เกณฑ์การตรวจมาตรฐาน การคุ้มครองข้อมูลส่วนบุคคล

Personal Data Protection Standards Inspection Criteria

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
The Office of the Personal Data Protection Committee (PDPC)

คำนำ

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้จัดทำ “แนวทางปฏิบัติและหลักเกณฑ์การประเมินความสอดคล้อง ด้านการคุ้มครองข้อมูลส่วนบุคคล ทั้ง 10 ด้าน” รวม 337 ข้อ เพื่อกำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับมาตรฐานสากล

เกณฑ์การตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลนี้ จัดทำขึ้นด้วยการนำแนวคิด Privacy Maturity Model (PMM) มาประยุกต์ใช้ ร่วมกับแนวทางปฏิบัติและหลักเกณฑ์การประเมินความสอดคล้อง เพื่อลดความซ้ำซ้อนของเนื้อหา ลดภาระด้านเอกสาร และเพิ่มประสิทธิภาพในการตรวจประเมินความสอดคล้องด้านการคุ้มครองข้อมูลส่วนบุคคล โดยมีเป้าหมายเพื่อสร้างความเชื่อมั่น ยกระดับมาตรฐาน และส่งเสริมให้หน่วยงานที่เกี่ยวข้องปฏิบัติตามแนวทางการคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม

การจัดทำเกณฑ์การตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ เพื่อให้องค์กรหรือบุคคลที่สนใจในการยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลนำไปประกอบการพิจารณาวางแนวทางการดำเนินงานตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในการขอรับการตรวจสอบและรับรองความสอดคล้องด้านการคุ้มครองข้อมูลส่วนบุคคล อีกทั้งเป็นส่วนส่งเสริมให้ทุกฝ่ายที่เกี่ยวข้องกับกฎหมายว่าด้วยการคุ้มครองส่วนบุคคลได้ดำเนินงานตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลต่อไป

คณะผู้จัดทำ

สารบัญ

หน้า

เกณฑ์การตรวจมาตรฐานการคุ้มครองครองข้อมูลส่วนบุคคล

เพื่อประเมินความพร้อมของการคุ้มครองข้อมูลส่วนบุคคลทั้งในหน่วยงานภาครัฐและภาคเอกชน สำนักงานจึงได้จัดทำเกณฑ์การตรวจมาตรฐานการคุ้มครองครองข้อมูลส่วนบุคคล โดยแบ่งออกเป็น 4 กลุ่ม จำนวน 128 ข้อ ดังนี้

กลุ่มที่ 1 นโยบายและการบริหารจัดการ

ด้านที่ 1 องค์กรและการกำกับดูแล (Organization and Oversight)
ด้านที่ 2 นโยบายและแนวปฏิบัติ (Policies and Procedures)

กลุ่มที่ 2 การพัฒนาทรัพยากรบุคคลขององค์กร

ด้านที่ 3 การอบรมและการสร้างความตระหนักรู้ (Training and awareness)

กลุ่มที่ 3 กระบวนการและขั้นตอนการทำงาน

ด้านที่ 4 สิทธิของเจ้าของข้อมูลส่วนบุคคล (Individual Rights)
ด้านที่ 5 การแจ้งวัตถุประสงค์และความโปร่งใส (Transparency)
ด้านที่ 6 การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและการกำหนดฐานทางกฎหมาย (ROPA and Lawful Basis)
ด้านที่ 7 ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement and Data Processing Agreement)
ด้านที่ 8 ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Risks and Data Protection Impact Assessment)

กลุ่มที่ 4 ระบบเทคโนโลยีและความมั่นคงปลอดภัย และการแจ้งเหตุละเมิด

ด้านที่ 9 มาตรการรักษาความมั่นคงปลอดภัย (Data Security)
ด้านที่ 10 การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Breach Response)

โดยมีการจำแนกรายละเอียดการคุ้มครองข้อมูลส่วนบุคคลแต่ละด้าน ดังนี้

ด้านที่	ด้านการคุ้มครองข้อมูลส่วนบุคคล	จำนวนข้อ	จำแนกเป็น	
			Require by law	Best Practice
1	องค์กรและการกำกับดูแล	13	10	3
2	นโยบายและแนวปฏิบัติ	10	10	0
3	การอบรมและการสร้างความตระหนักรู้	7	5	2
4	สิทธิของเจ้าของข้อมูลส่วนบุคคล	11	9	2
5	การแจ้งวัตถุประสงค์และความโปร่งใส	11	7	4
6	การจัดทำบันทึกรายการและฐานทางกฎหมาย	17	14	3
7	ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล	19	14	5
8	ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล	7	5	2
9	มาตรการรักษาความมั่นคงปลอดภัย	17	17	0
10	การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	16	15	1
รวมจำนวนข้อทั้งสิ้น		**128**	**106**	**22**

กลุ่มที่ 1

นโยบายและการบริหารจัดการ

ด้านที่ 1 องค์กรและการกำกับดูแล (Organization and Oversight)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
1	องค์กรต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ตามมาตรา 41 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หากเข้าข่ายตามที่กฎหมายกำหนด (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 1.2.1)	การปฏิบัติงานหรือการดำเนินการของ DPO ครบถ้วนตามมาตรา 42 ตัวอย่างหลักฐาน: • รายงานการประชุมของผู้บริหาร หรือคณะกรรมการที่ทำหน้าที่กำกับดูแลด้าน PDPA • รายงานผลการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลของ DPO ที่มีเนื้อหาเรื่องการทำหน้าที่ตามกฎหมาย • เอกสารคำสั่งแต่งตั้ง DPO (ระบุหน้าที่ให้ครบทุกด้านตามที่กฎหมายกำหนด)
2	องค์กรต้องจัดสรรอำนาจ หน้าที่ และทรัพยากรที่เพียงพอให้แก่ DPO เพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพและเป็นอิสระ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 1.2.2)	ให้อำนาจ DPO เข้าถึงข้อมูลองค์กรและจัดสรรทรัพยากรสนับสนุน DPO ตัวอย่างหลักฐาน: • ภาพถ่ายอุปกรณ์ หรือเครื่องมือที่องค์กรจัดให้ DPO • บันทึกเอกสารการให้อำนาจ DPO เข้าถึงฐานข้อมูลองค์กร และบันทึกที่แสดงว่า DPO มีสิทธิเข้าถึงฐานข้อมูลองค์กร

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
3	กรณีที่องค์กรไม่เข้าข่ายที่ต้องแต่งตั้ง DPO ตามกฎหมาย องค์กรต้องมอบหมายบุคลากรที่มีความเหมาะสมรับผิดชอบงานด้านการคุ้มครองข้อมูลส่วนบุคคลแทน พร้อมจัดสรรทรัพยากรที่เพียงพอที่จะดำเนินการต่าง ๆ ให้สอดคล้องกับหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 1.2.5)	จัดให้มีพนักงานรับผิดชอบด้าน PDPA และสนับสนุนทรัพยากร ตัวอย่างหลักฐาน: • รายงานการประชุมของผู้บริหาร หรือคณะกรรมการที่ทำหน้าที่กำกับดูแลด้าน PDPA • หลักฐานการแต่งตั้งหรือมอบหมายให้บุคคลใดบุคคลหนึ่งเป็นผู้รับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล • ภาพถ่ายอุปกรณ์หรือเครื่องมือที่องค์กรสนับสนุนหรือจัดหาให้
4	องค์กรต้องกำหนดให้ DPO มีความเป็นอิสระและรายงานตรงต่อผู้บริหารระดับสูง โดยต้องไม่มีผลประโยชน์ทับซ้อนในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 1.3.3)	ต้องจัดการให้ DPO ทำงานอย่างอิสระและไม่มีประโยชน์ทับซ้อน ตัวอย่างหลักฐาน: • รายงานการประชุมของผู้บริหาร หรือคณะกรรมการที่ทำหน้าที่กำกับดูแลด้าน PDPA • นโยบายขององค์กรที่ระบุชัดว่า DPO มีอิสระโดยไม่มีผลประโยชน์ทับซ้อน หรือ • สัญญาระบุชัดว่าให้ DPO เข้ามาทำงานโดยมีอิสระโดยไม่มีผลประโยชน์ทับซ้อน

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
5	องค์กรต้องเปิดช่องทางให้ DPO สามารถให้คำแนะนำแก่ผู้บริหารระดับสูงได้โดยตรง รวมถึงสามารถรายงานข้อกังวลด้านการคุ้มครองข้อมูลส่วนบุคคลได้อย่างอิสระ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 1.3.4)	ต้องมีช่องทาง หรือผังองค์กร หรือสายการบังคับบัญชาให้ DPO ให้คำแนะนำโดยตรงต่อผู้มีอำนาจตัดสินใจระดับสูงและแจ้งข้อกังวลได้กับผู้บริหารระดับสูงสุดได้ ตัวอย่างหลักฐาน: • รายงานการประชุมของผู้บริหาร หรือคณะกรรมการที่ทำหน้าที่กำกับดูแลด้าน PDPA • นโยบายขององค์กรที่ระบุชัดว่า DPO มีอิสระโดยไม่มีผลประโยชน์ทับซ้อน หรือ • สัญญาระบุชัดว่าให้ DPO เข้ามาทำงานโดยมีอิสระโดยไม่มีผลประโยชน์ทับซ้อน
6	องค์กรต้องจัดให้มีบุคลากรและกลไกสนับสนุน DPO เพื่อช่วยในการจัดการและกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 1.4.1)	ต้องดำเนินการให้เจ้าหน้าที่ปฏิบัติงานเกี่ยวกับ PDPA และกำกับข้อมูลจัดการและดูแลข้อมูล อย่างมีประสิทธิภาพและรักษาความปลอดภัยฯ อย่างเหมาะสม ตัวอย่างหลักฐาน: • รายงานการประชุมของผู้บริหาร หรือคณะกรรมการที่ทำหน้าที่กำกับดูแลด้าน PDPA • นโยบาย ประกาศ คำสั่ง แนวปฏิบัติที่ระบุถึงมาตรการรักษาความมั่นคงปลอดภัยฯ โดยเอกสารต้องระบุให้เห็นว่า “มีมาตรการรักษาความมั่นคงปลอดภัยฯ สำหรับพนักงานทุกด้าน”

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
7	องค์กรต้องจัดตั้งคณะทำงานหรือคณะกรรมการกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมการติดตาม KPI ปัญหาและความเสี่ยงที่เกี่ยวข้อง (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 1.5.5)	คณะทำงาน DPO ต้องดำเนินการเกี่ยวกับ PDPA ดังนี้ (1) ระบุปัญหา (2) ความเสี่ยง (3) ทำตัวชี้วัด (KPI) ครอบคลุมการดำเนินงาน PDPA ตัวอย่างหลักฐาน: • เอกสารแต่งตั้งคณะทำงานของ DPO โดยมีรายชื่อ DPO เป็นคณะทำงาน • รายงานการประชุมของผู้บริหาร หรือคณะกรรมการที่ทำหน้าที่กำกับดูแลด้าน PDPA
8	ผู้บริหารระดับสูงขององค์กรต้องพิจารณาประเด็นด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล และความเสี่ยงที่จัดทำโดยคณะทำงานของ DPO อย่างสม่ำเสมอ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 1.5.7)	คณะทำงานของ DPO รายงานประเด็น PDPA และการกำกับดูแลข้อมูล และความเสี่ยงองค์กรไปยังคณะกรรมการบริษัท หรือผู้บริหารสูงสุด ตัวอย่างหลักฐาน: • รายงานการประชุมคณะทำงานของ DPO หรือรายงานการประชุมของผู้บริหาร หรือคณะกรรมการที่ทำหน้าที่กำกับดูแลด้าน PDPA โดยต้องมีข้อความแสดงให้เห็นว่า “การคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลข้อมูล รวมถึงความเสี่ยงขององค์กร” และเป็นการรายงานโดยคณะทำงานของ DPO

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
9	องค์กรต้องมีการรายงานปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูลและความเสี่ยงใด ๆ ที่เกิดขึ้นไปยังคณะทำงานของ DPO (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 1.6.4)	กลุ่มปฏิบัติการ (พนักงานในระดับปฏิบัติการของฝ่ายงาน) รายงานปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูลรวมถึงประเด็นความเสี่ยงใดๆขององค์กรที่เกิดขึ้นไปยังคณะทำงานของ DPO ครบถ้วน ตัวอย่างหลักฐาน: • วาระการประชุม และรายงานการประชุมของคณะทำงาน DPO หรือกลุ่มปฏิบัติการ โดยต้องมีข้อความแสดงให้เห็นว่า “มีปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล และความเสี่ยงใด ๆ ที่เกิดขึ้น”
10	องค์กรมีการพัฒนากระบวนการและเครื่องมือเพิ่มเติมเพื่อสนับสนุนการทำงานของ DPO หรือไม่ และ DPO มีการตรวจสอบการดำเนินการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายและประกาศที่เกี่ยวข้อง (สอดคล้องกับ Privacy Maturity Model: PMM)	

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
11	องค์กรต้องประกาศแต่งตั้ง DPO อย่างเป็นทางการเป็นลายลักษณ์อักษร (สอดคล้องกับ Privacy Maturity Model: PMM)	
12	องค์กรต้องเผยแพร่ข้อมูลช่องทางการติดต่อ DPO อย่างชัดเจนผ่านสื่อสารต่าง ๆ ขององค์กร เพื่อให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกรับทราบ (สอดคล้องกับ Privacy Maturity Model: PMM)	
13	องค์กรต้องมีการตรวจสอบการปฏิบัติของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ว่าสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (สอดคล้องกับ Privacy Maturity Model: PMM)	

ด้านที่ 2 นโยบายและแนวปฏิบัติ (Policies and Procedures)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
14	องค์กรต้องจัดทำนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมการบริหารจัดการและมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 2.1.2)	จัดทำนโยบาย PDPA ที่มีประเด็นครอบคลุมครบถ้วน ตัวอย่างหลักฐาน: • นโยบาย PDPA โดยต้องมีข้อความแสดงเป็นหมวดหมู่ในด้าน “การบริหารจัดการข้อมูลส่วนบุคคล การรักษาความปลอดภัยของข้อมูล การกำหนดหน้าที่แก่พนักงาน”
15	องค์กรต้องจัดทำนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล พร้อมระบุบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องอย่างชัดเจน (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 2.1.4)	จัดทำนโยบาย PDPA ที่มีประเด็นครอบคลุมครบถ้วน ตัวอย่างหลักฐาน: • นโยบาย PDPA โดยต้องมีข้อความแสดงเป็นหมวดหมู่ให้เห็นว่า “การบริหารจัดการข้อมูลส่วนบุคคลการรักษาความปลอดภัยของข้อมูล การกำหนดหน้าที่แก่พนักงาน” • แนวทางปฏิบัติ และคู่มืออื่น ๆ เพื่อสนับสนุนนโยบายคุ้มครองข้อมูลส่วนบุคคล สำหรับพนักงานและผู้ที่เกี่ยวข้อง

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
16	องค์กรต้องกำหนดกระบวนการทบทวนและอนุมัตินโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลโดยผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมาย (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 2.2.2)	จัดให้มีการประชุมเพื่อทบทวนนโยบายและแนวปฏิบัติ โดยต้องประเมินความเหมาะสมของกระบวนการปฏิบัติงานให้เป็นไปตามนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลตามกรอบระยะเวลาที่แน่นอน ตัวอย่างหลักฐาน: • รายงานการประชุมเพื่อทบทวนนโยบายและแนวปฏิบัติ โดยต้องมีข้อความแสดงเป็นหมวดหมู่ให้เห็นว่า “ก) มีการทบทวนนโยบายและแนวปฏิบัติ ข) ต้องประเมินกระบวนการปฏิบัติงานซึ่งอาจต้องทำแบบประเมิน ค) ระบุว่ามีกรอบระยะเวลาการดำเนินการทุกๆ ... เดือน”
17	องค์กรต้องมีการทบทวนนโยบายและขั้นตอนปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างทันท่วงทีเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น มีการเปลี่ยนแปลงต่อองค์กรที่สำคัญ ๆ การตัดสินใจของหน่วยงานกำกับดูแล หรือการเปลี่ยนแปลงในแนวทางปฏิบัติงานของหน่วยงานผู้กำกับดูแล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 2.2.3)	องค์กรมีการทบทวนโยบาย PDPA และแนวปฏิบัติสำหรับ PDPA อย่างไม่ล่าช้าเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญต่อองค์กรที่สำคัญ ๆ การตัดสินใจของสำนักงานคุ้มครองข้อมูลส่วนบุคคลหรือการเปลี่ยนแปลงในแนวทางปฏิบัติของหน่วยงานที่กำกับดูแล ตัวอย่างหลักฐาน: • รายการประชุม

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
18	องค์กรต้องแจ้งให้พนักงานทุกคนทราบถึงนโยบายและขั้นตอนปฏิบัติที่ปรับปรุงใหม่ เพื่อให้เข้าใจและปฏิบัติได้อย่างถูกต้อง (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 2.3.2)	องค์กรแจ้งให้พนักงานได้ทราบเกี่ยวกับนโยบายและแนวปฏิบัติใหม่ ตัวอย่างหลักฐาน: • รายงานการประชุมชี้แจงนโยบายและแนวปฏิบัติที่ปรับปรุงใหม่ • เอกสารนโยบายและแนวปฏิบัติที่ปรับปรุงใหม่เพื่อเผยแพร่แก่พนักงาน
19	องค์กรต้องจัดทำนโยบายและขั้นตอนเพื่อให้แน่ใจว่าประเด็นการคุ้มครองข้อมูลได้รับการพิจารณาเมื่อมีการออกแบบและดำเนินการระบบ บริการ ผลิตภัณฑ์ และแนวทางธุรกิจที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลได้รับการคุ้มครองโดยค่าเริ่มต้น (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 2.4.2)	ตัวอย่างหลักฐาน: • นโยบายเกี่ยวกับการกำหนดค่าเริ่มต้นในการออกแบบและพัฒนาระบบ ผลิตภัณฑ์ และบริการ • ระบบเทคโนโลยีสารสนเทศ ที่ช่วยในการกำหนดค่าเริ่มต้นในการออกแบบและพัฒนาระบบ ผลิตภัณฑ์ และบริการ
20	องค์กรต้องกำหนดวิธีการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคล การป้องกันสิทธิ์ส่วนบุคคล ที่รวมถึงการจำกัดข้อมูลให้น้อยที่สุด(Data Minimization) การจำกัดวัตถุประสงค์การใช้งาน (Purpose Limitation) และการทำเป็นข้อมูลแฝง (Pseudonymization) (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 2.4.3)	ตัวอย่างหลักฐาน: • แนวปฏิบัติเพื่อกำหนดค่าเริ่มต้นในเรื่องการจำกัดข้อมูลให้น้อยที่สุด การจำกัดวัตถุประสงค์การใช้งาน และการทำเป็นข้อมูลแฝง • ระบบเทคโนโลยีสารสนเทศเพื่อกำหนดค่าเริ่มต้นในเรื่องการจำกัดข้อมูลให้น้อยที่สุด การจำกัดวัตถุประสงค์การใช้งาน และการทำเป็นข้อมูลแฝง

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
21	องค์กรมีการจัดทำแนวทางปฏิบัติและคู่มือในแต่ละกระบวนการย่อยเพื่อรองรับนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล และเพื่อให้พนักงานและผู้ที่เกี่ยวข้องสามารถปฏิบัติได้อย่างถูกต้อง (สอดคล้องกับ Privacy Maturity Model: PMM)	
22	องค์กรมีการทบทวนนโยบายและกระบวนการด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่ายังคงมีความถูกต้องและทันสมัย (สอดคล้องกับ Privacy Maturity Model: PMM)	
23	องค์กรมีการวัดผลดำเนินการหลังจากประกาศนโยบายและแนวทางปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลโดยสะท้อนให้เห็นว่า นโยบายดังกล่าวได้เข้ามาช่วยในการปกป้องข้อมูลส่วนบุคคลหรือลดความเสี่ยงต่างๆ ที่อาจเกิดขึ้น (เช่น ลดช่องว่างที่เกิดขึ้นจากการดำเนินการไม่ครบถ้วนตามกฎหมาย เป็นต้น) (สอดคล้องกับ Privacy Maturity Model: PMM)	

กลุ่มที่ 2

การพัฒนาทรัพยากรบุคคลขององค์กร

ด้านที่ 3 การอบรมและการสร้างความตระหนักรู้ (Training and awareness)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
24	องค์กรต้องจัดทำแผนการสร้างความตระหนักครอบคลุมไปถึงพนักงานทุกท่านที่อยู่ในกระบวนการปกป้องข้อมูลส่วนบุคคล เช่น การจัดการคำขอต่างๆ การแชร์ข้อมูลการรักษาความมั่นคงปลอดภัยของข้อมูล การละเมิดข้อมูล การบริหารจัดการต่างๆ ที่ เกี่ยวข้องกับข้อมูล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 3.1.2)	ตัวอย่างหลักฐาน: • เอกสารแสดงเนื้อหาของการอบรม
25	องค์กรต้องจัดสรรทรัพยากรที่เพียงพอสำหรับการดำเนินการฝึกอบรมและกิจกรรมสร้างความตระหนักรู้ให้แก่บุคลากรทุกระดับ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 3.1.6)	มีเอกสารที่ใช้ในการอบรมซึ่งสามารถเข้าถึงได้โดยง่าย โดยจัดทำในรูปแบบต่าง ๆ เช่น อิเล็กทรอนิกส์ หรือส่งผ่านทางอีเมล เป็นต้น ตัวอย่างหลักฐาน: • เอกสารที่ใช้ในการอบรม อาจจัดทำในรูปแบบอิเล็กทรอนิกส์
26	องค์กรต้องมีการทบทวนหลักสูตรการอบรมเพื่อสร้างความตระหนักในการปฏิบัติงานให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครอง ข้อมูลส่วนบุคคล และแนวทางการฝึกอบรมเพื่อให้มีความเหมาะสม ถูกต้อง และ	ตัวอย่างหลักฐาน: • รายงานการประชุมเพื่อทบทวนหลักสูตรสร้างความตระหนักของการฝึกอบรม

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
	เป็นปัจจุบัน (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 3.1.3)	
27	องค์กรต้องจัดให้พนักงานเข้ารับการฝึกอบรมเพื่อเป็นการเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล ภายในระยะเวลาที่เหมาะสมหรือได้รับการฝึกอบรมภายใน 1 เดือน นับตั้งแต่วันที่เริ่มต้นปฏิบัติงาน (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 3.2.2)	มีการอบรมและแบบทดสอบเพื่อประเมินผลเป็นการเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคลภายในระยะเวลาที่เหมาะสม หรือได้รับการฝึกอบรมภายใน 1 เดือน นับตั้งแต่วันที่เริ่มต้นปฏิบัติงาน ตัวอย่างหลักฐาน: • เอกสารเกี่ยวกับการจัดอบรมเกี่ยวกับการเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล • แบบทดสอบเกี่ยวกับการเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล
28	องค์กรต้องจัดให้พนักงานเข้ารับการฝึกอบรมเพิ่มเติมในช่วงเวลาที่เหมาะสม (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 3.2.4)	มีการจัดให้พนักงานได้รับการฝึกอบรมเพิ่มเติมภายในระยะเวลาที่เหมาะสม เช่น ทุก 6 เดือน และมีการทดสอบเพื่อประเมินผลหลังการฝึกอบรม ตัวอย่างหลักฐาน: • เอกสารเกี่ยวกับการฝึกอบรมเพิ่มเติม • แบบทดสอบเพื่อประเมินผลหลังการฝึกอบรมเพิ่มเติม

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
29	องค์กรต้องมีการประเมินผลหลังการอบรม เพื่อทดสอบความรู้ความเข้าใจและความพร้อมของพนักงาน โดยกำหนดเกณฑ์ขั้นต่ำในการผ่านการประเมิน (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 3.4.1)	มีการประเมินผลภายหลังการอบรม และมีการรายงานต่อพนักงานอาวุโสเกี่ยวกับผลการทดสอบของพนักงาน เพื่อวางแผนการฝึกอบรมในอนาคต ตัวอย่างหลักฐาน: • แบบทดสอบประเมินผลการอบรมของพนักงาน • สรุปผลว่าผ่านเกณฑ์การประเมินหรือไม่
30	องค์กรได้จัดให้มีการทบทวนการอบรมและสร้างความตระหนักเรื่องการปกป้องข้อมูลส่วนบุคคลอยู่เป็นประจำ อย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงของนโยบายและกระบวนการด้านการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ (สอดคล้องกับ Privacy Maturity Model: PMM)	

กลุ่มที่ 3

กระบวนการและขั้นตอนการทำงาน

ด้านที่ 4 สิทธิของเจ้าของข้อมูลส่วนบุคคล (Individual Rights)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
31	องค์กรต้องแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคลอย่างชัดเจน รวมถึงวิธีการใช้สิทธิตามที่กฎหมายกำหนด เช่น การเข้าถึง ขอสำเนา แก้ไข หรือ ลบข้อมูล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 4.1.1)	ตัวอย่างหลักฐาน: • Privacy Notice แจ้งเรื่อง เรื่องสิทธิและวิธีการใช้สิทธิตามกฎหมายของเจ้าของข้อมูลส่วนบุคคล รวมถึงการร้องเรียนองค์กรเนื่องจากพบปัญหาในการขอใช้สิทธิของตน และรายละเอียดการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
32	องค์กรต้องจัดทำนโยบายและขั้นตอนปฏิบัติในการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย(โดยมีเอกสาร SOP SLA หรือขั้นตอนกำกับอย่างชัดเจน) (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 4.1.3)	ตัวอย่างหลักฐาน: • Standard Operating Procedures (SOP) สำหรับกระบวนการขอใช้สิทธิตามกฎหมาย โดยอาจแยกเป็นกระบวนการใช้สิทธิแต่ละประเภท • กฎบัตร (Charter) ของคณะกรรมการหรือฝ่ายงานที่ดูแลเกี่ยวกับการจัดการและตอบสนองการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
33	ในกรณีที่องค์กรจะปฏิเสธการดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล องค์กรต้องจัดทำบันทึกการปฏิเสธคำขอดังกล่าว พร้อมด้วยเหตุผลไว้ในบันทึกรายการ	มีช่องสำหรับบันทึกการปฏิเสธคำขอพร้อมด้วยเหตุผลใน ROPA และมีกระบวนการแจ้งเหตุผลการปฏิเสธดังกล่าวไปยังเจ้าของข้อมูลส่วนบุคคล

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
	ของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA) และแจ้งเหตุผลของการปฏิเสธหรือข้อยกเว้นใด ๆ ไปยังเจ้าของข้อมูลส่วนบุคคลที่ขอใช้สิทธิ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 4.4.2)	ตัวอย่างหลักฐาน: • ROPA มีช่องสำหรับบันทึกการปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล • เอกสารการแจ้งเหตุผลการปฏิเสธคำขอใช้สิทธิไปยังเจ้าของข้อมูลส่วนบุคคล
34	องค์กรต้องจัดให้มีขั้นตอนและกระบวนการตามความเหมาะสมได้สัดส่วนและสมเหตุสมผลในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่เก็บไว้ และหากจำเป็นก็สามารถทำการแก้ไขข้อมูลนั้นได้ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 4.6.1)	มีขั้นตอนและระบบเทคโนโลยีสารสนเทศในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ตัวอย่างหลักฐาน: • เอกสารแสดงขั้นตอนและกระบวนการในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม • ระบบเทคโนโลยีสารสนเทศในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
35	องค์กรต้องดำเนินการลบข้อมูลส่วนบุคคลจากระบบสำรองข้อมูล รวมถึงระบบที่ใช้งานอยู่เมื่อจำเป็น และทำการชี้แจงให้บุคคลนั้นทราบอย่างชัดเจนว่าข้อมูลของพวกเขาจะถูกจัดการอย่างไร	มีการดำเนินการแก่เจ้าของข้อมูลส่วนบุคคลที่ขอใช้สิทธิดำเนินการลบข้อมูลส่วนบุคคลออกจากระบบสำรองและระบบใช้งานจริง โดยใช้ระบบเทคโนโลยีสารสนเทศ

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
	(สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 4.7.1)	ตัวอย่างหลักฐาน: • แบบฟอร์มการขอใช้สิทธิลบข้อมูลส่วนบุคคล • แบบฟอร์มและเอกสารสำหรับชี้แจงแก่เจ้าของข้อมูลส่วนบุคคลเกี่ยวกับขั้นตอนหรือวิธีการในการลบหรือทำลายข้อมูลส่วนบุคคล • ระบบเทคโนโลยีสารสนเทศในการลบข้อมูลส่วนบุคคลที่มีประสิทธิภาพ
36	ในกรณีที่เป็นไปได้และหากบุคคลร้องขอองค์กรสามารถส่งข้อมูลไปยังองค์กรอื่นด้วยวิธีการทางอิเล็กทรอนิกส์ได้โดยตรง (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 4.9.2)	จัดให้มีการส่งข้อมูลไปยังองค์กรอื่นด้วยวิธีการทางอิเล็กทรอนิกส์ได้โดยตรงและการส่งหรือโอนข้อมูลส่วนบุคคลมีความปลอดภัยเป็นไปตามมาตรฐานขั้นต่ำตามที่กฎหมายกำหนด ตัวอย่างหลักฐาน: • เอกสารหรือหลักฐานแสดงการส่งข้อมูลไปยังองค์กรอื่นด้วยวิธีการทางอิเล็กทรอนิกส์
37	องค์กรต้องแจ้งให้เจ้าของข้อมูลทราบถึงสิทธิในการร้องเรียนต่อ สคส. หรือกรรมการผู้เชี่ยวชาญในประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Privacy Notice/Privacy Policy) (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 4.11.2)	มีรายละเอียดแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเกี่ยวกับสิทธิในการร้องเรียนต่อ สคส. หรือกรรมการผู้เชี่ยวชาญใน Privacy Notice/Privacy Policy พร้อมแนะนำขั้นตอนในการร้องเรียนอย่างชัดเจน ตัวอย่างหลักฐาน: • Privacy Notice/Privacy Policy ขององค์กร

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
38	องค์กรมีการปรับปรุงนโยบายและกระบวนการการจัดการกับคำขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคลโดยวิเคราะห์จากแนวโน้มคำขอต่าง ๆ (สอดคล้องกับ Privacy Maturity Model: PMM)	
39	องค์กรมีการแจ้งให้เจ้าของข้อมูลทราบถึงช่องทางในการขอเข้าถึงและขอสำเนาข้อมูลส่วนบุคคลตนเอง (Right to Access) (สอดคล้องกับ Privacy Maturity Model: PMM)	
40	องค์กรสามารถระงับหรือจำกัดการประมวลผลข้อมูลส่วนบุคคลในลักษณะที่เหมาะสมกับประเภทของการประมวลผลและระบบที่เกี่ยวข้อง เช่น การย้ายข้อมูลไปยังระบบอื่นชั่วคราวหรือลบออกจากเว็บไซต์ (สอดคล้องกับ Privacy Maturity Model: PMM)	
41	องค์กรมีการวัดผลการจัดการคำขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคลได้ว่าสามารถจัดการได้ครบถ้วน (สอดคล้องกับ Privacy Maturity Model: PMM)	

ด้านที่ 5 การแจ้งวัตถุประสงค์และความโปร่งใส (Transparency)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
42	องค์กรต้องมีการแจ้งรายละเอียดเกี่ยวกับข้อมูลการติดต่อที่เกี่ยวข้อง ได้แก่ (1) ข้อมูลชื่อและรายละเอียด รวมถึงสถานที่ติดต่อและวิธีการติดต่อของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) (2) ข้อมูลชื่อและรายละเอียด รวมถึงสถานที่ติดต่อและวิธีการติดต่อของตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล (ถ้ามี) (3) ข้อมูลชื่อและรายละเอียด รวมถึงสถานที่ติดต่อและวิธีการติดต่อของ DPO ของผู้ควบคุมข้อมูลส่วนบุคคล (ถ้ามี) (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 5.1.1)	แจ้งรายละเอียดเกี่ยวกับข้อมูลการติดต่อของผู้ควบคุมข้อมูลสส่วนบุคคล ตัวแทน (ถ้ามี) และ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างครบถ้วนตามมาตรา 23 (5) แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตัวอย่างหลักฐาน: • ประกาศการคุ้มครองข้อมูลส่วนบุคคล
43	องค์กรต้องมีการแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ฐานทางกฎหมายที่ใช้และอาจรวมถึงประโยชน์โดยชอบด้วยกฎหมายของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลนั้น (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 5.1.2)	แจ้งวัตถุประสงค์ ฐานทางกฎหมาย และประโยชน์โดยชอบด้วยกฎหมายครบถ้วน ตัวอย่างหลักฐาน: • ประกาศการคุ้มครองข้อมูลส่วนบุคคล

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
44	องค์กรต้องมีการแจ้งประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวม และแหล่งที่มาของข้อมูลส่วนบุคคล ในกรณีที่ข้อมูลส่วนบุคคลดังกล่าวได้มาจากแหล่งอื่น (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 5.1.3)	มีการแจ้งประเภทของข้อมูลส่วนบุคคลที่เก็บรวบรวม และแหล่งที่มาของข้อมูลส่วนบุคคลครบถ้วน ตัวอย่างหลักฐาน: • ประกาศการคุ้มครองข้อมูลส่วนบุคคล
45	องค์กรต้องมีการแจ้งประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย รวมถึงรายละเอียดการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 5.1.4)	มีการแจ้งประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย รวมถึงรายละเอียดการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศครบถ้วน ตัวอย่างหลักฐาน: • ประกาศการคุ้มครองข้อมูลส่วนบุคคล
46	องค์กรต้องมีการแจ้งระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน มีการแจ้งระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 5.1.5)	มีการแจ้งระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลครบถ้วน ตัวอย่างหลักฐาน: • ประกาศการคุ้มครองข้อมูลส่วนบุคคล • เอกสารแสดงการอ้างอิงกฎหมายที่กำหนดไว้เป็นการเฉพาะ

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
47	องค์กรต้องมีการแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงสิทธิในการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล (กรณีมีการขอความยินยอม) และสิทธิในการร้องเรียนในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 5.1.6)	มีการแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคลทราบครบถ้วน ตัวอย่างหลักฐาน: • ประกาศการคุ้มครองข้อมูลส่วนบุคคล
48	องค์กรต้องมีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลในขณะที่ข้อมูลส่วนบุคคลถูกเก็บรวบรวม อาทิ ในขณะที่กรอกแบบฟอร์ม หรือจากกรณีที่อาจสังเกตเห็นได้เอง (or by observation) เช่น การถูกบันทึกภาพโดยระบบกล้องวงจรปิด หรือการถูกติดตามพฤติกรรมออนไลน์ เป็นต้น (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 5.2.1)	มีหลักฐานการได้รับแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลครบถ้วน ตัวอย่างหลักฐาน: • หลักฐานการได้รับแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล เช่น ข้อความในรูปแบบ SMS, Email, ภาพถ่ายป้ายที่แสดงว่ามีการเก็บข้อมูลผ่านกล้องวงจรปิดเป็นต้น

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
49	องค์กรต้องมีการทบทวนประกาศคุ้มครองข้อมูลส่วนบุคคลโดยพิจารณาเปรียบเทียบกับบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA) เพื่อให้มั่นใจว่าข้อมูลเป็นปัจจุบันและอธิบายสิ่งที่เกิดขึ้นกับข้อมูลส่วนบุคคลของบุคคลได้จริง (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 5.6.2)	มีการทบทวนประกาศการคุ้มครองข้อมูลส่วนบุคคลโดยการพิจารณาเปรียบเทียบกับบันทึกรายการอย่างครบถ้วน ตัวอย่างหลักฐาน: • หลักฐานการทบทวนประกาศข้อมูลส่วนบุคคลแสดงการเปรียบเทียบกับ ROPA เช่น การจัดประชุมของผู้ที่มีส่วนเกี่ยวข้องหรือได้รับมอบหมาย
50	องค์กรต้องมีการดำเนินการทดสอบโดยผู้ใช้เพื่อประเมินประสิทธิภาพของการแจ้งข้อมูลเกี่ยวกับวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 5.6.4)	มีการทดสอบกับผู้ใช้และประเมินประสิทธิภาพ ตัวอย่างหลักฐาน: • หลักฐานการทดสอบกับผู้ใช้เพื่อประเมินประสิทธิภาพของการแจ้ง ตัวอย่างหลักฐาน:
51	องค์กรต้องจัดทำประกาศการคุ้มครองข้อมูลส่วนบุคคลที่มีความชัดเจนและง่ายสำหรับการเข้าถึงของสาธารณะ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 5.7.1)	มีประกาศการคุ้มครองข้อมูลส่วนบุคคลชัดเจนและง่ายในการเข้าถึง ตัวอย่างหลักฐาน: • ช่องทางในการเผยแพร่ประกาศการคุ้มครองข้อมูลส่วนบุคคล
52	องค์กรมีการปรับปรุงและพัฒนาประสิทธิภาพของแนวทางการแจ้ง Privacy Notice (สอดคล้องกับ Privacy Maturity Model: PMM)	

ด้านที่ 6 การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล และการกำหนดฐานทางกฎหมาย (ROPA and Lawful Basis)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
53	องค์กรต้องจัดทำหรือทบทวนแผนผังข้อมูล (Data Mapping) เพื่อทำความเข้าใจการไหลเวียนของข้อมูลส่วนบุคคลภายในองค์กร (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 6.1.1)	มีการจัดทำแผนผังข้อมูลที่ชัดเจนและมีประสิทธิภาพ ตัวอย่างหลักฐาน: • แผนผังข้อมูล
54	องค์กรต้องจัดทำ ROPA โดยมีรายการอย่างน้อยตามที่กำหนดไว้ในมาตรา 39 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังต่อไปนี้ (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท (3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล (5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิ์เข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น	จัดทำบันทึกรายการโดยมีรายการที่บันทึกครบถ้วนตามรายการขั้นต่ำที่กฎหมายกำหนด ตัวอย่างหลักฐาน: • ROPA

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
	(6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม (7) การปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด (หากมี) (8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1) (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 6.3.1)	
55	กรณีที่องค์กรมีผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) องค์กรต้องกำกับให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำ ROPA ในส่วนที่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งให้แก่องค์กร ทั้งนี้ ROPA ต้องมีรายการที่บันทึกอย่างน้อยตามที่กฎหมายกำหนด (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 6.3.2)	มีเอกสารหรือหลักฐานแสดงถึงการกำกับให้ผู้ประมวลผลข้อมูลส่วนบุคคลของตนจัดทำบันทึกรายการตามที่กฎหมายกำหนด ตัวอย่างหลักฐาน: • ROPA • เอกสารหรือหลักฐานที่แสดงถึงการที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำบันทึกรายการ
56	องค์กรต้องกำหนดฐานทางกฎหมาย (Lawful Basis) ที่เหมาะสมและสอดคล้องกับวัตถุประสงค์ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 6.5.1)	ตัวอย่างหลักฐาน: • นโยบายหรือแนวปฏิบัติขององค์กรที่เกี่ยวกับการพิจารณาฐานทางกฎหมาย

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
57	องค์กรต้องจัดทำประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Privacy Notice) อยู่ในรูปแบบที่เข้าถึงได้โดยง่ายและอ่านเข้าใจง่าย (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 6.6.3)	ประกาศการคุ้มครองข้อมูลส่วนบุคคลเข้าถึงได้ง่าย และเข้าใจง่ายตัวอย่างหลักฐาน: • ประกาศการคุ้มครองข้อมูลส่วนบุคคลระบุฐานทางกฎหมาย
58	องค์กรมีมาตรการที่เหมาะสมในการตรวจสอบว่าบุคคลดังกล่าวสามารถให้ความยินยอมด้วยตนเองได้ (ตรวจสอบอายุและความสามารถของบุคคล) ในกรณีที่ไม่ได้ต้องมีมาตรการที่เหมาะสมในการได้รับความยินยอมจากผู้ใช้อำนาจปกครอง แล้วแต่กรณี (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 6.9.2)	มีมาตรการในการตรวจสอบที่มีประสิทธิภาพและเหมาะสม ตัวอย่างหลักฐาน: • นโยบายหรือแนวปฏิบัติ และกระบวนการในการขอความยินยอมจากผู้ใช้อำนาจปกครอง แล้วแต่กรณี
59	ในกรณีที่เป็นการขอความยินยอมจากผู้เยาว์หรือบุคคลไร้ความสามารถหรือเสมือนไร้ความสามารถ องค์กรมีมาตรการตรวจสอบที่เหมาะสมว่าบุคคลที่ให้ความยินยอมแทนเป็นผู้มีอานาจกระทำการแทนเจ้าของข้อมูลส่วนบุคคลอย่างแท้จริง (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 6.9.4)	มีมาตรการในการตรวจสอบผู้มีอำนาจกระทำการแทน และมีขั้นตอนการขอเอกสารประกอบการพิจารณาที่ชัดเจน ตัวอย่างหลักฐาน: • แนวปฏิบัติหรือกลไกในการตรวจสอบสถานะผู้ให้ความยินยอมแทนเจ้าของข้อมูลส่วนบุคคล

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
60	องค์กรต้องมีการจัดทำ ROPA มีการทบทวนกระบวนการและแก้ไข ROPA (สอดคล้องกับ Privacy Maturity Model: PMM)	
61	องค์กรมีการทบทวนฐานทางกฎหมายที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล (สอดคล้องกับ Privacy Maturity Model: PMM)	
62	ROPA ขององค์กรมีการระบุ “ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล” (สอดคล้องกับ Privacy Maturity Model: PMM)	
63	ROPA ขององค์กรมีการระบุ “สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขในการเข้าถึงข้อมูล” เช่น ต้องผ่านการยืนยันตัวตนก่อนได้รับสิทธิ (สอดคล้องกับ Privacy Maturity Model: PMM)	

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
64	ROPA ขององค์กรมีการระบุ “การใช้หรือเปิดเผยข้อมูลให้หน่วยงานอื่น” และมีเอกสารหรือ Dashboard แสดงจำนวนกิจกรรม จำนวนข้อมูล และจำนวนเจ้าของข้อมูลส่วนบุคคลขององค์กรเพื่อนำไปใช้เป็นตัวชี้วัดประสิทธิภาพของกระบวนการ (สอดคล้องกับ Privacy Maturity Model: PMM)	
65	ROPA ขององค์กรมีการระบุ “การปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด” (สอดคล้องกับ Privacy Maturity Model: PMM)	
66	ROPA ขององค์กรมีการระบุ “คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย” (สอดคล้องกับ Privacy Maturity Model: PMM)	
67	ในการขอความยินยอม องค์กรมีขั้นตอนการยืนยันตัวตนเจ้าของข้อมูลด้วย (สอดคล้องกับ Privacy Maturity Model: PMM)	

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
68	องค์กรมีการแยกเอกสารขอความยินยอมออกจากสัญญาอย่างชัดเจน (สอดคล้องกับ Privacy Maturity Model: PMM)	
69	องค์กรมีการแจ้งเจ้าของข้อมูลส่วนบุคคลเรื่องช่องทางการถอนความยินยอม (สอดคล้องกับ Privacy Maturity Model: PMM)	

ด้านที่ 7 ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement and Data Processing Agreement)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
70	องค์กรต้องมีขั้นตอนตรวจสอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์กรระหว่างประเทศก่อนการโอนข้อมูลส่วนบุคคลไปต่างประเทศ โดยอ้างอิงหลักเกณฑ์ของคณะกรรมการ (Adequacy Decision) หรือเอกสารสนับสนุน (ถ้ามี) (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 7.3.1)	มีการตรวจสอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์กรระหว่างประเทศที่รับข้อมูลส่วนบุคคล ตามหลักเกณฑ์ที่ประกาศกำหนด และมีเอกสารสนับสนุน ตัวอย่างหลักฐาน: • รายงานแสดงว่าองค์กรได้มีการตรวจสอบว่าประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและเป็นไปตามที่กฎหมายกำหนด
71	เมื่อมีการโอนข้อมูลส่วนบุคคลไปต่างประเทศ การส่งหรือโอนดังกล่าวมีความสอดคล้องกับข้อกำหนดของกฎหมายในกรณีอื่น ๆ ตามที่กำหนดในมาตรา 28 หรือมาตรา 29 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และต้องมีฐานทางกฎหมายที่เหมาะสมรองรับการโอน (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 7.3.2)	มีการตรวจสอบความสอดคล้องและฐานทางกฎหมายครบถ้วน และมีเอกสารสนับสนุน ตัวอย่างหลักฐาน: • รายงานแสดงว่าองค์กรได้มีการตรวจสอบว่าประเทศปลายทางมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและเป็นไปตามที่กฎหมายกำหนด Binding Corporate Rules (BCRs) • มาตรการที่เหมาะสมในการโอนข้อมูล เช่น MCCs, SCCs • หลักฐานในการพิจารณาฐานทางกฎหมายในการโอนข้อมูลไปต่างประเทศ

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
72	องค์กรต้องทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) กับผู้ประมวลผลข้อมูลทุกรายที่เกี่ยวข้องกับองค์กร (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 7.4.1)	มีการจัดทำ DPA กับผู้ประมวลผลข้อมูลส่วนบุคคลครบถ้วนทุกราย ตัวอย่างหลักฐาน: • รายชื่อของผู้ประมวลผลข้อมูลส่วนบุคคลขององค์กร • DPA
73	องค์กรต้องจัดทำ DPA โดยมีเงื่อนไขอย่างน้อยตามที่มาตรา 40 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด ได้แก่ (1) ดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งเท่านั้น (2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม (3) แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น (4) จัดทำและเก็บรักษา ROPA (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 7.4.2)	มีการจัดทำ DPA และประกอบเงื่อนไขตามที่กำหนดในกฎหมายครบถ้วน ตัวอย่างหลักฐาน: • DPA
74	DPA ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยทั้งด้านองค์กรและเทคนิค เช่น การเข้ารหัสข้อมูล การทำข้อมูลแฝง และการกู้คืนระบบ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 7.5.2)	มีการกำหนดมาตรการด้านความมั่นคงปลอดภัยใน DPA ตัวอย่างหลักฐาน: • DPA

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
75	DPA ต้องมีข้อกำหนดที่อนุญาตให้องค์กรดำเนินการตรวจสอบ (Right to Audit) เพื่อยืนยันว่าผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามข้อกำหนดและเงื่อนไขตามสัญญาทั้งหมด (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 7.7.1)	มีข้อกำหนดที่ครอบคลุมถึงการที่องค์กรสามารถมอบหมายให้บุคคลอื่นเข้าตรวจสอบได้ด้วย ตัวอย่างหลักฐาน: • DPA
76	หากมีบุคคลที่สามจัดหาผลิตภัณฑ์หรือบริการเพื่อประมวลผลข้อมูลส่วนบุคคล องค์กรต้องเลือกผู้ค้า (Supplier) ที่มีมาตรฐานในการปกป้องข้อมูลส่วนบุคคล โดยออกแบบผลิตภัณฑ์หรือบริการของตนโดยคำนึงถึงการปกป้องข้อมูลด้วยการออกแบบ (Privacy by Design) (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 7.8.1)	มีการตรวจสอบนโยบาย แนวปฏิบัติหรือการดำเนินการของผู้ค้า และมีเอกสารสนับสนุน ตัวอย่างหลักฐาน: • แนวปฏิบัติหรือการดำเนินการขององค์กรในการตรวจสอบหลัก “การปกป้องข้อมูลด้วยการออกแบบ” (Data Protection by Design) ของผู้ค้า (Supplier)
77	องค์กรต้องสามารถระบุผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ทั้งหมด ที่ส่งข้อมูลส่วนบุคคลมาให้องค์กร (สอดคล้องกับ Privacy Maturity Model: PMM)	

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
78	องค์กรต้องสามารถระบุผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ทั้งหมดภายในประเทศที่ดำเนินการประมวลผลข้อมูลส่วนบุคคล	
79	องค์กรต้องจัดทำ DPA ให้ครอบคลุมผู้ประมวลผลข้อมูลส่วนบุคคล และมีเอกสารหรือ Dashboard ที่แสดงจำนวนข้อตกลง สัญญา สถานะ และระยะเวลาผูกพัน ของทุกคู่สัญญาเพื่อนำไปใช้เป็นตัวชี้วัดประสิทธิภาพของกระบวนการดำเนินงาน (สอดคล้องกับ Privacy Maturity Model: PMM)	
80	องค์กรได้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ ตามมาตรา 29 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (การส่งข้อมูลในลักษณะ Binding Coperate Rule) (สอดคล้องกับ Privacy Maturity Model: PMM)	
81	องค์กรได้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ ตามมาตรา 29 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (การส่งข้อมูลในลักษณะ Standard Contractual Clauses) (สอดคล้องกับ Privacy Maturity Model: PMM)	

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
82	ในกรณีที่การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกัน องค์กรได้ว่ามีนโยบายคุ้มครองข้อมูลส่วนบุคคลที่สามารถบังคับใช้ครอบคลุมไปถึงเครือกิจการหรือเครือธุรกิจเดียวกันได้ (ตามมาตรา 29 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (BCR))	
83	ในกรณีที่การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ องค์กรมีการกำหนดมาตราการที่เหมาะสมภายในสัญญากับผู้ประมวลผลข้อมูลส่วนบุคคล (ตามมาตรา 29 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (SSC)) (สอดคล้องกับ Privacy Maturity Model: PMM)	
84	องค์กรต้องบันทึกการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลรายอื่น ทั้งที่ได้รับความยินยอมและกรณียกเว้นตามกฎหมาย (ตามมาตรา 27 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562) (สอดคล้องกับ Privacy Maturity Model: PMM)	

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
85	องค์กรต้องจัดทำแบบฟอร์ม (Template) สำหรับบันทึกการโอนข้อมูลส่วนบุคคลไปต่างประเทศตามมาตรา 28 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (สอดคล้องกับ Privacy Maturity Model: PMM)	
86	องค์กรต้องจัดทำ Template ของนโยบายคุ้มครองข้อมูลส่วนบุคคลที่สามารถบังคับใช้ครอบคลุมไปถึงเครือกิจการหรือเครือธุรกิจเดียวกัน (สอดคล้องกับ Privacy Maturity Model: PMM)	
87	องค์กรต้องจัดทำ Template ของสัญญาที่ระบุมาตรการคุ้มครองข้อมูลส่วนบุคคล (สอดคล้องกับ Privacy Maturity Model: PMM)	
88	องค์กรต้องจัดทำ Template ของ DPA สำหรับใช้กับผู้ประมวลผลข้อมูลส่วนบุคคล (สอดคล้องกับ Privacy Maturity Model: PMM)	

ด้านที่ 8 ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Risks and Data Protection Impact Assessment)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
89	องค์กรต้องระบุและจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล โดยบันทึกไว้ในทะเบียนการจัดการความเสี่ยง (Risk Register) ที่ชัดเจน เชื่อมโยงกับแผนกหรือส่วนงานที่เกี่ยวข้อง และประเมินความเสี่ยงของสินทรัพย์สารสนเทศ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 8.1.2)	นโยบายภายในสำหรับการจัดทำทะเบียนจัดการความเสี่ยงทั่วไปและทะเบียนจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตัวอย่างหลักฐาน: • ทะเบียนจัดการความเสี่ยง (Risk Register) ทั่วไป • ทะเบียนจัดการความเสี่ยง (Risk Register) ของฝ่ายเทคโนโลยีสารสนเทศ • รายงานเหตุการณ์ด้านความเสี่ยงของข้อมูลส่วนบุคคล • รายงานผลการตรวจสอบทะเบียนจัดการความเสี่ยง (Risk Register) ทั่วไป • รายงานการตรวจสอบทะเบียนจัดการความเสี่ยง (Risk Register) ของฝ่ายเทคโนโลยีสารสนเทศ

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
90	องค์กรต้องมีขั้นตอนอย่างเป็นระบบในการระบุ บันทึก และจัดการความเสี่ยงเพื่อให้มั่นใจว่าเกี่ยวข้องกับทรัพย์สินสารสนเทศในทะเบียนควบคุมทรัพย์สินสารสนเทศ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 8.1.5)	ตัวอย่างหลักฐาน: • นโยบายในการกำหนดขั้นตอนการระบุ บันทึก และจัดการความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินสารสนเทศในทะเบียนควบคุมทรัพย์สินสารสนเทศ • ทะเบียนควบคุมทรัพย์สินสารสนเทศ
91	องค์กรต้องจัดทำและทดสอบมาตรการลดความเสี่ยง ตามที่ได้ระบุไว้ใน Risk Categories เพื่อให้มั่นใจว่ามาตรการเหล่านั้นมีประสิทธิภาพ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 8.1.6)	องค์กรมีมาตรการเพื่อลดความเสี่ยงที่ระบุในประเภทความเสี่ยง และมีการทดสอบประสิทธิภาพของมาตรการเป็นประจำ ตัวอย่างหลักฐาน: • นโยบายในการทดสอบมาตรการเพื่อลดความเสี่ยงที่ระบุในประเภทความเสี่ยง • รายงานผลการทดสอบมาตรการดังกล่าว
92	องค์กรต้องมีการติดตามและทบทวนความเสี่ยงที่ระบุไว้ เพื่อประเมินว่าความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้ (Residual Risk) (สอดคล้องกับ Privacy Maturity Model: PMM)	

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
93	องค์กรต้องกำหนดรอบการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงที่มีนัยสำคัญต่อการประมวลผลข้อมูล (สอดคล้องกับ Privacy Maturity Model: PMM)	
94	องค์กรต้องวัดผลความมีประสิทธิภาพของกระบวนการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล โดยเปรียบเทียบผลลัพธ์กับระดับความเสี่ยงที่เหลือ (Residual Risk) (สอดคล้องกับ Privacy Maturity Model: PMM)	
95	องค์กรต้องปรับปรุงขั้นตอนและนำเทคโนโลยีใหม่มาใช้ เพื่อเพิ่มประสิทธิภาพในการระบุ จัดการ และลดความเสี่ยงด้านข้อมูลส่วนบุคคลให้สอดคล้องกับผลการประเมิน (สอดคล้องกับ Privacy Maturity Model: PMM)	

กลุ่มที่ 4

ระบบเทคโนโลยีและความมั่นคงปลอดภัย และการแจ้งเหตุละเมิด

ด้านที่ 9 มาตรการรักษาความมั่นคงปลอดภัย (Data Security)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
96	องค์กรต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลระหว่างการส่งหรือโอนข้อมูล เช่น การเข้ารหัส การใช้โปรโตคอลที่ปลอดภัย หรือ VPN (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.2.3)	เมื่อต้องมีการส่งหรือโอนข้อมูลออกไปยังนอกสถานที่ วิธีการที่ใช้ในการส่งหรือโอนข้อมูลมีความปลอดภัย เช่น เลือกใช้แมสเซนเจอร์ที่มีความน่าเชื่อถือ ใช้การเข้ารหัสข้อมูล ใช้โปรโตคอลในการส่งหรือโอนข้อมูลที่มีความมั่นคงปลอดภัย หรือใช้ VPN เป็นต้น รวมทั้งมี การตรวจสอบว่าข้อมูลที่จัดส่งไปนั้นได้รับอย่างถูกต้อง ตัวอย่างหลักฐาน: • นโยบายเพื่อรักษาความปลอดภัยด้านการโอนข้อมูลส่วนบุคคล • ทะเบียนการส่งหรือโอนข้อมูลส่วนบุคคล • หนังสือรับโอนข้อมูลส่วนบุคคล
97	องค์กรต้องจัดให้มีมาตรการทดสอบคุณภาพของข้อมูลส่วนบุคคลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้อง เหมาะสม และไม่ถูกเก็บเกินความจำเป็น (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.3.1)	มีการทบทวนคุณภาพของรายการข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้อง เหมาะสม และไม่จัดเก็บไว้เกินกว่าความจำเป็น ตัวอย่างหลักฐาน • นโยบายการทบทวนข้อมูลส่วนบุคคล • นโยบายการทำให้ข้อมูลสมบูรณ์ถูกต้อง และเป็นปัจจุบัน

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
98	องค์กรต้องกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลที่เหมาะสม โดยอ้างอิงข้อกำหนดทางธุรกิจหรือกฎหมาย และต้องมีการทบทวนอย่างต่อเนื่อง (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.4.1)	มีการกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลตามความต้องการทางธุรกิจ สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และหลักการที่เกี่ยวข้อง ตัวอย่างหลักฐาน: • นโยบายระยะเวลาการจัดเก็บข้อมูลและการเก็บรักษาข้อมูลส่วนบุคคล • รายงานตรวจสอบการจัดเก็บและการเก็บรักษาข้อมูลส่วนบุคคล • หนังสือแจ้งการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคล
99	องค์กรต้องทบทวนข้อมูลที่จัดเก็บไว้อย่างสม่ำเสมอ เพื่อลดปริมาณการจัดเก็บข้อมูล และแปลงข้อมูลให้เป็นข้อมูลแฝง (Pseudonymization) หรือทำให้ข้อมูลนิรนาม (Anonymization) (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.4.4)	มีการทบทวนข้อมูลที่จัดเก็บไว้เพื่อระบุโอกาสในการลดการจัดเก็บข้อมูล (เช่น หากสามารถลบหรือทำลายได้ก็ให้ดำเนินการ) การแปลงข้อมูลให้เป็นข้อมูลแฝง (Pseudonymization) หรือการทำให้ข้อมูลเป็นนิรนาม (Anonymization) และมีเอกสารประกอบครบถ้วน ตัวอย่างหลักฐาน: • นโยบายการควบคุมระยะเวลาในการประมวลผลข้อมูลส่วนบุคคล • ทะเบียนการประมวลผลข้อมูลส่วนบุคคล • หนังสือแจ้งการลบ ทำลาย หรือส่งคืนข้อมูลส่วนบุคคล หรือแปลงข้อมูลส่วนบุคคลนั้นให้เป็นข้อมูลแฝง (Pseudonymization) หรือทำให้เป็นนิรนาม (Anonymization)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
100	องค์กรต้องจัดทำบัญชีทรัพย์สินสารสนเทศ (Information Asset Register) ครอบคลุมฮาร์ดแวร์ ซอฟต์แวร์ ระบบ และแอปพลิเคชันที่ใช้ประมวลผลข้อมูลส่วนบุคคล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.6.1)	มีการจัดทำบัญชีทรัพย์สินสารสนเทศ โดยบัญชีดังกล่าวได้รวมถึงเจ้าของทรัพย์สิน สถานที่จัดเก็บทรัพย์สิน ระยะเวลาการจัดเก็บ และมาตรการความมั่นคงปลอดภัย ตัวอย่างหลักฐาน: • นโยบายการจัดทำบัญชีทรัพย์สินสารสนเทศ • บัญชีทรัพย์สินสารสนเทศ
101	องค์กรต้องประเมินความเสี่ยงของทรัพย์สินสารสนเทศที่บันทึกไว้ในบัญชี และดำเนินการตรวจสอบทางกายภาพเพื่อให้มั่นใจว่าทรัพย์สินมีความถูกต้องและครบถ้วน (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.6.3)	มีการประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในรายการบัญชีทรัพย์สินสารสนเทศ มีการดำเนินการตรวจสอบทางกายภาพ เพื่อให้มั่นใจว่าทรัพย์สินในบัญชีมีความถูกต้องและครบถ้วน ตัวอย่างหลักฐาน: • การประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในบัญชีทรัพย์สินสารสนเทศ • รายงานการประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในบัญชีทรัพย์สินสารสนเทศ • รายงานความเห็นประกอบการพิจารณา • รายงานการประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในบัญชีทรัพย์สินสารสนเทศ • หนังสือการพิจารณาการประเมินความเสี่ยงสำหรับทรัพย์สินที่อยู่ในบัญชีทรัพย์สินสารสนเทศ

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
102	องค์กรต้องจัดให้มีการเก็บบันทึกการเข้าถึงระบบ (Access Logs) ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.8.4)	มีการเก็บล็อกสำหรับการเข้าถึงระบบ ตัวอย่างหลักฐาน: • นโยบายควบคุมการเข้าถึงข้อมูลส่วนบุคคล • ทะเบียนการควบคุมการเข้าถึงข้อมูลส่วนบุคคล • มาตรการทางเทคนิคเพื่อจำกัดการเข้าถึงข้อมูลส่วนบุคคลตามทะเบียนของบุคลากรที่ได้รับอนุญาต
103	องค์กรต้องจำกัดสิทธิการเข้าถึงข้อมูลส่วนบุคคล โดยใช้หลักการให้สิทธิน้อยที่สุด (Principle of Least Privilege) (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.9.1)	มีการจำกัดการเข้าถึงระบบหรือแอปพลิเคชันที่ประมวลผลข้อมูลส่วนบุคคล โดยให้สิทธิการเข้าถึงให้น้อยที่สุดตามความจำเป็น (the principle of least privilege) และมีเอกสารสนับสนุน ตัวอย่างหลักฐาน: • นโยบายจำกัดการเข้าถึงระบบหรือแอปพลิเคชันที่ประมวลผลข้อมูลส่วนบุคคลป้องกันการเข้าถึง การรวบรวมและการใช้งานโดยไม่ได้รับอนุญาต • ทะเบียนของบุคลากรที่ได้รับอนุญาตให้เข้าถึงข้อมูลส่วนบุคคล
104	องค์กรต้องกำหนดนโยบายการตั้งรหัสผ่านที่มีความซับซ้อนและปลอดภัย รวมถึงการจำกัดจำนวนครั้งที่ล็อกอินผิดพลาด (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.9.2)	มีการกำหนดให้มีการตั้งรหัสผ่านให้มีความซับซ้อน รวมถึงการจากัดจำนวนครั้งที่สามารถล็อกอินผิดพลาดในการเข้าสู่ระบบ เช่น กำหนดจำนวนครั้งที่สามารถล็อกอินผิดพลาดได้ไม่เกิน 3 ครั้ง เป็นต้น

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
		ตัวอย่างหลักฐาน: • นโยบายการตั้งรหัสผ่านที่มีความซับซ้อน และจำกัดจานวนครั้งที่สามารถล็อกอินผิดพลาดในการเข้าสู่ระบบ • หนังสือประกอบการอบรมความปลอดภัยด้านการคุ้มครองข้อมูลส่วนบุคคลประเภทเทคโนโลยีสารสนเทศและการจำกัดสิทธิการเข้าถึงข้อมูลส่วนบุคคล
105	องค์กรต้องมีมาตรการจัดการรหัสผ่านอย่างปลอดภัย เช่น การเปลี่ยนรหัสผ่านเริ่มต้น การห้ามแชร์รหัสผ่าน และการจัดเก็บอย่างมั่นคงปลอดภัย (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.9.3)	มีการบริหารจัดการรหัสผ่านให้มีความมั่นคงปลอดภัย เช่น การเปลี่ยนรหัสผ่านที่มาจากผู้ผลิต การควบคุมการใช้รหัสผ่านที่มีการแชร์ใช้งานร่วมกัน และการจัดเก็บรหัสผ่านให้มีความมั่นคงปลอดภัยอย่างครบถ้วน ตัวอย่างหลักฐาน: • การจัดการรหัสผ่านให้มีความมั่นคงปลอดภัย • หนังสือประกอบการอบรมความปลอดภัยด้านการคุ้มครองข้อมูลส่วนบุคคลประเภทเทคโนโลยีสารสนเทศและการจำกัดสิทธิการเข้าถึงข้อมูลส่วนบุคคล

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
106	องค์กรต้องจัดให้มีมาตรการรักษาความปลอดภัยของพื้นที่ที่จำเป็น เช่น การควบคุมการเข้าออก การติดตั้งกล้องวงจรปิด หรือสัญญาณกันขโมย (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.11.1)	มีการป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย โดยมีมาตรการควบคุมการเข้าออกเคร่งครัด ตัวอย่างหลักฐาน: • นโยบายการป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย • สัญญาจ้างบริการป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัย
107	องค์กรต้องมีขั้นตอนการควบคุมการเข้าถึงของบุคคลภายนอก เช่น การแลกบัตร ลงนามเข้าออก ก่อนเข้าสู่พื้นที่ภายในที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.11.2)	มีข้อปฏิบัติสำหรับการแลกบัตรและลงนามก่อนเข้าถึงพื้นที่ภายในองค์กรและมีการปฏิบัติตามอย่างเคร่งครัด ตัวอย่างหลักฐาน: • นโยบายการป้องกันพื้นที่ที่จำเป็นต้องรักษาความมั่นคงปลอดภัยภายในองค์กร

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
108	องค์กรต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และแผนกู้คืนจากภัยพิบัติ (Disaster Recovery Plan: DRP) ที่ครอบคลุมระบบ ข้อมูล และบริการที่สำคัญ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.12.1)	มีแผนความต่อเนื่องทางธุรกิจ เพื่อบริหารจัดการการหยุดชะงักทางธุรกิจหรือภัยพิบัติต่าง ๆ ที่เกิดขึ้น และเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ชัดเจน ตัวอย่างหลักฐาน: • นโยบายการจัดทำแผนความต่อเนื่องทางธุรกิจ เพื่อบริหารจัดการการหยุดชะงักทางธุรกิจหรือภัยพิบัติต่าง ๆ ที่เกิดขึ้น และเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง • แผนความต่อเนื่องทางธุรกิจ เพื่อบริหารจัดการการหยุดชะงักทางธุรกิจหรือภัยพิบัติต่าง ๆ ที่เกิดขึ้น และเพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง
109	องค์กรต้องมีการสำรองข้อมูลส่วนบุคคลอย่างสม่ำเสมอ และจัดเก็บสำเนาข้อมูลสำรองในสถานที่ที่ปลอดภัยนอกสถานที่ปฏิบัติงานหลัก (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.12.2)	มีการสำรองข้อมูลและนำไปจัดเก็บไว้นอกสถานที่ ตัวอย่างหลักฐาน: • นโยบายการสำรองข้อมูลและนำไปจัดเก็บไว้นอกสถานที่ • บันทึกข้อตกลงการประมวลผลข้อมูลส่วนบุคคล • บันทึกข้อตกลงรักษาความลับ • มาตรการทางกายภาพ มาตรการทางเทคนิค และมาตรการด้านการบริหารจัดการ

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
110	องค์กรต้องทดสอบการเข้าถึงและการกู้คืนข้อมูลจากระบบสำรอง เพื่อให้มั่นใจในการเตรียมพร้อมสำหรับการกู้คืนระบบ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 9.12.4)	มีการทดสอบการเข้าถึงข้อมูลที่สำรองไว้ รวมทั้งทดสอบขั้นตอนการกู้คืนระบบ เพื่อให้เกิดความมั่นใจในการเตรียมความพร้อมสำหรับการกู้คืนระบบ และมีเอกสารครบถ้วน ตัวอย่างหลักฐาน: • นโยบายการทดสอบการเข้าถึงข้อมูลที่สำรองไว้ รวมทั้งทดสอบขั้นตอนการกู้คืนระบบ • รายงานผลทดสอบการเข้าถึงข้อมูลที่สำรองและขั้นตอนการกู้คืนระบบเบื้องต้น • รายงานผลทดสอบการเข้าถึงข้อมูลที่สำรองและขั้นตอนการกู้คืนระบบ • รายงานพิจารณาผลทดสอบการเข้าถึงข้อมูลที่สำรองและขั้นตอนการกู้คืนระบบ
111	องค์กรต้องมีนโยบายและกระบวนการตรวจสอบช่องโหว่ (Vulnerability Assessment) และปรับปรุงระบบ/เทคโนโลยีเพื่ออุดช่องโหว่อย่างต่อเนื่อง(สอดคล้องกับ Privacy Maturity Model: PMM)	
112	องค์กรต้องจัดทำตัวชี้วัด (KPI) เพื่อติดตามและประเมินประสิทธิภาพมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ และปรับปรุงมาตรการเมื่อยังไม่เป็นไปตามเป้าหมาย (สอดคล้องกับ Privacy Maturity Model: PMM)	

ด้านที่ 10 การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Breach Response)

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
113	องค์กรต้องกำหนดขั้นตอนการแจ้งเหตุด้านความมั่นคงปลอดภัยและการละเมิดข้อมูลส่วนบุคคลภายในองค์กร ให้พนักงานสามารถ รายงานต่อผู้ที่เกี่ยวข้องได้ทันที (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.1.3)	มีแผนกำหนดให้พนักงานมีการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ทีมหรือบุคลากรดังกล่าวเพื่อดำเนินการตรวจสอบเหตุที่เกิดขึ้นนั้นว่าเข้า เงื่อนไขเป็น “เหตุการณ์ละเมิดข้อมูลส่วนบุคคล” หรือไม่ และมีเอกสารรายงานของเหตุการณ์ ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ตัวอย่างหลักฐาน: • นโยบายแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแบบแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล • หนังสือรับการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล • รายงานเบื้องต้นของเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล • รายงานของเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
		• รายละเอียดการติดต่อทีมหรือบุคลากรที่ทำหน้าที่บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
114	องค์กรต้องมีแผนรับมือเหตุด้านความมั่นคงปลอดภัยและเหตุละเมิดข้อมูลส่วนบุคคลโดยกำหนดบทบาทและความรับผิดชอบอย่างชัดเจน (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.1.4+10.1.5)	องค์กรมีแผนรับมือต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล มีขั้นตอนบริหารจัดการ และมีรายงานสรุปผลการดำเนินการ ตัวอย่างหลักฐาน: • แผนรับมือต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล • ขั้นตอนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล • รายงานสรุปผลการดำเนินการรับมือด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
115	องค์กรต้องมีแบบฟอร์มบันทึกเหตุละเมิดข้อมูลส่วนบุคคล ที่ระบุประเภทของเหตุการณ์ ผลกระทบและมาตรการแก้ไข/ป้องกัน (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.1.5+10.1.7)	มีแบบการบันทึกเหตุการณ์ละเมิดข้อมูล โดยมีรายการข้อมูลอย่างน้อยดังต่อไปนี้ (1) ลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล (2) ชื่อ สถานที่ติดต่อ และวิธีการ

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
		ติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม (3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (4) ข้อมูลเกี่ยวกับมาตรการที่องค์กรใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย ตัวอย่างหลักฐาน: • นโยบายภายในการจัดให้มีระบบรวมศูนย์ในการบันทึกข้อมูลเหตุการณ์ละเมิดข้อมูลส่วนบุคคล • การแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล • รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคล • บันทึกล็อก (Log) แจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
116	องค์กรต้องมีขั้นตอนการประเมินผลกระทบจากเหตุละเมิดข้อมูลส่วนบุคคล โดยพิจารณาความรุนแรงและโอกาสที่อาจกระทบสิทธิและเสรีภาพของบุคคล (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.2.1)	แนวปฏิบัติในการประเมินโอกาสและความรุนแรงของความเสี่ยงต่อบุคคลอันเป็นผลจากการละเมิดข้อมูลส่วนบุคคล และมีรายงานการประเมิน ตัวอย่างหลักฐาน: • นโยบายการประเมินความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล • ขั้นตอนการประเมินโอกาสและความรุนแรงของความเสี่ยงต่อบุคคล • รายงานการประเมินโอกาสและความรุนแรงของความเสี่ยงต่อบุคคล
117	องค์กรต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง นับแต่ทราบเหตุตามที่กฎหมายกำหนดโดยอาจแจ้งบางส่วนก่อนได้ หากยังไม่มีข้อมูลทั้งหมด (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.2.2)	มีแนวปฏิบัติสำหรับการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. ได้รับทราบภายในระยะเวลา 72 ชั่วโมงนับแต่ทราบเหตุ (โดยอาจแจ้งบางส่วนก่อนได้ หากยังไม่มีข้อมูลทั้งหมดเกี่ยวกับเหตุการณ์ละเมิด) และแจ้งภายในกรอบระยะเวลาที่กฎหมายกำหนด และมีหลักฐานสนับสนุน ตัวอย่างหลักฐาน: นโยบายแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. ทราบภายในกรอบระยะเวลาที่กฎหมายกำหนด

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
118	องค์กรต้องจัดทำรายละเอียดที่เพียงพอในการแจ้งเหตุละเมิดต่อ สคส. เช่น ลักษณะของเหตุการณ์ ผลกระทบ และมาตรการแก้ไข (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.3.3+ 10.2.3)	ข้อมูลที่ได้ทำการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลต้องมีสาระสำคัญดังต่อไปนี้: ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือผู้ประสานงานที่ได้รับมอบหมาย ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ตัวอย่างหลักฐาน: • หนังสือแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
119	กรณีที่องค์กรพิจารณาว่าเหตุละเมิดไม่ก่อให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูล องค์กรต้องบันทึกเหตุผลในการไม่แจ้งเหตุไว้เป็นหลักฐาน (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.2.4)	หากองค์กรพิจารณาว่าไม่จำเป็นต้องแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้ สคส. ทราบองค์กรได้บันทึกเหตุผลที่องค์กรพิจารณาว่าการละเมิดไม่ส่งผลให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล และมีขั้นตอนการ

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
		พิจารณาที่ชัดเจน รวมถึงมีเอกสารประกอบการพิจารณาสนับสนุน ตัวอย่างหลักฐาน: • บันทึกรายงานแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
120	หากเหตุละเมิดมีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล องค์กรต้องแจ้งเจ้าของข้อมูลให้ทราบโดยไม่ชักช้า (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.3.1)	มีแนวปฏิบัติสำหรับการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและมีเอกสารครบถ้วน ตัวอย่างหลักฐาน: • นโยบายและแนวปฏิบัติสำหรับการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
121	การแจ้งเจ้าของข้อมูลต้องทำอย่างชัดเจน กระชับ และใช้ภาษาที่เข้าใจง่าย พร้อมให้ข้อมูลที่จำเป็น เช่น ลักษณะของเหตุการณ์ ผลกระทบ และช่องทางติดต่อ (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.3.2)	มีขั้นตอนหรือแนวปฏิบัติในการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงโดยไม่ชักช้า และใช้ภาษาและคำอธิบายที่เรียบง่ายชัดเจนและสามารถทำความเข้าใจได้โดยง่าย ตัวอย่างหลักฐาน: • นโยบายวิธีการและรายละเอียดการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
122	การแจ้งเจ้าของข้อมูลต้องรวมแนวทางการเยียวยา และมาตรการป้องกันที่องค์กรได้ดำเนินการหรือจะดำเนินการต่อไป (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.3.3)	ข้อมูลที่ได้ทำการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลต้องมีสาระสำคัญดังต่อไปนี้: ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือผู้ประสานงานที่ได้รับมอบหมาย ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และ ข้อมูลโดยสังเขปเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ตัวอย่างหลักฐาน: • หนังสือแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
123	องค์กรต้องให้คำแนะนำแก่เจ้าของข้อมูลส่วนบุคคล เกี่ยวกับวิธีการป้องกันความเสียหายจากผลกระทบที่อาจเกิดจากเหตุละเมิด (สอดคล้องกับแนวทางปฏิบัติและหลักเกณฑ์ฯ ข้อ 10.3.4)	มีการให้คำแนะนำแก่เจ้าของข้อมูลส่วนบุคคลเพื่อให้สามารถป้องกันตนเองจากผลกระทบของเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นนั้น และมีเอกสารสนับสนุน ตัวอย่างหลักฐาน: • นโยบายการเผยแพร่ขั้นตอนการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล • นโยบายการเผยแพร่สิทธิของเจ้าของข้อมูลส่วนบุคคล

ข้อ	เกณฑ์การตรวจมาตรฐาน	การดำเนินงาน/เอกสาร
124	องค์กรต้องตรวจสอบข้อเท็จจริงของเหตุละเมิด และจัดทำรายงานสรุปผลการดำเนินงาน พร้อมจัดทำแดชบอร์ดติดตามจำนวนเหตุการณ์ (สอดคล้องกับ Privacy Maturity Model: PMM)	
125	แบบบันทึกเหตุละเมิดข้อมูลส่วนบุคคลต้องมีรายละเอียดครบถ้วน ได้แก่ ลักษณะของเหตุการณ์ ผลกระทบ มาตรการแก้ไข และการเยียวยา (สอดคล้องกับ Privacy Maturity Model: PMM)	
126	องค์กรต้องจัดทำตัวชี้วัด (KPI) เพื่อติดตามประสิทธิภาพของกระบวนการจัดการเหตุละเมิด และใช้ผลการประเมินเพื่อปรับปรุงอย่างต่อเนื่อง (สอดคล้องกับ Privacy Maturity Model: PMM)	
127	องค์กรต้องมีการปรับปรุงและพัฒนาแผนรับมือเหตุด้านความมั่นคงปลอดภัยและเหตุละเมิดข้อมูลส่วนบุคคลเป็นประจำ เพื่อให้สอดคล้องกับสถานการณ์จริง (สอดคล้องกับ Privacy Maturity Model: PMM)	
128	องค์กรต้องวิเคราะห์แนวโน้มของเหตุละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น และนำผลการวิเคราะห์มาใช้ในการออกมาตรการเชิงป้องกันไม่ให้เกิดเหตุซ้ำ (สอดคล้องกับ Privacy Maturity Model: PMM)	

สคส.

สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

120 หมู่ 3 ชั้น 7 อาคารรัฐประศาสนภักดี ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา
5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

www.pdpc.or.th

PDPC Thailand

PDPC Thailand

saraban@pdpc.or.th