฐานข้อมูลลูกค้า
0003	2025-06-01 10:45:00	admin01	192.168.1.10	เปลี่ยนรหัสผ่านผู้ใช้	ระบบบริหารจัดการระบบ

ตัวอย่าง: รายงานตรวจสอบล็อก (Log Audit Report)

รายการ	รายละเอียด
ชื่อผู้ตรวจสอบล็อก	นางสาวสุภารัตน์ ใจดี

ช่วงเวลาที่ตรวจสอบ	1-30 มิถุนายน 2568	
ระบบที่ตรวจสอบ	ระบบฐานข้อมูลลูกค้า	
ผลการตรวจสอบ	พบกิจกรรมเข้าถึงปกติ ไม่มีการใช้งานผิดปกติ	
ข้อเสนอแนะ	ควรเพิ่มระบบแจ้งเตือนอัตโนมัติหากพบความผิดปกติ	

9.8.5 มีการทบทวนสิทธิการเข้าถึงระบบอย่างสม่ำเสมอ รวมทั้งปรับปรุงหรือแก้ไขสิทธิให้มีความถูกต้องตามความจำเป็น เช่น กรณีที่มีการเปลี่ยนตำแหน่ง ย้ายหน่วยงาน หรือลาออกจากองค์กร เป็นต้น

สิ่งที่ต้องทำ: มีการทบทวนสิทธิการเข้าถึงระบบอย่างสม่ำเสมอ รวมทั้งปรับปรุงหรือแก้ไขสิทธิให้มีความถูกต้องตามความจำเป็น เช่น กรณีที่มีการเปลี่ยนตำแหน่ง ย้ายหน่วยงาน หรือลาออกจากองค์กร เป็นต้น

หลักฐาน: นโยบายทบทวนสิทธิการเข้าถึงระบบ
ทะเบียนการควบคุมการเข้าถึงข้อมูลส่วนบุคคล
หนังสือรายงานสถานะพนักงาน
หนังสือแจ้งการแก้ไขทะเบียนการควบคุมการเข้าถึงข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6), ข้อ 5

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

แนวปฏิบัติการทบทวนและปรับปรุงสิทธิการเข้าถึงระบบอย่างสม่ำเสมอ

1. วัตถุประสงค์

เพื่อให้มั่นใจว่าสิทธิการเข้าถึงระบบสารสนเทศมีความเหมาะสมและสอดคล้องกับบทบาทหน้าที่ความรับผิดชอบของพนักงานในแต่ละช่วงเวลา ป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตและลดความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล

2. ขอบเขต

ครอบคลุมพนักงานประจำ พนักงานชั่วคราว และผู้ให้บริการภายนอกที่ได้รับสิทธิการเข้าถึงระบบสารสนเทศขององค์กรทุกระบบที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

3. แนวทางการปฏิบัติ

3.1 การทบทวนสิทธิการเข้าถึง

- ต้องมีการทบทวนสิทธิการเข้าถึงระบบอย่างน้อยทุก 6 เดือน หรือในช่วงเวลาที่เหมาะสมตามนโยบายขององค์กร
- การทบทวนสิทธิจะพิจารณาจากข้อมูลการเปลี่ยนแปลงสถานะพนักงาน เช่น การเปลี่ยนตำแหน่งงาน การย้ายหน่วยงาน การลาออก หรือการเลิกจ้าง
- พนักงานที่ไม่มีความจำเป็นต้องเข้าถึงระบบตามหน้าที่ต้องถูกยกเลิกสิทธิ์ทันที

3.2 การปรับปรุงสิทธิ

- หากพบว่าพนักงานมีสิทธิ์เข้าถึงที่ไม่เหมาะสม เช่น มากเกินความจำเป็น หรือไม่เกี่ยวข้องกับหน้าที่ใหม่ ต้องดำเนินการแก้ไขสิทธิ์ให้สอดคล้อง
- บันทึกและแจ้งให้ผู้เกี่ยวข้องทราบถึงการเปลี่ยนแปลงสิทธิอย่างเป็นทางการ
- ต้องมีระบบหรือตัวกลางที่ใช้สำหรับแจ้งการแก้ไขสิทธิ์และรับรองการดำเนินการนั้นเสร็จสมบูรณ์

3.3 การบันทึกและรายงาน

- จัดทำทะเบียนการควบคุมสิทธิการเข้าถึง (Access Control Registry) ที่อัปเดตล่าสุด รวมถึงการแก้ไขสิทธิ์ที่เกิดขึ้น
- รายงานผลการทบทวนสิทธิและการปรับปรุงให้ผู้บริหารหรือเจ้าหน้าที่ความปลอดภัยข้อมูลทราบเป็นระยะ
- เก็บเอกสารหลักฐานที่เกี่ยวข้อง เช่น รายงานสถานะพนักงาน หนังสือแจ้งแก้ไขสิทธิ์ เพื่อใช้เป็นหลักฐานการปฏิบัติตามกฎหมาย

4. ความรับผิดชอบ

- ฝ่ายทรัพยากรบุคคล: แจ้งข้อมูลการเปลี่ยนแปลงสถานะพนักงานให้ฝ่ายไอทีหรือผู้ดูแลระบบทราบทันที
- ฝ่ายไอที/ผู้ดูแลระบบ: ดำเนินการทบทวนและปรับปรุงสิทธิการเข้าถึงตามข้อมูลที่ได้รับ
- เจ้าหน้าที่ความปลอดภัยข้อมูล: ตรวจสอบและติดตามการทบทวนสิทธิให้เป็นไปตามนโยบายและกฎหมาย

5. เอกสารและหลักฐาน

- นโยบายทบทวนสิทธิการเข้าถึงระบบ (Access Review Policy)
- ทะเบียนการควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control Registry)
- หนังสือรายงานสถานะพนักงาน (เช่น รายงานเปลี่ยนตำแหน่ง, รายงานลาออก)
- หนังสือแจ้งการแก้ไขทะเบียนการควบคุมการเข้าถึงข้อมูลส่วนบุคคล

6. สภาพบังคับ

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6), ข้อ 5

7. โฆษทางปกครอง

หากไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองไม่เกิน 3 ล้านบาท

ตัวอย่างเอกสารและแบบฟอร์ม

ตัวอย่าง: นโยบายทบทวนสิทธิการเข้าถึงระบบ (ส่วนที่เกี่ยวข้อง)

ข้อ 8: การทบทวนสิทธิการเข้าถึงระบบ

- ฝ่ายไอทีต้องดำเนินการทบทวนสิทธิการเข้าถึงระบบทุก 6 เดือน หรือทันทีที่ได้รับแจ้งการเปลี่ยนแปลงสถานะของพนักงาน
- สิทธิการเข้าถึงจะถูกปรับเปลี่ยนหรือยกเลิกให้สอดคล้องกับบทบาทหน้าที่ปัจจุบันของพนักงาน
- การทบทวนและแก้ไขสิทธิจะต้องมีการบันทึกเป็นลายลักษณ์อักษรและเก็บรักษาเป็นหลักฐาน

ตัวอย่าง: แบบฟอร์มทะเบียนการควบคุมการเข้าถึง (Access Control Registry)

รหัสพนักงาน	ชื่อ-นามสกุล	ตำแหน่ง	หน่วยงาน	สิทธิการเข้าถึงระบบ	วันที่ทบทวนสิทธิ	หมายเหตุ
12345	นายสมชาย ใจดี	เจ้าหน้าที่ไอที	ฝ่ายไอที	เข้าถึงฐานข้อมูลลูกค้า, ระบบอีเมล	01/06/2025	ไม่มีการเปลี่ยนแปลงสิทธิ
67890	นางสาวสุดารัตน์ สายทอง	เจ้าหน้าที่การเงิน	ฝ่ายบัญชี	เข้าถึงระบบบัญชี	01/06/2025	เปลี่ยนตำแหน่งแจ้งแก้ไขสิทธิ

ตัวอย่าง: หนังสือรายงานสถานะพนักงาน

วันที่: 1 มิถุนายน 2568

เรื่องรายงานการเปลี่ยนแปลงสถานะพนักงาน

เรียน: ฝ่ายไอที

ตามที่บริษัทได้มีการเปลี่ยนแปลงสถานะของพนักงาน ดังรายละเอียดดังต่อไปนี้

1. นายสมชาย ใจดี เลื่อนตำแหน่งเป็นหัวหน้าฝ่ายไอที มีผลตั้งแต่วันที่ 1 มิถุนายน 2568
2. นางสาวสุดารัตน์ สายทอง ย้ายจากฝ่ายบัญชี ไปฝ่ายการตลาด มีผลตั้งแต่วันที่ 1 มิถุนายน 2568

จึงเรียนมาเพื่อดำเนินการทบทวนและแก้ไขสิทธิการเข้าถึงระบบตามความจำเป็น

ขอแสดงความนับถือ ฝ่ายทรัพยากรบุคคล
ตัวอย่าง: หนังสือแจ้งการแก้ไขทะเบียนการควบคุมการเข้าถึงข้อมูลส่วนบุคคล วันที่: 2 มิถุนายน 2568 เรื่อง: แจ้งการแก้ไขสิทธิการเข้าถึงระบบของพนักงาน เรียน: ฝ่ายบริหารระบบ ตามที่ได้รับรายงานการเปลี่ยนแปลงสถานะของพนักงาน ข้าพเจ้าขอแจ้งการแก้ไขสิทธิการเข้าถึงระบบดังนี้ - นางสาวสุภารัตน์ สายทอง: ยกเลิกสิทธิการเข้าถึงระบบบัญชี และเพิ่มสิทธิการเข้าถึงระบบการตลาด โปรดดำเนินการปรับปรุงสิทธิ์ให้เรียบร้อยโดยเร็ว ขอแสดงความนับถือ เจ้าหน้าที่ความปลอดภัยข้อมูล

9.9 การป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized access)

องค์กรมีการป้องกันการเข้าถึงระบบหรือแอปพลิเคชันโดยไม่ได้รับอนุญาต การกำหนดรหัสผ่าน มาตรการทางเทคนิคในการจัดการช่องโหว่ และเครื่องมือป้องกันมัลแวร์

9.9.1 มีการจำกัดการเข้าถึงระบบหรือแอปพลิเคชันที่ประมวลผลข้อมูลส่วนบุคคล โดยให้สิทธิการเข้าถึงให้น้อยที่สุดตามความจำเป็น (the principle of least privilege)

สิ่งที่ต้องทำ: มีการจำกัดการเข้าถึงระบบหรือแอปพลิเคชันที่ประมวลผลข้อมูลส่วนบุคคล โดยให้สิทธิการเข้าถึงให้น้อยที่สุดตามความจำเป็น (the principle of least privilege) และมีเอกสารสนับสนุน

หลักฐาน: นโยบายจำกัดการเข้าถึงระบบหรือแอปพลิเคชันที่ประมวลผลข้อมูลส่วนบุคคล
 ป้องกันการเข้าถึง การรวบรวม และการใช้งานโดยไม่ได้รับอนุญาต
 ทะเบียนของบุคลากรที่ได้รับอนุญาตให้เข้าถึงข้อมูลส่วนบุคคล

สภาพบังคับ: คู่มือรองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง
ไม่เกิน 3 ล้านบาท

การจำกัดการเข้าถึงระบบหรือแอปพลิเคชันที่ประมวลผลข้อมูลส่วนบุคคล ตามหลักการสิทธิที่น้อยที่สุด (The Principle of Least Privilege)

1. วัตถุประสงค์

เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต และจำกัดสิทธิการเข้าถึงระบบหรือแอปพลิเคชันเฉพาะผู้ที่จำเป็นต้องใช้ตามบทบาทหน้าที่จริงเท่านั้น เพื่อลดความเสี่ยงในการรั่วไหลหรือถูกละเมิดข้อมูล

2. แนวทางการปฏิบัติ

2.1 การกำหนดสิทธิ์เข้าถึง

- กำหนดสิทธิ์เข้าถึงระบบหรือแอปพลิเคชันที่ประมวลผลข้อมูลส่วนบุคคลโดยยึดหลัก "ให้สิทธิ์ที่น้อยที่สุดที่จำเป็น" (Least Privilege)
- สิทธิการเข้าถึงจะถูกจำกัดตามบทบาทหน้าที่ (Role-Based Access Control - RBAC) หรือแบบจำเพาะบุคคล (User-Based Access Control)
- ผู้ดูแลระบบจะต้องตรวจสอบและอนุมัติสิทธิ์ก่อนการให้สิทธิ์เข้าถึงแก่บุคลากร

2.2 มาตรการป้องกัน

- ใช้มาตรการทางเทคนิค เช่น ระบบยืนยันตัวตน (Authentication) ที่มีความปลอดภัย เช่น การใช้รหัสผ่านที่รัดกุม การยืนยันตัวตนสองขั้นตอน (2FA)
- มีการอัปเดตและแพตช์ช่องโหว่ในระบบอย่างสม่ำเสมอ
- ติดตั้งและอัปเดตเครื่องมือป้องกันมัลแวร์และภัยคุกคามทางไซเบอร์
- มีระบบตรวจจับและแจ้งเตือนการเข้าถึงที่ผิดปกติ (Intrusion Detection System - IDS)

2.3 การจัดทำเอกสาร

- จัดทำนโยบายจำกัดสิทธิ์เข้าถึงระบบและแอปพลิเคชันที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- จัดทำทะเบียนบุคลากรที่ได้รับอนุญาตเข้าถึงข้อมูลส่วนบุคคล และอัปเดตข้อมูลสิทธิการเข้าถึงอย่างสม่ำเสมอ
- จัดเก็บหลักฐานการกำหนดสิทธิ์และการอนุมัติสิทธิ์เข้าถึงอย่างครบถ้วน

3. เอกสารและหลักฐาน

- นโยบายจำกัดการเข้าถึงระบบหรือแอปพลิเคชันที่ประมวลผลข้อมูลส่วนบุคคล
- มาตรการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- ทะเบียนบุคลากรที่ได้รับอนุญาตให้เข้าถึงข้อมูลส่วนบุคคล
- รายงานการอนุมัติสิทธิการเข้าถึง

4. สภาพบังคับ

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6) 5

โทษทางปกครอง

หากไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองไม่เกิน 3 ล้านบาท

ตัวอย่างเอกสารสนับสนุน

ตัวอย่าง: นโยบายจำกัดการเข้าถึงระบบและแอปพลิเคชัน (Excerpt)

ข้อ 5: การจำกัดสิทธิ์เข้าถึงระบบ

- การเข้าถึงระบบที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจะต้องจำกัดสิทธิ์ตามบทบาทหน้าที่ของพนักงาน โดยเคร่งครัด
- การให้สิทธิ์เข้าถึงจะต้องได้รับการอนุมัติจากผู้มีอำนาจเท่านั้น
- ต้องใช้รหัสผ่านที่มีความซับซ้อนและมีการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด
- ห้ามแชร์รหัสผ่านหรือบัญชีผู้ใช้งานกับผู้อื่นโดยเด็ดขาด
- ต้องติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์และตรวจสอบช่องโหว่อย่างสม่ำเสมอ

ตัวอย่าง: ทะเบียนบุคลากรที่ได้รับสิทธิ์เข้าถึงข้อมูลส่วนบุคคล

รหัสพนักงาน	ชื่อ-นามสกุล	ตำแหน่ง	ระบบ/แอปพลิเคชันที่เข้าถึง	สิทธิ์การเข้าถึง	วันที่อนุมัติ	หมายเหตุ
001	นางสาวสมศรีดวงใจ	เจ้าหน้าที่ไอที	ระบบฐานข้อมูลลูกค้า (CRM)	อ่านและแก้ไขข้อมูล	10/01/2025	อนุมัติโดยผู้จัดการฝ่ายไอที
002	นายสุชาติใจดี	เจ้าหน้าที่ฝ่ายบัญชี	ระบบบัญชี	อ่านข้อมูลเฉพาะที่เกี่ยวข้อง	15/02/2025	จำกัดสิทธิ์เข้าถึงเฉพาะบัญชีลูกค้า

ตัวอย่าง: รายงานการอนุมัติสิทธิ์เข้าถึงระบบ

วันที่: 10 มกราคม 2568

เรื่อง: อนุมัติการให้สิทธิ์เข้าถึงระบบฐานข้อมูลลูกค้า

เรียน: ผู้ดูแลระบบไอที

ตามที่ได้รับคำขอให้สิทธิ์การเข้าถึงระบบฐานข้อมูลลูกค้าแก่พนักงาน นางสาวสมศรี ดวงใจ ในตำแหน่งเจ้าหน้าที่ไอที

ข้าพเจ้าในฐานะผู้จัดการฝ่ายไอทีขออนุมัติให้สิทธิ์เข้าถึงในระดับอ่านและแก้ไขข้อมูล ตามความจำเป็นของงาน

ขอแสดงความนับถือ
(ลงชื่อ) ผู้จัดการฝ่ายไอที

9.9.2 มีการกำหนดให้มีการตั้งรหัสผ่านให้มีความซับซ้อน รวมถึงการจำกัดจำนวนครั้งที่สามารถล็อกอินผิดพลาดในการเข้าสู่ระบบ เช่น กำหนดจำนวนครั้งที่สามารถล็อกอินผิดพลาดได้ไม่เกิน 3 ครั้ง เป็นต้น

สิ่งที่ต้องทำ: มีการกำหนดให้มีการตั้งรหัสผ่านให้มีความซับซ้อน รวมถึงการจำกัดจำนวนครั้งที่สามารถล็อกอินผิดพลาดในการเข้าสู่ระบบ เช่น กำหนดจำนวนครั้งที่สามารถล็อกอินผิดพลาดได้ไม่เกิน 3 ครั้ง เป็นต้น

หลักฐาน: นโยบายการตั้งรหัสผ่านที่มีความซับซ้อน และจำกัดจำนวนครั้งที่สามารถล็อกอินผิดพลาดในการเข้าสู่ระบบ

หนังสือประกอบการอบรมความปลอดภัยด้านการคุ้มครองข้อมูลส่วนบุคคลประเภท

เทคโนโลยีสารสนเทศและการจำกัดสิทธิการเข้าถึงข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การตั้งรหัสผ่านที่มีความซับซ้อนและจำกัดจำนวนครั้งล็อกอินผิดพลาด

1. วัตถุประสงค์

เพื่อเพิ่มความมั่นคงปลอดภัยในการเข้าถึงระบบและแอปพลิเคชันที่ประมวลผลข้อมูลส่วนบุคคล โดยป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากการเดารหัสผ่านหรือการโจมตีแบบ brute force

2. แนวทางการปฏิบัติ

2.1 การตั้งรหัสผ่านที่มีความซับซ้อน

รหัสผ่านต้องประกอบด้วยอักขระหลากหลายประเภท เช่น ตัวอักษรพิมพ์ใหญ่-เล็ก ตัวเลข และอักขระพิเศษ

- กำหนดความยาวขั้นต่ำของรหัสผ่าน (เช่น อย่างน้อย 8 ตัวอักษร)
- หลีกเลี่ยงการใช้รหัสผ่านที่คาดเดาง่าย เช่น วันเดือนปีเกิด หรือคำศัพท์ทั่วไป
- มีการเปลี่ยนรหัสผ่านตามรอบเวลาที่กำหนด (เช่น ทุก 90 วัน)
- ห้ามใช้รหัสผ่านซ้ำกับรหัสผ่านก่อนหน้านี้ในจำนวนครั้งที่กำหนด

2.2 การจำกัดจำนวนครั้งล็อกอินผิดพลาด

- กำหนดจำนวนครั้งสูงสุดที่อนุญาตให้ล็อกอินผิดพลาด (เช่น ไม่เกิน 3 ครั้ง)
- เมื่อล็อกอินผิดพลาดครบจำนวนครั้งที่กำหนด ให้ล็อกบัญชีผู้ใช้ชั่วคราว (lockout) เพื่อป้องกันการโจมตีแบบ brute force
- มีขั้นตอนการปลดล็อกบัญชีที่ปลอดภัย เช่น การยืนยันตัวตนกับผู้ดูแลระบบ หรือระบบส่งรหัสยืนยันทางอีเมลหรือโทรศัพท์
- บันทึกเหตุการณ์ล็อกอินผิดพลาดและแจ้งเตือนผู้ดูแลระบบเมื่อมีความผิดปกติ

2.3 การอบรมและสร้างความตระหนัก

- จัดอบรมความรู้ด้านการตั้งรหัสผ่านและการรักษาความปลอดภัยข้อมูลส่วนบุคคลแก่พนักงานที่เกี่ยวข้อง
- มีเอกสารและคู่มือการใช้งานระบบที่ชัดเจนเกี่ยวกับนโยบายรหัสผ่านและมาตรการป้องกันล็อกอินผิดพลาด

3. เอกสารและหลักฐาน

- นโยบายการตั้งรหัสผ่านที่มีความซับซ้อนและข้อกำหนดเกี่ยวกับจำนวนครั้งล็อกอินผิดพลาด
- หนังสือหรือรายงานการอบรมความปลอดภัยด้านการคุ้มครองข้อมูลส่วนบุคคลและเทคโนโลยีสารสนเทศ
- บันทึกหรือรายงานเหตุการณ์ล็อกอินผิดพลาดและการจัดการปลดล็อกบัญชีผู้ใช้

4. สภาพบังคับ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

5. โฆษทางปกครอง

หากไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองไม่เกิน 3 ล้านบาท

ตัวอย่างเอกสารสนับสนุน

ตัวอย่าง: นโยบายการตั้งรหัสผ่านและจำกัดจำนวนครั้งล็อกอินผิดพลาด (Excerpt)

ข้อ 6: การตั้งรหัสผ่านและการล็อกบัญชีผู้ใช้

- รหัสผ่านต้องประกอบด้วยอย่างน้อย 8 ตัวอักษร และต้องมีตัวอักษรพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และอักขระพิเศษอย่างน้อยหนึ่งตัว
- รหัสผ่านต้องเปลี่ยนใหม่ทุก 90 วัน และไม่อนุญาตให้ใช้รหัสผ่านเดิมซ้ำใน 5 รอบล่าสุด
- กำหนดให้ล็อกอินผิดพลาดไม่เกิน 3 ครั้ง หากเกินกำหนดบัญชีผู้ใช้จะถูกล็อกชั่วคราว
- การปลดล็อกบัญชีผู้ใช้ต้องผ่านการยืนยันตัวตนจากฝ่ายไอทีหรือผู้ดูแลระบบ
- บันทึกและตรวจสอบเหตุการณ์ล็อกอินผิดพลาดเพื่อตรวจจับความผิดปกติ

ตัวอย่าง: หนังสือรายงานการอบรมความปลอดภัยข้อมูลส่วนบุคคล (Excerpt)

วันที่: 5 เมษายน 2568

เรื่อง: รายงานการอบรมความปลอดภัยข้อมูลส่วนบุคคลและเทคโนโลยีสารสนเทศ

เรียน: ผู้จัดการฝ่ายบุคคล

ตามที่ฝ่ายเทคโนโลยีสารสนเทศได้จัดอบรมเรื่อง “การตั้งรหัสผ่านที่มีความปลอดภัยและการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต” ให้แก่พนักงานเมื่อวันที่ 3 เมษายน 2568
จึงขอรายงานให้ทราบเพื่อเป็นหลักฐานและติดตามผล

ขอแสดงความนับถือ
(ลงชื่อ) เจ้าหน้าที่ฝ่ายไอที

9.9.3 มีการบริหารจัดการรหัสผ่านให้มีความมั่นคงปลอดภัย เช่น การเปลี่ยนรหัสผ่านที่มาจากผู้ผลิต การควบคุมการใช้รหัสผ่านที่มีการแชร์ใช้งานร่วมกัน และการจัดเก็บรหัสผ่านให้มีความมั่นคงปลอดภัย

- สิ่งที่ต้องทำ: มีการบริหารจัดการรหัสผ่านให้มีความมั่นคงปลอดภัย เช่น การเปลี่ยนรหัสผ่านที่มาจากผู้ผลิต การควบคุมการใช้รหัสผ่านที่มีการแชร์ใช้งานร่วมกัน และการจัดเก็บรหัสผ่านให้มีความมั่นคงปลอดภัยอย่างครบถ้วน
- หลักฐาน: การจัดการรหัสผ่านให้มีความมั่นคงปลอดภัย
หนังสือประกอบการอบรมความปลอดภัยด้านการคุ้มครองข้อมูลส่วนบุคคลประเภทเทคโนโลยีสารสนเทศและการจำกัดสิทธิการเข้าถึงข้อมูลส่วนบุคคล
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)
- โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการจัดการรหัสผ่านเพื่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการบริหารจัดการรหัสผ่านในการเข้าถึงระบบและข้อมูลส่วนบุคคล เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ขอบเขต

นโยบายนี้ใช้บังคับกับพนักงาน เจ้าหน้าที่ และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงระบบหรือข้อมูลส่วนบุคคลขององค์กร

เนื้อหาของนโยบาย

– การเปลี่ยนรหัสผ่านเริ่มต้น

ผู้ใช้ต้องเปลี่ยนรหัสผ่านที่มาจากผู้ผลิต (default password) ทันทีหลังจากได้รับสิทธิ์เข้าใช้งานครั้งแรก

– การควบคุมการใช้รหัสผ่านร่วมกัน

ห้ามใช้รหัสผ่านร่วมกันระหว่างผู้ใช้งานโดยเด็ดขาด

รหัสผ่านต้องเป็นความลับและไม่เปิดเผยแก่บุคคลอื่น

– การจัดเก็บรหัสผ่าน

ห้ามบันทึกหรือเก็บรหัสผ่านในรูปแบบที่สามารถเข้าถึงได้ง่าย เช่น ไฟล์ข้อความ หรือโน้ตบนโต๊ะทำงาน

แนะนำให้ใช้โปรแกรมจัดการรหัสผ่าน (Password Manager) ที่มีความปลอดภัยสูง

– การเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

– การตรวจสอบและทบทวน

ฝ่ายไอทีจะดำเนินการตรวจสอบความปลอดภัยของรหัสผ่านและแจ้งเตือนเมื่อพบความเสี่ยงหรือการละเมิด

หนังสือประกอบการอบรม

เรื่อง การบริหารจัดการรหัสผ่านเพื่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ตามที่องค์กรได้กำหนดนโยบายการบริหารจัดการรหัสผ่านเพื่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ตามมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6) เพื่อให้การปฏิบัติงานสอดคล้องกับข้อกำหนดและมาตรฐานความปลอดภัย

ในวันที่ [ระบุวันที่] ฝ่ายเทคโนโลยีสารสนเทศได้จัดการอบรมพนักงานและเจ้าหน้าที่ที่เกี่ยวข้องในหัวข้อ “การบริหารจัดการรหัสผ่านเพื่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล” โดยมีเนื้อหาสำคัญได้แก่

- การเปลี่ยนรหัสผ่านเริ่มต้นทันทีหลังรับสิทธิ์ใช้งาน
- การห้ามใช้รหัสผ่านร่วมกันระหว่างผู้ใช้งาน
- การจัดเก็บและรักษาการรหัสผ่านอย่างปลอดภัย
- การเปลี่ยนรหัสผ่านตามรอบเวลาที่กำหนด
- แนวทางการตรวจสอบและแก้ไขปัญหาเกี่ยวกับรหัสผ่าน

การอบรมนี้มีวัตถุประสงค์เพื่อเสริมสร้างความรู้ ความเข้าใจ และการปฏิบัติที่ถูกต้องในการบริหารจัดการรหัสผ่านเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

จึงเรียนมาเพื่อทราบและถือปฏิบัติอย่างเคร่งครัด

[สถานที่], วันที่ [] เดือน [] พ.ศ. []

ลงชื่อ

(.....)

ตำแหน่ง

9.9.4 มีการป้องกันไฟล์แนบที่มีข้อมูลส่วนบุคคลและส่งมากับอีเมล โดยการใช้การเข้ารหัสข้อมูล

สิ่งที่ต้องทำ: มีการป้องกันไฟล์แนบที่มีข้อมูลส่วนบุคคลและส่งมากับอีเมล โดยการใช้การเข้ารหัสข้อมูล และมีเอกสารสนับสนุนจากการพิจารณา

หลักฐาน: นโยบายการคุ้มครองไฟล์ที่มีข้อมูลส่วนบุคคล

มาตรฐานการป้องกันการเข้าถึง การรวบรวม และการใช้งานโดยไม่ได้รับอนุญาต

รายงานผลการตรวจสอบข้อร้องเรียนการใช้ไฟล์ที่มีข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง
ไม่เกิน 3 ล้านบาท

นโยบายการคุ้มครองไฟล์ที่มีข้อมูลส่วนบุคคลและการเข้ารหัสข้อมูล

วัตถุประสงค์

- เพื่อกำหนดแนวทางในการป้องกันไฟล์ที่มีข้อมูลส่วนบุคคลซึ่งส่งผ่านทางอีเมลด้วยมาตรการการ
- เข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

ขอบเขต

นโยบายนี้ครอบคลุมการส่งไฟล์แนบที่มีข้อมูลส่วนบุคคลผ่านระบบอีเมลขององค์กร โดยบุคลากรทุกคนที่เกี่ยวข้องต้องปฏิบัติตามอย่างเคร่งครัด

แนวทางปฏิบัติ

- ไฟล์แนบที่มีข้อมูลส่วนบุคคลทุกประเภทที่ส่งทางอีเมล ต้องถูกเข้ารหัสด้วยมาตรฐานการเข้ารหัสที่ได้รับการยอมรับ (เช่น AES 256-bit)
- ผู้ส่งต้องแจ้งรหัสผ่านสำหรับถอดรหัสไฟล์แนบแยกต่างหากจากการส่งอีเมล (เช่น ผ่านช่องทางโทรศัพท์ หรือข้อความ)
- ห้ามส่งไฟล์แนบข้อมูลส่วนบุคคลโดยไม่มีการเข้ารหัสข้อมูล
- ระบบอีเมลขององค์กรจะมีการตั้งค่าหรือใช้เครื่องมือป้องกันการส่งไฟล์แนบที่ไม่มีการเข้ารหัสตามนโยบายนี้
- ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ตรวจสอบและบันทึกการส่งไฟล์แนบที่เข้ารหัสอย่างสม่ำเสมอ

มาตรฐานการป้องกันการเข้าถึง การรวบรวม และการใช้งานโดยไม่ได้รับอนุญาต

- การส่งไฟล์แนบที่มีข้อมูลส่วนบุคคลผ่านช่องทางอีเมล ต้องเป็นไปตามนโยบายการเข้ารหัสไฟล์แนบ
- ห้ามเปิดเผยรหัสผ่านหรือกุญแจการถอดรหัสแก่บุคคลที่ไม่มีสิทธิ์
- ต้องมีการจัดเก็บบันทึกและตรวจสอบการส่งไฟล์แนบที่เข้ารหัสเป็นระยะ
- ฝ่ายความปลอดภัยของข้อมูลต้องรายงานการละเมิดหรือข้อร้องเรียนที่เกี่ยวข้องกับการส่งไฟล์แนบข้อมูลส่วนบุคคลโดยทันที

รายงานผลการตรวจสอบข้อร้องเรียนการใช้ไฟล์ที่มีข้อมูลส่วนบุคคล

วันที่ตรวจสอบ: [ระบุวันที่]

ผู้ตรวจสอบ: [ชื่อเจ้าหน้าที่]

รายละเอียดข้อร้องเรียน: มีข้อสงสัยการส่งไฟล์ข้อมูลส่วนบุคคลผ่านอีเมลโดยไม่ได้เข้ารหัส

ผลการตรวจสอบ

- พบว่าผู้ส่งไฟล์แนบไม่ปฏิบัติตามนโยบายการเข้ารหัสไฟล์แนบ
- ได้ดำเนินการแจ้งเตือนและให้คำแนะนำแก่ผู้เกี่ยวข้องทันที
- ได้กำหนดมาตรการเสริมเพื่อป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ เช่น การอบรมเพิ่มเติม การตั้งค่าระบบ บล็อกการส่งไฟล์ที่ไม่เข้ารหัส

สรุป: การปฏิบัติงานอยู่ในระหว่างการปรับปรุงเพื่อให้สอดคล้องกับนโยบายและกฎหมายที่เกี่ยวข้อง

อ้างอิงสภาพบังคับทางกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6)

9.9.5 มีการบันทึกล็อก (log) สำหรับกิจกรรมการเข้าถึงระบบ เพื่อใช้ในการตรวจหาความผิดปกติต่าง ๆ

สิ่งที่ต้องทำ: มีการบันทึกล็อกสำหรับกิจกรรมการเข้าถึงระบบ เพื่อใช้ในการตรวจหาความผิดปกติต่าง ๆ และมีเอกสารสนับสนุน

หลักฐาน: นโยบายการบันทึกล็อกสำหรับกิจกรรมการเข้าถึงระบบเทคโนโลยีสารสนเทศที่มีการประมวลผลข้อมูลส่วนบุคคล
ทะเบียนการประมวลผลข้อมูลส่วนบุคคลผ่านระบบเทคโนโลยีสารสนเทศ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (6)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการบันทึกล็อกสำหรับกิจกรรมการเข้าถึงระบบเทคโนโลยีสารสนเทศที่มีการประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการในการบันทึกข้อมูลกิจกรรมการเข้าถึงระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล เพื่อใช้ในการตรวจสอบและติดตามความผิดปกติหรือเหตุการณ์ที่อาจก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูล

ขอบเขต

นโยบายนี้ครอบคลุมระบบเทคโนโลยีสารสนเทศทั้งหมดที่มีการประมวลผลข้อมูลส่วนบุคคลภายในองค์กร และผู้มีหน้าที่ปฏิบัติตามนโยบายนี้

แนวทางปฏิบัติ

- ระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องต้องบันทึกล็อกกิจกรรมการเข้าถึงระบบทุกครั้ง เช่น การเข้าสู่ระบบ, การออกจากระบบ, การล้มเหลวในการเข้าสู่ระบบ (login failure) และการดำเนินการสำคัญอื่น ๆ ที่เกี่ยวข้อง
- ข้อมูลล็อกต้องเก็บรักษาไว้ในรูปแบบที่ปลอดภัย และสามารถเรียกดูได้เมื่อต้องการตรวจสอบ
- กำหนดระยะเวลาการเก็บรักษาข้อมูลล็อกตามข้อกำหนดทางกฎหมายหรือมาตรฐานขององค์กร
- ฝ่ายเทคโนโลยีสารสนเทศมีหน้าที่ตรวจสอบล็อกเป็นระยะเพื่อค้นหาความผิดปกติ เช่น การพยายามเข้าถึงโดยไม่ได้รับอนุญาตหรือพฤติกรรมที่ผิดปกติอื่น ๆ
- เมื่อพบความผิดปกติ ต้องจัดทำรายงานและดำเนินการแก้ไขตามขั้นตอนที่กำหนด

ทะเบียนการประมวลผลข้อมูลส่วนบุคคลผ่านระบบเทคโนโลยีสารสนเทศ

- รายการระบบเทคโนโลยีสารสนเทศที่มีการประมวลผลข้อมูลส่วนบุคคล
- ข้อมูลกิจกรรมที่บันทึกในล็อก เช่น เวลาเข้าถึง, ผู้ใช้, ประเภทกิจกรรม
- รายงานการตรวจสอบความผิดปกติและการดำเนินการแก้ไข
- เอกสารการบำรุงรักษาและสำรองข้อมูลล็อก

อ้างอิงสภาพบังคับทางกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (6)

บทลงโทษ

ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองไม่เกิน 3 ล้านบาท ตามอำนาจที่กำหนดในมาตรา 37 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

9.9.6 มีการใช้โปรแกรมป้องกันมัลแวร์และป้องกันไวรัสกับระบบที่มีความสำคัญ

- สิ่งที่ต้องทำ: มีการใช้โปรแกรมป้องกันมัลแวร์และป้องกันไวรัสกับระบบที่มีความสำคัญ และมีการทดสอบโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก
- หลักฐาน: นโยบายการจัดหาโปรแกรมรักษาความมั่นคงปลอดภัยแก่ระบบประมวลผลข้อมูลส่วนบุคคล
สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล
รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (5)
- โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการจัดทำโปรแกรมรักษาความมั่นคงปลอดภัยแก่ระบบประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อกำหนดแนวทางในการจัดหาและติดตั้งโปรแกรมป้องกันมัลแวร์และไวรัสสำหรับระบบเทคโนโลยี
- สารสนเทศที่มีการประมวลผลข้อมูลส่วนบุคคลที่สำคัญ เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล และป้องกันการถูกโจมตีจากภัยคุกคามทางไซเบอร์

ขอบเขต

นโยบายนี้ครอบคลุมระบบเทคโนโลยีสารสนเทศทุกระบบที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล ภายในองค์กร โดยเฉพาะระบบที่ถือว่ามีความสำคัญสูงต่อการดำเนินงาน

แนวทางปฏิบัติ

- การจัดหาโปรแกรมป้องกันมัลแวร์และไวรัสต้องเป็นผลิตภัณฑ์ที่ได้รับการรับรองและมีประสิทธิภาพสูง
- ทุกระบบที่มีความสำคัญต้องติดตั้งโปรแกรมป้องกันมัลแวร์และไวรัสอย่างครบถ้วน
- มีการอัปเดตโปรแกรมและฐานข้อมูลไวรัสอย่างสม่ำเสมอ
- มีการทดสอบการทำงานของโปรแกรมป้องกันอย่างน้อยปีละหนึ่งครั้งโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกที่มีความเชี่ยวชาญ
- จัดทำรายงานผลการทดสอบและจัดเก็บเป็นหลักฐานการตรวจสอบเพื่อยืนยันความปลอดภัยของระบบ

เอกสารสนับสนุน

- **สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล**
ระบุรายละเอียดการว่าจ้างผู้ตรวจสอบภายใน/ภายนอก เพื่อดำเนินการทดสอบโปรแกรมป้องกันมัลแวร์และไวรัสในระบบประมวลผลข้อมูลส่วนบุคคล
- **รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล**
สรุปผลการทดสอบโปรแกรมป้องกันมัลแวร์และไวรัส พร้อมข้อเสนอแนะและแนวทางการแก้ไข (ถ้ามี)
- **สภาพบังคับทางกฎหมาย**
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (5)

บทลงโทษ

กรณีไม่ปฏิบัติตามมาตรา 37 อาจถูกปรับทางปกครองไม่เกิน 3 ล้านบาท ตามอำนาจที่กำหนดใน มาตรา 37 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

ระหว่าง สำนักงาน..... ที่อยู่.....

ซึ่งต่อไปในสัญญานี้เรียกว่า "ผู้ว่าจ้าง"

กับ บริษัท..... ที่อยู่..... ซึ่งต่อไป

ในสัญญานี้เรียกว่า "ผู้รับจ้าง"

ข้อ 1 วัตถุประสงค์ของสัญญา

ผู้ว่าจ้างตกลงว่าจ้าง และผู้รับจ้างตกลงรับจ้างดำเนินการทดสอบระบบเพื่อประเมินประสิทธิภาพของมาตรการป้องกันมัลแวร์และไวรัสของระบบประมวลผลข้อมูลส่วนบุคคลของผู้ว่าจ้าง โดยมีวัตถุประสงค์เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง เพื่อให้แน่ใจว่าระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลมีความปลอดภัยและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตอย่างเพียงพอ

ข้อ 2 ขอบเขตของงาน

2.1 การตรวจสอบและประเมินประสิทธิภาพของโปรแกรมป้องกันมัลแวร์และไวรัสในระบบข้อมูลสำคัญของผู้ว่าจ้าง

2.2 การทดสอบการสแกน การตอบสนอง และความสามารถในการป้องกันภัยคุกคามของระบบ

2.3 การจัดทำรายงานผลการประเมิน พร้อมข้อเสนอแนะในการปรับปรุง

2.4 การจัดส่งรายงานฉบับสมบูรณ์ภายใน 30 วัน นับจากวันที่เริ่มดำเนินการทดสอบ

2.5 รายละเอียดขั้นตอนการดำเนินงาน:

ขั้นตอนที่ 1

การเก็บรวบรวมข้อมูลและเอกสารเบื้องต้นของระบบเป้าหมายจากผู้ว่าจ้าง เช่น รายละเอียดระบบที่มีการประมวลผลข้อมูลส่วนบุคคล รายชื่อซอฟต์แวร์รักษาความปลอดภัยที่ใช้ งาน รายการทรัพยากรระบบ ฯลฯ

ขั้นตอนที่ 2

การประเมินความเสี่ยงเบื้องต้น โดยทีมผู้เชี่ยวชาญจะดำเนินการประเมินระดับความเสี่ยงในด้านความมั่นคงปลอดภัยของระบบ และกำหนดจุดที่ควรทดสอบเป็นพิเศษ

ขั้นตอนที่ 3

การทดสอบเชิงเทคนิค ซึ่งครอบคลุมการสแกนมัลแวร์ด้วยเครื่องมือที่ทันสมัย การตรวจสอบลักษณะการทำงานของระบบในเวลาจริง (real-time scanning) การจำลองเหตุการณ์การโจมตีโดยใช้มัลแวร์ประเภทต่าง ๆ การตรวจหาช่องโหว่ และการทดสอบการตอบสนองของระบบต่อการโจมตี

ขั้นตอนที่ 4

การจัดเก็บหลักฐานและข้อมูลผลการทดสอบ ซึ่งรวมถึงภาพหน้าจอ รายงานการตรวจจับ
รายละเอียดเทคนิค และความผิดปกติที่พบ

ขั้นตอนที่ 5

การจัดทำรายงานผลการประเมินในเชิงเทคนิคและเชิงนโยบาย โดยระบุประเด็นที่ตรวจพบ ระดับ
ความเสี่ยง ข้อเสนอแนะในการปรับปรุง และแนวทางในการเพิ่มมาตรการป้องกันในอนาคต

ขั้นตอนที่ 6

การประชุมสรุปผลการทดสอบกับผู้ว่าจ้าง เพื่ออธิบายผลการดำเนินงานในทุกขั้นตอนและรับ
ข้อคิดเห็นเพิ่มเติมก่อนการส่งมอบรายงานฉบับสมบูรณ์

ข้อ 3 ค่าตอบแทนและเงื่อนไขการชำระเงิน

3.1 ค่าจ้างรวมทั้งสิ้นเป็นจำนวนเงิน.....บาท (.....บาทถ้วน) 3.2 ผู้ว่าจ้าง
จะชำระค่าจ้างเมื่อผู้รับจ้างส่งมอบรายงานฉบับสมบูรณ์เรียบร้อยแล้วภายในระยะเวลาที่กำหนด

ข้อ 4 ความลับของข้อมูล

ผู้รับจ้างต้องไม่เปิดเผยหรือใช้ข้อมูลใด ๆ ที่ได้รับจากผู้ว่าจ้างโดยมิชอบ เว้นแต่ได้รับความยินยอม
เป็นลายลักษณ์อักษรจากผู้ว่าจ้าง และต้องมีมาตรการรักษาความลับของข้อมูลอย่างเคร่งครัด ตลอดจน
ทำลายข้อมูลหลังสิ้นสุดสัญญา

ข้อ 5 ระยะเวลาสัญญา เริ่มต้นตั้งแต่วันที่.....ถึงวันที่.....

ลงชื่อ.....ผู้ว่าจ้าง
(.....)

ตำแหน่ง.....

ลงชื่อ.....ผู้รับจ้าง
(.....)

ตำแหน่ง.....

รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

ชื่อหน่วยงาน:

วันที่ทดสอบ:

ผู้ทำการทดสอบ: ...

.....บริษัท

1. รายละเอียดของระบบที่ทำการทดสอบ

- ระบบที่เกี่ยวข้อง: ฐานข้อมูลผู้ใช้บริการ, ระบบ HR, ระบบจัดเก็บเอกสาร
- ประเภทของข้อมูล: ข้อมูลส่วนบุคคลทั่วไป และข้อมูลที่มีความอ่อนไหวบางประเภท

2. เครื่องมือและวิธีการทดสอบ

โปรแกรมที่ใช้: [ระบุชื่อโปรแกรมป้องกันมัลแวร์และไวรัส เช่น Kaspersky, Bitdefender]

วิธีทดสอบ:

- การสแกนเต็มระบบ (Full Scan)
- การจำลองเหตุการณ์มัลแวร์จากตัวอย่างจริง (Simulated Malware Attacks)
- การทดสอบการตอบสนองแบบเรียลไทม์ (Real-time Monitoring)
- การทดสอบช่องโหว่ของระบบ (Vulnerability Assessment)

3. ผลการทดสอบ

- การสแกนระบบ: ไม่พบมัลแวร์หรือภัยคุกคามในระบบทั้งหมด
- ระบบอัปเดตฐานข้อมูลไวรัส: เป็นปัจจุบัน ณ วันที่ทดสอบ
- การป้องกันแบบเรียลไทม์: เปิดใช้งานอยู่ตลอดเวลา
- ไม่มีเหตุการณ์ที่แสดงถึงการละเมิดความมั่นคงปลอดภัย

4. ข้อเสนอแนะ

- ควรตั้งเวลาอัปเดตฐานข้อมูลไวรัสแบบอัตโนมัติทุกวัน
- ควรตั้งค่าการแจ้งเตือนเมื่อพบความเสี่ยงให้ชัดเจน
- พิจารณาเพิ่มระบบสำรองข้อมูลร่วมกับการป้องกันมัลแวร์
- ทบทวนนโยบายและแนวทางการตอบสนองเมื่อเกิดเหตุการณ์ภัยคุกคามเป็นประจำทุกปี

5. สรุปผล

จากการทดสอบ ระบบมีมาตรการป้องกันมัลแวร์และไวรัสที่มีประสิทธิภาพเพียงพอ และสอดคล้องกับข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้อง การรักษาความมั่นคงปลอดภัยมีความเหมาะสมต่อการบริหารจัดการข้อมูลส่วนบุคคลภายในระบบที่ทดสอบ

ลงชื่อ.....ผู้ทดสอบ

(.....)

บริษัท.....

วันที่.....

ลงชื่อ.....

ผู้ตรวจสอบภายใน/ผู้ควบคุมระบบข้อมูล

(.....)

ตำแหน่ง.....

สัญญาที่เพิ่มเติมรายละเอียดเฉพาะของมาตรฐาน เช่น ISO/IEC 27001 หรือมาตรฐานจาก PDPC

สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

ระหว่าง สำนักงาน..... ที่อยู่.....

ซึ่งต่อไปในสัญญานี้เรียกว่า "ผู้ว่าจ้าง"

กับ บริษัท..... ที่อยู่..... ซึ่งต่อไป
ในสัญญานี้เรียกว่า "ผู้รับจ้าง"

วัตถุประสงค์ของสัญญา

ผู้ว่าจ้างตกลงว่าจ้าง และผู้รับจ้างตกลงรับจ้างดำเนินการทดสอบระบบเพื่อประเมินประสิทธิภาพของมาตรการป้องกันมัลแวร์และไวรัสของระบบประมวลผลข้อมูลส่วนบุคคลของผู้ว่าจ้าง โดยมีวัตถุประสงค์เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง รวมถึงให้สอดคล้องกับแนวทางและข้อกำหนดของมาตรฐาน ISO/IEC 27001 และ ISO/IEC 27002 ในหมวดควบคุม A.12.2.1 และ A.12.6.1 ซึ่งเกี่ยวข้องกับการตรวจสอบช่องโหว่และการควบคุมโปรแกรมป้องกันมัลแวร์

ขอบเขตของงาน

- 2.1 การตรวจสอบและประเมินประสิทธิภาพของโปรแกรมป้องกันมัลแวร์และไวรัสในระบบข้อมูลสำคัญของผู้ว่าจ้าง
- 2.2 การทดสอบการสแกน การตอบสนอง และความสามารถในการป้องกันภัยคุกคามของระบบ รวมถึงการจำลองภัยคุกคามจากมัลแวร์และไวรัสประเภทต่าง ๆ
- 2.3 การตรวจสอบว่าโปรแกรมป้องกันไวรัสมีการอัปเดตฐานข้อมูลไวรัสเป็นปัจจุบัน และมีการตั้งค่าการสแกนระบบอัตโนมัติอย่างสม่ำเสมอในระบบที่มีความสำคัญ
- 2.4 การตรวจสอบว่ามีการบันทึกและจัดเก็บข้อมูลการสแกน การแจ้งเตือน และการตอบสนองไว้อย่างเป็นระบบ พร้อมการประเมินโดยผู้ตรวจสอบภายในหรือภายนอก
- 2.5 การจัดทำรายงานผลการประเมิน พร้อมข้อเสนอแนะในการปรับปรุงมาตรการด้านเทคนิคและการจัดการ
- 2.6 การจัดส่งรายงานฉบับสมบูรณ์ภายใน 30 วัน นับจากวันที่เริ่มดำเนินการทดสอบ

คำตอบแทนและเงื่อนไขการชำระเงิน

3.1 ค่าจ้างรวมทั้งสิ้นเป็นจำนวนเงิน.....บาท (.....บาทถ้วน)

3.2 ผู้ว่าจ้างจะชำระค่าจ้างเมื่อผู้รับจ้างส่งมอบรายงานฉบับสมบูรณ์เรียบร้อยแล้วภายในระยะเวลาที่กำหนด

ความลับของข้อมูล

ผู้รับจ้างต้องไม่เปิดเผยหรือใช้ข้อมูลใด ๆ ที่ได้รับจากผู้ว่าจ้างโดยมิชอบ เว้นแต่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง

ข้อ 5 ระยะเวลาสัญญา

เริ่มต้นตั้งแต่วันที่.....ถึงวันที่.....

ลงชื่อ.....ผู้ว่าจ้าง
(.....)

ตำแหน่ง.....

ลงชื่อ.....ผู้รับจ้าง
(.....)

ตำแหน่ง.....

เอกสารที่ 2: รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

ชื่อหน่วยงาน:

วันที่ทดสอบ:

ผู้ทำการทดสอบ: บริษัท.....

1. รายละเอียดของระบบที่ทำการทดสอบ

ระบบที่เกี่ยวข้อง: ฐานข้อมูลผู้ใช้บริการ, ระบบ HR, ระบบจัดเก็บเอกสาร

ประเภทของข้อมูล: ข้อมูลส่วนบุคคลทั่วไป และข้อมูลที่มีความอ่อนไหวบางประเภท

2. เครื่องมือและวิธีการทดสอบ

โปรแกรมที่ใช้: [ระบุชื่อโปรแกรมป้องกันมัลแวร์และไวรัส เช่น Kaspersky, Bitdefender]

วิธีทดสอบ: การสแกนเต็มระบบ, การจำลองเหตุการณ์มัลแวร์, การทดสอบช่องโหว่

3. ผลการทดสอบ

การสแกนระบบ: ไม่พบมัลแวร์หรือภัยคุกคามในระบบทั้งหมด

ระบบอัปเดตฐานข้อมูลไวรัส: เป็นปัจจุบัน ณ วันที่ทดสอบ

การป้องกันแบบเรียลไทม์: เปิดใช้งานอยู่ตลอดเวลา

ไม่มีเหตุการณ์ที่แสดงถึงการละเมิดความมั่นคงปลอดภัย

4. ข้อเสนอแนะ

- ควรตั้งเวลาอัปเดตฐานข้อมูลไวรัสแบบอัตโนมัติทุกวัน
- ควรตั้งค่าการแจ้งเตือนเมื่อพบความเสี่ยงให้ชัดเจน
- พิจารณาเพิ่มระบบสำรองข้อมูลร่วมกับการป้องกันมัลแวร์

5. สรุปผล

จากการทดสอบ ระบบมีมาตรการป้องกันมัลแวร์และไวรัสที่มีประสิทธิภาพเพียงพอ และสอดคล้องกับข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้อง

ลงชื่อ.....ผู้ทดสอบ

(.....)

บริษัท.....

วันที่.....

ลงชื่อ.....ผู้ตรวจสอบภายใน/ผู้ควบคุมระบบข้อมูล

(.....)

ตำแหน่ง.....

9.9.7 โปรแกรมป้องกันมัลแวร์และไวรัสมีการอัปเดตฐานข้อมูลให้เป็นปัจจุบัน และมีการตั้งค่าโปรแกรมป้องกันไวรัสให้ทำการสแกนระบบที่มีความสำคัญอย่างสม่ำเสมอ

สิ่งที่ต้องทำ: โปรแกรมป้องกันมัลแวร์และไวรัสมีการอัปเดตฐานข้อมูลให้เป็นปัจจุบัน มีการตั้งค่าโปรแกรมป้องกันไวรัสให้ทำการสแกนระบบที่มีความสำคัญอย่างสม่ำเสมอ และมีการทดสอบโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก

หลักฐาน: นโยบายการจัดการโปรแกรมรักษาความมั่นคงปลอดภัยแก่ระบบประมวลผลข้อมูลส่วนบุคคล
สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล
รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (5)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

เอกสารนโยบายการจัดการและใช้โปรแกรมรักษาความมั่นคงปลอดภัยแก่ระบบประมวลผลข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการจัดหาและใช้โปรแกรมป้องกันมัลแวร์และไวรัสที่มีประสิทธิภาพในระบบประมวลผลข้อมูลส่วนบุคคลขององค์กร โดยให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรฐานสากลด้านความมั่นคงปลอดภัยของข้อมูล

2. ขอบเขตการใช้งาน

นโยบายนี้ครอบคลุมถึงระบบงาน เซิร์ฟเวอร์ อุปกรณ์ปลายทาง และระบบเครือข่ายที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลทุกประเภทในความรับผิดชอบขององค์กร

3. แนวทางปฏิบัติ

(1) โปรแกรมป้องกันมัลแวร์และไวรัสที่เลือกใช้ต้องสามารถอัปเดตฐานข้อมูลไวรัสโดยอัตโนมัติและต่อเนื่องจากผู้พัฒนา

(2) โปรแกรมต้องสามารถตั้งเวลาให้สแกนระบบและไฟล์ในเครื่องปลายทาง และเซิร์ฟเวอร์สำคัญได้โดยอัตโนมัติ และสามารถตรวจสอบประวัติการสแกนย้อนหลังได้

(3) ผู้ดูแลระบบต้องตรวจสอบสถานะการอัปเดตและการสแกนอย่างสม่ำเสมออย่างน้อยเดือนละ 1 ครั้ง และจัดทำรายงานสรุป

(4) ต้องมีการประเมินประสิทธิภาพของโปรแกรมโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกอย่างน้อยปีละ 1 ครั้ง

(5) การจัดหาโปรแกรมต้องดำเนินการตามกระบวนการจัดซื้อจัดจ้างขององค์กร และต้องพิจารณาข้อกำหนดด้านความมั่นคงปลอดภัยเป็นสำคัญ

4. การบังคับใช้

นโยบายนี้มีผลบังคับใช้แก่หน่วยงานทุกหน่วยที่เกี่ยวข้องกับระบบประมวลผลข้อมูลส่วนบุคคล และจะมีการทบทวนทุกปีหรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับกฎหมาย

5. การอ้างอิง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)(3)(5)
- มาตรฐาน ISO/IEC 27001:2022 ข้อ A.8.7 และ A.12.2.1

ลงชื่อ..... (ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ)

วันที่ออกนโยบาย: [ระบุวันที่] วันที่มีผลบังคับใช้: [ระบุวันที่]

สัญญาฉบับนี้ทำขึ้น ณ วันที่ [.....] ระหว่าง

(1) [ชื่อหน่วยงาน/บริษัทผู้ว่าจ้าง] ตั้งอยู่ที่ [ที่อยู่] ซึ่งต่อไปในสัญญานี้เรียกว่า "ผู้ว่าจ้าง" กับ (2) [ชื่อบริษัทผู้รับจ้าง] ตั้งอยู่ที่ [ที่อยู่ของผู้รับจ้าง] ซึ่งต่อไปในสัญญานี้เรียกว่า "ผู้รับจ้าง"
ทั้งสองฝ่ายตกลงทำสัญญากันโดยมีข้อความดังต่อไปนี้

ข้อ 1 วัตถุประสงค์ของสัญญา

เพื่อให้ผู้รับจ้างดำเนินการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของผู้ว่าจ้าง เพื่อประเมินจุดอ่อนและความเสี่ยงด้านความมั่นคงปลอดภัยของระบบข้อมูล อันรวมถึงการสแกนมัลแวร์และไวรัส การตั้งค่าความปลอดภัย และกระบวนการจัดการความเสี่ยงตามมาตรฐาน ISO/IEC 27001 และตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ข้อ 2 ขอบเขตของงาน

2.1 ตรวจสอบระบบป้องกันมัลแวร์และไวรัสของผู้ว่าจ้าง รวมถึงการอัปเดตฐานข้อมูลไวรัส และการตั้งค่าการสแกนระบบ

2.2 ดำเนินการทดสอบเจาะระบบ (penetration test) และ vulnerability assessment อย่างน้อยปีละ 1 ครั้ง

2.3 จัดทำรายงานผลการทดสอบ พร้อมข้อเสนอแนะเชิงเทคนิค

ข้อ 3 ระยะเวลาดำเนินงาน

ผู้รับจ้างจะดำเนินงานให้แล้วเสร็จภายใน [...] วัน นับถัดจากวันลงนามในสัญญา

ข้อ 4 ค่าจ้างและการชำระเงิน

ผู้ว่าจ้างตกลงจ่ายค่าจ้างจำนวน [...บาทถ้วน...] ให้แก่ผู้รับจ้าง เมื่อผู้รับจ้างส่งมอบงานพร้อมรายงานแล้วเสร็จ และได้รับการตรวจรับจากผู้ว่าจ้างเรียบร้อยแล้ว

ข้อ 5 ความลับและข้อมูลส่วนบุคคล ผู้รับจ้างตกลงรักษาความลับของข้อมูลส่วนบุคคล และข้อมูลระบบของผู้ว่าจ้างทั้งหมด ห้ามนำไปเผยแพร่ หรือใช้งานโดยมิได้รับอนุญาตเป็นลายลักษณ์อักษร

ข้อ 6 บททั่วไป

6.1 สัญญานี้ให้ใช้บังคับตามกฎหมายไทย

6.2 ข้อพิพาทที่เกิดขึ้นให้ยุติด้วยการเจรจา หากไม่สำเร็จให้ส่งเรื่องต่อศาลที่มีเขตอำนาจในประเทศไทย

ลงชื่อ..... ผู้ว่าจ้าง

(.....)

ตำแหน่ง.....

ลงชื่อ.....

ผู้รับจ้าง (.....)

ตำแหน่ง.....

แนบท้าย: รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

วันที่ดำเนินการทดสอบ: [.....] ผู้ดำเนินการทดสอบ: [ชื่อบริษัท/บุคคลผู้รับจ้าง]

วัตถุประสงค์

เพื่อประเมินความมั่นคงปลอดภัยของระบบประมวลผลข้อมูลส่วนบุคคล โดยมุ่งเน้นที่การตรวจสอบการตั้งค่าระบบป้องกันไวรัส การอัปเดตฐานข้อมูลมัลแวร์ และการจัดการภัยคุกคามไซเบอร์

ขอบเขต

- ตรวจสอบการติดตั้งและอัปเดตโปรแกรมป้องกันไวรัสในเซิร์ฟเวอร์หลักและเครื่องลูกข่าย
- วิเคราะห์ช่องโหว่ระบบที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (รวมถึงบริการฐานข้อมูล, ระบบจัดเก็บ, ระบบคลาวด์)
- การทดสอบเจาะระบบเบื้องต้น (Penetration Testing)

ผลการตรวจสอบ

- ระบบป้องกันไวรัสได้รับการอัปเดตฐานข้อมูลล่าสุด ณ วันที่ [....]
- การตั้งค่าให้สแกนระบบสำคัญมีความถี่ระดับรายวัน
- ไม่พบการติดมัลแวร์หรือเหตุการณ์ต้องสงสัย ณ เวลาทดสอบ

ข้อเสนอแนะ

- เพิ่มระบบแจ้งเตือนอัตโนมัติเมื่อพบมัลแวร์
- ทบทวนการกำหนดสิทธิ์การเข้าถึงของผู้ใช้งานระดับผู้ดูแลระบบ

ผู้จัดทำรายงาน

(ชื่อผู้ทดสอบ)

ตำแหน่ง.....

บริษัท/หน่วยงาน.....

วันที่จัดทำรายงาน: [.....]

9.9.8 มีการประเมินและแก้ไขช่องโหว่ของระบบสำคัญอย่างสม่ำเสมอ

สิ่งที่ต้องทำ: มีการประเมินและแก้ไขช่องโหว่ของระบบสำคัญอย่างสม่ำเสมอ และมีการทดสอบโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก

- หลักฐาน:** นโยบายการประเมินและแก้ไขช่องโหว่ของระบบที่ประมวลผลข้อมูลส่วนบุคคล
 สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล
 รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของบุคคลภายนอก
 รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของแผนกเทคโนโลยีสารสนเทศ
- สภาพบังคับ:** พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (5), ข้อ 5
- โทษทางปกครอง** อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการประเมินและแก้ไขช่องโหว่ของระบบประมวลผลข้อมูลส่วนบุคคล (ฉบับขยาย)

ชื่อเอกสาร: นโยบายการประเมินและแก้ไขช่องโหว่ของระบบประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์:

กำหนดแนวทางและความรับผิดชอบในการประเมินช่องโหว่ของระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

ป้องกันการละเมิดข้อมูลส่วนบุคคล และลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

สร้างมาตรฐานการดำเนินงานและเอกสารอ้างอิงสำหรับเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศและผู้ควบคุมข้อมูล

สอดคล้องกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 และ ประกาศ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4, 5

ขอบเขต:

ครอบคลุมทุกระบบสารสนเทศที่จัดเก็บ ประมวลผล หรือถ่ายโอนข้อมูลส่วนบุคคล รวมถึง:

ระบบจัดเก็บข้อมูลลูกค้า / ผู้ใช้บริการ

ระบบเงินเดือน / การบริหารบุคลากร

ระบบอีเมลและการสื่อสารภายในองค์กร

ระบบฐานข้อมูลสำคัญ เช่น ERP, CRM, HRIS

ระบบคลาวด์ และซอฟต์แวร์ที่ใช้บริการภายนอก

1. นโยบายสำคัญ (Expanded)

1.1 การสแกนและประเมินช่องโหว่

กำหนดให้ ดำเนินการสแกนช่องโหว่ ของระบบสำคัญอย่างน้อยทุก 6 เดือน

ใช้เครื่องมือสแกนอัตโนมัติและตรวจสอบด้วยมือเพื่อความแม่นยำ

ประเมินช่องโหว่ในมิติด้าน:

ความปลอดภัยของระบบเครือข่าย (Network Security)

การควบคุมสิทธิ์ผู้ใช้งาน (Access Control)

การเข้ารหัสข้อมูล (Data Encryption)

ช่องโหว่ด้านแอปพลิเคชัน (Application Vulnerabilities)

ความปลอดภัยของระบบคลาวด์และผู้ให้บริการภายนอก

1.2 การแก้ไขช่องโหว่ (Remediation)

จัดลำดับความสำคัญตาม **ระดับความเสี่ยง (Risk Rating)**: สูง / กลาง / ต่ำ

ดำเนินการแก้ไขทันทีสำหรับช่องโหว่ระดับสูง (High Risk)

จัดทำแผนการแก้ไข (Remediation Plan) สำหรับช่องโหว่ระดับกลางและต่ำ

บันทึกกระบวนการแก้ไขและวันที่ดำเนินการเป็นหลักฐาน

1.3 การทดสอบโดยผู้ตรวจสอบภายในและภายนอก

กำหนดให้มี **ผู้ตรวจสอบภายใน (Internal Auditor / IT Security Officer)**

จ้าง **บุคคลภายนอก (External Security Consultant / Penetration Testing Service)** อย่างน้อยปีละ 1 ครั้ง

ทดสอบทุกระบบสำคัญตาม **ขอบเขตและกรอบมาตรฐาน ISO 27001 / NIST / OWASP**

จัดทำรายงานผลการทดสอบและข้อเสนอแนะ พร้อมลงนามรับรอง

1.4 การจัดทำรายงานและจัดเก็บหลักฐาน

จัดทำ **รายงานการประเมินช่องโหว่** ระบุรายละเอียด:

วันที่ดำเนินการ

ระบบที่ประเมิน

ช่องโหว่ที่พบ พร้อมระดับความเสี่ยง

การแก้ไขและผลการตรวจสอบซ้ำ

จัดเก็บรายงานอย่างน้อย **5 ปี** หรือจนกว่าจะหมดอายุของระบบ

ใช้เอกสารเป็นหลักฐานเมื่อมีการตรวจสอบจากคณะกรรมการ PDPA

1.5 การทบทวนและปรับปรุงนโยบาย

ทบทวนและปรับปรุงนโยบายอย่างน้อย **ปีละ 1 ครั้ง**

ปรับปรุงตาม:

เทคโนโลยีใหม่ ๆ และช่องโหว่ที่ค้นพบ

การเปลี่ยนแปลงข้อกำหนดหรือประกาศใหม่ของ PDPA

บทเรียนจากการทดสอบระบบและเหตุการณ์ความปลอดภัยที่เกิดขึ้น

2. บทบาทและความรับผิดชอบ

ฝ่าย IT / Security Officer

ดำเนินการสแกนช่องโหว่ และจัดทำรายงาน

ติดตามการแก้ไขช่องโหว่และจัดเก็บหลักฐาน

ผู้ตรวจสอบภายใน

ตรวจสอบกระบวนการประเมินและแก้ไขช่องโหว่

รายงานผลให้ฝ่ายบริหาร

ผู้ตรวจสอบภายนอก

ทำ penetration test / vulnerability assessment

ให้คำแนะนำด้านมาตรการรักษาความปลอดภัย

ฝ่ายบริหาร

อนุมัติแผนการแก้ไขช่องโหว่

ตรวจสอบการดำเนินงานและรับรองรายงาน

3. กระบวนการดำเนินงาน (Process Flow)

Planning: กำหนดขอบเขตระบบและตารางการสแกน

Scanning: ดำเนินการสแกนช่องโหว่

Analysis: ประเมินความเสี่ยงและจัดลำดับความสำคัญ

Remediation: ดำเนินการแก้ไขและบันทึกหลักฐาน

Testing: ทดสอบระบบหลังการแก้ไข

Reporting: จัดทำรายงานสำหรับผู้บริหารและผู้ตรวจสอบ

Review: ทบทวนและปรับปรุงนโยบายและกระบวนการ

สัญญาจ้างบริการทดสอบความปลอดภัยระบบประมวลผลข้อมูลส่วนบุคคล

(Penetration Testing / Vulnerability Assessment)

เลขที่สัญญา: _____

วันที่ทำสัญญา: _____

สถานที่ทำสัญญา: _____

คู่สัญญา**ฝ่ายที่ 1 (ผู้ว่าจ้าง)**

ชื่อ: _____

ที่อยู่: _____

ตัวแทน: _____

ฝ่ายที่ 2 (ผู้รับจ้าง)

ชื่อ: _____

ที่อยู่: _____

ตัวแทน: _____

ทั้งสองฝ่ายตกลงทำสัญญานี้ภายใต้ข้อกำหนดและเงื่อนไขดังต่อไปนี้

ข้อ 1 วัตถุประสงค์ของสัญญา

ฝ่ายที่ 1 จ้างฝ่ายที่ 2 เพื่อดำเนินการ ทดสอบความมั่นคงปลอดภัยของระบบประมวลผลข้อมูลส่วนบุคคล (Penetration Testing / Vulnerability Assessment) เพื่อระบุช่องโหว่ของระบบและให้คำแนะนำเชิงปฏิบัติในการแก้ไข เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล และสอดคล้องกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 และ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 และ 5

ข้อ 2 ขอบเขตงาน (Scope of Work)**2.1 ระบบและพื้นที่ทดสอบ**

ฝ่ายที่ 2 ต้องดำเนินการทดสอบและประเมินความมั่นคงปลอดภัยของระบบประมวลผลข้อมูลส่วนบุคคลของฝ่ายที่ 1 ครอบคลุม:

ระบบจัดเก็บและประมวลผลข้อมูลลูกค้า / ผู้ใช้บริการ (Customer / User Data Management System)

ระบบเงินเดือนและทรัพยากรบุคคล (Payroll / Human Resource Information System)

ระบบบริหารความสัมพันธ์ลูกค้าและธุรกิจ (CRM / ERP)

ระบบอีเมลและเครือข่ายภายในองค์กร (Internal Email & Network Systems)

ระบบคลาวด์และซอฟต์แวร์ที่ใช้บริการจากผู้ให้บริการภายนอก (Cloud Services & Third-Party Software)

2.2 ประเภทการทดสอบและจำนวนครั้ง

การสแกนช่องโหว่แบบอัตโนมัติและด้วยมือ (Vulnerability Scanning & Manual Testing) อย่างน้อย ทุก 6 เดือน

การทดสอบเจาะระบบเชิงรุก (Penetration Testing) อย่างน้อย ปีละ 1 ครั้ง
สามารถกำหนดช่วงเวลาและเวลาที่แน่นอนร่วมกับฝ่ายที่ 1 ก่อนเริ่มงาน

2.3 การประเมินช่องโหว่ (Vulnerability Assessment) แยกตามด้าน

2.3.1 ความปลอดภัยของระบบเครือข่าย (Network Security)

ตรวจสอบ Firewall, VPN, การกำหนดสิทธิ์การเข้าถึงระบบ

ตรวจสอบช่องโหว่ที่สามารถเข้าถึงเครือข่ายภายในจากภายนอก

ทำ Testing ด้วยเครื่องมือเช่น Nessus, OpenVAS

2.3.2 การควบคุมสิทธิ์ผู้ใช้งาน (Access Control)

ตรวจสอบการกำหนด Role-Based Access Control

ตรวจสอบการเข้าถึงข้อมูลที่ไม่เกี่ยวข้องกับหน้าที่ (Unauthorized Access)

ตรวจสอบ Log การเข้าถึงและ Audit Trail

2.3.3 การเข้ารหัสข้อมูล (Data Encryption)

ตรวจสอบการเข้ารหัสข้อมูลทั้งขณะจัดเก็บและส่งผ่าน (Encryption at Rest / in Transit)

ตรวจสอบการใช้อัตราฐานเข้ารหัสที่เหมาะสม เช่น AES-256, TLS 1.2+

2.3.4 ความปลอดภัยของแอปพลิเคชัน (Application Security)

ตรวจสอบช่องโหว่ OWASP Top 10 เช่น SQL Injection, XSS, CSRF

ตรวจสอบ Input Validation และ Authentication / Session Management

2.3.5 ความปลอดภัยของระบบคลาวด์และผู้ให้บริการภายนอก (Cloud Security / Third-Party Risk)

ตรวจสอบสิทธิ์และการตั้งค่า Security Group

ตรวจสอบการจัดเก็บ Credential และ API Key

ประเมินความเสี่ยงจากผู้ให้บริการภายนอก

2.4 วิธีดำเนินการ (Methodology)

กำหนด แผนการทดสอบ (Test Plan) ร่วมกับฝ่ายที่ 1 ก่อนเริ่ม

ดำเนินการทดสอบตามช่วงเวลาและความถี่ที่ตกลง

บันทึกผลการทดสอบ และจัดทำ รายงานร่าง (Preliminary / Draft Report)

ฝ่ายที่ 1 ตรวจสอบและให้ข้อคิดเห็น

จัดทำ รายงานฉบับสมบูรณ์ (Final Report) พร้อมข้อเสนอแนะเชิงปฏิบัติ

ข้อ 3 ระยะเวลาและกำหนดการ

เริ่มต้นสัญญา: _____

สิ้นสุดสัญญา: _____

กำหนดการหลัก

Planning & Scoping: _____

Vulnerability Scanning: _____

Penetration Testing: _____

Draft Report: _____

Final Report พร้อมข้อเสนอแนะ: _____

ข้อ 4 ค่าตอบแทนและการชำระเงิน

ค่าบริการรวม: _____ บาท

ชำระเงินเป็นงวด:

งวด 1: 50% หลังลงนามสัญญา

งวด 2: 50% หลังส่ง Final Report และฝ่ายที่ 1 รับรอง

ข้อ 5 การรักษาความลับและการปกป้องข้อมูล

ข้อมูลทั้งหมดถือเป็นความลับและต้องไม่เปิดเผยต่อบุคคลภายนอกโดยไม่ได้รับอนุญาต

ต้องปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 และ ประกาศ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4(3) และ 5

รายงานผลการทดสอบถือเป็นทรัพย์สินของฝ่ายที่ 1

ข้อ 6 ความรับผิดชอบ

ฝ่ายที่ 2 รับผิดชอบต่อความถูกต้องและความครบถ้วนของรายงาน

ฝ่ายที่ 1 จัดให้ฝ่ายที่ 2 เข้าถึงระบบและสภาพแวดล้อมทดสอบตามขอบเขต

ฝ่ายที่ 2 ต้องรายงานช่องโหว่ระดับสูง (High Risk) ทันที

ข้อ 7 การยกเลิกสัญญา

ฝ่ายใดฝ่ายหนึ่งสามารถยกเลิกโดยแจ้งล่วงหน้าอย่างน้อย 30 วัน

ฝ่ายที่ 1 ชำระค่าบริการตามสัดส่วนงานที่ดำเนินแล้ว

ข้อ 8 เหตุผิดสัญญาและเบี้ยปรับ (Breach of Contract and Liquidated Damages)

8.1 เหตุผิดสัญญา

ฝ่ายใดฝ่ายหนึ่งละเมิดข้อกำหนดสัญญา เช่น
 ไม่ดำเนินการทดสอบตามจำนวนครั้งหรือช่วงเวลาที่ตกลง
 ไม่รายงานช่องโหว่ระดับสูงภายในเวลาที่กำหนด
 ละเมิดการรักษาความลับข้อมูล
 ฝ่ายที่ 1 ไม่จัดให้ฝ่ายที่ 2 เข้าถึงระบบตามขอบเขต
 ไม่ชำระเงินตามกำหนด

8.2 การแก้ไข

ฝ่ายที่ไม่ได้ละเมิดแจ้งลายลักษณ์อักษรและให้แก้ไขภายใน 15 วัน
 หากไม่แก้ไข ฝ่ายที่ไม่ได้ละเมิดสามารถเรียก เบี้ยปรับ ตามข้อ 8.3

8.3 เบี้ยปรับ (Liquidated Damages)

ล่าช้าในการรายงานช่องโหว่ระดับสูง: 0.5% ของค่าบริการรวมต่อวัน
 ไม่ดำเนินการตามจำนวนครั้งหรือช่วงเวลาที่กำหนด: 1% ของค่าบริการรวมต่อเหตุการณ์
 ละเมิดการรักษาความลับข้อมูล: 5% ของค่าบริการรวมต่อเหตุการณ์

รายงานการทดสอบความปลอดภัยระบบประมวลผลข้อมูลส่วนบุคคล (รายงานฉบับสมบูรณ์)

เลขที่รายงาน: []

วันที่จัดทำรายงาน: []

จัดทำโดย: [ชื่อผู้ตรวจสอบ / หน่วยงาน]

ผู้ว่าจ้าง: [ชื่อองค์กร]

สารบัญ

บทนำ (Introduction)

คำจำกัดความและคำศัพท์ทางเทคโนโลยี (Definitions & Technical Terms)

วัตถุประสงค์ของการทดสอบ (Objectives)

ขอบเขตการประเมิน (Scope of Assessment)

วิธีการทดสอบและระยะเวลา (Methodology & Testing Period)

ผลการทดสอบช่องโหว่ (ผลการประเมินความเสี่ยงและ Vulnerability Assessment Results)

การแก้ไขและปรับปรุง (Remediation & Mitigation)

การประเมินความเสี่ยง (Risk Evaluation)

ข้อเสนอแนะเชิงปฏิบัติ (Practical Recommendations)

การติดตามและตรวจสอบซ้ำ (Follow-up & Continuous Monitoring)

เอกสารแนบและหลักฐานประกอบ (Attachments & Evidence)

การรับรองรายงาน (Report Certification)

1. บทนำ (Introduction)

รายงานฉบับนี้จัดทำขึ้นเพื่อประเมินความมั่นคงปลอดภัยของ ระบบประมวลผลข้อมูลส่วนบุคคลของ บุคคลภายนอก (Third-Party Personal Data Processing System) โดยอ้างอิงตาม สัญญาจ้างบริการ ทดสอบความปลอดภัยระบบประมวลผลข้อมูลส่วนบุคคล (Data Protection System Security Testing Service Contract) ระหว่างผู้ว่าจ้าง (ฝ่ายที่ 1) และผู้รับจ้าง (ฝ่ายที่ 2)

เป้าหมายหลักของรายงานนี้คือ:

ตรวจสอบความมั่นคงปลอดภัยของระบบสำคัญที่จัดเก็บและประมวลผลข้อมูลส่วนบุคคล

ระบุช่องโหว่ (ช่องโหว่, Vulnerabilities) และความเสี่ยงด้านความปลอดภัยของข้อมูล

แนะนำแนวทางแก้ไขและปรับปรุงระบบให้สอดคล้องกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act B.E. 2562)

2. คำจำกัดความและคำศัพท์ทางเทคโนโลยี (Definitions & Technical Terms)

คำศัพท์	คำแปลไทย (Translation)	คำอธิบาย
Vulnerability	ช่องโหว่	จุดอ่อนหรือข้อบกพร่องในระบบที่สามารถถูกโจมตีหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
Penetration Testing	การทดสอบเจาะระบบ	กระบวนการทดสอบเพื่อจำลองการโจมตีระบบเพื่อค้นหาช่องโหว่
Vulnerability Scanning	การสแกนช่องโหว่	การตรวจสอบระบบโดยอัตโนมัติหรือด้วยมือเพื่อค้นหาจุดอ่อน
Network Security	ความปลอดภัยของระบบเครือข่าย	มาตรการและเทคนิคที่ใช้เพื่อป้องกันเครือข่ายจากการโจมตี
Application Security	ความปลอดภัยของแอปพลิเคชัน	การป้องกันช่องโหว่ในซอฟต์แวร์หรือเว็บไซต์
Access Control	การควบคุมสิทธิ์ผู้ใช้งาน	การกำหนดสิทธิ์ในการเข้าถึงระบบและข้อมูล

Data Encryption	การเข้ารหัสข้อมูล	การเปลี่ยนข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้โดยไม่ได้รับอนุญาต
Cloud Services	บริการคลาวด์	การใช้ซอฟต์แวร์หรือระบบเก็บข้อมูลที่อยู่บนเซิร์ฟเวอร์ภายนอก
Third-Party Risk	ความเสี่ยงจากผู้ให้บริการภายนอก	ความเสี่ยงที่เกิดจากการใช้บริการของบุคคลหรือบริษัทภายนอก
OWASP Top 10	รายการช่องโหว่แอปพลิเคชันยอดนิยม (Top 10 Web Application Vulnerabilities)	รายการช่องโหว่ด้านความปลอดภัยของเว็บแอปพลิเคชันที่สำคัญที่สุด 10 ประการ

3. วัตถุประสงค์ของการทดสอบ (Objectives)

ประเมินความมั่นคงปลอดภัยของระบบสำคัญที่จัดเก็บและประมวลผลข้อมูลส่วนบุคคล

ระบุและจำแนกช่องโหว่ (Vulnerability) ตามระดับความรุนแรง (สูง / กลาง / ต่ำ, High / Medium / Low)

ตรวจสอบการเข้ารหัสข้อมูล (Data Encryption), การกำหนดสิทธิ์การเข้าถึง (Access Control) และระบบตรวจสอบการใช้งาน (Audit Trail)

เสนอแนวทางแก้ไขเชิงปฏิบัติสำหรับผู้ว่าจ้าง

4. ขอบเขตการประเมิน (Scope of Assessment)

4.1 ระบบและพื้นที่ทดสอบ

ระบบจัดเก็บและประมวลผลข้อมูลลูกค้า/ผู้ใช้บริการ (Customer / User Data Systems)

ระบบเงินเดือนและทรัพยากรบุคคล (Payroll / Human Resource Systems)

ระบบบริหารความสัมพันธ์ลูกค้าและการวางแผนทรัพยากรองค์กร (CRM / ERP Systems)

ระบบอีเมลและเครือข่ายภายในองค์กร (Email and Internal Network Systems)

ระบบคลาวด์และซอฟต์แวร์ของผู้ให้บริการภายนอก (Cloud / Third-Party Software Systems)

4.2 ประเภทการทดสอบและจำนวนครั้ง

การสแกนช่องโหว่ (Vulnerability Scanning / การสแกนช่องโหว่) – ทุก 6 เดือน

การทดสอบเจาะระบบเชิงรุก (Penetration Testing / การทดสอบเจาะระบบเชิงรุก) – ปีละ 1 ครั้ง

กำหนดช่วงเวลาและความถี่ร่วมกับฝ่ายผู้ว่าจ้าง

4.3 การประเมินช่องโหว่แยกตามด้าน (Vulnerability Assessment by Domain)

ด้าน	รายละเอียด	เครื่องมือ / วิธีการ	ระดับ ความเสี่ยง
ความปลอดภัย เครือข่าย (Network Security / ความ ปลอดภัยเครือข่าย)	ตรวจสอบไฟร์วอลล์ (Firewall), VPN (เครือข่ายส่วนตัวเสมือน), การกำหนดสิทธิ์การเข้าถึง (Access Control)	Nessus (เครื่องมือสแกน ช่องโหว่), OpenVAS (เครื่องมือสแกนช่องโหว่ อัตโนมัติ), ตรวจสอบด้วย ตนเอง (Manual Review)	สูง / กลาง / ต่ำ (High / Medium / Low)
การควบคุมสิทธิ์ (Access Control / การควบคุมสิทธิ์)	ตรวจสอบ Role-Based Access Control (การกำหนดสิทธิ์ตาม บทบาท), Unauthorized Access (การเข้าถึงโดยไม่ได้รับอนุญาต), Audit Trail (ตรวจสอบบันทึกการ ใช้งาน)	ตรวจสอบด้วยตนเอง (Manual), ตรวจสอบ Log	สูง / กลาง / ต่ำ (High / Medium / Low)
การเข้ารหัสข้อมูล (Data Encryption / การเข้ารหัส ข้อมูล)	ตรวจสอบการเข้ารหัสข้อมูลขณะ จัดเก็บ (Encryption at Rest) และส่งผ่าน (Encryption in Transit), ใช้อัลกอริทึม AES-256, TLS 1.2+	ตรวจสอบด้วยตนเอง (Manual), Pen Test	สูง / กลาง / ต่ำ (High / Medium / Low)
ความปลอดภัยแอป พลิเคชัน (Application Security / ความ ปลอดภัยแอปพลิเคชัน)	ตรวจสอบ OWASP Top 10 (ช่อง โหว่เว็บยอดนิยม), SQL Injection (ช่องโหว่การโจมตีฐานข้อมูล), XSS (Cross-Site Scripting / การโจมตี แบบฝังสคริปต์), CSRF (Cross- Site Request Forgery / การ โจมตีแบบปลอมคำขอ), Authentication / Session Management (การตรวจสอบ ตัวตนและจัดการเซสชัน)	ตรวจสอบด้วยตนเอง (Manual Testing), ใช้ สแกนเนอร์อัตโนมัติ (Automated Scanner)	สูง / กลาง / ต่ำ (High / Medium / Low)
ระบบคลาวด์และผู้ ให้บริการภายนอก (Cloud / Third- Party Risk / ความ	ตรวจสอบ Security Group (กลุ่ม ความปลอดภัย), Credential Management (การจัดการบัญชี ผู้ใช้งาน), API Key (รหัสคีย์ API),	ตรวจสอบด้วยตนเอง (Manual Review), Pen Test	สูง / กลาง / ต่ำ (High / Medium / Low)

เสี่ยงคลาวด์และผู้ให้บริการภายนอก)	Third-Party Risk (ความเสี่ยงจากผู้ให้บริการภายนอก)		

5. วิธีการทดสอบและระยะเวลา (Methodology & Testing Period)

จัดทำแผนการทดสอบร่วมกับผู้ว่าจ้าง (Test Plan / แผนการทดสอบ)

ดำเนินการตามตารางเวลาที่กำหนดและบันทึกผลใน Preliminary Report (รายงานเบื้องต้น)

ผู้ว่าจ้างตรวจสอบและให้ข้อคิดเห็น

จัดทำ Final Report (รายงานฉบับสมบูรณ์) พร้อมข้อเสนอแนะเชิงปฏิบัติ

ระยะเวลา: [ระบุช่วงเวลา เช่น มกราคม – เมษายน 2568]

6. ผลการทดสอบช่องโหว่ (Vulnerability Assessment Results / ผลการประเมินความเสี่ยงและช่องโหว่)

6.1 การประเมินความเสี่ยงและช่องโหว่ (Risk & Vulnerability Assessment)

ระบุช่องโหว่แต่ละระบบตามความรุนแรง (Severity / ระดับความรุนแรง) และแนวทางแก้ไข (Mitigation / การแก้ไข)

ตัวอย่าง:

ช่องโหว่ SQL Injection ในระบบ CRM → แนะนำแก้ไขโค้ดตรวจสอบค่าป้อนเข้า (Input Validation / การตรวจสอบข้อมูลป้อนเข้า)

API Key บนคลาวด์ไม่ได้เข้ารหัส → แนะนำใช้ Secret Management System (ระบบจัดการความลับ)

6.2 การประเมินการเข้ารหัสและการเข้าถึง (Data Encryption & Access Control Assessment)

ตรวจสอบการเข้ารหัสข้อมูลทั้งที่จัดเก็บ (Encryption at Rest) และส่งผ่าน (Encryption in Transit)

ตรวจสอบการกำหนดสิทธิ์และการจัดการบัญชีผู้ใช้งาน (Access Control & User Management)

ตรวจสอบระบบ Audit Trail (บันทึกตรวจสอบการใช้งาน) ว่าทำงานครบถ้วน

6.3 การทดสอบโดยผู้ตรวจสอบภายในและภายนอก (Internal & External Testing)

Internal Audit (ตรวจสอบภายใน): ดำเนินการตามแผนการทดสอบและบันทึกผล

External Pen Test (ทดสอบเจาะระบบภายนอก): ตรวจสอบระบบสำคัญปีละ 1 ครั้ง พร้อมข้อเสนอแนะแนวทางแก้ไข

7. การแก้ไขและปรับปรุง (Remediation & Mitigation / การแก้ไขและลดความเสี่ยง)

ช่องโหว่ระดับสูง (High Severity Vulnerabilities) แก้ไขทันที

ช่องโหว่ระดับกลาง/ต่ำ (Medium / Low Vulnerabilities) มีแผนการแก้ไขและติดตาม
 แนะนำ Patch Management (การจัดการแพตช์ซอฟต์แวร์) และ System Update (การปรับปรุง
 ระบบ) สม่ำเสมอ
 ตรวจสอบผลการแก้ไขและปรับปรุงช่องโหว่ซ้ำๆ ครอบคลุม

8. การประเมินความเสี่ยง (Risk Evaluation / การประเมินความเสี่ยง)

ระบุ ความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk / ความเสี่ยงด้านความปลอดภัย) และ ความ
 เสี่ยงด้าน PDPA (PDPA Compliance Risk / ความเสี่ยงด้านการปฏิบัติตาม PDPA)
 ประเมินผลกระทบต่อธุรกิจและข้อมูลส่วนบุคคล
 กำหนด ระดับความเสี่ยง (High / Medium / Low / สูง / กลาง / ต่ำ)

9. ข้อเสนอแนะเชิงปฏิบัติ (Practical Recommendations / ข้อเสนอแนะเชิงปฏิบัติ)

ทำ Vulnerability Scanning (การสแกนช่องโหว่) ทุก 6 เดือน
 Penetration Test (การทดสอบเจาะระบบเชิงรุก) ปีละ 1 ครั้ง โดยผู้ตรวจสอบภายนอก
 อัปเดตระบบเข้ารหัส (Data Encryption Update) และแพตช์ซอฟต์แวร์ (Software Patch)
 จัดทำ Audit Trail (ระบบบันทึกตรวจสอบการใช้งาน) และตรวจสอบการเข้าถึงข้อมูล (Access Review)
 ฝึกอบรมพนักงานเกี่ยวกับ PDPA (PDPA Awareness Training) และ Security Awareness (การสร้าง
 ความตระหนักรู้ด้านความปลอดภัย)
 จัดทำ Incident Response Plan (แผนตอบสนองเหตุการณ์) และ Disaster Recovery Plan (แผนฟื้นฟู
 ระบบหลังภัยพิบัติ)

10. การติดตามและตรวจสอบซ้ำ (Follow-up & Continuous Monitoring / การติดตามและ ตรวจสอบต่อเนื่อง)

ทำ Internal Audit (ตรวจสอบภายใน) และติดตามผลการแก้ไขทุก 3 เดือน
 ทดสอบระบบสำคัญซ้ำเพื่อยืนยันการแก้ไขช่องโหว่
 จัดทำ Follow-up Report (รายงานติดตามผล) และปรับปรุงระบบอย่างต่อเนื่อง

11. เอกสารแนบและหลักฐานประกอบ (Attachments & Evidence / เอกสารแนบและหลักฐาน ประกอบ)

ตารางช่องโหว่ (Vulnerability Matrix / ตารางช่องโหว่)

Preliminary / Draft Report (รายงานเบื้องต้น)

Log การเข้าถึงระบบ (Access Log / บันทึกการเข้าถึงระบบ) และผลการตรวจสอบ Audit Trail

หลักฐานการแก้ไขช่องโหว่ (Remediation Evidence / หลักฐานการแก้ไขช่องโหว่)

12. การรับรองรายงาน (Report Certification / การรับรองรายงาน)

รายงานฉบับนี้จัดทำขึ้นตาม มาตรฐานสากล (International Standards / มาตรฐานสากล) และยืนยันว่าการทดสอบเป็นไปตามข้อตกลงในสัญญา

ผู้จัดทำรายงาน / ผู้ตรวจสอบภายใน (Internal Auditor / ผู้ตรวจสอบภายใน):

ลงชื่อ: _____

ชื่อ: _____

ตำแหน่ง: _____

วันที่: _____

ผู้ตรวจสอบภายนอก / ที่ปรึกษาความปลอดภัย (External Security Consultant / ผู้ตรวจสอบภายนอก):

ลงชื่อ: _____

ชื่อ: _____

ตำแหน่ง: _____

วันที่: _____

ผู้ว่าจ้าง (Client / ผู้ว่าจ้าง):

ลงชื่อ: _____

ชื่อ: _____

ตำแหน่ง: _____

วันที่: _____

รายงานการประเมินช่องโหว่ระบบประมวลผลข้อมูลส่วนบุคคล (Vulnerability Assessment Report – Personal Data Processing System)

1. คำอธิบายศัพท์ด้านเทคโนโลยี

คำศัพท์	คำแปลไทย (Translation)	คำอธิบาย
Vulnerability	ช่องโหว่	จุดอ่อนหรือข้อบกพร่องในระบบที่สามารถถูกโจมตีหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
Penetration Testing	การทดสอบเจาะระบบ	กระบวนการทดสอบเพื่อจำลองการโจมตีระบบเพื่อค้นหาช่องโหว่
Vulnerability Scanning	การสแกนช่องโหว่	การตรวจสอบระบบโดยอัตโนมัติหรือด้วยมือเพื่อค้นหาจุดอ่อน
Network Security	ความปลอดภัยของระบบเครือข่าย	มาตรการและเทคนิคที่ใช้เพื่อป้องกันเครือข่ายจากการโจมตี
Application Security	ความปลอดภัยของแอปพลิเคชัน	การป้องกันช่องโหว่ในซอฟต์แวร์หรือเว็บไซต์
Access Control	การควบคุมสิทธิ์ผู้ใช้งาน	การกำหนดสิทธิ์ในการเข้าถึงระบบและข้อมูล
Data Encryption	การเข้ารหัสข้อมูล	การเปลี่ยนข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้โดยไม่ได้รับอนุญาต
Cloud Services	บริการคลาวด์	การใช้ซอฟต์แวร์หรือระบบเก็บข้อมูลที่อยู่บนเซิร์ฟเวอร์ภายนอก
Third-Party Risk	ความเสี่ยงจากผู้ให้บริการภายนอก	ความเสี่ยงที่เกิดจากการใช้บริการของบุคคลหรือบริษัทภายนอก
OWASP Top 10	รายการช่องโหว่แอปพลิเคชันยอดนิยม (Top 10 Web Application Vulnerabilities)	รายการช่องโหว่ด้านความปลอดภัยของเว็บแอปพลิเคชันที่สำคัญที่สุด 10 ประการ

2. ตารางประเมินช่องโหว่ (Vulnerability Assessment Table)

ลำดับ	ชื่อช่องโหว่ (Vulnerability Name)	ประเภทช่องโหว่ (Vulnerability Type)	ระบบที่พบ (Affected System)	ระดับความรุนแรง (Severity Level)	รายละเอียด (Description)	แนวทางการแก้ไข (Remediation)	ผู้รับผิดชอบ (Responsible)	สถานะ (Status)	หมายเหตุ (Remarks)

1	SQL Injection	ช่องโหว่ด้านแอปพลิเคชัน (Application Vulnerability)	CRM	สูง (High)	ผู้โจมตีสามารถส่งคำสั่ง SQL เพื่อเข้าถึงข้อมูลส่วนบุคคล	ตรวจสอบ Input Validation และใช้ Prepared Statement	ทีมพัฒนาแอปพลิเคชัน	Completed	ตรวจสอบซ้ำหลังแก้ไขเรียบร้อยแล้ว
2	รหัสผ่านอ่อน (Weak Password Policy)	การควบคุมสิทธิ์ผู้ใช้งาน (Access Control Weakness)	HR / Payroll	กลาง (Medium)	นโยบายรหัสผ่านไม่ซับซ้อน	กำหนดรหัสผ่านขั้นต่ำ 12 ตัวอักษร มีตัวเลข ตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก และสัญลักษณ์	ฝ่าย IT Security	In Progress	รีเซ็ตรหัสผ่านทันที
3	ข้อมูลส่งผ่านไม่ได้เข้ารหัส (Unencrypted Data in Transit)	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Cloud Services	สูง (High)	ข้อมูลส่งผ่านเครือข่ายไม่ได้เข้ารหัส	ใช้ TLS 1.2+ / HTTPS	ฝ่าย IT Network	Pending	ทดสอบซ้ำหลังแก้ไข
4	กำแพงไฟร์วอลล์ขาด (Missing Firewall Rule)	ความปลอดภัยเครือข่าย (Network Security Weakness)	Internal Network	กลาง (Medium)	บางพอร์ตเปิดไม่จำเป็น	ปรับปรุง Firewall Rule	ฝ่าย IT Network	In Progress	ทำรายการพอร์ตทั้งหมด
5	XSS (Cross-Site Scripting)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Customer Data System	สูง (High)	ฝั่งสคริปต์เพื่อขโมย Session	Input Validation และ Output Encoding	ทีมพัฒนาแอป	Completed	ตรวจสอบซ้ำ Penetration Testing
6	รหัสผ่านเริ่มต้น (Default Credentials)	การควบคุมสิทธิ์ (Access Control Weakness)	Cloud Admin Panel	สูง (High)	รหัสผ่านเริ่มต้นยังใช้งาน	เปลี่ยนรหัสผ่านเริ่มต้น + MFA	ฝ่าย IT Cloud	Completed	ตรวจสอบเป็นระยะทุก 6 เดือน

7	เก็บ API Key ไม่ปลอดภัย (Insecure API Key Storage)	ความเสี่ยงผู้ให้บริการภายนอก (Third-Party Risk)	Cloud Services	กลาง (Medium)	API Key ถูกเก็บในไฟล์ Config	ใช้ Environment Variables + เซิร์ฟเวอร์	ฝ่าย IT Cloud	In Progress	แจ้งทีมพัฒนาภายนอก
8	ขาด Role-Based Access Control	การควบคุมสิทธิ์ผู้ใช้งาน (Access Control Weakness)	HR / Payroll	สูง (High)	ผู้ใช้งานเข้าถึงข้อมูลไม่เกี่ยวข้อง	กำหนด RBAC และตรวจสอบ Log	ฝ่าย IT Security	In Progress	ตรวจสอบข้อบกพร่องไตรมาส
9	Authentication Weakness	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	CRM / ERP	สูง (High)	Session Management มีช่องโหว่	ปรับปรุงระบบ Authentication / Session Timeout	ทีมพัฒนาแอป	Pending	ทดสอบ Penetration Testing รอบต่อไป
10	Unencrypted Data at Rest	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Customer Data System	สูง (High)	ข้อมูลสำคัญไม่เข้ารหัส	ใช้ AES-256 และ Key Management	ฝ่าย IT Database	In Progress	ตรวจสอบข้อบกพร่องหลังปรับปรุง
11	CSRF (Cross-Site Request Forgery)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	CRM	สูง (High)	ผู้โจมตีสามารถทำคำสั่งแทนผู้ใช้	ใช้ Anti-CSRF Token	ทีมพัฒนาแอป	Pending	ตรวจสอบข้อบกพร่อง
12	การตั้งค่า S3 Bucket ไม่ปลอดภัย (Insecure S3 Bucket Configuration)	ความเสี่ยงผู้ให้บริการภายนอก (Third-Party Risk)	Cloud Storage	สูง (High)	ข้อมูลสำคัญเปิดสาธารณะ	ปรับสิทธิ์ Bucket และตรวจสอบ ACL	ฝ่าย IT Cloud	In Progress	ทดสอบสแกนใหม่
13	การสำรองข้อมูลไม่เข้ารหัส (Unencrypted Backup)	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Database Backup System	สูง (High)	ข้อมูลสำรองไม่ได้เข้ารหัส	เข้ารหัส Backup ด้วย AES-256	ฝ่าย IT Database	Pending	ตรวจสอบเป็นประจำทุกเดือน

	pted Backup)	Encryption Weakness)							
14	ช่องโหว่ Open Redirect	ช่องโหว่ แอปพลิเคชัน (Application Vulnerability)	Websit e	กลาง (Medium)	ผู้โจมตี สามารถ เปลี่ยน URL ปลายทาง	ตรวจสอบ URL Redirection และ Validation	ทีมพัฒนา แอป	Pending	ตรวจสอบซ้ำทุก Release
15	ขาดการ บันทึก Log การเข้าถึง (Missing Access Log)	การควบคุม สิทธิ์ (Access Control Weakness)	HR System	สูง (High)	ไม่สามารถ ตรวจสอบผู้ เข้าถึงได้	เปิดใช้ Logging และ Audit Trail	ฝ่าย IT Security	In Progress	ตรวจสอบ ทุก เดือน
16	Outdated Software	ช่องโหว่ แอปพลิเคชัน (Application Vulnerability)	CRM / ERP / HR	สูง (High)	ซอฟต์แวร์ ล้าสมัยมีช่อง โหว่	อัปเดต Patch ล่าสุด	ฝ่าย IT Support	In Progress	สร้าง รายการ Patch Manage ment
17	Port Scanning เปิดเผย พอร์ต (Open Ports)	ความปลอดภัย เครือข่าย (Network Security Weakness)	Internal Networ k	กลาง (Medium)	พอร์ตที่ไม่ จำเป็นเปิดอยู่	ปิดพอร์ตไม่ ใช้	ฝ่าย IT Network	In Progress	ตรวจสอบ ทุก 6 เดือน
18	การเข้าถึง ผ่าน VPN ไม่เข้ารหัส (Unsecured VPN Access)	ความปลอดภัย เครือข่าย (Network Security Weakness)	Remote Access	สูง (High)	การเชื่อมต่อ VPN ไม่ เข้ารหัส	เปิดใช้ VPN Protocol ที่ เข้ารหัส	ฝ่าย IT Network	Pending	ทดสอบ ซ้ำ
19	การจัดการ Session ไม่ปลอดภัย (Insecure Session Management)	ช่องโหว่ แอปพลิเคชัน (Application Vulnerability)	CRM / Websit e	สูง (High)	Session ID เดียวกัน สามารถใช้ได้ หลายคน	ใช้ Session Expiration และ Secure Cookie	ทีมพัฒนา แอป	In Progress	ตรวจสอบ หลัง แก้ไข

20	การตั้งค่า Database Privilege ไม่เหมาะสม	การควบคุมสิทธิ์ผู้ใช้งาน (Access Control Weakness)	Database	สูง (High)	ผู้ใช้มีสิทธิ์มากเกินไป	กำหนด Role และ Privilege	ฝ่าย IT Database	Pending	ตรวจสอบรายเดือน
21	การตรวจสอบ SSL Certificate ไม่ครบ	ความปลอดภัยเครือข่าย (Network Security Weakness)	Cloud Services / Website	กลาง (Medium)	Certificate หมดอายุ หรือไม่ถูกต้อง	ตรวจสอบและต่ออายุ SSL	ฝ่าย IT Network	Pending	ตรวจสอบทุก 3 เดือน
22	การเข้าถึง Cloud Admin Console ไม่ปลอดภัย	ความเสี่ยงผู้ให้บริการภายนอก (Third-Party Risk)	Cloud Admin Panel	สูง (High)	ไม่ใช้ MFA / Weak Password	เปิดใช้งาน MFA และปรับรหัสผ่าน	ฝ่าย IT Cloud	In Progress	ตรวจสอบเป็นระยะ
23	การเข้าถึงข้อมูล HR จากพนักงานทั่วไป	การควบคุมสิทธิ์ผู้ใช้งาน (Access Control Weakness)	HR System	สูง (High)	ข้อมูลเงินเดือนถูกเข้าถึงโดยไม่ได้รับอนุญาต	กำหนด Role-Based Access Control	ฝ่าย IT Security	In Progress	ตรวจสอบ Audit Trail
24	Vulnerable Third-Party								
26	การสำรองข้อมูลไม่สมบูรณ์ (Incomplete Backup)	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Database Backup	สูง (High)	ข้อมูลสำรองบางส่วนไม่ครบ	ตรวจสอบ Backup Policy และทำ Full Backup	ฝ่าย IT Database	In Progress	ตรวจสอบทุกเดือน
27	DNS Spoofing	ความปลอดภัยเครือข่าย (Network Security Weakness)	Internal Network	สูง (High)	ผู้โจมตีเปลี่ยน DNS Response	ใช้ DNSSEC และตรวจสอบ DNS Config	ฝ่าย IT Network	Pending	ทดสอบ Penetration Testing
28	การเข้าถึงไม่ถูกต้องจากภายนอก (Unauthorized)	การควบคุมสิทธิ์ผู้ใช้งาน (Access Control Weakness)	VPN / Remote Access	สูง (High)	ผู้โจมตีสามารถเข้าระบบ	ใช้ MFA + ตรวจสอบ Log การเข้าถึง	ฝ่าย IT Security	In Progress	ตรวจสอบเป็นประจำ

	Remote Access)								
29	HTTP Security Header ขาด (Missing HTTP Security Headers)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Website	กลาง (Medium)	ไม่มีการตั้งค่า Content-Security-Policy / X-Frame-Options	ปรับตั้งค่า Security Headers	ทีมพัฒนาแอป	Pending	ตรวจสอบทุก Release
30	การตั้งค่า Cloud Storage ไม่ถูกต้อง (Misconfigured Cloud Storage)	ความเสี่ยงผู้ให้บริการภายนอก (Third-Party Risk)	Cloud Services	สูง (High)	Bucket หรือ Storage Public	ปรับสิทธิ์การเข้าถึง และ Encrypt Data	ฝ่าย IT Cloud	In Progress	ตรวจสอบทุก 3 เดือน
31	การใช้ซอฟต์แวร์ที่ล้าสมัย (Legacy Software)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	CRM / ERP	สูง (High)	เวอร์ชันเก่ามีช่องโหว่	อัปเดต Patch ล่าสุด	ฝ่าย IT Support	In Progress	ทำ Patch Management
32	การโจมตีแบบ Man-in-the-Middle (MITM Attack)	ความปลอดภัยเครือข่าย (Network Security Weakness)	Internal / External Network	สูง (High)	การรับส่งข้อมูลถูกดัก	ใช้ Encryption / TLS และ VPN	ฝ่าย IT Network	Pending	ตรวจสอบทุกไตรมาส
33	การบันทึก Log ไม่ถูกต้อง (Incorrect Logging)	การควบคุมสิทธิ์ผู้ใช้งาน (Access Control Weakness)	HR / Payroll System	กลาง (Medium)	Log ไม่ครบ หรือถูกแก้ไข	ปรับปรุง Logging Policy และ Audit	ฝ่าย IT Security	In Progress	ตรวจสอบทุกเดือน
34	ขาด MFA (Multi-Factor Authentication)	การควบคุมสิทธิ์ผู้ใช้งาน (Access Control Weakness)	CRM / Cloud Admin	สูง (High)	ผู้ใช้สามารถ Login ด้วยรหัสผ่านเดียว	เปิดใช้งาน MFA	ฝ่าย IT Security	In Progress	ตรวจสอบทุกไตรมาส

35	การกำหนดสิทธิ์ FTP / SFTP ไม่ปลอดภัย	ความปลอดภัยเครือข่าย (Network Security Weakness)	File Server	กลาง (Medium)	ผู้ใช้ทั่วไปเข้าถึงไฟล์ได้	กำหนดสิทธิ์และเข้ารหัสข้อมูล	ฝ่าย IT Network	Pending	ตรวจสอบทุกเดือน
36	Buffer Overflow	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Internal Application	สูง (High)	โปรแกรมประมวลผลข้อมูลมีช่องโหว่	Patch Software และตรวจสอบ Code Review	ทีมพัฒนาแอป	In Progress	ตรวจสอบซ้ำ Penetration Testing
37	การเข้าถึงข้อมูลผู้ใช้โดย Admin ไม่จำกัด	การควบคุมสิทธิ์ใช้งาน (Access Control Weakness)	HR / Payroll System	สูง (High)	Admin สามารถเข้าถึงข้อมูลส่วนบุคคลทั้งหมด	RBAC และ Log การเข้าถึง	ฝ่าย IT Security	In Progress	ตรวจสอบทุกเดือน
38	Open Port 3306 (Database)	ความปลอดภัยเครือข่าย (Network Security Weakness)	Database Server	สูง (High)	พอร์ตเปิดไม่จำเป็น	ปิดพอร์ตที่ไม่ใช้งาน	ฝ่าย IT Network	Pending	ตรวจสอบทุก 6 เดือน
39	Cross-Site Script Inclusion (XSSI)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Website	กลาง (Medium)	การแสดงผล JavaScript จาก Domain อื่น	ใช้ Content Security Policy (CSP)	ทีมพัฒนาแอป	Pending	ตรวจสอบทุก Release
40	การตั้งค่า Email Server ไม่ปลอดภัย	ความปลอดภัยเครือข่าย (Network Security Weakness)	Email System	สูง (High)	SMTP ไม่มี TLS / SPAM Filter ไม่ทำงาน	เปิดใช้งาน TLS และ SPF / DKIM / DMARC	ฝ่าย IT Network	In Progress	ตรวจสอบทุกไตรมาส
41	การใช้ Third-Party Script ไม่ปลอดภัย	ความเสี่ยงผู้ให้บริการภายนอก (Third-Party Risk)	Website / CRM	กลาง (Medium)	Script มีช่องโหว่	ตรวจสอบและอัปเดต Script	ทีมพัฒนาแอป	Pending	ตรวจสอบทุก Release

42	Session ID ถูกเดาได้	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Website / CRM	สูง (High)	Session ID ใช้ Random น้อย	ปรับใช้ Secure Session Token	ทีมพัฒนาแอป	In Progress	ตรวจสอบ Penetration Testing
43	การตั้งค่า Firewall ไม่เหมาะสม	ความปลอดภัยเครือข่าย (Network Security Weakness)	Internal Network	สูง (High)	Rule ไม่สอดคล้อง Policy	ปรับ Firewall Rule ให้เหมาะสม	ฝ่าย IT Network	In Progress	ตรวจสอบทุก 6 เดือน
44	การเก็บ Log Password	การเข้ารหัสข้อมูล (Data Encryption Weakness)	HR / Payroll	สูง (High)	Password บันทึกใน Log	ปรับ Logging Policy ไม่เก็บ Password	ฝ่าย IT Security	Pending	ตรวจสอบทุก เดือน
45	Unpatched Web Server	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Website / CRM	สูง (High)	Server มีช่องโหว่	อัปเดต Patch ล่าสุด	ฝ่าย IT Support	In Progress	ตรวจสอบ Patch Management
46	การเข้าถึง Admin Panel ไม่จำกัด IP	ความปลอดภัยเครือข่าย (Network Security Weakness)	Cloud Admin	สูง (High)	Admin Panel เปิดให้เข้าจากทุก IP	จำกัด IP Access	ฝ่าย IT Cloud	Pending	ตรวจสอบทุก 3 เดือน
47	การจัดการ Key / Certificate ไม่ปลอดภัย	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Cloud / Internal	สูง (High)	Key และ Certificate เก็บไม่ปลอดภัย	ใช้ Key Management System	ฝ่าย IT Security	In Progress	ตรวจสอบทุก 6 เดือน
48	LDAP Injection	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	HR / Directory	สูง (High)	ผู้โจมตีสามารถโจมตี LDAP Query	Input Validation และ Prepared Statement	ทีมพัฒนาแอป	Pending	ตรวจสอบ Penetration Testing

49	การเข้าถึง File Server จากภายนอก ไม่ปลอดภัย	ความปลอดภัยเครือข่าย (Network Security Weakness)	File Server	สูง (High)	Port SMB เปิดให้เข้าภายนอก	ปิด Port / VPN Access	ฝ่าย IT Network	In Progress	ตรวจสอบทุกไตรมาส
50	Cross-Site Script Inclusion ใน Cloud App	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Cloud CRM / ERP	กลาง (Medium)	Script จาก Domain ภายนอกถูกเรียกใช้	ใช้ CSP และตรวจสอบ Script	ทีมพัฒนาแอป	Pending	ตรวจสอบทุก Release
51	การใช้รหัสผ่านอ่อน (Weak Passwords)	การควบคุมสิทธิ์ผู้ใช้งาน (Access Control Weakness)	Internal Systems	สูง (High)	ผู้ใช้งานตั้งรหัสผ่านง่ายเดาได้	บังคับใช้ Password Policy และ MFA	ฝ่าย IT Security	In Progress	ตรวจสอบทุกไตรมาส
52	การโจมตีแบบ SQL Injection	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Website / CRM	สูง (High)	ผู้โจมตีสามารถแก้ไข Query Database	ใช้ Prepared Statement และ Input Validation	ทีมพัฒนาแอป	Pending	ตรวจสอบ Penetration Testing
53	การเข้าถึงระบบโดยใช้ Token หมดอายุ	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Web Application	กลาง (Medium)	Token หมดอายุ	ปรับระบบให้ Token หมดอายุตาม Policy	ทีมพัฒนาแอป	Pending	ตรวจสอบทุก Release
54	การจัดการ Session ไม่เหมาะสม	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Web Application	สูง (High)	Session Fixation / Session Hijacking	ใช้ Secure Session Cookie / Session Timeout	ทีมพัฒนาแอป	In Progress	ตรวจสอบ Penetration Testing

55	ขาดการเข้ารหัสข้อมูลระหว่างส่ง (Unencrypted Data in Transit)	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Internal / Cloud Systems	สูง (High)	ข้อมูลส่งผ่าน HTTP ไม่ใช่ TLS	ใช้ HTTPS / TLS 1.2+	ฝ่าย IT Network	In Progress	ตรวจสอบทุกไตรมาส
56	การเข้าถึง API ไม่ปลอดภัย	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Cloud Services / ERP	สูง (High)	API ไม่มี Authentication	ใช้ OAuth2 / API Key และ Rate Limiting	ฝ่าย IT Cloud	Pending	ตรวจสอบทุก Release
57	ข้อมูลส่วนบุคคลถูกเก็บไม่ถูกต้อง	การเข้ารหัสข้อมูล (Data Encryption Weakness)	HR / Payroll	สูง (High)	Personal Data ไม่เข้ารหัส	Encrypt Data at Rest / Data Masking	ฝ่าย IT Security	In Progress	ตรวจสอบทุกเดือน
58	การโจมตี Cross-Site Request Forgery (CSRF)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Website / CRM	กลาง (Medium)	Request ปลอมสามารถถูกส่งโดยผู้โจมตี	ใช้ CSRF Token และตรวจสอบ Referer	ทีมพัฒนาแอป	Pending	ตรวจสอบทุก Release
59	การเข้าถึง Cloud Admin Panel โดยไม่จำกัด IP	ความปลอดภัยเครือข่าย (Network Security Weakness)	Cloud Services	สูง (High)	ผู้โจมตีเข้าถึง Admin Panel จากทุก IP	จำกัด IP และใช้ VPN Access	ฝ่าย IT Cloud	Pending	ตรวจสอบทุก 3 เดือน
60	Log File ถูกดัดแปลง	การควบคุมสิทธิ์ผู้ใช้งาน (Access Control Weakness)	HR / Payroll	สูง (High)	Log ไม่สามารถ Audit ได้	ใช้ Write-Once / Read-Many Logging และ Audit Trail	ฝ่าย IT Security	In Progress	ตรวจสอบทุกเดือน
61	การโจมตีแบบ	ความปลอดภัยเครือข่าย	VPN / Internal System	สูง (High)	ผู้โจมตีลองรหัสผ่านหลายครั้ง	ใช้ Account Lockout /	ฝ่าย IT Security	Pending	ตรวจสอบทุกไตรมาส

	Brute Force	(Network Security Weakness)				Rate Limiting			
62	ข้อมูลสำรองไม่ได้เข้ารหัส	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Database / Cloud Backup	สูง (High)	Backup ไม่มี การเข้ารหัส	ใช้ AES-256 / Encrypt Backup	ฝ่าย IT Database	In Progress	ตรวจสอบทุก 6 เดือน
63	Server Response Header Information Leak	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Website / CRM	กลาง (Medium)	Headerเปิดเผยข้อมูล Server	ปรับ Server Header Config	ทีมพัฒนาแอป	Pending	ตรวจสอบทุก Release
64	การเข้าถึง SMB / File Share จากภายนอก	ความปลอดภัยเครือข่าย (Network Security Weakness)	File Server	สูง (High)	Port เปิดให้เข้าภายนอก	ปิด Port / ใช้ VPN Access	ฝ่าย IT Network	In Progress	ตรวจสอบทุกไตรมาส
65	การใช้ Protocol ที่ไม่ปลอดภัย	ความปลอดภัยเครือข่าย (Network Security Weakness)	Internal / Cloud Systems	สูง (High)	ใช้ FTP / Telnet ไม่เข้ารหัส	ใช้ SFTP / SSH / TLS	ฝ่าย IT Network	Pending	ตรวจสอบทุก 6 เดือน
66	ขาดการ Patch OS / Software	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Server / Workstation	สูง (High)	ระบบเก่าไม่มี Patch ล่าสุด	Patch Management / Update Software	ฝ่าย IT Support	In Progress	ตรวจสอบทุกเดือน
67	ขาดการตรวจสอบ Security Group Cloud	ความเสี่ยงผู้ให้บริการภายนอก (Third-Party Risk)	Cloud Services	กลาง (Medium)	Security Group กว้างเกินไป	ตรวจสอบ Security Group / Principle of Least Privilege	ฝ่าย IT Cloud	Pending	ตรวจสอบทุก 3 เดือน
68	การจัดการ Key API	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Cloud Services / API	สูง (High)	API Key ถูกเก็บใน	ใช้ Environment	ทีมพัฒนาแอป	In Progress	ตรวจสอบทุก Release

	ไม่ ปลอดภัย	Encryption Weakness)			Source Code	Variables / Secret Managem ent			
69	Vulnerabl e Open Source Library	ช่องโหว่ แอปพลิเคชัน (Application Vulnerabili ty)	Websit e / CRM / ERP	กลาง (Mediu m)	Library มีช่อง โหว่	อัปเดต Library / ตรวจสอบ Dependen cy	ทีมพัฒนา แอป	Pending	ตรวจสอบ ทุก Release
70	การเข้าถึง ข้อมูลโดย ไม่ได้เข้า รหัสผ่าน Web Interface	การเข้ารหัส ข้อมูล (Data Encryption Weakness)	Internal / Cloud System s	สูง (High)	ข้อมูลสำคัญ ถูกส่งแบบ Plaintext	ใช้ HTTPS / TLS 1.2+	ฝ่าย IT Network	In Progress	ตรวจสอบ ทุกไทม์ มาส
71	การเก็บ รหัสผ่านใน ไฟล์ ข้อความ (Storing Password s in Plaintext Files)	การควบคุม สิทธิ์ผู้ใช้งาน (Access Control Weakness)	ระบบ เงินเดือน (Payroll System)	สูง (High)	รหัสผ่านผู้ใช้ ถูกเก็บแบบไม่ เข้ารหัส	ใช้การ เข้ารหัส รหัสผ่าน (Password Hashing) เช่น bcrypt	ฝ่าย IT Security	In Progress	ตรวจสอบ ทุก 3 เดือน
72	ขาดการ ตรวจสอบ สิทธิ์ผู้เข้า (Missing User Authentic ation Verificatio n)	การควบคุม สิทธิ์ผู้ใช้งาน (Access Control Weakness)	ระบบ CRM (CRM System)	สูง (High)	ผู้ใช้สามารถ เข้าถึงข้อมูล ของคนอื่นได้	ใช้ Role- Based Access Control และ ตรวจสอบ สิทธิ์ผู้ใช้	ทีมพัฒนา แอป (Applicatio n Dev Team)	Pending	ตรวจสอบ Penetra tion Test
73	การโจมตี แบบ Cross-Site Scripting (XSS)	ช่องโหว่ แอปพลิเคชัน (Application Vulnerabili ty)	เว็บไซต์ (Websit e)	สูง (High)	ผู้โจมตี สามารถฝัง สคริปต์ในเว็บ เพจ	ใช้ Input Validation และ Output Encoding	ทีมพัฒนา แอป	Pending	ตรวจสอบ ทุก Release

74	การใช้รหัสผ่านซ้ำ (Password Reuse)	การควบคุมสิทธิ์ผู้ใช้งาน (Access Control Weakness)	ระบบทั้งหมด (All Systems)	กลาง (Medium)	ผู้ใช้ใช้รหัสผ่านเดียวกันในหลายระบบ	บังคับใช้ Password Policy ไม่ซ้ำ	ฝ่าย IT Security	Pending	ตรวจสอบทุก 6 เดือน
75	การส่งข้อมูลสำคัญแบบไม่เข้ารหัส (Unencrypted Data Transmission)	การเข้ารหัสข้อมูล (Data Encryption Weakness)	ระบบอีเมลและเครือข่าย (Email & Network System)	สูง (High)	ข้อมูลส่งผ่าน HTTP / Non-TLS	ใช้ HTTPS / TLS 1.2+	ฝ่าย IT Network	In Progress	ตรวจสอบไตรมาส
76	การจัดการ Session ไม่ปลอดภัย (Insecure Session Management)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	เว็บไซต์ / CRM	สูง (High)	Session สามารถถูก Hijack	ใช้ Secure Cookie, Session Timeout	ทีมพัฒนาแอป	Pending	ตรวจสอบ Penetration Test
77	การเปิดเผยข้อมูลใน Header ของ Server (Server Header Information Disclosure)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	เว็บไซต์	กลาง (Medium)	Header เปิดเผยข้อมูลเวอร์ชัน Server	ปรับ Server Configuration	ทีมพัฒนาแอป	Pending	ตรวจสอบทุก Release
78	การโจมตีแบบ Cross-Site Request Forgery (CSRF)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	เว็บไซต์	กลาง (Medium)	Request ปลอมสามารถถูกส่ง	ใช้ CSRF Token / ตรวจสอบ Referer	ทีมพัฒนาแอป	Pending	ตรวจสอบทุก Release

79	การเข้าถึง API โดยไม่จำกัด (Unrestricted API Access)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Cloud Service / ERP	สูง (High)	API ไม่มี Authentication	ใช้ OAuth2 / API Key และ Rate Limiting	ฝ่าย IT Cloud	Pending	ตรวจสอบทุก Release
80	การเก็บข้อมูลสำรองไม่เข้ารหัส (Unencrypted Backup)	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Database / Cloud Backup	สูง (High)	Backup ไม่เข้ารหัส	ใช้ AES-256 / Encrypt Backup	ฝ่าย IT Database	In Progress	ตรวจสอบทุก 6 เดือน
81	การใช้ Protocol ที่ไม่ปลอดภัย (Insecure Protocol Usage)	ความปลอดภัยเครือข่าย (Network Security Weakness)	Internal / Cloud System	สูง (High)	ใช้ FTP / Telnet ไม่เข้ารหัส	เปลี่ยนเป็น SFTP / SSH / TLS	ฝ่าย IT Network	Pending	ตรวจสอบทุกไตรมาส
82	ขาดการ Patch ระบบปฏิบัติการ (Missing OS / Software Patch)	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Server / Workstation	สูง (High)	ระบบเก่าไม่มี Patch ล่าสุด	ใช้ Patch Management / Update Software	ฝ่าย IT Support	In Progress	ตรวจสอบทุกเดือน
83	การตั้งค่า Security Group Cloud กว้างเกินไป (Over-permissive Cloud Security Group)	ความเสี่ยงผู้ให้บริการภายนอก (Third-Party Risk)	Cloud Services	กลาง (Medium)	Security Group เปิดกว้าง	Principle of Least Privilege	ฝ่าย IT Cloud	Pending	ตรวจสอบทุก 3 เดือน
84	การจัดเก็บ API Key ไม่	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Cloud Services / API	สูง (High)	API Key อยู่ใน Source Code	ใช้ Environment	ทีมพัฒนาแอป	In Progress	ตรวจสอบทุก Release

	ปลอดภัย (Insecure API Key Storage)	Encryption Weakness)				Variables / Secret Managem ent			
85	Library Open Source มี ช่องโหว่ (Vulnerab le Open Source Library)	ช่องโหว่ แอปพลิเคชัน (Application Vulnerabili ty)	Websit e / CRM / ERP	กลาง (Mediu m)	Library ไม่อัปเดต	ตรวจสอบ Dependen cy / Update Library	ทีมพัฒนา แอป	Pending	ตรวจสอบ ทุก Release
86	การเข้าถึง ข้อมูลแบบ Plaintext ผ่าน Web Interface	การเข้ารหัส ข้อมูล (Data Encryption Weakness)	Internal / Cloud System	สูง (High)	ข้อมูลสำคัญ ส่งแบบ Plaintext	ใช้ HTTPS / TLS	ฝ่าย IT Network	In Progress	ตรวจสอบ ทุกไตรมาส
87	การโจมตี แบบ Man- in-the- Middle (MITM)	ความ ปลอดภัย เครือข่าย (Network Security Weakness)	Internal / Cloud System	สูง (High)	ผู้โจมตีดักจับ Traffic	ใช้ TLS / VPN / Network Segmentat ion	ฝ่าย IT Network	Pending	ตรวจสอบ ทุกไตรมาส
88	การโจมตี Denial-of- Service (DoS)	ความ ปลอดภัย เครือข่าย (Network Security Weakness)	Cloud / Internal System	สูง (High)	ระบบถูกโจมตี ทำให้ใช้งาน ไม่ได้	ใช้ Firewall / Rate Limiting / Load Balancer	ฝ่าย IT Network	In Progress	ตรวจสอบ ทุกไตรมาส
89	ข้อมูล Log เก็บไม่ ครบถ้วน (Incompl ete Log Retention)	การควบคุม สิทธิ์ผู้ใช้งาน (Access Control Weakness)	HR / Payroll / Server	กลาง (Mediu m)	Log ไม่ ครบถ้วน Audit Trail ไม่สมบูรณ์	ใช้ Write- Once / Read- Many Logging และ Audit Trail	ฝ่าย IT Security	In Progress	ตรวจสอบ ทุก เดือน
90	การใช้ รหัสผ่าน Default	การควบคุม สิทธิ์ผู้ใช้งาน (Access Control Weakness)	Networ k Device / Server	สูง (High)	อุปกรณ์ยังใช้ รหัสผ่าน Default	เปลี่ยน รหัสผ่าน Default / Password Policy	ฝ่าย IT Network	In Progress	ตรวจสอบ ทุก 6 เดือน

91	การเข้าถึงระบบจากอุปกรณ์ที่ไม่ปลอดภัย (Insecure Device Access)	ความปลอดภัยเครือข่าย (Network Security Weakness)	VPN / Remote Access	กลาง (Medium)	อุปกรณ์ไม่ได้ติดตั้ง Security Software	บังคับใช้ Endpoint Security / Antivirus	ฝ่าย IT Security	Pending	ตรวจสอบทุก 6 เดือน
92	การส่งอีเมลไม่ปลอดภัย (Unsecured Email Transmission)	การเข้ารหัสข้อมูล (Data Encryption Weakness)	Email System	สูง (High)	Email ส่งแบบ Plaintext	ใช้ TLS / S/MIME / PGP	ฝ่าย IT Network	In Progress	ตรวจสอบไตรมาส
93	การโจมตี Directory Traversal	ช่องโหว่แอปพลิเคชัน (Application Vulnerability)	Web Application	สูง (High)	ผู้โจมตีเข้าถึงไฟล์ระบบ	ใช้ Input Validation และ Restrict Path	ทีมพัฒนาแอป	Pending	ตรวจสอบทุก Release
94	การเปิด Port ที่ไม่จำเป็น	ความปลอดภัยเครือข่าย (Network Security Weakness)	Server / Firewall	กลาง (Medium)	Port เปิดเกินความจำเป็น	ปิด Port ไม่จำเป็น / Firewall Rules	ฝ่าย IT Network	Pending	ตรวจสอบไตรมาส

คำอธิบายเพิ่มเติม

ระดับความรุนแรง (Severity Level)

สูง (High) – ช่องโหว่ที่อาจทำให้ข้อมูลส่วนบุคคลรั่วไหลหรือระบบถูกโจมตีอย่างรุนแรง

กลาง (Medium) – ช่องโหว่ที่มีความเสี่ยงปานกลางและควรแก้ไขเพื่อป้องกันเหตุการณ์ในอนาคต

ต่ำ (Low) – ช่องโหว่ที่ไม่ส่งผลกระทบต่อข้อมูลสำคัญโดยตรง แต่ควรปรับปรุงเพื่อมาตรฐานความปลอดภัย

แนวทางแก้ไข (Remediation)

ต้องเป็นขั้นตอนปฏิบัติที่ชัดเจน เช่น การปรับปรุงซอฟต์แวร์ การเข้ารหัสข้อมูล การกำหนดสิทธิ์ หรือการติดตั้งเครื่องมือรักษาความปลอดภัย

ควรมีการกำหนดผู้รับผิดชอบและกำหนดระยะเวลาในการดำเนินการ

สถานะ (Status)

Pending = รอดำเนินการ

In Progress = อยู่ระหว่างแก้ไข

Completed = แก้ไขเรียบร้อยแล้ว

การอัปเดตรายงาน

ควรทำสม่ำเสมอทุก 6 เดือน สำหรับการสแกนช่องโหว่ (Vulnerability Scanning)

Penetration Testing ควรทำอย่างน้อยปีละ 1 ครั้ง

รายงานการประเมินและทดสอบระบบประมวลผลข้อมูลส่วนบุคคล: การประเมินและแก้ไขช่องโหว่ของระบบสำคัญอย่างสม่ำเสมอ

บทนำ

ตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล และเพื่อให้สอดคล้องกับ **เกณฑ์ 9.9.8** ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act, B.E. 2562 – “PDPA”) หน่วยงานเทคโนโลยีสารสนเทศ (IT Department) ขององค์กรได้จัดทำรายงานประเมินช่องโหว่และทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของบุคคลภายนอกและภายในอย่างสม่ำเสมอ ทั้งนี้เพื่อให้แน่ใจว่าระบบสำคัญขององค์กรสามารถรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลส่วนบุคคลได้อย่างปลอดภัย และสอดคล้องกับข้อกำหนดทางกฎหมาย

วัตถุประสงค์

เพื่อประเมินช่องโหว่ (Vulnerability Assessment) ของระบบสำคัญในการประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing System)

เพื่อแก้ไขและลดความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่ของระบบ

เพื่อจัดทำรายงานหลักฐาน (Evidence Report) สำหรับการตรวจสอบภายใน (Internal Audit) และการตรวจสอบภายนอก (External Audit)

เพื่อให้เป็นไปตามข้อกำหนดทางกฎหมาย และแนวทางปฏิบัติที่ดีด้านการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security Best Practice)

ขอบเขตของการประเมิน

การประเมินช่องโหว่และการทดสอบระบบครอบคลุม:

ระบบฐานข้อมูล (Database Systems) ที่จัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการและพนักงาน

ระบบแอปพลิเคชันภายใน (Internal Applications) เช่น ระบบเงินเดือน (Payroll System), ระบบทรัพยากรบุคคล (HR System), ระบบ CRM (Customer Relationship Management)

ระบบเครือข่าย (Network Systems) ภายในองค์กรและเครือข่ายที่เชื่อมต่อกับบุคคลภายนอก

ระบบสำรองข้อมูลและ Cloud Storage

ระบบป้องกันความปลอดภัย เช่น Firewall, IDS/IPS, Endpoint Security

คำจำกัดความ

เพื่อความชัดเจน รายงานฉบับนี้ใช้คำจำกัดความดังนี้:

ช่องโหว่ (Vulnerability) หมายถึง จุดอ่อนหรือข้อบกพร่องของระบบที่อาจถูกผู้ไม่ประสงค์ดีโจมตีหรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ความรุนแรง (Severity) หมายถึง ระดับความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้นจากช่องโหว่

สูง (High): อาจทำให้ข้อมูลส่วนบุคคลรั่วไหลหรือเสียหายอย่างร้ายแรง

กลาง (Medium): อาจทำให้ข้อมูลเสียหายหรือเข้าถึงโดยไม่ได้รับอนุญาตบางส่วน

ต่ำ (Low): ผลกระทบจำกัด สามารถจัดการได้ง่าย

ผู้ตรวจสอบภายใน (Internal Auditor) หมายถึง พนักงานหรือทีมตรวจสอบภายในในองค์กรที่มีความเชี่ยวชาญด้าน IT Security

ผู้ตรวจสอบภายนอก (External Auditor) หมายถึง หน่วยงานหรือผู้เชี่ยวชาญภายนอกที่ได้รับการรับรองด้านการทดสอบระบบความปลอดภัย

การแก้ไขช่องโหว่ (Remediation) หมายถึง การดำเนินการเพื่อลดหรือป้องกันความเสี่ยงที่เกิดจากช่องโหว่ เช่น การ Patch ระบบ การปรับ Configuration การใช้ระบบเข้ารหัส (Encryption) หรือการใช้ระบบยืนยันตัวตนแบบหลายชั้น (Multi-Factor Authentication, MFA)

วิธีการประเมินและทดสอบ

การประเมินและทดสอบช่องโหว่ระบบสำคัญ ดำเนินการตามขั้นตอนดังนี้:

1. การระบุและจัดลำดับช่องโหว่

ดำเนินการ **Vulnerability Scan** ด้วยเครื่องมือมาตรฐาน เช่น Nessus, OpenVAS, Qualys (เครื่องมือสแกนช่องโหว่ระบบ – Vulnerability Scanning Tools)

ตรวจสอบ **Patch Management** ของระบบและซอฟต์แวร์ทั้งหมด

จัดทำ **รายการช่องโหว่ (Vulnerability Inventory)** พร้อมระดับความรุนแรง

2. การทดสอบการเจาะระบบ (Penetration Testing)

ดำเนินการทดสอบโดย ผู้ตรวจสอบภายใน และ ผู้ตรวจสอบภายนอก เพื่อจำลองการโจมตีจากผู้ไม่ประสงค์ดี

ครอบคลุมช่องทาง:

การเข้าถึงข้อมูลผ่านเว็บแอปพลิเคชัน

การเข้าถึงข้อมูลผ่านเครือข่าย (Network)

การเข้าถึงข้อมูลในระบบสำรองและ Cloud

บันทึก ผลการทดสอบ (Test Results) และ ช่องโหว่ที่พบ

3. การประเมินผลกระทบ (Impact Assessment)

ประเมินผลกระทบต่อความลับ (Confidentiality), ความสมบูรณ์ (Integrity), และความพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล

จัดลำดับความรุนแรงตามเกณฑ์ High, Medium, Low

4. การกำหนดแนวทางแก้ไข (Remediation Planning)

สำหรับช่องโหว่ระดับสูง: ดำเนินการ Patch หรือ Configuration Change ทันที

สำหรับช่องโหว่ระดับกลาง: วางแผนดำเนินการในระยะเวลา 1-3 เดือน

สำหรับช่องโหว่ระดับต่ำ: จัดทำ Monitoring Plan และตรวจสอบอย่างสม่ำเสมอ

5. การบันทึกและรายงานผล

จัดทำ Vulnerability Assessment Report โดยระบุ:

รายการช่องโหว่ที่พบ

ระดับความรุนแรง

แนวทางแก้ไข

ผู้รับผิดชอบ

สถานการณ์แก้ไข

รายงานฉบับสมบูรณ์นี้เก็บไว้ในฐานข้อมูลของฝ่าย IT Security เพื่อเป็นหลักฐานการปฏิบัติตามเกณฑ์ 9.9.8

ตารางตัวอย่างช่องโหว่และแนวทางแก้ไข

ลำดับ	ชื่อช่องโหว่ (Vulnerability Name)	ระดับความรุนแรง (Severity Level)	แนวทางแก้ไข (Remediation)	สถานะ (Status)

1	การเก็บรหัสผ่านในไฟล์ข้อความ (Storing Passwords in Plaintext Files)	สูง (High)	ใช้การเข้ารหัสรหัสผ่าน (Password Hashing) เช่น bcrypt	In Progress
2	การส่งข้อมูลแบบไม่เข้ารหัส (Unencrypted Data Transmission)	สูง (High)	ใช้ HTTPS / TLS 1.2+	Completed
3	การใช้รหัสผ่านซ้ำ (Password Reuse)	กลาง (Medium)	บังคับใช้ Password Policy ไม่ซ้ำ	Pending
4	การโจมตี Cross-Site Scripting (XSS)	สูง (High)	ใช้ Input Validation และ Output Encoding	In Progress
5	การเข้าถึง API โดยไม่จำกัด (Unrestricted API Access)	สูง (High)	ใช้ OAuth2 / API Key และ Rate Limiting	Pending

หมายเหตุ: ตารางฉบับเต็มจะมี 100 รายการตามรายการประเมินช่องโหว่ที่จัดทำไว้ก่อนหน้านี้

ผลการประเมิน

ระบบสำคัญทั้งหมดถูกสแกนและประเมินช่องโหว่อย่างสม่ำเสมออย่างน้อยทุก **ไตรมาส**

พบช่องโหว่รวม **100 รายการ** โดย:

สูง (High) จำนวน 35 รายการ

กลาง (Medium) จำนวน 45 รายการ

ต่ำ (Low) จำนวน 20 รายการ

ช่องโหว่ระดับสูงได้รับการแก้ไขทันทีหรือกำหนดระยะเวลาแก้ไขไม่เกิน 30 วัน

ช่องโหว่ระดับกลางและต่ำมีแผนการแก้ไขและตรวจสอบอย่างสม่ำเสมอ

ข้อเสนอแนะ

ควรปรับปรุงกระบวนการ **Patch Management** ให้ครอบคลุมระบบทั้งหมดและมีการติดตามอย่างต่อเนื่อง

จัดทำ **Security Awareness Training** ให้พนักงานทุกคนเพื่อลดความเสี่ยงจาก Social Engineering
เพิ่มการตรวจสอบและบันทึก **Audit Log** ของการเข้าถึงข้อมูลสำคัญ

ดำเนินการ **Penetration Test** อย่างน้อยปีละ 2 ครั้ง และรายงานผลต่อผู้บริหาร

สรุป

จากการประเมินและทดสอบช่องโหว่ระบบสำคัญพบว่า ระบบขององค์กรมีความปลอดภัยในระดับที่ดี แต่ยังมีช่องโหว่บางส่วนที่ต้องแก้ไข ซึ่งการดำเนินการแก้ไขช่องโหว่และทดสอบระบบอย่างสม่ำเสมอเป็นการปฏิบัติตาม **เกณฑ์ 9.9.8** อย่างครบถ้วน ทั้งนี้รายงานฉบับนี้ถือเป็น **หลักฐานทางราชการและหลักฐานภายในองค์กร** ที่แสดงว่าองค์กรได้ปฏิบัติตาม PDPA อย่างเคร่งครัด

แนบเอกสารประกอบ

ตารางประเมินช่องโหว่ทั้งหมด 100 รายการ
รายงานผลการทดสอบ Penetration Test โดยผู้ตรวจสอบภายในและภายนอก
หลักฐานการแก้ไขช่องโหว่ (Patch Logs, Configuration Change Logs)

ตัวอย่างรายงานช่องโหว่ (Vulnerability Report)

#	ชื่อช่องโหว่ (อังกฤษ)	ประเภท	ระบบ/แอป	ระดับ	คำอธิบาย	แนวทางแก้ไข	ผู้รับผิดชอบ	สถานะ	หมายเหตุ
1	บัฟเฟอร์ล้น (Buffer Overflow)	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	สูง (High)	โปรแกรมเขียนข้อมูลเกินขนาดบัฟเฟอร์ ทำให้เกิดการรันโค้ดจากระยะไกล (RCE)	ตรวจสอบขนาดข้อมูล / ใช้ฟังก์ชันปลอดภัย (Safe Functions)	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบในโมดูลอัปโหลดไฟล์ (Upload Module)
2	ฮีปล้น (Heap Overflow)	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	สูง (High)	การเขียนข้อมูลเกิน heap ทำให้เกิด crash หรือ RCE	ใช้การจัดการหน่วยความจำอย่างปลอดภัย (Safe Memory Handling)	ทีมพัฒนา (Dev Team)	เปิด (Open)	ตรวจพบใน Memory Allocation
3	ตัวเลขล้น (Integer Overflow)	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	สูง (High)	การคำนวณตัวเลขเกินขอบเขต ทำให้เกิดผลลัพธ์ไม่คาดคิด	ตรวจสอบค่าก่อนคำนวณ (Input Validation)	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบในฟังก์ชัน Payment
4	ช่องโหว่สตริงฟอร์แมต (Format String Vulnerability)	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	สูง (High)	ข้อมูลผู้ใช้ถูกใช้ในฟังก์ชัน printf โดยไม่ตรวจสอบ	ตรวจสอบค่า Input / ใช้ฟังก์ชันปลอดภัย	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Logging Module

5	เงื่อนไข แข่งขัน (Race Condition)	การทำงาน พร้อมกัน (Concurren- cy)	แอปพลิเคชัน (Application)	ปาน กลาง (Mediu m)	หลาย process เข้าถึง resource เดียวกันพร้อม กัน ทำให้เกิด ข้อผิดพลาด	ใช้ Lock / Mutex	ทีมพัฒนา (Dev Team)	เปิด (Open)	ตรวจพบใน Order Processin g
6	ตรวจสอบค่า ผู้ใช้ไม่ เพียงพอ (Improper Input Validation)	การ ตรวจสอบ Input (Validation)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ระบบไม่ได้ ตรวจสอบค่าที่ ผู้ใช้ส่งเข้ามา	ตรวจสอบ และทำ ความ สะอาด ข้อมูล (Validate / Sanitize Input)	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน ฟอร์ม Registrati on
7	การปลอมคำ ขอจากฝั่ง เซิร์ฟเวอร์ (Server-Side Request Forgery, SSRF)	ความ ปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ผู้โจมตีบังคับ เซิร์ฟเวอร์ไป เรียก URL ภายใน	ตรวจสอบ URL / Block Internal Access	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน API Fetch
8	การโหลดไฟล์ ภายในเครื่อง โดยไม่ได้รับ อนุญาต (Local File Inclusion, LFI)	ความ ปลอดภัยไฟล์ (File Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ผู้โจมตีโหลดไฟล์ ในเครื่องโดย ไม่ได้รับอนุญาต	ตรวจสอบ Path / จำกัดสิทธิ์ การเข้าถึง	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Page Include
9	การโหลดไฟล์ จากภายนอก (Remote File Inclusion, RFI)	ความ ปลอดภัยไฟล์ (File Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ผู้โจมตีโหลดไฟล์ จาก URL ภายนอก	ตรวจสอบ URL / ปิด Remote Include	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Legacy PHP
10	การเข้าถึง ข้อมูลโดยตรง ไม่ปลอดภัย (Insecure Direct Object Reference, IDOR)	การควบคุม สิทธิ์ (Authorizati on)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ผู้ใช้เข้าถึงข้อมูล ของผู้อื่นโดยตรง	ใช้ Access Control Check	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน API Endpoint
11	การเข้ารหัส การส่งข้อมูล ไม่เพียงพอ (Insufficient Transport Layer Protection)	ความ ปลอดภัย เครือข่าย (Network Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ข้อมูลส่งผ่าน เครือข่ายไม่ เข้ารหัส	ใช้ HTTPS / TLS 1.2+	ทีมรักษา ความ ปลอดภัย (Security Team)	เปิด (Open)	พบใน Form Submissio n

12	นโยบายรหัสผ่านอ่อนแอ (Weak Password Policy)	การพิสูจน์ตัวตน (Authentication)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ระบบอนุญาตรหัสผ่านง่าย	ใช้นโยบายรหัสผ่านแข็งแกร่ง (Strong Password Policy)	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Login Module
13	รหัสผ่านใน URL (Password in URL)	การพิสูจน์ตัวตน (Authentication)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	รหัสผ่านถูกส่งผ่าน URL	ส่งผ่าน POST / HTTPS	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Reset Password
14	รหัสผ่านปรากฏใน Log (Credential Exposure in Logs)	ความปลอดภัยข้อมูล (Data Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	รหัสผ่านหรือ Token ถูกเก็บใน Log	ซ่อนข้อมูลสำคัญใน Log (Sanitize / Mask Sensitive Info)	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Logging
15	รหัสผ่านฝังในโค้ด (Hardcoded Credentials)	ความปลอดภัยโค้ด (Code Security)	แอปพลิเคชัน (Application)	สูง (High)	รหัสผ่านฝังอยู่ในโค้ด	ใช้ Config File / Secret Manager	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Config File
16	ซอฟต์แวร์ล้าสมัย (Unpatched Software)	การจัดการ Patch (Patch Management)	เซิร์ฟเวอร์ (Server)	สูง (High)	ใช้ซอฟต์แวร์เวอร์ชันเก่า	อัปเดต / Patch Software	ผู้ดูแลระบบ (SysAdmin)	เปิด (Open)	ตรวจพบ Apache 2.4.29
17	การแสดงรายการไดเรกทอรี (Directory Listing Enabled)	การตั้งค่าเซิร์ฟเวอร์ (Configuration)	เว็บเซิร์ฟเวอร์ (Web Server)	ปานกลาง (Medium)	เว็บเซิร์ฟเวอร์แสดงรายการไฟล์	ปิด Directory Listing	ผู้ดูแลระบบ (SysAdmin)	เปิด (Open)	พบใน /public_html
18	โปรโตคอล SSL/TLS ล้าสมัย (Outdated SSL/TLS Protocol)	ความปลอดภัยเครือข่าย (Network Security)	เว็บเซิร์ฟเวอร์ (Web Server)	สูง (High)	ใช้ SSL 3.0 / TLS 1.0	ใช้ TLS 1.2+	ผู้ดูแลระบบ (SysAdmin)	เปิด (Open)	พบใน HTTPS
19	การใช้ Cipher Suite อ่อนแอ (Weak Cipher Suite)	ความปลอดภัยเครือข่าย (Network Security)	เว็บเซิร์ฟเวอร์ (Web Server)	สูง (High)	ใช้ Cipher ที่ไม่ปลอดภัย	ปรับใช้ Cipher แข็งแรง (Strong Cipher)	ผู้ดูแลระบบ (SysAdmin)	เปิด (Open)	พบ AES-128-CBC
20	ขาด Security Header (Missing)	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	HTTP Header เช่น HSTS / X-Content-Type-Options ไม่มี	เพิ่ม Security Headers	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Response Header

	Security Headers)								
21	การโจมตีแบบ Cross-Site Scripting (XSS)	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ผู้โจมตีแทรกสคริปต์ในเว็บเพจเพื่อขโมย Cookie หรือทำ RCE	ทำการ Encode / Escape Input	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบในฟอร์ม Comment
22	การโจมตีแบบ Cross-Site Request Forgery (CSRF)	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ผู้โจมตีบังคับผู้ใช้ส่งคำขอโดยไม่รู้ตัว	ใช้ Token ตรวจสอบคำขอ	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Form Submit
23	การโจมตีแบบ Clickjacking	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	เว็บถูกฝังใน iframe ทำให้ผู้ใช้คลิกโดยไม่ตั้งใจ	ใช้ X-Frame-Options / CSP Frame Ancestors	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบในหน้า Dashboard
24	การเข้าถึง API โดยไม่ตรวจสอบสิทธิ์ (Broken Access Control)	การควบคุมสิทธิ์ (Authorization)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	API สามารถเข้าถึงโดยไม่ได้ตรวจสอบสิทธิ์	ตรวจสอบ Token / Role	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน API /user
25	การจัดเก็บรหัสผ่านไม่ปลอดภัย (Insecure Password Storage)	ความปลอดภัยข้อมูล (Data Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	รหัสผ่านเก็บในรูปแบบ plaintext	ใช้ Hash + Salt เช่น bcrypt	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน DB User Table
26	การจัดการ Session ไม่ปลอดภัย (Insecure Session Management)	การพิสูจน์ตัวตน (Authentication)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	Session ID ไม่ปลอดภัย / ไม่หมดอายุ	ใช้ Secure, HttpOnly Cookies / Session Expiry	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Login Module
27	การใช้ JWT ไม่ปลอดภัย (Insecure JWT Implementation)	การพิสูจน์ตัวตน (Authentication)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	JWT ไม่มี Signature / Algorithm Weak	ใช้ Algorithm แข็งแรง และตรวจสอบ Signature	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน API Authorization
28	การเปิดเผยข้อมูลเซิร์ฟเวอร์ (Information Disclosure)	ความปลอดภัยเว็บ (Web Security)	เว็บเซิร์ฟเวอร์ (Web Server)	ปานกลาง (Medium)	ข้อมูลเวอร์ชัน / Stack แสดงใน Response	ปิด Server Banner / Error Detail	ผู้ดูแลระบบ (SysAdmin)	เปิด (Open)	พบใน Error Page

29	การเรียกใช้คำสั่งจากระยะไกล (Remote Code Execution, RCE)	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	สูง (High)	ผู้โจมตีรันโค้ดบนเซิร์ฟเวอร์	ตรวจสอบ Input / Patch Vulnerability	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Module Upload
30	การโจมตีแบบ SQL Injection	ช่องโหว่โค้ด (Code Vulnerability)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ผู้โจมตีสอดแทรกคำสั่ง SQL	ใช้ Prepared Statement / ORM	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Forum Login
31	การโจมตีแบบ LDAP Injection	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	สูง (High)	ผู้โจมตีสอดแทรกคำสั่ง LDAP	ตรวจสอบ Input / Escape LDAP	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Authentication Module
32	การโจมตีแบบ XML External Entity (XXE)	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	สูง (High)	XML parser โหลดไฟล์ภายนอก / DTD	ปิด External Entity / ใช้ Parser Safe Mode	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน XML Parser Module
33	การโจมตีแบบ Command Injection	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	สูง (High)	ผู้โจมตีรันคำสั่ง OS จาก Input	Escape / Validate Input	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Shell Exec Module
34	การโจมตีแบบ Path Traversal	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	สูง (High)	ผู้โจมตีเข้าถึงไฟล์นอก Directory	ตรวจสอบ Path / จำกัด Directory	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน File Download Module
35	การโจมตีแบบ Unrestricted File Upload	ความปลอดภัยไฟล์ (File Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ผู้โจมตีอัปโหลดไฟล์ไม่ปลอดภัย	ตรวจสอบ File Type / Antivirus Scan	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Upload Module
36	การโจมตีแบบ Insecure Deserialization	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	สูง (High)	การ Deserialize ข้อมูลไม่ปลอดภัย ทำให้เกิด RCE	ตรวจสอบ Class / ใช้ Library ปลอดภัย	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Java Module
37	การโจมตีแบบ Server-Side Template Injection (SSTI)	ช่องโหว่โค้ด (Code Vulnerability)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	Template Engine แทรก Input โดยไม่ตรวจสอบ	Escape Input / Update Template Engine	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Template Module
38	การโจมตีแบบ Open Redirect	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	URL redirect สามารถนำผู้ใช้ไปไซต์อันตราย	ตรวจสอบ URL / Whitelist	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Login Redirect

39	การโจมตีแบบ Clickjacking	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	หน้าเว็บถูกฝังใน iframe ทำให้คลิกโดยไม่ได้ตั้งใจ	ใช้ X-Frame-Options / CSP	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบในหน้า Dashboard
40	การโจมตีแบบ Weak Session ID	การพิสูจน์ตัวตน (Authentication)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	Session ID ทายได้ง่าย	ใช้ Random, Long Session ID	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Login Module
41	การโจมตีแบบ HTTP Response Splitting	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	ผู้โจมตีแทรก Header ใหม่	Escape Input / Validate	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Header Response
42	การโจมตีแบบ Open Port	ความปลอดภัยเครือข่าย (Network Security)	เซิร์ฟเวอร์ (Server)	ปานกลาง (Medium)	พอร์ตเปิดเกินจำเป็น เสี่ยงถูกโจมตี	ปิด Port ไม่จำเป็น / Firewall	ผู้ดูแลระบบ (SysAdmin)	เปิด (Open)	ตรวจพบ Port 21, 23
43	การโจมตีแบบ Default Credentials	การพิสูจน์ตัวตน (Authentication)	อุปกรณ์เครือข่าย (Network Device)	สูง (High)	ใช้รหัสผ่าน Default	เปลี่ยน Default Credentials	ผู้ดูแลระบบ (SysAdmin)	เปิด (Open)	พบใน Router / Switch
44	การโจมตีแบบ Misconfigured Permissions	การควบคุมสิทธิ์ (Authorization)	ระบบไฟล์ (File System)	ปานกลาง (Medium)	สิทธิ์ไฟล์/โฟลเดอร์ไม่ถูกต้อง	ตรวจสอบ Permission / Principle of Least Privilege	ผู้ดูแลระบบ (SysAdmin)	เปิด (Open)	ตรวจพบ Folder /var/www/html
45	การโจมตีแบบ Weak Encryption	ความปลอดภัยข้อมูล (Data Security)	แอปพลิเคชัน (Application)	สูง (High)	ใช้อัลกอริทึมเข้ารหัสอ่อน	ใช้ AES 256 / Strong Algorithm	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Config Encryption
46	การโจมตีแบบ Missing Audit Log	ความปลอดภัยข้อมูล (Data Security)	แอปพลิเคชัน (Application)	ปานกลาง (Medium)	ไม่มีการบันทึกกิจกรรมสำคัญ	เปิด Logging / Audit	ทีมพัฒนา (Dev Team)	เปิด (Open)	ตรวจพบใน User Management
47	การโจมตีแบบ Unvalidated Redirects	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	URL redirect ไม่ตรวจสอบ	Validate / Whitelist URL	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Redirect Module
48	การโจมตีแบบ Server Misconfiguration	การตั้งค่าเซิร์ฟเวอร์ (Configuration)	เซิร์ฟเวอร์ (Server)	สูง (High)	การตั้งค่าเซิร์ฟเวอร์ไม่ปลอดภัย	ปรับ Config / Apply Security Best Practices	ผู้ดูแลระบบ (SysAdmin)	เปิด (Open)	พบใน Apache / Nginx
49	การโจมตีแบบ Insecure API	ความปลอดภัยเว็บ (Web Security)	API (API)	สูง (High)	API ไม่มี Authentication / Authorization	ใช้ Token / OAuth2	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน REST API

50	การโจมตีแบบ Memory Leak	ช่องโหว่โค้ด (Code Vulnerability)	แอปพลิเคชัน (Application)	ปานกลาง (Medium)	การจัดการหน่วยความจำไม่ดี ทำให้แอปสั่ม	ตรวจสอบ Memory Management	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Module Image Processing
51	การโจมตีแบบ Hardcoded API Key	ความปลอดภัยโค้ด (Code Security)	แอปพลิเคชัน (Application)	สูง (High)	API Key ผิ้งในโค้ด	ใช้ Config / Secret Management	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Mobile App
52	การโจมตีแบบ Path Disclosure	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	Error แสดง Path ของไฟล์ / Folder	ปิด Error Detail / Escape Path	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Error Page
53	การโจมตีแบบ Unencrypted Sensitive Data	ความปลอดภัยข้อมูล (Data Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ข้อมูลสำคัญส่งหรือเก็บไม่เข้ารหัส	ใช้ HTTPS / Encrypt Database	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Payment Module
54	การโจมตีแบบ Improper Error Handling	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	ข้อความ Error เปิดเผยข้อมูลภายใน	Escape Error / Custom Error Page	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Login Module
55	การโจมตีแบบ Lack of Rate Limiting	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	ไม่มีจำกัดจำนวนคำขอ	ใช้ Rate Limit / Throttling	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน API Login
56	การโจมตีแบบ Directory Traversal	ช่องโหว่โค้ด (Code Vulnerability)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	เข้าถึงไฟล์นอก Directory	ตรวจสอบ Path / Limit Directory	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน File Access
57	การโจมตีแบบ Insecure Cookie	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	Cookie ไม่ใช่ Secure / HttpOnly	Set Secure / HttpOnly Flags	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Session Cookie
58	การโจมตีแบบ Insufficient Logging	ความปลอดภัยข้อมูล (Data Security)	แอปพลิเคชัน (Application)	ปานกลาง (Medium)	กิจกรรมสำคัญไม่ได้ถูกบันทึก	เพิ่ม Logging / Audit	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Admin Module
59	การโจมตีแบบ Weak Password Recovery	การพิสูจน์ตัวตน (Authentication)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ระบบ Recovery ใช้คำถามง่าย	ใช้ Email OTP / Multi-factor	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Forgot Password
60	การโจมตีแบบ Sensitive Data Exposure	ความปลอดภัยข้อมูล (Data Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ข้อมูลสำคัญเปิดเผย	Encrypt Data / Mask Sensitive Info	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน User Profile
61	การโจมตีแบบ Missing Function	การควบคุมสิทธิ์	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ฟังก์ชันบางตัวเข้าถึงโดยไม่ตรวจสอบสิทธิ์	Implement Role-Based	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Admin Function

	Level Access Control	(Authorizati on)				Access Control			
62	การโจมตีแบบ No CSRF Token	ความ ปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ไม่มี Token ตรวจสอบค่าขอ	เพิ่ม CSRF Token	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Form Submit
63	การโจมตีแบบ Weak Session Expiration	การพิสูจน์ ตัวตน (Authenticat ion)	เว็บแอปพลิเคชัน (Web Application)	ปาน กลาง (Mediu m)	Session ไม่ หมดอายุเร็ว	ตั้ง Session Expiry	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Login Module
64	การโจมตีแบบ Broken Cryptograph y	ความ ปลอดภัย ข้อมูล (Data Security)	แอปพลิเคชัน (Application)	สูง (High)	ใช้การเข้ารหัส อ่อน	ใช้ AES 256 / Strong Algorithm	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Config Encryptio n
65	การโจมตีแบบ Insufficient Transport Layer Protection	ความ ปลอดภัย เครือข่าย (Network Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	Data ส่งไม่ เข้ารหัส	ใช้ HTTPS / TLS	ทีมรักษา ความ ปลอดภัย (Security Team)	เปิด (Open)	พบใน Form Submissio n
66	การโจมตีแบบ Insufficient Input Validation	การตรวจสอบ Input (Validation)	แอปพลิเคชัน (Application)	สูง (High)	ระบบตรวจสอบ ค่าที่ผู้ใช้ส่งเข้า มาไม่เพียงพอ	Validate / Sanitize Input	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Registrati on Form
67	การโจมตีแบบ XML Injection	ช่องโหว่โค้ด (Code Vulnerabilit y)	แอปพลิเคชัน (Application)	สูง (High)	ผู้โจมตีแทรก XML ไม่ ปลอดภัย	Validate / Escape XML Input	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน XML Parser
68	การโจมตีแบบ Insufficient Session Expiration	การพิสูจน์ ตัวตน (Authenticat ion)	เว็บแอปพลิเคชัน (Web Application)	ปาน กลาง (Mediu m)	Session ไม่ หมดอายุทันที หลัง Logout	Session Expiry / Invalidate Session	ทีมพัฒนา (Dev Team)	เปิด (Open)	
69	การโจมตีแบบ Insecure Direct Object Reference (IDOR)	การควบคุม สิทธิ์ (Authorizati on)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	ผู้ใช้เข้าถึงข้อมูล ของผู้ใช้คนอื่น โดยตรง	ตรวจสอบ Authoriza tion / Use Indirect Reference	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน URL /user?id=
70	การโจมตีแบบ Local File Inclusion (LFI)	ช่องโหว่โค้ด (Code Vulnerabilit y)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	โหลดไฟล์ภายใน เซิร์ฟเวอร์โดย ไม่ได้รับอนุญาต	Validate / Sanitize Path	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Include Module
71	การโจมตีแบบ Remote File Inclusion (RFI)	ช่องโหว่โค้ด (Code Vulnerabilit y)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	โหลดไฟล์จาก ระยะไกลและรัน บนเซิร์ฟเวอร์	Validate / Block Remote URLs	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Include Module
72	การโจมตีแบบ Insufficient	การควบคุม สิทธิ์	แอปพลิเคชัน (Application)	สูง (High)	ระบบไม่ ตรวจสอบสิทธิ์ เพียงพอ	Impleme nt Role-	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Admin Function

	Authorizatio n	(Authorizati on)				Based Access			
73	การโจมตีแบบ Insecure Deserializati on	ช่องโหว่โค้ด (Code Vulnerabilit y)	แอปพลิเคชัน (Application)	สูง (High)	การ Deserialize ข้อมูลจากผู้ที่ไม่ ปลอดภัย	Validate / Use Safe Libraries	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Java Module
74	การโจมตีแบบ Server-Side Request Forgery (SSRF)	ความ ปลอดภัย เครือข่าย (Network Security)	เซิร์ฟเวอร์ / API (Server/API)	สูง (High)	เซิร์ฟเวอร์ถูก บังคับให้เรียก Resource ภายใน	Validate URLs / Block Internal Requests	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน API Fetch Module
75	การโจมตีแบบ Insecure Temporary File	ความ ปลอดภัยไฟล์ (File Security)	แอปพลิเคชัน (Application)	ปาน กลาง (Mediu m)	Temp File ไม่ ปลอดภัย / ถูก เข้าถึงได้	สร้าง Temp File แบบ Secure / Delete หลังใช้	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Upload Module
76	การโจมตีแบบ Race Condition	ช่องโหว่โค้ด (Code Vulnerabilit y)	แอปพลิเคชัน (Application)	สูง (High)	การเข้าถึง Resource พร้อมกันทำให้ เกิดความ เสียหาย	Lock / Mutex / Transacti on	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Bank Module
77	การโจมตีแบบ Integer Overflow	ช่องโหว่โค้ด (Code Vulnerabilit y)	แอปพลิเคชัน (Application)	ปาน กลาง (Mediu m)	การคำนวณ จำนวนเต็มเกิน ขอบเขต	Validate Input / Use Safe Data Type	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Calculatio n Module
78	การโจมตีแบบ Buffer Overflow	ช่องโหว่โค้ด (Code Vulnerabilit y)	แอปพลิเคชัน / ไบนารี (Application /Binary)	สูง (High)	เขียนข้อมูลเกิน ขอบเขต Buffer	ใช้ Safe Functions / Bounds Check	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน C Module
79	การโจมตีแบบ Cross-Site WebSocket Hijacking (CSWH)	ความ ปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	แฮก WebSocket Session	ตรวจสอบ Origin / Authentic ate WebSock et	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Chat Module
80	การโจมตีแบบ OAuth Token Leak	การพิสูจน์ ตัวตน (Authenticat ion)	เว็บแอปพลิเคชัน / API (Web/API)	สูง (High)	Token OAuth ถูกเปิดเผย	ใช้ Secure Storage / HTTPS	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Mobile App
81	การโจมตีแบบ Information Leakage via Error	ความ ปลอดภัย ข้อมูล (Data Security)	เว็บแอปพลิเคชัน (Web Application)	ปาน กลาง (Mediu m)	ข้อความ Error เปิดเผยข้อมูล สำคัญ	Custom Error Page / Escape Details	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Module Login
82	การโจมตีแบบ Weak Password Policy	การพิสูจน์ ตัวตน (Authenticat ion)	แอปพลิเคชัน (Application)	สูง (High)	ระบบอนุญาตใช้ รหัสผ่านง่าย เกินไป	กำหนด Policy ความ ซับซ้อน	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Registrati on

83	การโจมตีแบบ Insecure Mobile Storage	ความปลอดภัยอุปกรณ์ (Mobile Security)	Mobile App	สูง (High)	ข้อมูลสำคัญเก็บในที่ที่ไม่ปลอดภัย	ใช้ Encrypted Storage	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน App Local DB
84	การโจมตีแบบ Insecure Bluetooth / Wi-Fi	ความปลอดภัยอุปกรณ์ (Device Security)	Mobile App / IoT	ปานกลาง (Medium)	การเชื่อมต่อไร้สายไม่เข้ารหัส	ใช้ Encrypted Protocol / Pairing	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน IoT Device
85	การโจมตีแบบ Insecure Push Notification	ความปลอดภัยแอป (App Security)	Mobile App	ปานกลาง (Medium)	ข้อความ Push เปิดเผยข้อมูล	ใช้ Encrypted Push	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Notification Module
86	การโจมตีแบบ Hardcoded Credentials	ความปลอดภัยโค้ด (Code Security)	แอปพลิเคชัน / Mobile	สูง (High)	Credentials ฝังในโค้ด	ใช้ Secret Management	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Config File
87	การโจมตีแบบ Insufficient Cryptographic Key Management	ความปลอดภัยข้อมูล (Data Security)	แอปพลิเคชัน (Application)	สูง (High)	การจัดการ Key อ่อนแอ	ใช้ Secure Key Store	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Encryption Module
88	การโจมตีแบบ Lack of Multi-Factor Authentication	การพิสูจน์ตัวตน (Authentication)	แอปพลิเคชัน / เว็บแอป (Web Application)	สูง (High)	ไม่มี MFA เพิ่มความปลอดภัย	Implement MFA	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Login Module
89	การโจมตีแบบ Insecure WebSocket	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	WebSocket ไม่เข้ารหัส	ใช้ WSS / Authenticate	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Chat Module
90	การโจมตีแบบ Improper Input Sanitization	การตรวจสอบ Input (Validation)	แอปพลิเคชัน (Application)	สูง (High)	Input ไม่ถูกตรวจสอบทำให้เกิด Injection	Sanitize / Validate Input	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Form Submit
91	การโจมตีแบบ Insecure Logging	ความปลอดภัยข้อมูล (Data Security)	แอปพลิเคชัน (Application)	ปานกลาง (Medium)	Log เก็บข้อมูล Sensitive	Mask / Encrypt Logs	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Admin Module
92	การโจมตีแบบ Insufficient Transport Layer Security	ความปลอดภัยเครือข่าย (Network Security)	เว็บแอปพลิเคชัน (Web Application)	สูง (High)	การส่งข้อมูลไม่เข้ารหัส	ใช้ TLS 1.2+ / HTTPS	ทีมรักษาความปลอดภัย (Security Team)	เปิด (Open)	พบใน Form Submission
93	การโจมตีแบบ Insecure	ช่องโหว่โค้ด (Code)	แอปพลิเคชัน / เว็บแอป	สูง (High)	ใช้ Library ไม่ปลอดภัย	Update / Patch Library	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Dependencies

	Third-Party Libraries	Vulnerability)							
94	การโจมตีแบบ Lack of Security Headers	ความปลอดภัยเว็บ (Web Security)	เว็บแอปพลิเคชัน (Web Application)	ปานกลาง (Medium)	ไม่มี HTTP Security Headers	ตั้งค่า Security Headers	ทีมพัฒนา (Dev Team)	เปิด (Open)	พบใน Response Header

คำอธิบายท้ายตาราง (Glossary / Explanations)

1. การฉีดคำสั่ง SQL (SQL Injection)

SQL Injection (SQLi) เปรียบเสมือน การแอบใส่กุญแจปลอมเข้าไปในล็อกบ้าน เพื่อให้เปิดประตูโดยไม่ต้องใช้กุญแจจริง หากเว็บเป็นบ้านของข้อมูลผู้ใช้ กุญแจปลอมนี้จะช่วยให้ผู้โจมตีเข้าถึงข้อมูลทั้งหมดในระบบได้

ตัวอย่างง่าย ๆ:

คิดว่าคุณมีบ้านที่ล็อกด้วยรหัส 4 หลัก และใครสักคนรู้ว่าประตูนี้มีช่องแอบใส่รหัส ผู้โจมตีใส่ ' OR '1'='1 ในช่องรหัสประตู บ้านก็เปิดทันทีโดยไม่ต้องรู้รหัสจริง

ตัวอย่างสถานการณ์จริง:

ในปี 2009 บริษัท Heartland Payment Systems ถูกโจมตีด้วย SQLi ทำให้ข้อมูลบัตรเครดิตของลูกค้านับล้านรายการรั่วไหล ผู้โจมตีสามารถดึงข้อมูลสำคัญไปใช้ได้โดยตรง

ผลกระทบ:

ข้อมูลผู้ใช้ถูกขโมย, ระบบถูกเปลี่ยนแปลง, หรือแม้แต่ข้อมูลทั้งหมดถูกลบ

2. การแทรกโค้ดบนเว็บไซต์ (Cross-Site Scripting)

Cross-Site Scripting (XSS) เปรียบเหมือน การเขียนข้อความหลอกบนกระดานสาธารณะ ที่แท้จริงคือกับดัก เมื่อคนอื่นเข้ามาอ่าน ข้อความนี้จะรันคำสั่งอันตรายโดยไม่รู้ตัว

ตัวอย่างง่าย ๆ:

คุณโพสต์ข้อความ `<script>alert('ถูกแฮ็กแล้ว!')</script>` ในเว็บบอร์ด เมื่อคนอื่นเปิดข้อความบนเว็บของเขา ระบบจะทำงานตามโค้ดทันที

ตัวอย่างสถานการณ์จริง:

ในปี 2005 เว็บไซต์ MySpace ถูกโจมตี XSS ทำให้ผู้โจมตีสามารถเผยแพร่ข้อความบนหน้าโปรไฟล์ของผู้ใช้คนอื่นโดยอัตโนมัติ

ผลกระทบ:

ข้อมูลส่วนตัวถูกขโมย, session ถูก hijack, หรือแม้แต่บัญชีผู้ใช้ถูกควบคุม

3. การปลอมคำขอของผู้ใช้ (Cross-Site Request Forgery)

Cross-Site Request Forgery (CSRF) เปรียบเหมือน การหลอกให้คุณกดปุ่มในบ้านของคุณเองโดยไม่รู้ตัว เช่น ลิงก์ในอีเมลที่ทำให้คุณโอนเงินโดยไม่ได้ตั้งใจ

ตัวอย่างง่าย ๆ:

คุณเปิดอีเมลที่ดูเหมือนจากธนาคาร คลิกลิงก์ และเงินในบัญชีถูกโอนออกไปทันที โดยที่คุณไม่ได้ยินคำสั่งใด ๆ

ตัวอย่างสถานการณ์จริง:

ในปี 2006 ธนาคารหลายแห่งโดน CSRF ใช้ในการโอนเงินจากบัญชีผู้ใช้โดยที่ผู้ใช้ไม่รู้ตัว

ผลกระทบ:

เงินในบัญชีถูกโอนโดยไม่ได้รับอนุญาต, การควบคุมบัญชีหายไป, และผู้ใช้เสียความเชื่อถือ

4. การพิสูจน์ตัวตนไม่ปลอดภัย (Broken Authentication)

Broken Authentication (การพิสูจน์ตัวตนไม่ปลอดภัย) เปรียบเหมือน กุญแจบ้านที่สามารถเปิดได้ง่ายเกินไป ระบบล็อกอินไม่แข็งแรง เช่น รหัสผ่านง่ายหรือ session ไม่หมดอายุ

ตัวอย่างง่าย ๆ:

เว็บอนุญาตรหัสผ่านเป็น "123456" ผู้โจมตีสามารถเดารหัสผ่านและเข้าบัญชีคนอื่นได้ง่าย

ตัวอย่างสถานการณ์จริง:

หลายเว็บไซต์ที่ไชรหัสผ่านง่าย ๆ ถูกโจมตี ทำให้ข้อมูลผู้ใช้รั่วไหล เช่น บัญชีอีเมล, เว็บช้อปปิ้งออนไลน์

ผลกระทบ:

บัญชีผู้ใช้ถูกเข้าถึงโดยไม่ได้รับอนุญาต, ข้อมูลส่วนตัวรั่วไหล, และเกิดการปลอมตัวเพื่อหลอกลวง

5. การเปิดเผยข้อมูลสำคัญ (Sensitive Data Exposure)

Sensitive Data Exposure (การเปิดเผยข้อมูลสำคัญ) เปรียบเหมือน เก็บเงินสดไว้บนโต๊ะโดยไม่มีตู้เซฟ ข้อมูลสำคัญเช่น รหัสผ่านหรือหมายเลขบัตรเครดิตถูกเก็บในรูปแบบที่ใครก็อ่านได้

ตัวอย่างง่าย ๆ:

เว็บไซต์เก็บรหัสผ่านเป็นตัวอักษรธรรมดา (plain text) หาก server ถูกโจมตี ข้อมูลทั้งหมดจะรั่วทันที

ตัวอย่างสถานการณ์จริง:

Adobe ปี 2013 เก็บรหัสผ่านลูกค้าเป็น plain text ทำให้ข้อมูลของผู้ใช้ 150 ล้านบัญชีถูกขโมย

ผลกระทบ:

ข้อมูลส่วนตัวถูกขโมย, บัญชีถูกเข้าถึง, และอาจเกิดการโจมตีต่อบัญชีอื่นที่ไชรหัสผ่านเดียวกัน

6. การกำหนดสิทธิ์ไม่เหมาะสม (Broken Access Control)

Broken Access Control (การกำหนดสิทธิ์ไม่เหมาะสม) เปรียบเหมือน บ้านที่มีประตูพิเศษ แต่คุณให้กุญแจทุกคนโดยไม่เลือก ผู้โจมตีสามารถเข้าถึงข้อมูลหรือฟังก์ชันที่ไม่ควรเข้าถึงได้

ตัวอย่างง่าย ๆ:

ผู้ใช้ A สามารถเข้าหน้าเว็บของผู้ใช้ B และดูข้อมูลส่วนตัวได้ เพราะระบบไม่ได้ตรวจสอบสิทธิ์

ตัวอย่างสถานการณ์จริง:

Facebook เคยมีบั๊กที่ผู้ใช้สามารถดูโพสต์ส่วนตัวของผู้อื่นได้เพราะ Access Control ไม่ถูกต้อง

ผลกระทบ:

ข้อมูลส่วนตัวรั่ว, ผู้โจมตีสามารถเปลี่ยนแปลงข้อมูล, หรือเข้าถึงฟังก์ชันลับ

7. การโจมตีด้วยการอัปโหลดไฟล์อันตราย (Unrestricted File Upload)

Unrestricted File Upload (การอัปโหลดไฟล์อันตราย) เปรียบเหมือน ให้คนส่งพัสดุเข้าบ้านโดยไม่ตรวจสอบอะไร พักดูอาจเป็นระเบิดหรือสารพิษ

ตัวอย่างง่าย ๆ:

เว็บอนุญาตให้ผู้ใช้ upload ไฟล์ได้ทุกชนิด ผู้โจมตี upload ไฟล์ .exe หรือ .php อันตราย ทำให้ server ถูกควบคุม

ตัวอย่างสถานการณ์จริง:

เว็บไซต์บางแห่งถูกโจมตีด้วยไฟล์ PHP ที่ผู้ใช้ upload เข้าไป ทำให้ผู้โจมตีสามารถรันคำสั่งบน server ได้

ผลกระทบ:

Server ถูกควบคุม, ข้อมูลรั่วไหล, หรือระบบล่ม

8. การโจมตีแบบการประดิษฐ์เซสชัน (Session Fixation)

Session Fixation (การประดิษฐ์เซสชัน) เปรียบเหมือน ผู้โจมตีส่งรหัสล็อกบ้านให้คุณโดยที่เขารู้รหัส นั้น เมื่อคุณเข้าไปใช้ เขาสามารถเข้าบ้านของคุณได้เช่นกัน

ตัวอย่างง่าย ๆ:

ผู้โจมตีส่ง link พร้อม session ID ให้คุณ คุณล็อกอินตาม link เข้าระบบ เขาก็สามารถเข้าบัญชีคุณได้

ตัวอย่างสถานการณ์จริง:

เว็บไซต์หลายแห่งในอดีตที่ใช้ session ID คงที่ ถูกโจมตีแบบนี้ ทำให้ผู้โจมตีเข้าบัญชีผู้ใช้ได้

ผลกระทบ:

บัญชีผู้ใช้ถูกเข้าถึงโดยไม่ได้รับอนุญาต, ข้อมูลสำคัญรั่ว

9. การโจมตีแบบการบังคับรหัสผ่าน (Credential Stuffing)

Credential Stuffing (การบังคับรหัสผ่าน) เปรียบเหมือน ผู้โจมตีลองกุญแจเก่าของคุณทุกบ้านที่เขา
รู้ หากคุณใช้รหัสผ่านเดียวกันในหลายเว็บไซต์

ตัวอย่างง่าย ๆ:

คุณใช้รหัสผ่านเดียวกันในเว็บ A และเว็บ B ผู้โจมตีเอาข้อมูลรหัสผ่านเว็บ A มาลองล็อกอินเว็บ B

ตัวอย่างสถานการณ์จริง:

หลายเว็บไซต์โดน Credential Stuffing เพราะผู้ใช้ใช้รหัสผ่านซ้ำ ทำให้บัญชีถูกแฮ็ก

ผลกระทบ:

บัญชีผู้ใช้หลายบัญชีถูกแฮ็ก, ข้อมูลส่วนตัวถูกขโมย, การเข้าถึงระบบสำคัญ

10. การโจมตีด้วยการทำนายรหัสผ่าน (Password Spraying)

Password Spraying (การทำนายรหัสผ่าน) เปรียบเหมือน ลองกุญแจเดียวกับทุกบ้าน แต่ไม่ลองซ้ำ
บ้านเดิมบ่อย ๆ เพื่อไม่ให้เจ้าของบ้านสังเกต

ตัวอย่างง่าย ๆ:

ผู้โจมตีใช้รหัส "123456" ลองล็อกอินกับบัญชีผู้ใช้หลายบัญชี

ตัวอย่างสถานการณ์จริง:

องค์กรใหญ่หลายแห่งโดน Password Spraying ทำให้บัญชีผู้ใช้บางบัญชีถูกล็อกอินโดยไม่ได้รับอนุญาต

ผลกระทบ:

บัญชีผู้ใช้ถูกเข้าถึง, ข้อมูลสำคัญรั่ว, ความเสียหายต่อระบบ

11. การโจมตีแบบ Man-in-the-Middle

Man-in-the-Middle (MITM) การโจมตีแบบคนกลาง) เปรียบเหมือน ผู้โจมตีแอบฟังและแก้ไข
จดหมายระหว่างผู้ส่งและผู้รับ

ตัวอย่างง่าย ๆ:

คุณส่งข้อมูลผ่าน Wi-Fi สาธารณะ ผู้โจมตีสามารถอ่านหรือเปลี่ยนข้อมูลก่อนถึงผู้รับ

ตัวอย่างสถานการณ์จริง:

การโจมตี MITM บน Wi-Fi ร้านกาแฟ ทำให้ข้อมูลบัตรเครดิตถูกขโมย

ผลกระทบ:

ข้อมูลส่วนตัวถูกขโมย, ข้อมูลถูกแก้ไข, การสื่อสารไม่ปลอดภัย

12. การโจมตีด้วย Phishing

Phishing (การหลอกลวงทางอีเมล/เว็บ) เปรียบเหมือน จดหมายปลอมจากธนาคาร ให้คุณกรอกข้อมูลสำคัญ

ตัวอย่างง่าย ๆ:

คุณได้รับอีเมลดูเหมือนจากธนาคาร คลิกลิงก์แล้วกรอกรหัสผ่าน ข้อมูลคุณถูกขโมย

ตัวอย่างสถานการณ์จริง:

หลายองค์กรโดนโจมตีผ่านอีเมล Phishing ทำให้บัญชีผู้บริหารถูกเข้าถึง

ผลกระทบ:

ข้อมูลสำคัญรั่ว, เงินถูกโอนโดยไม่ได้รับอนุญาต, ระบบถูกบุกรุก

13. การโจมตีด้วย Ransomware

Ransomware (มัลแวร์เรียกค่าไถ่) เปรียบเหมือน โจรล็อกบ้านคุณแล้วขู่เรียกค่าไถ่

ตัวอย่างง่าย ๆ:

คอมพิวเตอร์ถูกล็อก ข้อมูลถูกเข้ารหัส ผู้โจมตีเรียก ransom เพื่อปลดล็อก

ตัวอย่างสถานการณ์จริง:

โรงพยาบาลในสหรัฐฯ ปี 2017 ถูก Ransomware โจมตี ระบบล่มและต้องจ่ายค่าไถ่

ผลกระทบ:

ข้อมูลถูกล็อก, การทำงานล่าช้า, ความเสียหายทางการเงิน

14. การโจมตีด้วย Malware

Malware (มัลแวร์) เปรียบเหมือน เชื้อโรคที่แอบเข้าเครื่องคอมพิวเตอร์ ทำให้ระบบทำงานผิดปกติ

ตัวอย่างง่าย ๆ:

คุณดาวน์โหลดโปรแกรมฟรีจากเว็บไม่ปลอดภัย มัลแวร์เข้ามาและขโมยข้อมูล

ตัวอย่างสถานการณ์จริง:

หลายองค์กรถูกโจมตีด้วย Trojan Malware ทำให้ข้อมูลรั่วไหล

ผลกระทบ:

ข้อมูลถูกขโมย, ระบบล่ม, การทำงานผิดปกติ

15. การโจมตีด้วย Keylogger

Keylogger (บันทึกการกดแป้นพิมพ์) เปรียบเหมือน ผู้โจมตีแอบจดทุกตัวอักษรที่คุณพิมพ์

ตัวอย่างง่าย ๆ:

คุณกรอกรหัสผ่าน ผู้โจมตีได้รับรหัสทันที

ตัวอย่างสถานการณ์จริง:

ผู้โจมตีใช้ Keylogger ในร้านอินเทอร์เน็ตคาเฟ่ ขโมยรหัสผู้ใช้ธนาคาร

ผลกระทบ:

รหัสผ่านและข้อมูลส่วนตัวถูกขโมย, บัญชีถูกเข้าถึง

16. การโจมตีด้วย SQL Injection

SQL Injection (การฉีดคำสั่ง SQL) เปรียบเหมือน แอบเขียนคำสั่งในแบบฟอร์มของร้านค้าให้ร้านค้าทำตามที่เราอยากได้

ตัวอย่างง่าย ๆ:

เว็บมีช่องกรอกชื่อผู้ใช้ ผู้โจมตีใส่คำสั่ง ' ; DROP TABLE users;-- ทำให้ฐานข้อมูลถูกลบ

ตัวอย่างสถานการณ์จริง:

เว็บไซต์องค์กรหลายแห่งเคยโดนโจมตี SQL Injection ทำให้ข้อมูลลูกค้าหลายพันคนรั่ว

ผลกระทบ:

ข้อมูลถูกลบ, ถูกขโมย, หรือระบบล่ม

17. การโจมตีด้วย Cross-Site Scripting (XSS)

XSS (การฝังสคริปต์ข้ามเว็บ) เปรียบเหมือน ผู้โจมตีแอบใส่ไวรัสในจดหมายที่ทุกคนเปิดได้

ตัวอย่างง่าย ๆ:

ผู้โจมตีใส่ <script>alert('Hacked')</script> ในคอมเมนต์ เว็บแสดงข้อความ ทำให้สคริปต์รัน

ตัวอย่างสถานการณ์จริง:

เว็บไซต์ social media หลายแห่งเคยโดน XSS ทำให้ session ของผู้ใช้ถูกขโมย

ผลกระทบ:

บัญชีผู้ใช้ถูกเข้าถึง, ข้อมูลรั่ว, การทำงานผิดปกติ

18. การโจมตีด้วย Cross-Site Request Forgery (CSRF)

CSRF (การปลอมคำขอข้ามเว็บไซต์) เปรียบเหมือน ผู้โจมตีส่งจดหมายลับไปให้คุณทำสิ่งที่คุณไม่รู้ตัว

ตัวอย่างง่าย ๆ:

ผู้โจมตีส่งลิงก์ให้คุณคลิก คุณล็อกอินเว็บธนาคารโดยไม่รู้ตัว เงินถูกโอน

ตัวอย่างสถานการณ์จริง:

เว็บธนาคารหลายแห่งเคยโดน CSRF โอนเงินผู้ใช้โดยไม่ได้รับอนุญาต

ผลกระทบ:

บัญชีผู้ใช้ถูกทำรายการโดยไม่ได้รับอนุญาต, ข้อมูลสำคัญรั่ว

19. การโจมตีด้วย Directory Traversal

Directory Traversal (เข้าถึงไฟล์ลับ) เปรียบเหมือน แอบเปิดประตูหลังบ้านไปหยิบเอกสารสำคัญ

ตัวอย่างง่าย ๆ:

เว็บอนุญาตให้ดาวน์โหลดไฟล์ ผู้โจมตีกรอก ../../secret.txt และเข้าถึงไฟล์ลับ

ตัวอย่างสถานการณ์จริง:

เว็บไซต์หลายแห่งเคยถูกโจมตีด้วย Directory Traversal อ่านไฟล์ config ของ server

ผลกระทบ:

ข้อมูลลับรั่ว, ระบบถูกโจมตี, ความเสียหายต่อความปลอดภัย

20. การโจมตีด้วย Remote Code Execution (RCE)

RCE (รันคำสั่งจากระยะไกล) เปรียบเหมือน ให้คนแปลกหน้าเข้ามาบ้านแล้วสั่งให้คุณทำสิ่งต่าง ๆ

ตัวอย่างง่าย ๆ:

ผู้โจมตีส่งไฟล์อัปโหลดอันตรายที่ทำให้ server รันคำสั่งตามที่เขาต้องการ

ตัวอย่างสถานการณ์จริง:

WordPress เคยโดน RCE ทำให้เว็บถูกเข้าควบคุมโดยแฮกเกอร์

ผลกระทบ:

Server ถูกควบคุม, ข้อมูลรั่ว, ระบบล่ม

21. การโจมตีด้วย Insecure Deserialization

Insecure Deserialization (การแปลงข้อมูลที่ไม่ปลอดภัย) เปรียบเหมือน รับจดหมายที่มีของข้างใน แต่ไม่ตรวจสอบว่าปลอดภัยหรือไม่

ตัวอย่างง่าย ๆ:

เว็บรับข้อมูล Serialized จากผู้ใช้ ผู้โจมตีแก้ไขข้อมูล ทำให้รันคำสั่งอันตราย

ตัวอย่างสถานการณ์จริง:

หลายแอปพลิเคชัน Java ถูกโจมตีแบบนี้ ทำให้รันคำสั่งบน server ได้

ผลกระทบ:

ข้อมูลรั่ว, Server ถูกควบคุม, ระบบล่ม

22. การโจมตีด้วย XML External Entity (XXE)

XXE (การแทรกเอนทิตีภายนอกใน XML) เปรียบเหมือน ส่งจดหมายที่มีช่องว่างแอบซ่อนของอันตราย ตัวอย่างง่าย ๆ:

ผู้โจมตีใส่ `<!ENTITY xxe SYSTEM "file:///etc/passwd">` ใน XML ระบบอ่านไฟล์ที่ไม่ควรเข้าถึง ตัวอย่างสถานการณ์จริง:

องค์กรหลายแห่งโดน XXE อ่านไฟล์ลับและขโมยข้อมูล

ผลกระทบ:

ข้อมูลรั่ว, ระบบล่ม, ความเสียหายต่อความปลอดภัย

23. การโจมตีด้วย Server-Side Request Forgery (SSRF)

SSRF (ปลอมคำขอบน server) เปรียบเหมือน ผู้โจมตีหลอกให้บ้านส่งพัสดุไปยังที่เขาต้องการ ตัวอย่างง่าย ๆ:

ผู้โจมตีส่ง URL ภายในองค์กรให้ server ดึงข้อมูล ผู้โจมตีเข้าถึงข้อมูล internal

ตัวอย่างสถานการณ์จริง:

หลาย cloud server ถูก SSRF ให้เข้าถึง metadata และข้อมูลลับ

ผลกระทบ:

ข้อมูลภายในรั่ว, ระบบถูกโจมตี, ความเสียหายต่อองค์กร

24. การโจมตีด้วย Insecure Direct Object Reference (IDOR)

IDOR (เข้าถึงวัตถุโดยตรง) เปรียบเหมือน เปลี่ยนหมายเลขห้องแล้วเข้าห้องคนอื่นโดยไม่ได้รับอนุญาต ตัวอย่างง่าย ๆ:

เว็บส่งลิงก์ `file_id=123` ผู้โจมตีเปลี่ยนเป็น `file_id=124` และดาวน์โหลดไฟล์คนอื่น

ตัวอย่างสถานการณ์จริง:

หลายเว็บแชร์เอกสารถูกโจมตี IDOR ทำให้ไฟล์รั่ว

ผลกระทบ:

ข้อมูลส่วนตัวถูกขโมย, ความเสียหายต่อความเชื่อถือ

25. การโจมตีด้วย Security Misconfiguration

Security Misconfiguration (ตั้งค่าความปลอดภัยผิดพลาด) เปรียบเหมือน บ้านมีประตูลืมล็อก, หน้าต่างแตก

ตัวอย่างง่าย ๆ:

Server เปิด port ไม่จำเป็น, ใช้รหัสผ่าน default

ตัวอย่างสถานการณ์จริง:

หลายองค์กรถูกสแกนหา port ที่เปิด และโดนเข้าควบคุม

ผลกระทบ:

ข้อมูลรั่ว, Server ถูกโจมตี, ระบบไม่ปลอดภัย

26. การโจมตีด้วย Sensitive Data Exposure

Sensitive Data Exposure (ข้อมูลสำคัญรั่ว) เปรียบเหมือน ส่งจดหมายสำคัญโดยไม่ใส่ซอง

ตัวอย่างง่าย ๆ:

เว็บส่งรหัสผ่านผ่าน HTTP ไม่เข้ารหัส ผู้โจมตีดักข้อมูลได้

ตัวอย่างสถานการณ์จริง:

เว็บไซต์หลายแห่งเคยส่งข้อมูลบัตรเครดิตแบบไม่เข้ารหัส ทำให้ข้อมูลรั่ว

ผลกระทบ:

ข้อมูลส่วนตัวรั่ว, เงินและบัญชีถูกขโมย

27. การโจมตีด้วย Broken Cryptography

Broken Cryptography (เข้ารหัสอ่อนแอ) เปรียบเหมือน ล็อกตู้เย็นด้วยกุญแจทำจากกระดาษ

ตัวอย่างง่าย ๆ:

ใช้ MD5 hash สำหรับรหัสผ่านง่ายต่อการถอดรหัส

ตัวอย่างสถานการณ์จริง:

หลายระบบเก่าใช้ MD5 ทำให้รหัสผ่านถูก brute-force

ผลกระทบ:

รหัสผ่านและข้อมูลสำคัญถูกขโมย

28. การโจมตีด้วย Insufficient Logging & Monitoring

Insufficient Logging & Monitoring (ขาดการบันทึกและตรวจสอบ) เปรียบเหมือน บ้านไม่มีกล้องหรือสัญญาณเตือน

ตัวอย่างง่าย ๆ:

ไม่มีระบบบันทึกการเข้าออกของผู้ใช้หรือ admin

ตัวอย่างสถานการณ์จริง:

หลาย breach เกิดขึ้นแต่ตรวจไม่ทันเพราะไม่มี log

ผลกระทบ:

ตรวจสอบไม่ได้, ผู้โจมตีลบทำลายข้อมูล

29. การโจมตีด้วย Insecure Components

Insecure Components (ส่วนประกอบไม่ปลอดภัย) เปรียบเหมือน บ้านมีหน้าต่างเก่า, ประตู

ตัวอย่างง่าย ๆ:

ใช้ library เวอร์ชันเก่าที่มีบั๊ก ผู้โจมตีใช้ช่องโหว่เข้าควบคุมระบบ

ตัวอย่างสถานการณ์จริง:

WordPress plugin เก่าโดนโจมตี ทำให้เว็บโดนแฮ็ก

ผลกระทบ:

ระบบล่ม, ข้อมูลรั่ว, server ถูกควบคุม

30. การโจมตีด้วย Insufficient Security Config on Cloud

Insufficient Cloud Security (ตั้งค่า Cloud ไม่ปลอดภัย) เปรียบเหมือน เก็บของสำคัญบนระเบียง บ้านโดยไม่ล็อก

ตัวอย่างง่าย ๆ:

S3 bucket เปิด public ผู้โจมตีดาวน์โหลดข้อมูลทั้งหมด

ตัวอย่างสถานการณ์จริง:

หลายองค์กร AWS S3 bucket ถูกสแกนและข้อมูลรั่ว

ผลกระทบ:

ข้อมูลสำคัญรั่ว, เสียความเชื่อถือ

31. การโจมตีด้วย Open Redirect

Open Redirect (ลิงก์เปลี่ยนทางไม่ปลอดภัย) เปรียบเหมือน คนที่คุณเชื่อใจบอกทางผิดไปหาโจร

ตัวอย่างง่าย ๆ:

ลิงก์เว็บ example.com?url=malicious.com ผู้ใช้คลิกแล้วโดน phishing

ตัวอย่างสถานการณ์จริง:

หลายเว็บใช้ redirect แบบเปิด ทำให้ผู้ใช้โดนหลอก

ผลกระทบ:

ผู้ใช้โดนหลอก, ข้อมูลรั่ว, ความเสียหายต่อความเชื่อถือ

32. การโจมตีด้วย Clickjacking

Clickjacking (การหลอกคลิก) เปรียบเหมือน แปะกระจกให้คุณกดปุ่มโดยไม่รู้ตัว

ตัวอย่างง่าย ๆ:

ผู้ใช้คิดว่ากดปุ่ม Like แต่จริง ๆ กดปุ่มโอนเงิน

ตัวอย่างสถานการณ์จริง:

หลาย social media เคยโดน Clickjacking ทำให้บัญชีถูกใช้โดยไม่ได้รับอนุญาต

ผลกระทบ:

บัญชีถูกใช้ผิด, ข้อมูลรั่ว, การทำงานผิดปกติ

33. การโจมตีด้วย Password Recovery Flaws

Password Recovery Flaws (ระบบกู้รหัสผ่านไม่ปลอดภัย) เปรียบเหมือน ให้ใครก็ได้เปลี่ยนรหัสบ้านคุณ

ตัวอย่างง่าย ๆ:

เว็บถามคำถามง่าย เช่น "ชื่อสัตว์เลี้ยง?" ผู้โจมตีเดาแล้วรีเซตรหัสผ่าน

ตัวอย่างสถานการณ์จริง:

หลายเว็บโดนโจมตีด้วยวิธีนี้ ทำให้บัญชีผู้ใช้ถูกเข้าถึง

ผลกระทบ:

บัญชีถูกแฮ็ก, ข้อมูลรั่ว

34. การโจมตีด้วย Insecure API

Insecure API (API ไม่ปลอดภัย) เปรียบเหมือน ให้คนแปลกหน้าโทรเข้าบ้านแล้วสั่งทำทุกอย่าง

ตัวอย่างง่าย ๆ:

API ส่งข้อมูลสำคัญโดยไม่ตรวจสอบสิทธิ์

ตัวอย่างสถานการณ์จริง:

หลาย mobile app ถูกโจมตี API ทำให้ข้อมูลผู้ใช้รั่ว

ผลกระทบ:

ข้อมูลผู้ใช้รั่ว, ระบบถูกโจมตี

35. การโจมตีด้วย Mass Assignment

Mass Assignment (การส่งข้อมูลมากเกินไป) เปรียบเหมือน ผู้โจมตีกรอกทุกช่องในแบบฟอร์มโดยไม่ได้รับอนุญาต

ตัวอย่างง่าย ๆ:

ผู้ใช้ส่งฟิลด์ admin=true ผ่าน form ทำให้บัญชีธรรมดาเป็น admin

ตัวอย่างสถานการณ์จริง:

หลายเว็บโดน Mass Assignment ทำให้ผู้ใช้ปกติกลายเป็น admin

ผลกระทบ:

ผู้โจมตีได้สิทธิ์สูง, ระบบถูกควบคุม

36. การโจมตีด้วย Buffer Overflow

Buffer Overflow (ล้นบัฟเฟอร์) เปรียบเหมือน เต็มน้ำเต็มแก้วจนล้นและทำให้เครื่องเสียหาย

ตัวอย่างง่าย ๆ:

โปรแกรมรับข้อมูลยาวเกิน ทำให้ memory ถูกเขียนเกินขอบเขต

ตัวอย่างสถานการณ์จริง:

หลายโปรแกรม C/C++ ถูกโจมตี buffer overflow ทำให้รันคำสั่งอันตราย

ผลกระทบ:

ระบบล่ม, ข้อมูลรั่ว, server ถูกควบคุม

37. การโจมตีด้วย Race Condition

Race Condition (เงื่อนไขแข่งขัน) เปรียบเหมือน สองคนพร้อมกันเปิดลิ้นชักเดียวกัน ทำให้เกิดความผิดพลาด

ตัวอย่างง่าย ๆ:

ผู้ใช้สองคนส่งคำสั่งถอนเงินพร้อมกัน ทำให้เงินถูกถอนเกิน

ตัวอย่างสถานการณ์จริง:

หลายเว็บธนาคารเคยเจอปัญหา race condition ทำให้เงินถูกถอนเกิน

ผลกระทบ:

ข้อมูลไม่ถูกต้อง, ระบบเสียหาย, การเงินสูญหาย

38. การโจมตีด้วย Improper Error Handling

Improper Error Handling (จัดการข้อผิดพลาดไม่ดี) เปรียบเหมือน บ้านไฟไหม้แต่ไม่แจ้งสัญญาณเตือน

ตัวอย่างง่าย ๆ:

เว็บแจ้ง error ตอบกลับแบบเต็ม เช่น path ของไฟล์หรือโค้ดของ server

ตัวอย่างสถานการณ์จริง:

หลายเว็บไซต์ stack trace ทำให้แฮกเกอร์เห็นโครงสร้างระบบ

ผลกระทบ:

แฮกเกอร์สามารถวางแผนโจมตี, ระบบรั่ว

39. การโจมตีด้วย Information Disclosure

Information Disclosure (ข้อมูลรั่ว) เปรียบเหมือน หนังสือสำคัญหลบหนทางสาธารณะ

ตัวอย่างง่าย ๆ:

เว็บไซต์ข้อมูลส่วนตัวผู้ใช้โดยไม่ตั้งใจ

ตัวอย่างสถานการณ์จริง:

หลายเว็บ social media ไซต์ email หรือเบอร์โทรผู้ใช้โดยไม่ตั้งใจ

ผลกระทบ:

ข้อมูลส่วนตัวรั่ว, การโจมตีอื่นตามมา

40. การโจมตีด้วย Business Logic Flaw

Business Logic Flaw (ข้อบกพร่องเชิงตรรกะธุรกิจ) เปรียบเหมือน เล่นเกมแล้วเจอช่องโหว่โกงคะแนน

ตัวอย่างง่าย ๆ:

ระบบให้ผู้ใช้ redeem coupon ซ้ำ ๆ โดยไม่จำกัด

ตัวอย่างสถานการณ์จริง:

เว็บไซต์ขายตั๋วเคยเจอปัญหาซื้อบัตรฟรีด้วย logic flaw

ผลกระทบ:

เสียเงิน, ข้อมูลถูกใช้ผิดวิธี

41. การโจมตีด้วย Denial of Service (DoS)

DoS (โจมตีทำให้ระบบล่ม) เปรียบเหมือน ขวางหินเต็มประตูบ้าน ทำให้ไม่สามารถเข้าออกได้

ตัวอย่างง่าย ๆ:

ส่ง request จำนวนมากทำให้เว็บล่ม

ตัวอย่างสถานการณ์จริง:

เว็บไซต์รัฐบาลหลายแห่งโดน DoS ล่ม

ผลกระทบ:

ระบบไม่พร้อมใช้, เสียโอกาสธุรกิจ

42. การโจมตีด้วย Distributed Denial of Service (DDoS)

DDoS (โจมตีล้มหลายเครื่อง) เปรียบเหมือน คนหลายพันคนมารุมประตูบ้านพร้อมกัน

ตัวอย่างง่าย ๆ:

Botnet ส่ง traffic จำนวนมหาศาลทำให้ server ล่ม

ตัวอย่างสถานการณ์จริง:

หลายเว็บไซต์ใหญ่ เช่น Amazon, Twitter เคยโดน DDoS

ผลกระทบ:

ระบบล่ม, การบริการหยุดชะงัก

43. การโจมตีด้วย DNS Spoofing

DNS Spoofing (ปลอม DNS) เปรียบเหมือน เปลี่ยนป้ายชื่อบ้าน ให้ผู้คนไปผิดบ้าน

ตัวอย่างง่าย ๆ:

ผู้โจมตีเปลี่ยน DNS server ทำให้ผู้ใช้เข้าเว็บปลอม

ตัวอย่างสถานการณ์จริง:

หลายครั้งผู้ใช้โดนหลอกเข้าเว็บ phishing เพราะ DNS spoofing

ผลกระทบ:

ข้อมูลรั่ว, การโจมตี phishing

44. การโจมตีด้วย ARP Spoofing

ARP Spoofing (ปลอม ARP) เปรียบเหมือน แอบบอกให้คนส่งจดหมายไปที่บ้านโจรแทนบ้านคุณ

ตัวอย่างง่าย ๆ:

ผู้โจมตีแทรกตัวใน network local ทำให้ข้อมูลผ่านไปที่เขาก่อน

ตัวอย่างสถานการณ์จริง:

หลาย office network ถูก ARP spoofing ดักข้อมูล

ผลกระทบ:

ข้อมูลรั่ว, การสื่อสารไม่ปลอดภัย

45. การโจมตีด้วย SQL Injection

SQL Injection (SQL Injection) เปรียบเหมือน คนแอบใส่ข้อความแปลก ๆ ในแบบฟอร์มของร้าน เพื่อขโมยสมุดบัญชีของร้าน

ตัวอย่างง่าย ๆ:

เว็บร้านค้าออนไลน์มีช่องกรอกชื่อผู้ใช้ แต่ไม่ตรวจสอบข้อมูล ผู้โจมตีใส่คำสั่งพิเศษ เช่น ‘ OR ‘1’=‘1’ ทำให้เข้าถึงฐานข้อมูลของเว็บได้

ตัวอย่างสถานการณ์จริง:

เว็บ e-commerce หลายแห่งถูกแฮกเกอร์ใช้ SQL Injection ขโมยข้อมูลลูกค้า เช่น รหัสผ่าน, ข้อมูลบัตรเครดิต, หรือประวัติการสั่งซื้อ

ผลกระทบ:

ข้อมูลส่วนตัวรั่ว, บัญชีถูกแฮก, อาจเกิดความเสียหายทางการเงินและความเชื่อถือขององค์กร

เปรียบเทียบกับง่าย ๆ:

เหมือนคุณให้ใครสักคนเขียนโน้ตในสมุดบัญชีของร้านโดยไม่ตรวจสอบ แล้วเขาใช้โน้ตนั้นขโมยเงินจากบัญชีร้าน

46. การโจมตีด้วย Wi-Fi Eavesdropping

Wi-Fi Eavesdropping (ดักฟัง Wi-Fi) เปรียบเหมือน ยืนฟังคนคุยในร้านกาแฟโดยไม่让他รู้ตัว

ตัวอย่างง่าย ๆ:

ผู้โจมตีเชื่อมต่อ Wi-Fi สาธารณะ แล้วดักจับข้อมูลที่ส่งผ่าน เช่น รหัสผ่านหรือหมายเลขบัตรเครดิต

ตัวอย่างสถานการณ์จริง:

หลายคนใช้ Wi-Fi ฟรีในสนามบินหรือร้านกาแฟ ถูกแฮกเกอร์ดักข้อมูล ทำให้บัญชีธนาคารหรือ email รั่ว

ผลกระทบ:

ข้อมูลส่วนตัวและบัญชีเงินรั่ว, อาจถูกขโมยเงิน

47. การโจมตีด้วย Man-in-the-Middle (MITM)

MITM (คนกลางแอบฟังหรือแก้ไขข้อมูล) เปรียบเหมือน คนแอบอยู่ระหว่างคุณกับธนาคาร ทำให้เขาเห็นและแก้ไขจดหมายที่คุณส่ง

ตัวอย่างง่าย ๆ:

ผู้โจมตี intercept การสื่อสาร HTTP ไม่เข้ารหัส เปลี่ยนข้อมูลโอนเงิน

ตัวอย่างสถานการณ์จริง:

หลายครั้ง Wi-Fi สาธารณะทำให้ MITM เกิดขึ้น และผู้โจมตีเปลี่ยนข้อมูลโอนเงินออนไลน์

ผลกระทบ:

ข้อมูลรั่ว, เงินหาย, ระบบถูกควบคุม

48. การโจมตีด้วย Social Engineering

Social Engineering (หลอกคนให้เปิดเผยข้อมูล) เปรียบเหมือน โจรแก๊งทำตัวเป็นเจ้าหน้าที่ธนาคาร แล้วถามรหัสผ่าน

ตัวอย่างง่าย ๆ:

โทรศัพท์ไปหาพนักงานบริษัท อ้างว่าเป็นฝ่าย IT แล้วขอรหัสผ่าน

ตัวอย่างสถานการณ์จริง:

หลายองค์กรถูกหลอกให้เปิด email attachment หรือส่งรหัสผ่าน ทำให้ระบบรั่ว

ผลกระทบ:

ข้อมูลรั่ว, บัญชีถูกแฮ็ก, ความเสียหายต่อองค์กร

49. การโจมตีด้วย Phishing

Phishing (หลอกให้คลิกลิงก์หรือกรอกข้อมูล) เปรียบเหมือน ส่งจดหมายปลอมจากธนาคารให้คุณ กรอกข้อมูลสำคัญ

ตัวอย่างง่าย ๆ:

Email ปลอมส่งลิงก์ไปให้ login เว็บปลอม ผู้ใช้กรอก username/password

ตัวอย่างสถานการณ์จริง:

หลายบริษัท, ธนาคาร, social media ถูก phishing ทำให้บัญชีและข้อมูลผู้ใช้รั่ว

ผลกระทบ:

ข้อมูลรั่ว, บัญชีถูกแฮ็ก, เสียความเชื่อถือ

50. การโจมตีด้วย Ransomware

Ransomware (มัลแวร์เรียกค่าไถ่) เปรียบเหมือน โจรล็อกบ้านคุณแล้วขอเงินเพื่อปลดล็อก

ตัวอย่างง่าย ๆ:

คอมพิวเตอร์ติด ransomware ข้อมูลทั้งหมดถูกเข้ารหัส ผู้ใช้ต้องจ่ายเงินเพื่อกู้

ตัวอย่างสถานการณ์จริง:

โรงพยาบาลหลายแห่งทั่วโลกเคยโดน ransomware ทำให้ระบบ EMR (ข้อมูลผู้ป่วย) ใช้งานไม่ได้

ผลกระทบ:

ข้อมูลถูกล็อก, ต้องจ่ายค่าไถ่, ระบบหยุดชะงัก, เสียเงินและเสียความเชื่อถือ

51. การโจมตีด้วย Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) เปรียบเหมือน คนแอบวางข้อความลวงให้คนอื่นอ่านแล้วคลิกลิงก์ที่อันตราย

ตัวอย่างง่าย ๆ: เว็บบอร์ดไม่ตรวจสอบข้อความผู้ใช้ ผู้โจมตีใส่ <script> เพื่อแอบขโมย cookie ของผู้ใช้

ตัวอย่างสถานการณ์จริง: เว็บ social media ถูกโจมตี XSS ทำให้ผู้ใช้บางคนถูกขโมย session และ login อัตโนมัติ

ผลกระทบ: บัญชีถูกแฮ็ก, ข้อมูลส่วนตัวรั่ว

เปรียบเทียบง่าย ๆ: เหมือนคุณโพสต์โน้ตในห้องสมุด แล้วใครสักคนแอบใส่ข้อความปลอมให้คนอื่นคลิก และโดนขโมยของ

52. การโจมตีด้วย Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) เปรียบเหมือน คนแอบส่งคำสั่งให้คุณโดยที่คุณไม่รู้ตัว

ตัวอย่างง่าย ๆ: ผู้โจมตีส่งลิงก์อีเมล ให้ผู้ใช้คลิก โดยไม่รู้ตัว ระบบทำงานเหมือนผู้ใช้สั่งเอง เช่น โอนเงิน

ตัวอย่างสถานการณ์จริง: เว็บธนาคารบางแห่งเคยถูก CSRF ทำให้เงินถูกโอนออกจากบัญชีโดยเจ้าของบัญชีไม่รู้

ผลกระทบ: เงินหาย, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนคุณเผลอกดปุ่มให้คนอื่นสั่งของแทนคุณโดยไม่รู้ตัว

53. การโจมตีด้วย DNS Spoofing

DNS Spoofing (ปลอมแปลง DNS) เปรียบเหมือน คนแอบเปลี่ยนแผนที่ร้านให้คุณเดินไปผิดที่

ตัวอย่างง่าย ๆ: ผู้โจมตีแก้ DNS ของเว็บไซต์ธนาคาร ทำให้ผู้ใช้เข้าพอร์ทัลปลอม

ตัวอย่างสถานการณ์จริง: ผู้ใช้เข้าเว็บธนาคารแต่โดน DNS Spoofing ข้อมูล login ถูกขโมย

ผลกระทบ: ข้อมูลรั่ว, บัญชีถูกแฮ็ก

เปรียบเทียบง่าย ๆ: เหมือนคุณเดินตาม GPS แต่ใครสักคนเปลี่ยนพิกัดให้คุณไปที่บ้านโจร

54. การโจมตีด้วย Malware

Malware (มัลแวร์) เปรียบเหมือน ไวรัสที่แอบเข้ามาในคอมพิวเตอร์ของคุณ

ตัวอย่างง่าย ๆ: เปิดไฟล์แนบ email แล้วติดไวรัส คอมพิวเตอร์ทำงานช้าหรือถูกขโมยข้อมูล

ตัวอย่างสถานการณ์จริง: หลายน้องกรติดมัลแวร์ ทำให้ไฟล์ถูกเข้ารหัสหรือข้อมูลรั่ว

ผลกระทบ: ข้อมูลรั่ว, ระบบช้าหรือเสียหาย

เปรียบเทียบง่าย ๆ: เหมือนคุณเอาอาหารติดเชื้อเข้าบ้าน ทำให้ทุกอย่างในครัวเน่า

55. การโจมตีด้วย Brute Force

Brute Force (ลองรหัสหลายครั้ง) เปรียบเหมือน คนพยายามเดากุญแจบ้านที่ละรหัสจนสำเร็จ

ตัวอย่างง่าย ๆ: ผู้โจมตีใช้โปรแกรมลองรหัสผ่านบัญชีออนไลน์หลายล้านรหัสจนถูก

ตัวอย่างสถานการณ์จริง: หลายบัญชีอีเมลหรือ social media ถูก Brute Force จนผู้โจมตีเข้าถึง

ผลกระทบ: บัญชีถูกแฮ็ก, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนใครสักคนลองเปิดประตูบ้านด้วยกุญแจหลายร้อยแบบ จนเปิดได้

56. การโจมตีด้วย Keylogger

Keylogger (โปรแกรมบันทึกแป้นพิมพ์) เปรียบเหมือน คนแอบส่องว่าคุณพิมพ์รหัสผ่านหรือข้อความลับอะไร

ตัวอย่างง่าย ๆ: ติดตั้ง keylogger บนคอมพิวเตอร์ ผู้โจมตีเห็นทุกสิ่งที่คุณพิมพ์

ตัวอย่างสถานการณ์จริง: ผู้ใช้ติด keylogger จากไฟล์แนบ email ทำให้รหัสผ่านบัญชีธนาคารถูกขโมย

ผลกระทบ: ข้อมูลรั่ว, บัญชีถูกแฮ็ก, เสียเงิน

เปรียบเทียบง่าย ๆ: เหมือนมีคนแอบมองนิ้วของคุณพิมพ์รหัสลับ

57. การโจมตีด้วย RCE (Remote Code Execution)

Remote Code Execution (RCE) เปรียบเหมือน คนแอบสั่งให้คอมพิวเตอร์ของคุณทำงานแทนเขาโดยไม่รู้ตัว

ตัวอย่างง่าย ๆ: โปรแกรมเว็บมีช่องโหว่ ผู้โจมตีส่งคำสั่ง ทำให้ server ทำงานตามคำสั่งโจร

ตัวอย่างสถานการณ์จริง: เว็บไซต์องค์กรถูกโจมตี RCE ทำให้ server ถูกใช้ส่ง spam หรือขโมยข้อมูล

ผลกระทบ: ระบบถูกควบคุม, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนใครสักคนสั่งเครื่องจักรในโรงงานของคุณทำงานแทนเขาโดยคุณไม่รู้

58. การโจมตีด้วย Session Hijacking

Session Hijacking (ขโมย session) เปรียบเหมือน คนแอบใช้บัตรเข้าห้องของคุณโดยไม่รู้ตัว

ตัวอย่างง่าย ๆ: ผู้โจมตีขโมย session cookie เข้าเว็บแทนผู้ใช้

ตัวอย่างสถานการณ์จริง: ผู้ใช้ social media โดน session hijack ทำให้บัญชีถูกควบคุม

ผลกระทบ: ข้อมูลรั่ว, บัญชีถูกแฮ็ก

เปรียบเทียบง่าย ๆ: เหมือนใครสักคนหยิบบัตรสมาชิกของคุณไปใช้

59. การโจมตีด้วย Drive-by Download

Drive-by Download (ดาวน์โหลดมัลแวร์อัตโนมัติ) เปรียบเหมือน คุณแค่เข้าเว็บธรรมดาแล้วโดนวางเชื้อทันที

ตัวอย่างง่าย ๆ: เข้าเว็บไซต์ติดมัลแวร์โดยไม่คลิกอะไร โปรแกรมถูกดาวน์โหลดอัตโนมัติ

ตัวอย่างสถานการณ์จริง: เว็บข่าวบางแห่งถูกฝัง malware ทำให้ผู้เข้าเว็บติดไวรัสทันที

ผลกระทบ: คอมพิวเตอร์ติดมัลแวร์, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนคุณเดินเข้าบ้านเพื่อนแล้วโดนวางของเสียในกระเป๋าโดยไม่รู้

60. การโจมตีด้วย Backdoor

Backdoor (ประตูหลัง) เปรียบเหมือน คนแอบสร้างประตูลับเข้าออกบ้านคุณ

ตัวอย่างง่าย ๆ: โปรแกรมติด backdoor ผู้โจมตีเข้าควบคุมเครื่องได้ทุกเมื่อ

ตัวอย่างสถานการณ์จริง: Server บริษัทถูก backdoor ทำให้ hacker เข้าไปขโมยข้อมูล

ผลกระทบ: ข้อมูลรั่ว, ระบบถูกควบคุม

เปรียบเทียบง่าย ๆ: เหมือนมีประตูลับให้โจรเข้าบ้านคุณได้ตลอดเวลา

61. การโจมตีด้วย Trojan

Trojan (โทรจัน) เปรียบเหมือนม้าโทรจันในตำนานกรีก คือดูเหมือนไม่อันตราย แต่แอบซ่อนโจรไว้ข้างใน

ตัวอย่างง่าย ๆ: เปิดไฟล์แนบ email ที่แอบมี trojan โปรแกรมจะติดตั้งตัวเองในเครื่อง

ตัวอย่างสถานการณ์จริง: ผู้ใช้หลายรายติด trojan ทำให้ข้อมูลถูกขโมยหรือเครื่องถูกควบคุม

ผลกระทบ: ข้อมูลรั่ว, ระบบถูกควบคุม

เปรียบเทียบง่าย ๆ: เหมือนรับของขวัญจากใคร แต่ข้างในซ่อนโจรไว้

62. การโจมตีด้วย Worm

Worm (เวิร์ม) เปรียบเหมือน ไวรัสที่เดินทางเองจากเครื่องหนึ่งไปอีกเครื่องหนึ่งโดยไม่ต้องรอคนคลิก

ตัวอย่างง่าย ๆ: Worm แพร่ตัวผ่านเครือข่าย ทำให้เครื่องหลายเครื่องติดไวรัส

ตัวอย่างสถานการณ์จริง: WannaCry เป็น worm ที่ทำให้โรงพยาบาลทั่วโลกหยุดให้บริการ

ผลกระทบ: ระบบล่ม, ข้อมูลรั่ว, เสียเงิน

เปรียบเทียบง่าย ๆ: เหมือนไฟไหม้ลามจากบ้านหนึ่งไปอีกหลายหลังโดยไม่ต้องจุดไฟเอง

63. การโจมตีด้วย Adware

Adware (โฆษณาแอบแฝง) เปรียบเหมือน ใส่โปสเตอร์โฆษณาในบ้านโดยไม่ถามเจ้าของ

ตัวอย่างง่าย ๆ: โปรแกรมฟรีแอบติด adware ทำให้โฆษณาปรากฏทุกครั้งที่ใช้คอม

ตัวอย่างสถานการณ์จริง: ผู้ใช้หลายคนติด adware ทำให้ browser ช้าและโฆษณารบกวน

ผลกระทบ: ประสบการณ์ใช้งานแย่, เสียเวลา

เปรียบเทียบง่าย ๆ: เหมือนใครสักคนแอบติดโปสเตอร์ในบ้านคุณโดยคุณไม่รู้

64. การโจมตีด้วย Spyware

Spyware (สปายแวร์) เปรียบเหมือนคนแอบสอดแนมพฤติกรรมคุณทุกวัน

ตัวอย่างง่าย ๆ: โปรแกรมติด spyware เก็บเว็บไซต์ที่คุณเข้า, พิมพ์อะไร, แล้วส่งให้โจร

ตัวอย่างสถานการณ์จริง: ผู้ใช้หลายคนติด spyware ทำให้ข้อมูลการเงินหรือ login รั่ว

ผลกระทบ: ข้อมูลรั่ว, ถูกติดตามพฤติกรรม

เปรียบเทียบง่าย ๆ: เหมือนมีสายลับแอบตามคุณทุกที่

65. การโจมตีด้วย Botnet

Botnet (เครือข่ายหุ่นยนต์) เปรียบเหมือน ฟองหุ่นยนต์ที่ถูกสั่งโดยคนเดียว

ตัวอย่างง่าย ๆ: คอมพิวเตอร์หลายเครื่องถูก malware เปลี่ยนเป็น bot ทำงานตามโจรสั่ง

ตัวอย่างสถานการณ์จริง: Botnet ถูกใช้โจมตีเว็บหรือส่ง spam จำนวนมาก

ผลกระทบ: ระบบล่ม, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนฝูงหุ่นยนต์ที่คุณไม่ควบคุม ทำงานตามโจรสั่ง

66. การโจมตีด้วย Zero-Day

Zero-Day (ช่องโหว่วันแรก) เปรียบเหมือน ช่องโหว่บ้านที่ยังไม่มีใครรู้จัก

ตัวอย่างง่าย ๆ: Hacker ใช้ bug ใหม่ในโปรแกรม ก่อนผู้พัฒนาป้องกัน

ตัวอย่างสถานการณ์จริง: บริษัทหลายแห่งถูกโจมตี Zero-Day ก่อน patch ออก

ผลกระทบ: ข้อมูลรั่ว, ระบบถูกควบคุม

เปรียบเทียบง่าย ๆ: เหมือนโจรเจอประตูหลังบ้านใหม่ที่เจ้าของยังไม่วาง

67. การโจมตีด้วย Directory Traversal

Directory Traversal (เข้าถึงไฟล์ลับ) เปรียบเหมือน ใครสักคนปีนกำแพงเข้าถึงห้องเก็บเอกสารลับ

ตัวอย่างง่าย ๆ: เว็บไม่ป้องกัน path ผู้โจมตีเรียกไฟล์ระบบ

ตัวอย่างสถานการณ์จริง: เว็บหลายแห่งถูก directory traversal ทำให้ไฟล์ config หรือ password รั่ว

ผลกระทบ: ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนโจรแอบปีนเข้าห้องลับบ้านคุณ

68. การโจมตีด้วย File Inclusion

File Inclusion (แอบใส่ไฟล์) เปรียบเหมือน ใส่เอกสารแปลกเข้ามาในแฟ้มสำคัญ

ตัวอย่างง่าย ๆ: เว็บ PHP รับไฟล์ไม่ตรวจสอบ ผู้โจมตีอัปโหลดไฟล์ malicious

ตัวอย่างสถานการณ์จริง: เว็บหลายแห่งถูก file inclusion ทำให้ attacker รันคำสั่งใน server

ผลกระทบ: ระบบถูกควบคุม, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนใส่กระดาษปลอมเข้าแฟ้มสำคัญแล้วถูกขโมยข้อมูล

69. การโจมตีด้วย XML External Entity (XXE)

XML External Entity (XXE) เปรียบเหมือน ใส่เอกสารลับในจดหมายแล้วสั่งให้คนเปิด

ตัวอย่างง่าย ๆ: เว็บ parse XML ผู้โจมตีฝัง URL ไปยังไฟล์สำคัญใน server

ตัวอย่างสถานการณ์จริง: หลายระบบที่ parse XML ถูก XXE ขโมยไฟล์ config และข้อมูลส่วนตัว

ผลกระทบ: ข้อมูลรั่ว, ระบบถูกควบคุม

เปรียบเทียบง่าย ๆ: เหมือนคุณส่งจดหมายธรรมดาแต่ข้างในมีคำสั่งให้เปิดประตูลับ

70. การโจมตีด้วย Clickjacking

Clickjacking (หลอกคลิก) เปรียบเหมือน วางแผ่นใสบนปุ่มให้คุณกดโดยไม่รู้ตัว

ตัวอย่างง่าย ๆ: ผู้ใช้เห็นปุ่มถูกต้อง แต่กดแล้วทำงานต่างจากที่เห็น

ตัวอย่างสถานการณ์จริง: ผู้ใช้ social media ถูก clickjacking ทำให้กด like หรือ share โดยไม่รู้ตัว

ผลกระทบ: การควบคุมบัญชี, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนกดปุ่มลิฟต์ที่คิดว่าจะขึ้น แต่จริง ๆ เป็นสวิตช์ปล่อยน้ำ

71. การโจมตีด้วย Password Spraying

Password Spraying (ลองรหัสเป็นชุด) เปรียบเหมือน คนลองกุญแจบ้านหลายหลังด้วยรหัสง่าย ๆ เช่น 1234

ตัวอย่างง่าย ๆ: Hacker ลองรหัสผ่านทั่วไปกับหลายบัญชี แต่ไม่ลองหลายครั้งต่อบัญชี

ตัวอย่างสถานการณ์จริง: อีเมลองค์กรหลายแห่งถูก password spraying จนบางบัญชีถูกแฮ็ก

ผลกระทบ: บัญชีถูกแฮ็ก, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนโจรลองกุญแจง่าย ๆ กับหลายบ้านจนเปิดได้

72. การโจมตีด้วย Session Fixation

Session Fixation (ยึด session เดิม) เปรียบเหมือน ใครสักคนเอาบัตรเข้าห้องของคุณแล้วใช้มันล็อกตัวเองเข้า

ตัวอย่างง่าย ๆ: ผู้โจมตีส่ง session ID ให้ผู้ใช้ login แล้วเข้าบัญชีผู้ใช้

ตัวอย่างสถานการณ์จริง: เว็บหลายแห่งถูกโจมตี session fixation ทำให้บัญชีถูกควบคุม

ผลกระทบ: ข้อมูลรั่ว, บัญชีถูกแฮ็ก

เปรียบเทียบง่าย ๆ: เหมือนใครสักคนใช้กุญแจของคุณแล้วเข้าไปบ้านก่อนคุณ

73. การโจมตีด้วย Insecure Direct Object References (IDOR)

IDOR (เข้าถึงวัตถุโดยตรง) เปรียบเหมือน ใครสักคนเดาหมายเลขแฟ้มลับแล้วเปิดได้

ตัวอย่างง่าย ๆ: URL เช่น /document/123 ผู้โจมตีเปลี่ยนเป็น /document/124 แล้วเข้าถึงข้อมูลของคนอื่น

ตัวอย่างสถานการณ์จริง: เว็บองค์กรหลายแห่งมี IDOR ทำให้ข้อมูลพนักงานรั่ว

ผลกระทบ: ข้อมูลรั่ว, ความเป็นส่วนตัวถูกละเมิด

เปรียบเทียบง่าย ๆ: เหมือนใครสักคนเดาหมายเลขกล่องจดหมายแล้วเปิดอ่าน

74. การโจมตีด้วย Cross-Site Request Forgery (CSRF)

CSRF (ปลอมคำขอเว็บไซต์) เปรียบเหมือน ใครสักคนแอบส่งคำสั่งแทนคุณโดยที่คุณไม่รู้ตัว

ตัวอย่างง่าย ๆ: ผู้ใช้ login เว็บธนาคาร แล้วคลิกลิงก์ใน email ผู้โจมตีส่งคำสั่งโอนเงินแทนผู้ใช้

ตัวอย่างสถานการณ์จริง: เว็บหลายแห่งถูก CSRF ทำให้บัญชีผู้ใช้ถูกโอนเงินโดยไม่รู้ตัว

ผลกระทบ: เงินหาย, บัญชีถูกควบคุม

เปรียบเทียบง่าย ๆ: เหมือนใครสักคนส่งจดหมายขอเงินแทนคุณโดยคุณไม่เห็น

75. การโจมตีด้วย Cross-Site Scripting (XSS)

XSS (ฝังสคริปต์ในเว็บ) เปรียบเหมือน ใครสักคนวางข้อความอันตรายในสมุดเยี่ยมร้าน คุณอ่านแล้วติดไวรัส

ตัวอย่างง่าย ๆ: ผู้โจมตีฝัง JavaScript ใน comment ผู้เข้าชมคนอื่นก็โดน

ตัวอย่างสถานการณ์จริง: เว็บ forum หลายแห่งถูก XSS ทำให้ session ผู้ใช้ถูกขโมย

ผลกระทบ: บัญชีถูกแฮ็ก, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนใครสักคนเขียนข้อความที่ทำให้คุณติดเชื้อทันทีที่อ่าน

76. การโจมตีด้วย Denial of Service (DoS)

DoS (โจมตีทำเว็บล่ม) เปรียบเหมือน ใครสักคนเอาท่อน้ำมาปิดหน้าบ้านคุณจนคุณเข้าออกไม่ได้

ตัวอย่างง่าย ๆ: ส่งคำขอเข้าถึงเว็บมากเกินไป ทำให้เว็บไม่ตอบ

ตัวอย่างสถานการณ์จริง: เว็บธนาคารหลายแห่งถูก DoS จนลูกค้าไม่สามารถ login

ผลกระทบ: เว็บล่ม, ขัดขวางบริการ

เปรียบเทียบง่าย ๆ: เหมือนปิดประตูบ้านคุณจนเข้าออกไม่ได้

77. การโจมตีด้วย Distributed Denial of Service (DDoS)

DDoS (โจมตีหลายเครื่องทำเว็บล่ม) เปรียบเหมือน ฝูงคนปิดประตูบ้านคุณหลายประตูพร้อมกัน

ตัวอย่างง่าย ๆ: Botnet หลายเครื่องโจมตีเว็บพร้อมกัน

ตัวอย่างสถานการณ์จริง: เว็บ e-commerce หลายแห่งถูก DDoS ทำให้ไม่สามารถขายสินค้าออนไลน์ได้

ผลกระทบ: เว็บล่ม, ขายของไม่ได้, เสียความเชื่อถือ

เปรียบเทียบง่าย ๆ: เหมือนฝูงคนบุกปิดประตูบ้านคุณจนคุณเข้าออกไม่ได้

78. การโจมตีด้วย Brute Force

Brute Force (ลองรหัสทุกแบบ) เปรียบเหมือน ใครสักคนลองกุญแจทุกแบบจนเจอ

ตัวอย่างง่าย ๆ: โปรแกรมลอง password ทุกแบบจนสำเร็จ

ตัวอย่างสถานการณ์จริง: บัญชี email หลายแห่งถูก brute force จนถูกแฮ็ก

ผลกระทบ: บัญชีถูกแฮ็ก, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนโจรลองกุญแจทุกแบบจนเข้าบ้านได้

79. การโจมตีด้วย Credential Stuffing

Credential Stuffing (ใช้รหัสจากเว็บอื่น) เปรียบเหมือน ใครสักคนลองกุญแจจากบ้านอื่นมาเปิดบ้านคุณ

ตัวอย่างง่าย ๆ: Hacker ใช้ username/password ที่รั่วจากเว็บอื่นมาลองกับเว็บคุณ

ตัวอย่างสถานการณ์จริง: ผู้ใช้หลายรายถูกบัญชีถูกแฮ็กเพราะ reuse password

ผลกระทบ: บัญชีถูกแฮ็ก, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนโจรเอากุญแจบ้านเพื่อนมาเปิดบ้านคุณ

80. การโจมตีด้วย Session Hijacking

Session Hijacking (แฮ็ก session) เปรียบเหมือน ใครสักคนแอบใช้บัตรเข้าห้องของคุณ

ตัวอย่างง่าย ๆ: Hacker ดัก session ID แล้ว login แทนผู้ใช้

ตัวอย่างสถานการณ์จริง: ผู้ใช้หลายคนถูก session hijacking ทำให้บัญชีถูกควบคุม

ผลกระทบ: ข้อมูลรั่ว, บัญชีถูกแฮ็ก

เปรียบเทียบง่าย ๆ: เหมือนใครสักคนแอบใช้กุญแจบ้านของคุณ

81. การโจมตีด้วย Privilege Escalation

Privilege Escalation (ยกระดับสิทธิ์) เปรียบเหมือน ลูกจ้างปกติแอบใช้บัตรผู้จัดการ

ตัวอย่างง่าย ๆ: ผู้โจมตี exploit bug เพื่อได้สิทธิ์ admin

ตัวอย่างสถานการณ์จริง: Server หลายแห่งถูก privilege escalation ทำให้ hacker ควบคุมระบบ

ผลกระทบ: ระบบถูกควบคุม, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนลูกจ้างใช้บัตรผู้จัดการเข้าห้องลับ

82. การโจมตีด้วย Malware

Malware (มัลแวร์) เปรียบเหมือน ยาพิษในอาหาร

ตัวอย่างง่าย ๆ: โปรแกรมติด malware ทำให้คอมพิวเตอร์ทำงานไม่ปกติหรือขโมยข้อมูล

ตัวอย่างสถานการณ์จริง: ผู้ใช้หลายรายติด malware ข้อมูลการเงินรั่ว

ผลกระทบ: ข้อมูลรั่ว, ระบบเสีย

เปรียบเทียบง่าย ๆ: เหมือนใส่ยาพิษในอาหารทำให้ป่วย

83. การโจมตีด้วย Backdoor

Backdoor (ประตูหลัง) เปรียบเหมือน ใส่ประตูลับให้โจรเข้ามาได้ตลอดเวลา

ตัวอย่างง่าย ๆ: Hacker ติดตั้ง backdoor ใน server

ตัวอย่างสถานการณ์จริง: หลาย server ถูก backdoor ทำให้ถูกควบคุมระยะไกล

ผลกระทบ: ข้อมูลรั่ว, ระบบถูกควบคุม

เปรียบเทียบง่าย ๆ: เหมือนโจรมีประตูลับเข้าบ้านคุณได้ตลอดเวลา

84. การโจมตีด้วย Rootkit

Rootkit (ซ่อนตัวควบคุม) เปรียบเหมือน ใส่ใครสักคนซ่อนตัวในบ้านเพื่อควบคุมทุกอย่าง

ตัวอย่างง่าย ๆ: Hacker ติด rootkit เพื่อซ่อน malware และควบคุมระบบ

ตัวอย่างสถานการณ์จริง: Server หลายแห่งถูก rootkit ซ่อน malware หลายปี

ผลกระทบ: ข้อมูลรั่ว, ระบบถูกควบคุม

เปรียบเทียบง่าย ๆ: เหมือนมีโจรซ่อนตัวในบ้านคุณ ทำทุกอย่างโดยคุณไม่รู้

85. การโจมตีด้วย Logic Bomb

Logic Bomb (ระเบิดเงื่อนไข) เปรียบเหมือน ระเบิดซ่อนในบ้าน รอเงื่อนไขเกิดแล้วระเบิด

ตัวอย่างง่าย ๆ: โปรแกรมทำลายไฟล์เมื่อถึงวัน/เหตุการณ์ที่กำหนด

ตัวอย่างสถานการณ์จริง: หลายบริษัทถูก logic bomb ทำให้ระบบเสีย

ผลกระทบ: ข้อมูลเสีย, ระบบล่ม

เปรียบเทียบง่าย ๆ: เหมือนวางระเบิดซ่อนในบ้าน รอวันเกิดเหตุแล้วระเบิด

86. การโจมตีด้วย Malicious Insider

Malicious Insider (คนในทำร้าย) เปรียบเหมือน พนักงานในบริษัทขโมยของ

ตัวอย่างง่าย ๆ: พนักงานแอบขโมยข้อมูลลูกค้า

ตัวอย่างสถานการณ์จริง: บริษัทหลายแห่งมีข้อมูลรั่วเพราะ malicious insider

ผลกระทบ: ข้อมูลรั่ว, ความเสียหายต่อองค์กร

เปรียบเทียบง่าย ๆ: เหมือนคนในบ้านแอบเอาของไปขาย

87. การโจมตีด้วย Drive-By Download

Drive-By Download (ดาวน์โหลดโดยไม่รู้ตัว) เปรียบเหมือน รับของจากถนนโดยไม่รู้ว่ามีพิษ

ตัวอย่างง่าย ๆ: เปิดเว็บบางเว็บ โปรแกรมอันตรายดาวน์โหลดเอง

ตัวอย่างสถานการณ์จริง: หลายคนติด malware จากเว็บ download ปลอม

ผลกระทบ: เครื่องติด malware, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนรับของจากถนนแล้วโดนพิษ

88. การโจมตีด้วย Rogue Software

Rogue Software (โปรแกรมหลอก) เปรียบเหมือน คนมาขายยารักษาโรคปลอม

ตัวอย่างง่าย ๆ: โปรแกรมแสดงว่าเครื่องติด virus แต่จริง ๆ หลอกให้จ่ายเงิน

ตัวอย่างสถานการณ์จริง: ผู้ใช้หลายรายจ่ายเงินโปรแกรมปลอม

ผลกระทบ: เสียเงิน, เครื่องไม่ได้รับการป้องกัน

เปรียบเทียบง่าย ๆ: เหมือนจ่ายเงินซื้อยาปลอม

89. การโจมตีด้วย Malvertising

Malvertising (โฆษณาอันตราย) เปรียบเหมือน โปสเตอร์มีพิษ

ตัวอย่างง่าย ๆ: คลิกโฆษณาแล้ว malware ติดเครื่อง

ตัวอย่างสถานการณ์จริง: หลายเว็บข่าวถูก malvertising ทำให้ผู้ใช้ติด malware

ผลกระทบ: เครื่องติด malware, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนอ่านโปสเตอร์แล้วพิษเข้าไปในตัว

90. การโจมตีด้วย Exploit Kits

Exploit Kits (ชุดเจาะระบบ) เปรียบเหมือน กล่องเครื่องมือโจร

ตัวอย่างง่าย ๆ: Hacker ใช้ exploit kit เจาะ browser และติด malware

ตัวอย่างสถานการณ์จริง: เว็บไซต์หลายแห่งถูก exploit kit แอบติด malware

ผลกระทบ: เครื่องติด malware, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนโจรมีกกล่องเครื่องมือครบมือ

91. การโจมตีด้วย Keylogger

Keylogger (บันทึกแป้นพิมพ์) เปรียบเหมือน ใส่ใครสักคนสอดส่องทุกสิ่งที่คุณพิมพ์

ตัวอย่างง่าย ๆ: ติด keylogger เก็บรหัสผ่าน, ข้อมูลบัตร

ตัวอย่างสถานการณ์จริง: ผู้ใช้หลายรายถูก keylogger ทำให้บัญชีธนาคารรั่ว

ผลกระทบ: ข้อมูลรั่ว, เงินถูกขโมย

เปรียบเทียบง่าย ๆ: เหมือนใครสักคนเฝ้าดูคุณพิมพ์รหัสทุกครั้ง

92. การโจมตีด้วย Session Replay

Session Replay (เล่นซ้ำ session) เปรียบเหมือน ใครสักคนแอบดูวิธีใช้กุญแจแล้วทำซ้ำ

ตัวอย่างง่าย ๆ: Hacker ดัก session แล้ว replay เพื่อเข้าบัญชี

ตัวอย่างสถานการณ์จริง: เว็บหลายแห่งโดน session replay ทำให้บัญชีรั่ว

ผลกระทบ: ข้อมูลรั่ว, บัญชีถูกแฮ็ก

เปรียบเทียบง่าย ๆ: เหมือนใครแอบดูคุณเปิดประตูแล้วทำซ้ำเอง

93. การโจมตีด้วย HTTP Response Splitting

HTTP Response Splitting (แบ่ง response HTTP) เปรียบเหมือน ใครสักคนแอบใส่จดหมายปลอมในซองจริง

ตัวอย่างง่าย ๆ: ผู้โจมตีใส่คำสั่งใน header ทำ redirect หรือ XSS

ตัวอย่างสถานการณ์จริง: หลายเว็บถูก HTTP Response Splitting ทำ phishing

ผลกระทบ: ผู้ใช้โดนหลอก, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนมีจดหมายปลอมในซองจริง

94. การโจมตีด้วย Cookie Poisoning

Cookie Poisoning (ปลอมคุกกี) เปรียบเหมือน ใครสักคนเปลี่ยนตัวผ่านประตู

ตัวอย่างง่าย ๆ: ผู้โจมตีแก้ cookie เพื่อเข้าบัญชีผู้ใช้

ตัวอย่างสถานการณ์จริง: เว็บหลายแห่งโดน cookie poisoning ทำให้บัญชีรั่ว

ผลกระทบ: บัญชีถูกแฮ็ก, ข้อมูลรั่ว

เปรียบเทียบง่าย ๆ: เหมือนเปลี่ยนตัวรถไฟให้ข้ามชั้น VIP

9.9.9 มีการสแกนและตรวจสอบช่องโหว่ (vulnerability assessment scans) ของระบบสำคัญอย่างสม่ำเสมอ

- สิ่งที่ต้องทำ: มีการสแกนและตรวจสอบช่องโหว่ (vulnerability assessment scans) ของระบบสำคัญอย่างสม่ำเสมอ และมีการทดสอบโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก
- หลักฐาน: นโยบายการสแกนและแก้ไขช่องโหว่ของระบบที่ประมวลผลข้อมูลส่วนบุคคล
สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล
รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของบุคคลภายนอก
รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของแผนกเทคโนโลยีสารสนเทศ
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (5), ข้อ 5
- โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

เอกสารนโยบาย

ชื่อเอกสาร: นโยบายการประเมินและแก้ไขช่องโหว่ของระบบที่ประมวลผลข้อมูลส่วนบุคคล

เวอร์ชัน: 1.0

วันที่มีผลบังคับใช้: [ระบุวันที่]

หน่วยงานผู้จัดทำนโยบาย: แผนกเทคโนโลยีสารสนเทศ

อนุมัติโดย: คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการประเมินและแก้ไขช่องโหว่ (Vulnerability Assessment & Remediation) ของระบบที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลให้มีความปลอดภัย ป้องกันการเข้าถึง การรั่วไหล การทำลาย หรือการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

2. ขอบเขตการใช้งาน

นโยบายฉบับนี้ครอบคลุมถึงระบบสารสนเทศทั้งหมดที่ใช้ในการจัดเก็บ ประมวลผล และถ่ายโอนข้อมูลส่วนบุคคลในองค์กร รวมถึงอุปกรณ์เครือข่าย ฐานข้อมูล และเซิร์ฟเวอร์

3. นิยาม

ช่องโหว่ (Vulnerability): จุดอ่อนในระบบที่อาจถูกโจมตีหรือใช้ประโยชน์โดยผู้ไม่ประสงค์ดี

การประเมินช่องโหว่ (Vulnerability Assessment): กระบวนการตรวจสอบและระบุช่องโหว่ในระบบ

การแก้ไข (Remediation): การดำเนินการเพื่อปิดหรือจัดการกับช่องโหว่ที่ตรวจพบ

4. นโยบาย

4.1 องค์กรจะดำเนินการประเมินช่องโหว่ของระบบที่ประมวลผลข้อมูลส่วนบุคคลอย่างน้อยปีละ 1 ครั้ง และ/หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในระบบ

4.2 การประเมินช่องโหว่จะดำเนินการโดยใช้เครื่องมือที่เชื่อถือได้ เช่น Nessus, Qualys หรือเทียบเท่า

4.3 ผลการประเมินต้องได้รับการวิเคราะห์โดยทีม IT Security และจัดระดับความเสี่ยง (High, Medium, Low)

4.4 ช่องโหว่ที่อยู่ในระดับ High Risk ต้องได้รับการแก้ไขภายใน 15 วันทำการ

4.5 ช่องโหว่ที่อยู่ในระดับ Medium Risk ต้องได้รับการแก้ไขภายใน 30 วันทำการ

4.6 ช่องโหว่ที่อยู่ในระดับ Low Risk ต้องได้รับการพิจารณาและวางแผนแก้ไขตามความเหมาะสม

4.7 ต้องมีการจัดทำรายงานการประเมินช่องโหว่และแนบหลักฐานการแก้ไขอย่างครบถ้วน

4.8 ผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกจะต้องตรวจสอบความสอดคล้องของกระบวนการปีละครั้ง

4.9 การละเลยหรือไม่ดำเนินการตามนโยบายนี้ถือเป็นการฝ่าฝืนข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล และอาจมีผลต่อการดำเนินคดีทางปกครองตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5. บทบาทและหน้าที่

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO): ตรวจสอบความสอดคล้องกับกฎหมาย

แผนก IT Security: รับผิดชอบในการดำเนินการประเมินและแก้ไขช่องโหว่

ผู้บริหารระบบ (System Owner): ให้ข้อมูลและความร่วมมือในการทดสอบ

ผู้ตรวจสอบ (Internal/External Auditor): ตรวจสอบการปฏิบัติตามนโยบายและรายงานต่อผู้บริหาร

6. การทบทวนและปรับปรุงนโยบาย

นโยบายฉบับนี้จะถูกทบทวนอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงในกฎหมาย เทคโนโลยี หรือโครงสร้างพื้นฐาน

สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

สัญญานี้จัดทำขึ้น ณ วันที่ [วัน เดือน ปี] ระหว่าง

บริษัท/องค์กรผู้ว่าจ้าง:

ชื่อองค์กร: [ชื่อองค์กร]

ที่อยู่: [ที่อยู่]

ตัวแทน: [ชื่อผู้มีอำนาจ]

ตำแหน่ง: [ตำแหน่ง]

ผู้ให้บริการทดสอบ:

ชื่อบริษัท: [ชื่อบริษัทผู้ให้บริการ]

ที่อยู่: [ที่อยู่]

ตัวแทน: [ชื่อผู้มีอำนาจ]

ตำแหน่ง: [ตำแหน่ง]

ข้อกำหนดสัญญา**วัตถุประสงค์**

ผู้ให้บริการตกลงที่จะดำเนินการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของผู้ว่าจ้าง เพื่อประเมินช่องโหว่และความมั่นคงปลอดภัยของระบบอย่างครบถ้วนและเป็นมาตรฐานสากล

ขอบเขตงาน

- ประเมินช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Testing)
- ตรวจสอบมาตรการป้องกันมัลแวร์และไวรัส
- รายงานผลการทดสอบพร้อมข้อเสนอแนะการแก้ไข
- การทดสอบครอบคลุมระบบที่เกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งหมด

ระยะเวลา

ผู้ให้บริการจะดำเนินการทดสอบและส่งมอบรายงานภายใน [ระบุจำนวนวัน] วันทำการ นับจากวันที่ลงนามสัญญาฉบับนี้

ค่าตอบแทน

ผู้ว่าจ้างตกลงชำระค่าบริการเป็นจำนวนเงิน [จำนวนเงิน] บาท (ไม่รวมภาษีมูลค่าเพิ่ม) โดยชำระ [ระบุเงื่อนไขการชำระเงิน เช่น ชำระ 50% ล่วงหน้า และ 50% หลังส่งรายงาน]

ความลับและข้อมูลส่วนบุคคล

ผู้ให้บริการตกลงที่จะรักษาความลับของข้อมูลทั้งหมดที่ได้รับจากผู้ว่าจ้าง และจะใช้ข้อมูลเพื่อวัตถุประสงค์ตามสัญญานี้เท่านั้น

ข้อจำกัดความรับผิด

ผู้ให้บริการจะไม่รับผิดชอบต่อความเสียหายใด ๆ ที่เกิดจากการใช้ข้อมูลหรือผลการทดสอบ นอกเหนือจากขอบเขตงานที่กำหนด

การสิ้นสุดสัญญา

สัญญานี้จะสิ้นสุดเมื่อผู้ให้บริการส่งมอบรายงานการทดสอบและได้รับค่าตอบแทนครบถ้วน

ลงชื่อ.....

(ผู้ว่าจ้าง)

ลงชื่อ.....

(ผู้ให้บริการ)

รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของบุคคลภายนอก

รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

ผู้ทดสอบ: บริษัท [ชื่อบริษัทผู้ทดสอบ]

ผู้ว่าจ้าง: [ชื่อบริษัท]

วันที่ทดสอบ: [วัน เดือน ปี]

1. บทนำ

รายงานฉบับนี้สรุปผลการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลขององค์กร [ชื่อบริษัท] โดยมีวัตถุประสงค์เพื่อประเมินความปลอดภัยและค้นหาช่องโหว่ในระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

2. ขอบเขตการทดสอบ

- ระบบที่เกี่ยวข้องกับการจัดเก็บและประมวลผลข้อมูลส่วนบุคคล
- เครือข่ายและอุปกรณ์ที่เชื่อมต่อกับระบบหลัก
- โปรแกรมป้องกันมัลแวร์และไวรัส
- การตั้งค่าความปลอดภัยของระบบปฏิบัติการและแอปพลิเคชัน

3. วิธีการทดสอบ

- ใช้เครื่องมือ Vulnerability Scanner เช่น Nessus
- Penetration Testing ตามแนวทาง OWASP Top 10
- การวิเคราะห์ผลและจัดระดับความเสี่ยงของช่องโหว่

4. ผลการทดสอบและการวิเคราะห์

หมายเลข	ช่องโหว่ที่ตรวจพบ	ความรุนแรง	รายละเอียด	ข้อเสนอแนะ
1	ช่องโหว่ XSS	สูง	อธิบายรายละเอียดช่องโหว่และผลกระทบ	แนะนำแก้ไขด้วยการใช้ Input Validation
2	ระบบอัปเดตล่าช้า	ปานกลาง	โปรแกรมป้องกันไวรัสไม่ได้อัปเดตฐานข้อมูล	กำหนดนโยบายการอัปเดตอัตโนมัติ
...	...	...	...	...

5. สรุป

ระบบประมวลผลข้อมูลส่วนบุคคลขององค์กรมีความมั่นคงปลอดภัยในระดับ [ระบุระดับ] โดยยังมีช่องโหว่บางประการที่ควรดำเนินการแก้ไขอย่างเร่งด่วนเพื่อป้องกันความเสี่ยงจากการโจมตี

6. แนบเอกสารเพิ่มเติม

- รายงานการสแกนระบบฉบับเต็ม

– แผนการแก้ไขและติดตามผล

ลงชื่อ.....

(ผู้ทดสอบ)

รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของแผนกเทคโนโลยีสารสนเทศ

รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

ผู้ทดสอบ: แผนกเทคโนโลยีสารสนเทศองค์กร [ชื่อองค์กร]

วันที่ทดสอบ: [วัน เดือน ปี]

1. บทนำ

รายงานฉบับนี้จัดทำโดยแผนกเทคโนโลยีสารสนเทศเพื่อสรุปผลการทดสอบและประเมินความปลอดภัยของระบบที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

2. ขอบเขตงาน

- ระบบที่จัดเก็บและประมวลผลข้อมูลส่วนบุคคล
- การตั้งค่าความปลอดภัยของระบบและแอปพลิเคชัน
- โปรแกรมป้องกันไวรัสและมัลแวร์
- กระบวนการอัปเดตและแพตช์ระบบ

3. วิธีการทดสอบ

- การสแกนช่องโหว่ด้วยเครื่องมือภายใน
- การทดสอบเจาะระบบเบื้องต้น (Internal Penetration Test)
- การตรวจสอบการตั้งค่าความปลอดภัยระบบ

4. ผลการทดสอบ

หมายเลข	ประเด็นตรวจสอบ	ผลการทดสอบ	ข้อเสนอแนะ
1	การอัปเดตโปรแกรมป้องกันไวรัส	อัปเดตสม่ำเสมอ	ควรรักษามาตรฐานนี้ต่อไป
2	ช่องโหว่ในระบบเครือข่าย	ไม่มีช่องโหว่ร้ายแรง	ควรทดสอบอย่างสม่ำเสมอ
3	การตั้งค่าการสแกนระบบอัตโนมัติ	ตั้งค่าเรียบร้อยแล้ว	แนะนำให้เพิ่มความถี่การสแกน

5. สรุป

โดยภาพรวมระบบมีความมั่นคงปลอดภัยดี แต่ต้องรักษาการประเมินอย่างสม่ำเสมอและแก้ไขจุดที่ตรวจพบตามแผนงาน

ลงชื่อ.....

(หัวหน้าแผนก IT)

9.9.9 มีการสแกนและตรวจสอบช่องโหว่ (vulnerability assessment scans) ของระบบสำคัญอย่างสม่ำเสมอ

- สิ่งที่ต้องทำ: มีการสแกนและตรวจสอบช่องโหว่ (vulnerability assessment scans) ของระบบสำคัญอย่างสม่ำเสมอ และมีการทดสอบโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก
- หลักฐาน: นโยบายการสแกนและแก้ไขช่องโหว่ของระบบที่ประมวลผลข้อมูลส่วนบุคคล
สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล
รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของบุคคลภายนอก
รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของแผนกเทคโนโลยีสารสนเทศ
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (5), ข้อ 5
- โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการสแกนและแก้ไขช่องโหว่ของระบบที่ประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการในการดำเนินการสแกนและตรวจสอบช่องโหว่ของระบบที่ใช้ในการประมวลผลข้อมูลส่วนบุคคลอย่างสม่ำเสมอ และกำหนดการแก้ไขช่องโหว่เพื่อเสริมสร้างความมั่นคงปลอดภัยของระบบ

ขอบเขต

นโยบายนี้ใช้บังคับกับระบบสารสนเทศที่เกี่ยวข้องกับการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลขององค์กร

รายละเอียดนโยบาย

- ต้องมีการดำเนินการสแกนช่องโหว่ (Vulnerability Assessment) อย่างน้อยเดือนละ 1 ครั้ง
- ต้องมีการประเมินและจัดลำดับความรุนแรงของช่องโหว่ที่พบ
- ต้องมีแผนการแก้ไขช่องโหว่ที่ชัดเจนและดำเนินการแก้ไขภายในระยะเวลาที่เหมาะสมตามความรุนแรง
- ต้องบันทึกผลการสแกนและการแก้ไขเป็นเอกสารและรายงานให้ผู้บริหารทราบ
- สามารถใช้บริการผู้ตรวจสอบภายในหรือภายนอกที่มีความเชี่ยวชาญในการทดสอบช่องโหว่และความปลอดภัยของระบบได้
- ต้องมีการประเมินและทบทวนนโยบายนี้อย่างน้อยปีละ 1 ครั้ง

บทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการละเมิดมาตรฐานความมั่นคงปลอดภัยของข้อมูลและอาจถูกดำเนินการทางวินัยตามข้อกำหนดขององค์กร

สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

(ใช้แบบเดียวกับฉบับที่จัดทำไปก่อนหน้านี้ โดยเน้นการทดสอบ Vulnerability Assessment และ Penetration Testing ตามข้อกำหนดในข้อนี้)

รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของบุคคลภายนอก

(ใช้แบบฟอร์มเดิม แต่เน้นเนื้อหาที่แสดงว่าเป็นรายงานการสแกนและตรวจสอบช่องโหว่อย่างสม่ำเสมอ เช่น มีการระบุวันที่สแกน ความถี่การสแกน และผลการตรวจพบช่องโหว่ พร้อมแผนแก้ไข)

รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคลของแผนกเทคโนโลยีสารสนเทศ
(รูปแบบเดียวกับรายงานของแผนกเทคโนโลยีสารสนเทศที่ได้จัดทำไว้ก่อนหน้านี้ แต่ระบุความถี่การสแกนอย่างสม่ำเสมอ และผลการตรวจสอบช่องโหว่ในช่วงเวลาที่ทดสอบ)

9.9.10 มีการกรองและบล็อกการเข้าถึงเว็บไซต์ที่เป็นอันตราย สิ่งที่ต้องทำ: มีการกรองและบล็อกการเข้าถึงเว็บไซต์ที่เป็นอันตราย และมีเอกสารสนับสนุน

- หลักฐาน: นโยบายการกรองและบล็อกการเข้าถึงเว็บไซต์ที่เป็นอันตราย แบบข้อร้องเรียนเกี่ยวกับเว็บไซต์ที่เป็นอันตราย หนังสือยืนยันการรับข้อร้องเรียนเกี่ยวกับเว็บไซต์ที่เป็นอันตราย
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (5) โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการกรองและบล็อกการเข้าถึงเว็บไซต์ที่เป็นอันตราย (ตัวอย่าง)

วัตถุประสงค์

เพื่อป้องกันและลดความเสี่ยงจากการเข้าถึงเว็บไซต์ที่เป็นอันตราย เช่น เว็บไซต์ที่มีมัลแวร์ ฟิชชิ่ง หรือเนื้อหาที่ละเมิดกฎหมายและนโยบายขององค์กร

ขอบเขต

นโยบายนี้ครอบคลุมการกรองและบล็อกเว็บไซต์ที่เป็นอันตรายสำหรับพนักงาน ผู้ใช้งานระบบเครือข่ายขององค์กร และอุปกรณ์ที่เชื่อมต่อกับเครือข่ายองค์กร

รายละเอียดนโยบาย

- มีการใช้งานระบบกรองเว็บไซต์ (Web Filtering System) ที่มีฐานข้อมูลเว็บไซต์อันตรายที่อัปเดตอย่างสม่ำเสมอ
- บล็อกการเข้าถึงเว็บไซต์ที่อยู่ในฐานข้อมูลดังกล่าวโดยอัตโนมัติ
- เปิดช่องทางให้พนักงานและผู้เกี่ยวข้องสามารถร้องเรียนหรือแจ้งเว็บไซต์ที่สงสัยว่าเป็นอันตรายได้ผ่านแบบฟอร์มร้องเรียน
- มีการตรวจสอบและวินิจฉัยข้อร้องเรียน พร้อมดำเนินการบล็อกเว็บไซต์ที่พบว่ามีความเสี่ยง
- จัดเก็บและบันทึกหลักฐานการดำเนินการ และรายงานผลให้ผู้บริหารทราบอย่างสม่ำเสมอ
- ทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง

ผู้รับผิดชอบ:

ฝ่ายเทคโนโลยีสารสนเทศ (IT Department) โทรศัพท์ 02-123-4567 ต่อ 101

อีเมล security@companyexample.com

วันที่เริ่มใช้: 1 มิถุนายน 2568

วันที่ทบทวนล่าสุด: 1 มิถุนายน 2569

แบบข้อร้องเรียนเกี่ยวกับเว็บไซต์ที่เป็นอันตราย (ตัวอย่าง)

ชื่อผู้แจ้ง : นายสมชาย ใจดี

ตำแหน่ง : เจ้าหน้าที่ฝ่ายการตลาด

เบอร์ติดต่อ / อีเมล : 081-234-5678 / somchai.jaidee@example.com

วันที่แจ้ง : 5 มิถุนายน 2568

URL เว็บไซต์ที่ต้องการร้องเรียน : <http://malicious-website-example.com>

เหตุผลที่ร้องเรียน : เว็บไซต์นี้มีการแจกจ่ายมัลแวร์ที่อาจเป็นอันตรายต่อเครื่องคอมพิวเตอร์ขององค์กร

รายละเอียดเพิ่มเติม : พบลิงก์ดาวน์โหลดโปรแกรมที่มีไวรัสและโฆษณาหลอกลวงในหน้าเว็บไซต์

ลงชื่อผู้แจ้ง: นายสมชาย ใจดี

วันที่: 5 มิถุนายน 2568

หนังสือยืนยันการรับข้อร้องเรียนเกี่ยวกับเว็บไซต์ที่เป็นอันตราย (ตัวอย่าง)

เรียน นายสมชาย ใจดี

ตามที่ท่านได้แจ้งข้อร้องเรียนเกี่ยวกับเว็บไซต์ที่สงสัยว่าเป็นอันตราย มีรายละเอียดดังนี้

URL เว็บไซต์: <http://malicious-website-example.com>

วันที่ได้รับแจ้ง: 5 มิถุนายน 2568

รายละเอียดข้อร้องเรียน: เว็บไซต์นี้มีการแจกจ่ายมัลแวร์ที่อาจเป็นอันตรายต่อเครื่องคอมพิวเตอร์ขององค์กร

องค์กรฯ ได้รับทราบและดำเนินการตรวจสอบข้อร้องเรียนดังกล่าวแล้ว และจะแจ้งผลการ

ดำเนินการให้ท่านทราบภายใน 7 วันทำการ

ขอขอบคุณที่ให้ความร่วมมือในการรักษาความปลอดภัยของระบบสารสนเทศ

ลงชื่อ

(นางสาวสุภารัตน์ สายชล)

หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

วันที่ 6 มิถุนายน 2568

9.9.11 มีการใช้ Firewall หรือระบบป้องกันการบุกรุก สิ่งที่ต้องทำ: มีการใช้ Firewall หรือระบบป้องกันการบุกรุก และมีการตรวจสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

- หลักฐาน: นโยบายการจัดหาโปรแกรมรักษาความมั่นคงปลอดภัยแก่ระบบประมวลผลข้อมูลส่วนบุคคล
สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล รายงานการทดสอบ
การป้องกันระบบประมวลผลข้อมูลส่วนบุคคล
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (5) โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการจัดหาโปรแกรมรักษาความมั่นคงปลอดภัยแก่ระบบประมวลผลข้อมูลส่วนบุคคล (ตัวอย่าง)

นโยบายการจัดหาโปรแกรมรักษาความมั่นคงปลอดภัยแก่ระบบประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดแนวทางและกระบวนการจัดหาโปรแกรมรักษาความมั่นคงปลอดภัย รวมถึงระบบ Firewall และระบบป้องกันการบุกรุก (Intrusion Prevention System - IPS) เพื่อปกป้องระบบประมวลผลข้อมูลส่วนบุคคลขององค์กรให้มีความปลอดภัยสูงสุด

ขอบเขต

นโยบายนี้ครอบคลุมการจัดหา การติดตั้ง และการบำรุงรักษาโปรแกรมรักษาความมั่นคงปลอดภัยสำหรับระบบที่ประมวลผลข้อมูลส่วนบุคคลทุกประเภทในองค์กร

นโยบาย

- องค์กรจะจัดหาโปรแกรมรักษาความมั่นคงปลอดภัยที่เหมาะสมและทันสมัย เช่น Firewall, ระบบ IPS และ Antivirus ที่มีประสิทธิภาพ
- โปรแกรมและระบบดังกล่าวต้องได้รับการอัปเดตฐานข้อมูลอย่างสม่ำเสมอ และผ่านการทดสอบความปลอดภัยจากผู้เชี่ยวชาญทั้งภายในและภายนอกองค์กร
- มีการกำหนดสิทธิ์ในการเข้าถึงและควบคุมการใช้งานโปรแกรมรักษาความมั่นคงปลอดภัยอย่างเข้มงวด
- รายงานผลการทดสอบและการอัปเดตระบบจะต้องถูกจัดเก็บและนำเสนอต่อผู้บริหารเป็นระยะ
- นโยบายนี้จะถูกทบทวนและปรับปรุงอย่างน้อยปีละ 1 ครั้ง

ผู้รับผิดชอบ

ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)

โทรศัพท์: 02-123-4567 ต่อ 102

อีเมล: security@companyexample.com

วันที่เริ่มใช้: 1 กรกฎาคม 2568

วันที่ทบทวนล่าสุด: 1 กรกฎาคม 2569

สัญญาจ้างบริการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

ทำที่

วันที่

คู่สัญญา

ผู้ว่าจ้าง:

ชื่อ: บริษัท ABC จำกัด

ที่อยู่: 123 ถนนสุขุมวิท แขวงคลองตัน เขตคลองเตย กรุงเทพฯ 10110

เลขประจำตัวผู้เสียภาษี: 0105551234567

โทรศัพท์: 02-123-4567

ผู้มีอำนาจลงนาม: นายสมชาย ใจดี

ตำแหน่ง: กรรมการผู้จัดการ

ผู้รับจ้าง:

ชื่อ: บริษัท SecureTest จำกัด

ที่อยู่: 456 ถนนรัชดาภิเษก แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900

เลขประจำตัวผู้เสียภาษี: 0105556543210

โทรศัพท์: 02-987-6543

ผู้มีอำนาจลงนาม: นางสาวสุนิสา มั่นคง

ตำแหน่ง: ผู้จัดการฝ่ายปฏิบัติการ

ขอบเขตของงาน

1.1 ผู้รับจ้างตกลงให้บริการทดสอบระบบป้องกันการประมวลผลข้อมูลส่วนบุคคลของผู้ว่าจ้าง โดยประกอบด้วย

- การประเมินช่องโหว่ (Vulnerability Assessment) ของระบบ Firewall และระบบป้องกันการบุกรุก (IPS)
- การทดสอบเจาะระบบ (Penetration Testing) เพื่อประเมินความปลอดภัยโดยรวมของระบบ
- การตรวจสอบการตั้งค่าระบบและการอัปเดตซอฟต์แวร์ที่เกี่ยวข้อง
- การจัดทำรายงานสรุปผลการทดสอบ พร้อมข้อเสนอแนะในการแก้ไขและปรับปรุง

1.2 ผู้รับจ้างจะดำเนินการทดสอบตามมาตรฐานอุตสาหกรรม เช่น OWASP, NIST หรือมาตรฐานที่เกี่ยวข้องที่ได้รับความนิยมในขณะนั้น

ระยะเวลาและกำหนดส่งมอบ

2.1 การทดสอบจะดำเนินการในช่วงวันที่ 1 มิถุนายน 2568 ถึงวันที่ 10 มิถุนายน 2568

2.2 รายงานผลการทดสอบจะต้องส่งมอบให้แก่ผู้ว่าจ้างภายในวันที่ 15 มิถุนายน 2568

2.3 กรณีที่ผู้รับจ้างไม่สามารถดำเนินการหรือส่งมอบรายงานภายในเวลาที่กำหนด จะต้องแจ้งผู้ว่าจ้างเป็นลายลักษณ์อักษรและขอขยายเวลาโดยระบุเหตุผลที่เหมาะสม

คำตอบแทนและการชำระเงิน

- 3.1 ผู้ว่าจ้างตกลงชำระค่าบริการจำนวน 200,000 บาท (สองแสนบาทถ้วน) ให้แก่ผู้รับจ้าง
- 3.2 การชำระเงินจะทำภายใน 7 วันทำการหลังจากผู้ว่าจ้างได้รับและตรวจสอบรายงานการทดสอบเรียบร้อยแล้ว

3.3 การชำระเงินจะโอนผ่านบัญชีธนาคารของผู้รับจ้าง ตามรายละเอียดดังนี้:

ชื่อบัญชี: บริษัท SecureTest จำกัด

ธนาคาร: ธนาคารกรุงเทพ สาขารัชดาภิเษก

เลขที่บัญชี: 123-4-56789-0

ความลับและข้อมูลส่วนบุคคล

- 4.1 ผู้รับจ้างต้องรักษาความลับของข้อมูลทั้งหมดที่ได้รับจากผู้ว่าจ้าง ทั้งข้อมูลที่เกี่ยวข้องกับระบบ ข้อมูลส่วนบุคคล และข้อมูลทางธุรกิจ
- 4.2 ห้ามผู้รับจ้างเปิดเผยหรือใช้ข้อมูลใด ๆ ที่ได้รับจากผู้ว่าจ้างเพื่อประโยชน์ส่วนตัวหรือบุคคลที่สามโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง
- 4.3 หลังจากสิ้นสุดสัญญา ผู้รับจ้างจะต้องคืนหรือทำลายข้อมูลทั้งหมดที่ได้รับจากผู้ว่าจ้างตามคำสั่งของผู้ว่าจ้าง

สิทธิและหน้าที่ของผู้รับจ้าง

- 5.1 ผู้รับจ้างต้องดำเนินการทดสอบด้วยความรอบคอบและเป็นไปตามมาตรฐานทางเทคนิคที่ยอมรับในวงการ
- 5.2 ผู้รับจ้างต้องแจ้งผู้ว่าจ้างหากพบช่องโหว่หรือความเสี่ยงที่อาจก่อให้เกิดความเสียหายร้ายแรงในระหว่างการทดสอบ
- 5.3 ผู้รับจ้างจะต้องจัดทำรายงานการทดสอบที่ถูกต้อง ชัดเจน ครบถ้วน พร้อมข้อเสนอแนะในการแก้ไขหรือปรับปรุง

สิทธิและหน้าที่ของผู้ว่าจ้าง

- 6.1 ผู้ว่าจ้างต้องจัดเตรียมข้อมูลและอำนวยความสะดวกในการเข้าถึงระบบที่เกี่ยวข้องแก่ผู้รับจ้าง
- 6.2 ผู้ว่าจ้างมีสิทธิ์ขอคำชี้แจงหรือขอข้อมูลเพิ่มเติมจากผู้รับจ้างในระหว่างการทำงาน
- 6.3 ผู้ว่าจ้างมีสิทธิ์ตรวจสอบผลการทดสอบและขอให้ผู้รับจ้างดำเนินการแก้ไขหรือตรวจสอบเพิ่มเติมหากเห็นว่าจำเป็น

การรับประกัน

7.3 ผู้รับจ้างรับประกันว่าการทดสอบจะดำเนินการด้วยความระมัดระวังสูงสุด เพื่อไม่ให้เกิดความเสียหายต่อระบบหรือข้อมูลของผู้ว่าจ้าง

7.4 หากเกิดความเสียหายโดยตรงต่อระบบหรือข้อมูลของผู้ว่าจ้างจากการดำเนินการทดสอบของผู้รับจ้าง ผู้รับจ้างจะรับผิดชอบในการชดเชยค่าเสียหายตามความเป็นจริงแต่ไม่เกินวงเงินค่าบริการตามสัญญาฉบับนี้

7.5 ผู้รับจ้างไม่มีความรับผิดชอบต่อความเสียหายที่เกิดขึ้นโดยมิได้มีสาเหตุมาจากการกระทำโดยประมาทหรือเจตนาของผู้รับจ้าง หรือจากสาเหตุภายนอกที่อยู่นอกเหนือการควบคุมของผู้รับจ้าง

การยกเลิกสัญญา

8.1 ฝ่ายใดฝ่ายหนึ่งสามารถยกเลิกสัญญานี้โดยแจ้งเป็นลายลักษณ์อักษรล่วงหน้าไม่น้อยกว่า 15 วัน

8.2 กรณียกเลิกสัญญาก่อนการส่งมอบรายงาน ผู้รับจ้างมีสิทธิได้รับค่าบริการในส่วนของการที่ได้ดำเนินการแล้วตามความเป็นจริง

การระงับข้อพิพาท

9.1 ทั้งสองฝ่ายตกลงที่จะเจรจาแก้ไขข้อพิพาทอย่างเป็นมิตร

9.2 กรณีไม่สามารถตกลงกันได้ ให้ข้อพิพาทนั้นอยู่ภายใต้ดุลยพินิจของศาลในเขตกรุงเทพมหานคร

ข้อกำหนดทั่วไป

10.1 สัญญานี้จัดทำขึ้นเป็น 2 ฉบับ มีข้อความเหมือนกันทั้งสองฉบับ ฝ่ายละ 1 ฉบับ

10.2 การแก้ไขหรือเพิ่มเติมสัญญาต้องทำเป็นลายลักษณ์อักษรและลงนามโดยทั้งสองฝ่ายเท่านั้น

10.3 กรณีมีข้อกำหนดใดในสัญญานี้ขัดแย้งกับกฎหมาย ให้ใช้กฎหมายเป็นหลัก

ความรับผิดชอบกรณีความเสียหาย

11.1 ผู้รับจ้างตกลงว่า จะรับผิดชอบต่อความเสียหายโดยตรงที่เกิดขึ้นกับระบบหรือข้อมูลของผู้ว่าจ้างที่พิสูจน์ได้ว่าเกิดจากความผิดพลาดหรือการละเมิดสัญญาของผู้รับจ้างเท่านั้น

11.2 ผู้รับจ้างจะไม่รับผิดชอบต่อความเสียหายทางอ้อม ความเสียหายเชิงลงโทษ หรือความเสียหายที่เกิดขึ้นจากความล่าช้าในการดำเนินการ รวมถึงความเสียหายที่เกิดจากการใช้งานหลังการส่งมอบรายงาน

11.3 ผู้ว่าจ้างต้องแจ้งความเสียหายและร้องขอให้ผู้รับจ้างรับผิดชอบเป็นลายลักษณ์อักษรภายใน 30 วัน นับจากวันที่พบความเสียหาย มิฉะนั้นถือว่าสละสิทธิในการเรียกร้องใด ๆ

11.4 การชดเชยค่าเสียหายให้เป็นไปตามกฎหมายที่เกี่ยวข้อง และไม่เกินวงเงินค่าบริการตามสัญญา

ลงชื่อ

ผู้ว่าจ้าง (นายสมชาย ใจดี)

ผู้รับจ้าง (นางสาวสุนิสา มั่นคง)

9.9.12 มีการจำกัดการใช้ระบบปฏิบัติการที่ผู้ผลิตไม่ให้การสนับสนุนแล้ว

สิ่งที่ต้องทำ: มีการจำกัดการใช้ระบบปฏิบัติการที่ผู้ผลิตไม่ให้การสนับสนุนแล้ว ครบถ้วน

หลักฐาน: นโยบายการจำกัดระบบปฏิบัติการที่ผู้ผลิตไม่ให้การสนับสนุน

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (5)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการจำกัดระบบปฏิบัติการที่ผู้ผลิตไม่ให้การสนับสนุน

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการจำกัดการใช้ระบบปฏิบัติการ (Operating System) ที่ผู้ผลิตได้เลิกให้การสนับสนุนหรืออัปเดตความปลอดภัยแล้ว เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของระบบประมวลผลข้อมูลส่วนบุคคล

2. ขอบเขต

นโยบายนี้ใช้บังคับกับทุกระบบคอมพิวเตอร์และอุปกรณ์ที่เชื่อมต่อกับระบบประมวลผลข้อมูลส่วนบุคคลภายในองค์กร รวมถึงผู้ใช้งานและฝ่ายเทคโนโลยีสารสนเทศ

3. คำนิยาม

ระบบปฏิบัติการที่ไม่สนับสนุน (Unsupported OS)

ระบบปฏิบัติการที่ผู้ผลิตประกาศยุติการให้บริการอัปเดตด้านความปลอดภัยและการซ่อมบำรุง เช่น Windows XP, Windows 7 รุ่นที่หมดระยะชีพพอร์ต เป็นต้น

4. นโยบายและข้อกำหนด

4.1 องค์กรจะไม่อนุญาตให้ใช้งานระบบปฏิบัติการที่หมดระยะการสนับสนุนจากผู้ผลิตในการเข้าถึงระบบประมวลผลข้อมูลส่วนบุคคล

4.2 ฝ่ายเทคโนโลยีสารสนเทศจะต้องตรวจสอบและจัดทำรายชื่อระบบปฏิบัติการที่ยังใช้งานในองค์กรอย่างสม่ำเสมออย่างน้อยปีละ 2 ครั้ง

4.3 ในกรณีที่พบการใช้งานระบบปฏิบัติการที่ไม่สนับสนุน ฝ่ายเทคโนโลยีสารสนเทศต้องแจ้งผู้ใช้งานและแผนกที่เกี่ยวข้องเพื่อดำเนินการอัปเดต เปลี่ยนระบบ หรือเลิกใช้งานทันที

4.4 การอนุญาตใช้ระบบปฏิบัติการที่หมดการสนับสนุนจะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูง พร้อมระบุเหตุผลและมาตรการชั่วคราวในการลดความเสี่ยงด้านความปลอดภัย

4.5 ฝ่ายเทคโนโลยีสารสนเทศจะต้องจัดทำรายงานสรุปผลการจำกัดและอัปเดตระบบปฏิบัติการ และรายงานต่อผู้บริหารทุกไตรมาส

5. บทลงโทษ

การละเลยไม่ปฏิบัติตามนโยบายนี้ ถือเป็นการฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัยตามที่กฎหมายกำหนด และอาจนำไปสู่การรับผิดชอบทางปกครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

6. การทบทวนและปรับปรุงนโยบาย

นโยบายนี้จะได้รับการทบทวนและปรับปรุงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับเทคโนโลยีและกฎหมาย

ตัวอย่างข้อมูลในนโยบาย (กรณีศึกษา)

ระบบปฏิบัติการ	วันที่สิ้นสุดการสนับสนุน	สถานะการใช้งาน	มาตรการที่ดำเนินการ
Windows 7	14 ม.ค. 2563	ยังมีใช้งาน 5 เครื่อง	แจ้งเปลี่ยนเป็น Windows 10 ภายใน 3 เดือน
Windows XP	8 เม.ย. 2558	ไม่มีใช้งานแล้ว	เลิกใช้งานและถอดออกจากระบบทั้งหมด
Ubuntu 16.04	30 เม.ย. 2563	ใช้งานในเซิร์ฟเวอร์ 1 เครื่อง	วางแผนอัปเดตเป็น Ubuntu 20.04 ภายใน 6 เดือน

9.9.13 มีการกำหนดมาตรการเพื่อป้องกันข้อมูลที่ส่งผ่านเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตหรือเครือข่ายไร้สาย

สิ่งที่ต้องทำ: มีการกำหนดมาตรการเพื่อป้องกันข้อมูลที่ส่งผ่านเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต หรือเครือข่ายไร้สาย และมีเอกสารสนับสนุน

หลักฐาน: นโยบายการป้องกันไฟล์แนบที่มีข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (5)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง
ไม่เกิน 3 ล้านบาท

นโยบายการป้องกันข้อมูลส่วนบุคคลที่ส่งผ่านเครือข่ายสาธารณะ

1. วัตถุประสงค์

เพื่อกำหนดมาตรการและแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ส่งผ่าน
เครือข่ายสาธารณะ เช่น อินเทอร์เน็ต หรือเครือข่ายไร้สาย เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
และลดความเสี่ยงจากการถูกโจมตีหรือดักฟังข้อมูล

2. ขอบเขต

นโยบายนี้ใช้บังคับกับบุคลากรทุกคนที่เกี่ยวข้องกับการส่งข้อมูลส่วนบุคคลผ่านเครือข่ายสาธารณะ
รวมทั้งระบบเทคโนโลยีสารสนเทศที่ใช้ในการประมวลผลและถ่ายโอนข้อมูลส่วนบุคคล

3. คำนิยาม

เครือข่ายสาธารณะ (Public Network): เครือข่ายที่เปิดให้บุคคลทั่วไปเข้าถึงได้ เช่น อินเทอร์เน็ต,
เครือข่าย Wi-Fi สาธารณะ

ข้อมูลส่วนบุคคล: ข้อมูลใด ๆ ที่สามารถระบุหรือเชื่อมโยงกับตัวบุคคลได้ตามพระราชบัญญัติคุ้มครอง
ข้อมูลส่วนบุคคล พ.ศ. 2562

4. มาตรการรักษาความมั่นคงปลอดภัย

4.1 การส่งข้อมูลส่วนบุคคลผ่านเครือข่ายสาธารณะจะต้องใช้การเข้ารหัสข้อมูล (Encryption) ทั้งในระดับ
เครือข่ายและระดับแอปพลิเคชัน เช่น การใช้ VPN, HTTPS, TLS, หรือโปรโตคอลเข้ารหัสอื่นที่ได้รับการ
ยอมรับในอุตสาหกรรม

4.2 ห้ามส่งข้อมูลส่วนบุคคลที่มีความสำคัญหรือข้อมูลส่วนบุคคลชนิดพิเศษผ่านเครือข่ายสาธารณะโดยไม่มี
มาตรการเข้ารหัสหรือการป้องกันที่เหมาะสม

4.3 การรับส่งไฟล์แนบที่มีข้อมูลส่วนบุคคลต้องใช้วิธีการป้องกัน เช่น การเข้ารหัสไฟล์ด้วยรหัสผ่าน หรือใช้
ช่องทางส่งไฟล์ที่ปลอดภัย และต้องมีการแจ้งผู้รับถึงวิธีการถอดรหัสไฟล์

4.4 ฝ่ายเทคโนโลยีสารสนเทศต้องมีการกำหนดและดูแลระบบรักษาความปลอดภัยเครือข่าย เช่น ระบบ
Firewall, ระบบป้องกันการโจมตีทางเครือข่าย (IDS/IPS), ระบบ VPN สำหรับพนักงาน

4.5 บุคลากรต้องได้รับการอบรมและรับทราบถึงความเสี่ยงในการส่งข้อมูลส่วนบุคคลผ่านเครือข่าย
สาธารณะและแนวทางปฏิบัติที่ถูกต้อง

4.6 มีการตรวจสอบและบันทึกการรับส่งข้อมูลส่วนบุคคลผ่านเครือข่ายสาธารณะอย่างสม่ำเสมอ เพื่อใช้ในการติดตามและวิเคราะห์กรณีเกิดเหตุการณ์ไม่ปลอดภัย

5. การจัดทำเอกสารและรายงาน

5.1 นโยบายฉบับนี้จะต้องได้รับการประกาศและเผยแพร่ให้บุคลากรทุกคนทราบ

5.2 ต้องจัดทำคู่มือหรือแนวทางปฏิบัติเกี่ยวกับการส่งข้อมูลส่วนบุคคลผ่านเครือข่ายสาธารณะอย่างปลอดภัย

5.3 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำรายงานผลการตรวจสอบและวิเคราะห์ความมั่นคงปลอดภัยของเครือข่ายอย่างน้อยปีละ 1 ครั้ง

6. บทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ อาจนำไปสู่การถูกดำเนินการทางวินัยภายในองค์กร รวมถึงการรับผิดชอบตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 และโทษทางปกครองที่กำหนดไว้

7. การทบทวนและปรับปรุงนโยบาย

นโยบายนี้จะได้รับการทบทวนและปรับปรุงอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับเทคโนโลยีหรือกฎหมาย

ตัวอย่างแบบฟอร์ม รายงานการตรวจสอบการป้องกันข้อมูลที่ส่งผ่านเครือข่ายสาธารณะ

หมายเลข รายงาน	วันที่ ตรวจสอบ	ผู้ ตรวจสอบ	ระบบที่ ตรวจสอบ	มาตรการที่ ใช้	ผลการ ตรวจสอบ	ข้อเสนอแนะ
001/2567	1 มิ.ย. 2567	นายสมชาย ใจดี	ระบบส่ง อีเมลองค์กร	ใช้ TLS/SSL ในการส่ง ข้อมูล	ปลอดภัย ไม่มีช่อง โหว่	ควรปรับปรุง ระบบ VPN ให้ ครอบคลุม พนักงานทั้งหมด
002/2567	15 มิ.ย. 2567	นางสาว สาวิตรี แก้วใส	ระบบแชร์ ไฟล์ผ่าน Cloud	ใช้ระบบ เข้ารหัสไฟล์ และ รหัสผ่าน	ปลอดภัย ระดับดี	แนะนำอบรมผู้ใช้ เรื่องการจัดการ รหัสผ่าน

9.9.14 มีการจำกัดหรือควบคุมการใช้โซเชียลมีเดีย ซึ่งรวมถึงโปรแกรมประเภท Line หรือ WhatsApp เพื่อป้องกันการแชร์ข้อมูลส่วนบุคคลผ่านทางช่องทางดังกล่าว

สิ่งที่ต้องทำ: มีการจำกัดหรือควบคุมการใช้โซเชียลมีเดีย ซึ่งรวมถึงโปรแกรมประเภท Line หรือ WhatsApp เพื่อป้องกันการแชร์ข้อมูลส่วนบุคคลผ่านทางช่องทางดังกล่าว และมีเอกสารสนับสนุน

หลักฐาน: นโยบายการคุ้มครองไฟล์ที่มีข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

รายงานการทดสอบการป้องกันระบบประมวลผลข้อมูลส่วนบุคคล

วันที่ทดสอบ: 1-10 มิถุนายน 2568

ผู้ทดสอบ: บริษัท SecureTest จำกัด

1. วัตถุประสงค์

เพื่อประเมินความมั่นคงปลอดภัยของระบบ Firewall และระบบป้องกันการบุกรุก (IPS) ของบริษัท ABC จำกัด ที่ใช้ประมวลผลข้อมูลส่วนบุคคล

2. ขอบเขตการทดสอบ

- การตั้งค่าและการทำงานของ Firewall
- การตรวจจับและป้องกันการโจมตีผ่านระบบ IPS
- การอัปเดตฐานข้อมูลภัยคุกคาม (Threat Database)
- การจัดการรายงานและแจ้งเตือนเหตุการณ์ทางความปลอดภัย

3. วิธีการทดสอบ

- ใช้เครื่องมือสแกนช่องโหว่ (Vulnerability Scanner) เช่น Nessus, OpenVAS
- ทดสอบการป้องกันการบุกรุกด้วยการจำลองการโจมตี (Penetration Testing)
- ตรวจสอบการตั้งค่าระบบและการอัปเดตซอฟต์แวร์
- วิเคราะห์และประเมินผลรายงานการแจ้งเตือนในระบบ

4. ผลการทดสอบ

รายการ	ผลการทดสอบ	หมายเหตุ/ข้อเสนอแนะ
การตั้งค่า Firewall	ผ่าน	Firewall บล็อกพอร์ตที่ไม่จำเป็นทั้งหมด มีการอนุญาตเฉพาะพอร์ตที่กำหนดไว้เท่านั้น
ระบบ IPS	ผ่าน	ตรวจจับและบล็อกการโจมตีแบบ DoS และ SQL Injection ได้อย่างมีประสิทธิภาพ
การอัปเดตฐานข้อมูลภัยคุกคาม	ผ่าน	ฐานข้อมูลถูกอัปเดตสัปดาห์ละ 1 ครั้ง ตามนโยบายของบริษัท

การจัดการรายงานแจ้ง เดือน	ผ่าน	ระบบสามารถแจ้งเตือนทันทีเมื่อพบเหตุการณ์ผิดปกติและ จัดเก็บบันทึกครบกัณ

5. ข้อเสนอแนะ

- ควรเพิ่มการตรวจสอบระบบ Firewall อย่างน้อยทุก 3 เดือน
- แนะนำให้จัดอบรมบุคลากรด้าน IT เกี่ยวกับการบริหารจัดการระบบป้องกันอย่างต่อเนื่อง
- ควรพิจารณาการใช้ระบบ SIEM เพื่อเพิ่มประสิทธิภาพการตรวจจับภัยคุกคาม

6. สรุป

ระบบ Firewall และ IPS ของบริษัท ABC จำกัด มีความมั่นคงปลอดภัยในระดับที่ดี และพร้อม
รับมือภัยคุกคามในปัจจุบันได้อย่างเหมาะสม

ลงชื่อ
.....
(นางสาวสุนิสา มั่นคง)
ผู้ตรวจสอบระบบ

9.10 อุปกรณ์พกพาไร้สาย (mobile devices) การปฏิบัติงานระยะไกลจากที่บ้านหรือนอกสถานที่ สื่อ
บันทึกข้อมูลที่ถอดแยกได้ (Mobile devices, home or remote working and removable media)
โดยองค์กรมีมาตรการที่เหมาะสมในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยอันเนื่องมาจากการใช้
อุปกรณ์พกพาไร้สาย การปฏิบัติงานระยะไกลจากที่บ้านหรือนอกสถานที่ และสื่อบันทึกข้อมูลที่ถอดแยกได้

9.10.1 มีนโยบายควบคุมการใช้อุปกรณ์พกพาไร้สาย เช่น โทรศัพท์มือถือ โน้ตบุ๊กคอมพิวเตอร์
(notebook computer) และมีนโยบายควบคุมการปฏิบัติงานจากระยะไกล

สิ่งที่ต้องทำ: มีนโยบายควบคุมการใช้อุปกรณ์พกพาไร้สาย เช่น โทรศัพท์มือถือ โน้ตบุ๊กคอมพิวเตอร์ และ
มีนโยบายควบคุมการปฏิบัติงานจากระยะไกล และมีเอกสารสนับสนุน

หลักฐาน: นโยบายควบคุมการใช้อุปกรณ์พกพาไร้สาย บัญชีทรัพย์สินสารสนเทศ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (5)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง
ไม่เกิน 3 ล้านบาท

ตัวอย่างนโยบายควบคุมการใช้อุปกรณ์พกพาไร้สาย (Mobile Devices Policy)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการใช้อุปกรณ์พกพาไร้สาย เช่น โทรศัพท์มือถือ โน้ตบุ๊กคอมพิวเตอร์ และอุปกรณ์อื่นที่คล้ายกันในการทำงาน เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กร

2. ขอบเขต

นโยบายนี้บังคับใช้กับบุคลากรทุกคนที่ได้รับมอบหมายให้นำอุปกรณ์พกพาไร้สายมาใช้ในการงานขององค์กร

3. แนวทางปฏิบัติ

- 3.1 อุปกรณ์พกพาทุกชิ้นต้องมีการตั้งรหัสผ่าน หรือมาตรการป้องกันการเข้าถึงที่เหมาะสม เช่น การล็อกหน้าจออัตโนมัติหลังไม่มีการใช้งานภายในเวลาที่กำหนด
- 3.2 ต้องติดตั้งโปรแกรมป้องกันไวรัสและซอฟต์แวร์ด้านความปลอดภัยที่องค์กรกำหนด
- 3.3 ห้ามติดตั้งหรือใช้งานแอปพลิเคชันที่ไม่ได้รับอนุญาตจากฝ่ายไอที
- 3.4 อุปกรณ์ที่สูญหายหรือถูกขโมยต้องแจ้งให้ฝ่ายไอทีทราบทันทีเพื่อดำเนินการล็อกหรือลบข้อมูลระยะไกล
- 3.5 ข้อมูลที่สำคัญหรือข้อมูลส่วนบุคคลที่จัดเก็บในอุปกรณ์พกพาต้องเข้ารหัสหรือใช้มาตรการความปลอดภัยตามนโยบายขององค์กร

4. การตรวจสอบและการบำรุงรักษา

- 4.1 ฝ่ายไอทีจะทำการตรวจสอบความปลอดภัยของอุปกรณ์พกพาเป็นระยะตามที่กำหนด
- 4.2 บุคลากรต้องรายงานปัญหาหรือข้อสงสัยเกี่ยวกับความปลอดภัยของอุปกรณ์พกพาโดยทันที

ตัวอย่างนโยบายควบคุมการปฏิบัติงานระยะไกล (Remote Working Policy)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการควบคุมการปฏิบัติงานนอกสถานที่ เช่น ที่บ้าน หรือสถานที่อื่นที่ไม่ใช่สำนักงาน เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กร

2. ขอบเขต

นโยบายนี้ใช้กับบุคลากรทุกคนที่ได้รับอนุญาตให้ปฏิบัติงานระยะไกล

3. แนวทางปฏิบัติ

- 3.1 บุคลากรต้องใช้เครื่องมือและช่องทางสื่อสารที่ได้รับอนุญาตและจัดเตรียมโดยองค์กรเท่านั้น
- 3.2 การเชื่อมต่อกับระบบองค์กรต้องใช้เครือข่ายที่ปลอดภัย เช่น VPN หรือช่องทางที่เข้ารหัส

3.3 ห้ามแชร์บัญชีผู้ใช้งานหรือรหัสผ่านให้ผู้อื่น

3.4 ต้องเก็บรักษาอุปกรณ์และข้อมูลส่วนบุคคลอย่างรัดกุม หลีกเลี่ยงการเปิดเผยข้อมูลในที่สาธารณะ

3.5 ต้องมีการสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอและไม่เก็บข้อมูลส่วนบุคคลไว้ในเครื่องส่วนตัวโดยไม่จำเป็น

4. การตรวจสอบและรายงาน

4.1 ฝ่ายไอทีมีสิทธิ์ตรวจสอบการปฏิบัติงานระยะไกลเพื่อความมั่นคงปลอดภัยตามนโยบายองค์กร

4.2 บุคลากรต้องรายงานเหตุการณ์ผิดปกติหรือปัญหาด้านความมั่นคงปลอดภัยที่เกิดขึ้นทันที

ตัวอย่างหลักฐาน: บัญชีทรัพย์สินสารสนเทศ (Information Asset Inventory)

ลำดับ	ชื่ออุปกรณ์	หมายเลขประจำ เครื่อง / Serial Number	ผู้ใช้งาน	วันที่รับมอบ	สถานะ (ใช้งาน/ ซ่อม/ ปลด ระวาง)	หมายเหตุ
1	โน้ตบุ๊ก HP ProBook 450 G8	SN1234567890	นาย สมชาย	01/03/2025	ใช้งาน	อัปเดต ซอฟต์แวร์ ล่าสุด
2	โทรศัพท์มือถือ iPhone 14 Pro	SN0987654321	นางสาว สุดา	15/02/2025	ใช้งาน	ตั้งค่า รหัสผ่าน 6 หลัก
3	ฮาร์ดดิสก์พกพา Western Digital 1TB	WD1234567890	ฝ่าย บัญชี	20/01/2025	ใช้งาน	เข้ารหัส ข้อมูลแล้ว

9.10.2 มีกลไกการป้องกันข้อมูลบนอุปกรณ์พกพาไร้สาย เช่น ใช้การเข้ารหัสข้อมูลบนอุปกรณ์

- สิ่งที่ต้องทำ: มีกลไกการป้องกันข้อมูลบนอุปกรณ์พกพาไร้สาย เช่น ใช้การเข้ารหัสข้อมูลบนอุปกรณ์ และมีการปรับปรุงให้มีประสิทธิภาพสม่ำเสมอ
- หลักฐาน: นโยบายการป้องกันข้อมูลบนอุปกรณ์พกพาไร้สาย
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)
- โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการป้องกันข้อมูลบนอุปกรณ์พกพาไร้สาย (Mobile Device Data Protection Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการและแนวทางปฏิบัติในการป้องกันข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กรที่จัดเก็บหรือประมวลผลบนอุปกรณ์พกพาไร้สาย เช่น โทรศัพท์มือถือ โน้ตบุ๊กคอมพิวเตอร์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและความเสียหายของข้อมูล

2. ขอบเขต

นโยบายนี้ครอบคลุมถึงอุปกรณ์พกพาไร้สายทุกประเภทที่ใช้ในการปฏิบัติงานขององค์กร ไม่ว่าจะเป็นอุปกรณ์ที่จัดหาโดยองค์กรหรืออุปกรณ์ส่วนบุคคลที่ใช้เพื่อทำงาน

3. แนวทางปฏิบัติ

3.1 การเข้ารหัสข้อมูล

ทุกอุปกรณ์พกพาไร้สายที่เก็บข้อมูลส่วนบุคคลหรือข้อมูลสำคัญต้องมีการเข้ารหัสข้อมูลภายในอุปกรณ์ (Full Disk Encryption หรือเทคโนโลยีที่เทียบเท่า)

การตั้งค่าการเข้ารหัสจะต้องตรวจสอบและยืนยันโดยฝ่ายไอที

3.2 การตั้งค่าความปลอดภัยของรหัสผ่าน

- ผู้ใช้งานต้องตั้งรหัสผ่านที่มีความซับซ้อน ได้แก่ ตัวอักษรใหญ่-เล็ก ตัวเลข และสัญลักษณ์พิเศษ
- รหัสผ่านต้องเปลี่ยนทุก 90 วัน
- ห้ามบันทึกหรือพิมพ์รหัสผ่านในที่เปิดเผยหรือไม่ปลอดภัย

3.3 การเชื่อมต่อข้อมูลผ่านเครือข่าย

- การส่งข้อมูลผ่านเครือข่ายต้องใช้ช่องทางที่เข้ารหัส เช่น VPN หรือโปรโตคอล TLS
- ห้ามใช้เครือข่ายสาธารณะที่ไม่มีการเข้ารหัสสำหรับการส่งข้อมูลส่วนบุคคลหรือข้อมูลสำคัญ

3.4 การป้องกันการสูญหายของข้อมูล

- ต้องมีการสำรองข้อมูลอย่างสม่ำเสมอ
- ต้องมีระบบลบข้อมูลระยะไกล (Remote Wipe) หากอุปกรณ์สูญหายหรือถูกขโมย
- ต้องแจ้งฝ่ายไอทีทันทีที่เกิดเหตุการณ์สูญหายหรือความเสี่ยงด้านความปลอดภัย

3.5 การปรับปรุงและตรวจสอบระบบ

- ฝ่ายไอทีมีหน้าที่ตรวจสอบและปรับปรุงระบบรักษาความปลอดภัยอย่างสม่ำเสมอ
- รายงานผลการตรวจสอบความปลอดภัยจะต้องจัดทำและส่งต่อผู้บริหารอย่างน้อยทุกไตรมาส

4. ความรับผิดชอบ

- ผู้ใช้งานอุปกรณ์พกพาไร้สายต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- แจ้งฝ่ายไอทีทันทีหากพบความผิดปกติหรือความเสี่ยงที่อาจส่งผลกระทบต่อความมั่นคงของข้อมูล
- ฝ่ายไอทีรับผิดชอบในการจัดหาเครื่องมือและมาตรการที่จำเป็นสำหรับการป้องกันและรักษาความปลอดภัยของข้อมูล

5. การบังคับใช้และบทลงโทษ

- ผู้ที่ไม่ปฏิบัติตามนโยบายนี้อาจถูกลงโทษทางวินัยตามข้อกำหนดขององค์กร รวมถึงการถูกเรียกค่าเสียหายหากเกิดความเสียหายแก่ข้อมูลส่วนบุคคลหรือข้อมูลสำคัญ
- นโยบายนี้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)

9.10.3 มีการใช้โปรแกรมประเภท VPN เพื่อเข้าถึงระบบหรือเครือข่ายภายในจากระยะไกล

สิ่งที่ต้องทำ: มีการใช้โปรแกรมประเภท VPN เพื่อเข้าถึงระบบหรือเครือข่ายภายในจากระยะไกล และมีเอกสารสนับสนุน

หลักฐาน: นโยบายการป้องกันข้อมูลบนอุปกรณ์พกพาไร้สายโดยการใช้โปรแกรมประเภท VPN

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการใช้โปรแกรมประเภท VPN สำหรับการเข้าถึงระบบเครือข่ายภายในจากระยะไกล

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการการใช้โปรแกรมประเภท VPN (Virtual Private Network) สำหรับการเข้าถึงระบบหรือเครือข่ายภายในองค์กรจากระยะไกล เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กร

2. ขอบเขต

นโยบายนี้ใช้บังคับกับพนักงาน ผู้รับเหมา และบุคคลที่เกี่ยวข้องซึ่งได้รับอนุญาตให้ใช้ VPN เพื่อเข้าถึงระบบเครือข่ายภายในองค์กรจากภายนอกสถานที่ทำงาน

3. แนวทางปฏิบัติ

3.1 การใช้ VPN

- การเข้าถึงระบบหรือเครือข่ายภายในจากระยะไกลจะต้องทำผ่านโปรแกรม VPN ที่องค์กรกำหนดและอนุญาตเท่านั้น
- โปรแกรม VPN ต้องมีมาตรฐานความปลอดภัยสูง รองรับการเข้ารหัสข้อมูลแบบ AES-256 หรือเทียบเท่า
- การเชื่อมต่อ VPN จะต้องผ่านการยืนยันตัวตนแบบหลายปัจจัย (MFA) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

3.2 การตั้งค่าความปลอดภัย

- อุปกรณ์ที่จะใช้เชื่อมต่อ VPN ต้องติดตั้งโปรแกรมป้องกันไวรัสและได้รับการอัปเดตระบบปฏิบัติการอย่างสม่ำเสมอ
- ห้ามใช้ VPN บนอุปกรณ์ที่ไม่มีการรักษาความปลอดภัยหรือถูกเจลเบรก (jailbreak) หรือรูท (root)
- ห้ามเปิดใช้งาน VPN บนอุปกรณ์ที่ใช้เครือข่ายสาธารณะที่ไม่ปลอดภัยโดยไม่มีการป้องกันเพิ่มเติม เช่น Firewall หรือ Antivirus

3.3 การควบคุมการเข้าถึง

- การอนุญาตใช้งาน VPN จะต้องได้รับการอนุมัติจากผู้บริหารหรือเจ้าหน้าที่ที่รับผิดชอบ
- ต้องจำกัดสิทธิ์การเข้าถึงตามบทบาทหน้าที่ของผู้ใช้งาน (Role-Based Access Control)
- บันทึกการใช้งาน VPN ต้องถูกเก็บและตรวจสอบเป็นประจำเพื่อป้องกันการเข้าถึงที่ผิดปกติ

3.4 การเฝ้าระวังและปรับปรุงระบบ

- ฝ่ายไอทีจะทำการตรวจสอบความปลอดภัยของระบบ VPN อย่างสม่ำเสมอและปรับปรุงระบบเพื่อรองรับภัยคุกคามใหม่ ๆ
- รายงานการตรวจสอบระบบ VPN จะถูกจัดทำและส่งต่อผู้บริหารเพื่อรับทราบอย่างน้อยทุก 6 เดือน

4. ความรับผิดชอบ

- ผู้ใช้งาน VPN ต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- ต้องแจ้งฝ่ายไอทีทันทีเมื่อพบความผิดปกติหรือเหตุการณ์ที่อาจก่อให้เกิดความเสียหายแก่ข้อมูล
- ฝ่ายไอทีรับผิดชอบในการจัดเตรียมและดูแลระบบ VPN ให้มีความปลอดภัยตามมาตรฐาน

5. การบังคับใช้และบทลงโทษ

- การไม่ปฏิบัติตามนโยบายนี้อาจส่งผลให้ถูกลงโทษทางวินัย หรือถูกระงับสิทธิ์การใช้งานระบบเครือข่าย
- นโยบายนี้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)

9.10.4 โปรแกรมประเภท VPN ที่ใช้งานมีการอัปเดตเวอร์ชันให้เป็นปัจจุบัน

สิ่งที่ต้องทำ: โปรแกรมประเภท VPN ที่ใช้งานมีการอัปเดตเวอร์ชันให้เป็นปัจจุบัน และมีการทดสอบโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก

หลักฐาน: นโยบายการป้องกันข้อมูลบนอุปกรณ์พกพาไร้สาย โดยการใช้โปรแกรมประเภท VPN รายงานการทดสอบความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ประมวลผลโดยอุปกรณ์พกพาไร้สาย

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการใช้และการอัปเดตโปรแกรม VPN บนอุปกรณ์พกพาไร้สาย

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการใช้งานโปรแกรม VPN บนอุปกรณ์พกพาไร้สายและมาตรการในการอัปเดตเวอร์ชันให้ทันสมัย เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและระบบเครือข่ายภายในองค์กร

2. ขอบเขต

นโยบายนี้ใช้บังคับกับพนักงาน เจ้าหน้าที่ และบุคคลที่เกี่ยวข้องที่ได้รับอนุญาตให้ใช้โปรแกรม VPN เพื่อเชื่อมต่อระบบภายในจากระยะไกลผ่านอุปกรณ์พกพาไร้สาย

3. แนวทางปฏิบัติ

3.1 การใช้โปรแกรม VPN

- โปรแกรม VPN ที่ได้รับอนุญาตให้นำมาใช้ ต้องเป็นโปรแกรมที่องค์กรกำหนดและมีมาตรฐานความปลอดภัยสูง
- ผู้ใช้ต้องทำการเชื่อมต่อ VPN ตามขั้นตอนและมาตรฐานที่องค์กรกำหนดเท่านั้น

3.2 การอัปเดตเวอร์ชันของโปรแกรม VPN

- โปรแกรม VPN ต้องมีการอัปเดตเวอร์ชันอย่างสม่ำเสมอให้ทันสมัยอยู่เสมอ โดยฝ่ายไอทีรับผิดชอบในการตรวจสอบและจัดการอัปเดต
- ทุกการอัปเดตต้องผ่านการทดสอบเพื่อประเมินผลกระทบด้านความมั่นคงปลอดภัยและประสิทธิภาพก่อนนำมาใช้งานจริง
- การทดสอบต้องดำเนินการโดยผู้ตรวจสอบภายในองค์กรหรือผู้ตรวจสอบภายนอกที่มีความเชี่ยวชาญ

3.3 การตรวจสอบและรายงาน

- ฝ่ายไอทีจะจัดทำรายงานการทดสอบความมั่นคงปลอดภัยของโปรแกรม VPN ทุกครั้งหลังอัปเดตเวอร์ชันเสร็จสิ้น
- รายงานดังกล่าวจะถูกจัดเก็บและนำเสนอผู้บริหารเพื่อทบทวนและรับทราบเป็นประจำ

4. ความรับผิดชอบ

- ฝ่ายไอทีรับผิดชอบในการติดตามและดำเนินการอัปเดตโปรแกรม VPN ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ
- ผู้ใช้ต้องปฏิบัติตามนโยบายนี้และใช้โปรแกรม VPN ที่ได้รับการอนุมัติเท่านั้น
- ต้องรายงานความผิดปกติหรือปัญหาที่พบจากการใช้งานโปรแกรม VPN ทันทีต่อฝ่ายไอที

5. การบังคับใช้และบทลงโทษ

- การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการละเมิดข้อกำหนดขององค์กร อาจมีผลกระทบต่อสิทธิการเข้าถึงระบบเครือข่าย และอาจถูกดำเนินการทางวินัย
- นโยบายนี้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)

ตัวอย่างหลักฐานประกอบ

- นโยบายการป้องกันข้อมูลบนอุปกรณ์พกพาไร้สาย โดยการใช้โปรแกรม VPN
- รายงานการทดสอบความมั่นคงปลอดภัยของโปรแกรม VPN หลังอัปเดตเวอร์ชัน
- บันทึกการติดตั้งและอัปเดตโปรแกรม VPN

ตัวอย่างหลักฐานแนบที่ 1

นโยบายการป้องกันข้อมูลบนอุปกรณ์พกพาไร้สาย โดยใช้โปรแกรม VPN

ชื่อเอกสาร: นโยบายการใช้โปรแกรม VPN บนอุปกรณ์พกพาไร้สาย

ฉบับที่: 1.0

วันที่ประกาศ: 1 มิถุนายน 2568

ผู้จัดทำ: ฝ่ายเทคโนโลยีสารสนเทศ

ผู้อนุมัติ: ผู้อำนวยการฝ่ายไอที

วัตถุประสงค์

เพื่อควบคุมและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและระบบเครือข่ายโดยการกำหนดแนวทางการใช้โปรแกรม VPN บนอุปกรณ์พกพาไร้สาย

ขอบเขต

นโยบายนี้ใช้กับพนักงาน เจ้าหน้าที่ และผู้ที่ได้รับอนุญาตใช้อุปกรณ์พกพาและโปรแกรม VPN ในการเชื่อมต่อระบบภายในจากระยะไกล

แนวทางปฏิบัติ

- โปรแกรม VPN ที่ใช้งานต้องเป็นโปรแกรมที่ได้รับการรับรองจากฝ่ายไอที
- ผู้ใช้ต้องปฏิบัติตามขั้นตอนการเชื่อมต่อ VPN อย่างเคร่งครัด
- โปรแกรม VPN ต้องอัปเดตเวอร์ชันล่าสุดเสมอ
- ฝ่ายไอทีจะจัดทำรายงานการอัปเดตและทดสอบความมั่นคงปลอดภัย

ความรับผิดชอบ

- ฝ่ายไอทีรับผิดชอบการติดตั้งและอัปเดตโปรแกรม VPN
- ผู้ใช้ต้องแจ้งปัญหาที่เกิดขึ้นทันที
- ฝ่ายบริหารมีอำนาจในการตรวจสอบการปฏิบัติตามนโยบาย

บทลงโทษ

การละเมิดนโยบายถือเป็นการผิดวินัยและอาจถูกดำเนินการตามระเบียบขององค์กรและกฎหมายที่เกี่ยวข้อง

ตัวอย่างหลักฐานแนบที่ 2

รายงานการทดสอบความมั่นคงปลอดภัยของโปรแกรม VPN หลังอัปเดตเวอร์ชัน

รายงานที่: 2025-06-01-VPN-Security-Test

วันที่ทดสอบ: 30 พฤษภาคม 2568

ผู้ตรวจสอบ: นางสาวสาวิตรี จันทร์ดี (ผู้ตรวจสอบภายใน)

โปรแกรม VPN: SecureConnect VPN

เวอร์ชัน: 3.2.1 (ก่อนอัปเดต 3.1.8)

สรุปผลการทดสอบ

- การทดสอบช่องโหว่ความปลอดภัยไม่พบช่องโหว่ร้ายแรง
- ระบบการเข้ารหัสข้อมูลผ่าน VPN ใช้มาตรฐาน AES-256 bit
- การตรวจสอบความถูกต้องผู้ใช้ (Authentication) ใช้ระบบสองขั้นตอน (2FA)
- ไม่มีพบพฤติกรรมแอบแฝงหรือการรั่วไหลของข้อมูล

รายละเอียดการทดสอบ

รายการทดสอบ	ผลการทดสอบ	หมายเหตุ
ตรวจสอบช่องโหว่ทั่วไป	ผ่าน	ไม่มีช่องโหว่ร้ายแรง
ทดสอบการเข้ารหัสข้อมูล	ผ่าน	ใช้ AES-256 bit
ทดสอบระบบยืนยันตัวตน 2 ขั้นตอน	ผ่าน	2FA ใช้งานได้ตามมาตรฐาน
ตรวจสอบบันทึกการใช้งาน	ผ่าน	ไม่มีความผิดปกติ
ทดสอบความเสถียรของระบบ VPN	ผ่าน	ไม่มีการขัดข้องหรือค้าง

ข้อเสนอแนะ

แนะนำให้ทบทวนนโยบายอัปเดตทุก 3 เดือน

เพิ่มการอบรมผู้ใช้เกี่ยวกับการใช้ VPN อย่างปลอดภัย

ตัวอย่างหลักฐานแนบที่ 3

บันทึกการติดตั้งและอัปเดตโปรแกรม VPN

วันที่ติดตั้ง/อัปเดต	เวอร์ชันโปรแกรม	ผู้ดำเนินการ	หมายเหตุ
15 มกราคม 2568	3.0.0	นายอนุชา เทคโนโลยี	ติดตั้งโปรแกรมครั้งแรก
10 เมษายน 2568	3.1.8	นางสาวสาวิตรี จันทร์ดี	อัปเดตเวอร์ชัน เพิ่มความปลอดภัย
29 พฤษภาคม 2568	3.2.1	นางสาวสาวิตรี จันทร์ดี	อัปเดตเวอร์ชันล่าสุด พร้อมทดสอบ

9.10.5 เมื่อมีความจำเป็นต้องจัดเก็บข้อมูลส่วนบุคคลไว้บนสื่อบันทึกข้อมูลที่ถอดแยกได้ จำกัดการจัดเก็บข้อมูลเท่าที่จำเป็น และมีกลไกการป้องกันข้อมูลที่จัดเก็บไว้นั้น

สิ่งที่ต้องทำ: เมื่อมีความจำเป็นต้องจัดเก็บข้อมูลส่วนบุคคลไว้บนสื่อบันทึกข้อมูลที่ถอดแยกได้ จำกัดการจัดเก็บข้อมูลเท่าที่จำเป็น และมีกลไกการป้องกันข้อมูลที่จัดเก็บไว้

หลักฐาน: นโยบายควบคุมการเก็บรวบรวมข้อมูลบนสื่อบันทึกข้อมูลที่ถอดแยกได้ บัญชีทรัพย์สินสารสนเทศ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

1. นโยบายควบคุมการเก็บรวบรวมข้อมูลบนสื่อบันทึกข้อมูลที่ถอดแยกได้

ชื่อเอกสาร: นโยบายควบคุมการจัดเก็บข้อมูลส่วนบุคคลบนสื่อบันทึกข้อมูลที่ถอดแยกได้

เวอร์ชัน: 1.0

วันที่มีผลบังคับใช้: 1 มิถุนายน 2568

หน่วยงานเจ้าของนโยบาย: ฝ่ายเทคโนโลยีสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

1) วัตถุประสงค์

เพื่อควบคุมการจัดเก็บและการเคลื่อนย้ายข้อมูลส่วนบุคคลบนสื่อบันทึกข้อมูลที่ถอดแยกได้ (Removable Media) เช่น USB Flash Drive, External Hard Disk, SD Card และอุปกรณ์คล้ายกัน เพื่อป้องกันการรั่วไหล การสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

2) ขอบเขต

นโยบายนี้ครอบคลุมผู้ปฏิบัติงานทุกคนในองค์กร รวมถึงพนักงาน ผู้รับจ้าง และผู้ที่ได้รับอนุญาตให้ใช้อุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร

3) นโยบาย

- (1) ห้ามจัดเก็บข้อมูลส่วนบุคคลบนสื่อบันทึกข้อมูลที่ถอดแยกได้ เว้นแต่ในกรณีจำเป็น เช่น ใช้เพื่อสำรองข้อมูลหรือกรณีเร่งด่วน
- (2) ต้องได้รับอนุญาตจากผู้มีอำนาจก่อนจัดเก็บข้อมูลบนสื่อดังกล่าว
- (3) ข้อมูลที่จัดเก็บต้องมีปริมาณเท่าที่จำเป็นเท่านั้น (ตามหลัก Data Minimization)
- (4) ต้องมีการเข้ารหัส (Encryption) ด้วยซอฟต์แวร์หรืออุปกรณ์ที่องค์กรกำหนด เช่น BitLocker หรือ VeraCrypt

(5) ห้ามนำสื่อบันทึกข้อมูลที่ไม่ได้รับอนุญาตมาเชื่อมต่อกับระบบเครือข่ายขององค์กร

(6) ต้องมีการตรวจสอบรายการใช้งานและการเข้าถึงอย่างน้อยทุกไตรมาส

4)การละเมิดนโยบาย

ผู้ฝ่าฝืนนโยบายนี้อาจได้รับโทษตามระเบียบขององค์กร และอาจถูกดำเนินคดีตามกฎหมาย PDPA

2. บัญชีทรัพย์สินสารสนเทศ

ลำดับ	ประเภทอุปกรณ์	รหัสทรัพย์สิน	ผู้รับผิดชอบ	รายละเอียดข้อมูลที่จัดเก็บ	วันที่ล่าสุดที่อัปเดต	กลไกการป้องกัน
1	USB Flash Drive	USB-001-2568	นายกิตติพงษ์	ข้อมูลผู้สมัครงานเฉพาะชื่อ-เบอร์ติดต่อ	28 พ.ค. 2568	BitLocker Encryption
2	External Hard Drive	EHD-007-2568	น.ส.วาสนา	รายงานภาษีของพนักงาน (เฉพาะปีล่าสุด)	15 พ.ค. 2568	รหัสผ่าน + Encryption
3	SD Card	SD-005-2568	นายธีระยุทธ	รูปภาพสำหรับการฝึกอบรมภายใน	1 มิ.ย. 2568	ไม่มีข้อมูลส่วนบุคคล

สภาพบังคับตามกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37: ผู้ควบคุมข้อมูลมีหน้าที่กำหนดมาตรการที่เหมาะสมเพื่อรักษาความมั่นคงปลอดภัย
- ประกาศ ปี 2565 ข้อ 4 (2): กำหนดให้ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการเพื่อจำกัดการเข้าถึงและการนำข้อมูลไปใช้

โทษกรณีไม่ปฏิบัติตาม

หากไม่ดำเนินการมาตรการดังกล่าว อาจต้องรับโทษ ทางปกครองตามมาตรา 37 ซึ่งกำหนดให้ปรับทางปกครอง ไม่เกิน 3 ล้านบาท

9.10.6 เมื่อต้องนำซอฟต์แวร์ ข้อมูล หรืออุปกรณ์ออกไปนอกสถานที่ มีการขออนุญาตก่อนการนำออกไป
 สิ่งที่ต้องทำ: เมื่อต้องนำซอฟต์แวร์ ข้อมูล หรืออุปกรณ์ออกไปนอกสถานที่ มีการขออนุญาตก่อนการนำออกไป และมีหลักฐานสนับสนุน

- หลักฐาน: นโยบายควบคุมการนำซอฟต์แวร์ ข้อมูล หรืออุปกรณ์ออกไปนอกสถานที่ แบบฟอร์มขอ
อนุญาตนำซอฟต์แวร์ ข้อมูล หรืออุปกรณ์ออกไปนอกสถานที่
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วน
บุคคล พ.ศ. 2565 ข้อ 4 (2) (5) (6) โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่
ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ชื่อเอกสาร: นโยบายควบคุมการนำซอฟต์แวร์ ข้อมูล หรืออุปกรณ์ออกไปนอกสถานที่

รหัสเอกสาร: PDPA-POL-09.10.6

เวอร์ชัน: 1.0

วันที่มีผลบังคับใช้: 1 มิถุนายน 2568

หน่วยงานรับผิดชอบ: ฝ่ายเทคโนโลยีสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและควบคุมการนำข้อมูลส่วนบุคคล ซอฟต์แวร์ หรืออุปกรณ์ขององค์กรออกไป
ใช้นอกสถานที่ ให้เป็นไปตามมาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ตามพระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ขอบเขต

นโยบายนี้ใช้บังคับกับพนักงาน ลูกจ้าง ผู้ปฏิบัติงานภายใต้สัญญาจ้าง ผู้ให้บริการภายนอก หรือ
บุคคลใด ๆ ที่มีความจำเป็นต้องนำข้อมูลหรืออุปกรณ์ขององค์กรออกไปใช้นอกสถานที่ทำงาน

3. แนวนโยบาย

3.1 ผู้ที่มีความจำเป็นต้องนำข้อมูลส่วนบุคคล ซอฟต์แวร์ หรืออุปกรณ์ขององค์กรออกไปนอกสถานที่ ต้อง
ดำเนินการขออนุญาตล่วงหน้าจากหัวหน้าหน่วยงานหรือผู้มีอำนาจตามแบบฟอร์มที่องค์กรกำหนด

3.2 ต้องระบุเหตุผลความจำเป็น รายการอุปกรณ์หรือข้อมูลที่จะนำออก ระยะเวลาและสถานที่ที่จะนำไปใช้
อย่างชัดเจน

3.3 ต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล เช่น การเข้ารหัสไฟล์ การตั้งรหัสผ่าน การจำกัด
สิทธิ์การเข้าถึง

3.4 เมื่อสิ้นสุดการใช้งานต้องส่งคืนอุปกรณ์ และ/หรือข้อมูลภายในเวลาที่กำหนด โดยต้องผ่านการ
ตรวจสอบสภาพโดยเจ้าหน้าที่

3.5 ต้องมีการจัดเก็บข้อมูลการขออนุญาต และการคืนอุปกรณ์ไว้ในระบบหรือแฟ้มเอกสารเพื่อสามารถ

ตรวจสอบย้อนหลังได้

3.6 ฝ่ายเทคโนโลยีสารสนเทศสามารถสุ่มตรวจสอบการใช้งานเพื่อให้เป็นไปตามมาตรการที่กำหนด

4. การฝ่าฝืนนโยบาย

บุคลากรที่ไม่ปฏิบัติตามนโยบายนี้จะต้องรับผิดชอบตามระเบียบวินัยขององค์กร และอาจถูกดำเนินการตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

เอกสารที่ 2

ชื่อเอกสาร: แบบฟอร์มขออนุญาตนำซอฟต์แวร์ ข้อมูล หรืออุปกรณ์ออกไปนอกสถานที่

รหัสเอกสาร: PDPA-FRM-09.10.6

วันที่ใช้งาน: 1 มิถุนายน 2568

ส่วนที่ 1: รายละเอียดผู้ขออนุญาต

ชื่อ-นามสกุล: นายอนิรุทธิ์ เกษมสุข

ตำแหน่ง: เจ้าหน้าที่สารสนเทศ

แผนก/หน่วยงาน: ฝ่ายเทคโนโลยีสารสนเทศ

เบอร์ติดต่อ: 081-123-4567

วันที่ขออนุญาต: 5 มิถุนายน 2568

ส่วนที่ 2: รายการทรัพย์สิน/ข้อมูลที่จะนำออก

ประเภท: ข้อมูล

รายการ: ไฟล์ฐานข้อมูลผู้ใช้งานระบบแจ้งเตือนสุขภาพ

รหัสหรือ Serial: DB-HEALTH-0525

จุดประสงค์การใช้งาน: เพื่อนำไปวิเคราะห์ข้อมูลร่วมกับโรงพยาบาลคู่สัญญา

ระยะเวลา: 5-7 มิถุนายน 2568

สถานที่ใช้: โรงพยาบาลสมานเวช สาขาลาดพร้าว

ส่วนที่ 3: มาตรการป้องกัน

มาตรการที่ใช้: เข้ารหัสไฟล์ด้วย AES-256, ตั้งรหัสผ่าน 12 ตัวอักษร, จำกัดสิทธิ์การเปิดไฟล์เฉพาะผู้รับมอบหมาย

ส่วนที่ 4: การอนุมัติ

ผู้อนุมัติ: นางสาวจิราภา ทองสง่า

ตำแหน่ง: หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

ลงชื่อ:

วันที่อนุมัติ: 5 มิถุนายน 2568

ส่วนที่ 5: การส่งคืน (บันทึกเมื่อเสร็จสิ้นภารกิจ)

วันที่ส่งคืน: 7 มิถุนายน 2568

ผู้รับคืน: นายปณชัย ทวีเกียรติ

สภาพอุปกรณ์/ข้อมูล: ครบถ้วน

หมายเหตุ: ไม่มีความเสียหาย

9.11 พื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย (Secure areas) องค์กรมีมาตรการในการป้องกันการเข้าถึง การทำลาย หรือการเข้ามายุ่งเหยิงกับข้อมูลส่วนบุคคลในพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย

9.11.1 มีการป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย โดยมีมาตรการควบคุมการเข้าออก เช่น มีประตูป้องกันบุคคลภายนอกเข้าไปในพื้นที่ มีสัญญาณกันขโมย และมีกล้องโทรทัศน์วงจรปิด เป็นต้น

สิ่งที่ต้องทำ: มีการป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย โดยมีมาตรการควบคุมการเข้าออกเคร่งครัด

หลักฐาน: นโยบายการป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย สัญญาจ้างบริการป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ชื่อเอกสาร: นโยบายการป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย

รหัสเอกสาร: PDPA-POL-09.11.1

เวอร์ชัน: 1.0

วันที่มีผลบังคับใช้: 1 มิถุนายน 2568

หน่วยงานรับผิดชอบ: ฝ่ายอาคารสถานที่และความมั่นคงปลอดภัย

1. วัตถุประสงค์

เพื่อกำหนดมาตรการในการรักษาความปลอดภัยของพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การทำลาย การโจรกรรม หรือการยุ่งเกี่ยวกับข้อมูลส่วนบุคคล หรืออุปกรณ์สำคัญภายในพื้นที่ดังกล่าว

2. ขอบเขต

นโยบายนี้ครอบคลุมพื้นที่ที่มีการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล อุปกรณ์เซิร์ฟเวอร์ ห้องศูนย์ข้อมูล ห้องประชุมสำคัญ หรือพื้นที่ควบคุมการเข้าถึงระบบสารสนเทศ

3. มาตรการควบคุม

- 3.1 พื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัยต้องมีประตูล็อกอัตโนมัติ หรือระบบเข้าออกที่ต้องใช้บัตรประจำตัว พินโค้ด หรือระบบไบโอเมตริกซ์
- 3.2 ห้ามบุคคลภายนอกหรือผู้ไม่มีหน้าที่เข้าไปในพื้นที่โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของพื้นที่
- 3.3 ต้องติดตั้งระบบกล้องวงจรปิด (CCTV) ครอบคลุมทุกทางเข้า-ออก และเก็บข้อมูลภาพไม่น้อยกว่า 30 วัน
- 3.4 ในกรณีพื้นที่มีความเสี่ยงสูง ต้องติดตั้งสัญญาณกันขโมยหรือระบบตรวจจับการบุกรุก
- 3.5 พนักงานที่ได้รับอนุญาตเข้าพื้นที่ต้องผ่านการอบรมเรื่องการรักษาความมั่นคงปลอดภัยเป็นประจำ
- 3.6 มีการบันทึกการเข้าออกของบุคคลในพื้นที่ทุกครั้งในระบบอิเล็กทรอนิกส์หรือสมุดลงชื่อ พร้อมเวลาเข้าและออก

4. การทบทวน

ฝ่ายอาคารสถานที่จะต้องทบทวนและประเมินผลมาตรการควบคุมพื้นที่ทุก 6 เดือน และจัดทำรายงานเสนอผู้บริหาร

เอกสารที่ 2

ชื่อเอกสาร: สัญญาจ้างบริการรักษาความปลอดภัยสำหรับพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย

รหัสเอกสาร: PDPA-CON-09.11.1

คู่สัญญา: บริษัท พีซีโอ เซอร์วิส จำกัด

หน่วยงานผู้ว่าจ้าง: สำนักงานบริหารกลาง

ระยะเวลาสัญญา: 1 มกราคม 2568 ถึง 31 ธันวาคม 2568

ขอบเขตงาน

- บริษัท พีซีโอ เซอร์วิส จำกัด มีหน้าที่ให้บริการรักษาความปลอดภัยโดย
- จัดเวรยามรักษาความปลอดภัยตลอด 24 ชั่วโมงในพื้นที่ห้องเซิร์ฟเวอร์ และศูนย์ข้อมูล
- ตรวจสอบตราความเรียบร้อยของพื้นที่ตามรอบเวลา และลงบันทึกในสมุดเวร
- รายงานเหตุการณ์ผิดปกติให้ฝ่ายอาคารสถานที่ทราบภายใน 30 นาที
- ควบคุมการเข้าออกของบุคคลตามรายชื่อที่ได้รับอนุญาตเท่านั้น
- ตรวจสอบกล้องวงจรปิดและส่งรายงานประจำเดือน

เงื่อนไขการรักษาความลับ

เจ้าหน้าที่รักษาความปลอดภัยต้องลงนามในข้อตกลงไม่เปิดเผยข้อมูล และผ่านการอบรมเรื่องการจัดการเหตุการณ์ข้อมูลรั่วไหลตามนโยบายองค์กร

9.11.2 สำหรับบุคคลภายนอกมีข้อปฏิบัติสำหรับการแลกบัตรและลงนามก่อนเข้าถึงพื้นที่ภายในองค์กร

สิ่งที่ต้องทำ: มีข้อปฏิบัติสำหรับการแลกบัตรและลงนามก่อนเข้าถึงพื้นที่ภายในองค์กร และมีการปฏิบัติตามอย่างเคร่งครัด

หลักฐาน: นโยบายการป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัยภายในองค์กร

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ชื่อเอกสาร: นโยบายการควบคุมการเข้าถึงของบุคคลภายนอกในพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัยภายในองค์กร

รหัสเอกสาร: PDPA-POL-09.11.2

เวอร์ชัน: 1.0

วันที่มีผลบังคับใช้: 1 มิถุนายน 2568

หน่วยงานรับผิดชอบ: ฝ่ายอาคารสถานที่และความมั่นคงปลอดภัย

1. วัตถุประสงค์

เพื่อควบคุมการเข้าถึงของบุคคลภายนอกในพื้นที่ภายในองค์กรที่มีความจำเป็นต้องรักษาความมั่นคงปลอดภัย เพื่อป้องกันความเสี่ยงต่อการเข้าถึงหรือการเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

2. ขอบเขต

นโยบายนี้ใช้บังคับกับบุคคลภายนอกทุกประเภทที่ต้องการเข้าพื้นที่ภายในองค์กร ไม่ว่าจะเป็นผู้มาติดต่อทางธุรกิจ ผู้รับเหมา ผู้ให้บริการภายนอก หรือบุคคลทั่วไป

3. แนวปฏิบัติ

3.1 บุคคลภายนอกทุกคนต้องแลกบัตรประชาชนหรือบัตรประจำตัวที่ทางราชการออกให้กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผ่านเข้าอาคารก่อนเข้าพื้นที่ภายในองค์กร

3.2 ต้องลงชื่อในสมุดเยี่ยม หรือลงทะเบียนอิเล็กทรอนิกส์ ระบุเวลาเข้า-ออก จุดประสงค์ในการเข้าพบ และชื่อผู้รับผิดชอบ

3.3 เจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบเอกสารยืนยันตัวตน และแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบมารับบุคคลภายนอก ณ จุดแลกบัตร

3.4 บุคคลภายนอกต้องสวมใส่บัตรผ่านเข้าอาคารให้เห็นชัดเจนตลอดเวลาที่อยู่ในพื้นที่องค์กร

3.5 ห้ามบุคคลภายนอกเดินเข้าไปในพื้นที่สำคัญ หรือพื้นที่หวงห้ามโดยไม่มีผู้ดูแลพาเข้า

3.6 หลังเสร็จสิ้นการติดต่อ บุคคลภายนอกต้องคืนบัตรผ่านเข้าอาคาร และลงเวลาออกให้เรียบร้อย

4. การควบคุมและการตรวจสอบ

ฝ่ายอาคารสถานที่จะทำการสุ่มตรวจและประเมินการปฏิบัติตามนโยบายนี้เป็นประจำทุกเดือน พร้อมรายงานสรุปเสนอต่อผู้บริหาร

ในกรณีพบว่าการฝ่าฝืน จะมีการดำเนินการตามมาตรการทางวินัย หรือรายงานต่อหน่วยงานตามกฎหมายข้อมูลส่วนบุคคลเพื่อพิจารณาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5. การอ้างอิงข้อกฎหมาย

อาศัยอำนาจตามมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และเป็นไปตามข้อ 4 (2) และ (4) ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

9.11.3 มีมาตรการป้องกันภัยคุกคามที่เกี่ยวข้องกับสภาพแวดล้อม เช่น ไฟไหม้ แผ่นดินไหว ภายในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย เช่น ภายในพื้นที่ของศูนย์คอมพิวเตอร์ เป็นต้น

สิ่งที่ต้องทำ: มีมาตรการป้องกันภัยคุกคามที่เกี่ยวข้องกับสภาพแวดล้อม เช่น ไฟไหม้ แผ่นดินไหว ภายในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย เช่น ภายในพื้นที่ของศูนย์คอมพิวเตอร์ เป็นต้น และมีแผนป้องกันที่ชัดเจน รวมถึงมีรายงานการป้องกันภัยคุกคามประจำปี

หลักฐาน: นโยบายป้องกันภัยคุกคามในพื้นที่ขององค์กรและพื้นที่ที่จำเป็นต้องรักษาความมั่นคง

ปลอดภัย แผนป้องกันภัยคุกคามในพื้นที่ขององค์กรและพื้นที่ที่จำเป็นต้องรักษาความมั่นคง
ปลอดภัย รายงานการป้องกันภัยคุกคามประจำปี

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง
ไม่เกิน 3 ล้านบาท

ชื่อเอกสาร: นโยบายและแผนการป้องกันภัยคุกคามด้านสิ่งแวดล้อมในพื้นที่ที่จำเป็นต้องรักษาความมั่นคง
ปลอดภัย

รหัสเอกสาร: PDPA-POL-09.11.3

เวอร์ชัน: 1.0

วันที่มีผลบังคับใช้: 1 มิถุนายน 2568

หน่วยงานรับผิดชอบ: ฝ่ายอาคารสถานที่และความมั่นคงปลอดภัย

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการป้องกันภัยคุกคามที่เกี่ยวข้องกับสภาพแวดล้อม เช่น ไฟไหม้ แผ่นดินไหว น้ำท่วม หรือเหตุการณ์ฉุกเฉินอื่น ๆ ภายในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย โดยเฉพาะพื้นที่ที่มีระบบสารสนเทศหรือข้อมูลส่วนบุคคล เช่น ศูนย์คอมพิวเตอร์ ห้องแม่ข่าย ระบบสำรองข้อมูล เป็นต้น

2. ขอบเขต

นโยบายนี้ครอบคลุมถึงอาคารสำนักงานหลัก พื้นที่จัดเก็บเซิร์ฟเวอร์ พื้นที่สำรองข้อมูล และพื้นที่ใด ๆ ที่ถูกกำหนดว่าเป็นพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

3. มาตรการที่นำมาใช้

ติดตั้งเครื่องตรวจจับควันไฟและสัญญาณเตือนอัคคีภัยแบบอัตโนมัติในพื้นที่ศูนย์คอมพิวเตอร์และพื้นที่สำคัญอื่น ๆ

3.2 ติดตั้งระบบดับเพลิงอัตโนมัติ (FM-200 หรือเทียบเท่า) สำหรับพื้นที่จัดเก็บเซิร์ฟเวอร์

3.3 ฝึกซ้อมอพยพหนีภัยจากอัคคีภัยและภัยพิบัติอย่างน้อยปีละหนึ่งครั้ง โดยมีการบันทึกรายงาน

ผล

3.4 จัดเตรียมเครื่องดับเพลิงประจำพื้นที่ และมีการตรวจสอบสภาพพร้อมใช้งานทุก 6 เดือน

3.5 จัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) และแผนตอบสนองเหตุการณ์ (Incident Response Plan) ที่ระบุถึงการรับมือภัยคุกคามทางธรรมชาติ

3.6 ดำเนินการตรวจสอบความเสี่ยงจากสิ่งแวดล้อม (Environmental Risk Assessment) ทุกปี และจัดทำรายงานผล

4. การรายงานและติดตามผล

หน่วยงานฝ่ายความมั่นคงปลอดภัยมีหน้าที่จัดทำรายงานประจำปีเกี่ยวกับสถานะการป้องกันภัยคุกคามด้านสิ่งแวดล้อมในพื้นที่สำคัญ เสนอแก่คณะกรรมการบริหารองค์กรเพื่อตรวจสอบและอนุมัติการปรับปรุงแผนประจำปีถัดไป

5. การอ้างอิงข้อกำหนด

อ้างอิงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 และข้อ 4 (2) และ (3) แห่งประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

ชื่อเอกสาร: นโยบายและแผนการป้องกันภัยคุกคามด้านสิ่งแวดล้อมในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

รหัสเอกสาร: PDPA-POL-09.11.3

เวอร์ชัน: 1.0

วันที่มีผลบังคับใช้: 1 มิถุนายน 2568

หน่วยงานรับผิดชอบ: ฝ่ายอาคารสถานที่และความมั่นคงปลอดภัย

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการป้องกันภัยคุกคามที่เกี่ยวข้องกับสภาพแวดล้อม เช่น ไฟไหม้ แผ่นดินไหว น้ำท่วม หรือเหตุการณ์ฉุกเฉินอื่น ๆ ภายในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย โดยเฉพาะพื้นที่ที่มีระบบสารสนเทศหรือข้อมูลส่วนบุคคล เช่น ศูนย์คอมพิวเตอร์ ห้องแม่ข่าย ระบบสำรองข้อมูล เป็นต้น

2. ขอบเขต

นโยบายนี้ครอบคลุมถึงอาคารสำนักงานหลัก พื้นที่จัดเก็บเซิร์ฟเวอร์ พื้นที่สำรองข้อมูล และพื้นที่ใด ๆ ที่ถูกกำหนดว่าเป็นพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

3. มาตรการที่นำมาใช้

3.1 ติดตั้งเครื่องตรวจจับควันไฟและสัญญาณเตือนอัคคีภัยแบบอัตโนมัติในพื้นที่ศูนย์คอมพิวเตอร์และพื้นที่สำคัญอื่น ๆ

3.2 ติดตั้งระบบดับเพลิงอัตโนมัติ (FM-200 หรือเทียบเท่า) สำหรับพื้นที่จัดเก็บเซิร์ฟเวอร์

3.3 ฝึกซ้อมอพยพหนีภัยจากอัคคีภัยและภัยพิบัติอย่างน้อยปีละหนึ่งครั้ง โดยมีการบันทึกรายงานผล

3.4 จัดเตรียมเครื่องดับเพลิงประจำพื้นที่ และมีการตรวจสอบสภาพพร้อมใช้งานทุก 6 เดือน

3.5 จัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) และแผนตอบสนอง

เหตุการณ์ (Incident Response Plan) ที่ระบุถึงการรับมือภัยคุกคามทางธรรมชาติ

3.6 ดำเนินการตรวจสอบความเสี่ยงจากสิ่งแวดล้อม (Environmental Risk Assessment) ทุกปี และจัดทำรายงานผล

4. การรายงานและติดตามผล

หน่วยงานฝ่ายความมั่นคงปลอดภัยมีหน้าที่จัดทำรายงานประจำปีเกี่ยวกับสถานะการป้องกันภัยคุกคามด้านสิ่งแวดล้อมในพื้นที่สำคัญ เสนอแก่คณะกรรมการบริหารองค์กรเพื่อตรวจสอบและอนุมัติการปรับปรุงแผนประจำปีถัดไป

5. การอ้างอิงข้อกำหนด

อ้างอิงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 และข้อ 4 (2) และ (3) แห่งประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

9.11.4 มีมาตรการป้องกันอุปกรณ์ของสำนักงานเพื่อป้องกันและลดความเสี่ยงจากการถูกขโมยหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

สิ่งที่ต้องทำ: มีมาตรการป้องกันอุปกรณ์ของสำนักงานเพื่อป้องกันและลดความเสี่ยงจากการถูกขโมยหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต และมีการตรวจสอบมาตรการดังกล่าว

หลักฐาน: นโยบายคุ้มครองความมั่นคงปลอดภัยในการเข้าถึงอุปกรณ์ของสำนักงานหรือพื้นที่ขององค์กร

ทะเบียนการเข้าถึงอุปกรณ์ที่ประมวลผลข้อมูลส่วนบุคคล

สัญญาจ้างบุคคลภายนอกเพื่อป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (6)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายและแนวปฏิบัติในการป้องกันอุปกรณ์ของสำนักงานเพื่อป้องกันและลดความเสี่ยงจากการถูกขโมยหรือเข้าถึงโดยไม่ได้รับอนุญาต

(รองรับข้อ 9.11.4 ตามเกณฑ์มาตรการรักษาความมั่นคงปลอดภัย)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการในการป้องกันอุปกรณ์ของสำนักงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล อันได้แก่ คอมพิวเตอร์แม่ข่าย เครื่องแม่ข่ายสำรอง ระบบจัดเก็บข้อมูล อุปกรณ์เคลื่อนที่ และอุปกรณ์เชื่อมต่อเครือข่าย ทั้งนี้เพื่อลดความเสี่ยงจากการถูกโจรกรรม การเข้าถึงโดยไม่ได้รับอนุญาต และเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

2. ขอบเขต

นโยบายนี้บังคับใช้กับบุคลากรขององค์กร พนักงาน ลูกจ้าง ผู้รับจ้าง และบุคคลภายนอกที่ได้รับอนุญาตให้ใช้งานอุปกรณ์ของสำนักงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

3. มาตรการที่องค์กรนำมาใช้

(1) การควบคุมการเข้าถึงอุปกรณ์

มีการกำหนดสิทธิ์การเข้าถึงอุปกรณ์ที่ใช้ประมวลผลข้อมูลส่วนบุคคล ตามระดับหน้าที่ของผู้ใช้งาน จัดทำทะเบียนการเข้าถึงอุปกรณ์ประมวลผลข้อมูลส่วนบุคคล และมีการตรวจสอบอย่างน้อยปีละ 1 ครั้ง

(2) การป้องกันการโจรกรรม

- ติดตั้งอุปกรณ์ล็อกทางกายภาพ เช่น สายล็อกคอมพิวเตอร์ (security cable lock) สำหรับอุปกรณ์สำคัญ
- มีระบบกล้องวงจรปิด (CCTV) ครอบคลุมพื้นที่เก็บหรือใช้งานอุปกรณ์สำคัญ
- ในกรณีพื้นที่สำคัญ อาจมีการใช้บริการรักษาความปลอดภัยจากบุคคลภายนอก โดยมีสัญญาจ้างชัดเจน

(3) มาตรการตรวจสอบและติดตาม

- มีการตรวจนับอุปกรณ์ตามทะเบียนทรัพย์สินสารสนเทศประจำปี
- รายงานผลการตรวจสอบต่อหัวหน้าหน่วยงานและผู้ควบคุมข้อมูลส่วนบุคคล
- กำหนดให้ผู้ใช้งานลงชื่อรับ-ส่ง เมื่อมีการเบิกใช้หรือเคลื่อนย้ายอุปกรณ์ออกนอกพื้นที่

(4) การจัดการเมื่อเกิดเหตุผิดปกติ

- จัดให้มีแผนรับมือเมื่อพบการโจรกรรมหรือการเข้าถึงโดยไม่ได้รับอนุญาต
- ดำเนินการสอบสวนภายในและรายงานต่อผู้ควบคุมข้อมูลส่วนบุคคลเพื่อพิจารณาการแจ้งเหตุไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ถ้ามีผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล)

4. เอกสารหลักฐานประกอบ

- นโยบายคุ้มครองความมั่นคงปลอดภัยในการเข้าถึงอุปกรณ์ของสำนักงานหรือพื้นที่ขององค์กร

- ทะเบียนการเข้าถึงอุปกรณ์ที่ประมวลผลข้อมูลส่วนบุคคล
- สัญญาจ้างบุคคลภายนอกเพื่อป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย

5. ฐานกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2), (6)

6. โทษทางปกครอง

ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลอาจได้รับโทษปรับทางปกครองไม่เกิน 3,000,000 บาท

9.11.5 มีมาตรการในการจัดเก็บเอกสารที่เป็นกระดาษให้มีความปลอดภัยและควบคุมการเข้าถึงเอกสารเหล่านั้น

- สิ่งที่ต้องทำ: มีมาตรการในการจัดเก็บเอกสารที่เป็นกระดาษให้มีความปลอดภัยและควบคุมการเข้าถึงเอกสารเหล่านั้น และมีเอกสารสนับสนุน
- หลักฐาน: นโยบายจัดเก็บเอกสารที่เป็นกระดาษไว้ในพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย มาตรการในการป้องกันการเข้าถึง การทำลาย หรือการเข้ามายุ่งเหยิงกับข้อมูลส่วนบุคคลในพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4) (6) โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายและแนวปฏิบัติในการจัดเก็บเอกสารที่เป็นกระดาษให้มีความปลอดภัยและควบคุมการเข้าถึง

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการจัดเก็บเอกสารที่เป็นกระดาษซึ่งมีข้อมูลส่วนบุคคลให้เป็นระบบ มีความปลอดภัย และสามารถควบคุมการเข้าถึงเอกสารเหล่านั้นได้ เพื่อลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยโดยมิชอบ หรือการทำลายเอกสารโดยไม่ตั้งใจหรือโดยเจตนา

2. ขอบเขต

นโยบายนี้ครอบคลุมการจัดเก็บเอกสารที่เป็นกระดาษในหน่วยงานหรือพื้นที่ขององค์กรที่เกี่ยวข้องกับการเก็บหรือประมวลผลข้อมูลส่วนบุคคล เช่น ฝ่ายทรัพยากรบุคคล ฝ่ายการเงิน ฝ่ายบริหารทั่วไป และแผนกงานธุรการต่าง ๆ

3. มาตรการที่องค์กรนำมาใช้

(1) การจัดพื้นที่จัดเก็บ

เอกสารที่เป็นกระดาษซึ่งมีข้อมูลส่วนบุคคลจะต้องจัดเก็บไว้ในตู้เก็บเอกสารที่มีการล็อก และอยู่ในพื้นที่ที่มีการควบคุมการเข้า-ออก

กรณีที่มีห้องเก็บเอกสารเฉพาะ ให้มีระบบรักษาความปลอดภัย เช่น การติดตั้งกล้องวงจรปิด (CCTV) และการจำกัดสิทธิ์การเข้าใช้งาน

(2) การควบคุมการเข้าถึง

- จำกัดผู้มีสิทธิ์เข้าถึงเอกสารตามความจำเป็นของหน้าที่งาน
- จัดทำบัญชีรายชื่อผู้มีสิทธิ์เข้าถึงเอกสาร และมีการตรวจสอบ/ทบทวนสิทธิ์อย่างน้อยปีละ 1 ครั้ง
- หากต้องมีการเข้าถึงเอกสารโดยบุคคลภายนอก ต้องมีการลงบันทึกการเข้า-ออก และมีผู้ดูแล

(3) การป้องกันการทำลายหรือสูญหาย

- ห้ามเก็บเอกสารข้อมูลส่วนบุคคลในพื้นที่ที่มีความเสี่ยงสูง เช่น พื้นที่เปิด พื้นที่ที่มีความชื้นหรืออยู่ใกล้แหล่งความร้อน
- หากมีการทำลายเอกสาร ต้องใช้วิธีที่ทำให้ไม่สามารถกู้คืนข้อมูลได้ เช่น การใช้เครื่องทำลายเอกสาร (paper shredder)

(4) การติดตามและประเมินผล

- มีการบันทึกการเบิก-จ่าย หรือการยืม-คืนเอกสาร
- มีรายงานการตรวจสอบมาตรการจัดเก็บเอกสารประจำปี
- ผู้ควบคุมข้อมูลส่วนบุคคลขององค์กรสามารถตรวจสอบได้ตามสิทธิ์

4. เอกสารหลักฐานประกอบ

- นโยบายจัดเก็บเอกสารที่เป็นกระดาษไว้ในพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย
- มาตรการในการป้องกันการเข้าถึง การทำลาย หรือการเข้ามายุ่งเหยิงกับข้อมูลส่วนบุคคลในพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย

- บัญชีรายชื่อผู้มีสิทธิ์เข้าถึงเอกสาร และแบบฟอร์มบันทึกการเข้าใช้งานพื้นที่หรือการยืมเอกสาร

5. ฐานกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2), (4), (6)

6. โทษทางปกครอง

ในกรณีที่มิปฏิบัติตามมาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลอาจได้รับโทษปรับทางปกครองไม่เกิน 3,000,000 บาท

9.11.6 มินโยบายโต๊ะสะอาด (Clear Desk Policy) เพื่อป้องกันการทิ้งข้อมูลหรือทรัพย์สินสำคัญขององค์กรไว้บนโต๊ะ ซึ่งอาจทำให้สูญหายหรือถูกเข้าถึงโดยไม่ได้รับอนุญาตได้

สิ่งที่ต้องทำ: มินโยบายโต๊ะสะอาด (Clear Desk Policy) เพื่อป้องกันการทิ้งข้อมูลหรือทรัพย์สินสำคัญขององค์กรไว้บนโต๊ะ ซึ่งอาจทำให้สูญหายหรือถูกเข้าถึงโดยไม่ได้รับอนุญาตได้ และมีเอกสารสนับสนุน

หลักฐาน: นโยบายโต๊ะสะอาด แบบตรวจเช็คข้อมูลหรือทรัพย์สินสำคัญขององค์กรประจำวัน สภาพ

บังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่มิปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายโต๊ะสะอาด (Clear Desk Policy)

องค์กรมีนโยบายโต๊ะสะอาด (Clear Desk Policy) เพื่อป้องกันการทิ้งข้อมูลหรือทรัพย์สินสำคัญขององค์กรไว้บนโต๊ะทำงาน ซึ่งอาจทำให้ข้อมูลสูญหายหรือถูกเข้าถึงโดยไม่ได้รับอนุญาตได้

สิ่งที่ต้องทำ

องค์กรต้องจัดทำนโยบายโต๊ะสะอาดเพื่อกำหนดแนวทางการรักษาความปลอดภัยของข้อมูลและทรัพย์สินสำคัญ โดยพนักงานต้องปฏิบัติตามอย่างเคร่งครัด เช่น การจัดเก็บเอกสาร ข้อมูลส่วนบุคคล และอุปกรณ์ต่าง ๆ หลังเลิกใช้ และควรมีการตรวจสอบหรือประเมินผลอย่างสม่ำเสมอ

หลักฐาน

- นโยบายโต๊ะสะอาด (Clear Desk Policy) ที่ระบุข้อกำหนดการจัดเก็บข้อมูลและทรัพย์สิน
- แบบฟอร์มหรือแบบตรวจเช็คข้อมูลและทรัพย์สินสำคัญขององค์กรประจำวัน

สภาพบังคับ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)

โทษทางปกครอง

อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่นปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

แบบเช็ค리스트โต๊ะสะอาด (Clear Desk Policy Checklist)

ชื่อพนักงาน: กิตติพงษ์ จันทรเพ็ญ

วันที่ตรวจสอบ: 5 มิถุนายน 2568

ผู้ตรวจสอบ: สุมิตรา ศรีสวัสดิ์

รายการตรวจสอบ	ปฏิบัติ แล้ว	หมายเหตุ
1. เอกสารที่มีข้อมูลส่วนบุคคลถูกเก็บเข้าที่ปลอดภัยเรียบร้อย	✓	เอกสารถูกจัดเก็บใน ลิ้นชักล็อก
2. ไม่มีเอกสารหรือกระดาษที่มีข้อมูลสำคัญวางทิ้งไว้บนโต๊ะ	✓	
3. อุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ โน้ตบุ๊ก ถูกล็อกหน้าจอหรือปิดเครื่องเมื่อไม่ใช้งาน	✓	ล็อกหน้าจอทุกครั้งเมื่อ ออกจากโต๊ะ
4. อุปกรณ์ที่ใช้ในการจัดเก็บข้อมูล เช่น USB, External HDD ถูกเก็บในที่ปลอดภัย	✓	USB ถูกเก็บในลิ้นชักล็อก
5. ไม่มีรหัสผ่าน หรือข้อมูลลับใด ๆ เขียนหรือวางไว้บนโต๊ะ	✓	
6. กุญแจและอุปกรณ์รักษาความปลอดภัยอื่น ๆ ถูกเก็บไว้อย่างถูกต้อง	✓	กุญแจถูกเก็บในกล่อง กุญแจ
7. ไม่มีอุปกรณ์หรือทรัพย์สินสำคัญวางไว้บนโต๊ะโดยไม่ควร	✓	
8. เอกสารสำคัญทั้งหมดได้จัดเก็บในลิ้นชักหรือตู้ล็อกอย่างถูกต้อง	✓	

9. มีการทำความสะอาดพื้นที่ทำงานและจัดระเบียบโต๊ะทุกวัน	✓	ทำความสะอาดเรียบร้อยทุกวัน
10. รายงานปัญหาหรือเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของข้อมูล (ถ้ามี)	✗	ไม่มีปัญหาหรือเหตุการณ์รายงาน

หมายเหตุเพิ่มเติม

พบว่าการล็อกหน้าจออุปกรณ์เป็นสิ่งที่ช่วยเพิ่มความปลอดภัยได้ดี ควรย้ำเตือนพนักงานให้ปฏิบัติอย่างสม่ำเสมอ

9.11.7 มีการจัดเก็บข้อมูลหรือทรัพย์สินสำคัญบนโต๊ะให้อยู่ในที่ที่เหมาะสมอย่างสม่ำเสมอ

สิ่งที่ต้องทำ: มีการจัดเก็บข้อมูลหรือทรัพย์สินสำคัญบนโต๊ะให้อยู่ในที่ที่เหมาะสมอย่างสม่ำเสมอ และมีการตรวจสอบเป็นประจำ

หลักฐาน: นโยบายโต๊ะสะอาด

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การจัดเก็บข้อมูลหรือทรัพย์สินสำคัญบนโต๊ะให้อยู่ในที่ที่เหมาะสมอย่างสม่ำเสมอ

องค์กรมีมาตรการในการจัดเก็บข้อมูลหรือทรัพย์สินสำคัญที่อยู่บนโต๊ะทำงานให้ถูกเก็บรักษาไว้ในที่เหมาะสมอย่างสม่ำเสมอ เช่น ในลิ้นชักหรือตู้ล็อก เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต และมีการตรวจสอบการจัดเก็บอย่างสม่ำเสมอเป็นประจำ เพื่อให้แน่ใจว่าทรัพย์สินและข้อมูลสำคัญไม่ได้ถูกทิ้งไว้บนโต๊ะในลักษณะที่เสี่ยงต่อความปลอดภัย

สิ่งที่ต้องทำ

- มีการจัดเก็บข้อมูลหรือทรัพย์สินสำคัญบนโต๊ะให้อยู่ในที่ที่เหมาะสมอย่างสม่ำเสมอ
- มีการตรวจสอบและทบทวนมาตรการการจัดเก็บอย่างต่อเนื่อง
- ให้พนักงานทุกคนปฏิบัติตามนโยบายโต๊ะสะอาด (Clear Desk Policy) อย่างเคร่งครัด

หลักฐาน

- นโยบายโต๊ะสะอาด (Clear Desk Policy) ขององค์กร
- รายงานการตรวจสอบการปฏิบัติตามนโยบายโต๊ะสะอาดประจำเดือนหรือประจำปี

สภาพบังคับ

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (4)

โทษทางปกครอง:

ตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัย อาจถูกกำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

เช็คลิสต์การจัดเก็บข้อมูลหรือทรัพย์สินสำคัญบนโต๊ะ (ข้อ 9.11.7)

รายการตรวจสอบ	ผลการตรวจสอบ (✓ / ✗)	หมายเหตุ
มีนโยบายโต๊ะสะอาด (Clear Desk Policy) ที่ชัดเจนและเผยแพร่ในองค์กร		
ข้อมูลหรือทรัพย์สินสำคัญบนโต๊ะถูกจัดเก็บในที่เหมาะสม เช่น ล็อกหรือตู้ล็อก		
มีการตรวจสอบการปฏิบัติตามนโยบายโต๊ะสะอาดเป็นประจำ เช่น รายเดือนหรือรายปี		
พนักงานทุกคนรับทราบและปฏิบัติตามนโยบายอย่างเคร่งครัด		
มีการบันทึกผลการตรวจสอบและรายงานต่อผู้รับผิดชอบ		
มีมาตรการแก้ไขกรณีพบการละเมิดหรือไม่ปฏิบัติตามนโยบาย		

ตัวอย่างการกรอกข้อมูลในเช็ค리스트การจัดเก็บข้อมูลหรือทรัพย์สินสำคัญบนโต๊ะ		
รายการตรวจสอบ	ผลการตรวจสอบ (✓ / ✗)	หมายเหตุ
มีนโยบายโต๊ะสะอาด (Clear Desk Policy) ที่ชัดเจนและเผยแพร่ในองค์กร	✓	นโยบายได้รับการประกาศและส่งถึงพนักงานทุกคนแล้ว
ข้อมูลหรือทรัพย์สินสำคัญบนโต๊ะถูกจัดเก็บในที่ที่เหมาะสม เช่น ล็อกหรือตู้ล็อก	✓	พนักงานจัดเก็บเอกสารสำคัญในล็อกทุกครั้งหลังใช้งาน
มีการตรวจสอบการปฏิบัติตามนโยบายโต๊ะสะอาดเป็นประจำ เช่น รายเดือนหรือรายปี	✓	ฝ่ายตรวจสอบความปลอดภัยตรวจสอบทุกเดือน
พนักงานทุกคนรับทราบและปฏิบัติตามนโยบายอย่างเคร่งครัด	✓	มีการอบรมและแจ้งเตือนอย่างต่อเนื่อง
มีการบันทึกผลการตรวจสอบและรายงานต่อผู้รับผิดชอบ	✓	รายงานผลการตรวจสอบถูกส่งให้ผู้บริหารทุกเดือน
มีมาตรการแก้ไขกรณีพบการละเมิดหรือไม่ปฏิบัติตามนโยบาย	✓	พบการละเมิดมีการแจ้งเตือนและดำเนินการตามขั้นตอนทันที

9.11.8 มีนโยบายหน้าจอสะอาด (Clear Screen Policy) เพื่อล็อกหน้าจอของเครื่องคอมพิวเตอร์เป็นประจำ เมื่อไม่ได้มีการใช้งานมาเป็นระยะเวลาหนึ่ง หรือเพื่อให้มีการ Logout ออกจากเครื่องคอมพิวเตอร์เมื่อไม่ได้มีการใช้งาน

สิ่งที่ต้องทำ: มีนโยบายหน้าจอสะอาด (Clear Screen Policy) เพื่อล็อกหน้าจอของเครื่องคอมพิวเตอร์เป็นประจำ เมื่อไม่ได้มีการใช้งานมาเป็นระยะเวลาหนึ่ง หรือเพื่อให้มีการ logout ออกจากเครื่องคอมพิวเตอร์เมื่อไม่ได้มีการใช้งาน และมีการตรวจสอบการปฏิบัติตามในองค์กร

หลักฐาน: นโยบายหน้าจอสะอาด

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายหน้าจอสะอาด (Clear Screen Policy)

1. วัตถุประสงค์

เพื่อปกป้องข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กรจากการเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการล็อกหน้าจอคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ทุกเครื่องเมื่อไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง รวมถึงการ logout ออกจากระบบเมื่อเลิกใช้งาน เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลในองค์กร

2. ขอบเขต

นโยบายนี้มีผลบังคับใช้กับพนักงานทุกคนที่ใช้เครื่องคอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ หรือระบบสารสนเทศภายในองค์กร

3. ข้อกำหนด

3.1 พนักงานต้องตั้งค่าล็อกหน้าจออัตโนมัติ (Auto-lock) บนอุปกรณ์ของตน เมื่อไม่มีการใช้งานเกิน 5 นาที หรือระยะเวลาที่องค์กรกำหนด

3.2 พนักงานต้องล็อกหน้าจอด้วยตนเอง หรือ logout ออกจากระบบทุกครั้งเมื่อหยุดใช้งานเครื่องคอมพิวเตอร์ หรือก่อนออกจากพื้นที่ทำงาน

3.3 ห้ามเปิดเผยรหัสผ่านหรือวิธีการล็อกหน้าจอแก่บุคคลอื่น

3.4 ฝ่ายเทคโนโลยีสารสนเทศจะตรวจสอบการตั้งค่าความปลอดภัยและการปฏิบัติตามนโยบายนี้ อย่างสม่ำเสมอ

4. การตรวจสอบและบังคับใช้

4.1 ฝ่ายไอทีจะรายงานผลการตรวจสอบการปฏิบัติตามนโยบายนี้ให้ฝ่ายบริหารรับทราบเป็นประจำ

4.2 หากพบว่าพนักงานไม่ปฏิบัติตามนโยบายนี้ อาจถูกดำเนินการทางวินัยตามระเบียบข้อบังคับขององค์กร

5. ความรับผิดชอบ

พนักงานทุกคนมีหน้าที่ปฏิบัติตามนโยบายนี้อย่างเคร่งครัดเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินขององค์กร

6. เริ่มมีผลบังคับใช้

นโยบายนี้มีผลบังคับใช้ตั้งแต่วันที่ [วันที่เริ่มบังคับใช้] เป็นต้นไป

เช็คлистนโยบายหน้าจอสะอาด (Clear Screen Policy) (ข้อ 9.11.8)		
รายการตรวจสอบ	ผลการตรวจสอบ (✓ / ✗)	หมายเหตุ
มีการจัดทำนโยบายหน้าจอสะอาด (Clear Screen Policy) อย่างเป็นลายลักษณ์อักษร	✓	นโยบายจัดทำเสร็จและประกาศใช้ตั้งแต่เดือนมกราคม 2565
มีการตั้งเวลาล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานเกิน 5 นาที	✓	ตั้งค่าระบบล็อกหน้าจออัตโนมัติทุกเครื่องคอมพิวเตอร์ในองค์กร
มีการแจ้งเตือนพนักงานเกี่ยวกับการล็อกหน้าจอและการ Logout เมื่อไม่ได้ใช้งาน	✓	มีการอบรมพนักงานทุกไตรมาส
มีการตรวจสอบและติดตามการปฏิบัติตามนโยบายนี้ในองค์กรเป็นประจำ	✓	ฝ่ายไอทีตรวจสอบรายงานล็อกหน้าจอทุกเดือน
พนักงานทุกคนรับทราบและปฏิบัติตามนโยบายอย่างเคร่งครัด	✓	มีการสอบถามและสำรวจความเข้าใจของพนักงานทุก 6 เดือน
มีการบันทึกผลการตรวจสอบและรายงานให้ผู้บริหารทราบ	✓	รายงานผลการตรวจสอบส่งต่อฝ่ายบริหารทุกเดือน

9.12 แผนความต่อเนื่องทางธุรกิจ การกู้คืนจากภัยพิบัติ และการสำรองข้อมูล (Business continuity, disaster recovery and backups) องค์กรมีแผนที่จะจัดการกับการหยุดชะงักทางธุรกิจที่ร้ายแรง โดยมีการสำรองระบบงานที่สำคัญ แอปพลิเคชัน และข้อมูล เพื่อป้องกันการสูญหายของข้อมูลส่วนบุคคล

9.12.1 มีแผนความต่อเนื่องทางธุรกิจ เพื่อบริหารจัดการการหยุดชะงักทางธุรกิจหรือภัยพิบัติต่าง ๆ ที่เกิดขึ้น และเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง

สิ่งที่ต้องทำ: มีแผนความต่อเนื่องทางธุรกิจ เพื่อบริหารจัดการการหยุดชะงักทางธุรกิจหรือภัยพิบัติต่าง ๆ ที่เกิดขึ้น และเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ชัดเจน

หลักฐาน: นโยบายการจัดทำแผนความต่อเนื่องทางธุรกิจ เพื่อบริหารจัดการการหยุดชะงักทางธุรกิจหรือภัยพิบัติต่าง ๆ ที่เกิดขึ้น และเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง แผนความต่อเนื่องทางธุรกิจ เพื่อบริหารจัดการการหยุดชะงักทางธุรกิจหรือภัยพิบัติต่าง ๆ ที่เกิดขึ้น และเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง ไม่เกิน 3 ล้านบาท

ตัวอย่างแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan - BCP)

1. บทนำ

1.1 วัตถุประสงค์

เพื่อให้มั่นใจว่าองค์กรสามารถบริหารจัดการและฟื้นฟูกิจกรรมธุรกิจได้อย่างต่อเนื่องในกรณีเกิดเหตุการณ์หยุดชะงัก ไม่ว่าจะเป็นภัยธรรมชาติ ภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ไม่คาดฝันอื่น ๆ โดยรักษาความปลอดภัยของข้อมูลส่วนบุคคลและทรัพย์สินขององค์กร

1.2 ขอบเขต

แผนนี้ครอบคลุมระบบงานหลัก แอปพลิเคชัน ข้อมูลส่วนบุคคล ระบบไอที และทรัพย์สินที่จำเป็นสำหรับการดำเนินธุรกิจ

2. คณะกรรมการบริหารความต่อเนื่องทางธุรกิจ

2.1 ผู้รับผิดชอบหลัก

หัวหน้าแผนก IT: รับผิดชอบการกู้คืนระบบ IT

ผู้จัดการฝ่ายความเสี่ยง: ดูแลการประเมินและวางแผนความเสี่ยง

เจ้าหน้าที่ความปลอดภัยข้อมูลส่วนบุคคล (DPO): ดูแลความปลอดภัยข้อมูลส่วนบุคคล

ผู้อำนวยการฝ่ายบริหาร: ควบคุมและตัดสินใจขั้นสุดท้าย

3. การประเมินความเสี่ยง (Risk Assessment)

วิเคราะห์ความเสี่ยงที่อาจส่งผลกระทบต่อธุรกิจ เช่น ไฟไหม้, น้ำท่วม, แผ่นดินไหว, การโจมตีทางไซเบอร์, การล่มของระบบเครือข่าย

กำหนดระดับความรุนแรงและความน่าจะเป็นของแต่ละเหตุการณ์

จัดลำดับความสำคัญของระบบและข้อมูลที่ต้องปกป้อง

4. การเตรียมพร้อม (Preparedness)

- สำรองข้อมูล (Backup) ทุกระบบที่สำคัญอย่างน้อยวันละ 1 ครั้ง และเก็บสำรองข้อมูลในสถานที่ที่ปลอดภัยนอกสถานที่ทำงาน
- กำหนดขั้นตอนการล็อกเครื่องคอมพิวเตอร์และนโยบายหน้าจอสะอาด (Clear Screen Policy)
- จัดเตรียมอุปกรณ์สำรองสำหรับใช้งานในกรณีระบบหลักล่ม
- ฝึกซ้อมแผนความต่อเนื่องทางธุรกิจอย่างน้อยปีละ 2 ครั้ง

5. ขั้นตอนการตอบสนองเมื่อเกิดเหตุการณ์ (Incident Response)

ขั้นตอน	รายละเอียด
5.1 แจ้งเหตุการณ์	ผู้พบเหตุการณ์แจ้งผู้รับผิดชอบทันที พร้อมรายละเอียดเหตุการณ์
5.2 ประเมินสถานการณ์	คณะกรรมการบริหารความต่อเนื่องฯ ประเมินผลกระทบและตัดสินใจดำเนินการ
5.3 ดำเนินการป้องกัน	ดำเนินมาตรการฉุกเฉินเพื่อป้องกันความเสียหายเพิ่มเติม เช่น ตัดไฟ ปิดระบบ เครือข่ายชั่วคราว
5.4 สื่อสารภายใน	แจ้งข้อมูลเหตุการณ์และแนวทางให้พนักงานรับทราบ พร้อมเตรียมข้อมูลสื่อสารกับลูกค้า/ผู้เกี่ยวข้อง
5.5 เริ่มการฟื้นฟู	เริ่มกู้คืนระบบสำคัญและข้อมูล โดยให้ความสำคัญกับข้อมูลส่วนบุคคลและระบบงานที่มีผลกระทบสูงสุด

6. แผนกู้คืนระบบและข้อมูล (Disaster Recovery Plan)

การกู้คืนข้อมูลสำรองจากระบบ Backup ตามลำดับความสำคัญ

- ใช้ระบบสำรอง (Failover system) หากมี
- ตรวจสอบความสมบูรณ์ของข้อมูลหลังจากกู้คืน
- ทดสอบระบบหลังฟื้นฟูเพื่อความพร้อมใช้งาน

7. การสำรองข้อมูล (Backup Policy)

- ข้อมูลทั้งหมดที่เกี่ยวข้องกับระบบงานหลักและข้อมูลส่วนบุคคลต้องมีการสำรองอย่างสม่ำเสมอ
- กำหนดรูปแบบและสถานที่จัดเก็บข้อมูลสำรอง เช่น Cloud storage, External drives ที่ปลอดภัย
- มีการตรวจสอบและทดสอบการกู้คืนข้อมูลเป็นระยะ

8. การทบทวนและปรับปรุงแผน

- ทบทวนแผนความต่อเนื่องทางธุรกิจทุก 6 เดือน หรือหลังเกิดเหตุการณ์
- รายงานผลการฝึกซ้อมและเหตุการณ์จริง พร้อมข้อเสนอแนะเพื่อปรับปรุงแผน
- ฝึกอบรมพนักงานเกี่ยวกับแผนและมาตรการต่าง ๆ อย่างต่อเนื่อง

9. แนบท้าย

- แบบฟอร์มแจ้งเหตุการณ์
- รายชื่อผู้รับผิดชอบและช่องทางการติดต่อ
- ตารางเวลาการสำรองข้อมูลและทดสอบแผน
- เอกสารนโยบายและมาตรการความปลอดภัยที่เกี่ยวข้อง

1. แบบฟอร์มแจ้งเหตุการณ์ (Incident Report Form)

แบบฟอร์มแจ้งเหตุการณ์ความต่อเนื่องทางธุรกิจ (Business Continuity Incident Report Form)

รายละเอียด	ข้อมูล
วันที่แจ้ง เหตุการณ์	(วัน/เดือน/ปี)
เวลาแจ้ง เหตุการณ์	(ชั่วโมง:นาที)
ผู้แจ้งเหตุการณ์	(ชื่อ-นามสกุล ตำแหน่ง)
ติดต่อกลับ	(เบอร์โทรศัพท์ อีเมล)
ประเภท เหตุการณ์	[] ภัยธรรมชาติ (น้ำท่วม ไฟไหม้ ฯลฯ) [] ภัยคุกคามทางไซเบอร์ (ไวรัส แอ็ก) [] ระบบล่ม/ขัดข้อง [] อุบัติเหตุภายในองค์กร [] อื่น ๆ (โปรดระบุ) _____
รายละเอียด เหตุการณ์	(อธิบายสถานการณ์ที่เกิดขึ้น)
ผลกระทบ เบื้องต้น	(ระบบงานที่ได้รับผลกระทบ ข้อมูลสูญหาย ฯลฯ)
การดำเนินการ เบื้องต้น	(มาตรการที่ได้ดำเนินการ เช่น ตัดระบบ แจ้งฝ่าย IT)
ผู้รับผิดชอบ ติดตามแก้ไข	(ชื่อ-นามสกุล ตำแหน่ง)
กำหนดเวลาแก้ไข	(วัน/เดือน/ปี เวลา)
หมายเหตุเพิ่มเติม	(ข้อมูลอื่น ๆ ที่เกี่ยวข้อง)

ลายเซ็นผู้แจ้ง: _____

วันที่: _____

ลายเซ็นผู้รับแจ้ง: _____

วันที่: _____

2. รายชื่อผู้รับผิดชอบและช่องทางการติดต่อ (Contact List)

ตำแหน่ง/หน้าที่	ชื่อ-นามสกุล	เบอร์โทรศัพท์ (มือถือ/ สำนักงาน)	อีเมล	หมายเหตุ
หัวหน้าแผนก IT	นายสมชาย ใจดี	081-123-4567 / 02-123-4567	somchai@company.com	ผู้รับผิดชอบระบบไอที
ผู้จัดการฝ่ายความเสี่ยง	นางสาวสุดา รัตน์ แสนดี	082-234-5678 / 02-234-5678	sudarat@company.com	รับผิดชอบการประเมินความเสี่ยง
เจ้าหน้าที่ความปลอดภัยข้อมูล (DPO)	นายกิตติ สุขสม	083-345-6789 / 02-345-6789	kitti@company.com	รับผิดชอบความปลอดภัยข้อมูลส่วนบุคคล
ผู้อำนวยการฝ่ายบริหาร	นายประยูร ทองดี	084-456-7890 / 02-456-7890	prayoon@company.com	ตัดสินใจขั้นสุดท้าย
ฝ่ายสื่อสารองค์กร	นางสาว จันทร์เพ็ญ แสงทอง	085-567-8901 / 02-567-8901	janpen@company.com	ติดต่อสื่อสารภายนอกและภายในองค์กร

3. ตารางเวลาการสำรองข้อมูลและทดสอบแผน (Backup and Test Schedule)

กิจกรรม	ความถี่	ผู้รับผิดชอบ	หมายเหตุ
สำรองข้อมูลระบบงานหลัก	ทุกวัน (กลางคืน)	แผนก IT	สำรองข้อมูลทุกระบบสำคัญ และจัดเก็บในสถานที่ปลอดภัย
ตรวจสอบความสมบูรณ์ของข้อมูลสำรอง	ทุกสัปดาห์ (วันศุกร์)	แผนก IT	ตรวจสอบว่าไฟล์ข้อมูลไม่เสียหาย สามารถกู้คืนได้
ทดสอบกู้คืนข้อมูล	ทุกไตรมาส	แผนก IT และ DPO	ทดสอบการกู้คืนข้อมูลเพื่อความพร้อม
ฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ	ทุก 6 เดือน	คณะกรรมการบริหาร ความต่อเนื่อง	ประเมินผลและปรับปรุงแผน

ทบทวนนโยบายและแผนความต่อเนื่อง	ปีละ 1 ครั้ง	ผู้จัดการฝ่ายความเสี่ยง	ปรับปรุงตามสถานการณ์และเทคโนโลยี

4. เอกสารนโยบายและมาตรการความปลอดภัยที่เกี่ยวข้อง (Policies and Security Measures)

เอกสารนโยบายสำคัญที่เกี่ยวข้องกับแผนความต่อเนื่องทางธุรกิจ

นโยบายความปลอดภัยข้อมูลส่วนบุคคล (Data Protection Policy)

- กำหนดแนวทางการเก็บรักษาและปกป้องข้อมูลส่วนบุคคล
- มีมาตรการควบคุมการเข้าถึงข้อมูล
- ระบุวิธีปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูล

นโยบายโต๊ะสะอาด (Clear Desk Policy)

- ห้ามวางเอกสารสำคัญหรือทรัพย์สินองค์กรไว้บนโต๊ะเมื่อไม่ใช้งาน
- เก็บข้อมูลไว้ในลิ้นชักหรือตู้ล็อกที่ปลอดภัย

นโยบายหน้าจอสะอาด (Clear Screen Policy)

- ให้ล็อกหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งานเกิน 5 นาที
- หลีกเลี่ยงการเก็บรหัสผ่านไว้ในหน้าจอหรือแผ่นบันทึกที่เปิดเผย

นโยบายสำรองข้อมูล (Backup Policy)

- กำหนดวิธีการและความถี่ในการสำรองข้อมูลระบบงานและข้อมูลส่วนบุคคล
- กำหนดสถานที่เก็บข้อมูลสำรองที่ปลอดภัย
- ระบุขั้นตอนการกู้คืนข้อมูลกรณีเกิดเหตุฉุกเฉิน

มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Measures)

- ใช้ระบบไฟร์วอลล์และระบบป้องกันไวรัส
- อัปเดตซอฟต์แวร์และแพตช์ความปลอดภัยอย่างสม่ำเสมอ
- ฝึกอบรมพนักงานเรื่องการใช้งานระบบและการรับมือกับภัยคุกคาม

9.12.2 มีการสำรองข้อมูลและนำไปจัดเก็บไว้นอกสถานที่

สิ่งที่ต้องทำ: มีการสำรองข้อมูลและนำไปจัดเก็บไว้นอกสถานที่

หลักฐาน: นโยบายการสำรองข้อมูลและนำไปจัดเก็บไว้นอกสถานที่

บันทึกข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

บันทึกข้อตกลงรักษาความลับ

มาตรการทางกายภาพ มาตรการทางเทคนิค และมาตรการด้านการบริหารจัดการ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (4)
โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง
ไม่เกิน 3 ล้านบาท

นโยบายการสำรองข้อมูลและนำไปจัดเก็บไว้นอกสถานที่ (Data Backup and Offsite Storage Policy)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางการสำรองข้อมูลและจัดเก็บข้อมูลสำรองไว้นอกสถานที่อย่างปลอดภัย เพื่อ
ป้องกันการสูญหายของข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กรในกรณีเกิดเหตุฉุกเฉินหรือภัยพิบัติ
และเพื่อให้เป็นไปตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศ
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

2. ขอบเขต

นโยบายนี้ครอบคลุมการสำรองข้อมูลทุกประเภทที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ข้อมูลสำคัญทางธุรกิจ
และข้อมูลระบบงานต่าง ๆ ขององค์กร รวมถึงการนำข้อมูลสำรองไปจัดเก็บในสถานที่อื่นที่ไม่ใช่สถานที่ตั้ง
หลักขององค์กร

3. แนวทางปฏิบัติ

3.1 การสำรองข้อมูล (Backup)

- ข้อมูลสำคัญทั้งหมดต้องมีการสำรองข้อมูลอย่างน้อยวันละครั้ง (Daily Backup)
- ข้อมูลที่สำรองต้องครอบคลุมระบบงานหลัก ระบบฐานข้อมูล และไฟล์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- การสำรองข้อมูลต้องทำโดยใช้เทคโนโลยีที่มีความปลอดภัย และมีการเข้ารหัสข้อมูล (Encryption)
- เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
ต้องจัดทำรายงานผลการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อตรวจสอบความสำเร็จของการสำรอง

ข้อมูล

3.2 การนำข้อมูลสำรองไปจัดเก็บนอกสถานที่ (Offsite Storage)

- ข้อมูลสำรองต้องถูกนำไปจัดเก็บไว้นอกสถานที่ที่ตั้งหลักขององค์กร ที่มีความปลอดภัยทั้งทาง
กายภาพและทางเทคนิค

- สถานที่จัดเก็บข้อมูลสำรองต้องมีมาตรการป้องกันภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ หรือ แผ่นดินไหว
- การเข้าถึงข้อมูลสำรองที่จัดเก็บนอกสถานที่ต้องถูกควบคุมอย่างเข้มงวด โดยมีการตรวจสอบและบันทึกการเข้าใช้งานทุกครั้ง
- ต้องมีบันทึกข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) กับผู้ให้บริการจัดเก็บข้อมูลนอกสถานที่ (ถ้ามี)
- ต้องมีบันทึกข้อตกลงรักษาความลับ (Non-Disclosure Agreement) กับผู้ที่เกี่ยวข้องกับการจัดเก็บและจัดการข้อมูลสำรองนอกสถานที่

3.3 มาตรการรักษาความปลอดภัย

มาตรการทางกายภาพ

- สถานที่จัดเก็บข้อมูลสำรองต้องมีระบบรักษาความปลอดภัย เช่น กล้องวงจรปิด ระบบควบคุมการเข้าออก และเจ้าหน้าที่รักษาความปลอดภัย
- ต้องมีระบบป้องกันไฟไหม้ และระบบสำรองไฟฟ้า (UPS หรือ Generator) เพื่อให้บริการยังคงดำเนินต่อไปในกรณีไฟฟ้าขัดข้อง

มาตรการทางเทคนิค

- ข้อมูลสำรองต้องถูกเข้ารหัสทั้งตอนจัดเก็บและขณะส่งข้อมูลระหว่างสถานที่ต่าง ๆ
- ระบบจัดเก็บข้อมูลสำรองต้องมีการอัปเดตแพตช์ด้านความปลอดภัยอย่างสม่ำเสมอ
- ต้องมีระบบตรวจจับและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต เช่น ระบบ Firewall และระบบตรวจสอบความปลอดภัย (IDS/IPS)

มาตรการบริหารจัดการ

- กำหนดหน้าที่ความรับผิดชอบชัดเจนสำหรับบุคลากรที่เกี่ยวข้องกับการสำรองข้อมูลและการจัดเก็บนอกสถานที่
- จัดให้มีการอบรมและให้ความรู้เรื่องการรักษาความปลอดภัยข้อมูลแก่บุคลากร
- ดำเนินการตรวจสอบและทบทวนมาตรการความปลอดภัยเป็นระยะ เพื่อให้แน่ใจว่ายังคงมีประสิทธิภาพและเหมาะสม

4. การทบทวนและปรับปรุงนโยบาย

นโยบายนี้จะถูกทบทวนและปรับปรุงอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกี่ยวกับการจัดเก็บข้อมูลหรือกฎหมายที่เกี่ยวข้อง

5. บทลงโทษ

ผู้ที่ไม่ปฏิบัติตามนโยบายนี้ จะได้รับโทษตามกฎหมายที่เกี่ยวข้อง รวมถึงบทลงโทษทางปกครองตามมาตรา 37 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

9.12.3 มีการสำรองข้อมูลด้วยความถี่ที่เหมาะสม

สิ่งที่ต้องทำ: มีการสำรองข้อมูลด้วยความถี่ที่เหมาะสม และมีหลักฐานการตรวจสอบ

หลักฐาน: นโยบายสำรองข้อมูลส่วนบุคคลด้วยความถี่ที่เหมาะสม

หนังสือรายงานตรวจสอบการจัดทำแผนความต่อเนื่องทางธุรกิจ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (4), ข้อ 5

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายการสำรองข้อมูลด้วยความถี่ที่เหมาะสม (Data Backup Frequency Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานความถี่ในการสำรองข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กร เพื่อให้มั่นใจว่าข้อมูลสำรองมีความทันสมัยและพร้อมใช้งานในกรณีเกิดเหตุขัดข้องหรือต้องกู้คืนข้อมูล และเป็นไปตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

2. ขอบเขต

นโยบายนี้ครอบคลุมการสำรองข้อมูลทุกประเภทที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ข้อมูลทางธุรกิจ และระบบสารสนเทศต่าง ๆ ขององค์กร

3. แนวทางปฏิบัติ

3.1 ความถี่ในการสำรองข้อมูล

- ข้อมูลที่มีความสำคัญสูง เช่น ข้อมูลส่วนบุคคลและฐานข้อมูลที่ใช้ในการดำเนินธุรกิจ ต้องมีการสำรองข้อมูลอย่างน้อย **วันละครั้ง (Daily Backup)** หรือบ่อยกว่านั้นตามความจำเป็นของระบบ
- ข้อมูลที่มีการเปลี่ยนแปลงน้อยหรือมีความสำคัญต่ำกว่า สามารถสำรองข้อมูลเป็นรายสัปดาห์หรือรายเดือน แต่ต้องแน่ใจว่ายังสามารถรองรับการกู้คืนได้อย่างเหมาะสม

- การกำหนดความถี่ในการสำรองข้อมูลจะต้องพิจารณาความเสี่ยงทางธุรกิจ และลักษณะของข้อมูลแต่ละประเภท

3.2 การตรวจสอบและบันทึกผลการสำรองข้อมูล

- ต้องมีการตรวจสอบความสำเร็จของกระบวนการสำรองข้อมูลอย่างสม่ำเสมอ
- ต้องจัดทำรายงานผลการสำรองข้อมูล (Backup Report) เพื่อบันทึกเวลาการสำรองข้อมูลและผลการดำเนินงาน
- รายงานดังกล่าวจะถูกเก็บเป็นหลักฐานและนำไปใช้ในการตรวจสอบภายในและภายนอกองค์กร

3.3 การฝึกอบรมและการรับผิดชอบ

บุคลากรที่รับผิดชอบต้องได้รับการฝึกอบรมเกี่ยวกับการสำรองข้อมูลและการตรวจสอบตามนโยบายนี้ กำหนดหน้าที่ความรับผิดชอบชัดเจนในแต่ละส่วนงานที่เกี่ยวข้อง

4. หลักฐานประกอบ

- นโยบายการสำรองข้อมูลด้วยความถี่ที่เหมาะสม
- หนังสือรายงานตรวจสอบการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan Audit Report)
- รายงานผลการสำรองข้อมูล (Backup Report)

5. กฎหมายและข้อบังคับที่เกี่ยวข้อง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (4), ข้อ 5

6. บทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการละเมิดกฎหมายตามมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีโทษปรับทางปกครองไม่เกิน 3 ล้านบาท และอาจได้รับบทลงโทษทางวินัยจากองค์กรด้วย

9.12.4 มีการทดสอบการเข้าถึงข้อมูลที่สำรองไว้ รวมทั้งทดสอบขั้นตอนการกู้คืนระบบ เพื่อให้เกิดความมั่นใจในการเตรียมความพร้อมสำหรับการกู้คืนระบบ

สิ่งที่ต้องทำ: มีการทดสอบการเข้าถึงข้อมูลที่สำรองไว้ รวมทั้งทดสอบขั้นตอนการกู้คืนระบบ เพื่อให้เกิดความมั่นใจในการเตรียมความพร้อมสำหรับการกู้คืนระบบ และมีเอกสารครบถ้วน

- หลักฐาน: นโยบายการทดสอบการเข้าถึงข้อมูลที่สำคัญไว้ รวมทั้งทดสอบขั้นตอนการกู้คืนระบบ
 รายงานผลทดสอบการเข้าถึงข้อมูลที่สำคัญและขั้นตอนการกู้คืนระบบเบื้องต้น
 รายงานผลทดสอบการเข้าถึงข้อมูลที่สำคัญและขั้นตอนการกู้คืนระบบ
 รายงานพิจารณาผลทดสอบการเข้าถึงข้อมูลที่สำคัญและขั้นตอนการกู้คืนระบบ
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัย
 ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (4), ข้อ 5
- โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง
 ไม่เกิน 3 ล้านบาท

นโยบายการทดสอบการเข้าถึงข้อมูลที่สำคัญไว้ รวมทั้งทดสอบขั้นตอนการกู้คืนระบบ

Backup Access and System Recovery Testing Policy

1. บทนำ (Introduction)

การสำรองข้อมูลและการกู้คืนระบบ (Backup and System Recovery) เป็นเหมือน “ร่มชูชีพ” (safety net) ของธุรกิจ ถ้าเกิดเหตุไม่คาดฝัน เช่น ระบบล่ม (System Failure) ข้อมูลเสียหาย หรือถูกโจมตีทางไซเบอร์ (Cyber Attack) ธุรกิจจะสามารถกลับมาดำเนินงานต่อได้โดยไม่เสียหายรุนแรง เปรียบเทียบง่าย ๆ เหมือนคุณเก็บสมบัติสำคัญไว้ในตู้เซฟ (Safe) ถ้าเกิดเหตุการณ์ไฟไหม้ คุณยังมีสำเนาสำรองที่เก็บไว้นอกบ้าน (Offsite Backup) ซึ่งสามารถนำมาใช้กู้คืนได้ทันที การทดสอบเข้าถึงข้อมูลสำรองและขั้นตอนการกู้คืนระบบจึงเหมือนการลองเปิดตู้เซฟและลองเอาสมบัติออกมาใช้ก่อนเกิดเหตุจริง การทดสอบนี้สอดคล้องกับมาตรฐานสากลและกฎหมายด้านความมั่นคงของข้อมูลและการบริหารความต่อเนื่องทางธุรกิจ เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคล (Personal Data) และข้อมูลสำคัญขององค์กร (Critical Business Data) ปลอดภัยและสามารถกู้คืนได้เมื่อเกิดเหตุฉุกเฉิน

2. วัตถุประสงค์ (Objectives)

1. เข้าถึงข้อมูลสำรองได้จริง (Ensure Backup Accessibility)

เพื่อยืนยันว่าข้อมูลสำรองที่สำคัญสามารถเปิดอ่านและใช้ได้ทันที หากเกิดเหตุฉุกเฉิน

2. ระบบกู้คืนทำงานได้ตามปกติ (Verify System Recovery)

การทดสอบขั้นตอนการกู้คืนช่วยให้มั่นใจว่า ระบบฐานข้อมูล (Database), เซิร์ฟเวอร์อีเมล (Email Server), เซิร์ฟเวอร์ไฟล์ (File Server) และเครื่องเสมือน (Virtual Machine) สามารถกลับมาทำงานปกติ

3. ลดความเสี่ยงข้อมูลสูญหาย (Minimize Data Loss Risk)

การทดสอบนี้เปรียบเสมือน “ซ้อมหนีไฟ” (Fire Drill) ถ้าพลาระบบจริงก็ยังมีโอกาสแก้ไข

4. สร้างความมั่นใจให้ผู้บริหารและพนักงาน (Assure Stakeholders)

ผู้บริหารจะมั่นใจว่าธุรกิจสามารถดำเนินต่อไปได้แม้เกิดเหตุการณ์ไม่คาดคิด

5. สอดคล้องมาตรฐานและกฎหมาย (Compliance with Standards & Laws)

การทดสอบต้องเป็นไปตาม ISO/IEC 27001:2013, ISO/IEC 22301:2019, PDPA (Personal Data Protection Act, Thailand) และ NIST SP 800-34

อธิบายง่าย ๆ: วัตถุประสงค์ทั้งหมดเหมือนการสร้าง “เครือข่ายความปลอดภัย” (Safety Net) ให้ธุรกิจไม่ว่าจะเกิดเหตุการณ์อะไร ก็ยังสามารถดำเนินงานต่อและปกป้องข้อมูลได้

3. ขอบเขต (Scope)

การทดสอบครอบคลุมระบบ IT สำคัญ (Critical Business Systems) ที่องค์กรต้องใช้ทุกวัน

ระบบ (System)	รายละเอียด (Details)	การทดสอบหลัก (Key Test)	อธิบายเพิ่ม (Explanation)
ฐานข้อมูล (Database)	ข้อมูลลูกค้า, ข้อมูลการขาย, ข้อมูลการเงิน	กู้คืนและตรวจสอบความสมบูรณ์	เปรียบเหมือนสมุดบัญชี หากข้อมูลเสียหายหรือหาย จะทำธุรกรรมไม่ได้
ระบบอีเมล (Email System)	Mailbox ของพนักงาน	Restore Mailbox และส่ง/รับอีเมล	เปรียบเหมือนจดหมายสำคัญที่ต้องส่งต่อให้พนักงาน ถ้าติดต่อไม่ได้ ธุรกิจสะดุด
เซิร์ฟเวอร์ไฟล์ (File Server)	เอกสารสำคัญ, โฟลเดอร์ร่วม	Restore ไฟล์และสิทธิ์การเข้าถึง	เปรียบเหมือนตู้เอกสารรวม ถ้าไฟล์หายจะทำงานไม่ได้
เครื่องเสมือน (Virtual Machine)	ระบบงาน HR, ระบบบัญชี, ระบบ CRM	Restore VM และแอปพลิเคชัน	เปรียบเหมือนคอมพิวเตอร์เสมือนที่รันระบบหลายตัว ถ้าเสีย ต้อง Restore ทุกระบบที่รันบน VM
ระบบเครือข่าย (Network)	Router, Switch, Firewall	ตรวจสอบการเชื่อมต่อ	เปรียบเหมือนถนนและสะพาน ถ้าเสียต้องซ่อมเพื่อให้การสื่อสารกลับมา

เหตุการณ์ล้มระบบที่ครอบคลุม:

- ฮาร์ดแวร์หลักเสีย (Primary Hardware Failure)
- Virtual Machine Crash
- สูญหายบางส่วนของไฟล์ (Partial File Loss)

- การโจมตีทางไซเบอร์ (Cyber Attack เช่น Ransomware)
- ไฟฟ้า น้ำ หรือภัยธรรมชาติ (Power, Water, Natural Disaster)

คำอธิบาย: การทดสอบไม่ใช่แค่เปิดไฟล์ดู แต่ต้องสร้างเหตุการณ์จริงเลียนแบบสถานการณ์ฉุกเฉิน เพื่อฝึกและประเมินความพร้อม

4. ความรับผิดชอบ (Roles and Responsibilities)

ฝ่าย/ตำแหน่ง (Role/Position)	ความรับผิดชอบ (Responsibilities)	อธิบายง่าย ๆ (Plain Explanation)
ผู้บริหาร IT (IT Manager)	กำกับดูแลการทดสอบและรับรองผล	เปรียบเหมือนหัวหน้าทีม ตรวจสอบให้ทุกอย่างเป็นไปตามแผน
ทีมระบบ (System Team)	ดำเนินการทดสอบเข้าถึง Backup และกู้คืนระบบ	เหมือนช่างเทคนิค ทำงานจริง ลอง Restore และเช็คระบบ
ฝ่ายความมั่นคงข้อมูล (Information Security Officer)	ตรวจสอบความถูกต้องและสอดคล้องกับ ISO/IEC 27001	ตรวจสอบว่าไม่มีข้อมูลรั่วไหล และกระบวนการปลอดภัย
ฝ่ายบริหารความต่อเนื่อง (Business Continuity Officer)	ประเมินผลทดสอบและจัดทำรายงานสรุป	วิเคราะห์ว่าเมื่อเกิดเหตุจริง ธุรกิจยังทำงานต่อได้หรือไม่
พนักงานทุกคน (All Staff)	ให้ความร่วมมือและปฏิบัติตามข้อกำหนดระหว่างทดสอบ	เหมือนนักเรียนที่ต้องร่วมซ้อมหนีไฟ ทำตามขั้นตอนอย่างเคร่งครัด

5. ขั้นตอนการทดสอบ (Testing Procedures)

5.1 การทดสอบการเข้าถึงข้อมูลสำรอง (Backup Access Testing)

1. ตรวจสอบสถานที่เก็บข้อมูลสำรอง (Verify Backup Storage Location) – เช่น Offsite, Cloud Storage
2. ตรวจสอบความครบถ้วนของไฟล์สำรอง (Check Backup Completeness) – เปรียบเหมือนนับสมุดบัญชีว่ามีครบทุกเล่ม
3. ทดลองเข้าถึงไฟล์และฐานข้อมูลจาก Backup (Access Test) – เช่น เปิดฐานข้อมูลลูกค้า หรือ ไฟล์เอกสารสำคัญ

4. ตรวจสอบสิทธิ์การเข้าถึง (Verify Access Permission) – ให้แน่ใจว่าคนที่มิลิทธิ์เท่านั้นเข้าถึงได้
5. บันทึกผลการทดสอบ (Record Test Results) – ใช้แบบฟอร์มรายวัน/รายเดือน

ตัวอย่างสถานการณ์:

- ทีม IT เปิดไฟล์สำรองฐานข้อมูลลูกค้า 50,000 รายการ ตรวจสอบ record ล่าสุดครบถ้วน
- ทดสอบไฟล์ mailbox ของพนักงาน 500 คน สามารถ Restore และส่ง/รับอีเมลได้

5.2 การทดสอบขั้นตอนการกู้คืนระบบ (System Recovery Testing)

1. เลือกระบบที่จะทดสอบ (Database, Email, File Server, VM)
2. จำลองเหตุการณ์ล้มระบบ (Simulate Failure Scenario) – เช่น ปิด VM, ลบไฟล์บางส่วน
3. กู้คืนระบบจาก Backup หรือ Snapshot (Restore from Backup/Snapshot)
4. ตรวจสอบการทำงานของระบบหลังการกู้คืน (Verify System Functionality)
5. ตรวจสอบความสมบูรณ์ของข้อมูลและการทำงานของแอปพลิเคชัน (Data Integrity & Application Test)
6. บันทึกผลการทดสอบในรายงาน (Record in Test Report Form)

ตัวอย่างสถานการณ์:

- กู้คืนฐานข้อมูลที่ถูกลบโดยไม่ได้ตั้งใจ 100%
- Restore File Server จาก Backup รายเดือน พบไฟล์เสีย 2 รายการ → ตรวจสอบและซ่อมแซม
- VM ระบบ HR ล่ม กู้คืนจาก snapshot ภายใน 1 ชั่วโมง ระบบพร้อมใช้งาน

6. แบบฟอร์มและเช็คลิสต์ (Forms & Checklists)

6.1 แบบฟอร์มรายวัน (Daily Test Form)

วันที่ (Date)	ระบบ (System)	ขั้นตอนทดสอบ (Test Step)	ผลลัพธ์ (Result)	หมายเหตุ (Notes)
01/09/2025	Database	ตรวจสอบ Backup	ผ่าน 100%	ไม่มี
01/09/2025	Email	Restore Mailbox	ผ่าน 100%	ไม่มี
01/09/2025	File Server	Restore Files	ผ่าน 98%	ไฟล์ 2 รายการ เสีย

6.2 แบบฟอร์มรายเดือน (Monthly Test Form)

เดือน (Month)	ระบบ (System)	การเข้าถึง Backup	กู้คืนระบบ (Recovery)	ปัญหาที่พบ (Issues)	ข้อเสนอแนะ (Recommendations)

		(Backup Access)			
กันยายน 2025	Database	ผ่าน 100%	ผ่าน 100%	ไม่มี	คงมาตรฐาน
กันยายน 2025	Email	ผ่าน 100%	ผ่าน 100%	ไม่มี	เพิ่ม Load Test
กันยายน 2025	File Server	ผ่าน 98%	ผ่าน 100%	ไฟล์เสีย 2 รายการ	ตรวจสอบสาเหตุไฟล์เสีย

6.3 เช็คลิสต์ทดสอบความต่อเนื่อง (Business Continuity Checklist)

- ตรวจสอบ Backup ล่าสุดครบถ้วน (Verify Latest Backup)
- ทดสอบการเข้าถึงไฟล์และฐานข้อมูล (Test Access)
- Restore ระบบจำลอง (Simulate Recovery)
- ตรวจสอบ Application หลัง Restore (Verify Applications)
- บันทึกผลในเอกสาร (Record Results)
- วิเคราะห์ปัญหาและขอเสนอแนะ (Analyze Issues & Recommendations)

7. การตรวจสอบและปรับปรุง (Review & Improvement)

- รายงานผลทดสอบต้องผ่านฝ่ายบริหาร IT และฝ่ายความมั่นคงข้อมูล
- ประเมินความเสี่ยงและปรับปรุงขั้นตอนกู้คืน (Risk Assessment & Procedure Update)
- ทดสอบอย่างน้อยรายไตรมาส (Quarterly Testing)
- บันทึกเหตุการณ์ผิดปกติและปรับปรุงแผน Backup & Recovery

คำอธิบายง่าย ๆ: เหมือนการตรวจสภาพรถขึ้นเครื่องบิน หากพบปัญหาต้องแก้ไขทันที

8. กรณีศึกษาและเหตุการณ์จำลอง (Case Studies & Simulation)

1. ไฟฟ้าขัดข้องที่ศูนย์ข้อมูล (Power Outage at Data Center) – Restore Database จาก Offsite Backup
2. ระบบอีเมลถูกโจมตีด้วย Ransomware (Email Server Ransomware Attack) – Restore Mailbox จาก Snapshot
3. File Server สูญหายบางส่วน (Partial File Server Loss) – Restore โฟลเดอร์สำคัญจาก Backup ล่าสุด
4. VM ล่ม (Virtual Machine Crash) – Restore VM และตรวจสอบ Application Functionality

5. Database Corruption – Restore Point-in-Time จาก Backup และตรวจสอบความสมบูรณ์

9. ข้อสรุป (Conclusion)

การทดสอบการเข้าถึงข้อมูลสำรองและขั้นตอนการกู้คืนระบบเป็นส่วนสำคัญของ **ความต่อเนื่องทางธุรกิจ (Business Continuity)** และการรักษาความมั่นคงของข้อมูล (**Information Security**)

- ข้อมูลสำรองสามารถเข้าถึงและใช้งานได้จริง
- ระบบสามารถกลับมาทำงานได้ตามปกติ (Recovery Time Objective – RTO)
- สอดคล้องมาตรฐาน ISO/IEC 27001, ISO/IEC 22301, NIST SP 800-34 และ PDPA
- พนักงานและผู้เกี่ยวข้องเข้าใจบทบาทและขั้นตอนการทดสอบ
- ลดความเสี่ยงต่อการสูญหายของข้อมูลและความเสียหายทางธุรกิจ

รายงานผลทดสอบการเข้าถึงข้อมูลที่สำรองและขั้นตอนการกู้คืนระบบเบื้องต้น

(Initial Test Report on Backup Data Accessibility and System Recovery Procedures)

1. วัตถุประสงค์ของรายงาน (Objective of the Report)

รายงานฉบับนี้จัดทำขึ้นเพื่อสรุปผลการทดสอบการเข้าถึงข้อมูลที่สำรองไว้ (Backup Data Accessibility Test) และขั้นตอนการกู้คืนระบบ (System Recovery Procedures) โดยมีเป้าหมายเพื่อสร้างความมั่นใจ (Confidence) ว่าองค์กรสามารถดำเนินการกู้คืนระบบ (System Restoration) ได้อย่างมีประสิทธิภาพ และทันเวลาที่ในกรณีที่เกิดเหตุการณ์ไม่คาดคิด (Unexpected Incidents) หรือเหตุการณ์ฉุกเฉิน (Emergency Events)

2. ขอบเขตการทดสอบ (Scope of Testing)

การทดสอบครอบคลุมในระบบงานหลัก (Core Systems) และระบบสนับสนุน (Supporting Systems) ดังนี้

- 1) ฐานข้อมูล (Database Systems)
- 2) อีเมลเซิร์ฟเวอร์ (Email Server)
- 3) ไฟล์เซิร์ฟเวอร์ (File Server)
- 4) เครื่องเสมือน (Virtual Machines – VM)
- 5) ระบบเครือข่ายและระบบจัดเก็บ (Network and Storage Systems)

3. วิธีการทดสอบ (Testing Methodology)

- 1) การจำลองเหตุการณ์ระบบล่ม (System Failure Simulation)
- 2) การกู้คืนข้อมูลจากสื่อสำรอง (Data Restoration from Backup Media)
- 3) การทดสอบการเข้าถึงหลังการกู้คืน (Post-Recovery Accessibility Test)
- 4) การบันทึกเวลาและผลการทดสอบ (Logging Recovery Time and Outcomes)
- 5) การตรวจสอบความถูกต้องของข้อมูล (Data Integrity Verification)

4. ผลการทดสอบ (Test Results)

1) ฐานข้อมูล (Database Recovery)

- สามารถกู้คืนฐานข้อมูลได้สำเร็จภายในเวลา 3 ชั่วโมง
- ข้อมูลล่าสุดสูญหายไม่เกิน 10 นาที

2) อีเมลเซิร์ฟเวอร์ (Email Server Recovery)

- สามารถกู้คืนกล่องจดหมายผู้ใช้งานได้ครบถ้วน
- ไม่มีความเสียหายของไฟล์แนบ

3) ไฟล์เซิร์ฟเวอร์ (File Server Recovery)

- กู้คืนได้ทั้งหมด ยกเว้นไฟล์บางไฟล์ที่ผู้ใช้แก้ไขระหว่างการสำรองข้อมูล

4) เครื่องเสมือน (Virtual Machine Recovery)

- สามารถกู้คืนเครื่องเสมือนทั้งหมด
- ระยะเวลาในการเริ่มต้นใช้งานใหม่เฉลี่ย 20 นาทีต่อเครื่อง

5. ข้อจำกัดของการทดสอบ (Limitations of the Test)

- ขอบเขตการทดสอบจำกัดเฉพาะระบบที่อยู่ในศูนย์ข้อมูลหลัก (Primary Data Center)
- ยังไม่ได้ทดสอบในกรณีที่มีภัยพิบัติรุนแรง (Disaster Scenario) เช่น ไฟไหม้ทั้งศูนย์ข้อมูล
- ความเร็วในการกู้คืนขึ้นอยู่กับประสิทธิภาพของอุปกรณ์จัดเก็บ (Storage Performance)

6. การวิเคราะห์ผลการทดสอบ (Test Result Analysis)

การวิเคราะห์นี้แบ่งออกเป็น 3 ส่วน ได้แก่ **ประสิทธิภาพของการกู้คืน (Recovery Performance)**, **ความถูกต้องของข้อมูล (Data Accuracy)**, และ **ความพร้อมของบุคลากร (Staff Readiness)**

6.1 ประสิทธิภาพของการกู้คืน (Recovery Performance)

- ฐานข้อมูลสามารถกู้คืนได้รวดเร็ว แต่ยังมีปัญหาการสูญหายของข้อมูลเล็กน้อย

- การกู้คืนเครื่องเสมือนใช้เวลาเหมาะสม แต่เมื่อจำนวนเครื่องมากขึ้น ความหน่วงเวลา (Latency) อาจเพิ่มขึ้น

6.2 ความถูกต้องของข้อมูล (Data Accuracy)

- โดยรวมข้อมูลมีความถูกต้อง (Data Integrity) เกินร้อยละ 99
- พบเพียงปัญหาข้อมูลบางไฟล์ที่ถูกเขียนทับระหว่างการสำรอง

6.3 ความพร้อมของบุคลากร (Staff Readiness)

- บุคลากรสามารถปฏิบัติตามขั้นตอนกู้คืนได้อย่างถูกต้อง
- แต่ยังมีความล่าช้าในการตัดสินใจและการประสานงานระหว่างทีม

6.4 สรุปภาพรวม

ผลการทดสอบครั้งนี้แสดงให้เห็นว่าองค์กรมีความพร้อมในระดับที่น่าพอใจ แต่ยังคงต้องปรับปรุง **ความเร็ว** และ **การประสานงาน** เพื่อให้มั่นใจว่าสามารถกู้คืนได้แม้ในสถานการณ์รุนแรง

7. การวิเคราะห์ปัญหาและข้อเสนอปรับปรุง (Problem Analysis and Improvement Suggestions)

7.1 ปัญหาที่พบ (Identified Issues)

- 1) เวลาการกู้คืน (Recovery Time) ยาวนานกว่าที่คาดการณ์ในบางระบบ
- 2) การสูญหายของข้อมูลล่าสุด (Recent Data Loss) แม้จะเล็กน้อยแต่กระทบต่อความเชื่อมั่น
- 3) การประสานงาน (Coordination) ขาดความคล่องตัวระหว่างทีมไอทีและผู้ใช้

7.2 ข้อเสนอปรับปรุง (Improvement Suggestions)

- 1) เพิ่มความถี่ในการสำรองข้อมูล (Increase Backup Frequency) เช่น ใช้ Real-time Replication
- 2) ฝึกซ้อมการกู้คืนระบบ (Conduct Regular Recovery Drills) ทุกไตรมาส
- 3) ใช้เครื่องมืออัตโนมัติ (Leverage Automation Tools) ในขั้นตอนการกู้คืน
- 4) ปรับปรุงคู่มือปฏิบัติ (Update Recovery Manuals) ให้เข้าใจง่ายและครอบคลุมทุกสถานการณ์

8. กรณีศึกษาองค์กรจริง (Real Organization Case Studies)

8.1 กรณีศึกษาธนาคารขนาดใหญ่ (Large Bank Case)

ธนาคารแห่งหนึ่งประสบปัญหา **ระบบฐานข้อมูลหลักล้ม (Core Database Failure)** ทำให้ธุรกรรมออนไลน์หยุดชะงักกว่า 8 ชั่วโมง การกู้คืนใช้เวลานานเนื่องจากไม่มีระบบสำรองแบบ Real-time ผลลัพธ์คือสูญเสียความเชื่อมั่นของลูกค้าอย่างมาก

บทเรียนที่ได้ (Lessons Learned):

- ต้องมี **แผนกู้คืนระบบ (Disaster Recovery Plan – DRP)** ที่สมบูรณ์
- ต้องทดสอบเป็นประจำ ไม่ใช่เพียงทำเอกสารไว้

8.2 กรณีศึกษาบริษัทอีคอมเมิร์ซ (E-commerce Case)

บริษัทไอคอมเมิร์ซแห่งหนึ่งเกิดเหตุ **ไฟล์เซิร์ฟเวอร์เสียหาย (File Server Corruption)** แต่สามารถกู้คืนได้ภายใน 2 ชั่วโมง เพราะมีการทดสอบซ้ำบ่อยครั้งและจัดทำ **คู่มือการกู้คืนแบบขั้นตอน (Step-by-Step Recovery Manual)**

บทเรียนที่ได้ (Lessons Learned):

- การฝึกซ้อมบ่อยครั้งช่วยลดความผิดพลาด
- คู่มือที่เข้าใจง่ายช่วยให้บุคลากรที่ไม่ใช่ผู้เชี่ยวชาญก็สามารถช่วยดำเนินการได้

9. แบบฟอร์มผลการทดสอบ (Test Result Form)

รายการทดสอบ (Test Item)	วันที่ (Date)	ผลลัพธ์ (Result)	เวลาในการกู้คืน (Recovery Time)	หมายเหตุ (Remarks)
ฐานข้อมูล (Database)	1 ส.ค. 2568	สำเร็จ (Success)	3 ชม.	สูญหาย 10 นาที
อีเมล (Email)	2 ส.ค. 2568	สำเร็จ (Success)	2 ชม.	ไม่มีปัญหา
ไฟล์เซิร์ฟเวอร์ (File Server)	3 ส.ค. 2568	สำเร็จบางส่วน (Partial)	3.5 ชม.	สูญหายบางไฟล์
เครื่องเสมือน (VM)	4 ส.ค. 2568	สำเร็จ (Success)	20 นาที/เครื่อง	ใช้งานได้ตามปกติ

10. สรุป (Conclusion)

รายงานฉบับนี้ยืนยันว่าองค์กรมีความพร้อมในระดับที่ดีต่อการกู้คืนระบบ (System Recovery Readiness) อย่างไรก็ตามยังมีพื้นที่ที่ต้องปรับปรุงเพื่อให้มั่นใจว่าในกรณีที่เกิดภัยพิบัติ (Disaster) หรือเหตุการณ์ไม่คาดคิด (Unexpected Events) องค์กรจะสามารถกลับมาดำเนินงานได้อย่าง **ต่อเนื่อง (Continuity)** และ **ปลอดภัย (Security)**

รายงานผลทดสอบการเข้าถึงข้อมูลที่สำคัญและขั้นตอนการกู้คืนระบบ
(Report on Backup Data Accessibility and System Recovery Testing)

1. บทนำ (Introduction)

การปกป้องข้อมูลและระบบงานเป็นหัวใจสำคัญขององค์กรในยุคดิจิทัล ข้อมูลเปรียบเสมือน **เลือดหล่อเลี้ยงธุรกิจ** (Business Bloodstream) หากข้อมูลสูญหายหรือระบบไม่สามารถทำงานได้ ธุรกิจก็เปรียบเสมือนร่างกายที่หยุดทำงาน

รายงานฉบับนี้เป็นผลจากการทดสอบ (Testing) ที่มุ่งเน้น 2 เรื่องหลักคือ:

- 1) **การเข้าถึงข้อมูลที่สำรองไว้ (Backup Data Accessibility)** – เพื่อให้มั่นใจว่าข้อมูลที่เรสำรองไว้นั้นสามารถเปิดใช้งานได้จริง ไม่ใช่เพียงไฟล์ที่เก็บไว้เฉย ๆ
- 2) **การกู้คืนระบบ (System Recovery Process)** – เพื่อทดสอบความสามารถขององค์กรในการฟื้นฟูระบบหลัก (Critical Systems) ให้กลับมาใช้งานได้ตามเวลาที่กำหนด

การทดสอบครั้งนี้จัดทำขึ้นภายใต้นโยบายขององค์กร และอ้างอิงตามมาตรฐานสากล ได้แก่

- ISO/IEC 27001:2013 – Information Security Management (มาตรฐานระบบการจัดการความมั่นคงสารสนเทศ)
- ISO/IEC 22301:2019 – Business Continuity Management (มาตรฐานการจัดการความต่อเนื่องทางธุรกิจ)
- PDPA – Personal Data Protection Act, Thailand (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล)
- NIST SP 800-34 – Contingency Planning Guide for Information Technology Systems (แนวทางการวางแผนสำรองสำหรับระบบสารสนเทศ)

2. วัตถุประสงค์การทดสอบ (Objectives of Testing)

วัตถุประสงค์หลักของการทดสอบแบ่งได้ดังนี้

1) ตรวจสอบความสมบูรณ์ของข้อมูลสำรอง (Backup Data Integrity Check)

เพื่อให้มั่นใจว่าข้อมูลที่สำรองไม่มีการสูญหายหรือเสียหาย (Corruption).

2) ยืนยันความสามารถในการกู้คืนระบบ (System Recovery Readiness Validation)

เพื่อทดสอบว่าระบบสามารถฟื้นตัวได้จริง ไม่เพียงแคในเอกสาร.

3) วัดเวลาและคุณภาพของการกู้คืน (Measure RTO and RPO)

- RTO (Recovery Time Objective) คือเวลาที่ต้องใช้ในการกู้คืนระบบ
- RPO (Recovery Point Objective) คือจุดเวลาของข้อมูลล่าสุดที่สามารถกู้คืนได้

4) สร้างความมั่นใจแก่ผู้มีส่วนได้เสีย (Build Stakeholder Confidence)

ไม่ว่าจะเป็นผู้บริหาร (Management), ลูกค้า (Customers), หรือพันธมิตรธุรกิจ (Partners).

3. ขอบเขตการทดสอบ (Scope of Testing)

การทดสอบนี้ครอบคลุมทั้งระบบสำคัญ (Critical Systems) และระบบสนับสนุน (Supporting Systems) ได้แก่:

- ระบบฐานข้อมูล (Database Systems) – เช่น ข้อมูลลูกค้า, ข้อมูลธุรกรรม
- ระบบอีเมล (Email Systems) – การสื่อสารภายในและภายนอก
- ไฟล์เซิร์ฟเวอร์ (File Server) – เอกสารและไฟล์งานร่วมกัน
- เครื่องเสมือน (Virtual Machines – VM) – ใช้สำหรับแอปพลิเคชันเฉพาะ
- ระบบเครือข่าย (Network Systems) – การเชื่อมโยงระหว่างระบบ
- ระบบจัดเก็บข้อมูล (Storage Systems) – ดิสก์และ SAN (Storage Area Network)

4. วิธีการทดสอบ (Testing Methodology)

การทดสอบดำเนินการโดยอาศัยแนวคิด **Simulation-Based Testing** (การจำลองสถานการณ์) และ **Practical Recovery Testing** (การกู้คืนจริง)

4.1 การจำลองเหตุการณ์ (Scenario Simulation)

- ไฟฟ้าดับ (Power Outage Simulation) – จำลองเหตุการณ์ศูนย์ข้อมูลไม่สามารถทำงานได้
- มัลแวร์/แรนซัมแวร์ (Malware/Ransomware Attack) – ทดสอบความสามารถในการกู้คืนไฟล์ที่ถูกเข้ารหัส
- ฮาร์ดแวร์เสียหาย (Hardware Failure) – เช่น ดิสก์เสีย, เครื่องแม่ข่ายล่ม
- ภัยพิบัติ (Natural Disaster) – น้ำท่วม, ไฟไหม้

4.2 ขั้นตอนการกู้คืน (Recovery Steps)

- 1) เลือกชุดข้อมูลสำรอง (Backup Set)
- 2) ทำการกู้คืน (Restore) ลงบนเครื่องสำรอง
- 3) ตรวจสอบความถูกต้องของไฟล์และฐานข้อมูล
- 4) ทดสอบการเปิดใช้งานระบบ (System Start-up Test)
- 5) บันทึกเวลาและผลลัพธ์

5. ผลการทดสอบ (Test Results)

5.1 ฐานข้อมูล (Database Recovery)

- กู้คืนฐานข้อมูลขนาด 200 GB ได้ครบถ้วน
- ใช้เวลา 3 ชั่วโมง ซึ่งต่ำกว่า RTO ที่กำหนดไว้ 4 ชั่วโมง
- ข้อมูลสูญหายไม่เกิน 10 นาที (ตรงตาม RPO)

5.2 ระบบอีเมล (Email Server Recovery)

- กู้คืนกล่องจดหมายผู้ใช้งาน 500 บัญชีได้ครบถ้วน
- ใช้เวลา 2 ชั่วโมง
- ไม่มีอีเมลสูญหาย

5.3 ไฟล์เซิร์ฟเวอร์ (File Server Recovery)

- กู้คืนไฟล์กว่า 50,000 ไฟล์
- พบว่าไฟล์ที่แก้ไขระหว่างสำรองข้อมูลสูญหายบางส่วน
- ใช้เวลา 3.5 ชั่วโมง

5.4 เครื่องเสมือน (VM Recovery)

- กู้คืน VM ได้ 15 เครื่อง
- แต่ละเครื่องใช้เวลาเฉลี่ย 20 นาที
- หลังการกู้คืนสามารถใช้งานได้ปกติ

6. การวิเคราะห์ผลการทดสอบ (Analysis of Test Results)

6.1 จุดแข็ง (Strengths)

- การสำรองข้อมูลเป็นระบบและตรวจสอบได้
- บุคลากรสามารถปฏิบัติตามขั้นตอนอย่างถูกต้อง

6.2 ข้อบกพร่อง (Weaknesses)

- การสูญหายของไฟล์บางส่วนจาก File Server
- เวลากู้คืนบางระบบเกินกว่าที่ผู้ใช้งานคาดหวัง

6.3 โอกาสปรับปรุง (Opportunities for Improvement)

- ควรเพิ่มการสำรองแบบ Real-time Replication
- ควรฝึกซ้อมทีมงานให้คล่องตัวมากขึ้น

6.4 ความเสี่ยง (Risks)

- หากเกิดภัยพิบัติใหญ่พร้อมกัน อาจต้องใช้เวลามากกว่าที่กำหนด
- ขึ้นอยู่กับความพร้อมของบุคลากรและโครงสร้างพื้นฐาน

7. กรณีศึกษา (Case Studies)

7.1 กรณีธนาคาร (Bank Case)

ระบบฐานข้อมูลล่ม 8 ชั่วโมงเพราะไม่มีการทดสอบแผนกู้คืน ผลคือความเชื่อมั่นของลูกค้าลดลง

7.2 กรณีบริษัทอีคอมเมิร์ซ (E-commerce Case)

กู้คืนไฟล์เซิร์ฟเวอร์ได้ใน 2 ชั่วโมง เพราะมีคู่มือการกู้คืนที่ละเอียด

7.3 กรณีโรงพยาบาล (Hospital Case)

ระบบ HIS (Hospital Information System) ถูกแรนซัมแวร์โจมตี โรงพยาบาลใช้เวลาสองวันในการกู้คืน เพราะไม่มีระบบ DR Site

8. แบบฟอร์มและเช็คลิสต์ (Forms and Checklists)

(เพิ่มรายละเอียดตาราง, แบบฟอร์มทดสอบ, เช็คลิสต์ประจำวัน/เดือน พร้อมคำอธิบาย)

9. การวิเคราะห์ปัญหาและข้อเสนอปรับปรุง (Problems and Recommendations)

- **ปัญหา:** สูญหายของไฟล์ที่แก้ไขระหว่างการสำรอง
ข้อเสนอ: ใช้ Continuous Data Protection (CDP).
- **ปัญหา:** เวลากู้คืนบางระบบยาวนาน
ข้อเสนอ: ลงทุนในระบบ High-Availability และ Snapshot.
- **ปัญหา:** บุคลากรบางส่วนไม่มั่นใจในขั้นตอน
ข้อเสนอ: จัดฝึกอบรมและซ้อมประจำทุกไตรมาส.

10. สรุปผล (Conclusion)

การทดสอบครั้งนี้ทำให้เห็นภาพชัดเจนว่า **องค์กรมีความพร้อมในระดับที่ดี** แต่ยังมีจุดที่ต้องพัฒนาเพื่อเพิ่มความรวดเร็ว ความแม่นยำ และลดความเสี่ยงให้เหลือน้อยที่สุด การดำเนินการปรับปรุงต่อเนื่อง (Continuous Improvement) จึงเป็นสิ่งจำเป็น เพื่อให้องค์กรสามารถรักษาความมั่นคงของข้อมูลและความต่อเนื่องทางธุรกิจได้

รายงานพิจารณาผลทดสอบการเข้าถึงข้อมูลที่สำคัญและขั้นตอนการกู้คืนระบบ

(Review Report on Backup Data Access and System Recovery Testing)

1. บทนำ (Introduction)

รายงานฉบับนี้จัดทำขึ้นเพื่อ **พิจารณาและประเมินผล** (Review and Evaluation) ของการทดสอบการเข้าถึงข้อมูลที่สำคัญ (Backup Data Access Testing) และการทดสอบขั้นตอนการกู้คืนระบบ (System Recovery Testing) ที่ดำเนินการตาม **นโยบายการบริหารจัดการความต่อเนื่องทางธุรกิจ** (Business Continuity Management Policy) และ **นโยบายการรักษาความมั่นคงปลอดภัย**

สารสนเทศ (Information Security Management Policy)

วัตถุประสงค์สำคัญ ได้แก่

1. เพื่อยืนยันว่า **ข้อมูลสำรอง** (Backup Data) สามารถเข้าถึงและใช้งานได้จริงเมื่อเกิดเหตุการณ์ฉุกเฉิน
2. เพื่อทดสอบว่า **ขั้นตอนการกู้คืนระบบ** (System Recovery Procedures) สามารถนำไปปฏิบัติได้ และทำงานตามที่กำหนดไว้
3. เพื่อหาข้อบกพร่อง (Weaknesses) หรือความเสี่ยง (Risks) ที่อาจเกิดขึ้น และจัดทำข้อเสนอเพื่อการปรับปรุง (Recommendations for Improvement)
4. เพื่อให้มั่นใจว่าองค์กรมี **ความพร้อมเชิงปฏิบัติ** (Operational Readiness) ในการรับมือภัยคุกคามทางไซเบอร์ (Cyber Threats) เหตุขัดข้องทางเทคนิค (Technical Failures) และภัยพิบัติทางธรรมชาติ (Natural Disasters)

2. ขอบเขตการพิจารณา (Scope of Review)

การพิจารณาครั้งนี้ครอบคลุม

1. **ระบบฐานข้อมูลหลัก** (Core Database System)
2. **ระบบอีเมล** (Email System)
3. **ระบบแฟ้มเอกสารและไฟล์เซิร์ฟเวอร์** (File Server System)
4. **ระบบเครื่องเสมือน** (Virtual Machine)
5. **ขั้นตอนการกู้คืนระบบในสถานการณ์จริง** (System Recovery Scenarios) เช่น
 - ไฟฟ้าขัดข้อง (Power Outage)
 - เซิร์ฟเวอร์ล่ม (Server Crash)
 - การโจมตีจากมัลแวร์หรือแรนซัมแวร์ (Malware/Ransomware Attack)
 - น้ำท่วมและภัยธรรมชาติ (Flooding and Natural Disaster)

3. กรอบมาตรฐานและกฎหมายที่เกี่ยวข้อง (Applicable Standards and Legal Frameworks)

การทดสอบและการพิจารณาผลในรายงานนี้อ้างอิงตามมาตรฐานสากลและกฎหมายไทย ดังนี้

1. **ISO/IEC 27001:2013 – Information Security Management**
→ การรักษาความมั่นคงปลอดภัยสารสนเทศ
2. **ISO/IEC 22301:2019 – Business Continuity Management**
→ การจัดการความต่อเนื่องทางธุรกิจ
3. **PDPA – พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act, Thailand)**
→ การปกป้องข้อมูลส่วนบุคคลของลูกค้า พนักงาน และคู่ค้า

4. NIST SP 800-34 – Contingency Planning Guide for Information Technology Systems

→ แนวทางวางแผนและดำเนินการด้านความต่อเนื่องของระบบสารสนเทศ

4. วิธีการพิจารณา (Methodology)

1. ตรวจสอบเอกสาร (Document Review)

- แผนกู้คืนระบบ (System Recovery Plan)
- แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan – BCP)
- นโยบายและขั้นตอนการสำรองข้อมูล (Backup Policy and Procedures)

2. การสัมภาษณ์ผู้เกี่ยวข้อง (Interviews with Stakeholders)

- ผู้จัดการฝ่าย IT (IT Manager)
- เจ้าหน้าที่ฝ่ายความมั่นคงปลอดภัยข้อมูล (Information Security Officer)
- ผู้ใช้งานหลัก (Key Users)

3. การทดสอบเชิงปฏิบัติ (Practical Testing)

- การเข้าถึงข้อมูลจากไฟล์สำรอง
- การกู้คืนระบบฐานข้อมูล
- การกู้คืนระบบอีเมล
- การกู้คืนเครื่องเสมือน (VM Recovery)

4. การประเมินผล (Evaluation)

- วัดจากตัวชี้วัด เช่น ระยะเวลาในการกู้คืน (Recovery Time Objective – RTO) และ ปริมาณข้อมูลที่กู้คืนได้ (Recovery Point Objective – RPO)

5. ผลการพิจารณา (Findings and Observations)

ผลการทดสอบพบประเด็นดังนี้

5.1 ความสำเร็จของการกู้คืนข้อมูล (Backup Data Recovery Success)

- สามารถกู้คืนฐานข้อมูลหลักได้ สมบูรณ์ภายใน 2 ชั่วโมง (Fully Restored within 2 Hours)
- ข้อมูลอีเมลสามารถกู้คืนได้ แต่มีบางไฟล์แนบ (Attachments) เสียหาย 3%
- การกู้คืนไฟล์จากไฟล์เซิร์ฟเวอร์ทำได้รวดเร็ว แต่มีปัญหาการจัดโครงสร้างโฟลเดอร์

5.2 ปัญหาที่พบ (Issues Identified)

1. การกู้คืนข้อมูลอีเมลใช้เวลานานกว่าที่กำหนดใน RTO
2. การทดสอบไม่ครอบคลุมผู้ใช้งานปลายทาง (End Users) ทำให้ยังไม่ทราบผลกระทบด้าน ประสิทธิภาพการใช้งานจริง

3. ระบบบันทึก (Logs) ของการกู้คืนข้อมูลไม่สมบูรณ์

5.3 ความสอดคล้องกับมาตรฐาน (Compliance with Standards)

- ISO/IEC 27001: มีการควบคุมด้านการเข้าถึงข้อมูลและความปลอดภัย แต่ยังคงปรับปรุงการบันทึกผลการทดสอบ
- ISO/IEC 22301: การกู้คืนระบบทำได้ภายในเวลาที่กำหนดในบางกรณี แต่ยังไม่ครอบคลุมทุกระบบ
- PDPA: ไม่มีข้อมูลส่วนบุคคลสูญหาย แต่ยังคงปรับปรุงเรื่องการเข้ารหัส (Encryption)
- NIST SP 800-34: การทดสอบมีการวางแผนที่ดี แต่ยังคงขาดการฝึกซ้อมซ้ำอย่างต่อเนื่อง

6. การวิเคราะห์ผลทดสอบ (Analysis of Test Results)

การวิเคราะห์นี้จะพิจารณาใน 3 มิติหลัก คือ **ปัญหา (Problems)**, **ข้อเสนอปรับปรุง (Recommendations)**, และ **กรณีศึกษา (Case Studies)**

6.1 ปัญหา (Problems)

- การกู้คืนอีเมลใช้เวลานานเกินไป → เสี่ยงต่อการหยุดชะงักของการสื่อสาร
- Logs ขาดความครบถ้วน → ทำให้การติดตามการดำเนินงานเป็นไปได้ยาก
- การทดสอบไม่ครอบคลุมผู้ใช้งานปลายทาง → เสี่ยงที่ระบบใช้งานจริงจะยังมีจุดบกพร่อง

6.2 ข้อเสนอปรับปรุง (Recommendations)

1. จัดทำ แบบฝึกซ้อมการกู้คืนระบบรายไตรมาส (Quarterly Recovery Drill)
2. จัดทำ ระบบติดตามผลการกู้คืนแบบอัตโนมัติ (Automated Recovery Monitoring System)
3. ขยายการทดสอบไปยังผู้ใช้งานจริง (End User Testing) เพื่อยืนยันว่าระบบพร้อมใช้งาน

6.3 กรณีศึกษา (Case Studies)

1. กรณีศึกษาในต่างประเทศ – Sony Pictures Hack (2014)

บริษัทสูญเสียข้อมูลครั้งใหญ่เพราะไม่มีแผนกู้คืนระบบที่มีประสิทธิภาพ → ยืนยันความสำคัญของการทดสอบซ้ำ

2. กรณีศึกษาในไทย – โรงพยาบาลถูกโจมตีด้วย Ransomware (2564)

ข้อมูลคนไข้ถูกเข้ารหัสทั้งหมด → โรงพยาบาลที่มีระบบสำรองและการทดสอบกู้คืนระบบสามารถกลับมาเปิดบริการได้ภายใน 3 วัน ในขณะที่บางแห่งใช้เวลาหลายสัปดาห์

7. สรุปผลการพิจารณา (Conclusion)

จากการพิจารณาพบว่า องค์กรมี **ระดับความพร้อมปานกลางถึงสูง (Moderate to High Readiness)** ในการเข้าถึงข้อมูลสำรองและการกู้คืนระบบ โดยสามารถกู้คืนระบบหลักได้ แต่ยังคงต้องปรับปรุงในบางส่วน เช่น การกู้คืนอีเมล การจัดเก็บ Logs และการทดสอบกับผู้ใช้งานปลายทาง

8. ข้อเสนอแนะเชิงกลยุทธ์ (Strategic Recommendations)

1. เพิ่มความถี่ในการทดสอบระบบสำรอง (Increase Frequency of Backup Testing)
2. จัดทำแบบฟอร์มบันทึกผลทดสอบมาตรฐาน (Standard Test Report Form)
3. บูรณาการกับนโยบาย PDPA และ ISO อย่างเคร่งครัด
4. จัดทำ คู่มือสำหรับผู้ใช้งานทั่วไป (End User Recovery Guide)

รายงานพิจารณาผลทดสอบการเข้าถึงข้อมูลที่สำคัญและขั้นตอนการกู้คืนระบบ

(Review Report on Backup Data Access and System Recovery Testing)

1. บทนำ (Introduction)

รายงานฉบับนี้จัดทำขึ้นเพื่อ **พิจารณาและประเมินผล** (Review and Evaluation) ของการทดสอบการเข้าถึงข้อมูลที่สำคัญไว้ (Backup Data Access Testing) และการทดสอบขั้นตอนการกู้คืนระบบ (System Recovery Testing) ที่ดำเนินการตาม **นโยบายการบริหารจัดการความต่อเนื่องทางธุรกิจ** (Business Continuity Management Policy) และ **นโยบายการรักษาความมั่นคงปลอดภัย**

สารสนเทศ (Information Security Management Policy)

วัตถุประสงค์สำคัญ ได้แก่

1. เพื่อยืนยันว่า **ข้อมูลสำรอง** (Backup Data) สามารถเข้าถึงและใช้งานได้จริงเมื่อเกิดเหตุการณ์ฉุกเฉิน
2. เพื่อทดสอบว่า **ขั้นตอนการกู้คืนระบบ** (System Recovery Procedures) สามารถนำไปปฏิบัติได้และทำงานตามที่กำหนดไว้
3. เพื่อหาข้อบกพร่อง (Weaknesses) หรือความเสี่ยง (Risks) ที่อาจเกิดขึ้น และจัดทำข้อเสนอเพื่อการปรับปรุง (Recommendations for Improvement)
4. เพื่อให้มั่นใจว่าองค์กรมี **ความพร้อมเชิงปฏิบัติ** (Operational Readiness) ในการรับมือภัยคุกคามทางไซเบอร์ (Cyber Threats) เหตุขัดข้องทางเทคนิค (Technical Failures) และภัยพิบัติทางธรรมชาติ (Natural Disasters)

2. ขอบเขตการพิจารณา (Scope of Review)

การพิจารณาครั้งนี้ครอบคลุม

1. **ระบบฐานข้อมูลหลัก** (Core Database System)
2. **ระบบอีเมล** (Email System)
3. **ระบบแฟ้มเอกสารและไฟล์เซิร์ฟเวอร์** (File Server System)
4. **ระบบเครื่องเสมือน** (Virtual Machine)
5. **ขั้นตอนการกู้คืนระบบในสถานการณ์จริง** (System Recovery Scenarios) เช่น
 - ไฟฟ้าขัดข้อง (Power Outage)
 - เซิร์ฟเวอร์ล่ม (Server Crash)
 - การโจมตีจากมัลแวร์หรือแรนซัมแวร์ (Malware/Ransomware Attack)
 - น้ำท่วมและภัยธรรมชาติ (Flooding and Natural Disaster)

3. กรอบมาตรฐานและกฎหมายที่เกี่ยวข้อง (Applicable Standards and Legal Frameworks)

การทดสอบและการพิจารณาผลในรายงานนี้อ้างอิงตามมาตรฐานสากลและกฎหมายไทย ดังนี้

1. ISO/IEC 27001:2013 – Information Security Management
→ การรักษาความมั่นคงปลอดภัยสารสนเทศ
2. ISO/IEC 22301:2019 – Business Continuity Management
→ การจัดการความต่อเนื่องทางธุรกิจ
3. PDPA – พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act, Thailand)
→ การปกป้องข้อมูลส่วนบุคคลของลูกค้า พนักงาน และคู่ค้า
4. NIST SP 800-34 – Contingency Planning Guide for Information Technology Systems
→ แนวทางวางแผนและดำเนินการด้านความต่อเนื่องของระบบสารสนเทศ

4. วิธีการพิจารณา (Methodology)

1. ตรวจสอบเอกสาร (Document Review)
 - แผนกู้คืนระบบ (System Recovery Plan)
 - แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan – BCP)
 - นโยบายและขั้นตอนการสำรองข้อมูล (Backup Policy and Procedures)
2. การสัมภาษณ์ผู้เกี่ยวข้อง (Interviews with Stakeholders)
 - ผู้จัดการฝ่าย IT (IT Manager)
 - เจ้าหน้าที่ฝ่ายความมั่นคงปลอดภัยข้อมูล (Information Security Officer)
 - ผู้ใช้งานหลัก (Key Users)
3. การทดสอบเชิงปฏิบัติ (Practical Testing)
 - การเข้าถึงข้อมูลจากไฟล์สำรอง
 - การกู้คืนระบบฐานข้อมูล
 - การกู้คืนระบบอีเมล
 - การกู้คืนเครื่องเสมือน (VM Recovery)
4. การประเมินผล (Evaluation)
 - วัดจากตัวชี้วัด เช่น ระยะเวลาในการกู้คืน (Recovery Time Objective – RTO) และ ปริมาณข้อมูลที่กู้คืนได้ (Recovery Point Objective – RPO)

5. ผลการพิจารณา (Findings and Observations)

ผลการทดสอบพบประเด็นดังนี้

5.1 ความสำเร็จของการกู้คืนข้อมูล (Backup Data Recovery Success)

- สามารถกู้คืนฐานข้อมูลหลักได้ สมบูรณ์ภายใน 2 ชั่วโมง (Fully Restored within 2 Hours)
- ข้อมูลอีเมลสามารถกู้คืนได้ แต่มีบางไฟล์แนบ (Attachments) เสียหาย 3%
- การกู้คืนไฟล์จากไฟล์เซิร์ฟเวอร์ทำได้รวดเร็ว แต่มีปัญหาการจัดโครงสร้างโฟลเดอร์

5.2 ปัญหาที่พบ (Issues Identified)

1. การกู้คืนข้อมูลอีเมลใช้เวลานานกว่าที่กำหนดใน RTO
2. การทดสอบไม่ครอบคลุมผู้ใช้งานปลายทาง (End Users) ทำให้ยังไม่ทราบผลกระทบด้านประสบการณ์การใช้งานจริง
3. ระบบบันทึก (Logs) ของการกู้คืนข้อมูลไม่สมบูรณ์

5.3 ความสอดคล้องกับมาตรฐาน (Compliance with Standards)

- ISO/IEC 27001: มีการควบคุมด้านการเข้าถึงข้อมูลและความปลอดภัย แต่ต้องปรับปรุงการบันทึกผลการทดสอบ
- ISO/IEC 22301: การกู้คืนระบบทำได้ภายในเวลาที่กำหนดในบางกรณี แต่ยังไม่ครอบคลุมทุกระบบ
- PDPA: ไม่มีข้อมูลส่วนบุคคลสูญหาย แต่ต้องปรับปรุงเรื่องการเข้ารหัส (Encryption)
- NIST SP 800-34: การทดสอบมีการวางแผนที่ดี แต่ขาดการฝึกซ้อมซ้ำอย่างต่อเนื่อง

6. การวิเคราะห์ผลทดสอบ (Analysis of Test Results)

การวิเคราะห์นี้จะพิจารณาใน 3 มิติหลัก คือ ปัญหา (Problems), ข้อเสนอปรับปรุง (Recommendations), และกรณีศึกษา (Case Studies)

6.1 ปัญหา (Problems)

- การกู้คืนอีเมลใช้เวลานานเกินไป → เสี่ยงต่อการหยุดชะงักของการสื่อสาร
- Logs ขาดความครบถ้วน → ทำให้การติดตามการดำเนินงานเป็นไปได้ยาก
- การทดสอบไม่ครอบคลุมผู้ใช้งานปลายทาง → เสี่ยงที่ระบบใช้งานจริงจะยังมีจุดบกพร่อง

6.2 ข้อเสนอปรับปรุง (Recommendations)

1. จัดทำ แบบฝึกซ้อมการกู้คืนระบบรายไตรมาส (Quarterly Recovery Drill)
2. จัดทำ ระบบติดตามผลการกู้คืนแบบอัตโนมัติ (Automated Recovery Monitoring System)
3. ขยายการทดสอบไปยังผู้ใช้งานจริง (End User Testing) เพื่อยืนยันว่าระบบพร้อมใช้งาน

6.3 กรณีศึกษา (Case Studies)

1. กรณีศึกษาในต่างประเทศ – Sony Pictures Hack (2014)

บริษัทสูญเสียข้อมูลครั้งใหญ่เพราะไม่มีแผนกู้คืนระบบที่มีประสิทธิภาพ → ยืนยันความสำคัญของการทดสอบซ้ำ

2. กรณีศึกษาในไทย – โรงพยาบาลถูกโจมตีด้วย Ransomware (2564)

ข้อมูลคนไข้ถูกเข้ารหัสทั้งหมด → โรงพยาบาลที่มีระบบสำรองและการทดสอบกู้คืนระบบสามารถกลับมาเปิดบริการได้ภายใน 3 วัน ในขณะที่บางแห่งใช้เวลาหลายสัปดาห์

7. สรุปผลการพิจารณา (Conclusion)

จากการพิจารณาพบว่า องค์กรมี **ระดับความพร้อมปานกลางถึงสูง** (Moderate to High Readiness) ในการเข้าถึงข้อมูลสำรองและการกู้คืนระบบ โดยสามารถกู้คืนระบบหลักได้ แต่ยังคงต้องปรับปรุงในบางส่วน เช่น การกู้คืนอีเมล การจัดเก็บ Logs และการทดสอบกับผู้ใช้งานปลายทาง

8. ข้อเสนอแนะเชิงกลยุทธ์ (Strategic Recommendations)

1. เพิ่มความถี่ในการทดสอบระบบสำรอง (Increase Frequency of Backup Testing)
2. จัดทำแบบฟอร์มบันทึกผลทดสอบมาตรฐาน (Standard Test Report Form)
3. บูรณาการกับนโยบาย PDPA และ ISO อย่างเคร่งครัด

จัดทำ **คู่มือสำหรับผู้ใช้งานทั่วไป** (End User Recovery Guide)

บทที่ 11

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Notification) เป็นหนึ่งในมาตรการสำคัญของการปกป้องข้อมูลส่วนบุคคลตาม PDPA (Personal Data Protection Act) ซึ่งมีวัตถุประสงค์เพื่อให้เจ้าของข้อมูลและหน่วยงานที่เกี่ยวข้องรับทราบถึงเหตุการณ์ที่อาจกระทบต่อความลับ ความสมบูรณ์ และความพร้อมของข้อมูล การแจ้งเหตุละเมิดช่วยให้องค์กรสามารถดำเนินมาตรการแก้ไขและลดผลกระทบได้อย่างทันท่วงที นอกจากนี้ยังเป็นเครื่องมือสำคัญในการสร้างความเชื่อมั่นและความโปร่งใสต่อเจ้าของข้อมูล การจัดทำขั้นตอนและแนวทางการแจ้งเหตุละเมิดข้อมูล (Data Breach Notification Procedure) ควรรวมถึงการระบุประเภทของเหตุละเมิด เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access) การสูญหายของข้อมูล (Data Loss) การรั่วไหลของข้อมูล (Data Leakage) และการแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Modification or Destruction) รวมถึงการประเมินความรุนแรงของเหตุการณ์และผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูล

นอกจากนี้ การแจ้งเหตุละเมิดควรกำหนดผู้รับผิดชอบ หน่วยงานภายในองค์กรที่จะดำเนินการ และระยะเวลาในการแจ้งให้เหมาะสมตามความรุนแรงของเหตุการณ์ และตามข้อกำหนดของ PDPA เพื่อให้การตอบสนองเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ การเก็บบันทึกเหตุละเมิด (Breach Log) รวมถึงหลักฐานการแจ้งและมาตรการแก้ไขที่ดำเนินการไปแล้ว เป็นสิ่งจำเป็นเพื่อใช้เป็นหลักฐานการปฏิบัติตามกฎหมายและเป็นข้อมูลสำหรับการทบทวนและปรับปรุงกระบวนการในอนาคต

โดยสรุป การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไม่เพียงแต่เป็นข้อกำหนดทางกฎหมาย แต่ยังเป็นแนวทางปฏิบัติที่สำคัญในการบริหารความเสี่ยงด้านข้อมูล ช่วยลดผลกระทบต่อเจ้าของข้อมูล เสริมสร้างความเชื่อมั่นในองค์กร และสนับสนุนการจัดการข้อมูลส่วนบุคคลอย่างมีความรับผิดชอบ โปร่งใส และปลอดภัย

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
1. การกำหนดขั้นตอนการแจ้งเหตุละเมิด (Breach Notification Procedure)	จัดทำขั้นตอนและแนวทางชัดเจนสำหรับการตรวจจับและแจ้งเหตุละเมิดข้อมูลส่วนบุคคล รวมถึงการระบุประเภท	เอกสารขั้นตอนการแจ้งเหตุละเมิด (Breach Notification SOP) Flowchart การแจ้งเหตุ Policy การจัดการเหตุละเมิด	มีขั้นตอนชัดเจน ครอบคลุมทุกประเภทเหตุละเมิด และสามารถปฏิบัติได้จริง

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
	ความเสี่ยงและระดับความรุนแรง		
2. การระบุประเภทเหตุละเมิดข้อมูล (Breach Type Identification)	จำแนกประเภทเหตุละเมิด เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การสูญหายของข้อมูล การรั่วไหล การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต	ตารางจำแนกเหตุละเมิด (Breach Classification Table) ตัวอย่างเหตุการณ์ที่ผ่านมา	ครอบคลุมทุกประเภทเหตุละเมิดหลัก มีการอ้างอิงชัดเจน
3. การประเมินความรุนแรงและผลกระทบ (Impact & Severity Assessment)	ประเมินผลกระทบต่อเจ้าของข้อมูลและองค์กร เช่น ผลกระทบต่อความลับ ความสมบูรณ์ ความพร้อม และความเชื่อมั่นของเจ้าของข้อมูล	แบบฟอร์มประเมินผลกระทบ (Impact Assessment Form) รายงานการวิเคราะห์ผลกระทบ	ประเมินครบทุกเหตุการณ์ มีเกณฑ์ชัดเจนและสอดคล้อง PDPA
4. การกำหนดผู้รับผิดชอบและหน่วยงานที่เกี่ยวข้อง (Responsibility Assignment)	ระบุผู้รับผิดชอบแจ้งเหตุละเมิด เช่น DPO ฝ่าย IT ฝ่ายกฎหมาย และหน่วยงานภายนอกที่ต้องแจ้ง	ตารางบทบาทและความรับผิดชอบ (Responsibility Matrix) Org Chart บันทึกมอบหมายงาน	ครอบคลุมทุกบทบาทและความรับผิดชอบ สามารถตรวจสอบการมอบหมายได้
5. การแจ้งเจ้าของข้อมูล (Notification to Data Subjects)	แจ้งเหตุละเมิดต่อเจ้าของข้อมูลโดยเร็วที่สุด รวมถึงข้อมูลเหตุการณ์ผลกระทบ และมาตรการแก้ไข	ตัวอย่างจดหมาย/อีเมลแจ้งเหตุละเมิด Log การส่งแจ้ง Template การแจ้งเหตุ	แจ้งครบถ้วนทันเวลา มีหลักฐานยืนยันการส่งและสามารถตรวจสอบได้

หัวข้อย่อย	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้คะแนน (เต็ม = สอดคล้องครบถ้วน)
6. การแจ้งหน่วยงานกำกับดูแล (Notification to Supervisory Authority)	แจ้งเหตุละเมิดต่อหน่วยงานกำกับดูแลตาม PDPA ภายในระยะเวลาที่กฎหมายกำหนด	รายงานแจ้งเหตุละเมิดต่อหน่วยงานกำกับดูแล Log การส่งรายงาน	แจ้งภายในระยะเวลาที่กำหนด ครบถ้วน และสามารถตรวจสอบย้อนหลังได้
7. การจัดทำบันทึกเหตุละเมิด (Breach Log / Record-Keeping)	จัดเก็บบันทึกเหตุละเมิดทุกกรณี พร้อมรายละเอียดการแจ้งผลกระทบ และมาตรการแก้ไข	Breach Log รายงานเหตุละเมิด Evidence of Mitigation	ครบถ้วน ทุกเหตุการณ์มีการบันทึกและตรวจสอบได้
8. การดำเนินการมาตรการแก้ไขและบรรเทาผลกระทบ (Mitigation & Corrective Action)	ดำเนินการมาตรการแก้ไขเหตุละเมิดและบรรเทาผลกระทบต่อเจ้าของข้อมูล เช่น การเข้ารหัสเพิ่มเติม การปิดช่องโหว่	รายงานมาตรการแก้ไข (Corrective Action Report) Log การดำเนินการ	มีหลักฐานดำเนินการจริง สามารถตรวจสอบและติดตามได้
9. การวิเคราะห์สาเหตุและปรับปรุงกระบวนการ (Root Cause Analysis & Process Improvement)	วิเคราะห์สาเหตุของเหตุละเมิดและปรับปรุงกระบวนการป้องกันไม่ให้เกิดซ้ำ	รายงานวิเคราะห์สาเหตุ (Root Cause Analysis Report) บันทึกปรับปรุง SOP	วิเคราะห์ครบถ้วน และมีหลักฐานปรับปรุงกระบวนการจริง
10. การทบทวนและฝึกซ้อม (Review & Simulation / Training)	ทบทวนประสิทธิภาพการแจ้งเหตุละเมิดและจัดฝึกซ้อมบุคลากรเกี่ยวกับขั้นตอน	บันทึกการทบทวน (Review Minutes) รายงานการฝึกซ้อม (Simulation Report) Attendance Sheet	ทบทวนและฝึกซ้อมสม่ำเสมอ บุคลากรเข้าใจขั้นตอน สามารถปฏิบัติได้จริง

หัวข้อย่อ	สิ่งที่ต้องดำเนินการ	เอกสาร/หลักฐานที่ต้องมี (Documents / Evidence)	เกณฑ์การให้คะแนน (เต็ม = สอดคล้อง ครบถ้วน)
11. การตรวจสอบภายในและประเมินความสอดคล้อง (Internal Audit / Compliance Check)	ตรวจสอบว่าการแจ้งเหตุละเมิดถูกนำไปปฏิบัติจริง และสอดคล้อง PDPA	รายงานตรวจสอบภายใน (Internal Audit Report) Checklist Compliance Evidence of Implementation	ตรวจสอบครบถ้วน พร้อมข้อเสนอแนะและหลักฐานการปฏิบัติจริง

การจัดทำเอกสารตามเกณฑ์

10.1 การตรวจพบ การบริหารจัดการ และการบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Detecting, managing and recording incidents and breaches)
องค์กรมีแนวปฏิบัติเพื่อให้มั่นใจว่าสามารถตรวจพบและจัดการเหตุการณ์ข้อมูลรั่วไหลและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลได้อย่างเหมาะสม

นโยบายการทดสอบการเข้าถึงข้อมูลสำรองและการกู้คืนระบบ (Backup Accessibility and Disaster Recovery Testing Policy)

1. วัตถุประสงค์

เพื่อกำหนดกรอบการดำเนินงานในการทดสอบการเข้าถึงข้อมูลที่สำรองไว้ และขั้นตอนการกู้คืนระบบ เพื่อสร้างความมั่นใจในประสิทธิภาพของแผนการกู้คืนข้อมูลและระบบ ให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่องในกรณีเกิดเหตุฉุกเฉินหรือภัยพิบัติ

2. ขอบเขต

นโยบายนี้ครอบคลุมการทดสอบข้อมูลสำรองทุกประเภทที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ระบบงาน และระบบสารสนเทศขององค์กร รวมถึงกระบวนการกู้คืนระบบหลังเกิดเหตุการณ์ไม่ปกติ

3. แนวทางปฏิบัติ

3.1 การทดสอบการเข้าถึงข้อมูลสำรอง

- ดำเนินการทดสอบการเข้าถึงข้อมูลที่สำรองไว้อย่างน้อยปีละ 2 ครั้ง เพื่อให้แน่ใจว่าข้อมูลสำรองสามารถเข้าถึงและใช้งานได้จริง
- ทดสอบความสมบูรณ์ของข้อมูลสำรอง และตรวจสอบว่าไม่มีความเสียหายหรือข้อมูลสูญหาย

3.2 การทดสอบขั้นตอนการกู้คืนระบบ (Disaster Recovery Testing)

- ทดสอบการกู้คืนระบบตามขั้นตอนที่ระบุในแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบภัยพิบัติ อย่างน้อยปีละ 1 ครั้ง
- ทดสอบการฟื้นฟูระบบงานสำคัญและแอปพลิเคชันหลัก เพื่อให้มั่นใจว่าระบบสามารถกลับมาใช้งานได้ตามมาตรฐานเวลาที่กำหนด (Recovery Time Objective - RTO)

3.3 การจัดทำรายงานและการวิเคราะห์ผลทดสอบ

- จัดทำรายงานผลการทดสอบการเข้าถึงข้อมูลและการกู้คืนระบบในทุกครั้งที่ดำเนินการ
- รายงานต้องระบุปัญหาที่พบ แนวทางแก้ไข และข้อเสนอแนะเพื่อปรับปรุงแผน
- รายงานผลทดสอบจะถูกนำเสนอให้ฝ่ายบริหารพิจารณา และจัดทำเป็นเอกสารประกอบการตรวจสอบภายใน

3.4 การปรับปรุงแผนและมาตรการ

- ปรับปรุงแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบตามผลการทดสอบและบทเรียนที่ได้รับอย่างสม่ำเสมอ
- ฝึกอบรมบุคลากรที่เกี่ยวข้องให้มีความเข้าใจและพร้อมปฏิบัติเมื่อต้องดำเนินการกู้คืนระบบจริง

4. หลักฐานประกอบ

- นโยบายการทดสอบการเข้าถึงข้อมูลที่สำรองไว้ รวมทั้งทดสอบขั้นตอนการกู้คืนระบบ
- รายงานผลทดสอบการเข้าถึงข้อมูลที่สำรองและขั้นตอนการกู้คืนระบบเบื้องต้น
- รายงานผลทดสอบการเข้าถึงข้อมูลที่สำรองและขั้นตอนการกู้คืนระบบฉบับเต็ม
- รายงานพิจารณาผลทดสอบการเข้าถึงข้อมูลที่สำรองและขั้นตอนการกู้คืนระบบ

5. กฎหมายและข้อบังคับที่เกี่ยวข้อง

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3) (4)

6. บทลงโทษ

การไม่ปฏิบัติตามนโยบายนี้ถือเป็นการละเมิดกฎหมายตามมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีโทษปรับทางปกครองไม่เกิน 3 ล้านบาท รวมถึงบทลงโทษทางวินัยจากองค์กร

เช็คลิสต์การทดสอบการเข้าถึงข้อมูลสำรองและกู้คืนระบบ (9.12.4)

ลำดับ	รายการตรวจสอบ	สถานะ (✓ / ✗)	หมายเหตุ/ รายละเอียด
1	มีการจัดทำแผนทดสอบการเข้าถึงข้อมูลสำรองและกู้คืนระบบ		
2	ดำเนินการทดสอบการเข้าถึงข้อมูลสำรองอย่างน้อยปีละ 2 ครั้ง		วันที่ทดสอบ:
3	ดำเนินการทดสอบขั้นตอนการกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง		วันที่ทดสอบ:
4	ตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลสำรอง		
5	รายงานผลการทดสอบจัดทำครบถ้วนและได้รับการอนุมัติ		วันที่รายงาน:
6	มีการวิเคราะห์ผลทดสอบและแนวทางแก้ไขข้อผิดพลาด		
7	ปรับปรุงแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบตามผลทดสอบ		
8	ฝึกอบรมบุคลากรที่เกี่ยวข้องเกี่ยวกับขั้นตอนการกู้คืนระบบ		วันที่ฝึกอบรม:
9	มีเอกสารนโยบายและรายงานการทดสอบครบถ้วนและเก็บรักษาไว้		

10.1.1 มีการอบรมและสร้างความตระหนักรู้เพื่อให้พนักงานสามารถรับรู้และแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่พบ สิ่งที่ต้องทำ: มีการอบรมและสร้างความตระหนักรู้เพื่อให้พนักงานสามารถรับรู้และแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่พบ และมีการทดสอบความเข้าใจ

หลักฐาน: นโยบายการฝึกอบรมบุคลากรที่มีการเข้าถึงข้อมูลส่วนบุคคล นโยบายการคัดเลือก DPO ที่ต้องศึกษาทางกฎหมาย หรือการฝึกอบรมที่ผ่านการรับรองด้านเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล นโยบายกำหนดหน้าที่แก่ DPO ในการจัดให้มีการอบรมและสร้างความตระหนักรู้แก่พนักงาน เรื่องที่เกี่ยวกับ “ความสามารถรับรู้และแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล” นโยบายการทดสอบความเข้าใจของ DPO และพนักงาน หลังจากที่ได้รับการอบรม ข้อสอบวัดความเข้าใจเรื่องที่ได้รับการอบรม

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (7)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ส่วนที่ 1: นโยบายการฝึกอบรมและสร้างความตระหนักรู้แก่พนักงาน

ชื่อเอกสาร

นโยบายการฝึกอบรมบุคลากรด้านการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 256X

วัตถุประสงค์

เพื่อกำหนดแนวทางการพัฒนาและเสริมสร้างความรู้ ความเข้าใจ และความตระหนักรู้แก่พนักงาน เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล เพื่อ ป้องกันและลดความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล

ขอบเขต

ครอบคลุมพนักงาน ลูกจ้าง พนักงานสัญญาจ้าง รวมถึงบุคคลภายนอกที่มีสิทธิ์เข้าถึงข้อมูลส่วนบุคคลในระบบขององค์กร

นโยบายหลัก

- องค์กรจะจัดให้มีการอบรมอย่างน้อยปีละ 1 ครั้งเกี่ยวกับ
 1. ความรู้ทั่วไปเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
 2. ความเสี่ยงและมาตรการด้านความมั่นคงปลอดภัย
 3. วิธีการสังเกตและรายงานเหตุการณ์ละเมิดข้อมูล (Data Breach Awareness)
- พนักงานใหม่ต้องเข้ารับการอบรมก่อนเริ่มปฏิบัติงานหรือภายใน 30 วันหลังเริ่มงาน
- ต้องมีแบบทดสอบวัดผลหลังการอบรมและเก็บประวัติการเข้าร่วมการอบรมไว้เป็นหลักฐาน
- DPO รับผิดชอบกำกับดูแลเนื้อหาและคุณภาพของหลักสูตร

หน่วยงานรับผิดชอบ: ฝ่ายทรัพยากรบุคคล ร่วมกับ DPO

ส่วนที่ 2: แนวทางการคัดเลือกและพัฒนาเจ้าหน้าที่ DPO

ชื่อเอกสาร

แนวปฏิบัติในการแต่งตั้งและพัฒนาเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

สาระสำคัญ

- DPO ต้องมีความรู้และความเข้าใจด้านกฎหมาย PDPA และเทคโนโลยีด้านความมั่นคงปลอดภัย
- ต้องได้รับการอบรมหรือถือใบรับรองจากสถาบันที่เชื่อถือได้ (เช่น PDPA Practitioner ISO/IEC 27001 Awareness)
- ต้องจัดให้มีแผนฝึกอบรมประจำปี และรายงานผลการอบรมให้ผู้บริหารทราบ

ภารกิจของ DPO

- จัดการอบรม/สัมมนาให้พนักงาน
- ตรวจสอบและประเมินความเข้าใจของบุคลากรต่อความเสี่ยงด้านข้อมูล

ส่วนที่ 3: รายงานผลการอบรมประจำปี (ตัวอย่าง)

ชื่อหลักสูตร

"รู้รับ รู้แจ้ง แจ้งเหตุข้อมูลรั่วไหลและ PDPA สำหรับองค์กร"

วันที่จัดอบรม: 10 มกราคม 256X

กลุ่มเป้าหมาย: พนักงานที่ประมวลผลข้อมูลส่วนบุคคล (ประมาณ 150 คน)

เนื้อหาหลัก

- บทนำ PDPA และข้อมูลส่วนบุคคล
- ประเภทของเหตุการณ์ข้อมูลรั่วไหล
- ขั้นตอนการแจ้งเหตุภายในองค์กร (Flowchart)
- ช่องทางการแจ้งเหตุ (ระบบแจ้งเหตุภายใน / DPO Hotline)
- กรณีศึกษาและกิจกรรมกลุ่ม

ผลการประเมิน

- คะแนนเฉลี่ยแบบทดสอบหลังการอบรม: 85%
- ผู้ผ่านเกณฑ์ (70% ขึ้นไป): 139 คน (92.7%)

แนบ: รายชื่อผู้เข้าร่วม / แบบทดสอบก่อน-หลัง / สไลด์ประกอบการอบรม

ส่วนที่ 4: แบบทดสอบความเข้าใจหลังอบรม

ชื่อเอกสาร

แบบทดสอบความเข้าใจเรื่องการรายงานเหตุการณ์ข้อมูลรั่วไหล (Data Breach Awareness Quiz)

จำนวนข้อ: 10 ข้อแบบปรนัย + 1 ข้อแบบอัตนัย

ตัวอย่างคำถาม

ข้อ 1: ข้อใดต่อไปนี้เป็นภาระละเมิดข้อมูลส่วนบุคคล? ก. ลืมรหัสผ่านเข้าใช้งานระบบ ข. ส่งไฟล์ข้อมูลลูกค้าผิดแผนกโดยไม่ได้เข้ารหัส ค. การใช้ VPN เพื่อเข้าระบบ ง. พนักงานลางานโดยไม่แจ้งล่วงหน้า

เฉลย: ข

ข้อ 6: หากพบเหตุการณ์ต้องสงสัยว่าเป็นข้อมูลรั่วไหลควรทำอะไร? ก. ปิดระบบทันที ข. แจ้งหัวหน้าและ DPO ภายใน 24 ชม. ค. ส่งอีเมลถึงลูกค้าอัตโนมัติ ง. เก็บข้อมูลไว้ดูเองก่อน

เฉลย: ข

เกณฑ์ผ่าน: 70% ขึ้นไป (ตอบถูกอย่างน้อย 8 ข้อจาก 11)

ส่วนที่ 5: φόρμบบันทึกรการแจ้งเหตุข้อมูลรั่วไหล (Internal Data Breach Reporting Form)

วันที่พบเหตุการณ์:

ผู้แจ้ง:

หน่วยงาน:

ลักษณะเหตุการณ์:

ประเภทข้อมูลที่ได้รับผลกระทบ:

แนวทางที่ดำเนินการเบื้องต้น:

วันที่/เวลาที่แจ้ง DPO:

ผู้รับเรื่อง:

หมายเหตุ: แบบฟอร์มนี้ DPO ต้องเก็บรวบรวมไว้เป็นเวลาอย่างน้อย 3 ปี

10.1.2 ทีมหรือบุคลากรที่กำหนดไว้มีการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

สิ่งที่ต้องทำ: มีการกำหนดทีมหรือบุคลากรสำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น และมีแผนการอบรมและแผนการตรวจสอบการจัดการของทั้งสองด้านดังกล่าวเป็นการเฉพาะ

หลักฐาน: นโยบายภายในการจัดตั้งทีมหรือบุคลากรที่ทำหน้าที่บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

นโยบายควบคุมการปฏิบัติหน้าที่ของทีมหรือบุคลากรที่ทำหน้าที่บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

แผนการอบรมด้านจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

แผนการอบรมการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมายอื่นที่เกี่ยวข้อง

แผนการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลภายในองค์กร

แผนการตรวจสอบการปฏิบัติตามนโยบายการจัดการข้อมูลส่วนบุคคล

แผนการประสานงานกับหน่วยงานผู้กำกับดูแล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3)

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณืละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง ไม่เกิน 3 ล้านบาท

หัวข้อ: ทีมหรือบุคลากรที่กำหนดไว้มีการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

1. นโยบายภายในการจัดตั้งทีมบริหารจัดการเหตุการณ์

ชื่อเอกสาร

นโยบายการจัดตั้งทีมบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยและการละเมิดข้อมูลส่วนบุคคล (Incident Response and Data Breach Team Policy)

สาระสำคัญ

(1) องค์กรแต่งตั้ง "ทีมบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและการละเมิดข้อมูลส่วนบุคคล" (Incident Response Team – IRT) เพื่อรับผิดชอบต่อการรับมือเหตุการณ์ที่เกี่ยวข้องกับระบบข้อมูลและข้อมูลส่วนบุคคลที่อาจรั่วไหลหรือถูกละเมิด

(2) ทีม IRT ประกอบด้วยบุคลากรจากหลากหลายหน่วยงาน ได้แก่

- หัวหน้าทีม (CISO หรือหัวหน้าฝ่าย IT)
- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- ตัวแทนฝ่ายกฎหมาย
- ตัวแทนฝ่าย HR (สำหรับประเด็นบุคลากรภายใน)
- ตัวแทนฝ่ายประชาสัมพันธ์ (หากมีการสื่อสารภายนอก)

o (3) หน้าที่ของทีม IRT ได้แก่

- ประเมินสถานการณ์และผลกระทบจากเหตุการณ์
- จัดทำแผนตอบสนองต่อเหตุการณ์
- ประสานกับหน่วยงานผู้กำกับดูแลและผู้มีส่วนได้เสีย
- จัดเก็บหลักฐานและรายงานเหตุการณ์อย่างเป็นทางการ

2. นโยบายควบคุมการปฏิบัติหน้าที่ของทีม IRT

ชื่อเอกสาร

ข้อกำหนดและแนวทางการปฏิบัติงานของทีมบริหารจัดการเหตุการณ์ข้อมูล

แนวทาง

(1) ทีม IRT ต้องสามารถเริ่มปฏิบัติการได้ภายใน 4 ชั่วโมงหลังพบเหตุการณ์ที่มีผลต่อความมั่นคงปลอดภัยหรือข้อมูลส่วนบุคคล

(2) ต้องมีการจัดเวรผู้รับผิดชอบแบบ 24/7 พร้อมข้อมูลติดต่อ

(3) การดำเนินการของทีมต้องสอดคล้องกับคู่มือ Incident Response Plan ขององค์กร

(4) หลังเหตุการณ์แต่ละครั้ง ทีมต้องจัดทำรายงาน Post-Incident Review และวิเคราะห์ช่องโหว่ เพื่อปรับปรุงมาตรการควบคุม

3. แผนการอบรมด้านการจัดการเหตุการณ์ (Security Incident Response Training Plan)

ชื่อเอกสาร

แผนการพัฒนาศักยภาพบุคลากรด้านการจัดการเหตุการณ์ความมั่นคงปลอดภัยและข้อมูลส่วนบุคคล พ.ศ. 256X

เป้าหมาย

- พัฒนาให้บุคลากรมีทักษะในการ
- รับมือเหตุการณ์ทางไซเบอร์
- ประเมินความรุนแรงของเหตุการณ์
- ดำเนินการตอบสนองและกู้คืนข้อมูล
- สื่อสารกับหน่วยงานที่เกี่ยวข้องได้อย่างถูกต้อง

ตารางฝึกอบรมประจำปี

เดือน	ชื่อหลักสูตร	กลุ่มเป้าหมาย	หน่วยงานจัด
กุมภาพันธ์	Cyber Incident Simulation	ทีม IRT	DPO + IT
พฤษภาคม	Forensics and Chain of Custody	ทีม IRT และกฎหมาย	External Trainer
กันยายน	Tabletop Exercise: Data Breach	ทุกหน่วยงาน	IT/DPO

4. แผนการอบรมการปฏิบัติตาม PDPA

ชื่อเอกสาร

แผนฝึกอบรม PDPA เฉพาะทางสำหรับทีมตอบสนองเหตุการณ์ พ.ศ. 256X

หัวข้อที่อบรม

- การจำแนกข้อมูลส่วนบุคคลและข้อมูลอ่อนไหว
- การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลและ กพท.

- การจัดทำบันทึกการประมวลผลข้อมูล (RoPA) ในสถานการณ์วิกฤติ
- การแจ้งเหตุภายใน 72 ชั่วโมงตามมาตรา 37 แห่ง PDPA

รอบอบรม: ไตรมาสละ 1 ครั้ง และเมื่อมีการปรับปรุงกฎหมาย

5. แผนการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลภายในองค์กร

ชื่อเอกสาร

แผนการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลประจำปี พ.ศ. 256X

วัตถุประสงค์

- ตรวจสอบความสอดคล้องของการประมวลผลข้อมูลกับ PDPA
- ประเมินความเหมาะสมของมาตรการป้องกันข้อมูล
- ปรับปรุงรายการข้อมูล RoPA และบันทึก Data Flow

แนวทางการดำเนินการ

- ทีม DPO จะจัดตรวจสอบภายในร่วมกับ IT และหน่วยงานเจ้าของข้อมูล
- ประเมินจากแบบฟอร์ม “Data Processing Audit Checklist”
- จัดลำดับความเสี่ยง (High – Medium – Low) และจัดทำแผนแก้ไข

ความถี่: อย่างน้อยปีละ 1 ครั้ง หรือหลังจากเกิดเหตุการณ์ละเมิดข้อมูลสำคัญ

6. แผนการตรวจสอบการปฏิบัติตามนโยบายการจัดการข้อมูลส่วนบุคคล

ชื่อเอกสาร

แผนการตรวจประเมินความสอดคล้องกับนโยบายข้อมูลส่วนบุคคล

แนวทาง

- DPO จัดทำตารางการตรวจประเมินร่วมกับฝ่ายตรวจสอบภายใน
- ตรวจเอกสารและขั้นตอนการให้ความยินยอม การเก็บ ใช้ เปิดเผย และลบข้อมูล
- สุ่มตรวจระบบที่มีการเก็บข้อมูล เช่น CRM HRMS ระบบสมัครเรียนออนไลน์ ฯลฯ

รูปแบบ

- ตรวจเชิงเอกสาร (Document Review)
- ตรวจภาคสนาม (On-site Interview)
- ทดสอบความปลอดภัยของระบบ (Vulnerability Assessment)

7. แผนการประสานงานกับหน่วยงานผู้กำกับดูแล

ชื่อเอกสาร

แนวทางการประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) และหน่วยงานอื่น

ขั้นตอนหลัก

- แต่งตั้ง DPO เป็นผู้ติดต่อประสานงานโดยตรงกับ PDPC
- จัดทำรายงานแจ้งเหตุละเมิดข้อมูลในรูปแบบที่ PDPC กำหนด
- ประสานและให้ความร่วมมือในการตรวจสอบภายหลังเหตุการณ์
- จัดการประชุมหรือส่งรายงานประจำปีเกี่ยวกับมาตรการคุ้มครองข้อมูลส่วนบุคคล
- หากองค์กรอยู่ภายใต้กฎหมายอื่น (เช่น ธปท. ก.ล.ต. กสทช.) ต้องประสานหน่วยงานเหล่านั้นตามคู่มือการแจ้งเหตุเฉพาะอุตสาหกรรม

10.1.3 พนักงานมีการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ทีมหรือบุคลากรดังกล่าวเพื่อดำเนินการตรวจสอบเหตุที่เกิดขึ้นนั้นว่าเข้าเงื่อนไขเป็น "เหตุการณ์ละเมิดข้อมูลส่วนบุคคล" หรือไม่

สิ่งที่ต้องทำ: มีแผนกำหนดให้พนักงานมีการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ทีมหรือบุคลากรดังกล่าวเพื่อดำเนินการตรวจสอบเหตุที่เกิดขึ้นนั้นว่าเข้าเงื่อนไขเป็น "เหตุการณ์ละเมิดข้อมูลส่วนบุคคล" หรือไม่ และมีเอกสารรายงานของเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

หลักฐาน: นโยบายแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
แบบแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
หนังสือรับรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
รายงานเบื้องต้นของเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
รายงานของเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

รายละเอียดช่องทางการติดต่อรายละเอียดการติดต่อทีมหรือบุคลากรที่ทำหน้าที่บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

1 นโยบายแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

1.1 วัตถุประสงค์

เพื่อกำหนดแนวทางในการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลโดยพนักงานต่อทีมหรือบุคลากรที่มีหน้าที่บริหารจัดการ เพื่อประเมินว่าเหตุการณ์นั้นเข้าเงื่อนไขเป็น "เหตุการณ์ละเมิดข้อมูลส่วนบุคคล" ตามกฎหมายหรือไม่

1.2 ขอบเขตการบังคับใช้

นโยบายนี้ใช้กับพนักงานทุกคนขององค์กร ไม่ว่าจะเป็นพนักงานประจำ พนักงานชั่วคราว หรือพนักงานจ้างเหมาบริการ

1.3 นิยาม

(1) เหตุการณ์ด้านความมั่นคงปลอดภัย: เหตุการณ์ที่กระทบต่อความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลในระบบสารสนเทศ

(2) เหตุการณ์ละเมิดข้อมูลส่วนบุคคล: เหตุการณ์ที่มีการเข้าถึง ใช้ เผยแพร่ แก้ไข หรือลบข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ไม่ชอบด้วยกฎหมาย หรือโดยมิชอบ

1.4 แนวทางปฏิบัติ

(1) พนักงานผู้พบเหตุการณ์ต้องแจ้งรายละเอียดเบื้องต้นผ่านแบบฟอร์มแจ้งเหตุ (ข้อ 2) ภายใน 24 ชั่วโมง นับแต่ทราบเหตุการณ์

(2) พนักงานต้องส่งแบบฟอร์มไปยังอีเมล incident@องค์กรของคุณ หรือช่องทางที่กำหนดไว้

(3) ทีมหรือบุคลากรที่รับผิดชอบจะประเมินและวิเคราะห์เบื้องต้นว่าเข้าเงื่อนไขเป็นเหตุการณ์ละเมิดข้อมูลส่วนบุคคลหรือไม่

(4) หากเป็นเหตุการณ์ที่เข้าข่ายละเมิดข้อมูลส่วนบุคคล ให้ดำเนินการตามข้อกำหนดในประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลฯ

2 แบบแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ชื่อ-นามสกุลผู้แจ้ง:

ตำแหน่ง:

หน่วยงาน:

วันที่แจ้งเหตุการณ์:

ช่องทางที่ใช้แจ้ง:

รายละเอียดของเหตุการณ์:

.....

ข้อมูลที่สามารถได้รับผลกระทบ

(1) ประเภทข้อมูล:

(2) จำนวนรายการ:

(3) ผู้ได้รับผลกระทบโดยประมาณ:

มาตรการเบื้องต้นที่ดำเนินการ:

.....

เอกสารแนบ (ถ้ามี):

3 หนังสือรับการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

หนังสือรับแจ้งเหตุการณ์เลขที่: INCIDENT-XXXX/256X

องค์กรขอรับทราบเหตุการณ์ที่ได้รับการแจ้งจาก

ชื่อผู้แจ้ง:

ตำแหน่ง:

เกี่ยวกับเหตุการณ์ที่เกิดขึ้นเมื่อวันที่

ซึ่งอาจเป็นเหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

องค์กรจะดำเนินการตรวจสอบข้อเท็จจริงโดยเร็ว และจะรายงานผลเบื้องต้นให้ทราบภายใน 7 วันทำการ นับแต่วันที่ได้รับแจ้ง

ลงชื่อ.....

(ชื่อ-นามสกุล ผู้มีอำนาจ)

ตำแหน่ง.....

วันที่.....

4 รายงานเบื้องต้นของเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ชื่อเหตุการณ์:

วันที่เกิดเหตุ:

วันที่ตรวจพบ:

หน่วยงานที่ได้รับผลกระทบ:

ประเภทข้อมูลที่เกี่ยวข้อง:

ความร้ายแรงของผลกระทบ: (ต่ำ / ปานกลาง / สูง)

สรุปสถานการณ์เบื้องต้น

.....

มาตรการเบื้องต้นที่ดำเนินการแล้ว

.....

สรุปผลการประเมินเบื้องต้น

☐ ไม่เข้าข่ายเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

☐ เข้าข่ายเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (ให้ดำเนินการแจ้งตามกฎหมาย)

ผู้ประเมิน:

ตำแหน่ง:

ลงชื่อ:

5 รายงานของเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (ฉบับสมบูรณ์)

สรุปเหตุการณ์

.....

สาเหตุของเหตุการณ์:

.....

ข้อมูลที่ได้รับผลกระทบ:

(1) ประเภทข้อมูล:

(2) จำนวนรายการ:

(3) กลุ่มผู้ได้รับผลกระทบ:

มาตรการที่องค์กรดำเนินการแล้ว:

(1) มาตรการด้านเทคนิค:

(2) มาตรการด้านการบริหาร:

(3) การแจ้งผู้ควบคุมข้อมูลส่วนบุคคล:

ข้อเสนอแนะเพื่อป้องกันเหตุซ้ำ:

.....

ผู้จัดทำรายงาน:

ชื่อ-ตำแหน่ง:

วันที่จัดทำ:

6 หนังสือรายละเอียดช่องทางการติดต่อของทีมหรือบุคลากรที่ทำหน้าที่บริหารจัดการเหตุการณ์ หน่วยจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและละเมิดข้อมูลส่วนบุคคล

ชื่อทีม: Incident Response and Privacy Breach Management Team

หัวหน้าทีม:

ตำแหน่ง:

อีเมล: incident@องค์กรของคุณ

โทรศัพท์: 0-2XXX-XXXX ต่อ XXXX

ช่องทางสำรอง: แบบฟอร์มบนเว็บไซต์ภายใน / LINE Official / Intranet

ผู้ได้รับมอบหมายสามารถติดต่อได้ตลอด 24 ชั่วโมงในกรณีเหตุการณ์ร้ายแรงหรือเร่งด่วน

ลงชื่อ.....

(ชื่อ-นามสกุล ผู้บริหารสูงสุดของหน่วยงาน)

ตำแหน่ง.....

วันที่.....

10.1.4 องค์กรมีแผนรับมือต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: องค์กรมีแผนรับมือต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล มีขั้นตอนบริหารจัดการ และมีรายงานสรุปผลการดำเนินการ

หลักฐาน: แผนรับมือต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
ขั้นตอนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

รายงานสรุปผลการดำเนินการรับมือด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) (3)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้ง
เหตุการณั้ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 5 (5)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง
ไม่เกิน 3 ล้านบาท

1 แผนรับมือต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

องค์กรได้จัดทำแผนรับมือต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
เพื่อเป็นแนวทางการดำเนินการเมื่อเกิดเหตุการณ์ขึ้นจริง โดยครอบคลุมเนื้อหาหลัก ดังนี้:

- (1) การระบุประเภทของเหตุการณ์ที่อาจเกิดขึ้น
- (2) การประเมินผลกระทบที่อาจเกิดกับเจ้าของข้อมูลส่วนบุคคล
- (3) การกำหนดบทบาทหน้าที่ของหน่วยงานหรือบุคลากรที่รับผิดชอบ
- (4) การกำหนดช่องทางและวิธีการแจ้งเหตุ
- (5) การกำหนดขั้นตอนการตอบสนองและฟื้นฟูระบบ
- (6) การประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง

2 ขั้นตอนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ขั้นตอนบริหารจัดการเหตุการณ์ที่กำหนดไว้ ประกอบด้วย

- (1) การรับแจ้งเหตุจากพนักงานหรือผู้เกี่ยวข้องผ่านแบบฟอร์มหรือช่องทางที่องค์กรกำหนด
- (2) การตรวจสอบและประเมินลักษณะของเหตุการณ์โดยทีมจัดการเหตุการณ์
- (3) การตัดสินใจว่าเข้าเงื่อนไขเป็นการละเมิดข้อมูลส่วนบุคคลหรือไม่
- (4) การดำเนินการมาตรการควบคุมความเสียหายและลดผลกระทบ
- (5) การจัดทำรายงานเหตุการณ์พร้อมข้อเสนอแนะการป้องกันในอนาคต
- (6) การแจ้งเหตุการณ์ให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามข้อกำหนดทางกฎหมาย

3 รายงานสรุปผลการดำเนินการรับมือด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ชื่อเหตุการณ์: การเข้าถึงระบบฐานข้อมูลโดยไม่ได้รับอนุญาต

วันที่เกิดเหตุ: 5 พฤษภาคม 2568

สรุปเหตุการณ์: ระบบฐานข้อมูลกลางขององค์กรถูกรายงานว่ามีการเข้าถึงจาก IP ภายนอกที่ไม่อยู่ใน
whitelist ของระบบ

การดำเนินการ: ทีมจัดการเหตุการณ์ได้ทำการตัดการเชื่อมต่อทันที ตรวจสอบ log ของระบบ พบว่าไม่มี
ข้อมูลส่วนบุคคลรั่วไหลออกนอกระบบ แต่พบจุดอ่อนในระบบการยืนยันตัวตน 2 ขั้นตอน

ผลการแก้ไข: ได้ปรับปรุงระบบยืนยันตัวตนโดยใช้ OTP และจัดอบรมเจ้าหน้าที่ด้านการรักษาความมั่นคงของระบบ

ข้อเสนอแนะ: ควรจัดทำทดสอบการเจาะระบบ (penetration test) อย่างน้อยปีละ 1 ครั้ง

10.1.5 แบบการบันทึกเหตุข้างต้นมีรายการข้อมูลอย่างน้อยดังต่อไปนี้

สิ่งที่ต้องทำ: มีแบบการบันทึกเหตุการณ์ละเมิดข้อมูล โดยมีรายการข้อมูลอย่างน้อยดังต่อไปนี้

- (1) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล
- (2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม
- (3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- (4) ข้อมูลเกี่ยวกับมาตรการที่องค์กรใช้หรือจะใช้เพื่อป้องกัน ระบุ หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย

หลักฐาน: นโยบายภายในการจัดให้มีระบบรวมศูนย์ในการบันทึกข้อมูลเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล บันทึกล็อก (Log) แจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัย
ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้ง
เหตุการณั้ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครอง
ไม่เกิน 3 ล้านบาท

1. นโยบายภายในการจัดให้มีระบบรวมศูนย์ในการบันทึกข้อมูลเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

นโยบายการบันทึกเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและเหตุการณ์ด้านความมั่นคงปลอดภัย

องค์กรได้จัดตั้งระบบรวมศูนย์สำหรับการรายงานและบันทึกเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและเหตุการณ์ด้านความมั่นคงปลอดภัย โดยมีวัตถุประสงค์เพื่อ

- (1) จัดเก็บข้อมูลเหตุการณ์ให้เป็นระบบ
- (2) ตรวจสอบเหตุการณ์ที่เกิดขึ้นโดยทีมงานที่ได้รับมอบหมาย
- (3) รายงานต่อหน่วยงานที่เกี่ยวข้องตามที่กฎหมายกำหนด

บันทึกข้อมูลจะต้องครอบคลุมถึงรายละเอียดของเหตุการณ์ ชื่อและข้อมูลติดต่อของผู้ประสานงาน (DPO) ผลกระทบที่อาจเกิดขึ้น และมาตรการที่ดำเนินการเพื่อระงับหรือเยียวยาความเสียหาย เจ้าหน้าที่ทุกคนมีหน้าที่ต้องรายงานเหตุการณ์ที่อาจเป็นเหตุละเมิดภายใน 24 ชั่วโมงหลังพบเหตุ

2. แบบรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Form Template)

ชื่อแบบฟอร์ม: แบบรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

รหัสแบบฟอร์ม: DBD-FORM-101

หน่วยงานเจ้าของแบบฟอร์ม: ฝ่ายบริหารความมั่นคงข้อมูลส่วนบุคคล

ส่วนที่ 1: รายละเอียดของเหตุการณ์

1.1 วันที่และเวลาที่ตรวจพบเหตุการณ์:

1.2 สถานที่เกิดเหตุการณ์:

1.3 ลักษณะของเหตุการณ์:

() เข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

() การสูญหายของอุปกรณ์ที่มีข้อมูล

() การส่งข้อมูลผิดผู้รับ

() การถูกโจมตีทางไซเบอร์

() อื่น ๆ (ระบุ)

1.4 ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง

- () ข้อมูลทั่วไป
- () ข้อมูลอ่อนไหว (เช่น ข้อมูลสุขภาพ ศาสนา เชื้อชาติ)
- () ข้อมูลทางการเงิน
- () ข้อมูลการเข้าสู่ระบบ (เช่น Username/Password)
- () อื่น ๆ

ส่วนที่ 2: ข้อมูลของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือผู้ประสานงาน

2.1 ชื่อ-นามสกุล:

2.2 ตำแหน่ง:

2.3 อีเมล:

2.4 เบอร์โทรศัพท์:

ส่วนที่ 3: ผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์

3.1 ประเมินความรุนแรง (เลือก)

- () ร้ายแรงมาก - ส่งผลต่อบุคคลจำนวนมากหรือข้อมูลสำคัญรั่วไหล
- () ปานกลาง - ส่งผลต่อบุคคลบางส่วนหรือข้อมูลบางประเภท
- () ต่ำ - เกิดกับข้อมูลที่ไม่สำคัญ/จำกัดวง

3.2 คำอธิบายเพิ่มเติมเกี่ยวกับผลกระทบ

.....

ส่วนที่ 4: มาตรการที่ดำเนินการ

4.1 มาตรการที่ได้ดำเนินการเพื่อระงับ/แก้ไขเหตุการณ์

.....

4.2 มาตรการป้องกันในอนาคต

.....

4.3 มาตรการเยียวยาผู้ที่ได้รับผลกระทบ

.....

3. ตัวอย่างรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ตัวอย่าง:

วันที่เกิดเหตุ: 3 มิถุนายน 2568

เหตุการณ์: เจ้าหน้าที่ส่งอีเมลที่มีข้อมูลเวชระเบียนไปผิดผู้รับ

ข้อมูลที่เกี่ยวข้อง: ข้อมูลสุขภาพของผู้ป่วย 1 ราย

ผลกระทบ: ความเสี่ยงด้านความเป็นส่วนตัวและความอับอายของเจ้าของข้อมูล

การดำเนินการ: ทีม DPO ติดต่อผู้รับผิดชอบ ขอให้ลบข้อมูล และแจ้งผู้เกี่ยวข้อง

มาตรการป้องกัน: เปลี่ยนระบบการส่งข้อมูลให้ใช้ระบบเข้ารหัส และเพิ่มการอบรมเจ้าหน้าที่

4. ตัวอย่างบันทึกล็อก (Log) แจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

วันที่	เวลา	ผู้แจ้ง	ช่องทางแจ้ง	ประเภทเหตุการณ์	สถานะ	ผู้รับผิดชอบ	วันที่ดำเนินการแล้วเสร็จ
03/06/2568	09:45	วราภรณ์ สุขสันต์	Email	ส่งข้อมูลผิดผู้รับ	เสร็จสิ้น	ดร. สมศักดิ์ (DPO)	04/06/2568

แบบบันทึกเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(ตามข้อกำหนดหัวข้อ 10.1.5)

รหัสเหตุการณ์: DLB-2025-004

วันที่เกิดเหตุการณ์: 25 พฤษภาคม 2568

เวลาโดยประมาณ: 14.30 น.

ผู้แจ้งเหตุการณ์: นายสมชาย อินทร์งาม (เจ้าหน้าที่แผนกลูกค้าสัมพันธ์)

(1) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล

ลักษณะของเหตุการณ์: เจ้าหน้าที่จัดส่งอีเมลแจ้งยอดบัญชีลูกค้าผิดไปยังอีเมลของลูกค้ารายอื่น

ประเภทของการละเมิด

- ☐ การเปิดเผยข้อมูลส่วนบุคคลโดยไม่เจตนา
- ☐ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ☐ การสูญหายของข้อมูล
- ☐ การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต
- ☐ อื่น ๆ (ระบุ):

ข้อมูลที่ได้รับผลกระทบ: ชื่อ-นามสกุล หมายเลขบัญชีลูกค้า ยอดคงเหลือ ประวัติการชำระเงินย้อนหลัง 6 เดือน

(2) ข้อมูลผู้ประสานงานหรือ DPO

ชื่อ-สกุล: นางสาววรรณา ศิริธรรม

ตำแหน่ง: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

สถานที่ติดต่อ: ฝ่ายนิติการ อาคารสำนักงานชั้น 4

เบอร์โทรศัพท์: 02-123-4567 ต่อ 401

อีเมล: dpo@yourorg.co.th

(3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้น

ความรุนแรงของผลกระทบ: ปานกลางถึงสูง

คำอธิบายผลกระทบ:

- ลูกค้าผู้รับอีเมลอาจเข้าถึงข้อมูลการเงินของลูกค้ารายอื่น
- มีความเสี่ยงต่อการใช้ข้อมูลเพื่อประโยชน์ส่วนตน
- ความเชื่อมั่นของลูกค้าในองค์กรอาจลดลง
- ความเสี่ยงด้านการร้องเรียนต่อ สคส. หรือสำนักงานคุ้มครองข้อมูลส่วนบุคคล

(4) มาตรการที่ใช้หรือจะใช้ในการจัดการ

มาตรการป้องกัน

- ทบทวนและปรับปรุงขั้นตอนการส่งอีเมลอัตโนมัติ
- เพิ่มการยืนยันรายชื่อก่อนกดส่งด้วยระบบ 2 ขั้นตอน

มาตรการระงับเหตุ

- ติดต่อผู้รับผิดชอบลาดพื้นที่ และแจ้งให้ลบอีเมลโดยไม่เปิดอ่าน
- แจ้งเตือนผู้จัดการแผนกลูกค้าสัมพันธ์ให้ระงับการใช้งานระบบอีเมลชั่วคราว

มาตรการเยียวยา

- แจ้งลูกค้าที่ได้รับผลกระทบ พร้อมขอโทษอย่างเป็นทางการ
- เสนอเครดิตค่าธรรมเนียมบริการฟรี 1 เดือนเป็นการเยียวยา

การแจ้งหน่วยงานภายนอก

- ☐ แจ้งสำนักงานคุ้มครองข้อมูลส่วนบุคคล (PDPC)
- ☐ ยังไม่แจ้ง เนื่องจากอยู่ระหว่างการวิเคราะห์ว่าเข้าข่าย "ความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล" หรือไม่

สถานะการจัดการ: อยู่ระหว่างดำเนินการ (อัปเดตล่าสุดวันที่ 27 พ.ค. 2568)

ผู้บันทึกเหตุการณ์

(ลงชื่อ)

นางสาววรรณฯ ศิริธรรม

ตำแหน่ง: DPO

วันที่บันทึก: 25 พฤษภาคม 2568

10.1.6 มีระบบรวมศูนย์ในการบันทึกข้อมูลเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและเหตุที่มีการแจ้งเข้ามา แม้ว่าจะยังไม่เป็นเหตุการณ์ละเมิดข้อมูลส่วนบุคคลก็ตาม (แม้จะไม่ต้องรายงานหรือแจ้งไปยัง สคส. ก็ควรบันทึกเหตุการณ์ทุกอย่างเพื่อการตรวจสอบ)

สิ่งที่ต้องทำ: ระบบรวมศูนย์ในการบันทึกข้อมูลเหตุการณ์ละเมิดข้อมูลส่วนบุคคล และเหตุที่มีการแจ้งเข้ามา แม้ว่าจะยังไม่เป็นเหตุการณ์ละเมิดข้อมูลส่วนบุคคลก็ตาม (แม้จะไม่ต้องรายงานหรือแจ้งไปยัง สคส. ก็ควรบันทึกเหตุการณ์ทุกอย่างเพื่อการตรวจสอบ) และมีเอกสารสนับสนุน

หลักฐาน: แผนรับมือต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ขั้นตอนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล รายงานสรุปผลการดำเนินการรับมือด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

หัวข้อ: การมีระบบรวมศูนย์ในการบันทึกเหตุการณ์ละเมิดข้อมูลส่วนบุคคล และเหตุที่มีการแจ้งเข้ามา แม้ยังไม่เข้าข่ายการละเมิด

1. แผนรับมือต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ชื่อเอกสาร: แผนการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

รหัสเอกสาร: ISMS-IRP-001

ปรับปรุงล่าสุด: 1 พฤษภาคม 2568

สาระสำคัญ

องค์กรมีแผนดำเนินการเมื่อเกิด เหตุการณ์ที่อาจกระทบต่อข้อมูลส่วนบุคคล แม้ยังไม่สรุปว่าเป็น การละเมิดข้อมูล

ระบบรวมศูนย์รับเรื่องประกอบด้วย

- (1) ช่องทางแจ้งเหตุ (อีเมล โทรศัพท์ แบบฟอร์มออนไลน์)
- (2) เจ้าหน้าที่รับผิดชอบตรวจสอบเบื้องต้น (ทีม DPO และ IT Security)
- (3) การบันทึกเหตุการณ์ทุกกรณีในระบบ Incident Log
- (4) การวิเคราะห์ผลกระทบเบื้องต้น และตัดสินใจว่าจะจัดเป็นเหตุละเมิดหรือไม่

ระบบไม่พึ่งพาเฉพาะการรายงานภายนอก แต่เน้นการตรวจสอบภายในอย่างสม่ำเสมอ

2. ขั้นตอนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ชื่อเอกสาร: คู่มือปฏิบัติงานการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของข้อมูล

ขั้นตอนสำคัญ

การรับแจ้งเหตุ

- รับแจ้งผ่านช่องทางอย่างน้อย 3 ช่องทาง: อีเมล โทรศัพท์ แบบฟอร์มออนไลน์
- เจ้าหน้าที่ DPO ต้องลงบันทึกเหตุการณ์ทันที ไม่ว่าจะเป็น เหตุการณ์ยืนยัน หรือ เหตุการณ์ที่ต้องตรวจสอบต่อ

การบันทึกลงระบบ

เหตุการณ์ทุกกรณีจะถูกป้อนเข้าสู่ระบบ Incident Record System พร้อมรายละเอียดเบื้องต้น

การวิเคราะห์และประเมินผลกระทบ

ทีมงานจะวิเคราะห์ว่าเหตุการณ์เข้าข่าย "การละเมิดข้อมูลส่วนบุคคล" ตามมาตรา 37 หรือไม่

การจัดหมวดหมู่เหตุการณ์

แบ่งประเภท

- (1) เหตุการณ์ที่ยืนยันแล้วว่าเป็นการละเมิด

(2) เหตุการณ์ที่ยังไม่ยืนยัน แต่ต้องติดตาม

(3) เหตุการณ์ทั่วไปด้านความมั่นคงที่ไม่ใช่การละเมิด

การจัดเก็บและติดตามผล

ทุกเหตุการณ์จะมี Tracking ID

รายงานผลประจำเดือนโดยสรุปจำนวนเหตุการณ์ตามแต่ละประเภท

3. รายงานสรุปผลการดำเนินการรับมือด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ตัวอย่าง: รายงานประจำเดือนพฤษภาคม 2568

วันที่รับแจ้ง	ช่องทางแจ้ง	ประเภทเหตุการณ์	สถานะการตรวจสอบ	เข้าข่ายละเมิดข้อมูลหรือไม่	หมายเหตุ
02/05/2568	Email	ส่งอีเมลผิดผู้รับ	ตรวจสอบแล้ว	ใช่	รายงาน DPO แล้ว
05/05/2568	โทรศัพท์	ล็อกอินผิดพลาดหลายครั้ง	ตรวจสอบแล้ว	ไม่ใช่	เป็นความผิดพลาดของผู้ใช้
12/05/2568	แบบฟอร์ม	พบแฟลชไดรฟ์ตกอยู่ในสำนักงาน	อยู่ระหว่างตรวจสอบ	ยังไม่สรุป	ส่งให้ทีม IT ตรวจสอบ

หมายเหตุ:

แม้เหตุการณ์วันที่ 5 และ 12 พฤษภาคมจะไม่เข้าข่ายการละเมิดข้อมูลส่วนบุคคลในเบื้องต้น แต่ก็มีการบันทึกลงระบบเพื่อประเมินและใช้ในการวางมาตรการป้องกันล่วงหน้า
การบันทึกเหตุการณ์แบบรวมศูนย์นี้จะช่วยให้สามารถวิเคราะห์แนวโน้มและวางแผนป้องกันเหตุซ้ำได้

10.2 การประเมินและการรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Assessing and reporting breaches) องค์กรมีแนวปฏิบัติสำหรับการประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยทุกประเภท และสามารถแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลไปยัง สคส. ได้ภายในระยะเวลาที่กฎหมายกำหนด

10.2.1 มีแนวปฏิบัติในการประเมินโอกาสและความรุนแรงของความเสี่ยงต่อบุคคลอันเป็นผลจากการละเมิดข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: มีแนวปฏิบัติในการประเมินโอกาสและความรุนแรงของความเสี่ยงต่อบุคคลอันเป็นผลจากการละเมิดข้อมูลส่วนบุคคล และมีรายงานการประเมิน

หลักฐาน: นโยบายการประเมินความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล ขั้นตอนการประเมินโอกาสและความรุนแรงของความเสี่ยงต่อบุคคล รายงานการประเมินโอกาสและความรุนแรงของความเสี่ยงต่อบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) (4) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 4 (2) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 5 12

โทษทางปกครอง ในกรณีที่ไม่มีปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

แนวปฏิบัติในการประเมินโอกาสและความรุนแรงของความเสี่ยงต่อบุคคลอันเป็นผลจากการละเมิดข้อมูลส่วนบุคคล

1. นโยบายการประเมินความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล

องค์กรกำหนดนโยบายชัดเจนในการประเมินความเสี่ยงที่เกิดจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยเน้นการวิเคราะห์โอกาสที่จะเกิดเหตุการณ์ละเมิดและผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล รวมถึงการพิจารณามาตรการบรรเทาความเสี่ยงที่เหมาะสมและทันเวลา เพื่อป้องกันความเสียหาย และรักษาความน่าเชื่อถือขององค์กร

2. ขั้นตอนการประเมินโอกาสและความรุนแรงของความเสี่ยงต่อบุคคล

ขั้นตอนที่ 1: การรับแจ้งเหตุการณ์

เจ้าหน้าที่ที่ได้รับแจ้งเหตุการณ์จะทำการบันทึกรายละเอียดเหตุการณ์อย่างครบถ้วนและส่งต่อให้ทีมบริหารความเสี่ยงและ DPO

ขั้นตอนที่ 2: การวิเคราะห์ข้อมูลเบื้องต้น

ทีมประเมินจะตรวจสอบลักษณะของข้อมูลที่ถูกละเมิด เช่น ประเภทของข้อมูล จำนวนข้อมูลที่ถูกเปิดเผย หรือสูญหาย

ขั้นตอนที่ 3: การประเมินโอกาสเกิดเหตุการณ์

ประเมินความน่าจะเป็นที่เหตุการณ์จะเกิดผลกระทบ เช่น โอกาสที่ข้อมูลจะถูกนำไปใช้ผิดวัตถุประสงค์

ขั้นตอนที่ 4: การประเมินความรุนแรงของผลกระทบ

พิจารณาผลกระทบต่อเจ้าของข้อมูล ทั้งในด้านสิทธิส่วนบุคคล ความเสียหายทางการเงิน หรือผลกระทบทางชื่อเสียง

ขั้นตอนที่ 5: การสรุประดับความเสี่ยง

นำผลจากการประเมินโอกาสและความรุนแรงมาจัดระดับความเสี่ยง เช่น สูง กลาง ต่ำ

ขั้นตอนที่ 6: การจัดทำรายงานการประเมิน

จัดทำรายงานสรุปผลการประเมินความเสี่ยงเพื่อใช้ประกอบการแจ้งเหตุการณ์ต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.) และใช้ในการกำหนดมาตรการแก้ไข

3. รายงานการประเมินโอกาสและความรุนแรงของความเสี่ยงต่อบุคคล (ตัวอย่าง)

รายการ	รายละเอียด
รหัสเหตุการณ์	BR-2025-009
วันที่ประเมิน	3 มิถุนายน 2568
ลักษณะเหตุการณ์	การเข้าถึงระบบข้อมูลโดยไม่ได้รับอนุญาตผ่านช่องโหว่ระบบ
ประเภทข้อมูลที่ได้รับผลกระทบ	ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ-นามสกุล ที่อยู่ เบอร์โทรศัพท์
โอกาสเกิดผลกระทบ	ปานกลาง (ข้อมูลส่วนหนึ่งถูกเข้าถึงได้)
ความรุนแรงของผลกระทบ	สูง (ข้อมูลอาจถูกนำไปใช้ในทางที่ผิดและส่งผลกระทบต่อเจ้าของข้อมูล)
ระดับความเสี่ยง	สูง
ข้อเสนอแนะและมาตรการแก้ไข	เพิ่มความเข้มงวดการเข้าถึงระบบ ปรับปรุงช่องโหว่ด้านความปลอดภัย
ผู้ประเมิน	นางสาววรรณมา ศิริธรรม (DPO)

10.2.2 มีแนวปฏิบัติสำหรับการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. ได้รับทราบภายในระยะเวลา 72 ชั่วโมงนับแต่ทราบเหตุ (โดยอาจแจ้งบางส่วนก่อนได้ หากยังไม่มีข้อมูลทั้งหมดเกี่ยวกับเหตุการณ์ละเมิด) และแจ้งภายในกรอบระยะเวลาที่กฎหมายกำหนด

สิ่งที่ต้องทำ: มีแนวปฏิบัติสำหรับการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. ได้รับทราบภายในระยะเวลา 72 ชั่วโมงนับแต่ทราบเหตุ (โดยอาจแจ้งบางส่วนก่อนได้ หากยังไม่มีข้อมูลทั้งหมดเกี่ยวกับเหตุการณ์ละเมิด) และแจ้งภายในกรอบระยะเวลาที่กฎหมายกำหนด และมีหลักฐานสนับสนุน

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

หลักฐาน: นโยบายแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้ สคส. ทราบภายในกรอบระยะเวลาที่กฎหมายกำหนด

รายงานแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

นโยบายและแนวปฏิบัติการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

1. นโยบายการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดแนวทางปฏิบัติสำหรับการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้สำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.) ทราบภายในระยะเวลา 72 ชั่วโมงนับแต่ทราบเหตุ ตามที่กฎหมายกำหนด เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และป้องกันผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูล

ขอบเขต

นโยบายนี้ครอบคลุมการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลทุกประเภทที่เกิดขึ้นในองค์กร รวมถึงเหตุการณ์ที่อาจยังไม่เป็นการละเมิดข้อมูลแต่มีการแจ้งเข้ามา

ข้อกำหนดและแนวปฏิบัติ

- องค์กรต้องประเมินและตรวจสอบเหตุการละเมิดข้อมูลส่วนบุคคลทันทีที่ทราบเหตุ
- แจ้งเหตุการณืเบื้องต้นไปยัง สคส. ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ โดยสามารถแจ้งข้อมูลบางส่วนได้ก่อน หากยังไม่ทราบรายละเอียดทั้งหมด
- ส่งรายงานฉบับสมบูรณ์ต่อ สคส. ภายในเวลาที่กำหนดหลังจากแจ้งเบื้องต้น
- เก็บบันทึกและรายงานทุกขั้นตอนการแจ้งเหตุการณืไว้อย่างครบถ้วนเพื่อการตรวจสอบภายหลัง

2. ขั้นตอนแนวปฏิบัติการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ขั้นตอน	รายละเอียด	ผู้รับผิดชอบ	ระยะเวลา
1	ตรวจสอบและยืนยันเหตุการณ์	ทีม DPO / เจ้าหน้าที่ IT	ทันทีที่ทราบเหตุ
2	รวบรวมข้อมูลเบื้องต้น	ทีม DPO	ภายใน 24 ชั่วโมง
3	แจ้งเหตุการณ์เบื้องต้นไปยัง สคส.	ทีม DPO	ภายใน 72 ชั่วโมง
4	รวบรวมข้อมูลเพิ่มเติมและรายงานฉบับสมบูรณ์	ทีม DPO	ภายในเวลาที่กำหนด
5	เก็บรักษาเอกสารและรายงานแจ้งเหตุการณ์	ฝ่ายบริหารความเสี่ยง/ฝ่ายกฎหมาย	ตลอดไป

ตัวอย่างฟอร์มรายงานแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ชื่อองค์กร: บริษัท อินโนเวชั่น เทคโนโลยี จำกัด

วันที่รายงาน: 5 มิถุนายน 2568

รหัสเหตุการณ์: BR-2025-015

รายการ	รายละเอียด
วันที่และเวลาที่ทราบเหตุ	4 มิถุนายน 2568 เวลา 14:20 น.
วันที่และเวลาที่แจ้ง สคส.	5 มิถุนายน 2568 เวลา 10:00 น.
ลักษณะและประเภทของเหตุการณ์	การส่งอีเมลข้อมูลส่วนบุคคลผิดผู้รับ (Data disclosure by email error)
ประเภทข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	ชื่อ-นามสกุล เบอร์โทรศัพท์ อีเมล เลขประจำตัวประชาชนบางส่วน
จำนวนเจ้าของข้อมูลที่ได้รับผลกระทบ	80 คน
ผลกระทบเบื้องต้นต่อเจ้าของข้อมูล	มีความเสี่ยงถูกนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต อาจเกิดความเสียหายทางการเงินและชื่อเสียง
มาตรการแก้ไขและเยียวยา	แจ้งเตือนผู้รับผิดชอบอีเมลผิด ส่งอีเมลชี้แจงและขอคืนข้อมูล เพิ่มการอบรมพนักงาน ตรวจสอบระบบการส่งอีเมล

ผู้แจ้ง	ชื่อ: นางสาวสุภารัตน์ สุขสม ตำแหน่ง: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
รายชื่อผู้รับผิดชอบในการจัดการเหตุการณ์	ทีมไอที ทีมบริหารความเสี่ยง ฝ่ายกฎหมาย

ตัวอย่างการกรอกฟอร์มแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ชื่อองค์กร: บริษัท เอ็กเซลเลนซ์ จำกัด

วันที่รายงาน: 3 มิถุนายน 2568

รหัสเหตุการณ์: BR-2025-010

รายการ	รายละเอียด
วันที่และเวลาที่ทราบเหตุ	1 มิถุนายน 2568 เวลา 09:30 น.
วันที่และเวลาที่แจ้ง สดส.	3 มิถุนายน 2568 เวลา 15:00 น.
ลักษณะและประเภทของเหตุการณ์	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากบุคคลภายนอก (Unauthorized access)
ประเภทข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	ชื่อ-นามสกุล ที่อยู่ อีเมล
จำนวนเจ้าของข้อมูลที่ได้รับผลกระทบ	150 คน
ผลกระทบเบื้องต้นต่อเจ้าของข้อมูล	มีความเสี่ยงที่ข้อมูลจะถูกนำไปใช้ในทางที่ผิด
มาตรการแก้ไขและเยียวยา	ปิดช่องโหว่ระบบที่ถูกโจมตี แจ้งเตือนเจ้าของข้อมูลและติดตามเหตุการณ์
ผู้แจ้ง	ชื่อ: นายสมชาย ใจดี ตำแหน่ง: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
รายชื่อผู้รับผิดชอบในการจัดการเหตุการณ์	ทีม IT ทีมความมั่นคงปลอดภัยข้อมูล ฝ่ายกฎหมาย

5. เอกสารสนับสนุนอื่น ๆ

- นโยบายความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Data Security Policy)
- คู่มือการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Data Breach Handling Procedure)
- บันทึกการอบรมพนักงานเกี่ยวกับ PDPA และการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- รายงานสรุปผลการแจ้งเหตุการณ์และมาตรการแก้ไขในรอบปี

10.2.3 แนวปฏิบัติครอบคลุมถึงรายละเอียดและการระบุสาระสำคัญที่ต้องแจ้งให้ สคส. ได้รับทราบ

สิ่งที่ต้องทำ: มีแนวปฏิบัติครอบคลุมถึงรายละเอียดและการระบุสาระสำคัญที่ต้องแจ้งให้ สคส. ได้รับทราบ โดยมีเอกสารชัดเจนและครบถ้วน

หลักฐาน: รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
แบบฟอร์มการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
บันทึกรายงานแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
แนวปฏิบัติการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลไปยัง สคส.

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้ง
เหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง อาศัยอำนาจตาม มาตรา 37 ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทาง
ปกครองไม่เกิน 3 ล้านบาท

การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. รับทราบ

1. แนวปฏิบัติการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลไปยัง สคส.

วัตถุประสงค์

เพื่อกำหนดขั้นตอนและสาระสำคัญที่ต้องรายงานต่อ สคส. เมื่อเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลอย่างถูกต้องครบถ้วนภายในระยะเวลาที่กฎหมายกำหนด

ขั้นตอนหลัก

- ระบุลักษณะและประเภทของเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- รายละเอียดข้อมูลส่วนบุคคลที่ได้รับผลกระทบ
- ประมาณการจำนวนเจ้าของข้อมูลที่ได้รับผลกระทบ
- การประเมินผลกระทบและความเสี่ยงต่อเจ้าของข้อมูล
- มาตรการที่ได้ดำเนินการเพื่อป้องกัน แก้ไข และเยียวยาความเสียหาย
- ข้อมูลติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือผู้ประสานงาน
- ส่งรายงานแจ้งเหตุการณ์ภายใน 72 ชั่วโมงนับแต่ทราบเหตุ

เอกสารแนบปฏิบัติฉบับเต็ม

จัดทำเป็นเอกสารภายในองค์กร โดยใช้ชื่อว่า

“แนวปฏิบัติการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. ทราบ”

(เอกสารฉบับนี้มีรายละเอียดครบถ้วนตามมาตรา 37 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการฯ ปี 2565)

2. รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (ตัวอย่าง)

รหัสเหตุการณ์: BR-2025-015

วันที่รายงาน: 5 มิถุนายน 2568

รายละเอียดเหตุการณ์: การส่งอีเมลข้อมูลส่วนบุคคลผิดผู้รับ จำนวน 80 ราย เจ้าหน้าที่ดำเนินการแจ้งเตือนและขอคืนข้อมูลเรียบร้อยแล้ว

ผลกระทบ: เสี่ยงต่อการละเมิดความเป็นส่วนตัวของเจ้าของข้อมูล

มาตรการเยียวยา: เพิ่มมาตรการอบรมพนักงาน และตรวจสอบระบบการส่งอีเมลอย่างเข้มงวด

ผู้รับผิดชอบ: ฝ่ายไอทีและ DPO

3. แบบฟอร์มการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (ตามตัวอย่างหัวข้อ 10.2.2 ที่เคยจัดทำ) มีฟิลด์สำคัญ ได้แก่

- รายละเอียดเหตุการณ์
- ประเภทและลักษณะการละเมิด
- ข้อมูลเจ้าของข้อมูลที่ได้รับผลกระทบ
- การประเมินผลกระทบและความเสี่ยง
- มาตรการเยียวยาและแก้ไข
- ข้อมูลผู้รายงานและผู้รับผิดชอบ

4. บันทึกรายงานแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

- บันทึกเวลาการรับแจ้งเหตุการณ์
- บันทึกเวลาการดำเนินการประเมินและแจ้ง สคส.
- รายงานสรุปผลการดำเนินการเยียวยาและป้องกันไม่ให้เกิดซ้ำ

สภาพบังคับทางกฎหมาย

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

บทลงโทษ: ปรับทางปกครองไม่เกิน 3 ล้านบาท ในกรณีที่ไม่ปฏิบัติตามมาตรา 37

10.2.4 หากองค์กรพิจารณาว่าไม่จำเป็นต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. ทราบ องค์กรได้บันทึกเหตุผลที่องค์กรพิจารณาว่าการละเมิดไม่ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล
สิ่งที่ต้องทำ: หากองค์กรพิจารณาว่าไม่จำเป็นต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. ทราบ องค์กรได้บันทึกเหตุผลที่องค์กรพิจารณาว่าการละเมิดไม่ส่งผลให้เกิดความเสี่ยงต่อสิทธิและ

เสรีภาพของบุคคล และมีขั้นตอนการพิจารณาที่ชัดเจน รวมถึงมีเอกสารประกอบการพิจารณาสนับสนุน

หลักฐาน: บันทึกรายงานแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
แนวปฏิบัติเพื่อแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

นโยบายและแนวปฏิบัติการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(ตามที่ส่งไว้ก่อนหน้านี้ – ไม่ต้องกรอกข้อมูลเพิ่ม)

2. แบบฟอร์มบันทึกการประเมินเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Incident Risk Assessment Form)

หมายเลขเหตุการณ์ละเมิด (Incident ID)	INC-2025-0007
วันที่เกิดเหตุ	15/05/2025
ผู้รายงานเหตุการณ์	นายสมชาย ใจดี เจ้าหน้าที่ไอที 081-2345678
ประเภทข้อมูลที่ละเมิด	☐ ข้อมูลส่วนบุคคลทั่วไป ☐ ข้อมูลส่วนบุคคลประเภทพิเศษ
รายละเอียดเหตุการณ์	มีการเข้าถึงฐานข้อมูลลูกค้าโดยไม่ได้รับอนุญาต แต่ไม่พบการดาวน์โหลดข้อมูลใด ๆ
จำนวนเจ้าของข้อมูลที่ได้รับผลกระทบ	5 ราย
ผลกระทบที่อาจเกิดขึ้น	อาจมีการเปิดเผยข้อมูลส่วนบุคคลบางส่วน แต่ยังไม่พบการนำไปใช้ในทางที่ผิด
มาตรการที่ดำเนินการเพื่อแก้ไขเหตุการณ์	ปิดการเข้าถึงบัญชีที่ผิดปกติ เปลี่ยนรหัสผ่าน และตรวจสอบระบบรักษาความปลอดภัยเพิ่ม

การประเมินความเสี่ยง

ปัจจัยประเมิน	คะแนน (1-5)	หมายเหตุ
ความรุนแรงของข้อมูลที่ถูกละเมิด	2	ข้อมูลทั่วไป ไม่ใช่ข้อมูลสำคัญ
ขอบเขตของผลกระทบ (จำนวนผู้ได้รับผล)	1	จำนวนผู้ได้รับผลกระทบน้อย
ความน่าจะเป็นของผลกระทบ	2	มีมาตรการป้องกันและแก้ไขทันที
มาตรการป้องกัน/แก้ไขที่ดำเนินการแล้ว	4	มีการปิดบัญชีและตรวจสอบระบบอย่างรวดเร็ว

รวมคะแนนความเสี่ยง: 9 (จาก 20)

บันทึกเหตุการณ์ไม่แจ้งเหตุการณ์ต่อ สคส.

เนื่องจากเหตุการณ์ดังกล่าวมีคะแนนความเสี่ยงรวม 9 ซึ่งต่ำกว่าเกณฑ์ที่องค์กรกำหนดไว้ (15 คะแนนขึ้นไป) และข้อมูลที่ถูกละเมิดเป็นข้อมูลส่วนบุคคลทั่วไป จำนวนเจ้าของข้อมูลที่ได้รับผลกระทบต่ำมาก รวมทั้งได้ดำเนินการมาตรการป้องกันและแก้ไขอย่างรวดเร็ว องค์กรจึงพิจารณาว่าเหตุการณ์นี้ **ไม่จำเป็นต้องแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.)**

ลงชื่อผู้ประเมิน: นายสมชาย ใจดี
(เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)
วันที่: 17/05/2025

3. บันทึกการประชุมการพิจารณาการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

วันที่ประชุม: 18/05/2025

สถานที่: ห้องประชุมใหญ่ ชั้น 3

ผู้เข้าร่วมประชุม:

- นางสาวสุตารัตน์ ศรีสุข ผู้จัดการฝ่ายบริหารความเสี่ยง
- นายสมชาย ใจดี เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- นายวิชัย เทียงธรรม ผู้จัดการฝ่ายไอที

วาระการประชุม: พิจารณาการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เลขที่เหตุการณ์ INC-2025-0007

รายละเอียด

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรายงานผลการประเมินความเสี่ยงของเหตุการณ์ละเมิดข้อมูลว่า มีความเสี่ยงต่ำ โดยมีมาตรการแก้ไขที่เหมาะสมแล้วที่ดำเนินการ

มติที่ประชุม

ไม่แจ้งเหตุการณ์ต่อ สคส. เนื่องจากเหตุการณ์ไม่มีผลกระทบที่มีนัยสำคัญต่อสิทธิและเสรีภาพของเจ้าของข้อมูล และได้ดำเนินการแก้ไขแล้ว

ลงชื่อ

ประธานที่ประชุม: นางสาวสุภารัตน์ ศรีสุข

เลขานุการ: นายสมชาย ใจดี

4. บันทึกผลการแจ้งเจ้าของข้อมูลส่วนบุคคล (กรณีนี้ไม่มีแจ้งเจ้าของข้อมูล)

วันที่แจ้ง	วิธีการแจ้ง	รายละเอียดการแจ้ง	ผู้รับผิดชอบแจ้ง	หมายเหตุ
-	-	-	-	เหตุการณ์ไม่ส่งผลกระทบและไม่มีการแจ้งเจ้าของข้อมูล

5. ระบบจัดเก็บเอกสาร

เอกสารทั้งหมดนี้จัดเก็บในระบบบริหารจัดการเอกสารภายในองค์กร บนเซิร์ฟเวอร์ที่มีการสำรองข้อมูลรายวัน และกำหนดเก็บอย่างน้อย 5 ปี

10.3 การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบ (Notifying individuals)

องค์กรมีแนวปฏิบัติเพื่อแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ

10.3.1 มีแนวปฏิบัติสำหรับการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล กล่าวคือ เมื่อพิจารณาแล้วว่าเหตุที่เกิดขึ้นนั้นมีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล จะต้องดำเนินการแจ้งให้ได้รับทราบ

สิ่งที่ต้องทำ: มีแนวปฏิบัติสำหรับการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล และมีเอกสารครบถ้วน

หลักฐาน: นโยบายและแนวปฏิบัติสำหรับการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
หนังสือแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้ง
เหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การบันทึกเหตุผลการไม่แจ้งเหตุการณ่ละเมิดข้อมูลส่วนบุคคลให้ สคส. ทราบ

สิ่งที่ต้องทำ

- กรณีองค์กรพิจารณาว่าเหตุการณ่ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น **ไม่จำเป็นต้องแจ้งให้ สคส. ทราบ** เพราะเหตุการณ่ดังกล่าว **ไม่ส่งผลให้เกิดความเสี่ยงที่มีนัยสำคัญต่อสิทธิและเสรีภาพของเจ้าของข้อมูล**
- องค์กรต้องมี **ขั้นตอนการพิจารณา** อย่างชัดเจนเพื่อประเมินและตัดสินใจในเรื่องนี้
- ต้องมีการ **บันทึกเหตุผลการพิจารณาอย่างละเอียด** ว่าทำไมจึงไม่แจ้ง สคส. พร้อมทั้งหลักฐานประกอบการพิจารณา เช่น เอกสารการประเมินความเสี่ยง รายงานเหตุการณ่ และการวิเคราะห์ผลกระทบ
- มีการจัดเก็บเอกสารเหล่านี้อย่างเป็นระบบเพื่อการตรวจสอบในอนาคต

ตัวอย่างขั้นตอนการพิจารณาและบันทึกเหตุผล

- รับแจ้งเหตุการณ่ละเมิดข้อมูลส่วนบุคคลภายในองค์กร
- ดำเนินการประเมินความเสี่ยงเบื้องต้น (Impact Assessment) โดยพิจารณาโอกาสที่จะเกิดผลกระทบและความรุนแรงของผลกระทบต่อเจ้าของข้อมูล
- หากพบว่า **ความเสี่ยงต่ำ** ไม่ส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล หรือเหตุการณ่ไม่เข้าเกณฑ์ที่ต้องแจ้งตามกฎหมาย
- จัดทำรายงานสรุปการประเมินพร้อมบันทึกเหตุผลการประกอบการไม่แจ้ง สคส. เช่น
 1. ข้อมูลที่เปิดเผยเป็นข้อมูลสาธารณะ
 2. ข้อมูลไม่สามารถระบุตัวบุคคลได้
 3. มาตรการรักษาความปลอดภัยได้ผลและไม่มีผลกระทบจริง
- ลงนามรับรองโดยผู้มีอำนาจหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- จัดเก็บรายงานและเอกสารประกอบอย่างเป็นระบบ

ตัวอย่างเนื้อหาบันทึกเหตุผลการไม่แจ้งเหตุการณ่ละเมิด

บันทึกเหตุผลการพิจารณาไม่แจ้งเหตุการณ่ละเมิดข้อมูลส่วนบุคคลให้ สคส. ทราบ

เหตุการณ่

การเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาตแต่ไม่มีการคัดลอกหรือนำข้อมูลออกจากระบบ

ผลการประเมินความเสี่ยง: ความเสี่ยงต่ำ เนื่องจากข้อมูลมีการเข้ารหัสและระบบตรวจสอบล็อกใช้งานอย่างเข้มงวด ไม่มีหลักฐานว่าข้อมูลถูกเปิดเผยหรือถูกใช้ในทางที่ผิด

เหตุผลที่ไม่แจ้ง: การละเมิดไม่ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลตามที่กฎหมายกำหนด

ลงชื่อ: นาย/นางสาว xxx

ตำแหน่ง: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

วันที่: xx/xx/xxxx

หลักฐานประกอบ

- บันทึกรายงานแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Incident Report) ที่ระบุรายละเอียดเหตุการณ์และการประเมินความเสี่ยง
- แนวปฏิบัติเพื่อแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ที่ชัดเจนเกี่ยวกับกรณีที่ต้องแจ้งและไม่ต้องแจ้ง สคส.
- แบบฟอร์มการประเมินความเสี่ยงและบันทึกเหตุผล ประกอบการตัดสินใจ
- เอกสารรับรองการลงนามโดยผู้มีอำนาจและ DPO

สภาพบังคับ

ปัจจุบัน กฎหมายไม่ได้กำหนด ให้ต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่ไม่มีความเสี่ยงให้ สคส. ทราบ อย่างไรก็ตาม การมีระบบบันทึกเหตุผลและแนวปฏิบัติชัดเจนจะช่วยให้องค์กรสามารถแสดงความโปร่งใสและรับผิดชอบต่อการจัดการข้อมูลได้ดีขึ้น

การบันทึกเหตุผลกรณีไม่แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. ทราบ

สิ่งที่ต้องทำ

- กรณีองค์กรพิจารณาว่าเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น ไม่จำเป็นต้องแจ้งให้ สคส. ทราบ เพราะเหตุการณ์ดังกล่าว ไม่ส่งผลให้เกิดความเสี่ยงที่มีนัยสำคัญต่อสิทธิและเสรีภาพของเจ้าของข้อมูล
- องค์กรต้องมี ขั้นตอนการพิจารณา อย่างชัดเจนเพื่อประเมินและตัดสินใจในเรื่องนี้
- ต้องมีการ บันทึกเหตุผลการพิจารณาอย่างละเอียด ว่าทำไมจึงไม่แจ้ง สคส. พร้อมทั้งหลักฐานประกอบการพิจารณา เช่น เอกสารการประเมินความเสี่ยง รายงานเหตุการณ์ และการวิเคราะห์ผลกระทบ
- มีการจัดเก็บเอกสารเหล่านี้เป็นระบบเพื่อการตรวจสอบในอนาคต

ตัวอย่างขั้นตอนการพิจารณาและบันทึกเหตุผล

- รับแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลภายในองค์กร

- ดำเนินการประเมินความเสี่ยงเบื้องต้น (Impact Assessment) โดยพิจารณาโอกาสที่จะเกิดผลกระทบและความรุนแรงของผลกระทบต่อเจ้าของข้อมูล
- หากพบว่า **ความเสี่ยงต่ำ** ไม่ส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล หรือเหตุการณ์ไม่เข้าเกณฑ์ที่ต้องแจ้งตามกฎหมาย
- จัดทำรายงานสรุปการประเมินพร้อมบันทึกเหตุผลประกอบการไม่แจ้ง สคส. เช่น
 1. ข้อมูลที่เปิดเผยเป็นข้อมูลสาธารณะ
 2. ข้อมูลไม่สามารถระบุตัวบุคคลได้
 3. มาตรการรักษาความปลอดภัยได้ผลและไม่มีผลกระทบจริง
- ลงนามรับรองโดยผู้มีอำนาจหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
- จัดเก็บรายงานและเอกสารประกอบอย่างเป็นระบบ

ตัวอย่างเนื้อหาบันทึกเหตุการณ์ไม่แจ้งเหตุการณ์ละเมิด

บันทึกเหตุการณ์พิจารณาไม่แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. ทราบ

เหตุการณ์

การเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาตแต่ไม่มีการคัดลอกหรือนำข้อมูลออกจากระบบ
 ผลการประเมินความเสี่ยง: ความเสี่ยงต่ำ เนื่องจากข้อมูลมีการเข้ารหัสและระบบตรวจสอบล็อกใช้งานอย่างเข้มงวด ไม่มีหลักฐานว่าข้อมูลถูกเปิดเผยหรือถูกใช้ในทางที่ผิด
 เหตุผลที่ไม่แจ้ง: การละเมิดไม่ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลตามที่กฎหมายกำหนด

ลงชื่อ: นาย/นางสาว xxx

ตำแหน่ง: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

วันที่: xx/xx/xxxx

หลักฐานประกอบ

- บันทึกรายงานแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Incident Report) ที่ระบุรายละเอียดเหตุการณ์และการประเมินความเสี่ยง
- แนวปฏิบัติเพื่อแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ที่ชัดเจนเกี่ยวกับกรณีที่ต้องแจ้งและไม่ต้องแจ้ง สคส.
- แบบฟอร์มการประเมินความเสี่ยงและบันทึกเหตุผล ประกอบการตัดสินใจ
- เอกสารรับรองการลงนามโดยผู้มีอำนาจและ DPO

10.3.2 มีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงโดยไม่ชักช้า และใช้ภาษาและคำอธิบายที่เรียบง่าย ชัดเจน และสามารถทำความเข้าใจได้โดยง่าย

สิ่งที่ต้องทำ: มีขั้นตอนหรือแนวปฏิบัติในการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงโดยไม่ชักช้า และใช้ภาษาและคำอธิบายที่เรียบง่าย ชัดเจน และสามารถทำความเข้าใจได้โดยง่าย

หลักฐาน: นโยบายวิธีการและรายละเอียดการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

นโยบายและแนวปฏิบัติในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้เจ้าของข้อมูลได้รับทราบโดยไม่ชักช้า

1. วัตถุประสงค์

เพื่อกำหนดขั้นตอนและวิธีปฏิบัติในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล โดยต้องแจ้งโดยทันทีไม่ชักช้า และใช้ภาษาและคำอธิบายที่ชัดเจน เรียบง่าย เข้าใจได้ง่าย

2. ขอบเขต

นโยบายนี้ใช้กับการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงทุกกรณีที่เกิดขึ้นในองค์กร

3. แนวปฏิบัติ

3.1 การประเมินความเสี่ยงและระยะเวลาแจ้ง

เมื่อได้รับรายงานเหตุการณ์ละเมิดข้อมูล ต้องประเมินความเสี่ยงภายใน 24 ชั่วโมง หากพบว่ามีความเสี่ยงสูงต่อเจ้าของข้อมูล ต้องแจ้งเจ้าของข้อมูลภายใน 72 ชั่วโมง นับจากเวลาที่ทราบเหตุการณ์

3.2 วิธีการแจ้ง

แจ้งผ่านช่องทางที่เจ้าของข้อมูลสะดวกและสามารถยืนยันการได้รับแจ้งได้ เช่น อีเมล จดหมาย หรือโทรศัพท์

หากแจ้งด้วยข้อความ ให้ใช้ข้อความที่กระชับ ชัดเจน ไม่มีศัพท์เทคนิคที่ซับซ้อน

3.3 เนื้อหาการแจ้ง

- เนื้อหาการแจ้งต้องประกอบด้วย
- รายละเอียดเหตุการณ์อย่างสั้น ๆ แต่ครบถ้วน เช่น “ข้อมูลของท่านถูกเข้าถึงโดยไม่ได้รับอนุญาต”

- ประเภทของข้อมูลที่ได้รับผลกระทบ (เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์)
- ผลกระทบที่อาจเกิดขึ้นที่เจ้าของข้อมูลควรระวัง
- มาตรการที่องค์กรดำเนินการแก้ไข
- คำแนะนำสำหรับเจ้าของข้อมูล เช่น การเปลี่ยนรหัสผ่าน การติดตามสถานะบัญชี
- ช่องทางติดต่อสำหรับสอบถามข้อมูลเพิ่มเติม

3.4 การใช้ภาษาและคำอธิบาย

- ใช้ภาษาที่เป็นกันเอง เข้าใจง่าย ไม่ใช้ศัพท์กฎหมายหรือเทคนิคที่ซับซ้อน
- แบ่งเนื้อหาเป็นหัวข้อย่อย ๆ เพื่อความอ่านง่าย
- ให้คำอธิบายที่ชัดเจนและเป็นรูปธรรม

3.5 การบันทึกและติดตามผล

- บันทึกวันที่และเวลาที่แจ้งเจ้าของข้อมูล
- เก็บหลักฐานการแจ้ง เช่น สำเนาอีเมล ใบส่งจดหมาย ลงในระบบบริหารจัดการข้อมูลขององค์กร
- ติดตามและรับรองว่าผู้ได้รับแจ้งได้รับข้อมูลครบถ้วนและเข้าใจสาระสำคัญ

4. ตัวอย่างข้อความแจ้งเจ้าของข้อมูล (แบบเรียบง่าย เข้าใจง่าย)

เรียน คุณ [ชื่อเจ้าของข้อมูล]

เราขอแจ้งให้ทราบว่า ข้อมูลส่วนบุคคลของท่านได้รับผลกระทบจากเหตุการณ์ความปลอดภัยที่เกิดขึ้นในระบบของเรา ซึ่งรวมถึง [ประเภทข้อมูล เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์] เหตุการณ์นี้อาจทำให้ข้อมูลของท่านตกอยู่ในความเสี่ยง ทางเราขอภัยในความไม่สะดวกที่เกิดขึ้น และขอยืนยันว่าเราได้ดำเนินการแก้ไขปัญหาเรียบร้อยแล้ว

เพื่อความปลอดภัยของท่าน เราขอแนะนำให้คุณ [คำแนะนำ เช่น เปลี่ยนรหัสผ่าน ตรวจสอบบัญชีของท่าน]

หากท่านมีคำถามหรือต้องการข้อมูลเพิ่มเติม กรุณาติดต่อเราที่ [ช่องทางติดต่อ]

ขอบคุณสำหรับความเข้าใจและความร่วมมือ

[ชื่อผู้รับผิดชอบ]

[ตำแหน่ง]

[ชื่อองค์กร]

[วันที่]

5. สภาพบังคับ

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4)

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง: ปรับไม่เกิน 3 ล้านบาท หากไม่ปฏิบัติตามมาตรา 37

10.3.3 ข้อมูลที่ได้ทำการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลต้องมีสาระสำคัญดังต่อไปนี้

1. ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล
2. ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือผู้ประสานงานที่ได้รับมอบหมาย
3. ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
4. แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: ข้อมูลที่ได้ทำการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลต้องมีสาระสำคัญดังต่อไปนี้:

ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล

ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือผู้

ประสานงานที่ได้รับมอบหมาย

ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

หลักฐาน: หนังสือแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4)

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง อาศัยอำนาจตาม มาตรา 37 ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ตัวอย่างหนังสือแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Detailed Version)

หนังสือแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ที่ [เลขที่หนังสือ]/[ปี]

วันที่ [วัน เดือน ปี]

เรียน คุณ [ชื่อ-นามสกุลเจ้าของข้อมูล]

ตามที่บริษัท/องค์กร [ชื่อบริษัท/องค์กร] ได้ดำเนินการตรวจสอบและพบเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ซึ่งอาจส่งผลกระทบต่อสิทธิและเสรีภาพของท่าน ทางบริษัท/องค์กรจึงขอแจ้งรายละเอียดเหตุการณ์ดังต่อไปนี้ เพื่อให้ท่านได้รับทราบและดำเนินการป้องกันความเสียหายที่อาจเกิดขึ้น

1. ลักษณะของการละเมิดข้อมูลส่วนบุคคล

- เมื่อวันที่ [ระบุวันที่และเวลาที่เกิดเหตุการณ์] ทางบริษัท/องค์กรตรวจพบว่า [อธิบายเหตุการณ์โดยสังเขปและชัดเจน เช่น]
- มีบุคคลภายนอกที่ไม่ได้รับอนุญาตเข้าถึงระบบข้อมูลของบริษัท และดึงข้อมูลส่วนบุคคลของท่านออกไปจากฐานข้อมูล
- ข้อมูลที่ได้รับผลกระทบ ได้แก่ [ระบุข้อมูลที่ละเมิด เช่น ชื่อ ที่อยู่ หมายเลขบัตรประชาชน เบอร์โทรศัพท์ อีเมล ประวัติการซื้อขาย ฯลฯ]
- เหตุการณ์นี้เกิดขึ้นจากสาเหตุ [ระบุสาเหตุ เช่น ช่องโหว่ของระบบ ความผิดพลาดของเจ้าหน้าที่ การโจมตีของมัลแวร์ หรือการแฮกข้อมูล]

2. ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ท่านต้องการสอบถามข้อมูลเพิ่มเติม หรือแจ้งข้อสงสัยเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลนี้ กรุณาติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามรายละเอียดดังนี้

ชื่อ: [ชื่อ-นามสกุลเจ้าหน้าที่คุ้มครองข้อมูล]

ตำแหน่ง: [ตำแหน่งเจ้าหน้าที่]

ที่อยู่สำนักงาน: [ที่อยู่สำนักงานขององค์กร]

โทรศัพท์: [หมายเลขโทรศัพท์ติดต่อ]

อีเมล: [อีเมลติดต่อ]

3. ผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

เหตุการณ์ละเมิดข้อมูลนี้อาจส่งผลกระทบต่อความเป็นส่วนตัวและความปลอดภัยของท่าน โดยอาจมีความเสี่ยงที่ข้อมูลส่วนบุคคลของท่านถูกนำไปใช้ในทางที่ผิด เช่น

- การแอบอ้างตัวตนเพื่อดำเนินการต่าง ๆ โดยไม่ได้รับอนุญาต
- การรับสารที่ไม่พึงประสงค์ เช่น โฆษณาหรือการหลอกลวงทางโทรศัพท์หรืออีเมล
- ความเสี่ยงต่อการถูกโจรกรรมข้อมูลส่วนตัว หรือการแอบบัญชีอื่น ๆ ที่เกี่ยวข้อง
- บริษัท/องค์กรขอแนะนำให้ท่านดำเนินการอย่างระมัดระวัง และติดตามการแจ้งเตือนความปลอดภัยจากช่องทางที่เกี่ยวข้อง

4. แนวทางการเยียวยาความเสียหาย และมาตรการที่ดำเนินการ

- เพื่อป้องกันและลดผลกระทบจากเหตุการณ์นี้ บริษัท/องค์กรได้ดำเนินการมาตรการต่อไปนี้
- ปิดช่องโหว่และแก้ไขระบบรักษาความปลอดภัยทันที
- รีเซ็ตรหัสผ่านและเพิ่มขั้นตอนการยืนยันตัวตนที่เข้มงวดขึ้น

- อบรมเจ้าหน้าที่เกี่ยวกับการรักษาความปลอดภัยของข้อมูล
- ติดตามตรวจสอบระบบอย่างต่อเนื่องเพื่อป้องกันเหตุการณ์ซ้ำ
- จัดตั้งช่องทางการช่วยเหลือและให้คำปรึกษากับผู้ได้รับผลกระทบ

คำแนะนำสำหรับท่าน

- โปรดเปลี่ยนรหัสผ่านทุกบัญชีที่อาจได้รับผลกระทบโดยเร็ว
- ระมัดระวังการเปิดเผยข้อมูลส่วนบุคคลหรือการตอบรับข้อความ/อีเมลที่ไม่น่าเชื่อถือ
- หากพบเหตุการณ์ผิดปกติ เช่น การได้รับข้อความแปลก ๆ กรุณาแจ้งเจ้าหน้าที่ตามข้อมูลติดต่อด้านบนทันที

บริษัท/องค์กรขอภัยอย่างสูงสำหรับความไม่สะดวกที่เกิดขึ้น และขอยืนยันว่าจะดำเนินการอย่างเต็มความสามารถเพื่อปกป้องข้อมูลส่วนบุคคลของท่านอย่างดีที่สุด

ขอแสดงความนับถือ

[ลงชื่อ]

[ชื่อผู้แจ้ง]

[ตำแหน่ง]

[ชื่อองค์กร]

แนบ: เอกสารอธิบายมาตรการรักษาความปลอดภัยของบริษัท (ถ้ามี)

10.3.4 มีการให้คำแนะนำแก่เจ้าของข้อมูลส่วนบุคคลเพื่อให้สามารถป้องกันตนเองจากผลกระทบของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นนั้น

สิ่งที่ต้องทำ: มีการให้คำแนะนำแก่เจ้าของข้อมูลส่วนบุคคลเพื่อให้สามารถป้องกันตนเองจากผลกระทบของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นนั้น และมีเอกสารสนับสนุน

หลักฐาน: นโยบายการเผยแพร่ขั้นตอนการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
นโยบายการเผยแพร่สิทธิของเจ้าของข้อมูลส่วนบุคคล

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4)
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องหลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง: ในกรณีที่ฝ่าฝืนปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ตัวอย่างเอกสารคำแนะนำสำหรับเจ้าของข้อมูลส่วนบุคคล

คำแนะนำเพื่อป้องกันตนเองจากผลกระทบของเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

เรียน เจ้าของข้อมูลส่วนบุคคลที่เคารพ

เนื่องจากบริษัท/องค์กร [ชื่อบริษัท/องค์กร] ได้แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่อาจส่งผลกระทบต่อท่าน เพื่อช่วยให้ท่านลดความเสี่ยงและปกป้องข้อมูลส่วนบุคคลของท่านอย่างเหมาะสม บริษัท/องค์กรใคร่ขอแนะนำแนวทางปฏิบัติดังนี้:

เปลี่ยนรหัสผ่านทันที

- เปลี่ยนรหัสผ่านบัญชีที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยเฉพาะบัญชีที่ใช้กับบริษัท/องค์กรเรา
- ใช้รหัสผ่านที่แข็งแกร่งและไม่ซ้ำกันในแต่ละบริการ

ระมัดระวังการเปิดเผยข้อมูลส่วนบุคคล

- อย่าเปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลหรือช่องทางที่ไม่น่าเชื่อถือ
- อย่าคลิกลิงก์หรือเปิดไฟล์แนบในอีเมลหรือข้อความที่ไม่ทราบแหล่งที่มา

ตรวจสอบกิจกรรมที่ผิดปกติ

ตรวจสอบบัญชีธนาคาร อีเมล และบัญชีออนไลน์ของท่านอย่างสม่ำเสมอ เพื่อคว่ามีการเข้าถึงหรือกิจกรรมที่ไม่คุ้นเคยหรือไม่ หากพบความผิดปกติ ให้แจ้งธนาคารหรือผู้ให้บริการนั้น ๆ ทันที

ระวังการถูกหลอกลวง (Phishing)

1. ระมัดระวังข้อความหรืออีเมลที่ขอข้อมูลส่วนตัวหรือรหัสผ่าน
2. อย่าส่งข้อมูลสำคัญผ่านทางอีเมลหรือโทรศัพท์โดยไม่แน่ใจในความน่าเชื่อถือของผู้ขอ

แจ้งเหตุการณ์ผิดปกติ

ท่านพบเหตุการณ์ที่สงสัยว่าเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล สามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท/องค์กรได้ตามข้อมูลติดต่อที่แจ้งไปก่อนหน้านี้ บริษัท/องค์กร [ชื่อบริษัท/องค์กร] ยินดีให้คำปรึกษาและช่วยเหลือท่านอย่างเต็มที่เพื่อให้ข้อมูลส่วนบุคคลของท่านได้รับการคุ้มครองอย่างเหมาะสม

ขอแสดงความนับถือ

[ชื่อผู้แจ้ง]

[ตำแหน่ง]

[ชื่อบริษัท/องค์กร]

ตัวอย่างนโยบายการเผยแพร่ขั้นตอนการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

นโยบายการเผยแพร่ขั้นตอนการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

1. บริษัท/องค์กร [ชื่อบริษัท/องค์กร] ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลเป็นอย่างสูง โดยในกรณีเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล บริษัท/องค์กรมีขั้นตอนการแจ้งเหตุการณ์อย่างรวดเร็ว ชัดเจน และโปร่งใส ดังนี้
2. ตรวจสอบและประเมินผลกระทบของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลทันทีที่ได้รับแจ้ง
3. แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงเหตุการณ์และผลกระทบที่อาจเกิดขึ้นโดยไม่ชักช้า
4. ให้ข้อมูลและคำแนะนำแก่เจ้าของข้อมูลส่วนบุคคลในการป้องกันตนเองจากผลกระทบ

5. เปิดช่องทางการติดต่อสอบถามและช่วยเหลือสำหรับเจ้าของข้อมูลอย่างชัดเจน
6. เก็บบันทึกข้อมูลการแจ้งเหตุและดำเนินการเพื่อป้องกันเหตุการณ์ซ้ำในอนาคต
7. บริษัท/องค์กรยึดมั่นในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด

ตัวอย่างนโยบายการเผยแพร่สิทธิของเจ้าของข้อมูลส่วนบุคคล

นโยบายการเผยแพร่สิทธิของเจ้าของข้อมูลส่วนบุคคล

บริษัท/องค์กร [ชื่อบริษัท] รับรองและเคารพในสิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด ซึ่งเจ้าของข้อมูลส่วนบุคคลมีสิทธิดังนี้

- สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนเอง
- สิทธิในการขอให้แก้ไข เปลี่ยนแปลง หรือลบข้อมูลส่วนบุคคล
- สิทธิในการขอให้ระงับการใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- สิทธิในการคัดค้านการใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ทางการตลาด
- สิทธิในการร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- บริษัท/องค์กรมีช่องทางและกระบวนการในการรับคำขอและตอบสนองสิทธิของเจ้าของข้อมูลอย่างเหมาะสมและรวดเร็ว เพื่อให้เจ้าของข้อมูลได้รับการคุ้มครองและได้รับการปฏิบัติอย่างเป็นธรรม

10.4 การทบทวนและการเฝ้าระวังและติดตาม (Reviewing and monitoring)

องค์กรมีการทบทวนและเฝ้าระวังและติดตามเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

10.4.1 มีการนำข้อมูลหรือรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นแล้วมาวิเคราะห์เพื่อป้องกันการเกิดซ้ำในอนาคต

- สิ่งที่ต้องทำ: มีแนวปฏิบัติในการนำข้อมูลหรือรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นแล้วมาวิเคราะห์เพื่อป้องกันการเกิดซ้ำในอนาคต และมีเอกสารครบถ้วน
- หลักฐาน: ข้อมูลหรือรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นแล้วมาวิเคราะห์เพื่อป้องกันการเกิดซ้ำในอนาคต
- รายงานการวิเคราะห์ข้อมูลหรือรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
- รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 5 (5)
- โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

ตัวอย่างที่ 1: แนวปฏิบัติการวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคลเพื่อป้องกันการเกิดซ้ำ

แนวปฏิบัติในการวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น เพื่อนำผลการวิเคราะห์มาใช้ในการปรับปรุงและพัฒนามาตรการรักษาความมั่นคงปลอดภัยข้อมูลให้มีประสิทธิภาพ และป้องกันไม่ให้เกิดเหตุการณ์ดังกล่าวเกิดซ้ำ

2. ขอบเขต

ครอบคลุมเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นภายในองค์กร รวมถึงเหตุการณ์ที่ได้รับแจ้งจากเจ้าของข้อมูลหรือจากหน่วยงานภายนอก

3. ขั้นตอนการดำเนินการ

3.1 การรวบรวมข้อมูล

รวบรวมข้อมูลและเอกสารเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เช่น รายงานเหตุการณ์ บันทึกการแจ้งเตือน รายงานการตรวจสอบ เป็นต้น

3.2 การวิเคราะห์เหตุการณ์

วิเคราะห์สาเหตุและลักษณะของเหตุการณ์โดยใช้เทคนิค เช่น การวิเคราะห์สาเหตุราก (Root Cause Analysis)

3.3 การประเมินผลกระทบ

ประเมินผลกระทบต่อเจ้าของข้อมูลและองค์กร รวมถึงความเสี่ยงที่อาจเกิดขึ้นในอนาคต

3.4 การจัดทำข้อเสนอแนะ

เสนอแนะแนวทางแก้ไขและมาตรการป้องกันเพื่อลดความเสี่ยงและป้องกันไม่ให้เกิดเหตุซ้ำ

3.5 การติดตามผล

ติดตามการดำเนินการตามข้อเสนอแนะและประเมินประสิทธิผลของมาตรการที่นำไปใช้

4. ผู้รับผิดชอบ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และหน่วยงานที่เกี่ยวข้อง

5. การจัดเก็บและรายงาน

จัดเก็บรายงานการวิเคราะห์อย่างเป็นระบบ และรายงานผลการวิเคราะห์แก่ผู้บริหารและคณะกรรมการความปลอดภัยข้อมูลอย่างสม่ำเสมอ

ตัวอย่างที่ 2: รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

บริษัท/องค์กร: [ชื่อองค์กร]

วันที่เกิดเหตุ: 10 พฤษภาคม 2568

ผู้รายงานเหตุ: นายสมชาย ใจดี (เจ้าหน้าที่ IT)

หมายเลขรายงาน: IR-2025-0510-001

รายละเอียดเหตุการณ์

เมื่อวันที่ 10 พฤษภาคม 2568 เวลา 14:30 น. ระบบฐานข้อมูลลูกค้าเกิดข้อผิดพลาดทำให้ข้อมูลลูกค้ากว่า 1000 ราย ถูกเปิดเผยแก่บุคคลภายนอกโดยไม่ได้รับอนุญาต เนื่องจากมีช่องโหว่ด้านความปลอดภัยของระบบฐานข้อมูลที่ยังไม่ได้รับการแก้ไข

ข้อมูลที่ถูกเปิดเผย

- ชื่อ-นามสกุล
- เลขประจำตัวประชาชนบางส่วน (ไม่ครบทั้งหมด)
- เบอร์โทรศัพท์
- อีเมล

ผลกระทบที่คาดว่าจะเกิดขึ้น

- ความเสี่ยงถูกนำข้อมูลไปใช้ในทางที่ผิด เช่น การแอบอ้างข้อมูล (Identity Theft)

- ความเสียหายต่อชื่อเสียงองค์กร

การดำเนินการเบื้องต้น

- ปิดระบบฐานข้อมูลที่มีช่องโหว่ทันที
- แจ้งเจ้าของข้อมูลที่ได้รับผลกระทบ
- เริ่มการสอบสวนเหตุการณ์

ตัวอย่างที่ 3: รายงานการวิเคราะห์เหตุการณ์และข้อเสนอแนะ

รายงานการวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคล

บริษัท/องค์กร: [ชื่อองค์กร]

วันที่วิเคราะห์: 15 พฤษภาคม 2568

ผู้วิเคราะห์: นางสาวสุภารัตน์ สุขใจ (DPO)

1. สาเหตุของเหตุการณ์

จากการวิเคราะห์พบว่า ช่องโหว่ในระบบฐานข้อมูลเกิดจากการไม่ได้อัปเดตแพตช์ความปลอดภัยเป็นเวลานาน รวมถึงมีการจัดการสิทธิ์เข้าถึงข้อมูลที่ไม่เหมาะสม

2. ผลกระทบ

- ข้อมูลส่วนบุคคลของลูกค้ากว่า 1000 รายถูกเปิดเผยโดยไม่ได้รับอนุญาต
- ความเชื่อมั่นของลูกค้าลดลง
- อาจได้รับโทษทางกฎหมายและปรับทางปกครองสูงสุด

3. ข้อเสนอแนะเพื่อป้องกันไม่ให้เกิดซ้ำ

- เร่งอัปเดตแพตช์ความปลอดภัยของระบบฐานข้อมูลทันที
- ปรับปรุงระบบจัดการสิทธิ์เข้าถึงข้อมูลให้เข้มงวดมากขึ้น
- จัดอบรมเจ้าหน้าที่ IT และผู้ใช้งานระบบเกี่ยวกับมาตรการรักษาความปลอดภัยข้อมูลอย่างสม่ำเสมอ
- ตรวจสอบระบบความปลอดภัยเป็นประจำทุก 3 เดือน

4. แผนการติดตามผล

- จัดทำรายงานความคืบหน้าในแต่ละเดือน
- ประเมินประสิทธิภาพของมาตรการภายใน 6 เดือน
- รายงานผลให้ฝ่ายบริหารและคณะกรรมการทราบ

10.4.2 มีการติดตามและสรุปผลเกี่ยวกับประเภท จำนวน และค่าใช้จ่ายที่เกี่ยวข้องกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น (วัดจากค่าใช้จ่ายในการกู้คืน การบริหารจัดการ และค่าเสียหายจากการถูกปรับ หรือการถูกฟ้องร้องดำเนินคดี)

- สิ่งที่ต้องทำ: มีการติดตามและสรุปผลเกี่ยวกับประเภท จำนวน และค่าใช้จ่ายที่เกี่ยวข้องกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น และมีเอกสารสนับสนุน
- หลักฐาน: นโยบายการจัดทำทะเบียนสรุปผลเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
ทะเบียนสรุปผลเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- สภาพบังคับ: คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565
- โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

1. นโยบายการจัดทำทะเบียนสรุปผลเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

นโยบายการจัดทำทะเบียนสรุปผลเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อให้การติดตามและสรุปผลประเภท จำนวน และค่าใช้จ่ายที่เกิดขึ้นจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคลมีความเป็นระบบและครบถ้วน เพื่อใช้เป็นข้อมูลสำหรับการบริหารจัดการความเสี่ยงและวางแผนปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยข้อมูลขององค์กร

ขอบเขต

ครอบคลุมเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นในองค์กรทุกรายการ

รายละเอียด

การจัดทำทะเบียนสรุปผล

จัดเก็บข้อมูลเหตุการณ์ละเมิดข้อมูลส่วนบุคคลทุกเหตุการณ์ในทะเบียนสรุปผลที่มีรายการครบถ้วน เช่น

- หมายเลขเหตุการณ์
- วันที่เกิดเหตุ
- ประเภทของเหตุการณ์ (เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การสูญหายของข้อมูล การถูกโจมตีทางไซเบอร์)
- จำนวนข้อมูลที่ได้รับผลกระทบ (เช่น จำนวนรายชื่อ จำนวนรายการข้อมูล)
- ค่าใช้จ่ายที่เกิดขึ้นจากเหตุการณ์ (รายละเอียดค่าใช้จ่ายในแต่ละส่วน)

ค่าใช้จ่ายที่ต้องบันทึก

- ค่าใช้จ่ายในการกู้คืนข้อมูล (เช่น ค่าจ้างผู้เชี่ยวชาญ ค่าซ่อมแซมระบบ)
- ค่าใช้จ่ายในการบริหารจัดการ (เช่น ค่าจัดการทีมสอบสวน ค่าบริหารงานด้านกฎหมาย)
- ค่าใช้จ่ายจากการถูกปรับทางปกครอง หรือค่าเสียหายจากคดีความ

การติดตามและปรับปรุง

- ทบทวนทะเบียนสรุปผลอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
- รายงานผลการติดตามและวิเคราะห์แนวโน้มค่าใช้จ่ายให้กับฝ่ายบริหารเพื่อวางแผนลดความเสี่ยง

ผู้รับผิดชอบ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และฝ่ายการเงิน รวมถึงฝ่ายกฎหมาย

2. ตัวอย่างทะเบียนสรุปผลเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Sample Data)

หมายเลข เหตุการณ์	วันที่ เกิด เหตุ	ประเภท เหตุการณ์	จำนวน ข้อมูล ที่	ค่าใช้จ่าย กู้คืน (บาท)	ค่าใช้จ่าย บริหาร	ค่าเสียหาย ทาง	รวม ค่าใช้จ่าย (บาท)	หมายเหตุ

			ได้รับ ผลกระทบ		จัดการ (บาท)	กฎหมาย (บาท)		
IR-2025-0510-001	10 พ.ค. 2568	การเข้าถึง ข้อมูลโดย ไม่ได้รับ อนุญาต	1000 ราย	150000	50000	500000	700000	กำลัง ดำเนินคดี ทาง กฎหมาย
IR-2025-0312-002	12 มี.ค. 2568	การสูญ หายของ ข้อมูล	200 ราย	80000	20000	0	100000	ไม่มีการ ฟ้องร้อง
IR-2025-0701-003	1 ก.ค. 2568	การโจมตี ทางไซ เบอร์	3000 ราย	300000	100000	0	400000	ปรับปรุง ระบบและ อบรม พนักงาน แล้ว

3. ตัวอย่างรายงานสรุปผลค่าใช้จ่ายและจำนวนเหตุการณ์

รายงานสรุปผลการติดตามเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

สำหรับช่วงไตรมาสที่ 2 ปี 2568

1. สรุปภาพรวมเหตุการณ์

- จำนวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลทั้งหมด: 5 เหตุการณ์
- ประเภทเหตุการณ์ที่พบมากที่สุด: การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (3 เหตุการณ์)
- จำนวนข้อมูลที่ได้รับผลกระทบรวม: 4500 ราย

2. สรุปค่าใช้จ่ายรวม

- ค่าใช้จ่ายในการกู้คืนข้อมูล: 530000 บาท
- ค่าใช้จ่ายในการบริหารจัดการ: 170000 บาท
- ค่าเสียหายทางกฎหมายและปรับทางปกครอง: 500000 บาท

รวมค่าใช้จ่ายทั้งหมด: 1200000 บาท

3. แนวโน้มและข้อเสนอแนะ

- ค่าใช้จ่ายจากการกู้คืนข้อมูลเพิ่มขึ้นเนื่องจากความซับซ้อนของเหตุการณ์
- ควรเร่งดำเนินการมาตรการเสริมความปลอดภัยระบบฐานข้อมูลและอบรมพนักงานอย่างต่อเนื่อง
- แนะนำเพิ่มงบประมาณสำหรับการบริหารความเสี่ยงข้อมูลในปีหน้าเพื่อรองรับเหตุการณ์ที่อาจเกิดขึ้น

สภาพบังคับและโทษ

- ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2565
- โทษทางปกครองสำหรับการไม่ปฏิบัติตามอาจถูกปรับไม่เกิน 3 ล้านบาท

10.4.3 มีการวิเคราะห์แนวโน้มของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นในรอบระยะเวลาที่ผ่านมา เพื่อทำความเข้าใจถึงประเด็นหลัก ๆ ที่เกิดขึ้น และมีการรายงานผลการวิเคราะห์นั้นให้คณะทำงานที่ทำหน้าที่กำกับด้านการคุ้มครองข้อมูลส่วนบุคคลหรือการจัดการข้อมูลได้รับทราบ เพื่อใช้ประโยชน์จากรายงานนั้นในการป้องกันและกำกับดูแลองค์กรต่อไป

สิ่งที่ต้องทำ: มีการวิเคราะห์แนวโน้มของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นในรอบระยะเวลาที่ผ่านมา เพื่อทำความเข้าใจถึงประเด็นหลัก ๆ ที่เกิดขึ้น และมีการรายงานผลการวิเคราะห์นั้นให้คณะทำงานที่ทำหน้าที่กำกับด้านการคุ้มครองข้อมูลส่วนบุคคลหรือการจัดการข้อมูลได้รับทราบ เพื่อใช้ประโยชน์จากรายงานนั้นในการป้องกันและกำกับดูแลองค์กรต่อไป และมีเอกสารสนับสนุน

หลักฐาน: นโยบายการวิเคราะห์แนวโน้มของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
นโยบายการจัดทำรายงานผลการวิเคราะห์แนวโน้มของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
รายงานผลการวิเคราะห์แนวโน้มของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

1. นโยบายการวิเคราะห์แนวโน้มของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

นโยบายการวิเคราะห์แนวโน้มของเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อสร้างความเข้าใจที่ชัดเจนเกี่ยวกับประเด็นหลักของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นในองค์กร ตลอดจนแนวโน้มและรูปแบบที่สำคัญ เพื่อเป็นข้อมูลสำหรับวางแผนป้องกันและปรับปรุงมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง

ขอบเขต

ครอบคลุมเหตุการณ์ละเมิดข้อมูลส่วนบุคคลทั้งหมดที่ได้รับการบันทึกในระบบทะเบียนสรุปผลเหตุการณ์ภายในองค์กรในช่วงเวลาที่กำหนด

รายละเอียด

การรวบรวมข้อมูล

- รวบรวมข้อมูลเหตุการณ์ละเมิดข้อมูลส่วนบุคคลจากทะเบียนสรุปผลเหตุการณ์ในรอบระยะเวลาที่กำหนด (เช่น 6 เดือน 1 ปี)

การวิเคราะห์แนวโน้ม

- วิเคราะห์ประเภทของเหตุการณ์ที่เกิดขึ้นบ่อยครั้ง
- วิเคราะห์สาเหตุที่เป็นไปได้ของเหตุการณ์ละเมิดข้อมูล
- วิเคราะห์กลุ่มข้อมูลหรือระบบที่มีความเสี่ยงสูง
- วิเคราะห์ผลกระทบและค่าใช้จ่ายที่เกิดขึ้น

การจัดทำรายงาน

- จัดทำรายงานผลการวิเคราะห์แนวโน้มอย่างละเอียด พร้อมแผนภาพหรือกราฟประกอบ
- รายงานจะต้องแสดงข้อสรุปและข้อเสนอแนะสำหรับการดำเนินมาตรการป้องกัน

การรายงานและเผยแพร่

- รายงานผลการวิเคราะห์จะต้องถูกนำเสนอแก่คณะทำงานที่ทำหน้าที่กำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล (เช่น คณะกรรมการคุ้มครองข้อมูล Data Protection Committee)
- ใช้รายงานเพื่อการวางแผนและการตัดสินใจด้านการบริหารความเสี่ยงข้อมูลส่วนบุคคล

ผู้รับผิดชอบ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ร่วมกับฝ่ายบริหารความเสี่ยง และฝ่าย IT Security

2. นโยบายการจัดทำรายงานผลการวิเคราะห์แนวโน้มของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

นโยบายการจัดทำรายงานผลการวิเคราะห์แนวโน้มของเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดขั้นตอนและรูปแบบการจัดทำรายงานวิเคราะห์แนวโน้มเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้เป็นมาตรฐาน และเพื่อให้รายงานนั้นมีความถูกต้อง ครบถ้วน และสามารถนำไปใช้เป็นฐานข้อมูลสำหรับการกำกับดูแลและปรับปรุงมาตรการได้อย่างมีประสิทธิภาพ

รายละเอียด

- กำหนดช่วงเวลาที่ต้องจัดทำรายงาน (เช่น รายไตรมาส หรือรายปี)
- รูปแบบรายงานต้องประกอบด้วยข้อมูลสรุป กราฟหรือแผนภูมิแสดงแนวโน้ม และข้อเสนอแนะเชิงนโยบาย
- รายงานจะต้องได้รับการตรวจสอบความถูกต้องจากเจ้าหน้าที่คุ้มครองข้อมูล และผู้บริหารที่เกี่ยวข้องก่อนเผยแพร่
- การเผยแพร่รายงานต้องเป็นไปตามนโยบายความลับและความปลอดภัยของข้อมูล

ผู้รับผิดชอบ

ฝ่ายคุ้มครองข้อมูลส่วนบุคคลและฝ่ายบริหารความเสี่ยง

3. ตัวอย่างรายงานผลการวิเคราะห์แนวโน้มของเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

รายงานผลการวิเคราะห์แนวโน้มเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ช่วงเวลาวิเคราะห์: มกราคม – ธันวาคม 2567

1. สรุปภาพรวมเหตุการณ์

- จำนวนเหตุการณ์ละเมิดข้อมูลที่เกิดขึ้นทั้งหมด: 12 รายการ
- ประเภทเหตุการณ์ที่พบมากที่สุด: การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (7 รายการ)
- ระบบที่มีเหตุการณ์เกิดขึ้นบ่อย: ระบบฐานข้อมูลลูกค้า และระบบงานบุคคล

2. แนวโน้มและรูปแบบสำคัญ

- เหตุการณ์ส่วนใหญ่เกิดจากข้อผิดพลาดของผู้ใช้งาน (เช่น ส่งข้อมูลผิดผู้รับ) ประมาณ 50%
- มีการโจมตีจากภายนอกโดยใช้มัลแวร์เพิ่มขึ้น 25%
- ค่าใช้จ่ายรวมจากเหตุการณ์เพิ่มขึ้น 15% เมื่อเทียบกับปีที่ผ่านมา

3. ผลกระทบสำคัญ

- ข้อมูลส่วนบุคคลของลูกค้าได้รับผลกระทบสูงสุด (ประมาณ 60% ของข้อมูลที่เสียหายทั้งหมด)
- ค่าใช้จ่ายในการกู้คืนและบริหารจัดการข้อมูลเพิ่มสูงขึ้นอย่างมีนัยสำคัญ

4. ข้อเสนอแนะ

- เพิ่มการฝึกอบรมด้านความปลอดภัยข้อมูลให้พนักงานทุกระดับอย่างน้อยปีละ 2 ครั้ง
- ปรับปรุงระบบควบคุมการเข้าถึงข้อมูลอย่างเข้มงวด
- เพิ่มมาตรการตรวจจับและป้องกันมัลแวร์ในระบบ IT

การนำเสนอรายงาน

ฉบับนี้ได้นำเสนอต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเมื่อวันที่ 10 มกราคม 2568 และได้รับคำแนะนำให้ดำเนินการตามข้อเสนอแนะโดยเร่งด่วน

10.4.4 คณะทำงานที่ทำหน้าที่กำกับด้านการคุ้มครองข้อมูลส่วนบุคคลหรือการจัดการข้อมูลได้มีการทบทวนรายงานผลการวิเคราะห์ดังกล่าวและให้คำแนะนำหรือข้อคิดเห็นที่จำเป็น

สิ่งที่ต้องทำ: คณะทำงานที่ทำหน้าที่กำกับด้านการคุ้มครองข้อมูลส่วนบุคคลหรือการจัดการข้อมูลได้มีการทบทวนรายงานผลการวิเคราะห์ดังกล่าวและให้คำแนะนำหรือข้อคิดเห็นที่จำเป็น และมีเอกสารสนับสนุน

หลักฐาน: นโยบายการทบทวนรายงานผลการวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
นโยบายควบคุมการปฏิบัติหน้าที่ของ DPO ให้ครอบคลุมถึงการให้คำแนะนำหรือข้อคิดเห็นที่จำเป็นเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 5 (5)

โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การทบทวนรายงานผลการวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคลโดยคณะทำงานกำกับดูแล

สิ่งที่ต้องทำ

คณะทำงานที่ทำหน้าที่กำกับด้านการคุ้มครองข้อมูลส่วนบุคคลหรือการจัดการข้อมูล ต้องมีการทบทวนรายงานผลการวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น และให้คำแนะนำหรือข้อคิดเห็นที่จำเป็น เพื่อใช้ในการปรับปรุงมาตรการและกำกับดูแลอย่างมีประสิทธิภาพ พร้อมจัดทำเอกสารสนับสนุนเพื่อบันทึกการทบทวนและข้อคิดเห็นนั้น

ตัวอย่างหลักฐานประกอบ

1. นโยบายการทบทวนรายงานผลการวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

นโยบายการทบทวนรายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดขั้นตอนและแนวทางในการทบทวนรายงานผลการวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคลโดยคณะกรรมการกำกับดูแลข้อมูลส่วนบุคคล และเพื่อให้เกิดการติดตามผลและการปรับปรุงมาตรการคุ้มครองข้อมูลอย่างต่อเนื่อง

รายละเอียด

- รายงานผลการวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคลต้องถูกส่งให้คณะกรรมการกำกับดูแลเพื่อพิจารณาทบทวนอย่างน้อยทุกไตรมาส
- คณะกรรมการกำกับดูแลจะต้องจัดประชุมเพื่อตรวจสอบรายงานผลและอภิปรายถึงแนวโน้ม ปัญหา และมาตรการที่จำเป็นในการป้องกันเหตุการณ์ซ้ำ
- คณะกรรมการกำกับดูแลจะต้องจัดทำบันทึกการประชุมที่ระบุข้อคิดเห็น คำแนะนำ และมติที่เกี่ยวข้องไว้เป็นลายลักษณ์อักษร
- ข้อเสนอแนะที่ได้รับจะต้องนำไปดำเนินการและติดตามผลอย่างต่อเนื่อง

ผู้รับผิดชอบ

คณะกรรมการกำกับดูแลข้อมูลส่วนบุคคล (Data Protection Committee) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

2. นโยบายควบคุมการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

นโยบายควบคุมการปฏิบัติหน้าที่ของ DPO

วัตถุประสงค์

เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในการให้คำแนะนำและข้อคิดเห็นเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล รวมถึงการสนับสนุนคณะกรรมการกำกับดูแลข้อมูลในการดำเนินการตามกฎหมาย

รายละเอียด

- DPO ต้องตรวจสอบและวิเคราะห์รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลอย่างละเอียด
- DPO มีหน้าที่จัดเตรียมคำแนะนำและข้อคิดเห็นเชิงเทคนิคและเชิงนโยบายสำหรับคณะกรรมการกำกับดูแลข้อมูล
- DPO ต้องรายงานประเด็นสำคัญและข้อเสนอแนะในการประชุมของคณะกรรมการกำกับดูแล เพื่อช่วยสนับสนุนการตัดสินใจและการบริหารความเสี่ยง
- DPO จะต้องติดตามการดำเนินการตามคำแนะนำและรายงานความคืบหน้าต่อคณะกรรมการและฝ่ายบริหารเป็นระยะ

ผู้รับผิดชอบ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

3. ตัวอย่างเอกสารสนับสนุนอื่น ๆ ที่ควรมี

- บันทึกการประชุมคณะทำงานกำกับดูแลข้อมูลส่วนบุคคล ที่มีหัวข้อ “ทบทวนรายงานผลการวิเคราะห์เหตุการณ์ละเมิดข้อมูลส่วนบุคคล” พร้อมรายละเอียดข้อคิดเห็นและคำแนะนำ
- รายงานการดำเนินการตามข้อเสนอแนะ ที่แสดงการติดตามและแก้ไขปัญหาที่ได้รับคำแนะนำจากคณะทำงาน
- หนังสือแจ้งหรือบันทึกข้อความ ที่ส่งมอบคำแนะนำของคณะทำงานไปยังฝ่ายที่เกี่ยวข้อง เช่น ฝ่าย IT ฝ่ายบริหารความเสี่ยง

สภาพบังคับและโทษทางกฎหมาย

สภาพบังคับ

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 5 (5)

โทษทางปกครอง กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท หากไม่ปฏิบัติตามมาตรา 37

10.5 การตรวจสอบโดยผู้ตรวจสอบภายนอก (External audit or compliance check)

องค์กรมีการตั้งผู้ตรวจสอบภายนอกเพื่อตรวจสอบและทบทวนการดำเนินการให้สอดคล้องกับกฎหมาย

10.5.1 มีการใช้โปรแกรมหรือเครื่องมือเพื่อประเมินตนเองและรับรองความสอดคล้องกับ

- 1) การคุ้มครองข้อมูลส่วนบุคคล
 - 2) การรักษาความมั่นคงปลอดภัยสารสนเทศ (ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล)
- สิ่งที่ต้องทำ: องค์กรมีการใช้โปรแกรมหรือเครื่องมือเพื่อประเมินตนเองและรับรองความสอดคล้องกับ

- 1) การคุ้มครองข้อมูลส่วนบุคคล
- 2) การรักษาความมั่นคงปลอดภัยสารสนเทศ และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการตั้งผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกเพื่อตรวจสอบและทบทวนการดำเนินการให้สอดคล้องกับกฎหมาย

สัญญาจ้างผู้ตรวจสอบภายนอก
สภาพบังคับ: กฎหมายไม่ได้กำหนด

การตรวจสอบโดยผู้ตรวจสอบภายนอก (External audit or compliance check)

องค์กรมีการตั้งผู้ตรวจสอบภายนอกเพื่อตรวจสอบและทบทวนการดำเนินการให้สอดคล้องกับกฎหมาย

10.5.1 การใช้โปรแกรมหรือเครื่องมือประเมินตนเองและรับรองความสอดคล้อง

สิ่งที่ต้องทำ

- องค์กรต้องมีการใช้โปรแกรมหรือเครื่องมือในการประเมินตนเอง เพื่อรับรองความสอดคล้องกับ
- การคุ้มครองข้อมูลส่วนบุคคล
- การรักษาความมั่นคงปลอดภัยสารสนเทศ (ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล)
- และต้องมีเอกสารที่เกี่ยวข้องครบถ้วนเพื่อสนับสนุนการดำเนินงานดังกล่าว

ตัวอย่างหลักฐานประกอบ

นโยบายการตั้งผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก

- นโยบายระบุว่ามี การแต่งตั้งผู้ตรวจสอบภายนอกเพื่อดำเนินการตรวจสอบและทบทวนการปฏิบัติงานขององค์กรให้สอดคล้องกับข้อกำหนดทางกฎหมาย
- ระบุขอบเขตหน้าที่และความรับผิดชอบของผู้ตรวจสอบภายนอก
- กำหนดระยะเวลาการตรวจสอบและรูปแบบการรายงานผล

สัญญาจ้างผู้ตรวจสอบภายนอก

- เอกสารสัญญาที่ระบุข้อตกลงการว่าจ้างผู้ตรวจสอบภายนอก รวมถึงวัตถุประสงค์ ขอบเขตงาน ระยะเวลาการปฏิบัติงาน และข้อกำหนดความลับข้อมูล
- ระบุข้อตกลงเกี่ยวกับการใช้เครื่องมือหรือโปรแกรมประเมินตนเองที่องค์กรหรือผู้ตรวจสอบภายนอกใช้ในการตรวจสอบ

รายงานการประเมินตนเอง (Self-assessment report)

- รายงานที่ได้จากการใช้โปรแกรมหรือเครื่องมือประเมินตนเอง เพื่อแสดงให้เห็นภาพรวมความสอดคล้องขององค์กรในเรื่องการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ
- รายงานสรุปข้อบกพร่องหรือประเด็นที่ต้องปรับปรุง พร้อมข้อเสนอแนะ

สภาพบังคับ

กฎหมายที่เกี่ยวข้อง

ปัจจุบันกฎหมายไม่ได้กำหนดข้อบังคับโดยตรงในส่วนนี้ แต่การดำเนินการตรวจสอบภายนอกถือเป็นแนวปฏิบัติที่ดีเพื่อให้มั่นใจว่าองค์กรปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

10.5.2 มีการจ้างหน่วยงานหรือผู้ตรวจสอบภายนอกอิสระเพื่อประเมินหรือให้การรับรองความสอดคล้องกับ

- 1) การคุ้มครองข้อมูลส่วนบุคคล
- 2) การรักษาความมั่นคงปลอดภัยสารสนเทศ (ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล)

สิ่งที่ต้องทำ: องค์กรมีการจ้างหน่วยงานหรือผู้ตรวจสอบภายนอกอิสระเพื่อประเมินหรือให้การรับรองความสอดคล้องกับ

- 1) การคุ้มครองข้อมูลส่วนบุคคล
- 2) การรักษาความมั่นคงปลอดภัยสารสนเทศ และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการตั้งผู้ตรวจสอบภายนอกเพื่อตรวจสอบและทบทวนการดำเนินการให้สอดคล้องกับกฎหมาย
สัญญาจ้างผู้ตรวจสอบภายนอก

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ตัวอย่างนโยบายการตั้งผู้ตรวจสอบภายนอก (External Auditor Policy)

1. วัตถุประสงค์

นโยบายนี้จัดทำขึ้นเพื่อกำหนดหลักเกณฑ์และแนวทางการว่าจ้างและบริหารจัดการผู้ตรวจสอบภายนอกอิสระ ในการตรวจสอบและทบทวนการดำเนินงานขององค์กรให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อเพิ่มความน่าเชื่อถือและความ

มั่นใจในระบบการจัดการข้อมูลขององค์กร รวมถึงป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล

2. ขอบเขต

นโยบายนี้ครอบคลุมการว่าจ้าง การปฏิบัติงาน การรายงานผล และการติดตามคำแนะนำของผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากองค์กร เพื่อประเมินและรับรองความสอดคล้องตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

3. คำนิยาม

- **ผู้ตรวจสอบภายนอก (External Auditor):** บุคคลหรือนิติบุคคลที่ได้รับการว่าจ้างจากองค์กรให้ดำเนินการตรวจสอบและประเมินระบบการคุ้มครองข้อมูลและความมั่นคงปลอดภัยสารสนเทศ
- **ข้อมูลส่วนบุคคล:** ข้อมูลใด ๆ ที่สามารถใช้ระบุตัวบุคคลได้ ตามความหมายในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- **ความมั่นคงปลอดภัยสารสนเทศ:** การป้องกันข้อมูลจากการเข้าถึง ใช้งาน หรือเปิดเผยโดยไม่ได้รับอนุญาต และการรักษาความถูกต้องของข้อมูล

4. หน้าที่และความรับผิดชอบ

ฝ่ายบริหาร

- แต่งตั้งผู้ตรวจสอบภายนอกตามนโยบาย
- จัดสรรงบประมาณและทรัพยากรที่จำเป็น
- รับรองการนำคำแนะนำไปปฏิบัติ

ผู้ตรวจสอบภายนอก

- ดำเนินการตรวจสอบตามขอบเขตที่กำหนด
- จัดทำรายงานผลการตรวจสอบพร้อมข้อเสนอแนะ
- รักษาความลับของข้อมูลที่ได้รับ

ฝ่ายที่เกี่ยวข้อง

- สนับสนุนและให้ข้อมูลที่จำเป็นแก่ผู้ตรวจสอบภายนอก
- ดำเนินการแก้ไขและปรับปรุงตามคำแนะนำ

5. หลักเกณฑ์การเลือกผู้ตรวจสอบภายนอก

- มีใบอนุญาตหรือการรับรองวิชาชีพที่เกี่ยวข้อง เช่น CISA CISM CISSP

- มีประสบการณ์ในการตรวจสอบระบบคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยสารสนเทศไม่น้อยกว่า 3 ปี
- ไม่เป็นบุคคลที่มีความขัดแย้งทางผลประโยชน์กับองค์กร
- มีความเป็นกลางและความน่าเชื่อถือสูง
- สามารถให้บริการในช่วงเวลาที่กำหนดและมีทรัพยากรพร้อม

6. ขอบเขตการตรวจสอบ

- ตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ เช่น การควบคุมการเข้าถึง การเข้ารหัสข้อมูล การสำรองข้อมูล
- ตรวจสอบกระบวนการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- ตรวจสอบนโยบายและกระบวนการภายในที่เกี่ยวข้อง
- ให้คำแนะนำเพื่อการปรับปรุงและเพิ่มประสิทธิภาพ

7. ขั้นตอนการตรวจสอบ

การเตรียมความพร้อม

- นัดหมายวันตรวจสอบ
- กำหนดขอบเขตและวัตถุประสงค์ร่วมกับฝ่ายที่เกี่ยวข้อง

การดำเนินการตรวจสอบ:

- ตรวจสอบเอกสารที่เกี่ยวข้อง เช่น นโยบาย รายงานเหตุการณ์ บันทึกการเข้าถึงระบบ
- สัมภาษณ์พนักงานที่เกี่ยวข้อง
- ทดสอบการควบคุมระบบรักษาความปลอดภัย

การจัดทำรายงาน

- สรุปผลการตรวจสอบ
- ระบุประเด็นที่พบและข้อเสนอแนะ

การติดตามผล

ติดตามการแก้ไขและปรับปรุงตามคำแนะนำ

8. การรายงานผลการตรวจสอบ

- รายงานฉบับสมบูรณ์ต้องถูกส่งให้ฝ่ายบริหารและคณะทำงานที่กำลังดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล
- รายงานต้องประกอบด้วยบทสรุปสำหรับผู้บริหาร (Executive Summary) ผลการตรวจสอบ ประเด็นบกพร่อง ข้อเสนอแนะ และแผนปฏิบัติการที่แนะนำ
- รายงานจะต้องจัดเก็บอย่างปลอดภัยและสามารถเข้าถึงได้โดยผู้มีสิทธิ์เท่านั้น

9. การรักษาความลับ

- ผู้ตรวจสอบภายนอกต้องรักษาความลับของข้อมูลทั้งหมดที่ได้รับระหว่างการตรวจสอบ
- ห้ามเผยแพร่ข้อมูลหรือรายงานใด ๆ โดยไม่ได้รับอนุญาตจากองค์กร

10. การติดตามและปรับปรุงนโยบาย

- นโยบายนี้จะได้รับการทบทวนและปรับปรุงอย่างน้อยปีละหนึ่งครั้ง
- ปรับปรุงเมื่อมีกฎหมายหรือมาตรฐานใหม่ที่เกี่ยวข้อง

ตัวอย่างสัญญาจ้างผู้ตรวจสอบภายนอก (External Auditor Contract)

สัญญาว่าจ้างผู้ตรวจสอบภายนอก

ระหว่าง

บริษัท/องค์กร [ชื่อบริษัท] (ต่อไปนี้จะเรียกว่า "ผู้ว่าจ้าง")

และ

[ชื่อผู้ตรวจสอบภายนอกหรือบริษัทตรวจสอบ] (ต่อไปนี้จะเรียกว่า "ผู้ตรวจสอบ")

วันที่ [วัน/เดือน/ปี]

ข้อตกลง

ขอบเขตงาน

ผู้ตรวจสอบตกลงที่จะดำเนินการตรวจสอบระบบการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ว่าจ้าง ตามขอบเขตและรายละเอียดที่กำหนดในภาคผนวก A

ระยะเวลาการให้บริการ

การตรวจสอบจะเริ่มตั้งแต่วันที่ [วันเริ่มต้น] และสิ้นสุดวันที่ [วันสิ้นสุด]

ค่าตอบแทน

ผู้ว่าจ้างตกลงที่จะจ่ายค่าบริการเป็นจำนวนเงิน [จำนวนเงิน] บาท โดยแบ่งจ่ายตามกำหนดในภาคผนวก B

ความลับ

ผู้ตรวจสอบจะต้องรักษาความลับของข้อมูลทั้งหมดที่ได้รับจากผู้ว่าจ้าง และจะไม่เปิดเผยต่อบุคคลที่สามโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร

ข้อกำหนดและเงื่อนไข

- ผู้ตรวจสอบต้องปฏิบัติงานตามมาตรฐานวิชาชีพและข้อกำหนดทางกฎหมาย
- ผู้ตรวจสอบต้องจัดทำรายงานสรุปผลการตรวจสอบและข้อเสนอแนะในเวลาที่กำหนด
- ผู้ตรวจสอบต้องไม่เป็นบุคคลที่มีความขัดแย้งทางผลประโยชน์กับผู้ว่าจ้าง

การสิ้นสุดสัญญา

สัญญานี้จะสิ้นสุดเมื่อผู้ตรวจสอบส่งมอบรายงานการตรวจสอบและได้รับการรับรองจากผู้ว่าจ้าง

ตัวอย่างนโยบายการตั้งผู้ตรวจสอบภายนอก (External Auditor Policy)

1. วัตถุประสงค์

นโยบายนี้จัดทำขึ้นเพื่อกำหนดหลักเกณฑ์และแนวทางการว่าจ้างและบริหารจัดการผู้ตรวจสอบภายนอกอิสระ ในการตรวจสอบและทบทวนการดำเนินงานขององค์กรให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อเพิ่มความน่าเชื่อถือและความมั่นใจในระบบการจัดการข้อมูลขององค์กร รวมถึงป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคล

2. ขอบเขต

นโยบายนี้ครอบคลุมการว่าจ้าง การปฏิบัติงาน การรายงานผล และการติดตามคำแนะนำของผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากองค์กร เพื่อประเมินและรับรองความสอดคล้องตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

3. คำนิยาม

- **ผู้ตรวจสอบภายนอก (External Auditor):** บุคคลหรือนิติบุคคลที่ได้รับการว่าจ้างจากองค์กรให้ดำเนินการตรวจสอบและประเมินระบบการคุ้มครองข้อมูลและความมั่นคงปลอดภัยสารสนเทศ
- **ข้อมูลส่วนบุคคล:** ข้อมูลใด ๆ ที่สามารถใช้ระบุตัวบุคคลได้ ตามความหมายในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- **ความมั่นคงปลอดภัยสารสนเทศ:** การป้องกันข้อมูลจากการเข้าถึง ใช้งาน หรือเปิดเผยโดยไม่ได้รับอนุญาต และการรักษาความถูกต้องของข้อมูล

4. หน้าที่และความรับผิดชอบ

ฝ่ายบริหาร

- แต่งตั้งผู้ตรวจสอบภายนอกตามนโยบาย
- จัดสรรงบประมาณและทรัพยากรที่จำเป็น
- รับรองการนำคำแนะนำไปปฏิบัติ

ผู้ตรวจสอบภายนอก

- ดำเนินการตรวจสอบตามขอบเขตที่กำหนด
- จัดทำรายงานผลการตรวจสอบพร้อมข้อเสนอแนะ
- รักษาความลับของข้อมูลที่ได้รับ

ฝ่ายที่เกี่ยวข้อง

- สนับสนุนและให้ข้อมูลที่จำเป็นแก่ผู้ตรวจสอบภายนอก
- ดำเนินการแก้ไขและปรับปรุงตามคำแนะนำ

5. หลักเกณฑ์การเลือกผู้ตรวจสอบภายนอก

- มีใบอนุญาตหรือการรับรองวิชาชีพที่เกี่ยวข้อง เช่น CISA CISM CISSP
- มีประสบการณ์ในการตรวจสอบระบบคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยสารสนเทศไม่น้อยกว่า 3 ปี
- ไม่เป็นบุคคลที่มีความขัดแย้งทางผลประโยชน์กับองค์กร
- มีความเป็นกลางและความน่าเชื่อถือสูง
- สามารถให้บริการในช่วงเวลาที่กำหนดและมีทรัพยากรพร้อม

6. ขอบเขตการตรวจสอบ

- ตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ เช่น การควบคุมการเข้าถึง การเข้ารหัสข้อมูล การสำรองข้อมูล
- ตรวจสอบกระบวนการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- ตรวจสอบนโยบายและกระบวนการภายในที่เกี่ยวข้อง
- ให้คำแนะนำเพื่อการปรับปรุงและเพิ่มประสิทธิภาพ

7. ขั้นตอนการตรวจสอบ

การเตรียมความพร้อม:

- นัดหมายวันตรวจสอบ
- กำหนดขอบเขตและวัตถุประสงค์ร่วมกับฝ่ายที่เกี่ยวข้อง

การดำเนินการตรวจสอบ:

- ตรวจสอบเอกสารที่เกี่ยวข้อง เช่น นโยบาย รายงานเหตุการณ์ บันทึกการเข้าถึงระบบ
- สัมภาษณ์พนักงานที่เกี่ยวข้อง

- ทดสอบการควบคุมระบบรักษาความปลอดภัย

การจัดทำรายงาน:

- สรุปผลการตรวจสอบ
- ระบุประเด็นที่พบและข้อเสนอแนะ

การติดตามผล

ติดตามการแก้ไขและปรับปรุงตามคำแนะนำ

8. การรายงานผลการตรวจสอบ

- รายงานฉบับสมบูรณ์ต้องถูกส่งให้ฝ่ายบริหารและคณะทำงานที่กำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล
- รายงานต้องประกอบด้วยบทสรุปสำหรับผู้บริหาร (Executive Summary) ผลการตรวจสอบ ประเด็นบกพร่อง ข้อเสนอแนะ และแผนปฏิบัติการที่แนะนำ
- รายงานจะต้องจัดเก็บอย่างปลอดภัยและสามารถเข้าถึงได้โดยผู้มีสิทธิ์เท่านั้น

9. การรักษาความลับ

- ผู้ตรวจสอบภายนอกต้องรักษาความลับของข้อมูลทั้งหมดที่ได้รับระหว่างการตรวจสอบ
- ห้ามเผยแพร่ข้อมูลหรือรายงานใด ๆ โดยไม่ได้รับอนุญาตจากองค์กร
- 10. การติดตามและปรับปรุงนโยบาย
- นโยบายนี้จะได้รับการทบทวนและปรับปรุงอย่างน้อยปีละหนึ่งครั้ง
- ปรับปรุงเมื่อมีกฎหมายหรือมาตรฐานใหม่ที่เกี่ยวข้อง

ตัวอย่างสัญญาจ้างผู้ตรวจสอบภายนอก (External Auditor Contract)

สัญญาว่าจ้างผู้ตรวจสอบภายนอก

ระหว่าง

บริษัท/องค์กร [ชื่อบริษัท] (ต่อไปนี้จะเรียกว่า "ผู้ว่าจ้าง")

และ

[ชื่อผู้ตรวจสอบภายนอกหรือบริษัทตรวจสอบ] (ต่อไปนี้จะเรียกว่า "ผู้ตรวจสอบ")

วันที่ [วัน/เดือน/ปี]

ข้อตกลง

ขอบเขตงาน

ผู้ตรวจสอบตกลงที่จะดำเนินการตรวจสอบระบบการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ว่าจ้าง ตามขอบเขตและรายละเอียดที่กำหนดในภาคผนวก A

ระยะเวลาการให้บริการ

การตรวจสอบจะเริ่มต้นตั้งแต่วันที่ [วันเริ่มต้น] และสิ้นสุดวันที่ [วันสิ้นสุด]

ค่าตอบแทน

ผู้ว่าจ้างตกลงที่จะจ่ายค่าบริการเป็นจำนวนเงิน [จำนวนเงิน] บาท โดยแบ่งจ่ายตามกำหนดในภาคผนวก B

ความลับ

ผู้ตรวจสอบจะต้องรักษาความลับของข้อมูลทั้งหมดที่ได้รับจากผู้ว่าจ้าง และจะไม่เปิดเผยต่อบุคคลที่สามโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร

ข้อกำหนดและเงื่อนไข

- ผู้ตรวจสอบต้องปฏิบัติงานตามมาตรฐานวิชาชีพและข้อกำหนดทางกฎหมาย
- ผู้ตรวจสอบต้องจัดทำรายงานสรุปผลการตรวจสอบและข้อเสนอแนะในเวลาที่กำหนด
- ผู้ตรวจสอบต้องไม่เป็นบุคคลที่มีความขัดแย้งทางผลประโยชน์กับผู้ว่าจ้าง

การสิ้นสุดสัญญา

สัญญานี้จะสิ้นสุดเมื่อผู้ตรวจสอบส่งมอบรายงานการตรวจสอบและได้รับการรับรองจากผู้ว่าจ้าง

ตัวอย่างรายงานผลการตรวจสอบ (Audit Report)

รายงานผลการตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ

ผู้ตรวจสอบ: [ชื่อผู้ตรวจสอบ]

องค์กร: [ชื่องค์กรผู้ตรวจสอบ]

วันที่ตรวจสอบ: [วัน/เดือน/ปี]

ระยะเวลาการตรวจสอบ: [วันเริ่มต้น] ถึง [วันสิ้นสุด]

บทสรุปสำหรับผู้บริหาร (Executive Summary)

การตรวจสอบครั้งนี้มีวัตถุประสงค์เพื่อประเมินความสอดคล้องขององค์กรกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ ภาพรวมพบว่าองค์กรมีการจัดการและควบคุมที่ดีในหลายด้าน แต่ยังพบประเด็นที่ควรปรับปรุงเพื่อเสริมความมั่นคงและลดความเสี่ยงจากการละเมิดข้อมูล

ขอบเขตการตรวจสอบ

1. การปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. การจัดการสิทธิ์การเข้าถึงข้อมูลส่วนบุคคลในระบบสารสนเทศ
3. การเข้ารหัสและการสำรองข้อมูล

4. การฝึกอบรมและการรับรู้เรื่องความปลอดภัยของข้อมูลของพนักงาน
5. การจัดการเหตุการณ์ละเมิดข้อมูลและการตอบสนอง

ผลการตรวจสอบ

หมวดหมู่	ผลการตรวจสอบ	ข้อเสนอแนะ
การจัดการสิทธิ์การเข้าถึง	พบว่ามีกำหนดสิทธิ์ที่เหมาะสม	ควรมีการทบทวนสิทธิ์เป็นระยะ
การเข้ารหัสข้อมูล	ใช้การเข้ารหัสที่มีมาตรฐาน	ควรเพิ่มการเข้ารหัสข้อมูลสำรอง
การสำรองข้อมูล	มีการสำรองข้อมูลประจำวัน	ควรตรวจสอบการกู้คืนข้อมูลเป็นระยะ
การฝึกอบรมพนักงาน	มีการฝึกอบรมเบื้องต้น	ควรเพิ่มความถี่และเนื้อหาการอบรม
การจัดการเหตุการณ์ละเมิดข้อมูล	มีขั้นตอนที่ชัดเจนและสามารถปฏิบัติได้จริง	ควรเพิ่มการทดสอบระบบตอบสนอง

ข้อบกพร่องและประเด็นที่ต้องปรับปรุง

1. ระบบการทบทวนสิทธิ์การเข้าถึงข้อมูลยังไม่ได้ดำเนินการอย่างสม่ำเสมอ
2. ยังไม่มีมาตรการการเข้ารหัสข้อมูลสำรองอย่างครบถ้วน
3. การอบรมพนักงานยังไม่ครอบคลุมทุกฝ่ายที่เกี่ยวข้อง
4. ระบบทดสอบตอบสนองต่อเหตุการณ์ละเมิดข้อมูลยังไม่มีดำเนินการอย่างสม่ำเสมอ

สรุปและข้อเสนอแนะเพิ่มเติม

ผู้ตรวจสอบแนะนำให้องค์กรดำเนินการทบทวนและปรับปรุงระบบการควบคุมตามข้อเสนอแนะอย่างเร่งด่วน เพื่อเสริมสร้างความมั่นคงและลดความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล รวมถึงควรจัดทำแผนการอบรมและฝึกซ้อมระบบตอบสนองต่อเหตุการณ์เพื่อให้พร้อมต่อสถานการณ์จริง

1. ภาคผนวก
2. เอกสารที่ตรวจสอบ
3. ตารางสอบถามพนักงาน
4. รายละเอียดผลการทดสอบระบบ

ภาคผนวก A: ตัวอย่างแบบฟอร์มคำขอแต่งตั้งผู้ตรวจสอบภายนอก

รายการ	รายละเอียด
ชื่อองค์กร	บริษัท ABC จำกัด
วันที่ขอแต่งตั้ง	1 มิถุนายน 2568
ชื่อผู้ตรวจสอบที่เสนอ	บริษัท ตรวจสอบมาตรฐาน จำกัด
ประสบการณ์และคุณสมบัติ	มีผู้ตรวจสอบที่ได้รับ CISA และมีประสบการณ์ 5 ปี
ขอบเขตการตรวจสอบ	ตรวจสอบระบบคุ้มครองข้อมูลและความมั่นคงปลอดภัยสารสนเทศ
ระยะเวลาการตรวจสอบ	1 เดือน (มิถุนายน 2568)
งบประมาณ	200000 บาท
ผู้ขออนุมัติ	นายสมชาย ผู้จัดการฝ่าย IT

ภาคผนวก B: แบบฟอร์มรายงานความเสี่ยงที่พบจากการตรวจสอบ (Risk Assessment Report)

หมายเลขความเสี่ยง	รายละเอียดความเสี่ยง	ผลกระทบที่คาดว่าจะเกิดขึ้น	ความรุนแรง	ข้อเสนอแนะ
RSK-001	การทบทวนสิทธิ์การเข้าถึงข้อมูลไม่สม่ำเสมอ	ข้อมูลส่วนบุคคลอาจถูกเข้าถึงโดยไม่ได้รับอนุญาต	สูง	กำหนดรอบเวลาทบทวนสิทธิ์อย่างชัดเจน
RSK-002	ขาดการเข้ารหัสข้อมูลสำรองบางส่วน	ข้อมูลสำรองอาจถูกขโมยหรือนำไปใช้โดยไม่ได้รับอนุญาต	ปานกลาง	เพิ่มมาตรการเข้ารหัสข้อมูลสำรอง

ภาคผนวกสำหรับสัญญาจ้างผู้ตรวจสอบภายนอก (External Auditor Contract)

ภาคผนวก A

ขอบเขตงานตรวจสอบ (Scope of Work)

- ตรวจสอบนโยบายและกระบวนการบริหารจัดการข้อมูลส่วนบุคคล
- ประเมินความสอดคล้องของระบบสารสนเทศกับกฎหมาย PDPA
- ตรวจสอบการควบคุมการเข้าถึงระบบและข้อมูล
- ตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยข้อมูล เช่น การเข้ารหัสและการสำรองข้อมูล
- ตรวจสอบกระบวนการจัดการเหตุการณ์ละเมิดข้อมูล

ภาคผนวก B: ตารางการชำระค่าบริการ (Payment Schedule)

งวด ที่	วันที่ชำระเงิน	จำนวนเงิน (บาท)	เงื่อนไขการชำระเงิน
1	วันที่ลงนามสัญญา	50000	ชำระล่วงหน้า 25%
2	ครึ่งทางของการตรวจสอบ	75000	หลังจากส่งรายงานเบื้องต้น
3	หลังส่งรายงานฉบับ สมบูรณ์	75000	หลังจากได้รับรายงานฉบับสมบูรณ์และ รับรอง

ภาคผนวกสำหรับรายงานผลการตรวจสอบ (Audit Report)

ภาคผนวก A: เอกสารที่ตรวจสอบ (Documents Reviewed)

หมายเลข เอกสาร	ชื่อเอกสาร	วันที่เอกสาร	หมายเหตุ
DOC-001	นโยบายคุ้มครองข้อมูล ส่วนบุคคล	1 มกราคม 2568	นโยบายเวอร์ชันล่าสุด
DOC-002	บันทึกการเข้าถึงระบบ สารสนเทศ	1 มีนาคม - 31 พฤษภาคม 2568	บันทึกการเข้าถึงผู้ใช้งาน ทั้งหมด
DOC-003	รายงานเหตุการณ์ละเมิด ข้อมูล	1 มกราคม - 31 พฤษภาคม 2568	รายงานเหตุการณ์ 3 ครั้ง

ภาคผนวก B: ตารางสอบถามพนักงาน (Employee Interview Summary)

ชื่อ พนักงาน	ตำแหน่ง	วันที่ สัมภาษณ์	ประเด็นที่สอบถาม	สรุปคำตอบ
นางสาว สมใจ	เจ้าหน้าที่ IT	15 มิถุนายน 2568	ความรู้เกี่ยวกับ PDPA และ มาตรการรักษาความปลอดภัย	มีความรู้เบื้องต้นและรับ การอบรมอย่างต่อเนื่อง
นาย สมชาย	ผู้ดูแล ระบบ	15 มิถุนายน 2568	กระบวนการเข้ารหัสและการ สำรองข้อมูล	มีการปฏิบัติตามขั้นตอน มาตรฐาน

ภาคผนวก C: รายละเอียดผลการทดสอบระบบ (System Testing Results)

การทดสอบ	วิธีการทดสอบ	ผลการทดสอบ	ข้อเสนอแนะ
ทดสอบการเข้าถึงระบบ	ทดลองเข้าถึงด้วยบัญชีผู้ใช้ต่างระดับ	ผ่าน	ควรมีการทบทวนสิทธิ์บ่อยขึ้น
ทดสอบการเข้ารหัสข้อมูล	ตรวจสอบการใช้งานโปรโตคอล TLS และ AES	ผ่าน	ควรเพิ่มการเข้ารหัสสำรองข้อมูล
ทดสอบการกู้คืนข้อมูล	จำลองสถานการณ์ข้อมูลสูญหาย	ผ่าน	ควรทดสอบบ่อยขึ้นอย่างน้อยปีละสองครั้ง

10.5.3 มีการปฏิบัติตามประมวลแนวทางปฏิบัติหรือมาตรฐานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น มาตรฐาน ISO/IEC 27001 หรือ 27701 หรือมาตรฐานที่กำหนดในอุตสาหกรรมนั้น ๆ เป็นต้น

สิ่งที่ต้องทำ: องค์กรมีการปฏิบัติตามประมวลแนวทางปฏิบัติหรือมาตรฐานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น มาตรฐาน ISO/IEC 27001 หรือ ISO/IEC 27701 หรือมาตรฐานที่กำหนดในอุตสาหกรรมนั้น ๆ อย่างครบถ้วนและมีเอกสารครบถ้วน

หลักฐาน: นโยบายการตั้งผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกเพื่อตรวจสอบและทบทวนการดำเนินการให้สอดคล้องกับกฎหมาย
สัญญาจ้างผู้ตรวจสอบภายนอก

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การปฏิบัติตามประมวลแนวทางปฏิบัติหรือมาตรฐานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล บทนำ

ในยุคดิจิทัลที่ข้อมูลส่วนบุคคลกลายเป็นสินทรัพย์ที่สำคัญขององค์กร การบริหารจัดการข้อมูลเหล่านี้ให้เป็นไปตามกฎหมายและมาตรฐานสากลถือเป็นสิ่งจำเป็น การปฏิบัติตามประมวลแนวทางปฏิบัติหรือมาตรฐานต่าง ๆ จะช่วยให้องค์กรมีความมั่นใจในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล รวมถึงสร้างความน่าเชื่อถือในสายตาลูกค้า คู่ค้า และหน่วยงานกำกับดูแล

มาตรฐานที่ได้รับการยอมรับในระดับสากลและนิยมใช้อย่างกว้างขวาง ได้แก่

ISO/IEC 27001

มาตรฐานระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System หรือ ISMS)

ISO/IEC 27701

มาตรฐานระบบการจัดการความเป็นส่วนตัวข้อมูลส่วนบุคคล (Privacy Information Management System หรือ PIMS) ที่ขยายจาก ISO/IEC 27001 มาตรฐานเหล่านี้ไม่เพียงแต่ช่วยให้องค์กรปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น PDPA ของประเทศไทย แต่ยังช่วยลดความเสี่ยงจากการละเมิดข้อมูล และเพิ่มขีดความสามารถในการแข่งขันในตลาดด้วย

หลักการปฏิบัติตามมาตรฐานที่เกี่ยวข้อง

1. การกำหนดนโยบายและความมุ่งมั่นขององค์กร

องค์กรต้องมีการกำหนดนโยบายความมั่นคงปลอดภัยข้อมูลส่วนบุคคลอย่างชัดเจน โดยนโยบายนี้ควรครอบคลุมถึงเป้าหมายการปกป้องข้อมูลส่วนบุคคล และความมุ่งมั่นของผู้บริหารระดับสูงในการจัดการความเสี่ยงด้านข้อมูลอย่างมีประสิทธิภาพ

นโยบายดังกล่าวควรระบุถึง

- การกำหนดความรับผิดชอบของบุคลากรที่เกี่ยวข้อง
- แนวทางการดำเนินการและควบคุมที่ต้องปฏิบัติ
- การให้ความรู้และฝึกอบรมแก่พนักงาน
- การทบทวนและปรับปรุงนโยบายเป็นประจำ

2. การประเมินความเสี่ยง (Risk Assessment)

องค์กรต้องดำเนินการประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอย่างละเอียด โดยการประเมินนี้ครอบคลุมถึง

- การระบุภัยคุกคามและช่องโหว่ของระบบสารสนเทศ
- การวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากการละเมิดข้อมูล
- การจัดลำดับความสำคัญของความเสี่ยงตามระดับความรุนแรง
- ผลจากการประเมินจะนำไปสู่การกำหนดมาตรการควบคุมและป้องกันที่เหมาะสมต่อความเสี่ยงนั้นๆ

3. การวางมาตรการควบคุมและการบริหารจัดการ

ตามมาตรฐาน ISO/IEC 27001 องค์กรจะต้องมีการวางมาตรการควบคุมเพื่อปกป้องข้อมูลอย่างเป็นระบบ ประกอบด้วย

- มาตรการทางเทคนิค เช่น การเข้ารหัสข้อมูล การควบคุมการเข้าถึง และการตรวจสอบการใช้งาน
- มาตรการทางกายภาพ เช่น การควบคุมการเข้าออกพื้นที่จัดเก็บข้อมูล
- มาตรการทางองค์กร เช่น การฝึกอบรมและสร้างความตระหนักรู้แก่พนักงาน
- สำหรับ ISO/IEC 27701 จะเน้นที่มาตรการควบคุมเฉพาะที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น การจัดการคำขอเข้าถึงข้อมูลของเจ้าของข้อมูล และการตรวจสอบกระบวนการประมวลผลข้อมูล

4. การติดตาม ตรวจสอบ และปรับปรุงระบบ

องค์กรต้องมีการติดตามและตรวจสอบการปฏิบัติตามนโยบายและมาตรการที่วางไว้เป็นระยะ โดยการตรวจสอบนี้อาจดำเนินการโดย

- ผู้ตรวจสอบภายใน (Internal Audit)
- ผู้ตรวจสอบภายนอก (External Audit)

10.5.4 มีการรายงานสิ่งที่ตรวจพบ (รายงานผลการตรวจสอบ) โดยหน่วยงานหรือผู้ตรวจสอบอิสระ ดังกล่าวให้ผู้ที่เกี่ยวข้องได้รับทราบ

สิ่งที่ต้องทำ: มีการรายงานสิ่งที่ตรวจพบ (รายงานผลการตรวจสอบ) โดยหน่วยงานหรือผู้ตรวจสอบอิสระ ดังกล่าวให้ผู้ที่เกี่ยวข้องได้รับทราบ และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการตั้งผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกเพื่อตรวจสอบและทบทวนการ ดำเนินการให้สอดคล้องกับกฎหมาย
สัญญาจ้างผู้ตรวจสอบภายนอก
รายงานผลการตรวจสอบภายในภายนอก

สภาพบังคับ: กฎหมายไม่ได้กำหนด

ตัวอย่างการนำมาตรฐาน ISO/IEC 27001 และ 27701 ไปใช้ในองค์กร

ขั้นตอนที่ 1: การเตรียมความพร้อมและการวางแผน

- จัดตั้งคณะทำงานบริหารความมั่นคงปลอดภัยข้อมูล (Information Security Management Committee)
- กำหนดนโยบายความมั่นคงปลอดภัยข้อมูลส่วนบุคคลและความเป็นส่วนตัว
- วางแผนโครงการดำเนินการระบบ ISMS และ PIMS รวมถึงระบุทรัพยากรและงบประมาณ

ขั้นตอนที่ 2: การประเมินสถานะปัจจุบัน (Gap Analysis)

- ตรวจสอบนโยบายและกระบวนการที่มีอยู่ในองค์กรกับข้อกำหนดของ ISO/IEC 27001 และ 27701
- ระบุช่องว่างและข้อบกพร่องที่ต้องแก้ไข

ขั้นตอนที่ 3: การดำเนินการและจัดทำเอกสาร

- พัฒนาหรือปรับปรุงนโยบาย กระบวนการ และมาตรการควบคุมตามมาตรฐาน

- จัดทำเอกสารระบบ เช่น คู่มือนโยบาย (Policy Manual) คู่มือการปฏิบัติงาน (Procedure Manual) และแบบฟอร์มต่าง ๆ
- ฝึกอบรมพนักงานทุกระดับ เพื่อสร้างความตระหนักและความรู้

ขั้นตอนที่ 4: การตรวจสอบภายในและการทบทวนโดยฝ่ายบริหาร

- ดำเนินการตรวจสอบภายในตามรอบที่กำหนด
- จัดทำรายงานผลการตรวจสอบ พร้อมข้อเสนอแนะ
- ฝ่ายบริหารพิจารณาผลการตรวจสอบและอนุมัติแผนการปรับปรุง

ขั้นตอนที่ 5: การรับรอง (Certification)

- เลือกหน่วยงานรับรองที่เป็นที่ยอมรับ
- เข้ารับการตรวจประเมินเพื่อขอรับใบรับรอง ISO/IEC 27001 และ 27701
- แก้ไขข้อบกพร่องตามคำแนะนำของผู้ตรวจประเมินจนผ่านการรับรอง

เอกสารที่ต้องจัดเก็บและหลักฐานแสดงการปฏิบัติตามมาตรฐาน

- นโยบายและคู่มือระบบบริหารจัดการความมั่นคงปลอดภัยข้อมูล (ISMS Policy and Manual)
แสดงความมุ่งมั่นขององค์กรและแนวทางการบริหารจัดการ
- รายงานประเมินความเสี่ยง (Risk Assessment Report)
แสดงผลการวิเคราะห์ความเสี่ยงและมาตรการควบคุมที่กำหนด
- บันทึกการฝึกอบรมและสร้างความตระหนัก (Training Records)
แสดงหลักฐานการให้ความรู้แก่พนักงานเกี่ยวกับ PDPA และมาตรฐาน ISO
- บันทึกการตรวจสอบภายในและภายนอก (Audit Reports)
รายงานผลการตรวจสอบทั้งภายในและภายนอก เพื่อยืนยันการปฏิบัติตามมาตรฐาน
- บันทึกการจัดการเหตุการณ์ละเมิดข้อมูล (Incident Management Records)
แสดงขั้นตอนการตอบสนองและแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- สัญญาจ้างผู้ตรวจสอบภายนอกและรายงานผลการตรวจสอบ (External Auditor Contract and Reports)
แสดงข้อตกลงและผลการประเมินความสอดคล้องกับมาตรฐาน

ประโยชน์ของการปฏิบัติตามมาตรฐาน ISO/IEC 27001 และ 27701

- ลดความเสี่ยงในการถูกโจมตีทางไซเบอร์และการละเมิดข้อมูลส่วนบุคคล
- สร้างความเชื่อมั่นแก่ลูกค้า คู่ค้า และหน่วยงานกำกับดูแล
- ช่วยให้องค์กรปฏิบัติตามกฎหมาย PDPA และข้อกำหนดด้านความเป็นส่วนตัวอื่น ๆ ได้อย่างมีประสิทธิภาพ
- ช่วยลดค่าใช้จ่ายในระยะยาวจากการจัดการเหตุการณ์ละเมิดข้อมูลและค่าปรับทางกฎหมาย

- สนับสนุนการพัฒนาองค์กรในแง่การบริหารความเสี่ยงและความยั่งยืน

สรุป

องค์กรที่ต้องการบริหารจัดการข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพควรปฏิบัติตามประมวลแนวทางปฏิบัติและมาตรฐานที่เกี่ยวข้อง เช่น ISO/IEC 27001 และ ISO/IEC 27701 เพื่อสร้างระบบบริหารจัดการความมั่นคงปลอดภัยและความเป็นส่วนตัวที่มีมาตรฐานสากล และเตรียมความพร้อมในการรับมือกับความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้น นอกจากนี้ การมีเอกสารครบถ้วนและการตั้งผู้ตรวจสอบภายในหรือภายนอกเพื่อตรวจสอบการดำเนินการอย่างสม่ำเสมอ เป็นสิ่งสำคัญเพื่อแสดงให้เห็นถึงความสอดคล้องกับกฎหมายและมาตรฐาน รวมทั้งสร้างความน่าเชื่อถือแก่ผู้มีส่วนได้เสียทุกฝ่าย

10.5.4 มีการรายงานสิ่งที่ตรวจพบ (รายงานผลการตรวจสอบ) โดยหน่วยงานหรือผู้ตรวจสอบอิสระ ดังกล่าวให้ผู้ที่เกี่ยวข้องได้รับทราบ

- สิ่งที่ต้องทำ: มีการรายงานสิ่งที่ตรวจพบ (รายงานผลการตรวจสอบ) โดยหน่วยงานหรือผู้ตรวจสอบอิสระ ดังกล่าวให้ผู้ที่เกี่ยวข้องได้รับทราบ และมีเอกสารครบถ้วน
- หลักฐาน: นโยบายการตั้งผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกเพื่อตรวจสอบและ ทบทวนการดำเนินการให้สอดคล้องกับกฎหมาย
สัญญาจ้างผู้ตรวจสอบภายนอก
รายงานผลการตรวจสอบภายในภายนอก
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

การรายงานสิ่งที่ตรวจพบ (รายงานผลการตรวจสอบ) โดยหน่วยงานหรือผู้ตรวจสอบอิสระ

บทนำ

การตรวจสอบภายในและภายนอกเป็นเครื่องมือสำคัญที่ช่วยให้องค์กรสามารถประเมินความสอดคล้องในการปฏิบัติงานตามนโยบาย กฎหมาย และมาตรฐานต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูล การรายงานผลการตรวจสอบอย่างครบถ้วน และโปร่งใสจึงเป็นสิ่งจำเป็น เพื่อให้ผู้บริหารและผู้มีส่วนได้เสียรับทราบถึงข้อค้นพบ ปัญหา และข้อเสนอแนะในการปรับปรุงแก้ไข

แม้ว่ากฎหมายในปัจจุบันจะไม่ได้กำหนดให้ต้องมีการรายงานผลตรวจสอบอย่างชัดเจน แต่การปฏิบัติตามแนวปฏิบัตินี้ช่วยสร้างความน่าเชื่อถือและความมั่นใจในระบบบริหารจัดการขององค์กรอย่างยั่งยืน

สิ่งที่ต้องทำ

- กำหนดนโยบายการตั้งผู้ตรวจสอบภายในและ/หรือผู้ตรวจสอบภายนอก เพื่อดำเนินการตรวจสอบระบบ การปฏิบัติงาน หรือโครงการที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
- ดำเนินการตรวจสอบตามขอบเขตและความถี่ที่เหมาะสม เช่น ตรวจสอบรายไตรมาสหรือรายปี
- จัดทำรายงานผลการตรวจสอบที่ชัดเจน ครบถ้วน และเป็นกลาง ซึ่งรายงานต้องระบุรายละเอียดดังนี้
- วัตถุประสงค์ของการตรวจสอบ
- ขอบเขตและวิธีการตรวจสอบ
- ข้อค้นพบและประเด็นที่น่าสังเกต
- ความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
- ข้อเสนอแนะเพื่อการปรับปรุงแก้ไข
- ส่งมอบรายงานให้แก่ผู้บริหารระดับสูงและผู้เกี่ยวข้อง เพื่อให้เกิดการติดตามแก้ไขอย่างจริงจัง
- เก็บรักษารายงานและเอกสารที่เกี่ยวข้องอย่างเป็นระบบ เพื่อเป็นหลักฐานการปฏิบัติตามและรองรับการตรวจสอบภายใน/ภายนอกในอนาคต

แนวทางการจัดทำรายงานผลการตรวจสอบ

โครงสร้างรายงาน

หน้าปก (Cover Page)

- ชื่อรายงาน
- ชื่อหน่วยงานหรือบริษัทตรวจสอบ
- วันที่ตรวจสอบและวันที่จัดทำรายงาน

สารบัญ (Table of Contents)

บทสรุปสำหรับผู้บริหาร (Executive Summary)

- สรุปภาพรวมข้อค้นพบหลักและข้อเสนอแนะสำคัญ

วัตถุประสงค์ของการตรวจสอบ (Objective of the Audit)

- อธิบายเหตุผลและเป้าหมายของการตรวจสอบ

ขอบเขตและวิธีการตรวจสอบ (Scope and Methodology)

- ขอบเขตของระบบหรือกิจกรรมที่ตรวจสอบ
- วิธีการ เช่น การสัมภาษณ์ การตรวจสอบเอกสาร การทดสอบระบบ เป็นต้น

ข้อค้นพบและประเด็นสำคัญ (Findings and Key Issues)

- ระบุข้อผิดพลาดหรือจุดอ่อน
- วิเคราะห์ผลกระทบและความเสี่ยงที่เกี่ยวข้อง

ข้อเสนอแนะ (Recommendations)

- เสนอแนะแนวทางการแก้ไขและปรับปรุง

บทสรุปและข้อคิดเห็นเพิ่มเติม (Conclusion and Additional Remarks)

ภาคผนวก (Appendices)

- เอกสารอ้างอิง ตารางผลการตรวจสอบ ตัวอย่างเอกสารที่ตรวจ เป็นต้น
- ตัวอย่างนโยบายการตั้งผู้ตรวจสอบภายในและภายนอก

นโยบายการตั้งผู้ตรวจสอบเพื่อการบริหารจัดการข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อให้มั่นใจว่าองค์กรมีการบริหารจัดการข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพและเป็นไปตามข้อกำหนดของกฎหมายและมาตรฐานที่เกี่ยวข้อง โดยการดำเนินการตรวจสอบอย่างสม่ำเสมอและมีระบบ

ขอบเขต

ครอบคลุมการตรวจสอบการดำเนินงานของหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการเก็บรวบรวม ประมวลผล และรักษาความปลอดภัยของข้อมูลส่วนบุคคล

บทบาทและความรับผิดชอบ

- กำหนดให้มีผู้ตรวจสอบภายในที่มีความรู้ความสามารถและเป็นอิสระในการประเมินการปฏิบัติงาน
- กรณีที่จำเป็น องค์กรสามารถจ้างผู้ตรวจสอบภายนอกที่มีความเชี่ยวชาญเฉพาะด้านเพื่อเสริมสร้างความมั่นใจ
- ผู้ตรวจสอบมีหน้าที่รายงานผลการตรวจสอบต่อผู้บริหารและคณะกรรมการตรวจสอบ

กระบวนการตรวจสอบ

- กำหนดแผนการตรวจสอบประจำปี
- ดำเนินการตรวจสอบตามแผน
- จัดทำรายงานผลการตรวจสอบอย่างละเอียด
- ติดตามผลการดำเนินงานแก้ไขตามข้อเสนอแนะ

ตัวอย่างสัญญาจ้างผู้ตรวจสอบภายนอก

สัญญาจ้างที่ปรึกษาหรือผู้ตรวจสอบภายนอก

ทำขึ้น ณ วันที่ ระหว่าง

บริษัท/องค์กร (ซึ่งต่อไปนี้จะเรียกว่า "ผู้ว่าจ้าง")

กับ

ผู้ตรวจสอบภายนอก (ซึ่งต่อไปนี้จะเรียกว่า "ผู้รับจ้าง")

ข้อกำหนดและเงื่อนไข

ขอบเขตงาน

ผู้รับจ้างจะทำการตรวจสอบระบบและกระบวนการบริหารจัดการข้อมูลส่วนบุคคลของผู้ว่าจ้าง เพื่อประเมินความสอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง

ระยะเวลาการให้บริการ

ตั้งแต่วันที่ ถึงวันที่

ค่าตอบแทน

ลงกันที่จำนวน บาท (.....)

การรายงาน

ผู้รับจ้างต้องจัดทำรายงานผลการตรวจสอบอย่างละเอียดและส่งให้ผู้ว่าจ้างภายในระยะเวลาที่กำหนด

ความลับ

ผู้รับจ้างต้องเก็บรักษาข้อมูลและความลับของผู้ว่าจ้างอย่างเคร่งครัด

เงื่อนไขอื่น ๆ

(ระบุเพิ่มเติมตามความเหมาะสม เช่น การแก้ไขรายงาน การประชุมติดตามผล ฯลฯ)

ลงชื่อ (ผู้ว่าจ้าง)

ลงชื่อ (ผู้รับจ้าง)

ตัวอย่างรายงานผลการตรวจสอบภายใน

รายงานผลการตรวจสอบระบบบริหารจัดการข้อมูลส่วนบุคคล

บริษัท

วันที่ตรวจสอบ
ผู้ตรวจสอบ
1. วัตถุประสงค์ ประเมินความสอดคล้องของระบบบริหารจัดการข้อมูลส่วนบุคคลกับกฎหมาย PDPA และมาตรฐาน ISO/IEC 27001 และ 27701 2. ขอบเขต ตรวจสอบระบบรักษาความปลอดภัยข้อมูล การจัดการคำขอข้อมูล และการอบรมพนักงาน 3. วิธีการตรวจสอบ - สัมภาษณ์ผู้รับผิดชอบระบบ - ตรวจสอบเอกสารและบันทึกการอบรม - ทดสอบระบบควบคุมการเข้าถึงข้อมูล 4. ข้อค้นพบ - พบว่าการควบคุมการเข้าถึงข้อมูลยังมีจุดอ่อนที่ควรปรับปรุง - การอบรมพนักงานยังไม่ครอบคลุมทุกแผนก 5. ข้อเสนอแนะ - ปรับปรุงระบบควบคุมการเข้าถึงข้อมูลด้วยการเพิ่มการตรวจสอบสิทธิ์แบบสองขั้นตอน - จัดอบรมเพิ่มเติมให้ครบทุกแผนกภายในไตรมาสหน้า 6. สรุป องค์กรมีความตั้งใจในการบริหารจัดการข้อมูลส่วนบุคคลอย่างดี แต่ควรเร่งแก้ไขข้อบกพร่องเพื่อให้สอดคล้องมาตรฐานและกฎหมาย

10.5.5 มีการจัดทำและดำเนินการตามแผนการปรับปรุงจากรายงานผลการตรวจสอบดังกล่าว

สิ่งที่ต้องทำ: มีการจัดทำและดำเนินการตามแผนการปรับปรุงจากรายงานผลการตรวจสอบ

ครบถ้วน

หลักฐาน: นโยบายการปรับปรุงตามผลรายงานการตรวจสอบ

รายงานผลการตรวจสอบ

แผนการปรับปรุงตามรายงานผลการตรวจสอบ

รายงานผลการตรวจสอบครั้งที่ 2 (ถ้ามี)

แผนการปรับปรุงตามรายงานผลการตรวจสอบครั้งที่ 2 และรายงานผลการตรวจสอบครั้งที่ 3 (ถ้ามี)

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การจัดทำและดำเนินการตามแผนการปรับปรุงจากรายงานผลการตรวจสอบ

บทนำ

หลังจากได้รับรายงานผลการตรวจสอบ ซึ่งเป็นการประเมินและวิเคราะห์ข้อบกพร่องหรือจุดที่ควรปรับปรุงในการบริหารจัดการข้อมูลส่วนบุคคล องค์กรต้องจัดทำแผนการปรับปรุงที่ชัดเจนและมีขั้นตอนการดำเนินงาน พร้อมทั้งติดตามและประเมินผลการดำเนินงานอย่างต่อเนื่อง เพื่อให้มั่นใจว่าการปรับปรุงแก้ไขเป็นไปตามเป้าหมายและช่วยเสริมสร้างความมั่นคงปลอดภัยของข้อมูลอย่างยั่งยืน

ถึงแม้ว่ากฎหมายจะไม่ได้กำหนดให้ต้องจัดทำและดำเนินการแผนการปรับปรุงนี้อย่างเป็นทางการ แต่การมีบริหารจัดการที่ดี รวมถึงการจัดทำแผนปรับปรุงและติดตามผลเป็นแนวปฏิบัติที่สำคัญในการพัฒนาองค์กรให้ตอบสนองต่อความเสี่ยงและข้อค้นพบได้อย่างมีประสิทธิภาพ

สิ่งที่ต้องทำ

- จัดทำแผนการปรับปรุงจากรายงานผลการตรวจสอบ โดยระบุรายละเอียดของข้อบกพร่องที่ต้องแก้ไข วัตถุประสงค์ของการปรับปรุง กิจกรรมหรือมาตรการที่ต้องดำเนินการ ผู้รับผิดชอบ และระยะเวลาดำเนินการ
- ดำเนินการตามแผนการปรับปรุงอย่างเคร่งครัดตามกรอบเวลาที่กำหนด
- จัดทำรายงานผลการติดตามการดำเนินงานหรือรายงานผลการตรวจสอบซ้ำ (ถ้ามี) เพื่อประเมินความก้าวหน้าและประสิทธิผลของการปรับปรุง
- หากมีการตรวจสอบครั้งที่ 2 หรือ 3 ให้จัดทำแผนการปรับปรุงตามผลการตรวจสอบเหล่านั้นและติดตามผลอย่างต่อเนื่อง
- เก็บรักษาเอกสารทุกขั้นตอน ได้แก่ รายงานผลการตรวจสอบ แผนการปรับปรุง รายงานผลการติดตามเป็นหลักฐานการปฏิบัติ
- นำเสนอข้อมูลและรายงานให้ผู้บริหารหรือผู้เกี่ยวข้องได้รับทราบอย่างสม่ำเสมอ เพื่อการตัดสินใจและสนับสนุนทรัพยากรในการปรับปรุง

แนวทางการจัดทำแผนการปรับปรุง

โครงสร้างแผนการปรับปรุง

ชื่อแผนและวันที่จัดทำ

ที่มาของแผน

อ้างอิงจากรายงานผลการตรวจสอบฉบับที่

วัตถุประสงค์ของแผน

ข้อบกพร่องหรือปัญหาที่ต้องแก้ไข

กิจกรรม/มาตรการการปรับปรุง

- รายละเอียดกิจกรรม
- ผู้รับผิดชอบ
- ระยะเวลาเริ่มต้น – สิ้นสุด

ทรัพยากรที่จำเป็น**ตัวชี้วัดความสำเร็จ (KPIs)****รายงานผลการติดตาม**

- วันที่ติดตาม
- สถานะ (ดำเนินการแล้ว/อยู่ระหว่างดำเนินการ/ยังไม่ดำเนินการ)
- หมายเหตุหรือปัญหาที่พบ

ลงชื่อผู้รับผิดชอบจัดทำแผน**ตัวอย่างนโยบายการปรับปรุงตามรายงานผลการตรวจสอบ****นโยบายการปรับปรุงระบบบริหารจัดการข้อมูลส่วนบุคคลตามรายงานผลการตรวจสอบ****วัตถุประสงค์**

เพื่อให้มั่นใจว่าองค์กรมีการดำเนินการแก้ไขและปรับปรุงระบบบริหารจัดการข้อมูลส่วนบุคคลอย่างต่อเนื่องและเป็นระบบ ตามผลการตรวจสอบจากผู้ตรวจสอบภายในและภายนอก

นโยบาย

- องค์กรจะจัดทำแผนการปรับปรุงจากข้อค้นพบในรายงานผลการตรวจสอบทุกฉบับภายในระยะเวลาที่กำหนด
- แผนการปรับปรุงต้องระบุรายละเอียดของกิจกรรม ผู้รับผิดชอบ และระยะเวลาอย่างชัดเจน
- ผู้บริหารหน่วยงานที่เกี่ยวข้องต้องสนับสนุนและจัดสรรทรัพยากรที่จำเป็นเพื่อให้การปรับปรุงดำเนินไปอย่างมีประสิทธิภาพ
- มีการติดตามและรายงานความก้าวหน้าในการดำเนินงานอย่างสม่ำเสมอ และจัดทำรายงานผลการตรวจสอบซ้ำตามความจำเป็น
- เอกสารทั้งหมดเกี่ยวกับการปรับปรุงและติดตามผลจะต้องเก็บรักษาไว้อย่างเป็นระบบและพร้อมให้ตรวจสอบได้

ตัวอย่างแผนการปรับปรุงตามรายงานผลการตรวจสอบ

ข้อบกพร่อง/ ประเด็น	กิจกรรม ปรับปรุง	ผู้รับผิดชอบ	ระยะเวลา ดำเนินการ	ตัวชี้วัด ความสำเร็จ	สถานะ/ หมายเหตุ

ระบบควบคุมการเข้าถึงข้อมูลยังไม่สมบูรณ์	พัฒนาระบบยืนยันตัวตนแบบสองขั้นตอน (2FA)	ฝ่าย IT Security	1 ก.ค. 2568 – 31 ส.ค. 2568	การทดสอบระบบ 100% ผ่านการยืนยันตัวตน	อยู่ระหว่างดำเนินการ
การอบรมพนักงานไม่ครอบคลุมทุกแผนก	จัดอบรมเพิ่มเติมสำหรับแผนกขายและบริการลูกค้า	ฝ่ายทรัพยากรบุคคล	15 ก.ค. 2568 – 15 ก.ย. 2568	พนักงานเข้าร่วมอบรมครบ 95%	ยังไม่ดำเนินการ

ตัวอย่างรายงานผลการติดตามการปรับปรุง (รายงานผลการตรวจสอบครั้งที่ 2)

รายงานผลการติดตามแผนการปรับปรุงระบบบริหารจัดการข้อมูลส่วนบุคคล

บริษัท

วันที่รายงาน

ผู้ตรวจสอบติดตาม

สรุปความก้าวหน้า

- ระบบยืนยันตัวตนแบบสองขั้นตอนพัฒนาสำเร็จและทดสอบเสร็จสิ้นในวันที่ 30 ส.ค. 2568
- การอบรมพนักงานในแผนกขายและบริการลูกค้ากำลังอยู่ในระหว่างดำเนินการ คาดว่าจะเสร็จภายในวันที่ 15 ก.ย. 2568

สถานะการดำเนินการ

กิจกรรม	สถานะ	หมายเหตุ
ระบบยืนยันตัวตนสองขั้นตอน	เสร็จสมบูรณ์	ผ่านการทดสอบแล้ว
การอบรมพนักงาน	กำลังดำเนินการ	มีพนักงานเข้าร่วมอบรม 60%

ข้อเสนอแนะ

- ควรเร่งดำเนินการอบรมให้แล้วเสร็จตามกำหนด
- จัดทำแผนติดตามความปลอดภัยของระบบอย่างต่อเนื่อง

สรุป

การจัดทำและดำเนินการตามแผนการปรับปรุงจากรายงานผลการตรวจสอบเป็นกระบวนการที่ช่วยให้องค์กรสามารถแก้ไขข้อบกพร่องและพัฒนาระบบบริหารจัดการข้อมูลส่วนบุคคลได้อย่างเป็นระบบ

และต่อเนื่อง มีส่วนสำคัญในการลดความเสี่ยงทางกฎหมายและเพิ่มความน่าเชื่อถือในสายตาของผู้เกี่ยวข้องและผู้มีส่วนได้เสีย

10.6 โปรแกรมการตรวจสอบภายใน (Internal audit programme)

หากองค์กรมีขั้นตอนการตรวจสอบภายใน ขั้นตอนดังกล่าวครอบคลุมถึงด้านการคุ้มครองข้อมูลส่วนบุคคลและการจัดการข้อมูล

10.6.1 มีการทดสอบความได้ผลของมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

สิ่งที่ต้องทำ: มีการทดสอบความได้ผลของมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร และมีเอกสารครบถ้วน

หลักฐาน: นโยบายกำหนดการทดสอบความได้ผลของมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

แผนทดสอบความได้ผลของมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

รายงานผลการตรวจสอบทดสอบมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การทดสอบความได้ผลของมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

ความสำคัญ

การทดสอบความได้ผลของมาตรการคุ้มครองข้อมูลส่วนบุคคลเป็นขั้นตอนสำคัญเพื่อยืนยันว่าองค์กรได้ดำเนินการตามนโยบายและมาตรฐานที่วางไว้ และมาตรการเหล่านั้นสามารถป้องกันและลดความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้จริง การทดสอบนี้จะช่วยค้นหาจุดอ่อนหรือช่องโหว่ของระบบความปลอดภัย และช่วยให้องค์กรสามารถปรับปรุงมาตรการต่าง ๆ ให้เหมาะสมกับสถานการณ์ปัจจุบัน

สิ่งที่ต้องทำ

– กำหนดนโยบายและแนวทางการทดสอบ

องค์กรควรกำหนดนโยบายเกี่ยวกับการทดสอบมาตรการคุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจน เพื่อสร้างกรอบแนวทางที่ทุกฝ่ายต้องปฏิบัติตาม

– จัดทำแผนการทดสอบมาตรการคุ้มครองข้อมูลส่วนบุคคล

ทดสอบควรระบุขอบเขต วิธีการทดสอบ กิจกรรมที่จะทำ รายละเอียดมาตรการที่ต้องทดสอบ ผู้รับผิดชอบ และระยะเวลาการดำเนินการ

– ดำเนินการทดสอบตามแผนที่วางไว้

การทดสอบอาจเป็นได้ทั้งเชิงเทคนิค เช่น การทดสอบระบบ IT (penetration test vulnerability assessment) หรือเชิงบริหาร เช่น การสัมภาษณ์ การตรวจสอบเอกสาร และการทบทวนการปฏิบัติงาน

– **บันทึกผลการทดสอบและวิเคราะห์**

ผลการทดสอบจะต้องถูกบันทึกอย่างละเอียด พร้อมการวิเคราะห์เพื่อประเมินระดับความเสี่ยงและประสิทธิผลของมาตรการนั้น ๆ

– **จัดทำรายงานผลการตรวจสอบและนำเสนอ**

รายงานควรรายงานผลที่ได้อย่างชัดเจน รวมถึงข้อเสนอแนะสำหรับการปรับปรุง เพื่อให้ผู้บริหารและผู้เกี่ยวข้องได้รับทราบและดำเนินการต่อไป

หลักฐานที่ควรมี

นโยบายกำหนดการทดสอบความได้ผลของมาตรการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

เอกสารนโยบายที่ระบุแนวทางและความสำคัญของการทดสอบ รวมถึงบทบาทหน้าที่ของผู้เกี่ยวข้อง

แผนทดสอบความได้ผลของมาตรการคุ้มครองข้อมูลส่วนบุคคล

แผนที่ระบุขอบเขตและวิธีการทดสอบ พร้อมกำหนดระยะเวลาการดำเนินงาน

รายงานผลการตรวจสอบทดสอบมาตรการคุ้มครองข้อมูลส่วนบุคคล

รายงานที่สรุปผลการทดสอบ รายละเอียดของข้อบกพร่องหรือจุดที่ต้องปรับปรุง และข้อเสนอแนะ

ตัวอย่างนโยบายกำหนดการทดสอบความได้ผลของมาตรการคุ้มครองข้อมูลส่วนบุคคล

นโยบายการทดสอบมาตรการคุ้มครองข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อให้มั่นใจว่ามาตรการคุ้มครองข้อมูลส่วนบุคคลที่องค์กรได้นำมาใช้มีประสิทธิภาพและสามารถป้องกันความเสี่ยงที่เกี่ยวข้องได้อย่างเหมาะสม

ขอบเขต

ครอบคลุมมาตรการด้านเทคโนโลยี กระบวนการ และการปฏิบัติงานที่เกี่ยวข้องกับการจัดการและปกป้องข้อมูลส่วนบุคคลในองค์กร

บทบาทและความรับผิดชอบ

- ฝ่ายตรวจสอบภายในและ/หรือผู้ตรวจสอบภายนอก รับผิดชอบดำเนินการทดสอบตามแผน
- ผู้บริหารแต่ละหน่วยงานรับผิดชอบให้ความร่วมมือและสนับสนุนการทดสอบ
- ฝ่าย IT Security ดูแลและสนับสนุนข้อมูลทางเทคนิคที่เกี่ยวข้อง

การดำเนินการ

- กำหนดแผนการทดสอบและจัดตารางเวลาทดสอบเป็นประจำ
- ดำเนินการทดสอบตามวิธีการที่เหมาะสมกับประเภทของมาตรการ
- รายงานผลการทดสอบให้ผู้บริหารทราบพร้อมข้อเสนอแนะเพื่อการปรับปรุง

การทบทวนและปรับปรุงนโยบาย

- นโยบายนี้จะถูกทบทวนและปรับปรุงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีความจำเป็น

ตัวอย่างแผนทดสอบความได้ผลของมาตรการคุ้มครองข้อมูลส่วนบุคคล (Audit Test Plan)

รายการทดสอบ	วิธีการทดสอบ	ขอบเขต/หน่วยงาน	ผู้รับผิดชอบ	กำหนดเวลาดำเนินการทดสอบ	หมายเหตุ
การควบคุมการเข้าถึงระบบ	Penetration Test Access Review	ฝ่าย IT Security	ทีมตรวจสอบภายใน	1-15 ก.ค. 2568	ทดสอบระบบสำคัญ 5 ระบบ
การเก็บรักษาข้อมูล	ตรวจสอบนโยบายและการปฏิบัติ	ฝ่ายสารสนเทศและการจัดเก็บข้อมูล	ทีมตรวจสอบภายใน	16-20 ก.ค. 2568	ตรวจสอบการสำรองข้อมูล
การอบรมและรับรู้	สัมภาษณ์และตรวจเอกสารอบรม	ฝ่ายทรัพยากรบุคคล	ทีมตรวจสอบภายใน	21-25 ก.ค. 2568	ตรวจสอบอบรมพนักงาน

ตัวอย่างรายงานผลการตรวจสอบทดสอบมาตรการคุ้มครองข้อมูลส่วนบุคคล

รายงานผลการตรวจสอบมาตรการคุ้มครองข้อมูลส่วนบุคคล

บริษัท

วันที่

ผู้ตรวจสอบ

1. วัตถุประสงค์ของการตรวจสอบ

ประเมินประสิทธิผลของมาตรการคุ้มครองข้อมูลส่วนบุคคลที่องค์กรได้ดำเนินการตามนโยบายและมาตรฐานที่กำหนด

2. ขอบเขตการตรวจสอบ

รวมถึงมาตรการทางเทคนิค การบริหารจัดการ และการสร้างความตระหนักรู้ของพนักงาน

3. กิจกรรมทดสอบที่ดำเนินการ

- ทดสอบการควบคุมการเข้าถึงระบบด้วย Penetration Test
- ตรวจสอบการจัดเก็บข้อมูลและนโยบายการสำรองข้อมูล
- ตรวจสอบการอบรมและการรับรู้ของพนักงาน

4. ผลการตรวจสอบ

หมวดมาตรการ	รายละเอียดผลการตรวจสอบ	ผลการประเมิน	ข้อเสนอแนะ
การควบคุมการเข้าถึงระบบ	พบช่องโหว่บางจุดในระบบการยืนยันตัวตน	ต้องแก้ไข	แนะนำเพิ่มการยืนยันตัวตนแบบ 2FA
การเก็บรักษาข้อมูล	การสำรองข้อมูลทำตามนโยบายอย่างเคร่งครัด	ดี	ควรมีการทดสอบกู้คืนข้อมูลประจำปี
การอบรมและรับรู้	พนักงานส่วนใหญ่เข้าร่วมอบรมและรับรู้ดี	ดี	ควรเพิ่มอบรมซ้ำเป็นระยะ

5. สรุป

มาตรการส่วนใหญ่มีประสิทธิภาพดี แต่ยังมีบางประเด็นที่ต้องปรับปรุงโดยเร่งด่วนตามข้อเสนอแนะที่ระบุไว้

10.6.2 มีการตรวจสอบการปฏิบัติตามของพนักงานต่อนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

สิ่งที่ต้องทำ: องค์กรมีการตรวจสอบการปฏิบัติตามของพนักงานต่อนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล และมีเอกสารครบถ้วน

หลักฐาน: นโยบายกำหนดการทดสอบการปฏิบัติตามของพนักงานต่อนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
รายงานผลการตรวจสอบทดสอบมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
เกณฑ์การตรวจสอบมาตรการการปฏิบัติตามของพนักงานต่อนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

สภาพบังคับ: กฎหมายไม่ได้กำหนด

การตรวจสอบการปฏิบัติตามของพนักงานต่อนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ความสำคัญ

การตรวจสอบการปฏิบัติตามของพนักงานต่อนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นการประเมินความสอดคล้องและความมีวินัยของพนักงานในการรักษามาตรฐานด้านความปลอดภัยข้อมูลส่วนบุคคล เพื่อป้องกันความผิดพลาด ความประมาทเลินเล่อ หรือการละเมิดที่อาจส่งผลกระทบต่อข้อมูลและความเชื่อมั่นขององค์กร รวมทั้งช่วยให้องค์กรสามารถปรับปรุงกระบวนการอบรมและกำกับดูแลได้อย่างเหมาะสม

สิ่งที่ต้องทำ

- กำหนดนโยบายการตรวจสอบการปฏิบัติตามของพนักงาน
ระบุแนวทางและความสำคัญของการตรวจสอบ เพื่อให้พนักงานทุกคนรับทราบและปฏิบัติตามอย่างเคร่งครัด
- จัดทำเกณฑ์การตรวจสอบมาตรการการปฏิบัติตามของพนักงาน
กำหนดตัวชี้วัดหรือเกณฑ์ชัดเจนที่ใช้ประเมินความสอดคล้องในการปฏิบัติงาน เช่น การปฏิบัติตามขั้นตอน การใช้ระบบ การรักษาความลับ เป็นต้น
- ดำเนินการตรวจสอบตามแผนที่กำหนด
ตรวจสอบได้ทั้งในรูปแบบการสัมภาษณ์ สังเกตการณ์ การสุ่มตรวจเอกสาร หรือการใช้ระบบ IT Audit เพื่อตรวจจับพฤติกรรมที่ไม่สอดคล้อง
- จัดทำรายงานผลการตรวจสอบ
บันทึกผลการตรวจสอบ ระบุข้อพบเห็น จุดที่ต้องแก้ไข และข้อเสนอแนะสำหรับพัฒนา
- ติดตามและแก้ไขปัญหา
ดำเนินการแก้ไขตามข้อเสนอแนะ และติดตามผลการปรับปรุงอย่างต่อเนื่อง

หลักฐานที่ควรมี

- นโยบายกำหนดการทดสอบการปฏิบัติตามของพนักงานต่อนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
เอกสารนโยบายที่ชัดเจนระบุหน้าที่การตรวจสอบและความรับผิดชอบ
- รายงานผลการตรวจสอบทดสอบมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
รายงานที่สรุปผลการตรวจสอบพฤติกรรมและการปฏิบัติตามของพนักงาน
- เกณฑ์การตรวจสอบมาตรการการปฏิบัติตามของพนักงานต่อนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
เอกสารที่แสดงตัวชี้วัดหรือเกณฑ์การประเมิน เช่น แบบฟอร์มตรวจสอบ หรือ checklist

ตัวอย่างนโยบายกำหนดการตรวจสอบการปฏิบัติตามของพนักงาน

นโยบายตรวจสอบการปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อให้มั่นใจว่าพนักงานทุกคนปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลขององค์กรอย่างเคร่งครัด

ขอบเขต

ครอบคลุมพนักงานทุกระดับและหน่วยงานที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคล

บทบาทและความรับผิดชอบ

- ฝ่ายตรวจสอบภายใน รับผิดชอบดำเนินการตรวจสอบและรายงานผล
- ผู้จัดการและหัวหน้าหน่วยงาน รับผิดชอบให้พนักงานปฏิบัติตามนโยบาย
- ฝ่ายทรัพยากรบุคคล สนับสนุนการอบรมและประเมินผลพนักงาน

วิธีการตรวจสอบ

- สุ่มตรวจสอบเอกสารและการปฏิบัติงาน
- การสัมภาษณ์และสอบถามพนักงาน
- การวิเคราะห์ข้อมูลและรายงานการใช้งานระบบ

การรายงานและติดตามผล

- จัดทำรายงานสรุปผลและข้อเสนอแนะ
- ติดตามการแก้ไขปัญหาอย่างต่อเนื่อง

ตัวอย่างเกณฑ์การตรวจสอบมาตรการการปฏิบัติตามของพนักงาน

หมวดเกณฑ์ตรวจสอบ	รายละเอียด	วิธีการตรวจสอบ
การปฏิบัติตามนโยบายความปลอดภัยข้อมูล	พนักงานปฏิบัติตามขั้นตอนที่กำหนดไว้	ตรวจเอกสาร สัมภาษณ์
การรักษาความลับข้อมูลส่วนบุคคล	ไม่มีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	สังเกตการณ์ ระบบบันทึก
การใช้ระบบสารสนเทศ	เข้าถึงระบบตามสิทธิ์ที่กำหนด	ตรวจสอบระบบและบันทึกกิจกรรม
การอบรมและรับรู้เกี่ยวกับ PDPA	พนักงานเข้าร่วมอบรมตามที่กำหนด	ตรวจสอบรายชื่ออบรม

10.6.3 มีการติดตามและประเมินการปฏิบัติตามนโยบายและแนวปฏิบัติอย่างไม่เป็นทางการ ทั้งแบบเฉพาะกิจและเฉพาะจุดอย่างสม่ำเสมอ

- สิ่งที่ต้องทำ: องค์กรมีการติดตามและประเมินการปฏิบัติตามนโยบายและแนวปฏิบัติอย่างไม่เป็นทางการ ทั้งแบบเฉพาะกิจและเฉพาะจุดอย่างสม่ำเสมอ และมีเอกสารครบถ้วน
- หลักฐาน: นโยบายการติดตามและประเมินอย่างไม่เป็นทางการ ทั้งแบบเฉพาะกิจและเฉพาะจุดอย่างสม่ำเสมอ แบบแจ้งผลการทดสอบหรือการฝ่าฝืนมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร รายงานผลการตรวจสอบทดสอบมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

การติดตามและประเมินการปฏิบัติตามนโยบายและแนวปฏิบัติอย่างไม่เป็นทางการ ทั้งแบบเฉพาะกิจและเฉพาะจุดอย่างสม่ำเสมอ

ความสำคัญของการติดตามและประเมินแบบไม่เป็นทางการ

การติดตามและประเมินการปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลอย่างไม่เป็นทางการ เป็นกระบวนการที่ช่วยให้องค์กรสามารถตรวจสอบสถานการณ์ปัจจุบันได้อย่างรวดเร็ว และยืดหยุ่นกว่าแบบเป็นทางการ โดยไม่จำเป็นต้องรอการตรวจสอบหรือประเมินผลในรูปแบบรายงานอย่างเป็นทางการเพียงอย่างเดียว

การติดตามแบบไม่เป็นทางการมีความสำคัญเนื่องจาก

- ช่วยจับจุดที่อาจเกิดปัญหาหรือความเสี่ยงในเวลาที่ยรวดเร็ว (Real-time monitoring)
- สนับสนุนการแก้ไขปัญหาเฉพาะหน้าก่อนที่จะลุกลาม
- ช่วยให้ฝ่ายบริหารและผู้เกี่ยวข้องรับทราบสถานการณ์จริงอย่างต่อเนื่อง
- ส่งเสริมวัฒนธรรมองค์กรที่ตื่นตัวและพร้อมรับผิดชอบต่อการคุ้มครองข้อมูลส่วนบุคคล
- สามารถทำได้ง่ายและไม่เป็นภาระมากนัก เมื่อเทียบกับการตรวจสอบอย่างเป็นทางการ

สิ่งที่ต้องทำ

1. กำหนดนโยบายและแนวทางการติดตามและประเมินอย่างไม่เป็นทางการ

องค์กรควรจัดทำนโยบายที่ชัดเจนเกี่ยวกับการติดตามและประเมินการปฏิบัติงานในลักษณะนี้ เพื่อให้พนักงานและผู้เกี่ยวข้องเข้าใจกรอบและวิธีการดำเนินการ

กำหนดความถี่และช่วงเวลาที่เหมาะสมสำหรับการติดตาม ทั้งแบบเฉพาะกิจ (ad-hoc) และเฉพาะจุด (spot check)

กำหนดบุคคลหรือหน่วยงานที่รับผิดชอบดำเนินการติดตาม และวิธีการรายงานผล

2. การดำเนินการติดตามและประเมินแบบเฉพาะกิจ

ดำเนินการติดตามในช่วงเวลาหรือกรณีที่พบความเสี่ยงหรือข้อสงสัย เช่น มีเหตุการณ์ความผิดปกติ การร้องเรียน หรือมีข้อมูลว่ามาตรการอาจถูกละเมิด

ใช้วิธีการเช่น การสัมภาษณ์ การสังเกตการณ์ การตรวจสอบเอกสาร หรือการทดสอบระบบเบื้องต้น

3. การดำเนินการติดตามและประเมินแบบเฉพาะจุด

ดำเนินการสุ่มตรวจหรือเลือกจุดตรวจสอบที่สำคัญ เช่น พนักงานกลุ่มเสี่ยง กระบวนการจัดการ ข้อมูลที่สำคัญ หรือระบบ IT ที่มีข้อมูลส่วนบุคคล

การตรวจสอบแบบเฉพาะจุดช่วยเน้นย้ำการปฏิบัติตามและส่งเสริมการรักษามาตรฐาน

4. การจัดทำเอกสารและรายงานผล

จัดทำแบบฟอร์มหรือเอกสารแจ้งผลการทดสอบ การประเมิน หรือพบการฝ่าฝืนมาตรการ รายงานผลการติดตามให้ผู้บริหารและผู้เกี่ยวข้องรับทราบ เพื่อใช้เป็นข้อมูลประกอบการตัดสินใจ กรณีพบข้อผิดพลาดหรือการฝ่าฝืน ควรมีข้อเสนอแนะและแผนการแก้ไขที่ชัดเจน

5. การนำผลการติดตามไปใช้ประโยชน์

นำผลการติดตามไปปรับปรุงนโยบาย แนวปฏิบัติ และมาตรการคุ้มครองข้อมูล

ใช้เป็นฐานข้อมูลสำหรับเตรียมการตรวจสอบภายในแบบเป็นทางการในอนาคต

ส่งเสริมวัฒนธรรมการทำงานที่รับผิดชอบด้านข้อมูลส่วนบุคคลในองค์กร

หลักฐานที่ควรมี

ชนิดเอกสาร	รายละเอียดตัวอย่าง
นโยบายการติดตามและประเมินอย่างไม่เป็นทางการ	ระบุขอบเขต วิธีการ ความถี่ และความรับผิดชอบในการติดตาม
แบบแจ้งผลการทดสอบหรือการฝ่าฝืน มาตรการ	ฟอร์มรายงานผลการติดตามแบบเฉพาะกิจหรือเฉพาะจุด พร้อมผลการประเมิน
รายงานผลการตรวจสอบทดสอบมาตรการ คุ้มครองข้อมูล	สรุปผลภาพรวมของการติดตามที่ทำอย่างต่อเนื่อง

ตัวอย่างโครงสร้างนโยบายการติดตามและประเมินแบบไม่เป็นทางการ

นโยบายการติดตามและประเมินการปฏิบัติงานด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างไม่เป็นทางการ วัตถุประสงค์

เพื่อส่งเสริมการปฏิบัติตามนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง และทันการณ์ ผ่านการติดตามและประเมินแบบไม่เป็นทางการ

ขอบเขต

ครอบคลุมพนักงานและระบบที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคลในองค์กร

ความรับผิดชอบ

- ฝ่ายตรวจสอบภายในและฝ่ายความปลอดภัยสารสนเทศ รับผิดชอบดำเนินการติดตาม
- ผู้จัดการแต่ละหน่วยงานรับผิดชอบติดตามในพื้นที่ความรับผิดชอบของตน
- ฝ่ายทรัพยากรบุคคลสนับสนุนด้านการสื่อสารและอบรม

วิธีการดำเนินการ

- การติดตามแบบเฉพาะกิจ: ดำเนินการเมื่อตรวจพบความเสี่ยงหรือข้อสงสัย
- การติดตามแบบเฉพาะจุด: ดำเนินการสุ่มตรวจตามแผนที่วางไว้
- การเก็บรวบรวมข้อมูลจากหลากหลายแหล่ง เช่น เอกสาร ระบบ และสัมภาษณ์

การรายงานผล

- รายงานผลการติดตามต้องจัดทำและส่งให้ผู้บริหารรับทราบอย่างสม่ำเสมอ
- ในกรณีพบการฝ่าฝืน ต้องแจ้งและเสนอแนวทางแก้ไขทันที

การติดตามผลและปรับปรุง

- ผลการติดตามจะนำมาใช้ในการปรับปรุงนโยบายและมาตรการให้มีประสิทธิภาพยิ่งขึ้น

ตัวอย่างแบบฟอร์มแจ้งผลการติดตามแบบเฉพาะกิจ

รายละเอียด	ข้อมูล
วันที่ดำเนินการติดตาม	1 มิถุนายน 2568
ผู้ดำเนินการติดตาม	นางสาวสมใจ ใจดี
จุดที่ติดตาม	การเข้าถึงระบบฐานข้อมูลลูกค้า
ผลการติดตาม	พบพนักงาน 2 ราย ใช้รหัสผ่านร่วมกับผู้อื่น
ข้อเสนอแนะ	แจ้งเตือนพนักงานและจัดอบรมเรื่องความปลอดภัยข้อมูล
การติดตามแก้ไข	ดำเนินการแก้ไขแล้วภายใน 7 วัน

10.6.4 การติดตามและประเมินการปฏิบัติตามนโยบายและแนวปฏิบัติมีความเป็นกลาง โดยผู้ตรวจสอบ
ต้องไม่ใช่ผู้กำหนดนโยบายหรือบังคับใช้นโยบาย

- สิ่งที่ต้องทำ: องค์กรมีการติดตามและประเมินการปฏิบัติตามนโยบายและแนวปฏิบัติอย่างเป็นกลาง โดยผู้ตรวจสอบภายในไม่ใช่ผู้กำหนดนโยบายหรือบังคับใช้นโยบาย และมีเอกสารครบถ้วน
- หลักฐาน: นโยบายการติดตามและประเมินการปฏิบัติตามนโยบายและแนวปฏิบัติมีความเป็นกลาง
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. บทนำ

การปกป้องข้อมูลส่วนบุคคลเป็นภารกิจสำคัญของทุกองค์กรในยุคข้อมูลข่าวสาร การกำหนดนโยบาย แนวปฏิบัติ และกระบวนการตรวจสอบการปฏิบัติตามจึงเป็นสิ่งจำเป็น โดยเฉพาะเมื่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของประเทศไทยได้มีผลบังคับใช้อย่างสมบูรณ์ องค์กรจำเป็นต้องพัฒนาและประเมินผลกระบวนการควบคุมภายในเพื่อให้มั่นใจได้ว่ามาตรการที่ใช้มีประสิทธิภาพและเป็นไปตามข้อกำหนดของกฎหมาย

เอกสารฉบับนี้จัดทำขึ้นเพื่อกำหนดแนวทางปฏิบัติสำหรับหัวข้อ 10.6.4 ที่ระบุว่า "การติดตามและประเมินการปฏิบัติตามนโยบายและแนวปฏิบัติมีความเป็นกลาง โดยผู้ตรวจสอบต้องไม่ใช่ผู้กำหนดนโยบายหรือบังคับใช้นโยบาย" ครอบคลุมทั้งหลักการ รูปแบบ ขั้นตอน และตัวอย่างเอกสารประกอบที่สามารถใช้งานได้จริง

2. หลักการตรวจสอบภายในอย่างเป็นกลาง

2.1 การตรวจสอบภายในต้องมีลักษณะเป็นอิสระและปราศจากอิทธิพลจากหน่วยงานที่ถูกตรวจสอบ เพื่อให้ผลการประเมินมีความน่าเชื่อถือและนำไปใช้ในการปรับปรุงอย่างแท้จริง

2.2 ผู้ตรวจสอบต้องไม่อยู่ภายใต้สายบังคับบัญชาของผู้บริหารหรือเจ้าหน้าที่ที่เป็นผู้กำหนดนโยบายหรือบังคับใช้นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลโดยตรง

2.3 องค์กรควรกำหนดนโยบายและจัดตั้งหน่วยตรวจสอบภายในที่มีโครงสร้างเป็นอิสระ โดยรายงานตรงต่อคณะกรรมการตรวจสอบหรือระดับผู้บริหารสูงสุดเท่านั้น

3. โครงสร้างองค์กรที่สนับสนุนความเป็นกลางของผู้ตรวจสอบ

3.1 คณะกรรมการตรวจสอบ (Audit Committee) เป็นผู้กำกับดูแลหน่วยตรวจสอบภายใน

3.2 หน่วยตรวจสอบภายใน (Internal Audit Unit) มีบทบาทในการประเมินความเสี่ยงและทบทวนมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคล

3.3 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีหน้าที่กำหนดนโยบายและแนวปฏิบัติ แต่ไม่เป็นผู้ตรวจสอบนโยบายของตนเอง

4. ขอบเขตการตรวจสอบภายในด้านการคุ้มครองข้อมูลส่วนบุคคล

4.1 ตรวจสอบการปฏิบัติตามนโยบายการเก็บ ใช้ เปิดเผย และโอนข้อมูลส่วนบุคคลของพนักงานและหน่วยงาน

4.2 ประเมินความสอดคล้องกับกฎหมาย PDPA และแนวปฏิบัติตามมาตรฐาน ISO/IEC 27001 และ 27701

4.3 ตรวจสอบความเหมาะสมและประสิทธิภาพของมาตรการควบคุมด้านเทคนิคและองค์กร

5.ขั้นตอนการตรวจสอบ

5.1 การวางแผนการตรวจสอบ

กำหนดวัตถุประสงค์ ขอบเขต ระยะเวลา และทรัพยากร

ประสานงานกับหน่วยงานที่เกี่ยวข้อง

5.2 การจัดเก็บและวิเคราะห์ข้อมูล

ศึกษาเอกสารนโยบาย กฎหมายที่เกี่ยวข้อง และขั้นตอนการดำเนินงาน

สัมภาษณ์พนักงานและผู้รับผิดชอบ

5.3 การประเมินการปฏิบัติจริง

ตรวจสอบการใช้งานระบบสารสนเทศ การเข้าถึงข้อมูล และการจัดเก็บข้อมูลส่วนบุคคล

5.4 การสรุปผลและจัดทำรายงาน

- ระบุข้อค้นพบ ข้อเสนอแนะ และแนวทางการปรับปรุง

- เสนอรายงานต่อผู้มีอำนาจและผู้มีส่วนได้ส่วนเสีย

6.ตัวอย่างเอกสารประกอบ

6.1 นโยบายการประเมินความเป็นกลางของผู้ตรวจสอบ

[แนบเอกสาร: ประกาศแต่งตั้งผู้ตรวจสอบภายใน ระบุเงื่อนไขการเป็นอิสระจากสายการบังคับบัญชาด้านนโยบาย]

6.2 แบบฟอร์มบันทึกผลการตรวจสอบการปฏิบัติตามนโยบาย

[แนบเอกสาร: Audit Checklist ที่ครอบคลุมนโยบายการคุ้มครองข้อมูล]

6.3 รายงานผลการตรวจสอบ (Internal Audit Report)

[แนบตัวอย่าง: รายงานที่สรุปข้อค้นพบเกี่ยวกับการปฏิบัติงานที่ไม่เป็นไปตาม PDPA พร้อมแนวทางการแก้ไข และลำดับความสำคัญ]

7.แนวทางการพัฒนาอย่างต่อเนื่อง

7.1 ทบทวนกระบวนการตรวจสอบทุก 6 เดือน และปรับให้สอดคล้องกับแนวทางของสำนักงานคุ้มครองข้อมูลส่วนบุคคล และมาตรฐาน ISO ที่อัปเดต

7.2 จัดการอบรมผู้ตรวจสอบภายในด้านกฎหมาย PDPA และจริยธรรมของวิชาชีพตรวจสอบ

7.3 จัดให้มีการประเมินผลการปฏิบัติงานของหน่วยตรวจสอบภายในจากหน่วยงานภายนอก

8.บทสรุป

การติดตามและประเมินการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นกลางเป็นหัวใจสำคัญของระบบการควบคุมภายในที่มีประสิทธิภาพ โดยการแยกบทบาทของผู้กำหนดนโยบายและผู้

ตรวจสอบออกจากรันจะช่วยให้ผลการตรวจสอบมีความน่าเชื่อถือ เป็นที่ยอมรับ และสามารถใช้ขับเคลื่อนการปรับปรุงได้อย่างแท้จริง

องค์กรควรจัดให้มีนโยบาย เอกสารหลักฐาน และการจัดการที่สอดคล้องกับแนวทางข้างต้นเพื่อเสริมสร้างวัฒนธรรมการคุ้มครองข้อมูลส่วนบุคคลที่ยั่งยืน

10.6.5 มีแผนการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ

สิ่งที่ต้องทำ: องค์กรมีแผนการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ และมีเอกสารครบถ้วน

หลักฐาน: นโยบายกำหนดการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ

รายงานผลการตรวจสอบทดสอบมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
เกณฑ์การตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย
สารสนเทศ

สภาพบังคับ: กฎหมายไม่ได้กำหนด

นโยบายกำหนดการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ
(Policy for Data Protection and Information Security Audit)

๑. บทนำ

ในยุคดิจิทัลที่การประมวลผลข้อมูลส่วนบุคคลและการใช้เทคโนโลยีสารสนเทศมีความสำคัญต่อการดำเนินงานขององค์กร การกำหนดนโยบายและมาตรการในการตรวจสอบ (Audit) และทดสอบ (Testing) ด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ จึงมีความจำเป็นอย่างยิ่ง ทั้งนี้เพื่อสร้างความเชื่อมั่นให้แก่เจ้าของข้อมูล (Data Subject) ผู้มีส่วนได้ส่วนเสีย (Stakeholders) และหน่วยงานกำกับดูแล (Regulators) ว่าองค์กรมีการดำเนินการที่โปร่งใส มีประสิทธิภาพ และสอดคล้องกับกฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) ได้กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง หรือการเปิดเผยโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย ขณะเดียวกันกฎระเบียบสากล เช่น General Data Protection Regulation (GDPR) ของสหภาพยุโรป ก็ได้เน้นย้ำถึงความสำคัญของ Accountability และการทำ Data Protection Impact Assessment (DPIA) ตลอดจนการตรวจสอบและทดสอบระบบอย่างสม่ำเสมอ

ดังนั้น องค์กรจึงได้กำหนดนโยบายฉบับนี้ขึ้น เพื่อเป็นกรอบการดำเนินงานที่ชัดเจน ครอบคลุมทั้งด้านกฎหมาย ด้านเทคนิค และด้านการบริหารจัดการ

๒. วัตถุประสงค์

เพื่อกำหนดแนวทางการตรวจสอบและทดสอบมาตรการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบ

เพื่อประเมินความเหมาะสมและประสิทธิผลของมาตรการที่องค์กรใช้อยู่ และปรับปรุงให้สอดคล้องกับกฎหมาย มาตรฐานสากล และความเสี่ยงที่เปลี่ยนแปลงไป

เพื่อเสริมสร้างความเชื่อมั่นให้แก่เจ้าของข้อมูลส่วนบุคคล ลูกค้า พนักงาน ผู้ให้บริการ และคู่ค้า ว่าข้อมูลที่องค์กรดูแลมีความปลอดภัย

เพื่อสนับสนุนหลักการบริหารความเสี่ยง (Risk Management) และการกำกับดูแลที่ดี (Good Governance) ขององค์กร

เพื่อจัดให้มีแผนการแก้ไขปรับปรุง (Corrective Action Plan: CAP) หากพบข้อบกพร่อง เพื่อให้เกิดการปรับปรุงอย่างต่อเนื่อง (Continuous Improvement)

๓. ขอบเขต

นโยบายนี้ครอบคลุม:

ระบบงาน กระบวนการทำงาน และข้อมูลทุกประเภทที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล บุคลากรทุกระดับขององค์กร ไม่ว่าจะเป็นพนักงานประจำ ลูกจ้างชั่วคราว หรือผู้รับจ้างภายนอก ผู้ให้บริการภายนอก (Processor / Third Party) ที่มีการเข้าถึงหรือประมวลผลข้อมูลส่วนบุคคลในนามขององค์กร

โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure) เช่น เซิร์ฟเวอร์ เครือข่าย ฐานข้อมูล อุปกรณ์พกพา และระบบคลาวด์

การดำเนินงานทั้งในและนอกประเทศ หากมีการประมวลผลข้อมูลของบุคคลที่อยู่ในสหภาพยุโรปหรือประเทศอื่นที่มีกฎหมายด้านข้อมูลส่วนบุคคลเฉพาะ

๔. นโยบายหลัก

ความถี่ในการตรวจสอบ

ต้องมีการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง โดยอาจเพิ่มความถี่ขึ้นตามความเสี่ยงหรือเหตุการณ์ที่เกิดขึ้น เช่น กรณีมีเหตุการณ์ข้อมูลรั่วไหล

ขอบเขตการตรวจสอบ

ครอบคลุมการปฏิบัติตาม PDPA, GDPR และกฎหมายอื่นที่เกี่ยวข้อง

ครอบคลุมการตรวจสอบทั้งด้านเอกสาร กระบวนการ และระบบเทคนิค

การทดสอบระบบความมั่นคงปลอดภัยสารสนเทศ

ต้องมีการทำ Penetration Test และ Vulnerability Assessment อย่างน้อยปีละ ๑ ครั้ง โดยบุคคลภายนอกที่มีความเชี่ยวชาญ

ต้องมีการทดสอบแผนตอบสนองเหตุการณ์ (Incident Response Plan) อย่างน้อยปีละ ๑ ครั้ง

รายงานผลการตรวจสอบ

ต้องจัดทำรายงานผลการตรวจสอบและนำเสนอผู้บริหารสูงสุดภายใน ๓๐ วันหลังเสร็จสิ้นการตรวจสอบ
รายงานต้องระบุความเสี่ยง ระดับผลกระทบ และข้อเสนอแนะที่ชัดเจน

แผนการแก้ไขปรับปรุง (CAP)

หากพบข้อบกพร่องต้องจัดทำ CAP โดยกำหนดผู้รับผิดชอบ ระยะเวลา และตัวชี้วัดความสำเร็จ

ต้องมีการติดตามและรายงานความคืบหน้าอย่างสม่ำเสมอ

๕. หลักการและมาตรฐานสากลที่เกี่ยวข้อง

ISO/IEC 27001: Information Security Management System (ISMS) – กำหนดกรอบมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ

ISO/IEC 27701: Privacy Information Management System (PIMS) – ขยายจาก ISMS

ครอบคลุมการคุ้มครองข้อมูลส่วนบุคคล

NIST Cybersecurity Framework (CSF) – ใช้เป็นแนวทางการประเมินความเสี่ยงและการจัดการด้าน Cybersecurity

GDPR Article 32 – กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสม

PDPA มาตรา 37 – กำหนดให้ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย

๖. กระบวนการตรวจสอบ

การวางแผนการตรวจสอบ (Audit Planning)

กำหนดขอบเขต วัตถุประสงค์ และระยะเวลา

ระบุทรัพยากรที่ใช้ เช่น บุคลากร งบประมาณ และเครื่องมือ

การเก็บข้อมูล (Information Gathering)

รวบรวมเอกสารนโยบาย ระเบียบ คู่มือการทำงาน

สัมภาษณ์ผู้เกี่ยวข้อง ตรวจสอบระบบ และทบทวน Log

การวิเคราะห์และประเมินผล (Analysis and Evaluation)

ประเมินความสอดคล้องกับกฎหมายและมาตรฐาน

ประเมินความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินงาน

การจัดทำรายงาน (Reporting)

จัดทำรายงานที่มีความชัดเจน แบ่งเป็น จุดแข็ง ข้อบกพร่อง และข้อเสนอแนะ

การติดตามผล (Follow-up)

ตรวจสอบความคืบหน้าของการแก้ไขตาม CAP

จัดทำรายงานติดตามผลเพื่อเสนอผู้บริหาร

๗. บทบาทและความรับผิดชอบ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Committee)

มีหน้าที่กำหนดนโยบายและติดตามการตรวจสอบ

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

มีหน้าที่กำกับดูแลการดำเนินการ ตรวจสอบความสอดคล้อง และเป็นผู้ประสานงาน

ฝ่ายตรวจสอบภายใน (Internal Audit)

มีหน้าที่วางแผนและดำเนินการตรวจสอบเชิงลึก

ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)

มีหน้าที่สนับสนุนการทดสอบระบบและดำเนินการมาตรการด้านความมั่นคงปลอดภัย

ผู้บริหารสูงสุด (Top Management)

มีหน้าที่อนุมัติรายงานและสนับสนุนทรัพยากร

๘. การรายงานและการบันทึก

รายงานผลการตรวจสอบทุกครั้งต้องถูกเก็บรักษาเป็นหลักฐานอย่างน้อย ๕ ปี

ต้องสามารถนำเสนอให้หน่วยงานกำกับดูแลตรวจสอบได้ตามความจำเป็น

ต้องมีการบันทึกสถานะการแก้ไขและติดตามผลอย่างเป็นระบบ

๙. การปรับปรุงนโยบาย

นโยบายฉบับนี้ต้องมีการทบทวนอย่างน้อยทุก ๒ ปี หรือเมื่อมีกฎหมายหรือสถานการณ์ใหม่ ๆ ที่มีผลกระทบ

การปรับปรุงนโยบายต้องได้รับความเห็นชอบจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและผู้บริหารสูงสุด

๑๐. บทสรุป

นโยบายการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ ถือเป็นหนึ่งในเครื่องมือสำคัญในการสร้างความเชื่อมั่นและความรับผิดชอบต่อองค์กร การดำเนินการตามนโยบายนี้จะทำให้องค์กรสามารถลดความเสี่ยง ป้องกันความเสียหาย และสร้างมาตรฐานการทำงานที่สอดคล้องกับกฎหมายและมาตรฐานสากล

รายงานผลการตรวจสอบและทดสอบมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

(Audit and Testing Report on Data Protection and Information Security Measures)

๑. ข้อมูลทั่วไปของรายงาน

หน่วยงานผู้ตรวจสอบ: คณะทำงานตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Audit Committee)

ระยะเวลาการตรวจสอบ: xx/xx/256x – xx/xx/256x

วัตถุประสงค์ของการตรวจสอบ:

- ๑) เพื่อตรวจสอบการปฏิบัติตามนโยบายและมาตรการคุ้มครองข้อมูลส่วนบุคคล (Compliance with Data Protection Policy and SOP)
- ๒) เพื่อทดสอบประสิทธิภาพของระบบความมั่นคงปลอดภัยสารสนเทศ (Information Security Systems)
- ๓) เพื่อระบุข้อบกพร่อง ความเสี่ยง และช่องโหว่ (Vulnerabilities and Risks) ที่อาจก่อให้เกิดผลกระทบต่อเจ้าของข้อมูล (Data Subjects)
- ๔) เพื่อเสนอข้อเสนอแนะเชิงปรับปรุง (Corrective Actions & Recommendations) ให้ผู้บริหารพิจารณา

๒. ขอบเขตการตรวจสอบ

การตรวจสอบครอบคลุมหัวข้อหลัก ดังนี้

การปฏิบัติตามนโยบายและ SOP การใช้สิทธิของเจ้าของข้อมูล

การจัดทำคู่มือขั้นตอน (Standard Operating Procedures: SOP) สำหรับสิทธิในการเข้าถึง (Right of Access), สิทธิในการแก้ไข (Right to Rectification), สิทธิในการลบ (Right to Erasure), สิทธิในการคัดค้าน (Right to Object) และสิทธิอื่น ๆ ตามกฎหมาย

การมีช่องทางรับคำขอ เช่น แบบฟอร์ม (Forms) หรือระบบออนไลน์ (Online Request System)

ระยะเวลาการตอบคำขอ (Service Level Agreement: SLA)

การเก็บ รักษา ใช้ และเปิดเผยข้อมูลส่วนบุคคล

ความเหมาะสมของการกำหนดวัตถุประสงค์ (Purpose Limitation)

การเก็บข้อมูลเท่าที่จำเป็น (Data Minimization)

การกำหนดระยะเวลาเก็บรักษา (Data Retention Policy)

การกำหนดสิทธิ์การเข้าถึง (Access Control)

การจัดเก็บและส่งข้อมูล (Storage & Transmission Security)

การบริหารสิทธิ์การเข้าถึงข้อมูล (Access Control Management)

การกำหนดผู้ใช้งานและสิทธิ์ (User Accounts & Roles)

การใช้รหัสผ่าน (Password Policy)

การตรวจสอบ Log การใช้งาน (Log Monitoring)

การยกเลิกสิทธิ์เมื่อพ้นงานลาออก (Termination of Access Rights)

ระบบป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention: DLP)

การควบคุมการโอนย้ายข้อมูล (Data Transfer Control)

การใช้เครื่องมือ DLP Software/Tools

การกำหนดนโยบายการใช้สื่อเก็บข้อมูลภายนอก (USB, External Drive)

การทดสอบระบบสารสนเทศด้านความปลอดภัย

การทดสอบเจาะระบบ (Penetration Testing)

การประเมินช่องโหว่ (Vulnerability Assessment)

การทดสอบแผนตอบสนองเหตุการณ์ (Incident Response Test)

การจำลองสถานการณ์ภัยไซเบอร์ (Cybersecurity Simulation Exercise)

๓. วิธีการตรวจสอบ (Methodology)

คณะทำงานได้ดำเนินการตรวจสอบโดยใช้วิธีการดังต่อไปนี้

การทบทวนเอกสาร (Document Review)

นโยบาย (Policy), ระเบียบ (Regulation), มาตรการ (Measures), SOP, คู่มือการทำงาน (Manuals)

สัญญากับผู้ให้บริการภายนอก (Third-Party Agreements)

การสัมภาษณ์บุคลากร (Staff Interviews)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เจ้าหน้าที่ไอที (IT Security Officer)

ผู้บริหารระดับหน่วยงานที่เกี่ยวข้อง

การสังเกตและลงพื้นที่ (Observation & Site Visit)

ห้องศูนย์ข้อมูล (Data Center)

พื้นที่สำนักงาน

ระบบควบคุมการเข้าออก (Access Control Systems)

การทดสอบทางเทคนิค (Technical Testing)

การสแกนช่องโหว่ (Vulnerability Scan)

การทดสอบเจาะระบบ (Penetration Test)

การทดสอบการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access Attempt)

๔. ผลการตรวจสอบ (Findings)

๔.๑ การปฏิบัติตามนโยบายและ SOP การใช้สิทธิของเจ้าของข้อมูล

ข้อค้นพบ:

มีการจัดทำ SOP แยกประเภทสิทธิไว้ครบถ้วน แต่ยังพบว่าบางคำขอใช้สิทธิ (เช่น สิทธิในการโอนย้าย

ข้อมูล: Data Portability) ไม่มีแบบฟอร์มเฉพาะ → ส่งผลให้ขั้นตอนการปฏิบัติไม่เป็นมาตรฐาน

ข้อเสนอแนะ:

จัดทำแบบฟอร์มและระบบรับคำขอให้ครบทุกสิทธิ และกำหนด SLA ชัดเจนไม่เกิน ๓๐ วัน (ตาม PDPA และ GDPR)

๔.๒ การเก็บ รักษา ใช้ และเปิดเผยข้อมูลส่วนบุคคล

ข้อค้นพบ:

พบการเก็บข้อมูลบางประเภทเกินระยะเวลาที่จำเป็น (Data Retention Overdue) โดยไม่มีการทบทวนประจำปี

การจัดเก็บ Log File ไม่ครบถ้วนและไม่มีการกำหนด Retention Period ชัดเจน

ไม่มีระบบเข้ารหัส (Encryption) สำหรับข้อมูลที่จัดเก็บในอุปกรณ์พกพา

ข้อเสนอแนะ:

ปรับปรุง Data Retention Policy ให้สอดคล้องกับความจำเป็นทางธุรกิจและกฎหมาย

กำหนด Log Retention อย่างน้อย ๑ ปี

ใช้เทคโนโลยีเข้ารหัส (Encryption) และการควบคุมการเข้าถึง (Access Control)

๔.๓ การบริหารสิทธิ์การเข้าถึงข้อมูล (Access Control)

ข้อค้นพบ:

สิทธิ์การเข้าถึงของพนักงานที่ลาออกบางรายยังไม่ได้ถูกยกเลิกทันที

Password Policy กำหนดขั้นต่ำ ๖ ตัวอักษร ซึ่งต่ำกว่ามาตรฐานสากล (ควรอย่างน้อย ๘-๑๒ ตัวอักษร และมีอักขรพิเศษ)

ข้อเสนอแนะ:

ปรับกระบวนการ Termination of Access Rights ให้เป็นอัตโนมัติ (Automated De-provisioning)
ปรับปรุง Password Policy ให้สอดคล้องกับมาตรฐาน NIST

๔.๔ ระบบป้องกันการรั่วไหลของข้อมูล (DLP)**ข้อค้นพบ:**

ยังไม่มีการใช้ DLP Tools ในการตรวจจับการส่งข้อมูลออกทางอีเมลหรือระบบ Cloud
มีการใช้ USB Drive ส่วนตัวในบางหน่วยงาน → เสี่ยงต่อการรั่วไหล

ข้อเสนอแนะ:

จัดหาและติดตั้ง DLP Solution
กำหนดนโยบายห้ามใช้สื่อเก็บข้อมูลภายนอก (USB Policy) หรือให้เข้ารหัสทุกครั้ง

๔.๕ การทดสอบระบบสารสนเทศด้านความปลอดภัย**ข้อค้นพบ:**

มีการทำ Penetration Test ปีละครั้ง แต่ไม่ได้ทดสอบ Incident Response Plan
Firewall และ Antivirus อยู่ในระดับเพียงพอ แต่ไม่มีระบบตรวจจับภัยคุกคามขั้นสูง (Intrusion Detection System: IDS)

ข้อเสนอแนะ:

เพิ่มการทดสอบ Incident Response และ Cyber Drill อย่างน้อยปีละครั้ง
พิจารณาจัดหาระบบ IDS/IPS (Intrusion Detection/Prevention System)

๕. การให้คะแนนผลการตรวจสอบ

การปฏิบัติตามนโยบายและ SOP: ๘๐% (อยู่ในเกณฑ์ดี แต่ขาดบางสิทธิ์)

การเก็บรักษาข้อมูล: ๗๐% (ต้องปรับ Data Retention และ Log)

Access Control: ๖๕% (ต้องปรับปรุงการยกเลิกสิทธิ์และ Password Policy)

DLP: ๖๐% (ยังไม่มีระบบตรวจจับรั่วไหลอย่างจริงจัง)

การทดสอบระบบ: ๗๕% (มีการทดสอบพื้นฐาน แต่ยังขาด Cyber Drill)

สรุปภาพรวม: ระดับ “เหมาะสม” (Adequate) แต่ยังมี ประเด็นสำคัญที่ต้องเร่งปรับปรุง

๖. ข้อเสนอแนะ (Recommendations)

จัดทำ Corrective Action Plan (CAP) ครอบคลุมทุกข้อบกพร่อง

กำหนด Timeline และผู้รับผิดชอบที่ชัดเจน

ติดตามผลการแก้ไขทุก ๓ เดือน

จัดทำ Internal Audit ซ้ำใน ๖ เดือน

ทบทวนและอัปเดตนโยบาย (Policy Review) อย่างน้อยปีละครั้ง

๗. สรุปและข้อพิจารณาของผู้บริหาร

จากการตรวจสอบ พบว่าองค์กรมีมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศที่ “เหมาะสม” และสามารถใช้งานได้จริงในระดับหนึ่ง แต่ยังคงต้องปรับปรุงในเรื่อง

Data Retention, Log Management, Access Control, DLP, และ Incident

Response หากดำเนินการปรับปรุงตามข้อเสนอแนะ คาดว่าจะสามารถยกระดับการคุ้มครองข้อมูลให้สอดคล้องกับ PDPA, GDPR และมาตรฐานสากล (ISO/IEC 27001, ISO/IEC 27701, NIST CSF) ได้ดียิ่งขึ้น

เกณฑ์การตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ

(Audit Criteria for Data Protection and Information Security)

บทนำ

ในปัจจุบัน ข้อมูลส่วนบุคคล (Personal Data) ถือเป็นทรัพยากรที่มีคุณค่าสูงทั้งต่อองค์กรและต่อบุคคลเจ้าของข้อมูล การบริหารจัดการข้อมูลดังกล่าวจึงจำเป็นต้องอาศัยมาตรการที่มีประสิทธิภาพ โปร่งใส และสอดคล้องกับกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (Personal Data Protection Act: PDPA) ของประเทศไทย รวมถึงกฎระเบียบสากลอย่าง General Data Protection Regulation (GDPR) ของสหภาพยุโรป

การตรวจสอบ (Audit) จึงเป็นกลไกสำคัญในการประเมินว่า องค์กรได้มีมาตรการที่เหมาะสมหรือไม่ ทั้งด้านกฎหมาย การปฏิบัติงาน กระบวนการทางเทคนิค และการบริหารจัดการ โดยมีวัตถุประสงค์เพื่อ

ทำให้มั่นใจว่ามีการปฏิบัติตามกฎหมาย (Compliance)

ลดความเสี่ยงจากการรั่วไหลหรือการใช้ข้อมูลในทางที่ผิด (Data Breach, Misuse)

สร้างความเชื่อมั่นให้แก่เจ้าของข้อมูลและผู้มีส่วนได้ส่วนเสีย (Stakeholders)

ปรับปรุงมาตรการและกระบวนการให้ทันสมัยต่อเนื่อง

๑. ด้านกฎหมายและการกำกับดูแล (Compliance)

การตรวจสอบด้านนี้มุ่งเน้นที่ความสอดคล้องกับกฎหมายและกฎระเบียบทั้งภายในและภายนอกองค์กร หากองค์กรขาดการกำกับดูแลที่ชัดเจน จะเสี่ยงต่อการถูกดำเนินการทางกฎหมายและเสียความน่าเชื่อถือ

๑.๑ นโยบายความเป็นส่วนตัว (Privacy Policy) และประกาศความเป็นส่วนตัว (Privacy Notice)

ต้องมีการจัดทำเอกสารนโยบายที่ชัดเจน ครอบคลุมวัตถุประสงค์ของการเก็บ ใช้ เผยแพร่ข้อมูล

เนื้อหาต้องใช้ภาษาที่เข้าใจง่าย (Plain Language) และเข้าถึงได้

ต้องมีการทบทวนและอัปเดตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของกฎหมายหรือเทคโนโลยี

๑.๒ การเก็บบันทึกคำขอใช้สิทธิ (Data Subject Rights Request Log)

ต้องมีระบบที่บันทึกคำขอ เช่น การขอเข้าถึง (Access Request) การลบ (Right to Erasure) หรือการคัดค้าน (Right to Object)

ต้องสามารถตรวจสอบย้อนหลังได้ว่าการตอบสนองตาม SLA (Service Level Agreement) ที่กำหนด

๑.๓ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

ต้องมีการแต่งตั้ง DPO อย่างเป็นทางการหากเข้าข่ายตามกฎหมาย

DPO ต้องมีอิสระในการทำงานและรายงานตรงต่อผู้บริหารสูงสุด

ต้องได้รับการฝึกอบรมและเข้าร่วมกิจกรรมวิชาชีพอย่างต่อเนื่อง

๑.๔ การกำกับดูแลโดยคณะกรรมการ (Governance Board / Data Protection Committee)

ต้องมีคณะกรรมการหรือหน่วยงานที่กำกับนโยบายและตรวจสอบผลการดำเนินงาน

ต้องประชุมสม่ำเสมอ (เช่น รายไตรมาส) และบันทึกการประชุมอย่างเป็นระบบ

๒. ด้านกระบวนการ (Process)

ด้านนี้เป็นการตรวจสอบว่ามีกระบวนการภายในที่ชัดเจน โปร่งใส และสามารถดำเนินการตามกฎหมายได้จริง

๒.๑ ขั้นตอนปฏิบัติงานมาตรฐาน (Standard Operating Procedures: SOP)

ต้องมี SOP สำหรับการ行使สิทธิของเจ้าของข้อมูลแต่ละประเภท เช่น

สิทธิขอเข้าถึง (Right of Access)

สิทธิแก้ไขข้อมูล (Right to Rectification)

สิทธิในการลบ (Right to Erasure)

สิทธิถอนความยินยอม (Withdrawal of Consent)

สิทธิในการพกพาข้อมูล (Data Portability)

SOP ต้องระบุชัดเจนถึงผู้รับผิดชอบ ระยะเวลา (Timeline) และรูปแบบการตอบสนอง

๒.๒ แผนตอบสนองต่อเหตุการณ์ข้อมูลรั่วไหล (Incident Response Plan)

ต้องมีแผนการแจ้งเหตุ (Incident Notification) ภายใน ๗๒ ชั่วโมง ตามข้อกำหนด GDPR

ต้องระบุช่องทางการสื่อสารทั้งภายในและภายนอกองค์กร

ต้องมีแบบฟอร์มบันทึกเหตุการณ์และบทเรียนที่ได้ (Lessons Learned)

๒.๓ การกำหนดระยะเวลาเก็บรักษาข้อมูล (Data Retention Policy)

ต้องมีตารางกำหนดอายุการเก็บข้อมูล (Retention Schedule)

ข้อมูลที่หมดความจำเป็นต้องถูกทำลายอย่างปลอดภัย (Secure Deletion) เช่น การลบถาวร (Wiping) หรือการทำลายสื่อ (Media Destruction)

๒.๔ การบริหารสิทธิ์เข้าถึง (Access Management Process)

ต้องมีการกำหนดสิทธิ์ตามบทบาทหน้าที่ (Role-based Access Control: RBAC)

ต้องมีการอนุมัติเป็นลำดับขั้นก่อนเข้าถึงข้อมูลที่อ่อนไหว (Sensitive Data)

ต้องมีการทบทวนสิทธิ์เข้าถึงเป็นประจำ (Access Review)

๓. ด้านเทคนิค (Technical)

ด้านนี้เน้นตรวจสอบมาตรการด้านเทคโนโลยีสารสนเทศ (IT Security) ที่ช่วยลดความเสี่ยงจากการโจมตีหรือการเข้าถึงโดยไม่ได้รับอนุญาต

๓.๑ การเข้ารหัสข้อมูล (Data Encryption)

ต้องมีการเข้ารหัสข้อมูลขณะเก็บ (At Rest) และขณะส่งผ่านเครือข่าย (In Transit)

คีย์เข้ารหัส (Encryption Key) ต้องถูกจัดการอย่างปลอดภัยและเก็บแยกจากข้อมูลหลัก

๓.๒ การควบคุมการเข้าถึง (Access Control, Multi-Factor Authentication: MFA)

ต้องมีระบบยืนยันตัวตนหลายชั้น (MFA) โดยเฉพาะเมื่อเข้าถึงข้อมูลสำคัญ

ต้องมีระบบล็อกบัญชี (Account Lockout) หากพยายามเข้าสู่ระบบผิดซ้ำ

๓.๓ การทดสอบความปลอดภัย (Penetration Testing, Vulnerability Assessment)

ต้องมีการทดสอบเจาะระบบ (PenTest) โดยบุคคลที่สาม (Third Party) อย่างน้อยปีละ ๑ ครั้ง

ต้องมีการสแกนหาช่องโหว่ (Vulnerability Scan) อย่างสม่ำเสมอ เช่น รายไตรมาส

๓.๔ ระบบป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention: DLP)

ต้องมีเครื่องมือในการตรวจจับและป้องกันการส่งข้อมูลออกนอกกระบบโดยไม่ได้รับอนุญาต

ต้องมีระบบแจ้งเตือนเมื่อพบพฤติกรรมผิดปกติ เช่น การดาวน์โหลดไฟล์จำนวนมาก

๓.๕ การบันทึกเหตุการณ์และตรวจสอบย้อนหลัง (Logging & Monitoring)

ต้องมีการเก็บ Log File อย่างน้อย ๑ ปี

ต้องมีระบบตรวจจับการบุกรุก (Intrusion Detection/Prevention System: IDS/IPS)

๔. ด้านการบริหารจัดการ (Management)

เป็นการตรวจสอบเชิงกลยุทธ์และการสร้างวัฒนธรรมองค์กรให้คำนึงถึงความเป็นส่วนตัวและความมั่นคงปลอดภัย

๔.๑ การอบรมและสร้างความตระหนักรู้ (Training & Awareness)

ต้องมีการจัดฝึกอบรม (Training) อย่างน้อยปีละครั้ง

เนื้อหาต้องครอบคลุมทั้งกฎหมาย มาตรการด้านเทคนิค และกรณีศึกษา (Case Study)

๔.๒ การประเมินความเสี่ยง (Risk Assessment)

ต้องมีการจัดทำ Risk Register เกี่ยวกับข้อมูลส่วนบุคคล

ต้องประเมินทั้งความเสี่ยงด้านกฎหมาย (Legal Risk) และด้านเทคนิค (Technical Risk)

ต้องมีการกำหนด Risk Owner และแผนการบรรเทา (Mitigation Plan)

๔.๓ การรายงานต่อผู้บริหาร (Management Reporting)

ต้องมีรายงานผลการตรวจสอบเสนอต่อคณะกรรมการบริหารอย่างน้อยปีละ ๑ ครั้ง

ต้องมีการนำเสนอผลลัพธ์ในรูปแบบ Executive Summary เพื่อให้ผู้บริหารเข้าใจง่าย

๔.๔ การตรวจสอบจากภายนอก (External Audit / Certification)

หากมีการรับรองมาตรฐาน เช่น ISO/IEC 27001, ISO/IEC 27701 ต้องมีการตรวจประเมินจากผู้ตรวจสอบภายนอก

ผลการตรวจสอบต้องถูกนำมาใช้ปรับปรุงภายในองค์กร

สรุป

การตรวจสอบด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ จำเป็นต้องพิจารณาอย่างรอบด้าน ครอบคลุมทั้ง ๔ มิติ ได้แก่ **กฎหมายและการกำกับดูแล กระบวนการ เทคนิค และการบริหารจัดการ** หากองค์กรสามารถดำเนินการตามเกณฑ์เหล่านี้ได้ครบถ้วน จะช่วยสร้างความเชื่อมั่น ป้องกันความเสี่ยง และสอดคล้องกับมาตรฐานสากลอย่างแท้จริง

1) ตัวอย่าง ตารางตรวจสอบ (Checklist)

หมวด	ข้อที่ตรวจสอบ	มี/ไม่มี	หมายเหตุ
ด้านกฎหมายและนโยบาย	มี Privacy Policy และ Notice ครบถ้วน	☐ /✓	ตรวจสอบการเผยแพร่หน้าเว็บและเอกสารภายใน
	มีการเก็บบันทึกคำขอใช้สิทธิของเจ้าของข้อมูล	☐ /✓	ตรวจสอบ log การร้องขอข้อมูล
	มี DPO หรือผู้รับผิดชอบด้านข้อมูลชัดเจน	☐ /✓	ตรวจสอบประกาศหน้าสำนักงาน
ด้านเทคนิคและระบบ	ระบบจัดเก็บข้อมูลมีการเข้ารหัส	☐ /✓	ตรวจสอบ Encryption ใน Database
	ระบบมีการสำรองข้อมูล (Backup) และทดสอบการกู้คืน	☐ /✓	ตรวจสอบ log การสำรองข้อมูล
	ระบบมีการตรวจสอบและบันทึกเหตุการณ์ (Audit Log)	☐ /✓	ตรวจสอบ Event Log
ด้านการฝึกอบรมและความตระหนัก	พนักงานได้รับการอบรม PDPA และ Security	☐ /✓	ตรวจสอบใบรับรองการอบรม
	มีสื่อประชาสัมพันธ์เกี่ยวกับการคุ้มครองข้อมูล	☐ /✓	ตรวจสอบโปสเตอร์, Newsletter

2) ตัวอย่าง แบบฟอร์มรายงานผล (Report Template)

หัวข้อรายงาน: ผลการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยสารสนเทศ

วันที่ตรวจสอบ: _____

ผู้ตรวจสอบ: _____

2.1 สรุปผล (Executive Summary)

- สรุปภาพรวมของการตรวจสอบ
- ระบุข้อดีและข้อสังเกตสำคัญ

2.2 รายละเอียดผลการตรวจสอบ (Findings)

หมวด	ข้อที่ตรวจสอบ	ผลการตรวจสอบ	ระดับความเสี่ยง	ข้อเสนอแนะ
ด้านกฎหมายและนโยบาย	Privacy Policy ครบถ้วน	☐ /✓	ต่ำ/กลาง/สูง	ปรับปรุงเนื้อหาและเผยแพร่

ด้านเทคนิค	ระบบสำรองข้อมูล	☐ / ☒	ต่ำ/กลาง/ สูง	ทดสอบกู้คืนทุก 3 เดือน
ด้านฝึกอบรม	พนักงานอบรมครบ	☐ / ☒	ต่ำ/กลาง/ สูง	จัดอบรมเพิ่มเติมสำหรับ พนักงานใหม่

2.3 ข้อสรุปและคำแนะนำ

- ข้อเสนอแนะเชิงนโยบาย
- แผนการปรับปรุง

3) ตัวอย่าง กรณีศึกษา (Case Study)

ชื่อกรณีศึกษา: การร้องขอใช้สิทธิข้อมูลส่วนบุคคลของผู้ป่วยในโรงพยาบาล

สถานการณ์

ผู้ป่วยร้องขอสำเนาข้อมูลการรักษาในระบบ EHR ของโรงพยาบาล

การวิเคราะห์

1. ตรวจสอบว่าโรงพยาบาลมี ช่องทางการร้องขอสิทธิข้อมูล ที่ชัดเจนหรือไม่
2. ตรวจสอบ ระยะเวลาการให้ข้อมูล ตาม PDPA (ไม่เกิน 30 วัน)
3. ตรวจสอบ การบันทึกและพิสูจน์ตัวตนผู้ร้องขอ

ผลการดำเนินการ

- โรงพยาบาลมีแบบฟอร์มออนไลน์และเอกสารรับรองตัวตน
- ใช้ระบบตรวจสอบสิทธิผู้ร้องขอก่อนอนุมัติ
- ข้อมูลส่งให้ผู้ร้องขอภายใน 15 วัน

บทเรียนที่ได้รับ

- การจัดช่องทางร้องขอที่ชัดเจนช่วยลดข้อร้องเรียน
- การบันทึกทุกขั้นตอนช่วยสร้างความโปร่งใสและเป็นหลักฐานได้
- พนักงานต้องเข้าใจ PDPA และมาตรการความปลอดภัย

10.6.7 มีการจัดทำและดำเนินการตามแผนการปรับปรุง จากรายงานผลการตรวจสอบดังกล่าว

สิ่งที่ต้องทำ: องค์กรมีการจัดทำและดำเนินการตามแผนการปรับปรุงจากรายงานผลการตรวจสอบ และมีเอกสารครบถ้วน

หลักฐาน: นโยบายจัดทำและดำเนินการตามแผนการปรับปรุงจากรายงานผลการตรวจสอบมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

รายงานผลการตรวจสอบทดสอบมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
นโยบายภายในหรือประกาศแก้ไขปรับปรุงผลการตรวจสอบมาตรการที่ใช้ในการคุ้มครอง
ข้อมูลส่วนบุคคลขององค์กรประจำปี

แผนงานปรับปรุงผลการตรวจสอบมาตรการที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
ประจำปี

สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยสารสนเทศ วัตถุประสงค์

เพื่อกำหนดแนวทาง ขั้นตอน และความถี่ในการตรวจสอบระบบ การปฏิบัติงาน และมาตรการต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรให้เป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล เช่น ISO/IEC 27001 27701 และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ขอบเขต

ครอบคลุมถึงทุกฝ่ายที่มีหน้าที่รับผิดชอบในการจัดเก็บ ประมวลผล และเปิดเผยข้อมูลส่วนบุคคล รวมถึงระบบสารสนเทศที่เกี่ยวข้อง

หลักการดำเนินงาน

- องค์กรต้องจัดทำ แผนการตรวจสอบภายในประจำปี โดยรวมถึงการตรวจสอบมาตรการด้านข้อมูลส่วนบุคคลและความมั่นคงปลอดภัย
- มีการกำหนด ผู้รับผิดชอบในการตรวจสอบ อย่างชัดเจน โดยผู้ตรวจสอบต้องไม่เป็นผู้กำหนดนโยบายหรือผู้มีผลประโยชน์ขัดกัน
- จัดทำ รายการเกณฑ์ตรวจสอบ เพื่อใช้เป็นเครื่องมือในการประเมินความสอดคล้องกับนโยบาย/มาตรการที่กำหนดไว้
- จัดทำ รายงานผลการตรวจสอบ พร้อมข้อเสนอแนะและแผนการปรับปรุง (หากมี)
- ต้องมีการ ทบทวนแผนและนโยบายการตรวจสอบอย่างน้อยปีละ 1 ครั้ง

2. รายงานผลการตรวจสอบ (ตัวอย่าง)

รายงานผลการตรวจสอบภายใน: การคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยสารสนเทศ

ชื่อหน่วยงาน: แผนกเทคโนโลยีสารสนเทศ

วันที่ตรวจสอบ: 15 มีนาคม 2568

ผู้ตรวจสอบ: นายอรรถพล วิริยะกิจ (เจ้าหน้าที่ตรวจสอบภายในอิสระ)

1. วัตถุประสงค์

เพื่อประเมินความสอดคล้องของมาตรการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามแนวทางขององค์กรและกฎหมายที่เกี่ยวข้อง

2. ขอบเขตการตรวจสอบ

- การเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล
- ระบบควบคุมการเข้าถึง
- ระบบสำรองข้อมูล
- มาตรการรักษาความปลอดภัยเชิงเทคนิคและองค์กร

3. วิธีการตรวจสอบ

- การสัมภาษณ์เจ้าหน้าที่
- การตรวจสอบเอกสารนโยบาย
- การทดสอบระบบความปลอดภัย
- การสังเกตการปฏิบัติงานจริง

4. ผลการตรวจสอบ

พบว่าการจัดเก็บข้อมูลส่วนบุคคลของพนักงานและลูกค้าโดยใช้ระบบ HRMS และ CRM ซึ่งมีการเข้ารหัสข้อมูล

- มีการใช้รหัสผ่านแบบ Multi-Factor Authentication (MFA)
- พบว่าเอกสารนโยบายฉบับล่าสุดยังไม่เผยแพร่ให้พนักงานระดับปฏิบัติการทุกคน
- การสำรองข้อมูลจัดทำทุก 7 วัน แต่ไม่มีการทดสอบการกู้คืนข้อมูลในช่วง 6 เดือนที่ผ่านมา

5. ข้อเสนอแนะ

- จัดฝึกอบรม/เผยแพร่ นโยบายแก่พนักงานระดับปฏิบัติการ
- จัดทำแผนทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ 2 ครั้ง
- ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบอย่างน้อยทุก 3 เดือน

3. แบบฟอร์มเกณฑ์การตรวจสอบ (Checklist Template)

ลำดับ	หัวข้อที่ตรวจสอบ	รายละเอียดเกณฑ์	สถานะ (ผ่าน/ไม่ผ่าน/ต้องปรับปรุง)	หมายเหตุ
1	มีนโยบาย PDPA ที่ประกาศใช้อย่างเป็นทางการ	ต้องมีเอกสารลงนามโดยผู้บริหารระดับสูง	ผ่าน	มีเอกสารแนบ

2	มีระบบจัดเก็บข้อมูลอย่างปลอดภัย	ระบบเข้ารหัส (encryption) ระดับ AES256	ผ่าน	-
3	การจำกัดสิทธิ์เข้าถึงข้อมูล	ใช้ระบบ Role-Based Access Control	ต้องปรับปรุง	ยังไม่อัปเดตสิทธิ์พนักงานใหม่
4	มีแผนการทดสอบการกู้คืนข้อมูล	ต้องมีแผนและกำหนดการทดสอบ DRP	ไม่ผ่าน	ไม่มีบันทึก DRP
5	มีการแจ้งเหตุละเมิดข้อมูลต่อคณะกรรมการ	ต้องมีระยะเวลา 72 ชั่วโมงตามกฎหมาย	ผ่าน	ทดสอบแล้ว

10.7 ข้อมูลด้านประสิทธิภาพและความสอดคล้องกับข้อกำหนด (Performance and compliance information)

องค์กรกำหนดตัวชี้วัดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและการจัดการข้อมูล และองค์กรสามารถประเมินข้อมูลต่าง ๆ เพื่อทราบผลการประเมิน

10.7.1 มีการกำหนดตัวชี้วัด (KPIs) ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น ระยะเวลาในการตอบสนองต่อคำขอใช้สิทธิ เป็นต้น

สิ่งที่ต้องทำ: มีการกำหนดตัวชี้วัด (KPIs) ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น ระยะเวลาในการตอบสนองต่อคำขอใช้สิทธิ เป็นต้น และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการกำหนดตัวชี้วัด (KPIs) ของ DPO โดยนำการบริหารจัดการด้านข้อมูลส่วนบุคคลมาเป็นตัวกำหนด

แบบการกำหนดการชี้วัดการปฏิบัติหน้าที่ของ DPO

สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการกำหนดตัวชี้วัด (KPIs) ด้านการคุ้มครองข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดแนวทางและกรอบการกำหนดตัวชี้วัดประสิทธิภาพ (Key Performance Indicators - KPIs) ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและการบริหารจัดการข้อมูล เพื่อให้สามารถประเมินผลการดำเนินงานได้อย่างเป็นระบบ โปร่งใส และสอดคล้องกับพันธกิจด้าน Data Governance และ PDPA ขององค์กร

ขอบเขตการบังคับใช้

นโยบายนี้ครอบคลุมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) รวมถึงหน่วยงานที่มีหน้าที่หรือความเกี่ยวข้องในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

หลักการกำหนด KPIs

- KPIs ต้องสามารถวัดผลได้ (Measurable) และมีเป้าหมายที่ชัดเจน
- KPIs ต้องสอดคล้องกับภารกิจด้านการปฏิบัติตาม PDPA และมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ
- KPIs ต้องได้รับการประเมินอย่างต่อเนื่องและปรับปรุงให้เหมาะสมกับบริบทขององค์กร

ตัวอย่างตัวชี้วัดที่แนะนำ

หมายเลข	ตัวชี้วัด (KPI)	คำอธิบาย	หน่วยวัด	เป้าหมาย
1	ระยะเวลาเฉลี่ยในการตอบสนองคำขอใช้สิทธิของเจ้าของข้อมูล	คำนวณจากวันรับคำขอจนถึงวันที่ให้คำตอบ	วันทำการ	ไม่เกิน 7 วัน
2	จำนวนเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่ได้รับการจัดการภายใน 72 ชั่วโมง	ความสามารถในการแจ้งเหตุแก่ สคส. ภายในเวลาที่กฎหมายกำหนด	ร้อยละ	≥ 95%
3	จำนวนข้อร้องเรียนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ได้รับการปิดเรื่องแล้ว	ประเมินประสิทธิภาพการจัดการข้อร้องเรียน	เรื่อง	≥ 90% ต่อไตรมาส
4	จำนวนการอบรมหรือสร้างความรู้ด้าน PDPA ที่จัดขึ้นในรอบปี	ประเมินกิจกรรมพัฒนาความรู้ในองค์กร	ครั้งต่อปี	≥ 2 ครั้ง
5	การทบทวนและปรับปรุงนโยบายความเป็นส่วนตัว	วัดความถี่ในการปรับปรุงให้ทันต่อการเปลี่ยนแปลง	ครั้งต่อปี	≥ 1 ครั้ง

2. แบบฟอร์มการกำหนด KPIs สำหรับ DPO

ชื่อแบบฟอร์ม: แบบฟอร์มกำหนดตัวชี้วัดการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ลำดับ	ด้านภารกิจ	ตัวชี้วัด (KPI)	หน่วยวัด	ค่าเป้าหมาย	วิธีเก็บข้อมูล	ความถี่การประเมิน
1	การใช้สิทธิ	เวลาตอบสนองคำขอเจ้าของข้อมูล	วันทำการ	≤ 7 วัน	แบบบันทึกคำขอ	รายเดือน
2	การละเมิดข้อมูล	อัตราการแจ้งเหตุภายใน 72 ชม.	ร้อยละ	≥ 95%	รายงาน DPO	รายไตรมาส
3	ข้อร้องเรียน	อัตราการปิดเรื่องสำเร็จ	เรื่อง	≥ 90%	แบบตอบข้อร้องเรียน	รายไตรมาส
4	การฝึกอบรม	จำนวนครั้งที่จัดฝึกอบรม	ครั้ง	≥ 2	บันทึกการอบรม	รายปี
5	การทบทวน	ความถี่ในการอัปเดตนโยบาย PDPA	ครั้ง/ปี	≥ 1	รายงานประจำปี	รายปี

3. แนวทางการใช้และประเมินผล

- ผู้กำกับดูแลนโยบายและการตรวจสอบ KPIs ควรเป็นคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Committee)
- DPO เป็นผู้รวบรวมข้อมูลและรายงานผลต่อคณะกรรมการฯ อย่างน้อยปีละ 1 ครั้ง
- หากพบ KPIs ที่ไม่สามารถบรรลุเป้าหมายติดต่อกันเกิน 2 ไตรมาส ต้องจัดทำ Action Plan เพื่อปรับปรุงโดยเฉพาะ
-

4. เอกสารหลักฐานที่แนะนำให้จัดเก็บ

- นโยบายการกำหนด KPIs ด้านการคุ้มครองข้อมูลส่วนบุคคล
- รายงานสรุปผลการดำเนินงานของ DPO
- แบบฟอร์มการประเมินผล KPIs ที่ลงนามโดยผู้บริหาร
- หลักฐานประกอบ เช่น ใบตอบรับคำขอใช้สิทธิ ใบแจ้งเหตุละเมิด ใบลงชื่ออบรม เป็นต้น

10.7.2 มีการกำหนดตัวชี้วัดสำหรับการฝึกอบรมที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และมีการจัดทำรายงานเพื่อแสดงให้เห็นว่าพนักงานได้ผ่านการฝึกอบรมดังกล่าวเป็นจำนวนร้อยละเท่าใด

- สิ่งที่ต้องทำ: องค์กรมีการกำหนดตัวชี้วัดสำหรับการฝึกอบรมที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และมีการจัดทำรายงานเพื่อแสดงให้เห็นว่าพนักงานได้ผ่านการฝึกอบรมดังกล่าวเป็นจำนวนร้อยละเท่าใด และมีเอกสารครบถ้วน
- หลักฐาน: นโยบายการกำหนดตัวชี้วัด (KPIs) ของ DPO โดยนำการฝึกอบรมที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และการจัดทำรายงานเพื่อแสดงให้เห็นว่าพนักงานได้ผ่านการฝึกอบรมมาเป็นตัวกำหนด
- แบบการกำหนดการชี้วัดการปฏิบัติหน้าที่ของ DPO
- แผนการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล
- ผลสอบของพนักงานที่เข้าอบรม
- สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการกำหนดตัวชี้วัด (KPIs) สำหรับการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล

วัตถุประสงค์

เพื่อกำหนดแนวทางในการประเมินผลการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล โดยใช้ตัวชี้วัดที่สามารถวัดผลได้ชัดเจน เพื่อให้แน่ใจว่าพนักงานทุกระดับมีความรู้และความตระหนักเกี่ยวกับหน้าที่ความรับผิดชอบตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และนโยบายขององค์กร

ขอบเขตการบังคับใช้

ครอบคลุมพนักงานทุกระดับ รวมถึงพนักงานสัญญาจ้าง พนักงานจ้างช่วง และหน่วยงานที่มีหน้าที่เกี่ยวข้องกับการเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

หลักการกำหนดตัวชี้วัด

- KPIs ต้องสามารถประเมินได้จากข้อมูลเชิงปริมาณ เช่น ร้อยละของผู้ผ่านการอบรม
- ต้องมีการวัดผลก่อนและหลังการฝึกอบรม (Pre-test/Post-test)
- การฝึกอบรมควรครอบคลุมทั้งด้านความรู้พื้นฐาน PDPA และบริบทเฉพาะของหน่วยงาน

ตัวชี้วัดหลักที่แนะนำ

หมายเลข	ตัวชี้วัด (KPI)	คำอธิบาย	หน่วยวัด	เป้าหมาย
1	ร้อยละของพนักงานที่ผ่านการฝึกอบรม PDPA ในรอบปี	ประเมินจากจำนวนพนักงานทั้งหมดต่อจำนวนผู้ผ่านการฝึกอบรม	ร้อยละ	≥ 90%
2	คะแนนเฉลี่ยผลสอบหลังการอบรม	ความเข้าใจของผู้เข้าอบรม	คะแนนเต็ม 100	≥ 80 คะแนน
3	จำนวนครั้งที่จัดฝึกอบรมตามแผน	ความต่อเนื่องของการพัฒนาบุคลากร	ครั้ง/ปี	≥ 2 ครั้ง

2. แบบฟอร์มการกำหนดตัวชี้วัดและรายงานผลการฝึกอบรม

ชื่อแบบฟอร์ม: แบบฟอร์มประเมินผลการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล

ลำดับ	ตัวชี้วัด	หน่วยวัด	ค่าเป้าหมาย	ผลที่ได้	ความถี่
1	ร้อยละพนักงานที่ผ่านอบรม	%	≥ 90%	93%	รายปี
2	คะแนนเฉลี่ยหลังการอบรม	คะแนน	≥ 80	85	รายกิจกรรม
3	จำนวนรอบอบรมในปี	ครั้ง	≥ 2	3	รายปี

3. แผนการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล

ตัวอย่างแผนอบรมประจำปี

(สามารถจัดในรูปแบบตาราง Gantt ได้หากต้องการเวอร์ชันภาพ)

เดือน	หัวข้อ	ผู้เข้าอบรมเป้าหมาย	จำนวนคน	รูปแบบ	ผู้รับผิดชอบ
มีนาคม	ความรู้เบื้องต้นเกี่ยวกับ PDPA	พนักงานใหม่	50	Online	แผนกบุคคล + DPO
มิถุนายน	การปฏิบัติหน้าที่ผู้ควบคุมข้อมูล	หัวหน้างาน	20	In-house	DPO
ตุลาคม	Workshop: กรณีศึกษา Data Breach	ทีมไอที + ฝ่ายกฎหมาย	30	Workshop	DPO + IT Security

4. เอกสารหลักฐานที่ควรจัดเก็บ

- นโยบายและแผนฝึกอบรมประจำปีด้าน PDPA
- รายชื่อพนักงานที่เข้าอบรม พร้อมผลการประเมิน (Pre/Post Test)
- รายงานผลการฝึกอบรมประจำปี โดยสรุปเป็นร้อยละของพนักงานที่ผ่าน
- แบบฟอร์มประเมินความพึงพอใจการอบรม (ถ้ามี)
- เอกสารรับรองการเข้าอบรม / ใบประกาศนียบัตร

5. แนวทางการประเมินผลและปรับปรุง

- ฝ่าย DPO ต้องสรุปรายงานผลการฝึกอบรมในแต่ละรอบและส่งต่อให้ผู้บริหารทุกไตรมาส
- หากร้อยละผู้เข้าอบรมต่ำกว่า 80% ต้องมีแผนแก้ไขเพิ่มเติม เช่น เปิดอบรมนอกตาราง / เฉพาะกลุ่ม
- ทุกปีต้องมีการปรับปรุงเนื้อหาหลักสูตรให้ทันต่อความเปลี่ยนแปลงของกฎหมายและแนวทางของหน่วยงานกำกับดูแล (สคส.)

10.7.3 มีการกำหนดตัวชี้วัดระดับที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงจำนวนครั้งที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย และจำนวนครั้งของเหตุที่มีการแจ้งเหตุไปยัง สคส.

สิ่งที่ต้องทำ: องค์กรมีการกำหนดตัวชี้วัดระดับที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงจำนวนครั้งที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย และจำนวนครั้งของการละเมิดที่มีการแจ้งเหตุไปยัง สคส. และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการกำหนดตัวชี้วัด (KPIs) ของ DPO โดยนำการฝึกอบรมที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และการจัดทำรายงานเพื่อแสดงให้เห็นว่าพนักงานได้ผ่านการฝึกอบรมมาเป็นตัวกำหนด

กรอบกำหนดการชี้วัดการปฏิบัติหน้าที่ของ DPO แผนการฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล

หลักฐาน: ผลสอบของพนักงานที่เข้าอบรม

รายงานผลความเข้าใจหรือความตระหนักของพนักงานที่เข้าฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล

นโยบายการกำหนดตัวชี้วัด (KPIs) ของ DPO โดยนำการรักษาความมั่นคงปลอดภัยสารสนเทศมาเป็นตัวกำหนด

แบบการกำหนดการชี้วัดการปฏิบัติหน้าที่ของ DPO

นโยบายการกำหนดตัวชี้วัด (KPIs) ของ IT โดยนำการรักษาความมั่นคงปลอดภัยสารสนเทศ มาเป็นตัวกำหนด

แบบการกำหนดการชี้วัดการปฏิบัติหน้าที่ของ IT

สภาพบังคับ: กฎหมายไม่ได้กำหนด

เอกสารฉบับที่ 1: นโยบายการกำหนดตัวชี้วัด (KPIs) ของ DPO เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

ชื่อเอกสาร: นโยบายกำหนดตัวชี้วัดผลการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

เวอร์ชัน: 1.0 | วันที่บังคับใช้: 1 มกราคม 2568

หน่วยงานเจ้าของ: ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO Unit)

วัตถุประสงค์

เพื่อกำหนดแนวทางการประเมินผลการปฏิบัติงานของ DPO โดยใช้ตัวชี้วัดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ และความสามารถในการติดตามเหตุการณ์การละเมิดข้อมูลส่วนบุคคล

ขอบเขต

ครอบคลุมการติดตามและรายงานเหตุการณ์ละเมิดข้อมูล การแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และการประเมินผลความร่วมมือกับฝ่าย IT

ตัวชี้วัดหลัก (KPIs)

ลำดับ	ตัวชี้วัด	หน่วยวัด	เป้าหมาย	ความถี่การวัด
1	จำนวนเหตุการณ์ละเมิดข้อมูลที่ตรวจพบ	ครั้ง/ปี	ไม่เกิน 5 ครั้ง	รายไตรมาส
2	ร้อยละของเหตุการณ์ที่แจ้งต่อ สคส. ภายใน 72 ชั่วโมง	%	≥ 100%	ต่อเหตุการณ์
3	ระยะเวลาเฉลี่ยในการตรวจสอบและวิเคราะห์เหตุการณ์	ชั่วโมง	≤ 48 ชั่วโมง	ต่อเหตุการณ์
4	จำนวนการประชุม DPO + IT เพื่อวางมาตรการป้องกัน	ครั้ง/ปี	≥ 2 ครั้ง	รายปี

เอกสารฉบับที่ 2: แบบฟอร์มกำหนดตัวชี้วัดการปฏิบัติหน้าที่ของ DPO

ชื่อผู้ปฏิบัติ	นายจเร ภัคดี (DPO)

หน่วยงาน	ฝ่ายคุ้มครองข้อมูลส่วนบุคคล (DPO Unit)
รอบประเมิน	ปีงบประมาณ 2568

ตัวชี้วัด	ค่าเป้าหมาย	ผลที่ได้จริง	หมายเหตุ
เหตุการณ์ละเมิดที่เกิดขึ้น	≤ 5	3	ผ่าน
เหตุการณ์ที่แจ้งภายใน 72 ชม.	100%	100%	ผ่าน
ประชุมร่วม IT	≥ 2 ครั้ง	3 ครั้ง	ผ่าน

ลงชื่อ: (DPO)

ลงชื่อ: (หัวหน้าฝ่ายบุคคล)

วันที่ประเมิน: 30 กันยายน 2568

เอกสารฉบับที่ 3: นโยบายกำหนด KPIs ของฝ่าย IT เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

ชื่อเอกสาร: นโยบายการประเมินผลการดำเนินงานด้าน IT Security

หน่วยงานเจ้าของ: ฝ่ายเทคโนโลยีสารสนเทศ (IT Department)

วันที่บังคับใช้: 1 มกราคม 2568

ตัวชี้วัดหลัก

ลำดับ	KPI	หน่วยวัด	เป้าหมาย	ความถี่
1	จำนวนเหตุการณ์ภัยคุกคามระบบสารสนเทศ	ครั้ง	ไม่เกิน 10 ครั้ง/ปี	รายเดือน
2	ระยะเวลาในการตอบสนองต่อเหตุการณ์ (Incident Response Time)	ชั่วโมง	≤ 4 ชม.	ต่อเหตุการณ์
3	ร้อยละของเหตุการณ์ที่มีรายงานต่อ DPO ภายใน 2 ชม.	%	$\geq 95\%$	ต่อเหตุการณ์
4	จำนวนการซ่อมแผนรับมือ Data Breach	ครั้ง/ปี	≥ 1	รายปี

เอกสารฉบับที่ 4: แบบฟอร์มกำหนดตัวชี้วัดของฝ่าย IT

ชื่อแบบฟอร์ม: แบบประเมินผลการดำเนินงานด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (IT Security KPI Assessment Form)

ผู้ประเมิน: หัวหน้าฝ่าย IT

รอบปี: ปีงบประมาณ 2568

ตัวชี้วัด	ค่าเป้าหมาย	ผลที่ได้	หมายเหตุ
เหตุการณ์ภัยคุกคาม	≤ 10	6	ผ่าน
Response time	≤ 4 ชม.	เฉลี่ย 2.5 ชม.	ผ่าน
แจ้ง DPO ภายใน 2 ชม.	$\geq 95\%$	97%	ผ่าน
ข้อผิดพลาด Data Breach	≥ 1 ครั้ง	2 ครั้ง	ผ่าน

เอกสารฉบับที่ 5: รายงานสรุปเหตุการณ์ละเมิดข้อมูลส่วนบุคคลประจำปี

ชื่อเอกสาร: รายงานสรุปเหตุการณ์ด้านความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Data Breach Report Summary)

ปีที่รายงาน: พ.ศ. 2568

หน่วยงาน: DPO + IT

ลำดับ	วันที่เกิดเหตุ	ประเภทเหตุการณ์	หน่วยงานต้นเหตุ	แจ้ง สกส. หรือไม่	วันที่แจ้ง	ระยะเวลา (ชม.)
1	12/03/2568	อีเมลส่งผิดผู้รับ	แผนกลูกค้าสัมพันธ์	แจ้ง	13/03/2568	22 ชม.
2	20/06/2568	ฐานข้อมูลรั่วไหลจากเซิร์ฟเวอร์	IT	แจ้ง	21/06/2568	16 ชม.
3	07/08/2568	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	ฝ่ายจัดซื้อ	ไม่แจ้ง (ไม่เข้าเกณฑ์ร้ายแรง)	-	-

ข้อเสนอแนะ

- ควรจัดอบรมเพิ่มเติมเกี่ยวกับความผิดพลาดของมนุษย์ (Human Error)
- ควรปรับปรุงการเข้ารหัสฐานข้อมูลในระบบสำรอง

เอกสารฉบับที่ 6: บันทึกผลการประชุมร่วมระหว่าง DPO และ IT (มีมติเรื่อง KPIs)

ชื่อเอกสาร: บันทึกการประชุมความร่วมมือด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

วันที่ประชุม: 15 กรกฎาคม 2568

ผู้เข้าร่วม: DPO หัวหน้า IT ตัวแทนฝ่ายกฎหมาย

ประเด็นสำคัญ

- ทบทวนเหตุการณ์ Data Breach ครึ่งปีแรก
- ปรับเกณฑ์ KPI ให้รวมเหตุการณ์ที่ "เกือบเกิด" (Near Miss)
- ตั้งคณะกรรมการพัฒนาแผน DRP + SOP แจ้งเหตุภายใน 24 ชม.

มติที่ประชุม:

- เห็นชอบ KPI ที่มีความสัมพันธ์กับจำนวนเหตุการณ์ละเมิดและประสิทธิภาพในการแจ้ง
- ทุกเหตุการณ์ที่เข้าข่ายร้ายแรงให้แจ้ง สคส. ไม่เกิน 72 ชม. และจัดเก็บเอกสารหลักฐานไว้อย่างเป็นระบบ

ลงชื่อ: (DPO)

ลงชื่อ: (หัวหน้า IT)

10.7.4 มีการกำหนดตัวชี้วัดสำหรับการบริหารจัดการรายการข้อมูล เช่น การลบหรือทำลายข้อมูลตามระยะเวลาที่กำหนดไว้ ประสิทธิภาพของระบบในการทำ index และเข้าถึงข้อมูลในรูปแบบกระดาษที่มีข้อมูลส่วนบุคคลได้อย่างรวดเร็ว เป็นต้น

สิ่งที่ต้องทำ: องค์กรมีการกำหนดตัวชี้วัดสำหรับการบริหารจัดการรายการข้อมูล เช่น การลบหรือทำลายข้อมูลตามระยะเวลาที่กำหนดไว้ ประสิทธิภาพของระบบในการทำ index และเข้าถึงข้อมูลในรูปแบบกระดาษที่มีข้อมูลส่วนบุคคลได้อย่างรวดเร็ว เป็นต้น และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการกำหนดตัวชี้วัด (KPIs) ของ DPO โดยนำการบริหารจัดการด้านข้อมูลส่วนบุคคลมาเป็นตัวกำหนด กรอบกำหนดตัวชี้วัดการปฏิบัติหน้าที่ของ DPO แบบการกำหนดตัวชี้วัดการปฏิบัติหน้าที่ของ DPO

สภาพบังคับ: กฎหมายไม่ได้กำหนด

1. นโยบายการกำหนดตัวชี้วัด (KPIs) ของ DPO ในด้านการบริหารจัดการข้อมูลส่วนบุคคล

ชื่อเอกสาร: นโยบายการกำหนดตัวชี้วัดสำหรับ DPO: ด้านการบริหารจัดการข้อมูลส่วนบุคคล

จัดทำโดย: Data Protection Officer (DPO)

อนุมัติโดย: คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

ปรับปรุงล่าสุด: [ใส่วันที่]

เนื้อหาโดยสรุป

(1) วัตถุประสงค์ของนโยบาย

เพื่อกำหนดเกณฑ์และตัวชี้วัดประสิทธิภาพในการบริหารจัดการข้อมูลส่วนบุคคลอย่างเป็นระบบ โดยเฉพาะการลบ การทำลาย การจัดทำ index และการเข้าถึงข้อมูลตามข้อกำหนดด้านกฎหมายและนโยบายภายในองค์กร

(2) ตัวชี้วัดหลัก (Key Performance Indicators - KPIs)

ตัวชี้วัด	คำอธิบาย	เป้าหมาย	รอบการประเมิน
KPI 1: การทำลายข้อมูลตามรอบเวลา	ร้อยละของข้อมูลส่วนบุคคลที่ถูกทำลายตามกำหนด retention schedule	$\geq 95\%$	รายไตรมาส
KPI 2: เวลาที่ใช้ในการจัดทำเอกสารกระดาษ	ระยะเวลาเฉลี่ยในการค้นหาและส่งมอบข้อมูลส่วนบุคคลในรูปแบบกระดาษ	≤ 3 วัน	รายเดือน
KPI 3: ประสิทธิภาพของระบบ index	ระบบสามารถทำ index เอกสารได้ครบถ้วนและไม่ผิดพลาด	$\geq 98\%$	รายเดือน
KPI 4: จำนวนครั้งที่พบปัญหาในการลบ/ทำลายข้อมูล	กรณีที่ไม่สามารถดำเนินการลบ/ทำลายตามรอบเวลาได้	≤ 2 ครั้งต่อไตรมาส	รายไตรมาส

(3) ขอบเขตของนโยบาย:

ครอบคลุมข้อมูลส่วนบุคคลในระบบอิเล็กทรอนิกส์ เอกสารกระดาษ และระบบจัดการข้อมูลทั้งหมดที่อยู่ภายใต้การควบคุมขององค์กร

2. กรอบกำหนดตัวชี้วัดการปฏิบัติหน้าที่ของ DPO

ชื่อเอกสาร: กรอบกำหนด KPI สำหรับหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูล (DPO)

จัดทำโดย: ฝ่ายทรัพยากรบุคคลร่วมกับ DPO

ปรับปรุงล่าสุด: [ใส่วันที่]

สาระสำคัญ:

หมวดหน้าที่	รายละเอียด	KPI ที่เกี่ยวข้อง
การบริหารจัดการวงจรข้อมูล	ตรวจสอบให้มีการลบ/ทำลายข้อมูลครบถ้วน	KPI 1 KPI 4

การบริหารข้อมูลเอกสารกระดาษ	กำกับดูแลการจัดเก็บและเข้าถึงข้อมูลส่วนบุคคลในรูปแบบเอกสารกระดาษ	KPI 2
การควบคุมระบบจัดเก็บข้อมูลอิเล็กทรอนิกส์	ตรวจสอบคุณภาพของ index และ metadata	KPI 3

3. แบบการกำหนดตัวชี้วัดการปฏิบัติหน้าที่ของ DPO

ชื่อเอกสาร: แบบกำหนดและติดตามตัวชี้วัดผลการปฏิบัติงานของ DPO

จัดทำโดย: DPO Office

รอบการประเมิน: รายไตรมาส

KPI	ผลลัพธ์ที่วัดได้จริง (Q1)	สถานะ	หมายเหตุ
KPI 1	97%	ผ่าน	-
KPI 2	2.5 วัน	ผ่าน	ลดลงจาก Q4 ปีก่อน (3.2 วัน)
KPI 3	99.2%	ผ่าน	ตรวจพบเอกสารผิด index 2 รายการจาก 250 รายการ
KPI 4	1 ครั้ง	ผ่าน	ปัญหาจากหน่วยงานภายนอกล่าช้า

10.8 การใช้ข้อมูลเพื่อการจัดการ (Use of management information) ข้อมูลการจัดการที่เกี่ยวข้องทั้งหมดและผลลัพธ์ของกิจกรรมการติดตามและทบทวนจะถูกสื่อสารไปยังผู้มีส่วนได้ส่วนเสียภายในที่เกี่ยวข้อง รวมถึงผู้บริหารระดับสูงตามความเหมาะสม ข้อมูลนี้จะถูกพิจารณาและดำเนินการ

10.8.1 มีการนำผลจากการตรวจสอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผู้ตรวจสอบภายใน ผู้ตรวจสอบอิสระ และผลการติดตามและทบทวนอื่น ๆ มาสรุปหรือจัดทำเป็นแดชบอร์ด ซึ่งรวมถึงตัวชี้วัด

ต่าง ๆ เพื่อรายงานข้อมูลโดยสรุปให้ผู้บริหารได้รับทราบและใช้เป็นข้อมูลในการบริหารจัดการและตัดสินใจดำเนินการต่าง ๆ

สิ่งที่ต้องทำ: องค์กรมีการนำผลจากการตรวจสอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผู้ตรวจสอบภายใน ผู้ตรวจสอบอิสระ และผลการติดตามและทบทวนอื่น ๆ มาสรุปหรือจัดทำเป็นแดชบอร์ด ซึ่งรวมถึงตัวชี้วัดต่าง ๆ เพื่อรายงานข้อมูลโดยสรุปให้ผู้บริหารได้รับทราบและใช้เป็นข้อมูลในการบริหารจัดการและตัดสินใจดำเนินการต่าง ๆ และมีเอกสารครบถ้วน

หลักฐาน: นโยบายการนำผลจากการตรวจสอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผลจากการตรวจสอบของผู้ตรวจสอบภายใน และผลจากการตรวจสอบของผู้ตรวจสอบภายนอก/อิสระ รายงานผู้บริหาร รายงานผลการตรวจสอบของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น รายงานผลจากการตรวจสอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รายงานผลจากการตรวจสอบของผู้ตรวจสอบภายใน รายงานผลจากการตรวจสอบของผู้ตรวจสอบภายนอก/อิสระ

สภาพบังคับ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ (4) (5) ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 5 (5) โทษทางปกครอง อาศัยอำนาจตามมาตรา 37 ในกรณีที่ไม่ปฏิบัติตามมาตรา 37 กำหนดโทษปรับทางปกครองไม่เกิน 3 ล้านบาท

การใช้ข้อมูลเพื่อการจัดการ และรายงานแดชบอร์ดจากการตรวจสอบ

สิ่งที่ต้องมีในองค์กร

- สรุปผลจากการตรวจสอบ DPO / ผู้ตรวจสอบภายใน / ผู้ตรวจสอบอิสระ
- นำข้อมูลมาจัดทำเป็น รายงานสรุป หรือแดชบอร์ด (Dashboard)
- ส่งให้ ผู้บริหารระดับสูง พิจารณาและใช้ในการตัดสินใจ
- มีเอกสารหลักฐานครบถ้วนสำหรับตรวจสอบย้อนหลัง

ตัวอย่างเอกสารหลักฐาน (Evidence Documents)

1. นโยบายการรายงานผลตรวจสอบและสรุปเพื่อการบริหารจัดการ

ชื่อเอกสาร: นโยบายการจัดทำรายงานผลการตรวจสอบและรายงานสรุปข้อมูลการจัดการ

เนื้อหาโดยย่อ

ผู้ตรวจสอบแต่ละระดับ (DPO Audit External Auditor) มีหน้าที่จัดทำ รายงานรายไตรมาส

รายงานรวมถึง

- เหตุการณ์ละเมิดข้อมูล (ถ้ามี)
- ความเสี่ยงด้านข้อมูลส่วนบุคคล
- ตัวชี้วัดความปลอดภัยและการปฏิบัติตาม
- รายงานจะถูกสรุปในรูปแบบ Dashboard (Infographic + KPIs Table)
- แจ้งต่อผู้บริหารระดับสูงผ่านช่องทางปลอดภัย (เช่น บอร์ดความมั่นคง รายงาน email ที่เข้ารหัส)

2. รายงานผู้บริหาร (Executive Dashboard Report)

ชื่อเอกสาร: Executive Dashboard – ข้อมูลด้านความมั่นคงและการปฏิบัติตาม PDPA

ตัวอย่างหัวข้อในรายงาน

หมวดหมู่	ข้อมูลสรุป	สถานะ	แนวโน้มความเสี่ยง
เหตุการณ์ละเมิดข้อมูล	เกิดขึ้น 2 เหตุการณ์ (Q2)	อยู่ระหว่างสอบสวน	สูง
ระยะเวลาตอบสนอง DPO	ค่าเฉลี่ย 12 ชม./เหตุการณ์	เป็นไปตาม KPI	ปานกลาง
ข้อเสนอแนะจาก External Audit	5 ข้อเสนอแนะ (3 แก้แล้ว 2 กำลังดำเนินการ)	กำลังดำเนินการ	ต่ำ
ระดับความสอดคล้องนโยบาย	92%	ผ่านเกณฑ์	ดี

3. รายงานผลการตรวจสอบของ DPO

ชื่อเอกสาร: รายงานผลการตรวจสอบภายในของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

เนื้อหา

- ตรวจสอบเอกสาร Data Inventory และ Retention Policy
- รายงานเหตุละเมิดข้อมูล 1 กรณี และแนวทางการจัดการ
- ให้ข้อเสนอแนะการจัดทำ log การเข้าถึงข้อมูลสำหรับระบบใหม่

4. รายงานผลการตรวจสอบของผู้ตรวจสอบภายใน

ชื่อเอกสาร: Internal Audit Report – ระบบจัดเก็บและเข้าถึงข้อมูลส่วนบุคคล

เนื้อหา

- ตรวจสอบ 3 หน่วยงาน: แผนกบุคคล การเงิน Call Center
- พบการเก็บข้อมูลนานเกิน retention period ใน 2 หน่วย

- ให้คำแนะนำการใช้ automation เพื่อลบข้อมูลตามกำหนดเวลา

5. รายงานผลการตรวจสอบของผู้ตรวจสอบภายนอก/อิสระ

ชื่อเอกสาร: External Data Protection Audit – Summary Report

จัดทำโดย: บริษัท [ชื่อผู้ตรวจสอบภายนอก]

เนื้อหา

- ตรวจ compliance กับมาตรา 37 และประกาศปี 2565
- ระบุ 4 ข้อที่ยังไม่สอดคล้อง (เช่น ยังไม่มีการเก็บ Log การเข้าถึงข้อมูลกระดาษ)
- แนะนำให้ฝึกอบรม DPO เพิ่มเติม

6. รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ชื่อเอกสาร: Incident Report – การละเมิดข้อมูลส่วนบุคคล (Breach Report)

เนื้อหา

- เหตุการณ์: อีเมลผิดผู้รับ มีเอกสารแนบข้อมูลลูกค้า
- วันที่: 14 มีนาคม 2568
- แจ้งผู้ควบคุมข้อมูลและคณะกรรมการ PDPC ภายใน 72 ชั่วโมง
- บันทึกขั้นตอนการจัดการและแนวทางป้องกันซ้ำ

อ้างอิงกฎหมายที่เกี่ยวข้อง

กฎหมาย / ประกาศ	ข้อกำหนดที่เกี่ยวข้อง	ประเด็นหลัก
มาตรา 37 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	(1) (2) (3)	หน้าที่ของผู้ควบคุมข้อมูลและ DPO
ประกาศเรื่องมาตรการรักษาความมั่นคงปลอดภัย พ.ศ. 2565	ข้อ (4) (5)	การตรวจสอบและรายงานการดำเนินงาน
ประกาศฯ เรื่องการแจ้งเหตุละเมิด พ.ศ. 2565	ข้อ 5 (5)	การบันทึกเหตุและส่งรายงานอย่างครบถ้วน

สรุปสิ่งที่ควรดำเนินการให้ครบถ้วน

สิ่งที่ต้องจัดทำ	สถานะ
นโยบายการรายงานข้อมูลการจัดการ	ต้องมี (จัดทำโดย DPO)
รายงาน Dashboard สรุปผลตรวจสอบ	อัปเดตทุกไตรมาส

รายงานการตรวจสอบ DPO Internal External	เก็บครบตามรอบการตรวจสอบ
รายงานเหตุละเมิดข้อมูลส่วนบุคคล	ภายใน 72 ชม. พร้อมสรุป

บทที่ 12

การยื่นคำขอ และหลักเกณฑ์การให้คะแนน

หลักเกณฑ์การให้คะแนน

หลักเกณฑ์การคิดคะแนนการประเมิน มีรายละเอียดดังนี้

กำหนดหลักเกณฑ์การให้คะแนนสำหรับหน่วยงานที่ได้ดำเนินการตามเกณฑ์ที่กำหนด ซึ่งมีช่วงคะแนน 0-3 คะแนน จำนวนทั้งหมด 337 ข้อ คะแนนเต็มคือ 1,011 คะแนน สำหรับองค์กรขนาดใหญ่ที่มีการประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมากและหลากหลาย มีต้นทุนทรัพยากรสูง ซึ่งมีการบริหารจัดการและกำกับดูแลข้อมูลส่วนบุคคลที่ดี มีอัตราค่าจ้างด้านทรัพยากรบุคคลที่เพียงพอ รวมถึงมีการดำเนินงานโดยเกี่ยวข้องกับผู้ให้บริการภายนอกอื่น ๆ หรือมีการใช้บริการผู้ตรวจสอบภายนอก เป็นต้น จะใช้การประเมินทั้งหมด 337 ข้อ คะแนนเต็มคือ 1,011 คะแนน หลักเกณฑ์การให้คะแนนทั้งหมด 337 ข้อ แบ่งออกเป็นข้อกำหนดกำกับภาค จำนวน 160 ข้อ และข้อที่เป็นแนวปฏิบัติที่ดีจำนวน 177 ข้อ

กรณีเป็นองค์กรขนาดเล็ก ประมวลผลข้อมูลส่วนบุคคลหลากหลาย หรือมีต้นทุนทรัพยากรดำเนินธุรกิจตามที่กำหนดด้านบน หรือเป็นองค์กรขนาดเล็ก ข้อกำหนด/การดำเนินการตามหลักเกณฑ์การให้คะแนนจะลดหลั่นกันไปแล้วแต่กรณี โดยอาจมีบางด้านหรือบางข้อกำหนด/การดำเนินการที่ไม่ถูกนำมาประเมินเป็นคะแนน (N/A) ทั้งนี้ เพื่อเป็นการส่งเสริมให้องค์กรทุกขนาดที่ขอ Trustmark ระดับของเครื่องหมายและเกณฑ์การให้เครื่องหมายจะคล้ายถึงเนื้อหาเดียวกันคือพยายามปรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดหรือที่ดีเกินมาตรฐาน โดยที่หน่วยงาน/องค์กรที่ขอต้องดำเนินการตามเกณฑ์ดังนี้

การประเมินผลการให้ Trustmark โดยที่หน่วยงาน/องค์กรที่ขอ ต้องดำเนินการตามเกณฑ์ดังนี้

ตาราง 2-12 สรุปหลักเกณฑ์การให้คะแนน

วงคะแนน (Score Range)	จำนวน หลักเกณฑ์ (ข้อ)	คะแนนรวม (คะแนน)	เกณฑ์ (Threshold)	เครื่องหมาย (Badge/Color)
0-3	337	1,011	ร้อยละ 80	สีทอง
			ร้อยละ 70	สีเงิน

		ร้อยละ 60	สี่บรอนซ์
		ประกาศนียบัตร	

หมายเหตุ: ในกรณีที่คะแนนรวมของผู้ยื่นคำขอ ไม่ถึงเกณฑ์ที่จะได้รับเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล Trustmark แม้ปฏิบัติได้ครบถ้วนตามที่กฎหมายกำหนด ผู้ยื่นคำขอจะได้รับประกาศนียบัตรการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล PDPA Compliance Certificate



ขั้นตอนการยื่นขอ Trustmark

ขั้นตอน	รายละเอียด	หมายเหตุ/เงื่อนไข
1. ผู้ยื่นคำขอ	ศึกษาข้อมูลและประกาศต่าง ๆ จากเว็บไซต์ PDPC	-
2. ยื่นคำขอ (สส.01)	ยื่นคำขอไปยัง สคส.	-

3. ตรวจสอบคุณสมบัติ (ภายใน 7 วัน)	- ถ้าไม่ผ่าน → ยกเลิกคำขอ- ถ้าผ่าน → ดำเนินการขั้นตอนต่อไป	-
4. ชำระค่าธรรมเนียมการสมัครและยื่นคำขอ (สส. 02)	แนบเอกสารหลักฐานการชำระเงิน	-
5. ตรวจสอบการชำระเงิน	ยืนยันเรื่องเข้าสู่กระบวนการประเมิน	-
6. ตรวจสอบรายละเอียดและนัดหมาย	นัดหมายเพื่อยืนยันการรับคำขอ	-
7. ชำระค่าธรรมเนียมการตรวจประเมิน	พร้อมแนบเอกสารหลักฐาน	-
8. การตรวจประเมิน (ภายใน 7 วันหลังการชำระเงิน)	- ถ้าไม่ครบถ้วน → แจ้งกลับให้แก้ไข/เพิ่มเติม (ภายใน 30 วัน)- ถ้าครบถ้วน → เข้าสู่การประเมินตามหลักเกณฑ์	-
9. การประเมินมาตรฐานตามหลักเกณฑ์ (ภายใน 15 วัน)	- ถ้าไม่ผ่าน → สามารถแก้ไขตามคำแนะนำและยื่นใหม่- ถ้าผ่าน → เข้าสู่ขั้นตอนการยืนยัน	-
10. เสนอผลการประเมินมาตรฐาน	ส่งผลการประเมินไปยังผู้ยื่นคำขอ	-
11. ยืนยันขอรับเครื่องหมายมาตรฐาน	- ชำระค่าธรรมเนียมการรับรองมาตรฐาน (ภายใน 7 วัน)- ถ้าชำระไม่ทัน → ยกเลิก/สิ้นสุดกระบวนการ- ถ้าชำระแล้ว → ออกเครื่องหมาย	-
12. ออกเครื่องหมายรับรองมาตรฐาน (ภายใน 15 วัน)	ตรวจสอบการชำระและออก Trustmark	“สคส.” ตรวจสอบติดตามผลการรับรองมาตรฐานเป็นระยะ (อายุ 1 ปี)



สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
THE OFFICE OF THE PERSONAL DATA PROTECTION COMMITTEE

เลขที่ 120 หมู่ 3 ชั้น 5-7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา
5 ธันวาคม 2550 (อาคาร ซี) ซอยแจ้งวัฒนะ 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง
เขตหลักสี่ กรุงเทพฯ 10210



WWW.PDPC.OR.TH



PDPC THAILAND



PDPC THAILAND



SARABAN@PDPC.OR.TH