มาตรฐานการรักษาความมั่นคงปลอดภัย
ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น1)

ประจำปี 2547

จัดพิมพ์เพื่อเผยแพร่โดย
คณะอนุกรรมการด้านความมั่นคง
ภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

คำนำ

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ฉบับนี้จัดทำขึ้นโดยคณะอนุกรรมการด้านความมั่นคงภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ซึ่งจัดตั้งขึ้นตามพระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 คณะอนุกรรมการด้านความมั่นคง มีหน้าที่หลัก 5 ประการคือ

1) เสนอแนะนโยบายและมาตรการด้านความมั่นคงให้เกิดความเชื่อมั่นและปลอดภัยในการใช้ระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ของประเทศในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

2) ติดตามวิเคราะห์กลั่นกรองและเผยแพร่ข้อมูลที่เกี่ยวกับความมั่นคงของธุรกรรมทางอิเล็กทรอนิกส์ให้แก่หน่วยงานภาครัฐ ภาคธุรกิจและประชาชน

3) สร้างความตื่นตัวเพื่อให้ภาคเอกชนหรือประชาชนตระหนักถึงความสำคัญของความมั่นคงในการใช้ระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

4) ดำเนินการหรือประสานงานกับหน่วยงานอื่นๆในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงที่เป็นประโยชน์ต่อการทำงานหรือการพัฒนาบุคลากรในด้านดังกล่าว

5) ร่วมมือหรือประสานงานในการดำเนินการตามข้อ 1 ถึงข้อ 4 กับต่างประเทศ หรือองค์การระหว่างประเทศปฏิบัติการอื่นใดตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมาย

มาตรฐานนี้จึงเป็นหนึ่งในภารกิจที่คณะอนุกรรมการด้านความมั่นคงได้จัดทำขึ้นโดยมีวัตถุประสงค์ในเบื้องต้น ดังนี้

1) เป็นแนวทางศึกษาการดำเนินการให้เกิดความมั่นคงปลอดภัยในการประกอบธุรกรรม ทางอิเล็กทรอนิกส์ ซึ่งมาตรฐานดังกล่าวอ้างอิงจากมาตรฐานสากล ISO 17799 / IEC 17799: 2000 และมาตรฐานที่ใช้ในประเทศสหรัฐอเมริกา NIST(National Institute of Standards and Technology) Special Publication800-52 และมาตรฐานที่ใช้ในประเทศออสเตรเลีย นิวซีแลนด์ AS/NZS (BS) 7799 ซึ่งครอบคลุม Information Security Management System (ISMS)

2)เพื่อเป็นแนวทางเสริมสร้างการรักษาความมั่นคงปลอดภัยให้กับองค์กรหรือหน่วยงานที่เกี่ยวข้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์โดยเริ่มต้นจากการสร้างความมั่นคงปลอดภัยให้กับองค์กรในระดับพื้นฐาน (ระดับ 1) และเมื่อองค์กร

มีความพร้อมในระดับเบื้องต้นแล้วจึงได้ก้าวขึ้นสู่ระดับกลาง(2) และสูง(3) เพื่อองค์กรจะได้มีความมั่นคงปลอดภัยมากยิ่งขึ้นและเป็นพื้นฐานสู่การพัฒนาไปสู่การได้รับมาตรฐานในระดับสากลต่อไปซึ่งปัจจุบันได้มีองค์กรหรือหน่วยงานที่มีความตระหนักในด้านความมั่นคงปลอดภัยได้ก้าวล้ำไปสู่กระบวนการสร้างความมั่นคงปลอดภัยให้กับองค์กรในระดับ Best Practice แล้ว

สำหรับองค์กรเหล่านั้นไม่จำเป็นต้องกลับมาเริ่มต้นดำเนินการตามแนวทางแห่งมาตรฐานนี้สำหรับองค์ประกอบของมาตรฐานนี้ประกอบด้วยสิ่งจำเป็นสำหรับการเริ่มต้นสร้างมาตรฐานความมั่นคงปลอดภัยให้กับองค์กรในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งแบ่งเป็น 10 หัวข้อ ดังนี้

1) นโยบายความมั่นคงปลอดภัยขององค์กร
2) โครงสร้างความมั่นคงปลอดภัยภายในองค์กร
3) การจัดหมวดหมู่และการควบคุมทรัพย์สินขององค์กร
4) มาตรฐานของบุคลากรเพื่อสร้างความมั่นคงปลอดภัยให้กับองค์กร
5) ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร
6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร
7) การควบคุมการเข้าถึงระบบสารสนเทศขององค์กร
8) การพัฒนาและดูแลระบบสารสนเทศ
9) การบริหารความต่อเนื่องในการดำเนินงานขององค์กร
10) การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและบทลงโทษของการละเมิดนโยบาย

นแต่ละหัวข้อจะระบุวัตถุประสงค์ในการดำเนินการที่เกี่ยวข้องกับหัวข้อนั้น และมีข้อปฏิบัติ แยกตามวัตถุประสงค์ในแต่ละหัวข้อมีจำนวนข้อย่อยซึ่งจัดเป็นแนวทางปฏิบัติ รวมทั้งสิ้น 144 ข้อ และเพื่อให้องค์กรเริ่มต้นทำความเข้าใจกับแนวทางปฏิบัติเหล่านี้ คณะอนุกรรมการฯ จึงแบ่งระดับความยากง่ายในการเริ่มต้นสร้างความมั่นคงปลอดภัยให้กับองค์กรเป็น 3 ระดับ โดยพิจารณาจากความจำเป็นเบื้องต้นในการสร้างความมั่นคงปลอดภัยเกี่ยวกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์ และได้ให้ความหมายของแต่ละระดับไว้ดังนี้

ความมั่นคงปลอดภัยพื้นฐาน หมายถึง หัวข้อปฏิบัติที่คณะอนุกรรมการฯ ได้พิจารณาแล้วและเห็นว่าเหมาะสมกับองค์กรที่ต้องการระดับความมั่นคงปลอดภัยพื้นฐาน

ความมั่นคงปลอดภัยปานกลาง หมายถึง หัวข้อปฏิบัติที่คณะอนุกรรมการฯ ได้พิจารณาแล้วและเห็นว่าเหมาะสมกับองค์กรที่ต้องการระดับความมั่นคงปลอดภัยปานกลาง

ความมั่นคงปลอดภัยสูง หมายถึง หัวข้อปฏิบัติที่คณะอนุกรรมการฯ ได้พิจารณาแล้วและเห็นว่าเหมาะสมกับองค์กรที่ต้องการระดับความมั่นคงปลอดภัยสูง

สำหรับส่วนภาคผนวกของมาตรฐานนี้ คณะอนุกรรมการฯ ได้จัดหาข้อมูลที่จำเป็นเพื่อประกอบเป็นแนวทางปฏิบัติด้านความมั่นคงปลอดภัย ได้แก่

1) ตัวอย่างวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยที่ต้องใช้งานอย่างสม่ำเสมอ เช่น ตัวอย่างระเบียบในการใช้งานเครือข่าย การตั้งรหัสผ่านที่แข็งแกร่ง เป็นต้น

2) คำถามที่มีลักษณะเป็นเกณฑ์เพื่อใช้ประเมินความเสี่ยงขององค์กร คณะอนุกรรมการฯ พิจารณาเห็นว่าเกณฑ์เหล่านี้น่าจะเป็นประโยชน์ต่อการเริ่มต้นประเมินความเสี่ยงขององค์กร เพื่อให้สามารถดำเนินการตามแนวทางปฏิบัติแห่งมาตรฐานนี้ง่ายขึ้น จึงเรียบเรียงทำเกณฑ์ที่ใช้ประเมินระดับความเสี่ยงต่อระบบสารสนเทศขององค์กรหรือสารสนเทศที่ใช้

ประกอบธุรกรรมทางอิเล็กทรอนิกส์เป็นลักษณะคำถามให้แต่ละองค์กรสามารถประเมินระดับความเสี่ยงต่อสิ่งเหล่านั้น ผลจากการประเมินจะจัดระดับได้ 3 ระดับ คือ องค์กรที่มีความเสียงระดับต่ำ องค์กรที่มีความเสี่ยงระดับปานกลาง และองค์กรที่มีความเสี่ยงระดับสูง หากผลลัพธ์ที่ประเมินออกมาองค์กรมีความเสี่ยงอยู่ในระดับสูง องค์กรควรใช้แนวทางทั้งหมด ในการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศที่เกี่ยวข้องขององค์กร

อย่างไรก็ตาม หากองค์กรที่นำไปใช้พิจารณาเห็นว่าแนวทางปฏิบัติในระดับที่องค์กร ประเมินไว้ยังไม่ครอบคลุมความเสี่ยงอื่นๆที่อาจเกิดขึ้นได้ องค์กรสามารถนำแนวทางปฏิบัติในระดับที่สูงขึ้นมาร่วมปฏิบัติเพิ่มเติมได้ เพื่อให้ครอบคลุมความเสี่ยงอื่น ๆ อันอาจจะเกิดขึ้นจากลักษณะเฉพาะในการดำเนินงานขององค์กร เช่น องค์กรที่ต้องใช้ระบบการชำระเงินทางอินเทอร์เน็ต ควรพิจารณาองค์ประกอบของระบบนี้ให้มั่นคงปลอดภัยในระดับสูง เป็นต้น แต่หากยังขาดความพร้อมด้านงบประมาณก็สามารถเริ่มดำเนินการในระดับพื้นฐานและในข้อปฏิบัติที่จำเป็น จากนั้นวางแผนยกระดับบสำหรับปีต่อๆ ไปจนสามารถปฏิบัติได้ครบ 144 ข้อ ทั้งนี้ เพื่อให้มีระดับความมั่นคงปลอดภัยในการ ประกอบธุรกรรมทางอิเล็กทรอนิกส์ที่สูงขึ้น

3) ตัวอย่างองค์กรสำคัญที่เกี่ยวกับโครงสร้างพื้นฐานของประเทศจึงจัดว่าเป็นองค์กรที่มีความเสี่ยงสูง ต้องปฏิบัติตามแนวทางนี้อย่างครบถ้วน (ระดับที่ 1+2+3) เพื่อให้เกิดความมั่นคงปลอดภัยในระดับสูง

4) นิยามตำแหน่งงาน หน้าที่และความรับผิดชอบ ที่ใช้เป็นตัวแทนของผู้ปฏิบัติปรากฏตามวงเล็บในแต่ละข้อย่อยเป็นข้อมูลตามที่องค์กรสามารถพิจารณาให้เหมาะสมกับโครงสร้างองค์กร

อย่างไรก็ตาม มาตรฐานนี้จัดเป็นมาตรฐานด้านความมั่นคงปลอดภัยในการ ประกอบธุรกรรมทางอิเล็กทรอนิกส์เวอร์ชั่น1 เป็นแนวทางและเป็นฉบับแรกที่จัดทำขึ้นเพื่อใช้ในการศึกษาฉบับแรกสำหรับประเทศไทยที่จัดทำขึ้นเพื่อใช้ในการศึกษาเป็นแนวทางสร้างความมั่นคงปลอดภัยในการประกอบธุรกรรมทาง อิเล็กทรอนิกส์ให้กับองค์กรต่างๆ ดังนั้น แต่ละองค์กรสามารถนำไปประยุกต์ใช้ได้อย่างยืดหยุ่นตามความเหมาะสมหรือลักษณะการดำเนินงานขององค์กร

สำหรับผลที่คาดว่าจะได้รับคือการที่องค์กรในประเทศไทยสามารถยกระดับมาตรฐานความมั่นคงปลอดภัยขึ้นสู่ระดับที่สูงขึ้น การลดความเสียหาย ต่อการดำเนินงาน ทรัพย์สินบุคลากรและรายได้ขององค์กรและผลในระดับที่สูงกว่าคือการลดความเสียหายในระดับเศรษฐกิจและสังคมของประเทศและทำให้เป็นที่ยอมรับในระดับนานาชาติ

ท้ายสุดนี้ คณะอนุกรรมการฯ ยินดีที่จะรับความเห็นตอบกลับจากองค์กรต่างๆ ที่ได้รับมาตรฐานนี้ไปพิจารณาจากนั้นคณะอนุกรรมการฯจะได้รวบรวมความเห็นจากองค์กรของท่านและผู้เชี่ยวชาญต่างๆ ไปปรับปรุงให้เป็นมาตรฐานฉบับที่สมบูรณ์ยิ่งขึ้น

คณะอนุกรรมการด้านความมั่นคง
ภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
11 ตุลาคม 2547

สารบัญ

หัวข้อ **หน้า**

หัวข้อ **หน้า**

หัวข้อ **หน้า**

ตารางแสดงความหมายของสัญลักษณ์

สัญลักษณ์	ความหมาย
	ระดับ 1 คือ ระดับความมั่นคงปลอดภัยพื้นฐาน
	ระดับ 2 คือ ระดับความมั่นคงปลอดภัยปานกลาง
	ระดับ 3 คือ ระดับความมั่นคงปลอดภัยสูง
	มาตรการด้านการป้องกัน (preventive)
	มาตรการด้านการตรวจสอบ (detective)
	มาตรการด้านการแก้ไข (corrective)
	มาตรการที่เกี่ยวข้องกับบุคลากร (people)
	มาตรการที่เกี่ยวข้องกับกระบวนการ (process)
	มาตรการที่เกี่ยวข้องกับเทคโนโลยี (technology)

1. นโยบายความมั่นคงปลอดภัยขององค์กร (Security policy)

1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)
มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

ข้อที่ 1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document) (ดูตัวอย่างได้จากภาคผนวก ก)

(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษร และนโยบายนี้ต้องได้รับการอนุมัติจากผู้บริหารขององค์กรในการนำไปใช้

ข้อที่ 2 (ผู้บริหารองค์กร) ต้องจัดให้มีการเผยแพร่เอกสารนโยบายความมั่นคงปลอดภัยให้พนักงานทุกระดับในองค์กรทราบ

ข้อที่ 3 การตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัย (Review and evaluation)

(ผู้บริหารสารสนเทศ) ต้องดำเนินการตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย 1 ครั้งต่อปี

ข้อที่ 4 การลงนามยอมรับและปฏิบัติตามนโยบายความมั่นคงปลอดภัยขององค์กร

(พนักงาน) ทุกคนที่ใช้งานสารสนเทศในองค์กร ต้องลงนามยอมรับและปฏิบัติตามนโยบายความมั่นคงปลอดภัยขององค์กร

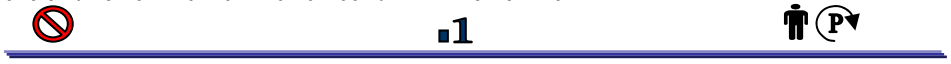
2. โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Organizational Security)

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยของสารสนเทศภายในองค์กร (Information security infrastructure)

จุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

ข้อที่ 5 คณะทำงานความมั่นคงปลอดภัยสำหรับสารสนเทศ (Management information security forum)

(ผู้บริหารองค์กร)ต้องจัดตั้งคณะหรือกลุ่มผู้ทำงานหลักเพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร



ข้อที่ 6 การกำหนดสิทธิในการใช้งานระบบสารสนเทศ (Authorization process for information processing facilities)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการกำหนดสิทธิของพนักงานการใช้งานระบบสารสนเทศทั้งระบบปัจจุบันที่มีอยู่แล้วและที่จะนำเข้ามาใช้งานใหม่

ข้อที่ 7 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)

(ผู้บริหารองค์กร) ต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร

ข้อที่ 8 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน

ข้อที่ 9 การประสานงานทางด้านความมั่นคงปลอดภัยระหว่างองค์กร (Co-operate between organizations)

(ผู้บริหารองค์กร)ต้องทำการติดต่อและประสานงานเพื่อสร้างความร่วมมือทางด้านความมั่นคงปลอดภัยระหว่างองค์กร เช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ องค์การโทรศัพท์ การสื่อสารแห่งประเทศไทย ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น

ข้อที่ 10 ผู้เชี่ยวชาญที่สามารถให้ คำแนะนำและคำปรึกษาทางด้านความมั่นคงปลอดภัย (Specialist information security advice)

(ผู้บริหารสารสนเทศ)ต้องกำหนดตัวบุคลากรในองค์กรเพื่อทำหน้าที่ให้คำแนะนำเกี่ยวกับการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กรหากในองค์กรไม่มีผู้เชี่ยวชาญต้องกำหนดบุคคลซึ่งสามารถขอคำปรึกษาจากผู้เชี่ยวชาญภายนอกได้ทันที

ข้อที่ 11 การตรวจสอบการปฏิบัติงานของพนักงานกับนโยบายความมั่นคงปลอดภัยโดยผู้ตรวจสอบอิสระ (Independent review of information security)

(ผู้บริหารสารสนเทศ)ต้องกำหนดให้มีการตรวจสอบว่าการปฏิบัติงานของพนักงานเป็นไปตามหรือสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรหรือไม่

2.2 การควบคุมความมั่นคงปลอดภัยแก่หน่วยงานภายนอกที่มีความจำเป็นต้องใช้งานระบบสารสนเทศขององค์กร (Security of third party access)

มีจุดประสงค์เพื่อควบคุมหน่วยงานภายนอก (เช่น ผู้ขายฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น)ในการใช้งานระบบสารสนเทศและทรัพยากรสารสนเทศอื่นขององค์กรให้เป็นไปอย่างปลอดภัย

ข้อที่ 12 การระบุลักษณะของการเข้าใช้งาน (Types of access)

(หัวหน้างานสารสนเทศ) ต้องระบุลักษณะการเข้าใช้งานระบบของหน่วยงาภายนอก เช่น การใช้งานผ่านทางเครือข่าย เทียบกับการใช้งานในสำนักงานโดยตรงซึ่งลักษณะทั้งสองนี้จะมีความเสี่ยงที่แตกต่างกัน เป็นต้น

ข้อที่ 13 การระบุเหตุผลความจำเป็นในการเข้าใช้งานระบบของหน่วยงานภายนอก (Reasons for access)

(หน่วยงานภายนอก) ต้องระบุเหตุผลความจำเป็นในการเข้าใช้งานอย่างชัดเจน

ข้อที่ 14 การควบคุมหน่วยงานภายนอกที่ปฏิบัติงานอยู่ในสำนักงาน (On-site contractors)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการควบคุมหน่วยงานภายนอกที่ปฏิบัติงานอยู่ในสำนักงานขององค์กรในการใช้งานระบบสารสนเทศและทรัพยากรสารสนเทศอื่นๆ ให้เป็นไปอย่างปลอดภัย(รวมทั้งในสัญญาที่ทำไว้กับหน่วยงานนั้นจะต้องระบุข้อกำหนดในการใช้งานไว้อย่างชัดเจน)

2.3 การมอบหมายงานทางด้านสารสนเทศให้กับหน่วยงานภายนอก(Outsourcing)

มีจุดประสงค์เพื่อควบคุมหน้าที่ความรับผิดชอบของหน่วยงานภายนอกที่ได้รับมอบหมายให้มาดูแลงานทางด้านสารสนเทศขององค์กร(อาจได้รับมอบหมายงานส่วนหนึ่งหรือทั้งหมดก็ได้)

ข้อที่ 15 การจัดทำสัญญาการปฏิบัติหน้าที่กับหน่วยงานภายนอก (Security requirements in outsourcing contracts)

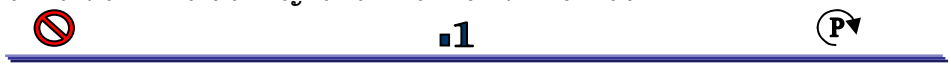
(หัวหน้างานสารสนเทศ) ต้องจัดทำสัญญาการปฏิบัติหน้าที่กับหน่วยงานภายนอกและสัญญาต้องมีความชัดเจน โดยระบุถึงเหตุผลความจำเป็นในการใช้งาน ลักษณะการใช้งาน รวมทั้งข้อกำหนดต่างๆ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นในอนาคต

3. การจัดหมวดหมู่และการควบคุมทรัพย์สินขององค์กร (Asset classification and control)

3.1 การจัดทำบัญชีทรัพย์สิน (Accountability for assets)
มีจุดประสงค์เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

ข้อที่ 16 การจัดทำบัญชีทรัพย์สิน (Inventory of assets)

(หัวหน้างานสารสนเทศ) ต้องจัดทำบัญชีทรัพย์สินขององค์กร (ซึ่งรวมถึงบัญชีครุภัณฑ์คอมพิวเตอร์และบัญชีข้อมูลที่เก็บไว้ในสื่อต่างๆทั้งหมด) เพื่อใช้ในการกำหนดมูลค่าทรัพย์สิน ระดับความสำคัญและวิธีการป้องกันที่เหมาะสม



ข้อที่ 17 การตรวจสอบทรัพย์สิน (Inventory check)

(ผู้บริหารสารสนเทศ) ต้องจัดให้มีการตรวจสอบบัญชีทรัพย์สินตามระยะเวลาที่กำหนดไว้ เช่น ปีละ 1 ครั้ง เป็นต้น

3.2 การจัดหมวดหมู่ข้อมูลและทรัพย์สินสารสนเทศ (Information classification)
มีจุดประสงค์เพื่อป้องกันสารสนเทศขององค์กรโดยวิธีการที่เหมาะสม

ข้อที่ 18 วิธีการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสาร (Classification guidelines)

(ผู้บริหารสารสนเทศ) ต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของข้อมูลและทรัพย์สินสารสนเทศ เช่น เอกสารลับ เอกสารเปิดเผยได้ เป็นต้น ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม

ข้อที่ 19 การจัดทำป้ายชื่อ และการจัดการข้อมูลและทรัพย์สินสารสนเทศ (Information labeling and handling)

(ผู้บริหารสารสนเทศ) ต้องจัดให้มีวิธีการจัดทำป้ายชื่อสำหรับข้อมูลและทรัพย์สินสารสนเทศ และต้องมีวิธีการจัดการข้อมูลและทรัพย์สินสารสนเทศ โดยแยกตามหมวดหมู่ที่กำหนดไว้แล้ว

4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Personnel Security)

4.1 การสร้างความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากร (Security in job definition and resourcing)

มีจุดประสงค์เพื่อลดความเสี่ยงจากความผิดพลาดการขโมยการปลอมแปลงและการนำไปใช้ในทางที่ไม่เหมาะสมของพนักงานอันเกิดจากการปฏิบัติงานกับระบบสารสนเทศและทรัพยากรสารสนเทศอื่นๆ ขององค์กร

ข้อที่ 20 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Including security in job responsibilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศในคุณสมบัติของบุคลากรที่ต้องการสรรหา

ข้อที่ 21 การตรวจสอบคุณสมบัติของผู้สมัคร (Personnel screening and policy)

(หัวหน้างานสารสนเทศ) ต้องตรวจสอบคุณสมบัติของผู้สมัครโดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา บุคคลหรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น

ข้อที่ 22 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment)

(หัวหน้างานสารสนเทศ) ต้องกำหนดเงื่อนไขการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศขององค์กร

ข้อที่ 23 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)

(หัวหน้างานบุคคล) ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานและองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างพนักงานนั้น)

4.2 การอบรมพนักงาน (User training)

มีจุดประสงค์เพื่อให้พนักงานได้ตระหนักถึงภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศรวมถึงให้ความรู้แก่พนักงานเพื่อให้สามารถป้องกันภัยดังกล่าวได้

ข้อที่ 24 การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security education and training)

(หัวหน้างานสารสนเทศ) ต้องจัดอบรมให้ความรู้แก่พนักงาน เกี่ยวกับวิธีปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศและเครือข่ายขององค์กร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัย และการเปลี่ยนแปลงที่เกิดขึ้นด้านสารสนเทศขององค์กรด้วย

4.3 การตอบโต้ต่อเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัย (Responding to security incidents and malfunctions)

มีจุดประสงค์เพื่อลดความเสียหายอันมีสาเหตุมาจากเหตุการณ์ละเมิดความมั่นคงปลอดภัย (เช่น ไวรัสคอมพิวเตอร์แพร่กระจาย ระบบถูกบุกรุก เป็นต้น) และระบบทำงานบกพร่อง รวมทั้งเพื่อให้บุคลากรในองค์กรได้เรียนรู้จากประสบการณ์ความเสียหายดังกล่าว

ข้อที่ 25 การรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัย (Reporting security incidents)

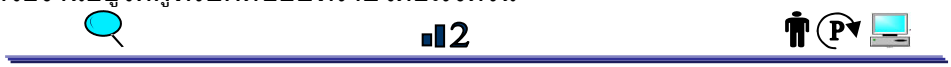
(พนักงาน) ต้องทำการรายงานเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยซึ่งเกิดขึ้นให้แก่ผู้ที่รับผิดชอบทราบโดยเร่งด่วน

ข้อที่ 26 การรายงานจุดอ่อนในระบบสารสนเทศ (Reporting security weaknesses)

(พนักงาน) ต้องรายงานจุดอ่อน ช่องโหว่ หรือภัยที่พบในระบบสารสนเทศที่ใช้งานอยู่ให้ผู้ที่รับผิดชอบทราบโดยเร่งด่วน

ข้อที่ 27 การรายงานการทำงานที่บกพร่องของระบบสารสนเทศ (Reporting software malfunctions)

(พนักงาน) ต้องรายงานการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟต์แวร์ที่ใช้งานอยู่ให้ผู้ที่รับผิดชอบทราบโดยเร่งด่วน



ข้อที่ 28 การเรียนรู้จากเหตุการณ์ละเมิดความมั่นคงปลอดภัย (Learning from Incidents)
(ผู้ดูแลระบบ) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า



ข้อที่ 29 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary process)
(ผู้บริหารองค์กร) ต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายความมั่นคงปลอดภัยหรือระเบียบปฏิบัติเพื่อความมั่นคงปลอดภัยขององค์กร




5. ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and environmental security)

5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงบริเวณที่ต้องการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นด้วย

ข้อที่ 30 การกั้นบริเวณล้อมรอบ (Physical security perimeter)

(หัวหน้างานสารสนเทศ) ต้องมีการจัดสรรพื้นที่ หรือ จัดทำกำแพง หรือผนังที่มีความแข็งแรงเพื่อล้อมรอบบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

ข้อที่ 31 การควบคุมการเข้าออก (Physical entry controls)

(หัวหน้างานสารสนเทศ) ต้องมีการควบคุมการเข้าออกในบริเวณพื้นที่ควบคุมโดยให้ผ่านเข้าออกได้เฉพาะผู้ที่มีสิทธิเท่านั้น

ข้อที่ 32 การรักษาความมั่นคงปลอดภัยในบริเวณพื้นที่ส่งมอบผลิตภัณฑ์ (Isolated delivery and loading areas)

(หัวหน้างานสารสนเทศ)ต้องมีมาตรการควบคุมบริเวณที่จัดไว้ให้เป็นพื้นที่สำหรับการส่งมอบ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดไว้ ทั้งนี้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อที่ 33 การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ (Securing offices, rooms and facilities)

(หัวหน้างานสารสนเทศ)ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับสำนักงานห้องทำงานและเครื่องมือต่างๆเช่นเครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมากสำนักงานหรือห้องจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าวประตูหน้าต่างของสำนักงานหรือห้องต้องใส่กุญแจเสมอเมื่อไม่มีคนอยู่ต้องตั้งเครื่องโทรสารหรือถ่ายเอกสารแยกออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น

ข้อที่ 34 การควบคุมการปฏิบัติงาน (Working in secure areas)

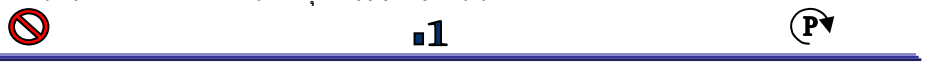
(หัวหน้างานสารสนเทศ)ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายรูปหรือวิดีโอในบริเวณนั้น เป็นต้น

5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับเครื่องมือหรืออุปกรณ์สำนักงาน

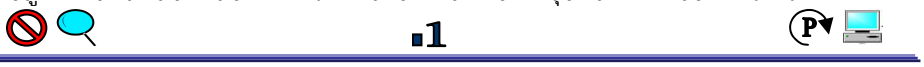
ข้อที่ 35 การจัดตั้งและการป้องกันอุปกรณ์ (Equipment siting and protection)

(พนักงาน)ต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น



ข้อที่ 36 การดูแลรักษาอุปกรณ์ (Equipment maintenance)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงปีละ 1 ครั้ง เป็นต้น



ข้อที่ 37 การป้องกันอุปกรณ์และทรัพย์สินสารสนเทศที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันอุปกรณ์ขององค์กร เช่น Notebook, Organizer, Mobile Phoneเมื่อถูกนำไปใช้งานนอกสำนักงานต้องกำหนดระเบียบปฏิบัติในการใช้งาน การยืม-คืน เป็นต้น

ข้อที่ 38 การทำลายอุปกรณ์ (Secure disposal or reuse of equipment)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น ทั้งนี้ เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว

ข้อที่ 39 ระบบกระแสไฟฟ้าสำรอง (Power supplies)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีระบบกระแสไฟฟ้าสำรอง เช่น เดินสายไฟฟ้า เส้นสำรองใช้ Uninterruptible Power Supply ใช้เครื่องปั่นไฟสำรอง เป็นต้น

ข้อที่ 40 การเดินสายไฟฟ้าและสายเคเบิล (Cabling security)

(หัวหน้างานสารสนเทศ)ต้องกำหนดให้มีการป้องกันการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน เช่น ผ่านเข้ามาทางใต้ดิน ผ่านช่องพิเศษที่จัดไว้ หรือเป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย เป็นต้น

5.3 การป้องกันทั่วไป (General controls)

มีจุดประสงค์เพื่อป้องกันการเปิดเผยหรือการขโมยสารสนเทศหรือระบบสารสนเทศขององค์กร

ข้อที่ 41 นโยบายควบคุมการไม่ทิ้งเอกสารสำคัญไว้ในที่ที่พบเห็นได้ง่าย (Clear desk and clear screen policy)

(พนักงาน) ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลที่สำคัญๆไว้ในที่ที่สามารถพบเห็นได้ง่ายโดยจัดเก็บไว้ในที่ที่ปลอดภัย ต้องทำการลงบันทึกออกจากคอมพิวเตอร์ (log off) เมื่อจำเป็นต้องหยุดการใช้งานคอมพิวเตอร์ไปเป็นระยะเวลาหนึ่ง นอกจากนี้ ตู้จ่ายเอกสารหรือจดหมายและเครื่องโทรสารจะต้องได้รับการดูแลให้ปลอดภัยด้วย

ข้อที่ 42 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)

(หัวหน้างานอาคาร) ต้องกำหนดให้มีการควบคุมการนำอุปกรณ์ เอกสารซอฟต์แวร์ หรือทรัพย์สินอื่นๆ ขององค์กรออกนอกสำนักงานอย่างมั่นคงปลอดภัย

6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)

6.1 การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน (Operational procedures and responsibilities)

มีจุดประสงค์เพื่อให้การใช้งานสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย จึงจำเป็นต้องมีการกำหนดหน้าที่ความรับผิดชอบ และวิธีการปฏิบัติงานไว้อย่างชัดเจน

ข้อที่ 43 คู่มือและขั้นตอนการปฏิบัติงาน (Documented operating procedures)

(หัวหน้างานสารสนเทศ) ต้องจัดทำคู่มือและขั้นตอนการปฏิบัติงานสำหรับระบบสารสนเทศ

ข้อที่ 44 การบริหารจัดการสารสนเทศภายนอกองค์กร (External facility management)

(หัวหน้างานสารสนเทศ) ต้องจัดทำข้อกำหนดหรือสัญญาเพื่อควบคุมหน่วยงานภายนอก ซึ่งได้รับมอบหมายให้บริหารและจัดการสารสนเทศขององค์กรโดยดำเนินการอยู่ภายนอกสำนักงาน ให้ใช้งานหรือเข้าถึงระบบตามสิทธิที่ตนได้รับ

ข้อที่ 45 วิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือละเมิดความมั่นคงปลอดภัย (Incident management procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือละเมิดความมั่นคงปลอดภัย ได้แก่ ระบบไม่สามารถให้บริการได้ ความผิดพลาดอันเกิดจากข้อมูลที่คีย์เข้าระบบไม่ถูกต้อง การเปิดเผยข้อมูลความลับขององค์กรหรือระบบขัดข้อง เป็นต้น

ข้อที่ 46 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)

(หัวหน้างานสารสนเทศ) ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศและเครือข่าย เพื่อให้เกิดความชัดเจนในการปฏิบัติหน้าที่และลดการทุจริตในการปฏิบัติหน้าที่

ข้อที่ 47 การแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาออกจากเครื่องที่ทำงานจริง (Separation of development and operational facilities)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบสารสนเทศ ออกจากเครื่องที่ใช้ทำงานจริงหรือเครื่องที่ให้บริการ

ข้อที่ 48 การควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ (Operational change control)

(หัวหน้างานสารสนเทศ)ต้องจัดให้มีการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ อาทิ จะต้องบันทึกการเปลี่ยนแปลงแก้ไขที่สำคัญๆ และแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบ

6.2 การวางแผนและการตรวจรับทรัพยากรระบบสารสนเทศ (System Planning and Acceptance)

มีจุดประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

ข้อที่ 49 การตรวจรับทรัพยากรสารสนเทศ (System acceptance)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่นๆรวมทั้งต้องทำการทดสอบก่อนที่จะตรวจรับระบบนั้นด้วย

ข้อที่ 50 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity planning)

(ผู้บริหารสารสนเทศ หรือ หัวหน้างานสารสนเทศ) ต้องมีการวางแผนกำหนดความต้องการใช้งานทรัพยากรสารสนเทศ อาทิ ความต้องการใน 1 ปีที่จะถึง เช่น ซีพียูที่เร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น เป็นต้น

6.3 การป้องกันซอฟต์แวร์และสารสนเทศขององค์กร (Protection against malicious Software)

มีจุดประสงค์เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายจากซอฟต์แวร์ที่ไม่ประสงค์ดี

ข้อที่ 51 การป้องกันซอฟต์แวร์ที่ไม่ประสงค์ดี (Controls against malicious software)

(ผู้ดูแลระบบ) ต้องมีการติดตั้งและใช้งานซอฟต์แวร์ป้องกันไวรัส หนอน และม้าโทรจัน เพื่อป้องกันความเสียหายของข้อมูลรวมทั้งมีกลไกเพื่อสร้างความตระหนักให้แก่ผู้ใช้ภายในองค์กร และดูแลมาตรการป้องกันให้ทันสมัยอยู่เสมอ

6.4 การสำรองข้อมูล (Housekeeping)

มีจุดประสงค์เพื่อจัดทำระบบสำรองข้อมูล

ข้อที่ 52 การสำรองข้อมูลภายในองค์กร (Information backup หมายถึง Full backup)

(ผู้ดูแลระบบ) ต้องสำรองข้อมูลที่สำคัญไว้ตามระยะเวลาที่เหมาะสม เช่น สำรองข้อมูลอย่างน้อย 1 ครั้งในรอบ 6 เดือน เป็นต้น

ข้อที่ 53 การจัดทำบันทึกการสำรองข้อมูล (Operator logs)

(ผู้ดูแลระบบ) ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น

ข้อที่ 54 การรายงานข้อผิดพลาด (Fault logging)

(ผู้ดูแลระบบ) ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

ข้อที่ 55 การสำรองข้อมูลภายนอกสำนักงาน (Off-site backup)

(ผู้บริหาร) ต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมของหน่วยงานเพื่อให้สามารถกู้ระบบกลับคืนได้อย่างรวดเร็วและเพื่อป้องกันระบบจากการถูกโจมตี หรือความหายนะที่อาจเกิดขึ้น

ข้อที่ 56 มีการเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup)

(ผู้ดูแลระบบ) ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญโดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

6.5 การบริหารและจัดการเครือข่ายขององค์กร (Network management)

มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยให้กับสารสนเทศและโครงสร้างที่สนับสนุนสารสนเทศขององค์กร

ข้อที่ 57 การบริหารและจัดการด้านความมั่นคงปลอดภัยบนเครือข่าย (Network controls)

(ผู้ดูแลระบบ) ต้องมีการบริหารและจัดการด้านความมั่นคงปลอดภัยบนเครือข่าย ได้แก่

- มีการกำหนดหน้าที่ความรับผิดชอบในการดูแลอย่างชัดเจน
- มีวิธีการในการป้องกันข้อมูลที่ต้องส่งผ่านออกไปยังอินเทอร์เน็ต โดยเฉพาะ การป้องกันความลับและความสมบูรณ์ของข้อมูล
- กลไกในการป้องกันโครงสร้างที่สนับสนุนสารสนเทศให้สามารถทำงานได้อย่างต่อเนื่อง

เป็นต้น

6.6 การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media handling and security)

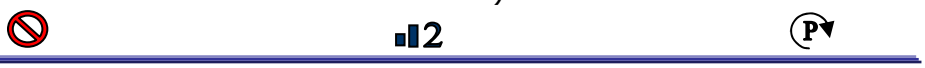
มีจุดประสงค์เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลขององค์กร

ข้อที่ 58 การทำลายสื่อบันทึกข้อมูล (Disposal of media)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีวิธีการกำจัดสื่อบันทึกข้อมูลที่มีความสำคัญสูงเมื่อไม่ได้มีการใช้งานแล้ว

ข้อที่ 59 การบริหารและจัดการสื่อบันทึกข้อมูลที่สามารถถอดแยกได้ (Management of removable computer media)

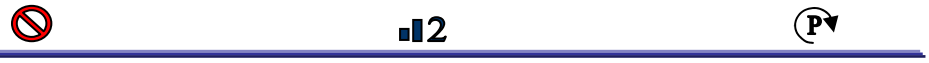
(หัวหน้างานสารสนเทศ) ต้องกำหนดวิธีปฏิบัติและสิทธิสำหรับการใช้งานสื่อบันทึกข้อมูลชนิดที่สามารถถอดแยกออกจากเครื่องคอมพิวเตอร์ได้ อาทิ สื่อบันทึกข้อมูลแบบพกพา เทปบันทึกข้อมูล(เช่นให้ทำการลบข้อมูลเดิมที่ไม่ได้ใช้งานทิ้งไปมีการกำหนดสิทธิว่าบุคคลใดสามารถถอดแยกสื่อบันทึกดังกล่าวได้ เป็นต้น)



ข้อที่ 60 วิธีปฏิบัติในการจัดเก็บสื่อบันทึกข้อมูล (Information handling procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดวิธีการปฏิบัติในการจัดเก็บสื่อบันทึกข้อมูลเพื่อป้องกันไม่ให้ข้อมูลที่สำคัญเกิดการรั่วไหลหรือเปิดเผยออกไป ได้แก่

- ต้องมีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน
- กำหนดบุคลากรที่มีสิทธิในการใช้งาน
- ต้องเก็บสื่อบันทึกไว้ในสถานที่และสิ่งแวดล้อมที่ปลอดภัยจากการเสียหายที่อาจเกิดขึ้นได้ เช่น อุณหภูมิสูงหรือต่ำเกินไป เป็นต้น



ข้อที่ 61 การจัดเก็บเอกสารที่เกี่ยวกับระบบสารสนเทศขององค์กรอย่างปลอดภัย (Security of system documentation)

(หัวหน้างานสารสนเทศ)ต้องจัดให้มีการป้องกันการรั่วไหลหรือการเปิดเผยของข้อมูลที่สำคัญที่อยู่ในเอกสารที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร

6.7 การแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ (Exchange of information and software)

มีจุดประสงค์เพื่อป้องกันการสูญหายของสารสนเทศและซอฟต์แวร์รวมทั้งเพื่อป้องกันการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาตหรือการนำสารสนเทศไปใช้ในทางที่ไม่เหมาะสม

ข้อที่ 62 ข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ระหว่างองค์กร (Information and software exchange agreements)

(หัวหน้างานสารสนเทศ)ต้องจัดทำข้อตกลงระหว่างองค์กรอย่างเป็นลายลักษณ์อักษรในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์

ข้อที่ 63 การควบคุมการใช้งานระบบสำนักงานอัตโนมัติให้มีความปลอดภัย (Security of electronic office systems)

(หัวหน้างานอาคารหัวหน้างานสารสนเทศ)ต้องร่วมกันกำหนดวิธีการเพื่อควบคุมกาใช้งานระบบสำนักงานอัตโนมัติ เช่น อุปกรณ์สื่อสารประเภทเคลื่อนที่ได้ เครื่องโทรสาร เครื่องโทรศัพท์ กล้องดิจิทัล เครื่องถ่ายเอกสาร เป็นต้น

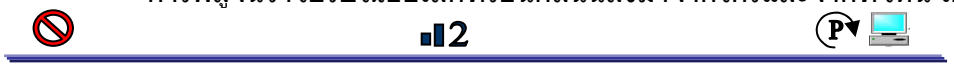
ข้อที่ 64 การจัดส่งสื่อบันทึกข้อมูลอย่างมั่นคงปลอดภัย (Security of media in transit)

(หัวหน้างานธุรการหัวหน้างานสารสนเทศ)ต้องร่วมกันกำหนดวิธีการการจัดส่งสื่อบันทึกข้อมูล(สารสนเทศหรือซอฟต์แวร์)ให้มีความมั่นคงปลอดภัยเช่นเลือกใช้บริการส่งไปรษณีย์ที่เชื่อถือได้ มีการหีบห่อสื่อเป็นอย่างดี มีการลงทะเบียนในการจัดส่ง เป็นต้น

ข้อที่ 65 การวิเคราะห์ความเสี่ยงและวิธีการป้องกัน (Security risks)

(ผู้ดูแลระบบ)ต้องกำหนดวิธีการเพื่อลดความเสี่ยงจากการใช้งานไปรษณีย์อิเล็กทรอนิกส์ ได้แก่

- การป้องกันการเข้าถึงหรือการเปลี่ยนแปลงแก้ไขข้อความในไปรษณีย์อิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต
- การพิสูจน์ว่าไปรษณีย์อิเล็กทรอนิกส์นั้นส่งมาจากใครและจากที่ไหน เป็นต้น



ข้อที่ 66 การแลกเปลี่ยนข้อมูลในรูปแบบอื่นๆ (Other forms of information exchange)

(หัวหน้างานอาคารหัวหน้างานสารสนเทศ)ต้องร่วมกันกำหนดวิธีปฏิบัติเพื่อควบคุมการใช้งานโสตทัศนอุปกรณ์ ได้แก่ เครื่องตอบรับโทรศัพท์อัตโนมัติ เครื่องวิดีโอ เครื่องบันทึกเสียง เป็นต้น ทั้งนี้เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงอุปกรณ์ดังกล่าวได้

ข้อที่ 67 ระเบียบปฏิบัติในการใช้งานไปรษณีย์อิเล็กทรอนิกส์ (Policy on electronic mail)

(หัวหน้างานสารสนเทศ) ต้องจัดทำระเบียบปฏิบัติในการใช้งานไปรษณีย์อิเล็กทรอนิกส์ว่าด้วยเรื่อง

- การป้องกันไวรัสคอมพิวเตอร์ หนอนอินเทอร์เน็ต และม้าโทรจัน
- การป้องกันข้อความและไฟล์แนบที่มีความสำคัญด้วยการเข้ารหัส
- การไม่ใช้ไปรษณีย์อิเล็กทรอนิกส์ในการส่งเอกสารสำคัญเพื่อป้องกันการถูกลักลอบอ่านข้อมูล
- การไม่ส่งไปรษณีย์อิเล็กทรอนิกส์ที่มีลักษณะเป็นการละเมิดสิทธิส่วนบุคคลหรือใช้ในทางไม่เหมาะสม

เป็นต้น

ข้อที่ 68 ความมั่นคงปลอดภัยของพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce security)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีวิธีการในการสร้างความมั่นคงปลอดภัยให้กับระบบพาณิชย์อิเล็กทรอนิกส์ ได้แก่

- ต้องมีการพิสูจน์ตัวตน
- ต้องมีการกำหนดสิทธิทั้งในส่วนของผู้ซื้อและผู้ขาย
- ต้องมีการป้องกันการเปลี่ยนหน้าเว็บไซต์
- ต้องสามารถตรวจสอบข้อมูลการชำระเงินได้เพื่อป้องกันการถูกโกง
- ต้องมีวิธีการชำระเงินที่ปลอดภัย

เป็นต้น

ข้อที่ 69 การป้องกันสารสนเทศที่ปรากฏในที่สาธารณะ (Publicly available systems)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีวิธีการป้องกันเพื่อไม่ให้ข้อมูลขององค์กรที่ปรากฏในที่สาธารณะ เช่น ข้อมูลบนเว็บเซิร์ฟเวอร์ถูกเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต เป็นต้น และมีกระบวนการในการตรวจสอบและอนุมัติก่อนที่ข้อมูลดังกล่าวจะถูกเผยแพร่ออกไปสู่สาธารณชน

7. การควบคุมการเข้าถึง (Access control)

7.1 การควบคุมการเข้าถึงระบบสารสนเทศ (Business requirements for access control)

มีจุดประสงค์เพื่อควบคุมการเข้าถึงระบบบสารสนเทศให้มีความมั่นคงปลอดภัย

ข้อที่ 70 นโยบายและความต้องการขององค์กร (Policy and business requirements)

(หัวหน้างานสารสนเทศ) ต้องจัดทำนโยบายและความต้องการในการใช้งานระบบสารสนเทศ เพื่อควบคุมการเข้าถึงให้ทำได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

ข้อที่ 71 กฎเกณฑ์และข้อห้ามในการเข้าถึงระบบ (Access control rules)

(หัวหน้างานสารสนเทศ หัวหน้างานบุคคล) ต้องร่วมกันกำหนดกฎเกณฑ์ข้อห้ามและบทลงโทษการเข้าถึงระบบสารสนเทศด้วย

7.2 การจัดการการเข้าถึงระบบของพนักงาน (User access management)

มีจุดประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้

ข้อที่ 72 การลงทะเบียนพนักงานใหม่ (User registration)

(หัวหน้างานสารสนเทศ หัวหน้างานบุคคล) ต้องร่วมกันจัดทำระเบียบปฏิบัติในการลงทะเบียนพนักงานใหม่เข้าเป็นสมาชิกขององค์กร เพื่อให้สามารถใช้งานระบบสารสนเทศหรือโครงสร้างสนับสนุนระบบสารสนเทศอื่นทั้งหมดได้นอกจากนี้ต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของพนักงานทันที ในกรณีที่มีการลาออกจากงาน

ข้อที่ 73 การบริหารจัดการรหัสผ่านของพนักงาน (User password management)
(ผู้ดูแลระบบ) ต้องบริหารจัดการรหัสผ่านของพนักงานให้มีความมั่นคงปลอดภัย (ดูตัวอย่างในภาคผนวก ก)

ข้อที่ 74 การบริหารสิทธิการเข้าถึงระบบของพนักงาน (Privilege management)
(ผู้ดูแลระบบ) ต้องกำหนดสิทธิของพนักงานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบด้วย

ข้อที่ 75 การทบทวนสิทธิในการเข้าถึงระบบของพนักงาน (Review of user access rights)
(ผู้ดูแลระบบ) ต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ (เช่น อย่างน้อย 1 ครั้งในรอบ 6 เดือน เป็นต้น)

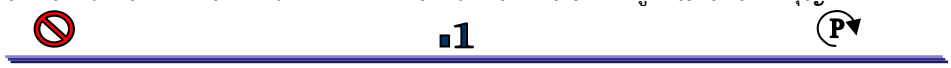
7.3 ความรับผิดชอบหน้าที่ของพนักงาน (User responsibilities)
มีจุดประสงค์เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ สามารถเข้าถึงระบบสารสนเทศได้

ข้อที่ 76 การใช้งานรหัสผ่าน (Password use)
(ผู้ดูแลระบบ) ต้องกำหนดวิธีปฏิบัติที่ดีในการเลือกใช้งานรหัสผ่าน การยกเลิกและการเปลี่ยนแปลงรหัสผ่าน

ข้อที่ 77 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)
(พนักงาน)ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล

7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)
มีจุดประสงค์เพื่อควบคุมการใช้บริการบนเครือข่ายขององค์กร

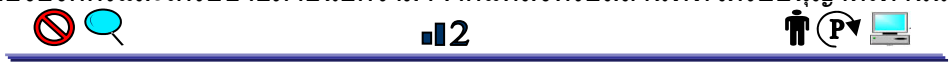
ข้อที่ 78 นโยบายควบคุมการเข้าถึงเครือข่าย (Policy on use of network services)
(หัวหน้างานสารสนเทศ) ต้องจัดทำนโยบายเพื่อควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต



ข้อที่ 79 การจัดแบ่งเครือข่ายภายในองค์กรกับภายนอกองค์กร (Segregation in networks)
(ผู้ดูแลระบบ) ต้องจัดแบ่งเครือข่ายระหว่างองค์กรและคู่ค้า โดยพิจารณาจากบริการเครือข่าย ระบบสารสนเทศ กลุ่มของผู้ใช้งานของทั้งสองฝ่าย

ข้อที่ 80 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)
(ผู้ดูแลระบบ)ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

ข้อที่ 81 การใช้งานเครือข่ายจากแหล่ง หรือสถานที่ที่ได้รับอนุญาต (Node authentication)
(ผู้ดูแลระบบ)ต้องจัดทำกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายขององค์กรและเครือข่ายภายนอกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตเท่านั้น



ข้อที่ 82 การควบคุมโมเด็มที่ผู้ดูแลระบบได้ติดตั้งไว้สำหรับการเข้าถึงจากภายนอก (Remote diagnostic port protection)
(หัวหน้างานสารสนเทศ)ต้องกำหนดให้มีการควบคุมการใช้งานโมเด็มที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กรเพื่อใช้ในการดูแลรักษาระบบจากภายนอก

ข้อที่ 83 ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of network services)

(หัวหน้างานสารสนเทศ ผู้ดูแลระบบ) ต้องจัดทำข้อกำหนดหรือข้อตกลงสำหรับคุณสมบัติด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่างองค์กรกับคู่ค้า

ข้อที่ 84 การควบคุมพนักงานในการใช้งานเครือข่าย (Network connection control)

(ผู้ดูแลระบบ)ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมพนักงานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

ข้อที่ 85 การจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน (Network routing control)

(ผู้ดูแลระบบ) ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

ข้อที่ 86 การจำกัดเส้นทางบนเครือข่าย (Enforced path)

(ผู้ดูแลระบบ) ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้พนักงานสามารถใช้เส้นทางอื่นๆ ได้

7.5 การควบคุมการใช้งานระบบที่ให้บริการ (Operating system access control)

มีจุดประสงค์เพื่อป้องกันการใช้งานเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต

ข้อที่ 87 การจำกัดระยะเวลาการใช้งาน (Limitation of connection time)

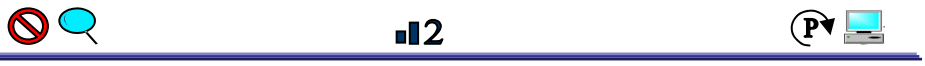
(ผู้ดูแลระบบต้องจำกัดระยะเวลาการใช้งานสำหรับระบบสารสนเทศที่มีความสำคัญสูงหรือมีความเสี่ยงสูง

ข้อที่ 88 การพิสูจน์ตัวตนสำหรับพนักงาน (User identification and authentication)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับพนักงานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

ข้อที่ 89 การบริหารจัดการรหัสผ่าน (Password management system)

(ผู้ดูแลระบบ) ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้พนักงานเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด



ข้อที่ 90 กระบวนการในการเข้าสู่ระบบให้บริการอย่างมั่นคงปลอดภัย (Terminal logon procedures)

(ผู้ดูแลระบบ) ต้องกำหนดกระบวนการในการเข้าสู่ระบบให้บริการอย่างเพื่อใช้งานเครื่องให้บริการที่มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการจะปฏิเสธการใช้งานหากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง เป็นต้น

ข้อที่ 91 การพิสูจน์ตัวตนสำหรับเครื่องลูกข่าย (Automatic terminal identification)

(ผู้ดูแลระบบ) ต้องมีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ก่อนที่จะอนุญาตให้เข้ามาใช้งานเครือข่ายขององค์กร

ข้อที่ 92 การตัดเวลาการใช้งานเครื่องลูกข่าย (Terminal time-out)

(ผู้ดูแลระบบ) ต้องมีวิธีการตัดเวลาการใช้งานเครื่องลูกข่ายเมื่อเครื่องลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อคหน้าจอและต้องใช้รหัสผ่านในการเข้าสู่ระบบ เป็นต้น

ข้อที่ 93 การควบคุมการใช้งานโปรแกรมยูทิลิตี้ (Use of system utilities)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ใครเป็นผู้ใช้งาน

เป็นต้น

ข้อที่ 94 การติดตั้งระบบเตือนภัยสำหรับระบบที่มีความสำคัญสูง (Duress alarm to safeguard users)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการติดตั้งระบบเตือนภัยให้กับผู้ใช้ที่ปฏิบัติงานกับระบบที่มีความสำคัญสูง

7.6 การควบคุมการใช้งานระบบสารสนเทศ (Application access control)

มีจุดประสงค์เพื่อป้องกันการใช้งานระบบสารสนเทศโดยไม่ได้รับอนุญาต

ข้อที่ 95 การจำกัดการใช้งานสารสนเทศ (Information access restriction)

(ผู้ดูแลระบบ) ต้องจัดให้มีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิในการใช้งาน เช่น เขียน อ่าน ลบได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

ข้อที่ 96 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)

(หัวหน้างานสารสนเทศ) ต้องแยกระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในองค์กร เป็นต้น

7.7 การเฝ้าดูการใช้งานระบบ (Monitoring system access and use)

ข้อที่ 97 การบันทึกการเข้าใช้งานระบบสารสนเทศ (Event logging)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีการบันทึกการเข้าใช้งานระบบสารสนเทศซึ่งข้อมูลที่เก็บ ได้แก่ ผู้ใช้งาน เวลาที่เข้าใช้และออกจากระบบ ต้นทางมาจากแอดเดรสใดบนเครือข่าย เป็นต้น รวมทั้งบันทึกนี้ต้องเก็บไว้เป็นระยะเวลาหนึ่ง

ข้อที่ 98 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)

(ผู้ดูแลระบบ)ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกัน โดยให้อิงกับเวลามาตรฐานกลางของโลกเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

ข้อที่ 99 วิธีการในการเฝ้าดูการใช้งานระบบสารสนเทศ (Procedures and areas of risk)

(ผู้ดูแลระบบ) ต้องจัดให้มีวิธีการในการเฝ้าดูการใช้งานระบบสารสนเทศว่าผู้ใช้ใช้ตามสิทธิที่ตนได้รับหรือไม่

ข้อที่ 100 การเฝ้าดูระบบสารสนเทศโดยพิจารณาจากปัจจัยความเสี่ยง (Risk factors)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการเฝ้าดูความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศตามระยะเวลาที่เหมาะสมโดยพิจารณาจากปัจจัยความเสี่ยงของแต่ละระบบ

ข้อที่ 101 การบันทึกและตรวจสอบข้อมูลกิจกรรมการใช้งาน (Logging and reviewing events)

(หัวหน้างานสารสนเทศ) ต้องกำหนดระยะเวลาที่เหมาะสม เพื่อตรวจสอบข้อมูลกิจกรรมการเข้าใช้งานที่ได้บันทึกเก็บไว้ (เช่นกำหนดเป็นระยะเวลา 3 เดือน หรือ 6 เดือน เป็นต้น ตามความถี่ที่เหมาะสม)

ข้อที่ 102 มีการตรวจสอบการทำงานของผู้ดูแลระบบในองค์กร (System Administrator)

(ผู้บริหารสารสนเทศ หรือ หัวหน้างานสารสนเทศ) ต้องมีการตรวจสอบการทำงานของผู้ดูแลระบบในองค์กร โดยมีการบันทึกการทำงานของผู้ดูแลระบบทุกการกระทำที่ทำต่อระบบ

7.8 คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถาน (Mobile computing and teleworking control)

มีจุดประสงค์เพื่อควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทเคลื่อนที่ได้รวมทั้งการปฏิบัติงานนอกสำนักงานให้เป็นไปอย่างปลอดภัย

ข้อที่ 103 การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Mobile computing)

(พนักงาน) ต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (notebook, palmtops, laptop) เช่น เมื่อปฏิบัติงานอยู่นอกสถานที่

- ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง
- ต้องใช้กุญแจล็อคเครื่องคอมพิวเตอร์พกพา
- ต้องเข้ารหัสข้อมูลที่สำคัญไว้

เป็นต้น

ข้อที่ 104 การปฏิบัติงานนอกสำนักงาน (Teleworking)

(พนักงาน) ต้องปฏิบัติตามนโยบายการปฏิบัติงานนอกสำนักงาน เช่น ใช้วิธีการป้องกันตามข้อ 103 สำหรับเครื่องคอมพิวเตอร์พกพา การติดต่อผ่านทางเครือข่ายจากนอกสำนักงานต้องได้รับการป้องกันการถูกลักลอบดูข้อมูล เป็นต้น

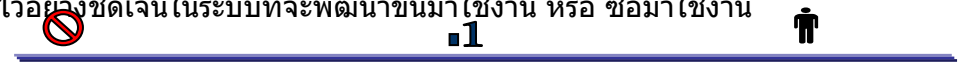
8. การพัฒนาและดูแลระบบสารสนเทศ (Systems development and maintenance)

8.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of systems)

มีจุดประสงค์เพื่อการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ

ข้อที่ 105 การกำหนดความต้องการด้านความมั่นคงปลอดภัย (Security requirements analysis and specification)

(หัวหน้างานสารสนเทศ) ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือ ซื้อมาใช้งาน



8.2 ความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security in application system)

มีจุดประสงค์เพื่อป้องกันการสูญหาย หรือ การเปลี่ยนแปลงแก้ไขข้อมูลในระบบสารสนเทศ รวมทั้งการนำข้อมูลในระบบสารสนเทศไปใช้ในทางที่ไม่เหมาะสม

ข้อที่ 106 การวิเคราะห์ความเสี่ยงที่ทำให้ข้อมูลเสียหาย (Areas of risk)

(หัวหน้างานสารสนเทศ) ต้องทำการวิเคราะห์ว่ามีความเสี่ยงใดบ้างที่อาจทำให้ข้อมูลเกิดความเสียหาย

ข้อที่ 107 วิธีการตรวจสอบข้อมูลนำเข้า (Checks and controls)

(ผู้ดูแลระบบ) ต้องมีวิธีการตรวจสอบข้อมูลนำเข้าระบบสารสนเทศว่าข้อมูลที่ได้รับเกิดความเสียหายหรือไม่

ข้อที่ 108 การพิสูจน์ข้อความ (Message authentication)

(ผู้ดูแลระบบ) ต้องมีวิธีการในการตรวจสอบว่า ข้อความที่ส่งมาทางอิเล็กทรอนิกส์ เช่น ไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น ถูกเปลี่ยนแปลงแก้ไขหรือไม่ หรือเกิดความเสียหายระหว่างที่ส่งมาหรือไม่

ข้อที่ 109 การตรวจสอบข้อมูลนำเข้า (Input data validation)

(ผู้ดูแลระบบ) ต้องตรวจสอบข้อมูลนำเข้าระบบสารสนเทศ ได้แก่ ตรวจสอบช่วงของค่าตัวเลขที่ใส่เข้ามา ตรวจสอบแต่ละตัวอักษรที่ใส่เข้ามา ตรวจสอบว่าข้อมูลใส่เข้ามาครบทุกฟิลด์ เป็นต้น

ข้อที่ 110 การตรวจสอบข้อมูลนำออก (Output data validation)

(ผู้ดูแลระบบ) ต้องตรวจสอบข้อมูลนำออกของระบบว่ามีความถูกต้องและเหมาะสมต่อการนำไปใช้งาน นอกจากนี้ ต้องมีกระบวนการบันทึก พิสูจน์ และรับรองข้อมูลนั้นๆด้วย

8.3 การใช้การเข้ารหัสกับสารสนเทศ (Cryptographic controls)

มีจุดประสงค์เพื่อรักษาความลับและความสมบูรณ์ของสารสนเทศที่ใช้งาน

ข้อที่ 111 การลงลายมือชื่ออิเล็กทรอนิกส์ (Digital signatures)

(พนักงาน) ต้องมีการลงลายมือชื่ออิเล็กทรอนิกส์กับเอกสารอิเล็กทรอนิกส์ที่ต้องการการยืนยันว่าใครเป็นผู้ลงนาม และเพื่อเป็นการป้องกันการเปลี่ยนแปลงแก้ไขเอกสารอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

ข้อที่ 112 การตรวจสอบเหตุการณ์ที่เกิดขึ้นแล้ว (Non-repudiation services)

(ผู้ดูแลระบบ) ต้องมีกลไกเพื่อใช้ในการตรวจสอบว่าเหตุการณ์หนึ่งที่เกิดขึ้นโดยผู้ใช้ได้เกิดขึ้นแล้ว ทั้งนี้เพื่อป้องกันการปฏิเสธความรับผิดชอบ

ข้อที่ 113 นโยบายการใช้งานการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีนโยบายการใช้งานการเข้ารหัสข้อมูล

ข้อที่ 114 การเข้ารหัสข้อมูล (Encryption)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการใช้วิธีการทางเทคนิคเพื่อทำการเข้ารหัสข้อมูลที่มีความสำคัญสูง

ข้อที่ 115 การป้องกันกุญแจที่ใช้ในการเข้ารหัส (Protection of cryptographic keys)

(พนักงาน ผู้ดูแลระบบ) ต้องมีวิธีการในการป้องกันกุญแจเข้ารหัสทั้งกุญแจส่วนตัว (private key) และกุญแจสาธารณะ (public key) รวมทั้งกุญแจลับ (secret key) ด้วยเพื่อไม่ให้กุญแจถูกเปิดเผยออกไปหรือสูญหาย

ข้อที่ 116 มาตรฐาน กระบวนการ และวิธีการในการเข้ารหัส (Standards, procedures and methods)

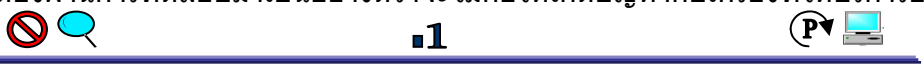
(ผู้ดูแลระบบ) ต้องมีกระบวนการในการบริหารจัดการกุญแจเข้ารหัส ได้แก่ การสร้างกุญแจ การสร้างใบรับรองอิเล็กทรอนิกส์ การส่งมอบกุญแจไปยังผู้รับการจัดเก็บกุญแจ การเปลี่ยนกุญแจ การยกเลิกกุญแจ การจัดการกับกุญแจที่ถูกเปิดเผยออกไป เป็นต้น

8.4 ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ (Security of system files)

มีจุดประสงค์เพื่อให้โครงการสารสนเทศได้รับการดำเนินการอย่างปลอดภัย

ข้อที่ 117 การควบคุมการติดตั้งซอฟต์แวร์ (Control of operational software)

(ผู้ดูแลระบบ) ต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบรารี่ ซอฟต์แวร์อุดช่องโหว่ลงไปยังเครื่องที่ใช้งานหรือเครื่องให้บริการ ทั้งนี้ ก่อนการติดตั้งต้องผ่านการทดสอบมาเป็นอย่างดีว่าจะไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่นั้น



ข้อที่ 118 การป้องกันข้อมูลจริงที่ใช้ในการทดสอบระบบ (Protection of system test data)

(หัวหน้างานสารสนเทศ) ต้องควบคุมการนำข้อมูลที่ใช้งานจริง (ในระบบที่ให้บริการอยู่) ไปใช้กับระบบที่อยู่ในระหว่างการทดสอบ ได้แก่ ข้อมูลจริงนั้นต้องได้รับการอนุมัติแล้วจึงจะนำไปใช้ได้ เมื่อใช้เสร็จแล้วต้องลบข้อมูลจริงนั้นออกจากระบบทดสอบทันที และต้องจัดทำบันทึกไว้เป็นหลักฐานว่าได้มีการนำข้อมูลจริงไปใช้ทดสอบอะไรบ้าง

ข้อที่ 119 การควบคุมการใช้งานซอฟต์แวร์ไลบรารี (Access control to program source library)

(ผู้ดูแลระบบ) ต้องจัดให้มีการควบคุมการใช้งานไลบรารีซึ่งประกอบด้วยซอร์สโค้ดของระบบที่ใช้งานจริงหรือให้บริการ เช่น

- ไม่ควรเก็บซอร์สโค้ดไว้ในเครื่องที่ใช้งานจริง
- ต้องแต่งตั้งผู้ที่มีอำนาจในการดูแลและปรับปรุงไลบรารี
- ต้องไม่เก็บซอร์สโค้ดที่อยู่ในระหว่างทำการทดสอบรวมไว้กับไลบรารีที่ใช้งานได้จริงแล้ว
- ต้องเก็บซอร์สโค้ดไว้ในที่ที่ปลอดภัย



8.5 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in development and support processes)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศรวมทั้งสารสนเทศในระบบด้วย·

ข้อที่ 120 กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (Change control procedures)

(ผู้ดูแลระบบ) ต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริงหรือให้บริการอยู่แล้ว เช่น

- คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ
- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
- ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
- ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

ข้อที่ 121 การตรวจสอบซอฟต์แวร์ที่จัดหามาใช้งาน (Covert channels and Trojan code)

(ผู้ดูแลระบบ) ต้องตรวจสอบซอฟต์แวร์ที่จัดหามาใช้งานก่อนติดตั้งเพื่อใช้งานจริง ทั้งนี้เพื่อป้องกันซอร์สโค้ดไม่ประสงค์ดีที่แฝงมากับซอฟต์แวร์นั้น

ข้อที่ 122 การควบคุมการว่าจ้างการพัฒนาระบบ (Outsourced software development)

(หัวหน้างานสารสนเทศ) ต้องมีการทำสัญญาว่าจ้างการพัฒนาระบบซึ่งต้องครอบคลุมถึงข้อตกลงทางด้านลิขสิทธิ์การใช้งานระบบ การตรวจสอบระบบโดยละเอียดก่อนติดตั้งเพื่อใช้งานจริง การรับรองคุณภาพของระบบ เป็นต้น

ข้อที่ 123 การตรวจสอบระบบสารสนเทศทั้งหมดที่เกี่ยวข้อง (Technical review of operating system changes)

(หัวหน้างานสารสนเทศ) ต้องตรวจสอบระบบสารสนเทศที่เกี่ยวข้องภายหลังจากที่ได้ทำการติดตั้งระบบปฏิบัติการใหม่หรือหลังจากที่ได้มีการปรับปรุงระบบปฏิบัติการของเครื่องที่มีระบบสารสนเทศนั้น ทั้งนี้เพื่อป้องกันปัญหาข้างเคียงที่อาจเกิดขึ้นได้

ข้อที่ 124 การควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ (Restrictions on changes to software packages)

(ผู้ดูแลระบบ) ต้องจัดให้มีการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจที่จัดซื้อมาจากผู้ขาย เช่น

- หลีกเลี่ยงการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ
- หากหลีกเลี่ยงไม่ได้ต้องขออนุญาตจากผู้ขายก่อนเปลี่ยนแปลง แก้ไขหรือขอให้ผู้ขายทำการเปลี่ยนแปลงให้
- ต้องเก็บซอฟต์แวร์ต้นฉบับไว้อีกชุดหนึ่ง
- การเปลี่ยนแปลงแก้ไขนั้นต้องได้รับการตรวจสอบเป็นอย่างดี เป็นต้น

9. การบริหารความต่อเนื่องของการดำเนินงานขององค์กร (Business continuity management)

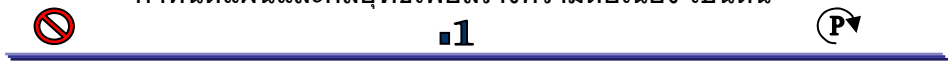
9.1 การบริหารความต่อเนื่องให้กับการดำเนินงานขององค์กร (Aspects of business continuity)

มีจุดประสงค์เพื่อป้องกันการหยุดชะงักในการดำเนินงานขององค์กรที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ·

ข้อที่ 125 กระบวนการในการสร้างความต่อเนื่อง (Business continuity management process)

(ผู้บริหารสารสนเทศ) ต้องมีกระบวนการในการบริหารและจัดการเพื่อให้การดำเนินงานขององค์กรเป็นไปได้อย่างต่อเนื่อง โดยมีองค์ประกอบสำคัญ เช่น

- ศึกษาความเสี่ยงที่เป็นไปได้ที่อาจทำให้การดำเนินงานหยุดชะงัก
- ศึกษาผลกระทบจากการหยุดชะงัก
- กำหนดแผนและกลยุทธ์เพื่อสร้างความต่อเนื่อง เป็นต้น



ข้อที่ 126 การวิเคราะห์ความเสี่ยงสำหรับการบริหารความต่อเนื่อง (Business continuity and impact analysis)

(ผู้บริหารสารสนเทศ) ต้องจัดให้มีการวิเคราะห์ความเสี่ยงสำหรับการบริหารความต่อเนื่องเพื่อป้องกันการหยุดชะงักในการดำเนินงาน

ข้อที่ 127 การจัดทำแผนสร้างความต่อเนื่องในการดำเนินงาน (Writing and implementing continuity plans)

(ผู้บริหารสารสนเทศ) ต้องจัดทำแผนและปฏิบัติตามแผน เพื่อสร้างความต่อเนื่องในการดำเนินงานขององค์กร

ข้อที่ 128 การกำหนดขอบเขตของแผนสร้างความต่อเนื่อง (Business continuity planning framework)

(ผู้บริหารสารสนเทศ) ต้องจัดทำแผนการสร้างความต่อเนื่องโดยมีองค์ประกอบดังนี้

- การระบุถึงเหตุการณ์ที่เกิดขึ้นที่ทำให้ต้องนำแผนมาใช้งาน
- วิธีปฏิบัติเมื่อมีเหตุการณ์ดังกล่าวเกิดขึ้น
- วิธีปฏิบัติเพื่อโยกย้ายกิจกรรมขององค์กรไปยังสถานที่ชั่วคราว
- วิธีปฏิบัติในการนำกลับสู่สภาวะปกติ
- มีกำหนดการในการตรวจสอบแผนเพื่อดูความพร้อมของแผน
- การให้ความรู้และสร้างความตระหนักแก่บุคคลที่เกี่ยวข้อง
- การกำหนดหน้าที่ความรับผิดชอบเมื่อมีเหตุการณ์เกิดขึ้น
- การกำหนดช่องทางการติดต่อเมื่อมีเหตุการณ์เกิดขึ้น



ข้อที่ 129 การทดสอบแผนสร้างความต่อเนื่อง (Testing the plans)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการทดสอบแผนสร้างความต่อเนื่องในการดำเนินงานขององค์กรตามระยะเวลาที่กำหนดไว้



ข้อที่ 130 การประเมินและปรับปรุงแผนสร้างความต่อเนื่อง (Maintaining and re-assessing the plans)

(ผู้บริหารสารสนเทศ) ต้องจัดให้มีการประเมินและปรับปรุงแก้ไขแผนสร้างความต่อเนื่องตามระยะเวลาที่กำหนดไว้ เพื่อให้สามารถรองรับความเสี่ยงใหม่ๆ ที่อาจเกิดขึ้นได้



10. การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร (Compliance)

10.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย (Compliance with legal requirements)

ข้อที่ 131 การระบุข้อกำหนดในการใช้งานระบบสารสนเทศ (Identification of applicable legislation)

(หัวหน้างานสารสนเทศ หัวหน้างานบุคคล หัวหน้างานนิติการ) ต้องร่วมกันระบุข้อกำหนดทางด้านกฎ ระเบียบ ข้อบังคับบทลงโทษ หรือสัญญา ที่ต้องปฏิบัติตามในการใช้ระบบสารสนเทศหนึ่งๆ ขององค์กร

ข้อที่ 132 ลิขสิทธิ์ (Copyright)

(พนักงาน) ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ในการใช้งานทรัพย์สินทางปัญญาที่องค์กรจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

ข้อที่ 133 ซอฟต์แวร์ลิขสิทธิ์ (Software copyright)

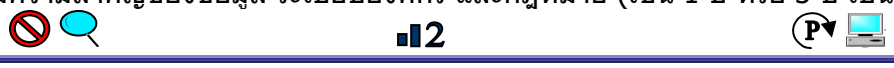
(พนักงาน) ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย ได้แก่ การลงทะเบียนเพื่อใช้งานซอฟต์แวร์ต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ ตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้องหรือไม่

ข้อที่ 134 การป้องกันข้อมูลส่วนตัวของพนักงาน (Data protection and privacy of personal information)

(ผู้ดูแลระบบ) ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัวของพนักงาน เช่น ข้อมูลในไปรษณีย์อิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล เป็นต้น

ข้อที่ 135 การเก็บและการป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงการปฏิบัติตามข้อกำหนด (Safeguarding of organizational records)

(หัวหน้างานสารสนเทศ) ต้องจัดเก็บข้อมูล เพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับ ที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบองค์กร และกฎหมาย (เช่น 1 ปี หรือ 3 ปี เป็นต้น)



ข้อที่ 136 การป้องกันการใช้ระบบสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities)

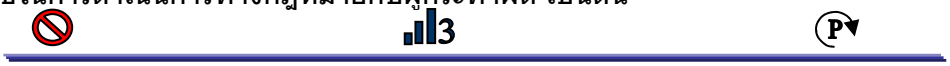
(ผู้ดูแลระบบ) ต้องทำการเฝ้าดูการใช้งานระบบสารสนเทศโดยพนักงาน เพื่อให้ใช้งานตามวัตถุประสงค์ขององค์กรและป้องกันไม่ให้ใช้งานนอกเหนือจากสิทธิที่ตนได้รับ รวมทั้งต้องดำเนินการทางวินัยหากตรวจพบการกระทำที่ละเมิดกฎระเบียบ

ข้อที่ 137 การศึกษาและปฏิบัติตามข้อกำหนดในการเข้ารหัสข้อมูลของประเทศ (Regulation of cryptographic controls)

(ผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ) ต้องทำการศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายของประเทศเกี่ยวกับการเข้ารหัสข้อมูล รวมทั้งเมื่อจำเป็นต้องโยกย้ายสารสนเทศที่เข้ารหัสไว้ หรืออุปกรณ์ หรือเครื่องมือ หรือระบบที่ใช้ในการเข้ารหัสข้อมูล ไปยังอีกประเทศหนึ่ง ให้ทำการศึกษาและปฏิบัติตาข้อกำหนดหรือกฎหมายของประเทศนั้นด้วย

ข้อที่ 138 กฎเกณฑ์ที่เกี่ยวข้องกับการเก็บหลักฐานอ้างอิง (Rules for evidence)

(หัวหน้างานสารสนเทศ หัวหน้างานนิติการ) ต้องศึกษากฎเกณฑ์ที่เกี่ยวข้อง เช่น ถ้อยแถลงในกฎหมายแพ่งหรืออาญา ซึ่งระบุถึงลักษณะของหลักฐานที่ต้องเก็บรวบรวมมาเพื่อใช้ในการดำเนินการทางกฎหมายกับผู้กระทำผิด เป็นต้น



ข้อที่ 139 หลักฐานที่ศาลยอมรับ (Admissibility of evidence)

(หัวหน้างานสารสนเทศ) ต้องศึกษาว่าหลักฐานนั้นสามารถนำไปใช้ในกระบวนการของศาลได้หรือไม่

ข้อที่ 140 คุณภาพและความสมบูรณ์ของหลักฐาน (Quality and completeness of evidence)

(หัวหน้างานสารสนเทศ) ต้องศึกษาว่าลักษณะของหลักฐานที่สมบูรณ์และมีคุณภาพเป็นอย่างไร

10.2 การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยและรายละเอียดทางเทคนิค (Reviews of security policy and technical compliance)

ข้อที่ 141 การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยขององค์กร (Compliance with security policy)

(ผู้ดูแลระบบ) ต้องทำการตรวจสอบระบบทั้งหมดขององค์กรตามระยะเวลาที่กำหนดไว้ว่าเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กรหรือไม่

ข้อที่ 142 การตรวจสอบรายละเอียดทางเทคนิค (Technical compliance checking)

(ผู้ดูแลระบบ) ต้องทำการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งานหรือให้บริการอยู่แล้วตามระยะเวลาที่กำหนดไว้ว่ามีความมั่นคงปลอดภัยอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (scan) และทดสอบการโจมตี ระบบ (penetration test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย เป็นต้น

10.3 การพิจารณาการตรวจสอบระบบ (System audit considerations)

มีจุดประสงค์เพื่อทำให้กระบวนการตรวจสอบระบบทั้งหมดมีผลกระทบน้อยที่สุดต่อการดำเนินงานขององค์กร

ข้อที่ 143 การวางแผนการตรวจสอบระบบทั้งหมด (System audit controls)

(หัวหน้างานสารสนเทศ) ต้องวางแผนการตรวจสอบระบบทั้งหมด โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบ และกระบวนการดำเนินงานขององค์กรน้อยที่สุด

ข้อที่ 144 การป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ (Protection of system audit tools)

(ผู้ดูแลระบบ) ต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการตรวจสอบระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด หรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น

วิธีการบริหารจัดการรหัสผ่านของพนักงานให้มีความมั่นคงปลอดภัย

กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่ ไม่จดหรือบันทึรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น) ต้องให้พนักงานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ กำหนดรหัสผ่านเริ่มต้นให้กับพนักงานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับพนักงานต้องเป็นไปอย่างปลอดภัย

ตัวอย่างระเบียบการใช้งานเครือข่าย

ตัวอย่างระเบียบ
ว่าด้วยการใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กรอย่างปลอดภัย

ด้วย(หน่วยงาน / บริษัท / ห้าง / ร้าน).....
ได้จัดให้มีเครือข่ายคอมพิวเตอร์ขึ้น เพื่ออำนวยความสะดวกแก่พนักงานในการปฏิบัติงานให้แก่องค์กร ดังนั้นเพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง เห็นสมควรวางระเบียบไว้ดังต่อไปนี้

บทที่ 1 คำนิยาม

"องค์กร" หมายความว่า ชื่อ (หน่วยงาน / บริษัท / ห้าง / ร้าน) .....
.....

"เครือข่ายคอมพิวเตอร์" หมายความถึง เครือข่ายคอมพิวเตอร์ขององค์กร .....
.....

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างขององค์กร / บริษัท / ห้าง / ร้าน.....

"พนักงาน" หมายความว่า พนักงานและลูกจ้างขององค์กร / บริษัท / ห้าง / ร้าน รวมถึงบุคคลอื่นที่องค์กรมอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลงหรือใบสั่งซื้อ

"ข้อมูล" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใดๆไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"ผู้ดูแลเครือข่ายคอมพิวเตอร์" หมายความถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

บทที่ 2 กำหนดอำนาจหน้าที่ของคณะกรรมการหรือผู้ดูแลความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ให้มี "คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์" ที่ผู้บังคับบัญชาแต่งตั้งจากพนักงานขององค์กร โดยคณะอนุกรรมการฯความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์มีอำนาจหน้าที่ดังต่อไปนี้

1) กำกับดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติงานของผู้ดูแลเครือข่ายคอมพิวเตอร์ในการปฏิบัติตามระเบียบนี้

2) ให้คำปรึกษาแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์เกี่ยวกับการปฏิบัติตามระเบียบนี้

3) ให้คำแนะนำและคำเสนอแนะต่อผู้บังคับบัญชาในการกำหนดนโยบายและมาตรการเกี่ยวกับการรักษาความปลอดภัยของข้อมูล

4) จัดทำรายงานเกี่ยวกับการปฏิบัติตามระเบียบนี้เสนอผู้บังคับบัญชาเป็นครั้งคราวตามความเหมาะสม

5) ปฏิบัติหน้าที่อื่นตามที่กำหนดไว้ในระเบียบนี้

6) ดำเนินการเรื่องอื่นตามที่ผู้บังคับบัญชามอบหมาย

บทที่ 3 ข้อปฏิบัติของพนักงานในการใช้งานเครือข่ายคอมพิวเตอร์

ข้อ 1 พนักงานมีสิทธิใช้เครือข่ายคอมพิวเตอร์ได้ภายใต้ข้อกำหนดแห่งระเบียบนี้ การฝ่าฝืนข้อกำหนดดังกล่าวในวรรคหนึ่ง และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่พนักงานที่ฝ่าฝืนตามความเหมาะสมต่อไป

ข้อ 2 พนักงานพึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ download ไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงานซึ่งมีการใช้เครือข่ายอย่างหนาแน่น

ข้อ 3 พนักงานพึงใช้ข้อความสุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้เครือข่ายอาทิ เช่น ไม่ใช้การส่ง mail แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น หรือการใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น เป็นต้น

ข้อ 4 พนักงานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่ายโดยเฉพาะอย่างยิ่งไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง

ข้อ 5 เพื่อประโยชน์ในการใช้รหัสผ่านส่วนบุคคล พนักงานจะต้องใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่พนักงานครอบครองใช้งานอยู่ ทั้งในระดับ BIOS และระดับระบบปฏิบัติการ (Operating System) โดยรหัสผ่านส่วนบุคคลดังกล่าวต้องมีความยาวไม่น้อยกว่า 6 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์ และไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

ข้อ 6 พนักงานจะต้องไม่ใช้เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ดังต่อไปนี้

1) เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
2) เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
3) เพื่อการพาณิชย์
4) เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กร หรือขององค์กร หรือบุคคลภายนอกก็ตาม
5) เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือของบุคคลอื่น

6) เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

7) เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่องค์กร เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังพนักงานหรือบุคคลอื่น เป็นต้น

8) เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ขององค์กร หรือของพนักงานอื่นขององค์กร หรือเพื่อให้เครือข่ายคอมพิวเตอร์ขององค์กร ไม่สามารถใช้งานได้ตามปกติ

9) เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กร ไปยังที่อยู่เว็บ (web site) ใด ๆ ในลักษณะที่จะก่อ หรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

10) เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่องค์กร

ข้อ 7 เพื่อความปลอดภัยในการใช้เครือข่ายคอมพิวเตอร์โดยส่วนรวมพนักงานจะต้อง

1) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

2) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาก่อน

3) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้นหรือเครือข่ายคอมพิวเตอร์ขององค์กร ได้

4) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องบริการ (server) ที่ต้องใช้งานตลอด 24 ชั่วโมง

5) ตรวจสอบข้อมูลที่ได้รับจากภายนอกองค์กร ทุกครั้งด้วยโปรแกรมคอมพิวเตอร์สำหรับตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ที่องค์กร จัดให้ และหากตรวจพบไวรัสคอมพิวเตอร์ฝังตัวอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์หรือข้อมูลนั้นโดยเร็วที่สุด

6) ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตนเพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

7) ใช้โปรแกรมคอมพิวเตอร์ที่มีการเข้ารหัสข้อมูลซึ่งองค์กร จัดให้สำหรับใช้ในการติดต่อกับเครือข่ายคอมพิวเตอร์จากภายนอกสถานที่ทำการขององค์กร

8) ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือคณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลของพนักงานและเครือข่ายคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์

หรือคณะกรรมการดังกล่าวด้วย

9) ระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์เหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์ แล้วแต่กรณี

10) ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ก่อนได้รับอนุญาต

11) คืนทรัพย์สินอันเกี่ยวข้องกับการใช้งานเครือข่ายคอมพิวเตอร์ที่เป็นขององค์กร เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้าหรือออก ฯลฯ ให้แก่องค์กร รวมทั้งขอรับข้อมูลส่วนบุคคลที่อยู่บนเครือข่ายคอมพิวเตอร์คืนจากองค์กร ภายในกำหนด 7 วัน นับแต่วันพ้นสภาพการเป็นพนักงาน

บทที่ 4 ข้อปฏิบัติของผู้ดูแลเครือข่ายคอมพิวเตอร์

ข้อ 1 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องดูแลรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งจะต้องสอดส่องดูแลการใช้เครือข่ายคอมพิวเตอร์ของพนักงานเพื่อให้เป็นไปตามระเบียบนี้

หากผู้ดูแลเครือข่ายคอมพิวเตอร์พบว่าพนักงานผู้ใดมีพฤติการณ์ส่อไปในทางที่จะละเมิดข้อกำหนดการใช้เครือข่ายคอมพิวเตอร์แห่งระเบียบนี้ ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องรายงานให้คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปทราบโดยเร็วที่สุด และในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นแก่องค์กร ผู้ดูแลเครือข่ายคอมพิวเตอร์มีอำนาจในการระงับการใช้งานเครือข่ายคอมพิวเตอร์ของพนักงานดังกล่าวได้ทันที

ข้อ 2 ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการเสนอความเห็นและข้อสังเกตต่อคณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปเพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหาเครือข่ายคอมพิวเตอร์ หรือปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ตามที่ผู้บังคับบัญชามอบหมาย

ข้อ 3 ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัสข้อมูลอัตโนมัติหรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

ข้อ 4 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และจะต้อง

ไม่เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

ข้อ 5 เมื่อผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นขององค์กร เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ให้แก่องค์กร ในทันทีที่พ้นหน้าที่ และให้คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ดำเนินการตรวจสอบการคืนทรัพย์สินของผู้ดูแลเครือข่ายคอมพิวเตอร์ที่พ้นจากหน้าที่โดยละเอียดเพื่อความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

ข้อ 6 ผู้ดูแลเครือข่ายคอมพิวเตอร์ที่ฝ่าฝืนข้อกำหนดในระเบียบนี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กร จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์นั้นตามความเหมาะสมต่อไป

คำนิยามตำแหน่งงาน

"พนักงาน" หมายความว่า พนักงานและลูกจ้างที่ปฏิบัติงานตามหน้าที่ความรับผิดชอบภายในองค์กร

"ผู้บริหารองค์กร" หมายความว่า พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับการดำเนินการทั้งหมดขององค์กร

"ผู้บริหารสารสนเทศ" หมายความว่า พนักงานระดับสูงขององค์กรที่มีหน้าที่บริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในองค์กร

"ผู้ดูแลระบบ" หมายความว่า พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์ และสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

"หัวหน้างานสารสนเทศ" หมายความว่า พนักงานที่มีหน้าที่ควบคุมดูแลการทำงานของผู้ดูแลระบบ พร้อมทั้งมีอำนาจสั่งการผู้ดูแลระบบเครือข่ายและสารสนเทศขององค์กร และรายงานต่อผู้บริหารสารสนเทศ

"หัวหน้างานบุคคล" หมายความว่า พนักงานที่มีหน้าที่ควบคุมดูแลการวางแผนทรัพยากรบุคคลทั้งคุณภาพ ปริมาณ และสัดส่วนให้มีความเหมาะสมกับภารกิจและแผนกลยุทธ์ของหน่วยงานระดับต่างๆ ทั้งในระยะสั้นและระยะยาว รวมถึงบริหารทรัพยากรบุคคลตามระเบียบ/หลักเกณฑ์ของสำนักงาน

"หัวหน้างานอาคาร" หมายความว่า พนักงานที่มีหน้าที่ควบคุมดูแลและบริหารจัดการระบบสาธารณูปโภคต่างๆ และทรัพยากรสิ่งอำนวยความสะดวกภายในอาคาร รวมถึงดูแลความเป็นระเบียบเรียบร้อยและการรักษาความปลอดภัยของสำนักงาน

"หน่วยงานภายนอก" หมายความว่า องค์กรอื่นๆ ที่เกี่ยวข้อง เช่น บริษัทขายฮาร์ดแวร์หรือซอฟต์แวร์ บริษัทให้คำปรึกษาเกี่ยวกับระบบสาสนเทศ เป็นต้น

"หัวหน้างานนิติการ" หมายความว่า พนักงานที่มีหน้าที่ให้ความคิดเห็นหรือตีความเกี่ยวกับระเบียบ ข้อกำหนด กฎเกณฑ์ ข้อบังคับ กฎหมาย พระราชบัญญัติ กฤษฎีกา หรือข้อความในเชิงระเบียบข้อบังคับอื่นๆ รวมทั้งจัดทำระเบียบ ข้อกำหนด กฎเกณฑ์ ข้อบังคับหรือคำสั่ง สำหรับใช้ในองค์กร

เกณฑ์การกำหนดระดับความเสี่ยง

ระดับความมั่นคงปลอดภัย	ประเภทของมาตรการป้องกัน				มาตรการป้องกันนั้นเกี่ยวข้องกับ			
	Preventive	Detective	Corrective	รวม	People	Process	Process	รวม
ระดับ 1	49	15	1	65	14	**51**	19	84
ระดับ 2	48	27	3	78	11	**53**	24	88
ระดับ 3	38	20	3	61	9	**40**	23	72
รวม	135	62	7		34	**144**	66	

ระดับ 1 หมายถึง ระดับความมั่นคงปลอดภัยพื้นฐาน มีจำนวน 51 ข้อ
ระดับ 2 หมายถึง ระดับความมั่นคงปลอดภัยขั้นกลาง มีจำนวน 104 ข้อ
ระดับ 3 หมายถึง ระดับความมั่นคงปลอดภัยขั้นสูง มีจำนวน 144 ข้อ

อธิบายเพิ่มเติมเกณฑ์การกำหนดระดับความเสี่ยง

ระดับ 1 หมายถึง ระดับความมั่นคงปลอดภัยพื้นฐาน มีจำนวน 51 ข้อ
(นับจากจำนวนข้อที่กำกับด้วยหมายเลข 1 มีจำนวนข้อทั้งสิ้น 51 ข้อ)

ระดับ 2 หมายถึง ระดับความมั่นคงปลอดภัยขั้นกลาง มีจำนวน 104 ข้อ
(นับจากจำนวนข้อที่กำกับด้วยหมายเลข 2 มีจำนวนข้อทั้งสิ้น 53 ข้อ และนับรวมกับระดับความปลอดภัยพื้นฐานซึ่งต้องดำเนินการมาก่อน รวมเป็น 51+53 = 104 ข้อ)

ระดับ 3 หมายถึง ระดับความมั่นคงปลอดภัยขั้นสูง มีจำนวน 144 ข้อ
(นับจากจำนวนข้อที่กำกับด้วยหมายเลข 3 มีจำนวนข้อทั้งสิ้น 40 ข้อ และนับรวมกับระดับความปลอดภัยพื้นฐานซึ่งต้องดำเนินการมาก่อน รวมเป็น 51+53+40 = 144 ข้อ)

1) ความเสี่ยงที่มีต่อองค์ประกอบความปลอดภัยหนึ่งมีระดับต่ำ

ควรมีการดำเนินการรักษาความมั่นคงปลอดภัยขั้นพื้นฐาน ระดับที่ 1 ถ้าการสูญเสียองค์ประกอบทางด้านความปลอดภัยนั้นจะก่อให้เกิดผลกระทบกับองค์กรในวงจำกัดโดยมีผลต่อการดำเนินงาน ทรัพย์สิน บุคลากรและชื่อเสียงขององค์กร ได้แก่

- *องค์กรสามารถดำเนินงานพื้นฐานได้ แต่ประสิทธิภาพลดลงบ้างโดยประมาณไม่เกิน 20%*
- *องค์กรได้รับความเสียหายต่อทรัพย์สินเล็กน้อยโดยประมาณไม่เกิน 5%*
- *องค์กรเกิดการสูญเสียทางการเงินเล็กน้อยโดยประมาไม่เกิน 5%*
- *บุคลากรขององค์กรได้รับอันตรายกับสุขภาพกายและจิตเล็กน้อยโดยไม่ถึงขนาดเข้ารับการรักษาที่โรงพยาบาล*
- *องค์กรเสียชื่อเสียงในวงจำกัด*

2) ความเสี่ยงที่มีต่อองค์ประกอบความปลอดภัยหนึ่งมีระดับปานกลาง

ควรมีการดำเนินการรักษาความมั่นคงปลอดภัยขั้นกลาง (ระดับที่ 2) ถ้าการสูญเสียองค์ประกอบทางด้านความปลอดภัยนั้นจะก่อให้เกิดผลกระทบกับองค์กรในระดับค่อนข้างมากโดยมีผลต่อการดำเนินงาน ทรัพย์สิน บุคลากร และชื่อเสียงขององค์กร ได้แก่ *องค์กรสามารถดำเนินงานพื้นฐานได้ แต่ประสิทธิภาพลดลงอย่างเห็นได้ชัดโดยประมาณไม่เกิน 40%*

- *องค์กรได้รับความเสียหายต่อทรัพย์สินค่อนข้างมากโดยประมาณไม่เกิน 10%*
- *องค์กรเกิดการสูญเสียทางการเงินค่อนข้างมากโดยประมาณไม่เกิน 10% ของรายได้รวม*
- *บุคลากรขององค์กรได้รับอันตรายมากถึง ขั้นต้องเข้ารับการรักษาโรงพยาบาล แต่ไม่ถึงกับเสียชีวิตหรือบาดเจ็บอย่างร้ายแรง*
- *องค์กรเสียชื่อเสียงในวงการธุรกิจของตน*

3) ความเสี่ยงที่มีต่อองค์ประกอบความปลอดภัยหนึ่งมีระดับสูง

ควรมีการดำเนินการรักษาความมั่นคงปลอดภัยขั้นสูง (ระดับที่ 3) ถ้าการสูญเสียองค์ประกอบทางด้านความปลอดภัยนั้นจะก่อให้เกิดผลกระทบกับองค์กรในระดับร้ายแรงหรือหายนะโดยมีผลต่อการดำเนินงาน ทรัพย์สิน บุคลากร และชื่อเสียงขององค์กร ได้แก่

- *บางหน่วยหรือหลายๆ หน่วยงานขององค์กรไม่สามารถดำเนินงานพื้นฐานได้และประสิทธิภาพลดลงเป็นอย่างสูงเกิน 40%*
- *องค์กรได้รับความเสียหายต่อทรัพย์สินเกิน 10%*
- *องค์กรเกิดการสูญเสียทางการเงินเป็นอย่างสูงเกิน 10% ของรายได้รวม*

- *บุคลากรขององค์กรได้รับอันตรายสูงถึงขั้นเสียชีวิตหรือบาดเจ็บอย่างร้ายแรงมาก*
- *องค์กรเสียชื่อเสียงในวงกว้างขวาง เช่น ตกเป็นข่าวในหน้าหนังสือพิมพ์เป็นต้น*

หมายเหตุ ในหัวข้อทั้ง 5 ประการดังกล่าว หากองค์กรใดมีความเสี่ยงที่จะมีความเสียหายเข้าเกณฑ์ในระดับความปลอดภัย (ต่ำ, กลาง, สูง) ให้ถือเอาเกณฑ์นั้นเป็นระดับความเสี่ยงขององค์กรที่มีความจำเป็นจะต้องดำเนินการรักษาความมั่นคงปลอดภัยตามระดับดังกล่าว

แหล่งข้อมูลอ้างอิง : National Institute of Standard and Technology Special Publication 800-60 Version 2.0

ตัวอย่างองค์กรที่มีความคาบเกี่ยวกับโครงสร้างพื้นฐานที่สำคัญของประเทศไทยและควรจัดจัดทำมาตรฐานนี้ในระดับความมั่นคงปลอดภัยสูงสุด (ระดับ 3)

สำหรับองค์กรที่มีความเกี่ยวข้องกับโครงสร้างพื้นฐานของประเทศนั้นจัดว่าเป็นองค์กรที่มีความเสี่ยงสูง จึงต้องเร่งดำเนินการจนถึงระดับความมั่นคงปลอดภัยสูงสุดแต่เนื่องจากบางองค์กรอาจไม่ได้จัดสรรงบประมาณในส่วนนี้ไว้ จึงสามารถเริ่มต้นดำเนินงานเฉพาะบางส่วนของระบบทั้งหมดที่มีอยู่ให้เข้ามาตรฐานปลอดภัยสูงสุดก่อน การดำเนินการบางระบบ เช่น ระบบประมวลผลหลัก ระบบที่เกี่ยวข้องกับการเงิน เป็นต้น ตัวอย่างองค์กรเหล่านั้น ได้แก่

1. กลุ่มไฟฟ้าและพลังงาน ประกอบด้วย
   - การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย
   - การไฟฟ้านครหลวง
   - การไฟฟ้าส่วนภูมิภาค
   - บริษัท ปตท. จำกัด (มหาชน)
   - กรมพัฒนาและส่งเสริมพลังงาน
   - เป็นต้น

2 . กลุ่มการเงิน การธนาคารและการประกันภัย
- กระทรวงการคลัง
- ธนาคารแห่งประเทศไทย
- ตลาดหลักทรัพย์แห่งประเทศไทย
- สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
- กรมการประกันภัย
- สมาคมประกันชีวิตไทย
- สมาคมประกันวินาศภัย
- ธนาคาร
- บริษัทหลักทรัพย์ต่างๆ
- เป็นต้น

3. กลุ่มการสื่อสาร โทรคมนาคมและขนส่ง
- บริษัท การบินไทย (มหาชน) จำกัด
- บริษัท ทศท คอร์ปปอเรชั่น จำกัด (มหาชน)
- บริษัท กสท คอร์ปปอเรชั่น จำกัด (มหาชน)
- บริษัทวิทยุการบินแห่งประเทศไทย
- การท่าอากาศยานแห่งประเทศไทย
- การรถไฟแห่งประเทศไทย
- กรมการบินพาณิชย์
- การท่าเรือแห่งประเทศไทย
- กระทรวงคมมนาคม
- กรมอุตุนิยมวิทยา
- เป็นต้น

4. กลุ่มความสงบสุขของสังคม
- กระทรวงศึกษาธิการ
- กระทรวงสาธาณสุข
- กรุงเทพมหานคร
- กระทรวงกลาโหม
- สำนักงานตำรวจแห่งชาติ
- กระทรวงเกษตรและสหกรณ์
- การประปานครหลวง
- การประปาส่วนภูมิภาค
- เป็นต้น

คำสั่งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
ที่ ๕/๒๕๔๖
เรื่อง การแต่งตั้งคณะอนุกรรมการด้านความมั่นคง

เพื่อให้การดำเนินงานของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ อาศัยอำนาจตามความในมาตรา ๔๒ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ประธานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงแต่งตั้งคณะอนุกรรมการด้านความมั่นคง โดยมีองค์ประกอบและอำนาจหน้าที่ดังต่อไปนี้

๑. องค์ประกอบ

๑.๑	นายทวีศักดิ์ กออนันตกูล	ประธานอนุกรรมการ
๑.๒	พันเอกนาพิกอดิภัค แสงสนิท	อนุกรรมการ
๑.๓	รองศาสตราจารย์ยืน ภู่วรวรรณ	อนุกรรมการ
๑.๔	นายไพศาล คูตระกูล	อนุกรรมการ
๑.๕	นายสมญา พัฒนวรพันธุ์	อนุกรรมการ
๑.๖	นายยรรยง เต็งอำนวย	อนุกรรมการ
๑.๗	นายกำพล ศรธนะรัตน์	อนุกรรมการ
๑.๘	นายพิพัฒน์ เอี่ยมซีรางกูร	อนุกรรมการ
๑.๙	นายชัยยุทธ สันทนานุการณ์	อนุกรรมการ
๑.๑๐	พันตำรวจเอกญาณพล ยั่งยืน	อนุกรรมการ
๑.๑๑	นายธีระมานพ ฟักทองพรรณ	อนุกรรมการ
๑.๑๒	นายวิริยะ อุปัติศฤงค์	อนุกรรมการ
๑.๑๓	นายสมหมาย จารุดิลกกุล	อนุกรรมการ
๑.๑๔	นางสุรีรัตน์ ทิพย์ตำแย	อนุกรรมการ
๑.๑๕	นายปริญญา หอมเอนก	อนุกรรมการ
๑.๑๖	นางสุรางคณา วายุภาพ	อนุกรรมการ
๑.๑๗	ผู้แทนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (นายโกเมน พิบูลย์โรจน์)	อนุกรรมการและเลขานุการ

/๑.๑๘ ผู้แทน ...

๑.๑๘	ผู้แทนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (นายศิวรักษ์ ศิวโมกษธรรม)	ผู้ช่วยเลขานุการ
๑.๑๙	ผู้แทนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (นายปฏิวัติ อุ่นเรือน)	ผู้ช่วยเลขานุการ

๒. อำนาจหน้าที่

๒.๑ เสนอแนะนโยบายและมาตรการด้านความมั่นคงให้เกิดความเชื่อมั่นและปลอดภัยในการใช้ระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ของประเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์

๒.๒ ติดตาม วิเคราะห์ กลั่นกรอง และเผยแพร่ข้อมูลที่เกี่ยวกับความมั่นคงของธุรกรรมทางอิเล็กทรอนิกส์ให้แก่หน่วยงานภาครัฐ ภาคธุรกิจและประชาชน

๒.๓ สร้างความตื่นตัวเพื่อให้ภาคเอกชนหรือประชาชนตระหนักถึงความสำคัญของความมั่นคงในการใช้ระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ในการทำธุรกรรมทางอิเล็กทรอนิกส์

๒.๔ ดำเนินการหรือประสานงานกับหน่วยงานอื่นๆ ในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงที่เป็นประโยชน์ต่อการทำงานหรือการพัฒนาบุคลากรในด้านดังกล่าว

๒.๕ ร่วมมือหรือประสานงานในการดำเนินการตามข้อ ๒.๑ ถึงข้อ ๒.๔ กับต่างประเทศหรือองค์การระหว่างประเทศ

๒.๖ ปฏิบัติการอื่นใดตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๕ ธันวาคม ๒๕๔๖

(นายแพทย์สุรพงษ์ สืบวงศ์ลี)
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

สำเนา

ประกาศสำนักนายกรัฐมนตรี

เรื่อง การคัดเลือกกรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

โดยที่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ มีผลใช้บังคับตั้งแต่วันที่ ๔ เมษายน ๒๕๔๕ เป็นต้นไป

อาศัยอำนาจตามความในมาตรา ๓๖ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ คณะรัฐมนตรีจึงได้มีมติเมื่อวันที่ ๒๓ กันยายน ๒๕๔๖ ให้แต่งตั้งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ที่ได้คัดเลือกจากผู้ทรงคุณวุฒิที่คณะกรรมการสรรหากรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เสนอจำนวน ๖ ด้าน ๆ ละ ๒ คน รวมทั้งสิ้น ๑๒ คน ดังต่อไปนี้

๑) ด้านการเงิน

ภาครัฐ	นายสถาพร	ชินะจิตร
ภาคเอกชน	นายชาติศิริ	โสภณพนิช

๒) ด้านพาณิชย์อิเล็กทรอนิกส์

ภาครัฐ	นางเสาวณี	สุวรรณชีพ
ภาคเอกชน	นางสาววิลาวรรณ	วนดุรงค์วรรณ

๓) ด้านนิติศาสตร์

ภาครัฐ	นายคัมภีร์	แก้วเจริญ
ภาคเอกชน	นายชวลิต	อัตถศาสตร์

๔) ด้านวิทยาการคอมพิวเตอร์

ภาครัฐ	นายสหัส	ตรีทิพยบุตร
ภาคเอกชน	นายครรชิต	มาลัยวงศ์

๕) ด้านวิทยาศาสตร์หรือวิศวกรรมศาสตร์

ภาครัฐ	นางเจริญศรี	มิตรภานนท์
ภาคเอกชน	นายประยูร	เชี่ยววัฒนา

๖) ด้านสังคมศาสตร์

ภาครัฐ	นายอาณัติ	ลีมัคเดช
ภาคเอกชน	นายสุคนธ์	กาญจนหัตถกิจ

ทั้งนี้ ตั้งแต่วันที่ ๒๓ กันยายน พ.ศ. ๒๕๔๖ เป็นต้นไป

ประกาศ ณ วันที่ ๒๖ กันยายน พ.ศ. ๒๕๔๖

(นายสุวิทย์ คุณกิตติ)
รองนายกรัฐมนตรี ปฏิบัติราชการแทน
นายกรัฐมนตรี

สำเนาถูกต้อง

(จ่าเอกชัยพล ภู
เจ้าหน้าที่วิเคราะห์นโย

1

รายชื่อคณะอนุกรรมการด้านความมั่นคง
ภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

.....

1. นายทวีศักดิ์ กออนันตกูล ประธานอนุกรรมการ
   (ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
   และกรรมการและเลขานุการในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์)

2. พันเอกนาฬิกอติภัค แสงสนิท ที่ปรึกษาและอนุกรรมการ
   (ผู้ช่วยรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร)

3. รองศาสตราจารย์ยืน ภู่วรวรรณ อนุกรรมการ
   (ผู้อำนวยการสำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์)

4. นายสมญา พัฒนวรพันธุ์ อนุกรรมการ
   (หัวหน้ากลุ่มสืบสวนต่อต้านข่าวกรอง สำนักข่าวกรองแห่งชาติ)

5. นายกำพล ศรธนะรัตน์ อนุกรรมการ
   (ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ
   สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์)

6. นายยรรยง เต็งอำนวย อนุกรรมการ
   (อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์
   คณะวิศวกรรมศาตร์ จุฬาลงกรณ์มหาวิทยาลัย)

7. นายธีระมานพ ฟักทองพรรณ อนุกรรมการ
   (ผู้อำนวยการอาวุโส สายงานพัฒนาระบบเชิงกลยุทธ์
   ธนาคารเอเชีย)

8. นายไพศาล คูตระกูล อนุกรรมการ
(ผู้ช่วยกรรมการผู้จัดการ ฝ่ายงานปฏิบัติการและเทคโนโลยีสารสนเทศ
บริษัท หลักทรัพย์ บัวหลวงจำกัด)

9. นายพิพัฒน์ เอี่ยมชีรางกูร อนุกรรมการ
(ผู้จัดการฝ่ายธนาคารกรุงเทพ ธนาคารกรุงเทพ จำกัด (มหาชน))

10. นายชัยยุทธ สันทนานุการ อนุกรรมการ
(หัวหน้าที่ทำการศูนย์บริการอินเทอร์เน็ต
บริษัท กสท.โทรคมนาคม จำกัด (มหาชน))

11. นายวิริยะ อุปัติศฤงค์ อนุกรรมการ
(หัวหน้าคณะผู้บริหารด้านเทคนิค
บริษัท ทรู อินเทอร์เน็ต จำกัด)

12. พ.ต.อ.ญาณพล ยั่งยืน อนุกรรมการ
(ผู้บัญชาการสำนักคดีเทคโนโลยีและสารสนเทศ
กรมสอบสวนคดีพิเศษ)

13. นายสมหมาย จารุดิลกกุล อนุกรรมการ
(ผู้ชำนาญการประจำฝ่ายวางแผนเทคโนโลยีสารสนเทศ
บริษัท ปตท. จำกัด (มหาชน))

14. นางสุรีรัตน์ ทิพย์ตำแย อนุกรรมการ
(ผู้บริหารส่วนสำนักพัฒนาระบบการชำระเงิน สายระบบการชำระเงิน
ธนาคารแห่งประเทศไทย)

15. นายปริญญา หอมเอนก อนุกรรมการ
(ผู้อำนวยการศูนย์ฝึกอบรมระบบเครือข่ายและความปลอดภัยข้อมูล)

16. นางสุรางคณา วายุภาพ อนุกรรมการ
(หัวหน้าโครงการ: สำนักงานเลขานุการคณะกรรมการธุรกรรมทาง
อิเล็กทรอนิกส์ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ)

17. นายโกเมน พิบูลย์โรจน์ อนุกรรมการและเลขานุการ
(ผู้แทนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ)

18. นายศิวรักษ์ ศิวโมกษธรรม ผู้ช่วยเลขานุการ
(ผู้แทนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ)

19. นายบรรจง หะรังษี ผู้ช่วยเลขานุการ
(ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ)

20. น.ส.ดวงกมล ทรัพย์พิทยากร ผู้ช่วยเลขานุการ
(ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ)

21. นายปฏิวัติ อุ่นเรือน ผู้ช่วยเลขานุการ
(ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ)
