นโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ

(Information Security Policy)

กรมบัญชีกลาง

รายละเอียดการควบคุมเอกสาร

หมายเลขเอกสาร	PO-ISMS-001
ชื่อเอกสาร	นโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ (Information Security Policy)
เวอร์ชัน	2.0
วันที่ปรับปรุง	23 เมษายน 2563
วันที่บังคับใช้	25 ธันวาคม 2563

ประวัติการปรับปรุงเอกสาร

เวอร์ชัน	วันที่ปรับปรุง	รายละเอียด	ผู้รับผิดชอบ	วันที่บังคับใช้
1.0	-	เอกสารใหม่	นางสาวสุดจิตร ลาภเลิศสุข	24 มกราคม 2562
2.0	23 เมษายน 2563	ทบทวนกฎหมายที่เกี่ยวข้อง และเพิ่มหมวด 13 การตั้งค่าเครื่องตามนโยบาย, หมวด 14 การรักษาความมั่นคงปลอดภัยคุกคามทางไซเบอร์ (Cyber Security), หมวด 15 การรักษาความมั่นคงปลอดภัยคุ้มครองข้อมูลส่วนบุคคล (Privacy Security) และ	นางสาวสุดจิตร ลาภเลิศสุข	25 ธันวาคม 2563

เวอร์ชัน	วันที่ปรับปรุง	รายละเอียด	ผู้รับผิดชอบ	วันที่บังคับใช้
		หมวด 16 การยกเว้นการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ (Policy Deviation)		

การอนุมัติเอกสาร

ผู้รับผิดชอบ	ผู้สอบทาน	ผู้อนุมัติ
ลงชื่อ _____	ลงชื่อ _____	ลงชื่อ _____
(นางสาวสุดจิตร ลาภเลิศสุข)	(นายเกียรติณรงค์ วงศ์น้อย)	(นายภูมิศักดิ์ อรัญญาเกษมสุข)
ผู้อำนวยการ	ที่ปรึกษา	อธิบดีกรมบัญชีกลาง
ศูนย์เทคโนโลยีสารสนเทศ	ด้านพัฒนาระบบการเงินการคลัง	
และการสื่อสาร		
วันที่ 24 / ธ.ค. / 63	วันที่ 24 / ธ.ค. / 63	วันที่ 24 / ธ.ค. / 63

สารบัญ

หน้า

นโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมบัญชีกลาง

คำนิยาม

1) **“องค์กร”** หมายถึง กรมบัญชีกลาง
2) **“นโยบายฯ”** หมายความว่า นโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมบัญชีกลาง
3) **“ผู้บังคับบัญชา”** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของกรมบัญชีกลาง
4) **“ศูนย์เทคโนฯ”** หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร
5) **“หัวหน้ากลุ่มงาน”** หมายถึง หัวหน้ากลุ่มงานในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รับผิดชอบในการกำหนดนโยบาย การควบคุมกำกับดูแลการใช้งาน ระบบสารสนเทศและระบบเครือข่ายในแต่ละระบบงานที่ได้รับมอบหมาย
6) **“ห้องศูนย์คอมพิวเตอร์”** หมายถึง ห้องเดต้าเซ็นเตอร์ (Data Center)
7) **“การรักษาความมั่นคงปลอดภัย”** หมายถึง การควบคุมและกำกับดูแล กำหนดมาตรการ การใช้งานสารสนเทศ ระบบเทคโนโลยีสารสนเทศ และเครือข่ายการสื่อสาร ซึ่งเป็นไปตามนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ
8) **“ความมั่นคงปลอดภัยด้านสารสนเทศ”** หมายความว่า การป้องกันทรัพย์สินจากการเข้าถึง การเปิดเผย การขัดขวาง การเปลี่ยนแปลงแก้ไข ความเสียหาย การทำลาย หรือล่วงรู้โดยมิชอบ โดยมีความหมายรวมถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability)
9) **“มาตรฐาน”** (Standard) หมายถึง กรอบหรือบรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
10) **“ขั้นตอนการปฏิบัติ”** (Procedure) หมายถึง รายละเอียดขั้นตอนการปฏิบัติงาน เพื่อให้เป็นไปตามนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและเป็นไปตามมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
11) **“แนวทางปฏิบัติ”** (Guideline) หมายถึง แนวทางที่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายตามนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ

12) **"ผู้ใช้งาน"** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งกำหนดไว้ดังนี้
   - **ผู้บริหาร** หมายถึง เป็นผู้มีอำนาจสั่งการตามโครงสร้างการแบ่งส่วนราชการ
   - **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
   - **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว ขององค์กร
   - **บุคคลภายนอก** หมายถึง ผู้รับจ้าง เจ้าหน้าที่ของหน่วยงานภายนอกอื่น ๆ ทั้งที่เป็นหน่วยงานราชการและเอกชน
13) **"คณะกรรมการความมั่นคงปลอดภัยสารสนเทศ" (ISMS Committee)** หมายถึง คณะทำงานความมั่นคงปลอดภัยสารสนเทศ (IS Working Team)
14) **"คณะทำงานฯ"** หมายถึง คณะทำงานความมั่นคงปลอดภัยสารสนเทศ (IS Working Team)
15) **"หน่วยงานภายนอก"** หมายถึง องค์กรหรือหน่วยงานภายนอก (Outsource) ที่องค์กรอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูลคอมพิวเตอร์
16) **"ทรัพย์สิน"**หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
17) **"ข้อมูลคอมพิวเตอร์"** หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
18) **"สารสนเทศ (Information)"** หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดนโยบายฯ ให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
19) **"ระบบคอมพิวเตอร์"** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

20) **"ระบบเครือข่ายคอมพิวเตอร์ (Network System)"** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศและการสื่อสารต่าง ๆ ขององค์กรได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
    - **ระบบแลน (LAN)** และ**ระบบอินทราเน็ต (Intranet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
    - **ระบบอินเทอร์เน็ต (Internet)** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
21) **"ระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information Technology System)"** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
22) **"สิทธิ์ของผู้ใช้งาน"** หมายความว่า สิทธิ์ในการเข้าถึง สิทธิ์ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร
23) **"พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace)"** หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยแบ่งเป็น
    - พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
    - พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)
    - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบเครือข่าย (IT equipment or network area)
    - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
    - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN overage area)
24) **"เจ้าหน้าที่ข้อมูล"** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
25) **"จดหมายอิเล็กทรอนิกส์ (e-mail)"** หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความ ระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกันข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย

ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

26) **"รหัสผ่าน (password)"** หมายถึงตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศและการสื่อสาร

27) **"ชุดคำสั่งไม่พึงประสงค์"** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

28) **"หน่วยงาน"** หมายความถึง สำนัก (ทุกสำนัก) กอง (ทุกกอง) กลุ่มงาน (ทุกกลุ่ม) ศูนย์ (ทุกศูนย์)

29) **"หัวหน้าหน่วยงาน"** หมายความถึง ผู้อำนวยการสำนัก ผู้อำนวยการกอง หัวหน้ากลุ่มงาน ผู้อำนวยการศูนย์ และให้หมายความรวมถึงหัวหน้าหน่วยงานเฉพาะกิจที่องค์กรแต่งตั้ง

30) **"เหตุการณ์ด้านความมั่นคงปลอดภัย"** หมายความว่า สิ่งที่เกิดขึ้นกับระบบ การให้บริการหรือเครือข่ายซึ่งอาจละเมิดต่อมาตรการควบคุมหรือนโยบายความมั่นคงปลอดภัยด้านสารสนเทศหรือเป็นเหตุการณ์ที่มีความสัมพันธ์ต่อความมั่นคงปลอดภัยด้านสารสนเทศ

31) **"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด"** หมายความว่า เหตุการณ์หรือลำดับเหตุการณ์ที่ไม่พึงประสงค์หรือเหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศที่ไม่ได้คาดคิด ซึ่งมีความน่าจะเป็นอย่างมีนัยสำคัญที่จะเป็นภัยต่อความมั่นคงปลอดภัยด้านสารสนเทศและอาจสร้างความเสียหายต่อการดำเนินธุรกิจ

32) **"มาตรการควบคุมการเข้าถึง"** หมายความว่า การกำหนดสิทธิ การอนุญาต หรือการมอบอำนาจให้ผู้ใช้งาน รวมถึงการกำหนดช่องทางการเข้าถึงหรือเงื่อนไขในการเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

หมวดที่ 1
การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ
(Security policy)

วัตถุประสงค์

เพื่อกำหนดทิศทางและเป็นกรอบแนวทางการดำเนินงานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางกฎหมาย และนโยบายฯ ที่เกี่ยวข้อง รวมถึง การกำหนดบทบาท หน้าที่ความรับผิดชอบ แนวทางปฏิบัติ ด้านความมั่นคงปลอดภัยและการควบคุมความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อคงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลสารสนเทศและระบบสารสนเทศของกรมบัญชีกลาง

1.1 นโยบายระบบความมั่นคงปลอดภัยด้านสารสนเทศ

1.1.1 จัดให้มีนโยบายการควบคุมการใช้งานสารสนเทศที่เป็นลายลักษณ์อักษรที่ถูกอนุมัติจากผู้บริหารระดับสูง (CEO) รวมถึงการแก้ไขเปลี่ยนแปลงนโยบายทุกครั้งต้องถูกอนุมัติ

1.1.2 มีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอยู่เสมอ โดยมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง ซึ่งมีการระบุความเสี่ยงที่เกี่ยวข้องโดยจัดลำดับตามความสำคัญของสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร

1.1.3 มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ในระบบเทคโนโลยีสารสนเทศและการสื่อสาร และกำหนดมาตรการหรือขั้นตอนการปฏิบัติในการควบคุมความเสี่ยงอย่างเหมาะสม

1.1.4 นโยบายที่จัดทำต้องมีการกำหนดวัตถุประสงค์ ความรับผิดชอบ และเนื้อหาอย่างชัดเจน

1.1.5 จัดเก็บ และเผยแพร่นโยบายฯ ให้กับเจ้าหน้าที่ และบุคคลเกี่ยวข้องทราบเพื่อสามารถปฏิบัติให้เป็นไปตามนโยบายฯ ที่กำหนด

1.1.6 กำหนดหน้าที่ และความรับผิดชอบของเจ้าหน้าที่ และบุคคลที่เกี่ยวข้องอย่างชัดเจน กรณีผู้ที่เกี่ยวข้องมีส่วนต่อการดำเนินการที่สอดคล้องต่อนโยบายฯ ให้จัดทำขั้นตอนการปฏิบัติเพื่อรองรับต่อการปฏิบัติตามนโยบายฯ ที่ได้กำหนดไว้

1.1.7 จัดทำระบบติดตามการปฏิบัติตามนโยบายฯ และดำเนินการตรวจสอบการปฏิบัติตามอย่างต่อเนื่องมีการตรวจสอบ รวมทั้งประเมินความเพียงพอของนโยบายฯ และระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง

1.1.8 รายงานผู้บริหารที่กำกับดูแล ให้ทราบโดยเร็วเมื่อมีกรณีที่นโยบายฯ ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ

หมวดที่ 2

การจัดโครงสร้างการบริหารจัดการด้านความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งภายในและภายนอกองค์กร

(Organization of information security)

วัตถุประสงค์

เพื่อกำหนดบทบาท หน้าที่ความรับผิดชอบในการบริหารและจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร และลดความเสี่ยง โดยมีการป้องกันการสูญหายหรือการเปลี่ยนแปลงแก้ไขหรือการเข้าถึง ประมวลผล การนำระบบเทคโนโลยีสารสนเทศและการสื่อสารไปใช้โดยไม่ได้รับอนุญาตหรือไม่เหมาะสม

2.1 โครงสร้างระบบความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.1 “ผู้บริหารสูงสุด” CEO (Chief Executive Officer) หมายถึง อธิบดีกรมบัญชีกลาง เป็นผู้พิจารณาอนุมัตินโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.1.2 “ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” CIO (Chief Information Officer) หมายถึง ผู้ที่อธิบดีกรมบัญชีกลาง มอบหมายให้ รับผิดชอบสั่งการและกำกับดูแล ติดตามการดำเนินงานด้านเทคโนโลยีสารสนเทศของกรมบัญชีกลาง

2.1.3 “ผู้อำนวยการศูนย์เทคโนฯ” หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.1.4 ผู้บริหาร ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมาย งานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความ มั่นคงปลอดภัยให้กับสารสนเทศ

2.1.5 ผู้บริหารต้องแต่งตั้งคณะหรือกลุ่มผู้ทำงานหลัก ตลอดจนทรัพยากรที่จำเป็น เพื่อบริหารและจัดการ ความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

2.1.6 ผู้บริหาร ต้องกำหนดให้มีตัวแทนเจ้าหน้าที่จากหน่วยงานต่าง ๆ ภายในองค์กรเพื่อประสานงานหรือ ร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้นจะมีบทบาท และลักษณะงานที่รับผิดชอบที่แตกต่างกัน

2.2 การบริหารจัดการ

2.2.1 จัดให้มีการจัดทำคำอธิบายลักษณะงาน (Job Description) ซึ่งระบุหน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของเจ้าหน้าที่ที่เกี่ยวข้องอย่างชัดเจน

2.2.2 กำหนดให้มีการแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบงานหลัก (Production Environment)

2.2.3 จัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีผู้ปฏิบัติงานหลักไม่สามารถดำเนินการได้

2.2.4 ระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในองค์กร ต้องกำหนดเจ้าของสารสนเทศ (Information owner) เพื่อควบคุม และกำหนดการเข้าใช้ข้อมูล ยกเว้นระบบงานหลักที่มีการใช้งานร่วมกันจากหลายหน่วยงานกำหนดให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้ระบุความรับผิดชอบให้กับผู้ที่ได้รับมอบหมายในการดูแล (System Administrator) และการอนุมัติในการใช้งาน (Authorized Owner)

2.2.5 กรณีที่เจ้าของสารสนเทศหรือผู้ได้รับมอบหมายในการอนุมัติสารสนเทศไม่อยู่ หรือไม่สามารถปฏิบัติงานได้ และไม่มีการมอบหมายล่วงหน้า ผู้บังคับบัญชาของเจ้าของสารสนเทศหรือผู้ได้รับมอบหมายในการอนุมัติสารสนเทศต้องเป็นผู้รับผิดชอบแทน หรือเป็นผู้มอบหมายให้บุคคลอื่นรับผิดชอบต่อ

2.2.6 การเปลี่ยนแปลงตำแหน่งหน้าที่ หรือการพ้นจากตำแหน่งหน้าที่ต้องมีการจัดการเรื่องสิทธิ์การเข้าถึงให้ถูกต้อง

2.2.7 การละเมิดนโยบายฯ หรือละเลยต่อความมั่นคงปลอดภัยสารสนเทศควรได้รับการพิจารณาดำเนินการอย่างเป็นทางการและเป็นไปด้วยความยุติธรรม

หมวดที่ 3

การบริหารจัดการทรัพย์สินสารสนเทศ

(Asset management)

วัตถุประสงค์

เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหาย หรือการนำไปใช้อย่างผิดวัตถุประสงค์ อันเกิดจากการปฏิบัติหน้าที่ของเจ้าหน้าที่ในองค์กร และบุคคลภายนอกที่เข้าถึงสารสนเทศขององค์กร โดยทรัพย์สินสารสนเทศจำเป็นต้องได้รับการจัดหมวดหมู่ และกำหนดระดับความสำคัญ และมีวิธีการควบคุมดูแลเพื่อให้เกิดความถูกต้อง เหมาะสม ปลอดภัย และมีผู้รับผิดชอบที่ชัดเจน

3.1 การจัดแบ่งระดับชั้นความลับข้อมูล และการจัดการสารสนเทศ

3.1.1 กำหนดให้มีการแบ่งระดับชั้นความลับข้อมูล โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้รับผิดชอบการจัดทำและประกาศสื่อสารให้กับเจ้าหน้าที่ภายในองค์กรทราบ

3.1.2 สารสนเทศที่มีความสำคัญต้องถูกกำหนดป้ายชื่อ (Label) กรณีที่ไม่มีการกำหนดจะถือว่าเป็นสารสนเทศที่ใช้เฉพาะภายในองค์กร (Internal Use Only) โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะเข้าร่วมดำเนินการในการแบ่งระดับชั้นความลับกับเจ้าของสารสนเทศ รวมถึงจัดทำขั้นตอนการปฏิบัติการจัดระดับชั้นความลับ

3.1.3 สารสนเทศที่อยู่ในชั้นความลับสูงกว่า**ใช้ภายในกรมบัญชีกลางเท่านั้น** ต้องมีการเข้ารหัสข้อมูลหรือมีการกำหนดสิทธิการเข้าถึงข้อมูลในหน่วยจัดเก็บของอุปกรณ์คอมพิวเตอร์ และการติดต่อระหว่างเครือข่าย

3.1.4 สารสนเทศที่อยู่ในชั้นความลับระดับสูงกว่า**ใช้เฉพาะในกรมบัญชีกลางเท่านั้น**เมื่อมีการนำข้อมูลออกจากอุปกรณ์คอมพิวเตอร์หรือองค์กร ต้องผ่านการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น หรือคณะทำงานที่ได้รับมอบหมาย โดยต้องมีการลงนามเป็นลายลักษณ์อักษร

3.1.5 กำหนดให้บันทึกและเก็บล็อก (Log) การเข้าถึงข้อมูลและสารสนเทศต่าง ๆ ทั้งรูปแบบอิเล็กทรอนิกส์และรูปแบบเอกสาร ที่มีชั้นความลับระดับสูงกว่า**ใช้ภายในกรมบัญชีกลางเท่านั้น**

3.1.6 กรณีที่มีการเปิดเผยข้อมูลที่ไม่ได้อยู่ในระดับชั้นที่เปิดเผยได้สู่สาธารณะต้องดำเนินการโดยผู้รับผิดชอบซึ่งได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น หรือคณะทำงานที่ได้รับมอบหมาย

3.1.7 กำหนดขั้นตอนการปฏิบัติและหน่วยงานที่รับผิดชอบในการทำลายข้อมูลสารสนเทศทั้งที่อยู่ในรูปแบบเอกสาร ไฟล์ หรือมีเดีย ตามระดับชั้นความลับ

3.2 ความเป็นส่วนตัวของสารสนเทศ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร

3.2.1 ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ใช้ภายในองค์กรถือเป็นทรัพย์สินขององค์กร

3.2.2 ต้องมีการบันทึกประวัติการเข้าใช้งาน (Log) ในการใช้งานจดหมายอิเล็กทรอนิกส์ และเครือข่าย เพื่อตรวจสอบกรณีมีการละเมิดต่อนโยบายฯ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

3.2.3 มีการแจ้งให้บุคคล หรือหน่วยงานอื่นที่ใช้เทคโนโลยีสารสนเทศขององค์กรได้รับทราบเกี่ยวกับนโยบายการยอมรับการใช้สารสนเทศ

3.2.4 หน่วยงานภายนอกที่เข้าใช้สารสนเทศภายใน ซึ่งมีระดับชั้นความลับมากกว่าระดับ**ทั่วไป**จะต้องลงนามในสัญญารักษาความลับ

3.2.5 ผู้ที่ละเมิดต่อการปฏิบัติตามนโยบายฯ การรักษาความลับข้อมูลขององค์กรจะพิจารณาบทลงโทษเบื้องต้นโดยการตักเตือนโดยผู้บังคับบัญชา และบทลงโทษอื่นต้องเป็นไปตามกฎระเบียบขององค์กร โดยตัวอย่างระดับของการฝ่าฝืนกฎระเบียบอยู่ในหมวดที่ 4 ข้อ 4.2.2 ส่วนกรณีที่มีการละเมิดต่อกฎหมายให้พิจารณาลงโทษตามข้อบัญญัติของกฎหมาย

3.3 ความเป็นส่วนตัวของเว็บ

3.3.1 ผู้ที่ไม่มีหน้าที่เกี่ยวข้องในการดูแลบริหารระบบและเครือข่าย หากต้องการใช้บริการต่าง ๆ นอกเหนือจากเว็บไซต์ และเว็บเพจขององค์กร ต้องมีการขออนุญาตอย่างเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อนที่จะเผยแพร่ข้อมูลสู่สาธารณะ

3.3.2 เว็บไซต์ต่าง ๆ ขององค์กรต้องมีข้อความประกาศให้ทราบเกี่ยวกับลิขสิทธิ์ และทรัพย์สินขององค์กร

3.3.3 การสื่อสารข้อมูลในระดับชั้นความลับระดับสูงกว่า**ใช้เฉพาะในกรมบัญชีกลางเท่านั้น (ระดับลับขึ้นไป)** ผ่านเครือข่ายภายนอกต้องผ่านการเข้ารหัสเพื่อให้ข้อมูลมีความปลอดภัยที่ได้รับการรับรองตามมาตรฐานความปลอดภัย

3.3.4 กำหนดผู้รับผิดชอบในการปรับปรุงเว็บไซต์อย่างชัดเจน กรณีที่มีข้อสงสัยให้ปรึกษาหน่วยงานที่สามารถให้คำปรึกษาด้านกฎหมาย สำหรับแหล่งที่มาของข้อมูลต่าง ๆ ที่ไม่ได้มาจากองค์กรต้องมีการระบุแหล่งที่มาอย่างชัดเจน ห้ามนำข้อมูลที่ไม่ทราบแหล่งที่มา ใช้ในการจัดทำเว็บไซต์ขององค์กร

3.3.5 เว็บไซต์ขององค์กรต้องมีการระบุช่องทางการติดต่อ ไว้ในหน้าของเว็บไซต์เพื่อใช้ติดต่อกรณีที่ผู้ใช้งานมีข้อสงสัยหรือต้องการข้อมูลเพิ่ม

3.4 การปฏิบัติงานของเจ้าหน้าที่ต่อทรัพย์สินขององค์กร

3.4.1 เจ้าหน้าที่ต้องไม่นำทรัพย์สินสารสนเทศองค์กรไปใช้ในงานส่วนตัว

3.4.2 นายทะเบียนเอกสารต้องทำการกำหนดรหัสเอกสาร และเจ้าของข้อมูลหรือสารสนเทศต้องทำการระบุระดับชั้นความลับข้อมูลที่ตนเป็นเจ้าของ

3.4.3 เจ้าหน้าที่ต้องรับผิดชอบในการรักษาสารสนเทศที่ตนเป็นเจ้าของให้อยู่ในสภาพที่สมบูรณ์

3.4.4 กรณีที่ระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในพื้นที่ปราศจากผู้ดูแล เจ้าหน้าที่ต้องดำเนินการจัดเก็บ หรือล็อคอุปกรณ์ไว้อย่างรัดกุม

3.4.5 เจ้าหน้าที่ต้องจัดเก็บเอกสารสำคัญไว้ในลิ้นชัก หรือพื้นที่ที่สามารถควบคุมหรือปกปิดข้อมูลได้ กรณีที่เป็นข้อความสำคัญที่ติดหรือเขียนอยู่บนบอร์ด โต๊ะ หรือกระดานทุกครั้งหลังเลิกใช้งานให้ดำเนินการปกปิด หรือลบออกเมื่อเสร็จสิ้นการใช้งาน

3.4.6 เจ้าหน้าที่ต้องเฝ้าระวังขณะพิมพ์รายงานที่มีความสำคัญ โดยมีการเฝ้าระวังรายงานที่จัดพิมพ์จากบุคคลที่ไม่เกี่ยวข้อง และนำเอกสารออกจากเครื่องพิมพ์ทันที

หมวดที่ 4
การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
(Human resources security)

วัตถุประสงค์

เพื่อให้เจ้าหน้าที่ รวมถึงหน่วยงานภายนอก เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตน ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย ทั้งก่อนการปฏิบัติหน้าที่ ระหว่างการปฏิบัติหน้าที่ และการสิ้นสุดหรือการเปลี่ยนการปฏิบัติหน้าที่ ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับกฎระเบียบขององค์กรและกฎหมาย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

4.1 การสร้างความมั่นคงปลอดภัยก่อนการปฏิบัติหน้าที่ (Prior to employment)

4.1.1 ต้องมีมาตรการตรวจสอบคุณสมบัติของผู้สมัคร

4.1.1.1 หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นผู้บริหารหรือเจ้าหน้าที่

4.1.1.2 หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลต้องทำการตรวจสอบประวัติอาชญากรรม และการกระทำผิดกฎหมายผู้สมัครงาน

4.1.1.3 หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคลต้องเตรียมข้อมูลที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารขององค์กร เพื่อให้เจ้าหน้าที่ที่เข้ามาใหม่ได้ศึกษาและรับทราบ

4.1.1.4 เจ้าหน้าที่ใหม่ทุกคนต้องลงนามรับทราบและยอมรับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ความรับผิดชอบ

4.1.2 ต้องทำการกำหนดเงื่อนไขการจ้างงานที่รวมถึงหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

4.1.2.1 ต้องจัดให้เจ้าหน้าที่รวมถึงหน่วยงานภายนอกทำการลงนามในสัญญารักษาความลับ โดยการลงนามนี้จะเป็นส่วนหนึ่งของการจ้างงาน ทั้งนี้ ต้องมีผลผูกพัน ทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นระยะเวลาที่องค์กรทำการกำหนดหลังจากที่สิ้นสุดการว่างจ้างแล้ว

4.1.3 ต้องมีการกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยในคุณสมบัติของบุคลากรที่ทำงานเกี่ยวข้องกับเทคโนโลยีสารสนเทศ

4.1.3.1 ตระหนักถึงความสำคัญของรหัสผ่าน และสามารถปกปิดรหัสผ่านที่ตนรับผิดชอบไม่ให้รั่วไหลได้

4.1.3.2 มีความรู้ความเข้าใจเกี่ยวกับมัลแวร์ (Malware) รวมถึงมีความรู้เบื้องต้นในการใช้งานแอนตี้ไวรัส

4.1.3.3 มีความรับผิดชอบต่อความมั่นคงปลอดภัยด้านสารสนเทศตามที่ได้รับมอบหมาย

4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการปฏิบัติหน้าที่ (During Employment)

4.2.1 การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน

4.2.1.1 ต้องจัดการประชุม สัมมนา หรืออบรมให้ความรู้แก่ผู้ใช้งาน เกี่ยวกับขั้นตอนการปฏิบัติเพื่อสร้างความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร โดยหลักสูตรการอบรมขึ้นอยู่กับหน้าที่ความรับผิดชอบของผู้ใช้งาน

4.2.1.2 ต้องทำการแจ้งให้เจ้าหน้าที่และผู้ที่เกี่ยวข้องทราบ เมื่อมีการเปลี่ยนแปลงใด ๆ ที่เกี่ยวข้องกับความปลอดภัยด้านสารสนเทศ

4.2.1.3 เจ้าหน้าที่ใหม่ขององค์กรทุกคนต้องได้รับการอบรมเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายฯ ที่เกี่ยวข้อง โดยต้องเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย

4.2.1.4 ต้องจัดการอบรม และสื่อสารเพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรของกรมบัญชีกลาง อย่างน้อยปีละ 1 ครั้ง

4.2.2 บทลงโทษกรณีไม่ปฏิบัติตามนโยบายฯ

4.2.2.1 การฝ่าฝืนนโยบายฯ โดยเล็กน้อยจากความไม่ตั้งใจหรือบังเอิญ หรือการกระทำอื่นใดที่ก่อให้เกิดความเสียหายต่อระบบสารสนเทศ ผู้ดูแลระบบอาจจะแจ้งเตือนด้วยวาจา หรือจดหมายอิเล็กทรอนิกส์ หรือเป็นลายลักษณ์อักษร แต่หากเป็นการกระทำผิดซ้ำซ้อน ผู้ดูแลระบบอาจระงับสิทธิ์ของผู้ใช้งานไว้ก่อนจนกว่าจะมีการตักเตือนอย่างเป็นลายลักษณ์อักษรโดยผู้บังคับบัญชา และได้ทำการแก้ไขแล้ว

4.2.2.2 การฝ่าฝืนนโยบายฯ ขั้นรุนแรง เกิดจากการละเมิดโดยเจตนาหรือจงใจสร้างความเสียหายให้แก่ระบบโดยไม่มีสิทธิ์และไม่ได้รับอนุญาต เช่น

- การจงใจสร้างความเสียหายแก่ซอฟต์แวร์หรือข้อมูลหรืออุปกรณ์ฮาร์ดแวร์ระบบ
- การขโมยหรือพยายามขโมยทรัพย์สินหรือสิ่งที่ไม่มีสิทธิ์ในการครอบครองมาไว้ในครอบครอง ซึ่งก่อให้เกิดความเสียหายแก่ผู้อื่น เช่น การลักลอบหรือใช้งานอุปกรณ์ระบบสื่อสาร คอมพิวเตอร์ เป็นต้น

- การเข้าถึงระบบโดยมิชอบ (Unauthorized access) ทั้งในระดับกายภาพ การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือข้อมูล และการเข้าถึงโดยผ่านเครือข่ายสาธารณะ เช่น การลักลอบดักฟังหรือดักเก็บข้อมูลที่มีชั้นความลับ ทั้งในส่วนของการติดตั้งซอฟต์แวร์และฮาร์ดแวร์ที่สามารถดักจับข้อมูล การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบเจาะระบบ (Penetration Test) การทดลองถอดรหัส เป็นต้น
- ประพฤติมิชอบในกิจกรรมใด ๆ ที่เกี่ยวข้องกับองค์กร เช่น การคดโกง หรือให้ข้อมูลที่ผิดแก่ทางองค์กรโดยเจตนา
- การก่อความวุ่นวายที่ขัดต่อกฎระเบียบขององค์กร หรือสร้างความเดือดร้อนรบกวนการทำงานของผู้ใช้งานอื่น ๆ ในระบบเครือข่าย

4.2.2.3 กรณีที่ฝ่าฝืนหรือละเมิดข้อกำหนดข้างต้น และก่อให้เกิดความเสียหายแก่องค์กรหรือบุคคลอื่น องค์กรจะพิจารณาดำเนินการทางวินัยและกฎหมายแก่ผู้ใช้งานนั้น ตามความเหมาะสมดังต่อไปนี้

- ผู้ดูแลระบบจะพิจารณาการระงับใช้งาน และจะแจ้งชื่อผู้ใช้งานที่ทำผิดนโยบายฯ ไปยังหน่วยงานต้นสังกัดให้รับทราบ หรือแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รับทราบและพิจารณาตั้งกรรมการสอบสวนข้อเท็จจริง เพื่อพิจารณาจากความรุนแรงหรือความเสียหายที่เกิดขึ้นเป็นรายกรณีไป และองค์กรอาจพิจารณาดำเนินการทางวินัยหรือทางกฎหมายแก่ผู้นั้นตามความเหมาะสม
- ลงโทษทางวินัยต่อผู้ละเมิดตามความเหมาะสม เพื่อมิให้เกิดการละเมิดซ้ำ และในกรณีที่ผู้ละเมิดเป็นหน่วยงานภายนอก ให้ดำเนินการตามกฎหมายต่อไป
- หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อองค์กรอย่างร้ายแรง หรือเข้าข่ายความผิดตามกฎหมาย ให้ส่งตัวไปดำเนินการตามกฎหมายต่อไป
- หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารและต้องเสียค่าใช้จ่ายในการกู้คืน องค์กรสามารถเรียกร้องค่าเสียหายในส่วนนี้ เพื่อเป็นค่าใช้จ่ายในการกู้คืน

4.2.3 กิจกรรมที่เกี่ยวข้องกับการทดสอบระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและการสื่อสาร ได้แก่ การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) การทดลองถอดรหัส

การตรวจสอบ Network Traffic เป็นต้น สามารถดำเนินการได้โดยหน่วยงานหรือบุคคลที่ได้รับอนุญาตหรือมอบหมายจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

4.3 การสร้างความมั่นคงปลอดภัยเมื่อสิ้นสุดหรือเปลี่ยนการจ้างงาน (Termination or change of employment)

4.3.1 การคืนทรัพย์สินขององค์กร

4.3.1.1 เมื่อสิ้นสุดหรือเปลี่ยนการจ้างงาน ผู้ใช้งานจะต้องคืนทรัพย์สินขององค์กร เช่น อุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ในทันทีที่พ้นหน้าที่

4.3.2 การถอดถอนสิทธิ์ในการเข้าถึง

4.3.2.1 หน่วยงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดเปลี่ยนแปลง หรือยกเลิกสิทธิ์ของผู้ใช้งาน เพื่อให้สอดคล้องกับการเปลี่ยนแปลงสถานะของการว่าจ้างนั้นทันที โดยต้องเก็บข้อมูลให้สามารถตรวจสอบประวัติการเปลี่ยนแปลงสิทธิ์ในระบบเทคโนโลยีสารสนเทศและการสื่อสารเหล่านั้นได้

4.4 การรับผิดชอบต่อความเสียหาย

กรณีเกิดความเสียหาย หรืออันตรายใดๆ ต่อระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ สำนักงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารสูงสุดของสำนักงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

หมวดที่ 5

การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

(Physical and environmental security)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต รวมถึงป้องกันทรัพย์สินขององค์กรไม่ให้เกิดความเสียหาย สูญหาย ถูกขโมย หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต และป้องกันไม่ให้การดำเนินงานต่าง ๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

5.1 ข้อกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Area)

5.1.1 สถานที่ซึ่งติดตั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารหลักขององค์กร ต้องมีการควบคุมการเข้าถึงทางกายภาพ ดังนี้

5.1.1.1 การอนุญาตให้มีการเข้าออกสถานที่

5.1.1.2 การกำหนดสิทธิ์ในการเข้าออกสถานที่

5.1.1.3 การบันทึกข้อมูลการเข้าออกเพื่อการตรวจสอบ

5.1.1.4 การทบทวนรายชื่อผู้ได้รับอนุญาตและสิทธิ์ในการเข้าออกสถานที่

5.1.2 การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

5.1.2.1 ภายในองค์กร ต้องมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศและการสื่อสารต่าง ๆ อย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

5.1.2.2 ต้องมีการกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน และประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว แบ่งออกได้เป็น

1) พื้นที่ทำงานทั่วไป (General working area)
2) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)
3) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT equipment area)
4) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
5) พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

5.1.2.3 ผู้บริหาร ต้องกำหนดสิทธิ์ให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

- จัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารและให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างน้อยปีละ 1 ครั้ง
- ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”
- จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นประจำทุกครั้ง

5.1.3 การควบคุมการเข้าออก อาคาร สถานที่

5.1.3.1 จัดทำเอกสารระบุสิทธิ์ของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้

- องค์กรต้องกำหนดสิทธิ์ ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน
- การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอกหรือผู้มาติดต่อ ต้องทำการแจ้งเจ้าหน้าที่รักษาความปลอดภัย และต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น
- บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในองค์กร
- เจ้าหน้าที่ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกได้ถูกต้อง
- บุคคลภายนอกหรือผู้ติดต่อ ต้องลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

5.1.3.2 ผู้ใช้งานจะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนด เพื่อใช้ในการทำงานเท่านั้น

5.1.3.3 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่องค์กรออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกข้อมูลบุคคลและการขอเข้าออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

5.1.4 กระบวนการควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์ (Data Center)

5.1.4.1 ผู้ดูแลระบบ ห้องศูนย์คอมพิวเตอร์ (Data Center) และเจ้าหน้าที่องค์กร มีแนวทางปฏิบัติ ดังนี้

- ผู้ดูแลระบบ ต้องจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เพื่อความสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น
- ห้องศูนย์คอมพิวเตอร์ (Data Center) ต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกห้องศูนย์คอมพิวเตอร์ (Data Center) โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่”
- สิทธิ์ในการเข้าออกห้องศูนย์คอมพิวเตอร์ (Data Center) ของเจ้าหน้าที่แต่ละคนต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยผ่านกระบวนการลงทะเบียนที่ระบุไว้ในเอกสารขั้นตอนการปฏิบัติ โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องศูนย์คอมพิวเตอร์ (Data Center)
- เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องทำบัตรผ่านเพื่อใช้ในการเข้าออกห้องศูนย์คอมพิวเตอร์ (Data Center) ตามกระบวนการที่ระบุในเอกสารขั้นตอนการปฏิบัติ
- ต้องจัดทำระบบเก็บบันทึกการเข้าออกห้องศูนย์คอมพิวเตอร์ (Data Center) ตามกระบวนการที่ระบุไว้ในเอกสารขั้นตอนการปฏิบัติ
- กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์ (Data Center) ต้องมีการควบคุมอย่างรัดกุม
- การเข้าถึงห้องคอมพิวเตอร์ ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร
- เจ้าหน้าที่ห้องศูนย์คอมพิวเตอร์ (Data Center) ทุกคนต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้าออกทุกคนต้องกรอกแบบฟอร์มดังกล่าว

5.1.4.2 ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติดังนี้

- ผู้ติดต่อจากหน่วยงานภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน ใบอนุญาตขับขี่ หรือบัตรที่ทางราชการออกให้ เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก

- ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกให้ถูกต้องชัดเจน และต้องผ่านการตรวจสอบด้านความมั่นคงปลอดภัยโดยเจ้าหน้าที่รักษาความปลอดภัยด้านสารสนเทศ และลงชื่อกำกับในแบบฟอร์มบันทึกรายการอุปกรณ์แต่ละรายการ
- ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้าออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา
- ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องตรวจสอบการคืนบัตรของผู้ติดต่อจากหน่วยงานภายนอกแต่ละคน
- เจ้าหน้าที่ผู้ดูแลศูนย์คอมพิวเตอร์ ต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มการขออนุญาตเข้าออกและตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง
- เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้าออกกับเจ้าหน้าที่รักษาความปลอดภัยด้านสารสนเทศเป็นประจำทุกเดือน
- เจ้าหน้าที่ผู้ดูแลศูนย์คอมพิวเตอร์ ต้องทำการทบทวนสิทธิ์การอนุญาตเข้าออกให้มีความถูกต้องอย่างสม่ำเสมอ อย่างน้อยปีละ 2 ครั้ง

5.1.5 กำหนดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยด้านสารสนเทศทางกายภาพและสภาพแวดล้อมโดยหน่วยงานอิสระ อย่างน้อยปีละ 2 ครั้ง

5.1.6 การปฏิบัติงานในพื้นที่ควบคุม

5.1.6.1 ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ ไม่อนุญาตให้ถ่ายภาพหรือวีดีโอในบริเวณพื้นที่ควบคุม หรือทำกิจกรรมอื่นใดที่เป็นการบันทึกภาพของระบบหรือภาพภายในพื้นที่ควบคุม หากมีความจำเป็นต้องแจ้งเจ้าหน้าที่ผู้กำกับดูแล

5.1.6.2 ต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวีดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

5.1.7 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

5.1.7.1 ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ต้องจัดเป็นบริเวณแยกออกมาต่างหาก

5.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของอุปกรณ์

5.2.1 ความมั่นคงปลอดภัยของอุปกรณ์

5.2.1.1 ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่าง ๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์ โดยไม่ได้รับอนุญาต และต้องมีการควบคุมการนำอุปกรณ์เข้าออกในบริเวณพื้นที่ควบคุม

5.2.1.2 อุปกรณ์ที่มีความสำคัญต่อระบบสารสนเทศ ต้องได้รับการปิดล็อคและป้องกันการเข้าถึง

5.2.1.3 ต้องมีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่าง ๆ ได้แก่ ระบบไฟฟ้า ระบบไฟฟ้าสำรอง ระบบน้ำประปา ระบบตรวจจับและดับเพลิง ระบบควบคุมอุณหภูมิและความชื้น

5.2.1.4 ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน เป็นไปตามมาตรฐานหรือคุณสมบัติของอุปกรณ์แต่ละระบบ ตามระยะเวลาและขั้นตอนที่อุปกรณ์แต่ละประเภทกำหนดหรือตามแผนการบำรุงรักษาระบบคอมพิวเตอร์นั้น ๆ

5.2.1.5 ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น ทั้งนี้ เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว

5.2.2 การปฏิบัติในการเคลื่อนย้ายทรัพย์สินสารสนเทศ เข้า-ออก หน่วยงาน

5.2.2.1 การนำทรัพย์สินสารสนเทศ เข้า-ออก หน่วยงาน จะต้องได้รับการอนุมัติจากหัวหน้าหน่วยงานก่อนทุกครั้ง หรือเจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน

5.2.2.2 กรณีที่มีการนำทรัพย์สินสารสนเทศขององค์กรไปปฏิบัติงานภายนอกสำนักงาน เช่น ที่บ้าน หรือที่สาธารณะ เป็นต้น ผู้ใช้งานจะต้องปกปิดทรัพย์สินสารสนเทศให้เป็นความลับและไม่เปิดเผยแก่บุคคลภายนอก พร้อมทั้งต้องดูแลรักษาทรัพย์สินสารสนเทศให้มีความปลอดภัยตลอดเวลา

5.2.2.3 กรณีที่มีการนำทรัพย์สินสารสนเทศกลับเข้ามาใช้ภายในสำนักงาน จะต้องมีการตรวจสอบโปรแกรมป้องกันและกำจัดมัลแวร์ให้เป็นปัจจุบัน รวมทั้งสื่อต่าง ๆ ที่จะนำกลับเข้ามาใช้งานให้ปลอดภัยก่อนการเชื่อมต่อกับระบบเครือข่ายฯ ขององค์กร

5.2.3 การปฏิบัติในการเคลื่อนย้ายทรัพย์สินสารสนเทศ เข้า-ออก ห้องศูนย์คอมพิวเตอร์ (Data Center)

5.2.3.1 ต้องมีการควบคุม ดูแล การเข้า-ออก ในบริเวณพื้นที่ควบคุม โดยให้ผ่าน เข้า-ออก ได้เฉพาะผู้ที่มีสิทธิ์หรือผู้ที่ได้รับอนุญาตเท่านั้น

5.2.3.2 การนำทรัพย์สินสารสนเทศ เข้า-ออก ห้องศูนย์คอมพิวเตอร์ (Data Center) จะต้องได้รับการอนุมัติจากหัวหน้าหน่วยงานก่อนทุกครั้ง หรือเจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน

5.2.3.3 กรณีที่มีการนำทรัพย์สินสารสนเทศกลับเข้ามาในห้องศูนย์คอมพิวเตอร์ (Data Center) จะต้องมีการตรวจสอบโปรแกรมป้องกันและกำจัดมัลแวร์ให้เป็นปัจจุบัน รวมทั้งสื่อต่าง ๆ ที่จะนำกลับเข้ามาใช้งานให้ปลอดภัยก่อนการเชื่อมต่อกับระบบเครือข่ายฯ ขององค์กร

หมวดที่ 6

การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(Communications and operations management)

วัตถุประสงค์

เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย รักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลง ลดความเสี่ยงจากการล้มเหลวของระบบ ป้องกันซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยชุดคำสั่งไม่พึงประสงค์ ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต

โดยประกอบด้วยนโยบายที่ได้แยกตามการดำเนินงาน ดังต่อไปนี้

6.1 นโยบายความมั่นคงปลอดภัยด้านเครือข่ายคอมพิวเตอร์
6.2 นโยบายการใช้งานอินเทอร์เน็ต
6.3 นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์
6.4 นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล
6.5 นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา
6.6 นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
6.7 นโยบายการใช้งานอุปกรณ์อิเล็กทรอนิกส์พกพา
6.8 นโยบายการแลกเปลี่ยนสารสนเทศ
6.9 นโยบายการเฝ้าระวังทางด้านความมั่นคงปลอดภัย

6.1 นโยบายความมั่นคงปลอดภัยด้านเครือข่ายคอมพิวเตอร์

6.1.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)

6.1.1.1 หัวหน้ากลุ่มงานที่เป็นเจ้าของระบบงาน ต้องจัดทำคู่มือและขั้นตอนการปฏิบัติงานของระบบงานนั้น ๆ

6.1.1.2 ในกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเทคโนโลยีสารสนเทศและการสื่อสาร เจ้าของระบบงาน ผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสารนั้น ต้องทำการบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ

6.1.1.3 หัวหน้ากลุ่มงานที่เป็นเจ้าของระบบงาน ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและการสื่อสารที่หน่วยงานนั้น ๆ รับผิดชอบ

6.1.1.4 หัวหน้ากลุ่มงานที่เป็นเจ้าของระบบงาน ต้องกำหนดหน้าที่ความรับผิดชอบรวมทั้งขั้นตอนการปฏิบัติเมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้ละเมิด

6.1.1.5 หัวหน้ากลุ่มงานที่เป็นเจ้าของระบบงาน ต้องแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารออกจากเครื่องที่ทำงานจริงหรือเครื่องให้บริการ

6.1.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management)

6.1.2.1 ต้องปรับปรุงเงื่อนไขการให้บริการต่อหน่วยงานภายนอก เมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงหรือพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารใหม่ การปรับปรุงนโยบายและขั้นตอนการปฏิบัติสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก โดยต้องได้รับการอนุมัติก่อนจึงจะสามารถดำเนินการได้ รวมทั้งปรับปรุงเอกสารที่เกี่ยวข้องให้ทันสมัยเมื่อมีการเปลี่ยนแปลงสารสนเทศ

6.1.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System planning and acceptance)

6.1.3.1 ต้องมีการวางแผนกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต โดยสำรวจความต้องการทรัพยากรสารสนเทศให้ครบถ้วน เพื่อไม่ให้โครงการเกิดความล่าช้า

ในการจัดซื้อจัดหา และต้องคำนึงถึงความมั่นคงปลอดภัยของสารสนเทศด้วย ซึ่งจะทำให้ระบบมีความมั่นคงปลอดภัยและไม่เกิดค่าใช้จ่ายในภายหลัง

6.1.3.2 ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบเทคโนโลยีสารสนเทศและการสื่อสารใหม่ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน เช่น การตรวจรับตามที่ได้กำหนดไว้ เป็นต้น

6.1.4 ชุดคำสั่งที่ไม่พึงประสงค์ (Protection against malicious and mobile code)

6.1.4.1 ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ต้องได้รับการดูแล บำรุงรักษาและป้องกันภัยจากการใช้งาน ภัยจากมัลแวร์ (Malware) และภัยจากการบุกรุก เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศและการสื่อสารมีความพร้อมต่อการให้บริการ

6.1.4.1.1 ห้ามนำเครื่องคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์หรือชุดคำสั่งที่ไม่ผ่านการตรวจสอบด้านความมั่นคงปลอดภัยมาติดตั้งใช้งาน

6.1.4.1.2 ห้ามผู้ใช้งานปรับแต่ง หรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันมัลแวร์ที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่องค์กรได้จัดหาให้

6.1.4.1.3 ผู้ใช้งานต้องมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบการอัปเดต (Update) ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบ หากไม่สามารถอัปเดต (Update) ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

6.1.4.1.4 ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อสงสัยว่ามีการติดมัลแวร์

6.1.5 การสำรองข้อมูล (Backup)

6.1.5.1 ระบบเทคโนโลยีสารสนเทศและการสื่อสารหลักต้องได้รับการสำรองข้อมูลอย่างสม่ำเสมอ โดยให้ผู้ดูแลระบบกำหนดเวลาในการสำรองข้อมูล และลักษณะการสำรองข้อมูล

6.1.5.2 ข้อมูลที่สำรองจะต้องได้รับการทดสอบเพื่อให้เกิดความมั่นใจว่าข้อมูลดังกล่าวสามารถนำกลับมาใช้ได้เมื่อต้องการ โดยให้ผู้ดูแลระบบกำหนดเวลาในการทดสอบข้อมูลสำรอง

6.1.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)

6.1.6.1 แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

6.1.6.1.1 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการอนุมัติแล้ว

6.1.6.1.2 ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

6.1.6.1.3 ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

6.1.6.1.4 ผู้ดูและระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือนอกบริเวณขอบเขตควบคุม

6.1.6.1.5 ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและต้องสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น

6.1.6.1.6 ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ Access Point (AP) มาใช้งาน

6.1.6.1.7 ผู้ดูแลระบบ ต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อ Login และรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

6.1.6.1.8 ผู้ดูแลระบบต้องกำหนดค่าในการเข้ารหัสระบบเครือข่ายไร้สายที่มีความปลอดภัย เช่น WPA หรือดีกว่า เพื่อให้ยากต่อการดักจับข้อมูล

6.1.6.1.9 ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้งานรหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

6.1.6.1.10 ผู้ดูแลระบบจะต้องมีการติดตั้งไฟร์วอลล์ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

6.1.6.1.11 ผู้ดูแลระบบ ต้องใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

6.1.6.2 แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายแบบสายสัญญาณสื่อสารสำหรับเชื่อมต่อเครื่องคอมพิวเตอร์ของผู้ใช้งาน

6.1.6.2.1 กำหนดให้มีมาตรการป้องกันช่องทางการสื่อสารระหว่างเครื่องคอมพิวเตอร์ ในกรณีที่ไม่ได้ใช้งานให้ทำการ Disable Port บนอุปกรณ์ Switch

6.1.6.2.2 กำหนดให้มีการควบคุมการเข้าถึงระบบเครือข่ายแบบสายสัญญาณสื่อสารเฉพาะพื้นที่การปฏิบัติงานของกรมเท่านั้น

6.1.6.2.3 ผู้ให้บริการภายนอกหรือบุคคลภายนอกที่มีความประสงค์จะใช้งานในระบบเครือข่ายแบบสายสัญญาณสื่อสาร ต้องลงทะเบียนในแบบฟอร์มที่กำหนด (แบบบันทึกการลงทะเบียนสิทธิผู้ใช้งาน (User Request) สำหรับบริษัท) เพื่อลงทะเบียนข้อมูล ได้แก่ ชื่อผู้ใช้งาน ชื่อบริษัท ระบบงานที่เข้ามาดำเนินงาน และหมายเลข MAC Address ของเครื่องคอมพิวเตอร์ เพื่อกำหนด IP Address ใช้งานภายในเครือข่ายเฉพาะกิจ และต้องได้รับอนุมัติจากผู้รับรองของบริษัท และเจ้าของระบบงาน

6.1.6.2.4 การควบคุมเส้นทางเครือข่ายของเจ้าหน้าที่บริษัท มีรายละเอียดดังนี้

ก) กำหนดหมายเลข IP Address เป็นการเฉพาะบุคคลที่ได้ลงทะเบียนตามข้อ 6.1.6.2.3

ข) ดำเนินการกรอกข้อมูล Request of Change รายละเอียดที่เกี่ยวข้อง และได้รับความเห็นชอบจากผู้ที่เกี่ยวข้องและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อนดำเนินการต่อไป

ค) ผู้ดูแลระบบจะดำเนินการควบคุม Port ที่ใช้เข้าถึงระบบงานให้เหมาะสมเพียงพอตามระยะเวลาที่ร้องขอ และสอดคล้องกับการใช้งาน

ง) ผู้ดูแลระบบต้องกำหนดให้มีการเก็บข้อมูลจลาจรในการเข้าถึงระบบงานตามที่ได้ร้อง เพื่อสามารถตรวจสอบย้อนหลังได้

6.1.7 แนวทางปฏิบัติในการควบคุมการใช้เครือข่ายตามนโยบายไฟร์วอลล์

6.1.7.1 กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข เปลี่ยนแปลงค่าพารามิเตอร์ต่าง ๆ ของไฟร์วอลล์ และการเชื่อมต่อระบบเครือข่ายอย่างชัดเจน

6.1.7.2 กำหนดขั้นตอนและวิธีปฏิบัติในการเปลี่ยนแปลงค่าพารามิเตอร์ ของไฟร์วอลล์และระบบสนับสนุนงานด้านความปลอดภัยต่าง ๆ

6.1.7.3 ตรวจสอบ การบุกรุกการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย การเปลี่ยนแปลงแก้ไขค่าพารามิเตอร์ และการปรับเปลี่ยนขอบเขตของเครือข่าย

6.1.7.4 ตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย

6.1.7.5 การใช้เครื่องมือต่าง ๆ (Tools) ในการตรวจสอบระบบเครือข่ายต้องได้รับอนุมัติจากผู้มีอำนาจหน้าที่

6.1.7.6 เครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดขององค์กรต้องติดตั้งในเครือข่ายหลังไฟร์วอลล์

6.1.7.7 ไฟร์วอลล์ที่อยู่ระหว่างเครือข่ายอินเตอร์เน็ต กับเครือข่ายภายในองค์กร ต้องมีรหัสผ่านไม่เหมือนกัน

6.1.7.8 การเปลี่ยนแปลงค่ากำหนดของไฟร์วอลล์ ในการเปิดบริการ และการกำหนดเส้นทางที่เชื่อมต่อต้องถูกจัดเก็บบันทึกลงล็อก (Log)

6.1.7.9 จัดเตรียมระบบการกำหนดสิทธิ์การเข้าถึงระบบ การป้องกันการแก้ไขเปลี่ยนแปลงบันทึก (Log) ต่าง ๆ และการบันทึกการเข้าใช้ระบบ เพื่อป้องกันการเข้าถึงโดยไม่มีสิทธิ์

6.1.8 แนวทางปฏิบัติในการควบคุมตรวจสอบและป้องกันการบุกรุกระบบเครือข่าย

6.1.8.1 ติดตั้งอุปกรณ์ IPS (Intrusion Prevention System) ในพื้นที่ที่มีความปลอดภัยและมีมาตรการควบคุมการเข้าถึง

6.1.8.2 กำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข เปลี่ยนแปลงค่าพารามิเตอร์ต่าง ๆ ของอุปกรณ์ IPS และการเชื่อมต่อระบบเครือข่ายอย่างชัดเจน

6.1.8.3 กำหนดวิธีการออกแบบ การติดตั้งตั้งอุปกรณ์ IPS และตำแหน่งการจัดวางในเครือข่ายให้เหมาะสม โดยเฉพาะเครือข่ายที่เชื่อมต่อกับภายนอก

6.1.8.4 ตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย

6.1.8.5 กำหนดวิธีการทดสอบ เพื่อใช้ทดสอบการปรับเปลี่ยนค่ากำหนดการอัปเดตฮาร์ดแวร์ ซอฟต์แวร์ และตรวจสอบผลการทดสอบทุกครั้งก่อนใช้งานจริง

6.1.8.6 ตรวจสอบช่องโหว่ที่พบในอุปกรณ์ IPS

6.1.8.7 จัดเตรียม และใช้งานระบบป้องกันการแก้ไขเปลี่ยนแปลงบันทึก (Log) ต่าง ๆ และกำหนดสิทธิ์การเข้าถึงบันทึกเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

6.1.9 การบริหารจัดการระบบเครื่องคอมพิวเตอร์แม่ข่าย

6.1.9.1 ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

6.1.9.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

6.1.9.3 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

6.1.9.4 ต้องดำเนินการติดตั้งอัปเดตระบบซอฟท์แวร์ให้เป็นปัจจุบัน เพื่อปิดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

6.1.9.5 ต้องมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

6.1.9.6 การติดตั้งและการเชื่อมต่อระบบเครื่องคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

6.2 นโยบายการใช้งานอินเทอร์เน็ต

6.2.1 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)

6.2.1.1 แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

6.2.1.1.1 ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IP เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น นอกเหนือจากที่กรมจัดเตรียมไว้

6.2.1.1.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการปิดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

6.2.1.1.3 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัส (Anti-virus) ก่อนการรับส่งข้อมูลทุกครั้ง

6.2.1.1.4 ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

6.2.1.1.5 ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร

6.2.1.1.6 ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

6.2.1.1.7 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

6.2.1.1.8 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

6.2.1.1.9 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้ จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

6.2.1.1.10 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

6.2.1.1.11 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

6.2.1.1.12 การใช้งานเว็บบอร์ด (Web Board) ขององค์กร ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์กร

6.2.1.1.13 ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

6.2.1.1.14 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

6.3 นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์

6.3.1 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)

6.3.1.1 แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

6.3.1.1.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กรให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ

6.3.1.1.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ขององค์กร

6.3.1.1.3 สำหรับผู้ใช้งานรายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

6.3.1.1.4 การกำหนดรหัสผ่านที่ดี (Good Password) ตามที่ระบุไว้ ในข้อ 7.2.1

6.3.1.1.5 รหัสผ่านจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “X” หรือ “O”ในการพิมพ์แต่ละตัวอักษร

6.3.1.1.6 ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน 3 ครั้ง

6.3.1.1.7 ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ต้องมีการ Logout ออกจากหน้าจอตัดการใช้งานผู้ใช้งานเมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ 60 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

6.3.1.1.8 ผู้ใช้งานไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

6.3.1.1.9 ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านทุก 6 เดือน

6.3.1.1.10 ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร

6.3.1.1.11 ผู้ใช้งาน ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

6.3.1.1.12 ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น

6.3.1.1.13 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

6.3.1.1.14 ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

6.3.1.1.15 ผู้ใช้งานไม่ควรเปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

6.3.1.1.16 ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

6.3.1.1.17 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

6.3.1.1.18 ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

6.3.1.1.19 ผู้ใช้งานต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

6.4 นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล

6.4.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)

6.4.1.1 กำหนดให้มีผู้ที่ทำหน้าที่ดูแลสื่อบันทึกข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยจัดลำดับความสำคัญและจัดเก็บในพื้นที่ที่เหมาะสม มีความปลอดภัย และพร้อมใช้งาน

6.4.1.2 กำหนดสิทธิ์และการควบคุมในการเข้าถึง สื่อบันทึกข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสาร และจัดทำทะเบียนผู้มีสิทธิ์ใช้สื่อบันทึกข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสาร

รวมทั้ง จัดให้มีการลงทะเบียนทุกครั้งที่มีการยืมหรือคืนสื่อบันทึกข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสาร

6.4.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of Media)

6.4.2.1 กำหนดระยะเวลาการเก็บ การลบ การทำลาย สื่อบันทึกข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสาร ข้อมูลของระบบเทคโนโลยีสารสนเทศและการสื่อสาร และการสำรองข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เหมาะสม ปลอดภัย ชัดเจน พร้อมทั้งจัดทำเอกสารแนวทางปฏิบัติ

6.4.2.2 กำหนดอายุการใช้งานของสื่อบันทึกข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสาร และให้มีการบันทึกวันเริ่มใช้งานและวันสิ้นสุดการใช้งาน

6.4.2.3 การทำลายสารสนเทศที่เก็บอยู่ในสื่อบันทึกข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ใช้วิธีการที่มั่นใจได้ว่าข้อมูลได้ถูกทำลายนั้นไม่สามารถกู้คืนได้อีก

6.5 นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

6.5.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)

6.5.1.1 การใช้งานทั่วไป

6.5.1.1.1 เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ผู้ใช้งานใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร

6.5.1.1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

6.5.1.1.3 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

6.5.1.1.4 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

6.5.1.1.5 ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

6.5.1.1.6 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

6.5.1.1.7 ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

6.5.1.1.8 การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

6.5.1.1.9 ไม่ใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

6.5.1.1.10 ไม่วางของทับบนหน้าจอและแป้นพิมพ์

6.5.1.1.11 การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

6.5.1.1.12 ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

6.5.1.1.13 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว และมีความชื้น

6.5.1.1.14 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ในสภาพแวดล้อมที่มีอุณหภูมิสูง จนอาจส่งผลกระทบต่อเครื่องคอมพิวเตอร์แบบพกพาได้

6.5.1.1.15 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

6.5.1.1.16 ไม่ควรติดตั้งหรือวางเครื่องคอมพิวเตอร์แบบพกพาในสถานที่ที่มีการสั่นสะเทือน

6.5.1.1.17 การเช็ดทำความสะอาดต้องทำอย่างระมัดระวัง ไม่ให้เกิดความเสียหายกับตัวเครื่อง

6.5.2 การป้องกันมัลแวร์ (Protection against malware)

6.5.2.1 แนวทางปฏิบัติในการป้องกันโปรแกรมประสงค์ร้ายในเครื่องคอมพิวเตอร์แบบพกพา

6.5.2.1.1 ผู้ใช้งานต้องทำการอัปเดต (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

6.5.2.1.2 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

6.5.2.1.3 หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malicious and mobile code) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

6.5.3 การสำรองข้อมูล (Backup)

6.5.3.1 แนวทางปฏิบัติในการสำรองข้อมูล

6.5.3.1.1 ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาโดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

6.5.3.1.2 ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

6.5.3.1.3 แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

6.5.3.1.4 แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

6.6 นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

6.6.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)

6.6.1.1 การใช้งานทั่วไป

6.6.1.1.1 เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้งาน ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร

6.6.1.1.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

6.6.1.1.3 ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร

6.6.1.1.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ขององค์กรเท่านั้น

6.6.1.1.5 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

6.6.1.1.6 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

6.6.1.1.7 ไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

6.6.1.1.8 ไม่ควรสร้าง Shortcut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์กร

6.6.1.1.9 ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยต้องปฏิบัติ ดังนี้

- ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

6.6.2 การป้องกันโปรแกรมประสงค์ร้าย (Protection against malicious and mobile code)

6.6.2.1 แนวทางปฏิบัติในการป้องกันโปรแกรมประสงค์ร้ายในคอมพิวเตอร์ส่วนบุคคล

6.6.2.1.1 ผู้ใช้งานต้องทำการอัปเดต (Update) ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

6.6.2.1.2 ผู้ใช้งานมีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

6.6.2.1.3 ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

6.6.2.1.4 ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

6.6.2.1.5 ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

6.6.2.1.6 ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลายถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

6.6.3 การสำรองข้อมูล (Backup)

6.6.3.1 แนวทางปฏิบัติในการสำรองข้อมูล

6.6.3.1.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

6.6.3.1.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

6.6.3.1.3 ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

6.7 นโยบายการใช้งานอุปกรณ์สื่อสารแบบพกพา

6.7.1 นโยบายและขั้นตอนการปฏิบัติสำหรับการใช้งานอุปกรณ์อิเล็กทรอนิกส์พกพา

6.7.1.1 ผู้ใช้งานต้องมีความตระหนักในการนำอุปกรณ์อิเล็กทรอนิกส์พกพา ได้แก่ Notebook, Smart phone และ Tablet ที่นำมาใช้งานภายในองค์กร หากอุปกรณ์ดังกล่าวมีการเข้าถึงสารสนเทศขององค์กร ต้องมีการตั้งค่าล็อคหน้าจอ (Passcode) ติดตั้งซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย และปรับปรุงระบบปฏิบัติการอย่างสม่ำเสมอ

6.7.1.2 หากผู้ใช้งานทำอุปกรณ์อิเล็กทรอนิกส์พกพาสูญหาย ผู้ใช้งานต้องแจ้งผู้ดูแลระบบทันทีเพื่อหาแนวทางในการแก้ไข

6.8 นโยบายการแลกเปลี่ยนสารสนเทศ

6.8.1 นโยบายและขั้นตอนการปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)

6.8.1.1 การเชื่อมต่อและแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานภายในและภายนอกต้องดำเนินการควบคุมให้เป็นไปตามหมวดที่ 15 ของนโยบายฯ ฉบับนี้

6.8.1.2 ต้องมีการร้องขอ และการอนุมัติให้เชื่อมต่อตามความจำเป็นในการใช้งาน และเป็นไปตามภารกิจที่ได้รับมอบหมาย

6.8.1.3 ต้องมีการกำหนดสิทธิ์ และผู้รับผิดชอบของหน่วยงานที่เชื่อมต่อ

6.8.1.4 กำหนดนโยบายการเชื่อมต่อให้มีความมั่นคงปลอดภัยสูงที่สุด

6.9 นโยบายการเฝ้าระวังทางด้านความมั่นคงปลอดภัย

6.9.1 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

6.9.1.1 ต้องกำหนดให้ทำการบันทึกกิจกรรมใช้งานของผู้ใช้งาน การปฏิเสธการให้บริการระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

6.9.1.1.1 กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน

6.9.1.2 ต้องกำหนดให้มีขั้นตอนการปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่ รวมถึงตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

6.9.1.3 ต้องกำหนดให้มีมาตรการป้องกันและจำกัดสิทธิ์การเข้าถึง ข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือเข้าถึงโดยไม่ได้รับอนุญาต

6.9.1.4 ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ

6.9.1.5 ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น เพื่อดำเนินการแก้ไขให้ถูกต้องต่อไป

6.9.1.6 ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง โดยเทียบเวลากับอุปกรณ์เทียบเวลาของที่องค์กรประกาศใช้ หรือระบบให้บริการเวลามาตรฐานทางอินเทอร์เน็ต (Network Time Protocol Server) เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

หมวดที่ 7

การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (Access control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)

7.1.1 ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีการควบคุมการเข้าถึง ดังนี้

7.1.1.1 การลงทะเบียนและยกเลิกทะเบียนผู้ใช้งาน

7.1.1.2 การระบุตัวตนผู้ใช้งาน (User identification) และการใช้งานรหัสผ่าน (Password)

7.1.1.3 การกำหนดสิทธิ์ของผู้ใช้งาน (Privilege) ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นไปตามบทบาท หน้าที่และความรับผิดชอบของผู้ใช้งาน

7.1.1.4 การทบทวนทะเบียนบัญชีและสิทธิ์ของผู้ใช้งาน

7.1.2 กระบวนการหลักในการควบคุมการเข้าถึงระบบ

7.1.2.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

7.1.2.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

7.1.2.3 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

7.1.2.4 ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ

7.1.2.5 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

7.1.3 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

7.1.3.1 ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ได้แก่ ผู้ใช้งานในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

7.1.3.2 เจ้าของข้อมูลและเจ้าของระบบงานจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

7.1.3.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

7.1.4 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

7.1.4.1 การลงทะเบียนเจ้าหน้าที่ใหม่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดให้มีขั้นตอนการปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนการปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

7.1.4.2 กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

7.1.4.3 ผู้ใช้งานต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

7.1.4.4 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

7.1.4.4.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ

7.1.4.4.2 การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตามข้อ 7.2.1 แนวทางปฏิบัติในการใช้รหัสผ่าน

7.1.4.4.3 กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

- ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ
- ต้องควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

7.1.5 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

7.1.5.1 ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

7.1.5.2 เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 2 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

7.1.5.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับข้อมูล

7.1.5.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XMLEncryption เป็นต้น

7.1.5.5 ต้องมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

7.1.5.6 ต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

7.2 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

7.2.1 แนวทางปฏิบัติในการใช้รหัสผ่าน

7.2.1.1 ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่าน ดังนี้

- กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวอักษรตัวใหญ่ ตัวอักษรตัวเล็ก ตัวเลข และสัญลักษณ์เข้าด้วยกัน
- ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม
- ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่เจ้าหน้าที่ครอบครองอยู่
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- ต้องให้เจ้าหน้าที่ลงนาม เพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
- กำหนดรหัสผ่านเริ่มต้นให้กับเจ้าหน้าที่ให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับเจ้าหน้าที่ต้องเป็นไปอย่างปลอดภัย

7.2.2 ข้อปฏิบัติของผู้ใช้งานในการใช้งานเครือข่ายคอมพิวเตอร์

7.2.2.1 ผู้ใช้งานที่มีสิทธิ์ใช้เครือข่ายคอมพิวเตอร์ภายใต้ข้อกำหนดแห่งนโยบายฯ นี้ การฝ่าฝืนข้อกำหนด และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กรหรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่เจ้าหน้าที่ที่ฝ่าฝืนตามความเหมาะสมต่อไป

7.2.2.2 ผู้ใช้งานพึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ Download ไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็นและไม่ควรปฏิบัติในระหว่างเวลาทำงานซึ่งมีการใช้เครือข่ายอย่างหนาแน่น

7.2.2.3 ผู้ใช้งานพึงใช้ข้อความสุภาพและถูกต้องตามธรรมเนียมปฏิบัติในการใช้เครือข่าย เช่น ไม่ส่ง E-mail แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น หรือการใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น เป็นต้น

7.2.2.4 ผู้ใช้งานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่ายโดยเฉพาะอย่างยิ่งไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้งานของตน

7.2.2.5 เพื่อประโยชน์ในการใช้รหัสผ่านส่วนบุคคล ผู้ใช้งานจะต้องใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่เจ้าหน้าที่ครอบครองใช้งานอยู่ระดับระบบปฏิบัติการ (Operating System) โดยรหัสผ่านส่วนบุคคลดังกล่าวต้องเป็นไปตามแนวปฏิบัติข้อ 7.2.1.1

7.2.2.6 ผู้ใช้งานจะต้องไม่ใช้เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ดังต่อไปนี้

- เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
- เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- เพื่อการพาณิชย์
- เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กรหรือบุคคลภายนอกก็ตาม
- เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กรหรือของบุคคลอื่น
- เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิ์ในข้อมูลดังกล่าว
- เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่องค์กร เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้จากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิ์ของบุคคลอื่นไปยังเจ้าหน้าที่หรือบุคคลอื่น เป็นต้น
- เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ขององค์กร หรือของเจ้าหน้าที่อื่นขององค์กรหรือเพื่อให้เครือข่ายคอมพิวเตอร์ขององค์กร ไม่สามารถใช้งานได้ตามปกติ
- เพื่อแสดงความเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กรไปยังที่เว็บไซต์ (Web site) ใด ๆ ในลักษณะที่จะก่อ หรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
- เพื่อการอื่นใดที่อาจขัดต่อประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่องค์กร

7.2.3 ความปลอดภัยทางด้านกายภาพ

7.2.3.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล๊อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

7.2.3.2 ผู้ใช้งานไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

7.2.3.3 ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

7.2.4 นโยบายการเคลียร์โต๊ะทำงานและหน้าจอ

7.2.4.1 ระบบเทคโนโลยีสารสนเทศและการสื่อสารต้องได้รับการควบคุมการตั้งเวลาล็อคหน้าจอ (Screen Lock) เพื่อป้องกันบุคคลผู้ไม่มีสิทธิ์เข้าใช้

7.2.4.2 สารสนเทศที่สำคัญเมื่อไม่มีความจำเป็นต้องใช้งานให้ทำการจัดเก็บออกจากโต๊ะ หรือปิดย่อหน้าจอคอมพิวเตอร์ที่มีสารสนเทศดังกล่าว เพื่อป้องกันการถูกเปิดเผย

7.2.5 การควบคุมการเข้าถึงระบบปฏิบัติการ

7.2.5.1 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

7.2.5.2 ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในแนวทางปฏิบัติในการใช้รหัสผ่าน

7.2.5.3 ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้น เมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

7.2.5.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

7.2.5.5 ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities) เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้ โดยการห้ามผู้ใช้งานใช้โปรแกรม ตรวจจับ/เฝ้าดู/สแกน ข้อมูลภายในเครือข่ายคอมพิวเตอร์ เพื่อดูข้อมูลที่ รับ-ส่ง ผ่านในเครือข่ายคอมพิวเตอร์ ยกเว้น ผู้ที่มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยของเครือข่ายคอมพิวเตอร์

7.2.5.6 ต้องกำหนดให้ระบบตัดการใช้งานของผู้ใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบมาเป็นระยะเวลา 10 นาที

7.2.5.7 ในกรณีที่มีระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีความสำคัญสูง ต้องทำการจำกัดระยะเวลาในการเชื่อมต่อระบบนั้น ๆ เช่น จำกัดระยะเวลาให้เข้าใช้ระบบได้เฉพาะในเวลาราชการ

7.2.5.8 ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน เช่น ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้งานต้อง Logout ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรมรักษาจอภาพ (Screen Saver)

7.2.6 การบริหารจัดการการเข้าถึงเครือข่าย (Network access control)

7.2.6.1 ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ต้องได้รับการควบคุมทางเครือข่าย ดังนี้

- แยกเครือข่ายระหว่างเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องผู้ใช้งาน
- ควบคุมการเข้าถึงและการใช้งานทางเทคนิค
- ควบคุมเส้นทางการรับส่งข้อมูลทางเครือข่าย (Routing)
- ติดตาม ตรวจสอบการเข้าถึงและการใช้งานเครือข่าย

7.2.6.2 การเข้าถึงเครือข่ายคอมพิวเตอร์ภายในองค์กร จากภายนอก ต้องมีการควบคุมการเชื่อมต่อ เช่น มีการระบุชื่อผู้ใช้งานและรหัสผ่าน หรือการขอใช้เครือข่ายส่วนบุคคลเสมือน (VPN) เป็นต้น

7.2.6.3 การนำอุปกรณ์เครือข่ายคอมพิวเตอร์ เช่น สวิทช์ (Switch) อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless network) มาเชื่อมต่อกับเครือข่ายขององค์กร ต้องได้รับการอนุมัติอย่างเป็นทางการและได้รับการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศก่อนดำเนินการ

7.2.6.4 ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

7.2.6.5 การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบเทคโนโลยีสารสนเทศและการสื่อสารก่อนที่จะสามารถใช้งานได้ในทุกกรณี

7.2.6.6 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

7.2.6.7 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

7.2.6.8 ผู้ดูแลระบบ ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

7.2.6.9 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องมีการทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

7.2.6.10 ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กร ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

7.2.6.11 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

7.2.6.12 การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

7.2.6.13 IP address ภายในของระบบงานเครือข่ายภายในขององค์กร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่าย และส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

7.2.6.14 ต้องจัดทำแผนผังระบบเครือข่าย (Network diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

7.2.6.15 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

7.2.6.16 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการหรือควบคุมโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

7.2.7 การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and information access control)

7.2.7.1 ผู้ดูแลระบบต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอปพลิเคชันตามนโยบายการเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ (หมวดที่ 7 นี้) โดยต้องแยกตามประเภทของผู้ใช้งาน การจำกัดสิทธิ์ของผู้ใช้งาน ต้องพิจารณาอยู่บนพื้นฐานความจำเป็นของระบบซอฟต์แวร์แต่ละระบบ โดยมีแนวทางปฏิบัติดังนี้

- เตรียมหน้าจอหรือเมนูสำหรับการควบคุมการเข้าถึงระบบ
- ควบคุมสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน
- ควบคุมสิทธิ์การเข้าถึงข้อมูลของระบบซอฟต์แวร์อื่น

7.2.7.2 เจ้าของระบบงานต้องแยกระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ

7.2.8 การควบคุมการเข้าใช้งานระบบจากภายนอก (Remote access control) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

7.2.8.1 การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กร ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์กร การควบคุมบุคคลที่เข้าสู่ระบบขององค์กรจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

7.2.8.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

7.2.8.3 ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

7.2.8.4 ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม อนุญาตเฉพาะพอร์ตที่จำเป็นต่อการทำงานเท่านั้น หากมีความเสี่ยงเจ้าหน้าที่ผู้รับผิดชอบมีสิทธิ์ระงับการใช้งานทันที

7.2.8.5 การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port ไว้โดยไม่จำเป็น ต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

7.2.9 การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก (User authentication for external connections)

7.2.9.1 ผู้ใช้งานระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

- การแสดงตัวตน (Identification) คือขั้นตอนที่ผู้ใช้งานแสดงชื่อผู้ใช้งาน (Username)
- การพิสูจน์ยืนยันตัวตน (Authentication) คือ วิธีตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB token ที่มีความสามารถ PKI เป็นต้น

7.2.9.2 การเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี

7.2.9.3 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

7.2.10 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

7.2.10.1 ต้องปฏิบัติตามนโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา ในหมวดที่ 6 ของนโยบายฯ ฉบับนี้

7.2.10.2 ถ้าองค์กรมีนโยบายอนุญาตให้เจ้าหน้าที่ปฏิบัติงานจากภายนอกองค์กร ต้องมีมาตรการเพื่อควบคุมการปฏิบัติงานจากภายนอกองค์กรด้วย

หมวดที่ 8

การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(Information systems acquisition, development and maintenance)

วัตถุประสงค์

เพื่อให้การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร ได้พิจารณาถึงประเด็นความมั่นคงปลอดภัยด้านสารสนเทศเป็นองค์ประกอบพื้นฐานที่สำคัญ

8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Security requirements of information systems)

8.1.1 การวิเคราะห์และระบุข้อกำหนดด้านความมั่นคงปลอดภัย

8.1.1.1 เจ้าของระบบและผู้พัฒนาระบบ ต้องวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย ในข้อกำหนดด้านเทคนิคของการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว

8.2 การประมวลผลสารสนเทศในแอปพลิเคชัน (Correct processing in applications)

8.2.1 การตรวจสอบข้อมูลนำเข้า

8.2.1.1 ผู้พัฒนาระบบ ต้องกำหนดกลไกสำหรับตรวจสอบข้อมูลนำเข้าของแอปพลิเคชันว่าข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป

8.2.1.2 เจ้าของสารสนเทศ ต้องนำเข้า ปรับปรุง สารสนเทศ ให้ครบถ้วน ถูกต้อง เชื่อถือได้ และเป็นปัจจุบัน

8.2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล

8.2.2.1 ผู้พัฒนาระบบ ต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ เช่น อาจมีสาเหตุจากความผิดพลาดในการประมวลผล การกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น

8.2.3 การตรวจสอบความถูกต้องของข้อความ

8.2.3.1 ผู้พัฒนาระบบ ต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอปพลิเคชัน เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้องรวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต

8.2.4 การตรวจสอบข้อมูลนำออก

8.2.4.1 ผู้พัฒนาระบบ ต้องกำหนดกลไกสำหรับการตรวจสอบข้อมูลนำออกจากแอปพลิเคชัน เพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม

8.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic controls)

8.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล

8.3.1.1 ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ให้พิจารณาใช้มาตรการควบคุมความลับและความถูกต้องของสารสนเทศ โดยเทคนิคการเข้ารหัสลับ เช่น การใช้งาน Secure Socket Layer (SSL) หรือการใส่รหัสผ่านในไฟล์อิเล็กทรอนิกส์ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าถึง เป็นต้น

8.3.1.2 ให้พิจารณาถึงการควบคุมกุญแจที่ใช้สำหรับการเข้ารหัสข้อมูล โดยครอบคลุมการสร้าง การจัดเก็บ การจัดส่ง และการแก้ไขเปลี่ยนแปลง

8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files)

8.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ

8.4.1.1 ต้องจัดให้มีขั้นตอนการปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่าง ๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้ เพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการนั้นเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้

8.4.2 การป้องกันข้อมูล ที่ใช้สำหรับทดสอบ

8.4.2.1 ผู้พัฒนาระบบ ต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการสำหรับทำการทดสอบระบบ หากมีความจำเป็นต้องใช้ ต้องกำหนดให้มีการป้องกันและควบคุมการใช้งาน เช่น ต้องลบทิ้งบางส่วนของข้อมูลที่เป็นความลับ ข้อมูลส่วนตัว หรือข้อมูลสำคัญ

8.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ

8.4.3.1 เจ้าของระบบและผู้ดูแลระบบ ต้องจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ ทั้งนี้ เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้น โดยไม่ได้รับอนุญาตหรือโดยไม่เจตนา

8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in Development and support processes)

8.5.1 ขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ

8.5.1.1 ต้องกำหนดขั้นตอนการปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งนี้ เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้

8.5.2 การตรวจสอบการทำงานของแอปพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

8.5.2.1 ผู้ดูแลระบบ ต้องทำการตรวจสอบทางเทคนิคภายหลังจากที่ทำการเปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าแอปพลิเคชันที่ทำงานอยู่บนระบบปฏิบัติการนั้น ทำงานผิดปกติ ไม่สามารถใช้งานได้ หรือมีปัญหาทางด้านความมั่นคงปลอดภัยเกิดขึ้นหรือไม่

8.5.3 การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต

8.5.3.1 ต้องหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นต้องแก้ไขต้องแก้ไขตามความจำเป็นเท่านั้น และต้องมีการควบคุมการแก้ไขนั้นอย่างเข้มงวดด้วย

8.5.4 การป้องกันการรั่วไหลของสารสนเทศ

8.5.4.1 ต้องกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กร หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป และในกรณีที่ต้องมีการทำงานร่วมกับบุคคลหรือหน่วยงานภายนอกที่จำเป็นต้องเข้าถึงสารสนเทศ หรือระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ให้บุคคลภายนอกลงนามไม่เปิดเผยข้อมูลจากการทำงาน (Non-Disclosure Agreement)

8.5.5 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

8.5.5.1 ต้องกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก และในกรณีที่จ้างให้จัดทำระบบงานหรือซอฟต์แวร์ หรือได้พัฒนาเพิ่มเติมจากโปรแกรมสำเร็จรูป ให้กำหนดในข้อตกลงการจ้างว่า ระบบงานหรือซอฟต์แวร์ที่พัฒนาขึ้นนั้นต้องเป็นลิขสิทธิ์ขององค์กร และต้องส่งมอบซอร์สโค้ดนั้นให้องค์กรด้วย

8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

8.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค

8.6.1.1 ต้องกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

8.6.2 มาตรการการทดสอบด้านความมั่นคงปลอดภัย

8.6.2.1 ต้องกำหนดให้มีการตรวจสอบด้านความมั่นคงปลอดภัย เช่น การตรวจสอบช่องโหว่ทางเทคนิค (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Testing) ระบบสารสนเทศที่มีความสำคัญ

หมวดที่ 9
การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด
(Information security incident management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)

9.1.1 หากผู้ใช้งานพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัย หรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัย หรือการทำงานที่ผิดปกติของซอฟต์แวร์ ผู้ใช้งานต้องรายงานสิ่งที่เกิดขึ้นให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบโดยเร็วที่สุดเท่าที่จะทำได้

9.1.2 ในกรณีที่ไม่สามารถติดต่อกับผู้ดูแลระบบได้ ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้นและรายงานให้หน่วยงานดูแลรับผิดชอบได้ทราบด้วย

9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)

9.2.1 ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

9.2.2 ผู้ดูแลระบบ ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้นจากความเสียหาย เพื่อที่จะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้วและเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

9.2.3 ต้องรวบรวมและจัดเก็บหลักฐานตามกฎ ระเบียบ หรือข้อบังคับที่กำหนดเอาไว้ สำหรับการอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

9.2.4 ผู้ดูแลระบบ มีหน้าที่รายงานเหตุการณ์ที่น่าสงสัยว่าเป็นเหตุการณ์ละเมิดความมั่นคงปลอดภัย เช่น เหตุการณ์ต่อไปนี้

9.2.4.1 พบว่ารหัสผ่านส่วนบุคคลของตนถูกล็อกโดยไม่ทราบสาเหตุ

9.2.4.2 เวลาการเข้าใช้งานระบบครั้งล่าสุดผิดปกติ

9.2.4.3 มีความพยายามที่จะเข้าใช้ระบบอย่างผิดวิธี ไม่ว่าจะสำเร็จหรือไม่

9.2.4.4 มีการแก้ไขค่าความปลอดภัยในระบบโดยผู้ดูแลระบบไม่ทราบ

9.2.5 ผู้ใช้งานมีหน้าที่รายงานเหตุการณ์ที่น่าสงสัยว่าเป็นเหตุการณ์ละเมิดความมั่นคงปลอดภัย เช่น เหตุการณ์ต่อไปนี้

9.2.5.1 พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน เช่น มีไฟล์ที่ไม่รู้จัก การเปลี่ยนแปลงของค่าต่าง ๆ

9.2.5.2 พบหรือคาดว่าสารสนเทศในระบบถูกทำลาย แก้ไข หรือลบทิ้ง

9.2.5.3 การให้บริการของระบบเกิดการชะงัก หรือไม่สามารถให้บริการได้

9.2.5.4 เกิดการละเมิดสิทธิ์เข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล

หมวดที่ 10
การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง (Business continuity management)

วัตถุประสงค์

เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานขององค์กร และป้องกันกระบวนการที่สำคัญต่อการดำเนินงานขององค์กรอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

10.1 หัวข้อพื้นฐานสำหรับการบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง (Information security aspects of business continuity management)

10.1.1 กระบวนการในการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

10.1.1.1 ต้องกำหนดให้มีกระบวนการในการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง และทำการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ กระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

10.1.2 การประเมินความเสี่ยงในการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

10.1.2.1 ต้องระบุเหตุการณ์ที่สามารถทำให้การดำเนินงานของหน่วยงานหรือองค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสการเกิดของเหตุการณ์ ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

10.1.3 การจัดทำและการใช้งานแผนการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

10.1.3.1 ต้องจัดทำแผนการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่องให้สามารถดำเนินการต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้การดำเนินงานของหน่วยงานหรือองค์กรเกิดการติดขัด หยุดชะงัก หรือล้มเหลว ในระบบงานหลักเจ้าของระบบจะต้องจัดให้มีแผนสำรองฉุกเฉิน (Contingency plan) และแผนกู้คืนระบบ (Disaster recovery plan) ให้สอดคล้องกับแผนการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง (Business continuity plan)

10.1.3.2 ต้องทำการทดสอบแผนสำรองฉุกเฉินและแผนกู้คืนระบบก่อนนำไปใช้จริง รวมถึงต้องมีการปรับปรุงให้ทันสมัยอย่างสม่ำเสมอ และต้องมีการจัดทำเป็นเอกสารประกอบ มีการจัดทำสำเนาและจัดเก็บไว้ในสถานที่ที่ปลอดภัย เพื่อให้สามารถนำมาใช้งานได้เมื่อมีเหตุการณ์

10.1.4 การกำหนดกรอบสำหรับการวางแผนการดำเนินงานของหน่วยงานหรือองค์กร เพื่อให้มีความต่อเนื่อง

10.1.4.1 ต้องกำหนดกรอบสำหรับการวางแผนการดำเนินงานของหน่วยงานหรือองค์กร เพื่อให้มีความต่อเนื่อง เพื่อให้แผนงานทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่าง ๆ ที่ต้องดำเนินการ

10.1.5 การทดสอบและการปรับปรุงแผนการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

10.1.5.1 ต้องกำหนดให้มีการทดสอบและปรับปรุงแผนการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่องอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลที่ดี

10.2 **ต้องพิจารณาถึงประเด็นด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง** เช่น สิทธิ์ของบุคลากรที่สามารถเข้าถึงสถานที่ ความปลอดภัยของพื้นที่ปฏิบัติงานในกรณีฉุกเฉิน เป็นต้น

หมวดที่ 11

การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

(Compliance)

วัตถุประสงค์

เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุด และมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการการดำเนินงานขององค์กรน้อยที่สุด

11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)

11.1.1 การระบุข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย

11.1.1.1 ต้องระบุข้อกำหนดทางด้านกฎหมาย ระเบียบปฏิบัติ และสัญญาว่าจ้าง รวมทั้งสัญญาที่ทำกับหน่วยงานภายนอก ที่เกี่ยวข้องกับการดำเนินงานขององค์กร ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร โดยในเบื้องต้น ข้อกำหนดทางด้านกฎหมายที่มีความเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ มีดังนี้

1) พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537
2) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
3) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544
4) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
5) พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
6) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
7) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550
8) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551
9) พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553
10) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

11) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
12) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
13) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556
14) พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558
15) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องรายชื่อหน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559
16) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
17) ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต

11.1.1.2 ต้องทำการปรับปรุงข้อกำหนดทางกฎหมายที่ได้บันทึกไว้เป็นลายลักษณ์อักษรให้ทันสมัยอยู่เสมอ

11.1.2 การป้องกันสิทธิ์และทรัพย์สินทางปัญญา

11.1.2.1 ให้มีหน่วยงานที่ต้องดำเนินการควบคุมการใช้ลิขสิทธิ์ซอฟต์แวร์ โดยต้องมีขั้นตอนการปฏิบัติที่ชัดเจนและมีการวางแผนการบริหารลิขสิทธิ์ซอฟต์แวร์เพื่อป้องกันการละเมิดลิขสิทธิ์

11.1.3 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร

11.1.3.1 เจ้าหน้าที่ ต้องปฏิบัติตามนโยบายต่าง ๆ ที่ได้ระบุไว้ในนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับนี้

11.1.4 การป้องกันข้อมูลส่วนตัว

11.1.4.1 ผู้ดูแลระบบ ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัวของเจ้าหน้าที่ เช่น ข้อมูลในไปรษณีย์อิเล็กทรอนิกส์ ข้อมูลในระบบบริหารงานบุคคล เป็นต้น เพื่อใช้เป็นหลักฐานอ้างอิงในทางกฎหมายในกรณีที่มีข้อพิพาทกัน

11.1.5 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์

11.1.5.1 อุปกรณ์ประมวลผลสารสนเทศขององค์กร มีไว้เพื่อใช้ในการดำเนินงานขององค์กรเท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บริหารขององค์กร

11.1.5.2 ผู้ใช้งานต้องไม่ทำการเปลี่ยนแปลงแก้ไข หรืออนุญาตให้ผู้ที่ไม่ได้รับอนุญาตทำการเปลี่ยนแปลงแก้ไขซอฟต์แวร์หรือประมวลผลสารสนเทศในอุปกรณ์ที่ตนรับผิดชอบ

11.1.5.3 ไม่อนุญาตให้ผู้ใช้งานติดตั้งซอฟต์แวร์หรืออุปกรณ์ในเครื่องคอมพิวเตอร์ขององค์กร การเปลี่ยนแปลงต่อระบบคอมพิวเตอร์ ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูล จะต้องได้รับอนุมัติจากหัวหน้าหน่วยงานที่ดูแลระบบงานนั้น ๆ เป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการดำเนินงานขององค์กร หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

11.1.6 การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด

11.1.6.1 หน่วยงานต่าง ๆ ที่เป็นเจ้าของข้อมูล ต้องใช้มาตรการการเข้ารหัสข้อมูลตามที่ได้กำหนดไว้

11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance)

11.2.1 การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย

ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information security audit and assessment) อย่างน้อยปีละ 1 ครั้ง ซึ่งต้องทำการตรวจสอบและประเมินความเสี่ยงเกี่ยวกับการสร้างความมั่นคงปลอดภัยในแต่ละด้านดังต่อไปนี้

11.2.1.1 การตรวจสอบและประเมินด้านบริหารจัดการ

11.2.1.2 การตรวจสอบและประเมินความพร้อมทางด้านการจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

11.2.1.3 การตรวจสอบและประเมินด้านการบริหารจัดการทรัพย์สินสารสนเทศ

11.2.1.4 การตรวจสอบและประเมินด้านบุคลากร

11.2.1.5 การตรวจสอบและประเมินด้านกายภาพและสภาพแวดล้อม

11.2.1.6 การตรวจสอบและประเมินด้านการสื่อสารและการดำเนินงาน

11.2.1.7 การตรวจสอบและประเมินการควบคุมการเข้าถึง

11.2.1.8 การตรวจสอบและประเมินด้านการจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบ

11.2.1.9 การตรวจสอบและประเมินด้านการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

11.2.1.10 การตรวจสอบและประเมินด้านการบริหารจัดการด้านการบริการหรือการดำเนินงานขององค์กรเพื่อให้มีความต่อเนื่อง

11.2.1.11 การตรวจสอบและประเมินด้านการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

เมื่อได้มีการประเมินความเสี่ยงด้านต่าง ๆ แล้ว ต้องดำเนินการจัดลำดับความสำคัญของความเสี่ยงนั้น และค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยงนั้น (Control) พร้อมทั้งข้อดีข้อเสียของวิธีการเหล่านั้น เพื่อให้ผู้บริหารขององค์กรตัดสินใจ ที่จะเลือกวิธีการดำเนินการเพื่อลดความเสี่ยงหรือเลือกที่จะยอมรับความเสี่ยงนั้น เมื่อเลือกวิธีการดำเนินการเพื่อลดความเสี่ยง (Control selection) แล้ว ผู้บริหารขององค์กรต้องจัดสรรทรัพยากรอย่างเพียงพอเพื่อดำเนินการ แนวทางการดำเนินการเพื่อลดความเสี่ยงซึ่งมีหลายวิธี สามารถแบ่งได้เป็นสามรูปแบบคือ การเลือกใช้เทคโนโลยี (Technology) การปรับเปลี่ยนกระบวนการ (Procedure) และการกำหนดให้เจ้าหน้าที่ดำเนินการปฏิบัติ (Person)

สำหรับการเลือกใช้วิธีการนำเทคโนโลยีมาใช้ในการลดความเสี่ยงเพื่อเพิ่มความมั่นคงปลอดภัยให้กับข้อมูลและระบบข้อมูลเป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ไฟร์วอลล์ มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้อุปกรณ์สมาร์ทการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอกองค์กร เป็นต้น

สำหรับการเลือกใช้วิธีการปรับเปลี่ยนกระบวนการ (Procedure) ก็อาจจำเป็นต้องมีการออกแบบกระบวนการใหม่ที่รัดกุมและสามารถรักษาความมั่นคงปลอดภัยของข้อมูลได้ดีขึ้น เมื่อออกแบบกระบวนการใหม่แล้วต้องมีการพิจารณาหารือความเหมาะสม ความเป็นไปได้ และผู้บริหารขององค์กรจะต้องเป็นผู้อนุมัติให้มีการบังคับใช้กระบวนการใหม่นั้น โดยอาจจำเป็นต้องมีการประชาสัมพันธ์ให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งอาจจำเป็นต้องมีการจัดฝึกอบรมเจ้าหน้าที่ที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามกระบวนการใหม่ได้อย่างราบรื่นและมีประสิทธิภาพ

11.3 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร

11.3.1 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดให้มีการตรวจสอบระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร

11.3.1.1 ผู้ดูแลระบบ ต้องขออนุญาตหัวหน้าหน่วยงานในกรณีที่มีการร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ในการประเมิน ตรวจสอบ ทดสอบหาช่องโหว่ อันเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ และทำการแก้ไขได้อย่างรวดเร็ว

11.3.1.2 ต้องมีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศ

11.4 การตรวจประเมินระบบเทคโนโลยีสารสนเทศและการสื่อสาร(Information systems audit considerations)

11.4.1 มาตรการการตรวจประเมินระบบเทคโนโลยีสารสนเทศและการสื่อสาร

11.4.2 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อการดำเนินงานขององค์กร

11.5 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบเทคโนโลยีสารสนเทศและการสื่อสาร

11.5.1 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบเทคโนโลยีสารสนเทศและการสื่อสาร เช่น ซอฟต์แวร์ที่ใช้ในการตรวจประเมิน เพื่อป้องกันการใช้งานผิดวัตถุประสงค์ หรือการเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต

หมวดที่ 12
การบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอก
(Supplier Relationships)

วัตถุประสงค์

เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่สามารถเข้าถึงได้โดยหน่วยงานภายนอก และเพื่อให้มีการรักษาไว้ ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของหน่วยงานภายนอก

12.1 ความมั่นคงปลอดภัยด้านสารสนเทศกับความสัมพันธ์กับหน่วยงานภายนอก (Information security in supplier relationships)

12.1.1 หน่วยงานภายนอกที่เข้าถึงสารสนเทศของหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร (Non-Disclosure Agreement)

12.1.2 ผู้อำนวยการศูนย์เทคโนฯ ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร อุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

12.1.3 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนสารสนเทศและการสื่อสาร

12.1.4 จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

- เหตุผลในการขอใช้
- ระยะเวลาในการใช้
- การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
- การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
- การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

12.1.5 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูลขององค์กร

12.1.6 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงสารสนเทศของหน่วยงาน ต้องมีการสื่อสารมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้หน่วยงานภายนอกรับทราบและปฏิบัติตาม

12.1.7 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

12.1.8 องค์กรมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

12.1.9 ต้องดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

12.1.10 ต้องมีการตรวจรับงานของผู้ให้บริการที่ครอบคลุมถึงความมั่นคงปลอดภัยด้านสารสนเทศ

12.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

12.2.1 เจ้าของโครงการต้องติดตามและตรวจทานการดำเนินงานของหน่วยงานภายนอกอย่างสม่ำเสมอ

12.2.2 เจ้าของโครงการต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยด้านสารสนเทศหากหน่วยงานภายนอกมีการเปลี่ยนแปลงรายละเอียดเกี่ยวกับการให้บริการ เช่น นโยบายการให้บริการ หรือเทคโนโลยีของการให้บริการ เป็นต้น

12.2.3 ต้องมีการกำหนดให้ผู้ให้บริการรายงานปัญหาต่าง ๆ และแนวทางการแก้ไขในการปฏิบัติงาน หรือมีการอัปเดตเทคโนโลยีที่เกี่ยวข้องกับระบบงาน และเข้ามามีส่วนร่วมกับการพัฒนาระบบการดำเนินงานขององค์กรเพื่อให้มีความต่อเนื่อง

หมวดที่ 13
การตั้งค่าเครื่องตามนโยบาย

วัตถุประสงค์

เพื่อกำหนดหลักเกณฑ์ในการตั้งค่าเครื่องของผู้ดูแลระบบ ผู้ใช้งาน และเครื่องคอมพิวเตอร์แม่ข่าย เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยในการเข้าใช้งานระบบ

13.1 การตั้งค่าเครื่องของผู้ดูแลระบบ

13.1.1 ผู้ดูแลระบบต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาไม่เกิน 10 นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้น เมื่อต้องการใช้งานผู้ดูแลระบบต้องใส่รหัสผ่าน

13.1.2 ผู้ดูแลระบบต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด ทุก 3 เดือน

13.1.3 ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งไม่ควรเกิน 10 ครั้ง

13.1.4 ผู้ดูระบบต้องกำหนดช่วงเวลาในการระงับบัญชีผู้ใช้งานที่มีการกรอกรหัสผิดพลาดเกินจำนวนครั้งที่ได้ตั้งไว้ตาม ข้อ 13.1.3 โดยกำหนดการตั้งค่าเวลาการยกเลิกการระงับไม่น้อยกว่า 10 นาที ทั้งนี้ หากระบบไม่สามารถตั้งค่าดังกล่าวได้ให้ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเป็นผู้ยกเลิกการระงับ

13.1.5 การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ผู้ดูแลระบบต้องปฏิบัติตาม ข้อ 7.2.1 แนวทางปฏิบัติในการใช้รหัสผ่าน

13.2 การตั้งค่าเครื่องของผู้ใช้งาน

13.2.1 ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาไม่เกิน 10 นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้น เมื่อต้องการใช้งานผู้ดูแลระบบต้องใส่รหัสผ่าน

13.2.2 ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด ทุก 6 เดือน

13.2.3 ผู้ใช้งานต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งไม่ควรเกิน 10 ครั้ง

13.2.4 ผู้ใช้งานต้องกำหนดช่วงเวลาในการระงับบัญชีผู้ใช้งานที่มีการกรอกรหัสผิดพลาดเกินจำนวนครั้งที่ได้ตั้งไว้ตาม ข้อ 13.2.3 โดยกำหนดการตั้งค่าเวลาการยกเลิกการระงับไม่น้อยกว่า 10 นาที ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเป็นผู้ยกเลิกการระงับ

13.2.5 การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ผู้ใช้งานต้องปฏิบัติตาม ข้อ 7.2.1 แนวทางปฏิบัติในการใช้รหัสผ่าน

13.3 การตั้งค่าเครื่องคอมพิวเตอร์แม่ข่ายของผู้ดูแลระบบ

13.3.1 ผู้ดูแลระบบต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด ทุก 3 เดือน

13.3.2 ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งไม่ควรเกิน 10 ครั้ง

13.3.3 ผู้ดูระบบต้องกำหนดช่วงเวลาในการระงับบัญชีผู้ใช้งานที่มีการกรอกรหัสผิดพลาดเกินจำนวนครั้งที่ได้ตั้งไว้ตาม ข้อ 13.3.2 โดยกำหนดการตั้งค่าเวลาการยกเลิกการระงับไม่น้อยกว่า 10 นาที ทั้งนี้ หากระบบไม่สามารถตั้งค่าดังกล่าวได้ให้ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเป็นผู้ยกเลิกการระงับ

13.3.4 การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ผู้ดูแลระบบต้องปฏิบัติตาม ข้อ 7.2.1 แนวทางปฏิบัติในการใช้รหัสผ่าน

13.3.5 การควบคุมการเข้าถึง มีการกำหนดสิทธิและทบทวนสิทธิ์ของผู้ใช้งานงานตามนโยบาย โดยสามารถเข้าถึงได้ตามที่ได้สิทธิและตามระยะเวลาที่ขออนุญาตเท่านั้น

13.3.6 ผู้ดูแลระบบ ต้องดำเนินการตรวจสอบการตั้งค่าระบบตามนโยบายอย่างน้อยปีละ 1 ครั้ง

หมวดที่ 14
การรักษาความมั่นคงปลอดภัยคุกคามทางไซเบอร์
(Cyber Security)

วัตถุประสงค์

เพื่อป้องกันเหตุการณ์ต่าง ๆ จากการคุกคามทางไซเบอร์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร เพื่อให้เชื่อว่ามั่นว่าเหตุการณ์ภัยคุกคามต่าง ๆ ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม มีวิธีการที่สอดคล้องและมีประสิทธิภาพในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

14.1 การรายงานเหตุการณ์การคุกคามทางไซเบอร์

14.1.1 ผู้ใช้งานพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัย หรือเหตุการณ์ที่อาจจะทำให้เกิดผลกระทบต่อความมั่นคงปลอดภัย หรือจนก่อให้เกิดการทำงานที่ผิดปกติต่อระบบสารสนเทศ ต้องรายงานสิ่งที่เกิดขึ้นให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบโดยเร็วที่สุด

14.1.2 กรณีที่ไม่สามารถติดต่อกับผู้ดูแลระบบได้ ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้นและรายงานให้หน่วยงานดูแลรับผิดชอบได้ทราบด้วย

14.2 ผู้ดูแลระบบต้องประเมินการคุกคามทางไซเบอร์ 3 ระดับ ดังนี้

14.2.1 ระดับไม่ร้ายแรง หมายถึงความเสี่ยงอย่างมีนัยสำคัญจนถึงทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญและบริการของรัฐด้อยประสิทธิภาพ

14.2.2 ระดับร้ายแรง หมายถึง ภัยคุกคามที่โจมตีระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์อันทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศได้รับความเสียหายจนไม่อาจใช้การได้ ซึ่งมีผลกระทบทั้งการบริการ ความมั่นคง ตลอดถึงความสัมพันธ์ระหว่างประเทศ

14.2.3 ระดับวิกฤติ หมายถึง ภัยคุกคามที่ส่งผลต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างกว้างทำให้ล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานของระบบคอมพิวเตอร์ได้ หรือภัยคุกคามที่มีผลกระทบต่อความสงบเรียบร้อยของประชาชน หรือความมั่นคงของรัฐ

14.3 ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติเพื่อรับมือกับเหตุการณ์การคุกคามทางไซเบอร์และขั้นตอนดังกล่าว ต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

14.4 ผู้ดูแลระบบ ต้องบันทึกเหตุการณ์การคุกคามทางไซเบอร์ ปริมาณที่เกิดขึ้นจากความเสียหายเพื่อที่จะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

14.5 ต้องรวบรวมและจัดเก็บหลักฐานตามกฎ ระเบียบ หรือข้อบังคับที่กำหนดเอาไว้ สำหรับการอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

หมวดที่ 15
การรักษาความมั่นคงปลอดภัยคุ้มครองข้อมูลส่วนบุคคล
(Privacy Security)

วัตถุประสงค์

เพื่อการบริหารจัดการข้อมูลส่วนบุคคลของกรมบัญชีกลางให้มีความมั่นคงปลอดภัย และสร้างความมั่นใจว่าข้อมูลส่วนบุคคลจะได้รับการดูแล ปกป้อง และรักษาความมั่นคงปลอดภัยจาก ภาวะคุกคามต่างๆ ซึ่งองค์กรต้องกำหนดทิศทางรองรับอย่างชัดเจน ที่สนับสนุน และมีการนำไปใช้จริง เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีความปลอดภัย

15.1 เจ้าของข้อมูลต้องให้ความยินยอม (consent) ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล โดยต้องเป็นไปตามวัตถุประสงค์ที่แจ้งไว้กับเจ้าของข้อมูลและ consent ต้องประกอบด้วย

15.1.1 ทำโดยชัดแจ้งเป็นหนังสือหรือผ่านระบบ electronic

15.1.2 แจ้งวัตถุประสงค์ และ Consent ต้องแยกส่วนจากข้อความอื่นอย่างชัดเจน

15.1.3 ข้อความต้องเข้าใจง่าย ไม่หลอกลวงหรือทำให้เข้าใจผิด

15.2 การเก็บข้อมูลส่วนบุคคลต้องเก็บข้อมูลเท่าที่จำเป็นเท่านั้น จากเจ้าของข้อมูลโดยตรง กรณีที่เก็บรวบรวมข้อมูลจากแหล่งอื่นต้องแจ้งเจ้าของข้อมูลทราบไม่เกิน 30 วันนับแต่วันที่เก็บรวมรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล รายละเอียดที่ต้องแจ้งให้เจ้าของข้อมูลทราบ

15.2.1 วัตถุประสงค์และระยะเวลาของการเก็บข้อมูล

15.2.2 กรณีที่ต้องให้ข้อมูลตามกฎหมายและผลกระทบของการไม่ให้ข้อมูล

15.2.3 ข้อมูลติดต่อกับผู้ควบคุมข้อมูล

15.3 ข้อมูลส่วนบุคคลที่ห้ามเก็บ (sensitive Data) เช่น ความเชื่อ/ศาสนา เชื้อชาติ ความคิดเห็นทางการเมือง ประวัติอาชญากรรม เผ่าพันธุ์ สุขภาพ พฤติกรรมทางเพศ ความพิการข้อมูลชีวภาพ ซึ่งเป็นไปตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เว้นแต่ เพื่อป้องกัน/ระงับอันตรายต่อชีวิต เป็นกิจกรรมที่ชอบโดยกฎหมาย ข้อมูลที่เปิดเผยสาธารณะโดยได้รับความยินยอมเพื่อก่อตั้งสิทธิเรียกร้องและเพื่อปฏิบัติตามกฎหมาย เว้นแต่เป็นไปตามนโยบายของรัฐและภารกิจที่องค์กรได้รับมอบหมาย

15.4 สิทธิของเจ้าของข้อมูลส่วนบุคคล

15.4.1 การเข้าถึง/ขอสำเนาและขอให้เปิดเผยการได้มาของข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม แต่ผู้ควบคุมข้อมูลสามารถปฏิเสธได้ตามกฎหมาย คำสั่งศาล หรือก่อให้เกิดความเสียหายแก่สิทธิและเสรีภาพของผู้อื่น

15.4.2 ขอให้จัดทำข้อมูลให้ถูกต้อง ผู้ควบคุมข้อมูลต้องทำให้ถูกต้องให้เป็นปัจจุบันและไม่ก่อให้เกิดความเข้าใจผิด

15.4.3 การร้องเรียน กรณีผู้ควบคุมข้อมูล/ผู้ประมวลผลข้อมูลฝ่าฝืนข้อกำหนดใน พ.ร.บ.ฉบับนี้ ซึ่งกระบวนการ

15.4.4 การส่ง/โอนข้อมูล ผู้ควบคุมข้อมูลส่งหรือโอนข้อมูลไปยังผู้ควบคุมอื่นโดยอัตโนมัติขอรับข้อมูลที่ส่ง/โอนให้ผู้ควบคุมอื่น ทั้งนี้ ผู้ควบคุมข้อมูลต้องทำข้อมูลให้อยู่ในรูปแบบที่อ่านหรือใช้งานได้โดยอัตโนมัติ

15.4.5 ขอให้ลบ/ทำลายข้อมูล ข้อมูลหมดความจำเป็นตามวัตถุประสงค์ การถอนความยินยอม การคัดค้านการเก็บ ใช้เปิดเผยข้อมูล การเก็บ การใช้ เปิดเผยข้อมูลโดยไม่ชอบด้วยกฎหมาย

15.4.6 คัดค้านการเก็บ ใช้ เปิดเผยข้อมูล การเก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรงเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาทางการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ

15.5 หน้าที่ของผู้ควบคุมข้อมูล

15.5.1 กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล

15.5.2 ป้องกันการใช้หรือเปิดเผยโดยมิชอบ

15.5.3 การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มีหน้าที่ในการแนะนำการปฏิบัติตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตรวจสอบการดำเนินงาน ประสานงานกับส านักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เมื่อเกิดปัญหา และการรักษาความลับของข้อมูล

15.5.4 บันทึกรายการเพื่อให้ตรวจสอบได้ เช่น การเก็บข้อมูลส่วนบุคคล วัตถุประสงค์ของการเก็บข้อมูล ระยะเวลาการเก็บข้อมูล ข้อมูลมาตรฐานการรักษาความมั่นคงปลอดภัย

15.5.5 แจ้งเหตุการณ์ละเมิดแก่สำนักงานภายใน 72 ชั่วโมง

15.5.6 มีระบบตรวจสอบเพื่อลบ/ทำลายข้อมูล หากพ้นระยะเวลาการเก็บ การเก็บเกินความจำเป็น หรือเจ้าของข้อมูลร้องขอ

หมวดที่ 16
การยกเว้นการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ (Policy Deviation)

วัตถุประสงค์

เพื่อกำหนดขั้นตอนการขอยกเว้นการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมบัญชีกลาง สำหรับผู้รับผิดชอบหรือผู้ดูแลระบบในกรณีที่มีมาตรการที่ไม่สามารถปฏิบัติตามได้ โดยมีสาเหตุมาจากข้อจำกัดบางประการ โดยเสนอผู้มีอำนาจในการพิจารณาอนุมัติในการขอยกเว้น และใช้เป็นหลักฐานนำมาทบทวนความเสี่ยงหรือปรับปรุงพัฒนาในข้อจำกัดดังกล่าวในอนนาคต

16.1 ในกรณีมีข้อจำกัด ไม่สามารถปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมบัญชีกลาง ผู้รับผิดชอบหรือผู้ดูแลระบบจะต้องแจ้งเหตุผลและความจำเป็นสำหรับการขอยกเว้น รวมถึงมาตรการควบคุมในปัจจุบัน โดยเสนอผ่านทางฝ่ายเลขานุการคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อขออนุมัติจากคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Committee: ISMS Committee) เป็นผู้พิจารณาอนุมัติ

16.2 ฝ่ายเลขานุการคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ ดำเนินการเก็บหลักฐานการขออนุมัติการขอยกเว้นการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมบัญชีกลาง ทั้งที่ได้รับการอนุมัติและไม่ได้รับการอนุมัติ

16.3 ฝ่ายเลขานุการคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศต้องดำเนินการติดตามการปรับปรุงการขอยกเว้นการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมบัญชีกลาง ว่าผู้รับผิดชอบหรือผู้ดูแลระบบสามารถปฏิบัติตามนโยบายฯ ได้แล้ว หรือยังคงสภาพการขอยกเว้นการปฏิบัติตามนโยบายฯ

ภาคผนวก ก

ข้อกำหนดของมาตรฐาน ISO/IEC 27001: 2013 (Requirement)

เลขมาตรฐาน	หัวข้อ	ข้อกำหนด
ISO 27001	A.5.1.1	Policies for information security A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
ISO 27001	A.5.1.2	Review of the policies for information security The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
ISO 27001	A.6.2.1	Mobile device policy A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
ISO 27001	A.6.2.2	Teleworking A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.
ISO 27001	A.9.1.1	Access control policy An access control policy shall be established, documented and reviewed based on business and information security requirements.
ISO 27001	A.10.1.1	Policy on the use of cryptographic controls A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
ISO 27001	A.10.1.2	Key management

เลขมาตรฐาน	หัวข้อ	ข้อกำหนด
		A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
ISO 27001	A.11.2.9	Clear desk and clear screen policy A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
ISO 27001	A.12.3.1	Information Backup Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
ISO 27001	A.13.2.1	Information transfer policies and procedures Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
ISO 27001	A.14.2.1	Secure development policy Rules for the development of software and systems shall be established and applied to developments within the organization.
ISO 27001	A.15.1.1	Information security policy for supplier relationships Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

ภาคผนวก ข

ข้อกำหนดทางด้านกฎหมาย

กฎหมาย	มาตรา	รายละเอียด
พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และฉบับที่ 2 พ.ศ. 2558	มาตรา 27	หากหน่วยงานกระทำอย่างใดอย่างหนึ่งแก่งานอันมีลิขสิทธิ์ตามพระราชบัญญัตินี้ โดยไม่ได้รับอนุญาตตามมาตรา 15 (5) ให้ถือว่าเป็นการละเมิดลิขสิทธิ์ ถ้าได้กระทำดังต่อไปนี้ (1) ทำซ้ำหรือดัดแปลง (2) เผยแพร่ต่อสาธารณชน
	มาตรา 30	หากหน่วยงานกระทำอย่างใดอย่างหนึ่งแก่โปรแกรมคอมพิวเตอร์อันมีลิขสิทธิ์ตามพระราชบัญญัตินี้ โดยไม่ได้รับอนุญาตตามมาตรา 15 (5) ให้ถือว่าเป็นการละเมิดลิขสิทธิ์ ถ้าได้กระทำดังต่อไปนี้ (1) ทำซ้ำหรือดัดแปลง (2) เผยแพร่ต่อสาธารณชน (3) ให้เช่าต้นฉบับหรือสำเนางานดังกล่าว
พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540	มาตรา 7	**การเปิดเผยข้อมูลข่าวสาร** หน่วยงานของรัฐต้องส่งข้อมูลข่าวสารของราชการอย่างน้อยดังต่อไปนี้ ลงพิมพ์ในราชกิจจานุเบกษา (1) โครงสร้างและการจัดองค์กรในการดำเนินงาน (2) สรุปอำนาจหน้าที่ที่สำคัญและวิธีการดำเนินงาน (3) สถานที่ติดต่อเพื่อขอรับข้อมูลข่าวสาร หรือคำแนะนำในการติดต่อกับหน่วยงานของรัฐ (4) กฎ มติคณะรัฐมนตรี ข้อบังคับ คำสั่ง หนังสือเวียน ระเบียบ แบบแผน นโยบาย หรือการตีความ (5) ข้อมูลข่าวสารอื่นตามที่คณะกรรมการกำหนด
	มาตรา 9	ภายใต้บังคับมาตรา 14 และมาตรา 15 หน่วยงานของรัฐต้องจัดให้มีข้อมูลข่าวสารของราชการอย่างน้อยดังต่อไปนี้ไว้ให้ประชาชนเข้าตรวจดูได้ (1) ผลการพิจารณาหรือคำวินิจฉัยที่มีผลโดยตรงต่อเอกชน รวมทั้งความเห็นแย้งและคำสั่งที่เกี่ยวข้องในการพิจารณาวินิจฉัยดังกล่าว

กฎหมาย	มาตรา	รายละเอียด
		(2) นโยบายหรือการตีความที่ไม่เข้าข่ายต้องลงพิมพ์ในราชกิจจานุเบกษา ตามมาตรา 7 (4) (3) แผนงาน โครงการ และงบประมาณรายจ่ายประจำปีของปีที่กำลังดำเนินการ (4) คู่มือหรือคำสั่งเกี่ยวกับวิธีปฏิบัติงานของเจ้าหน้าที่ของรัฐซึ่งมีผลกระทบถึงสิทธิหน้าที่ของเอกชน (5) สิ่งพิมพ์ที่ได้มีการอ้างอิงถึงตามมาตรา 7 วรรคสอง (6) สัญญาสัมปทาน สัญญาที่มีลักษณะเป็นการผูกขาดตัดตอน หรือสัญญาร่วมทุนกับเอกชนในการจัดทำบริการสาธารณะ (7) มติคณะรัฐมนตรี หรือมติคณะกรรมการที่แต่งตั้งโดยกฎหมาย หรือโดยมติคณะรัฐมนตรี (8) ข้อมูลข่าวสารอื่นตามที่คณะกรรมการกำหนด **ข้อมูลข่าวสารที่ไม่ควรเปิดเผย** - ข้อมูลข่าวสารของราชการที่อาจก่อให้เกิดความเสียหายต่อสถาบันพระมหากษัตริย์จะเปิดเผยมิได้ - ข้อมูลข่าวสารของราชการที่มีลักษณะอย่างหนึ่งอย่างใด ดังต่อไปนี้ หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้ (1) การเปิดเผยจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศ และความมั่นคงในทางเศรษฐกิจหรือการคลังของประเทศ (2) การเปิดเผยจะทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ หรือไม่อาจสำเร็จตามวัตถุประสงค์ได้ (3) ความเห็นหรือคำแนะนำภายในหน่วยงานของรัฐในการดำเนินการเรื่องหนึ่งเรื่องใด (4) การเปิดเผยจะก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลหนึ่งบุคคลใด (5) รายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคลซึ่งการเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมต้อง

กฎหมาย	มาตรา	รายละเอียด
		(6) ข้อมูลข่าวสารของราชการที่มีกฎหมายคุ้มครองมิให้เปิดเผย หรือข้อมูลข่าวสารที่มีผู้ให้มาโดยไม่ประสงค์ให้ทางราชการนำไปเปิดเผยต่อผู้อื่น (7) กรณีอื่นตามที่กำหนดให้พระราชกฤษฎีกา - เพื่อให้เกิดความชัดเจนในทางปฏิบัติว่าข้อมูลข่าวสารของราชการจะเปิดเผยต่อบุคคลใดได้หรือไม่ภายใต้เงื่อนไขเช่นใด และสมควรต้องมีวิธีรักษามิให้รั่วไหลให้หน่วยงานของรัฐกำหนดวิธีการคุ้มครองข้อมูลข่าวสารนั้น ทั้งนี้ ตามระเบียบที่คณะรัฐมนตรีกำหนดว่าด้วยการรักษาความลับของทางราชการ **ข้อมูลข่าวสารส่วนบุคคล** - หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลดังต่อไปนี้ (1) ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น (2) พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูลโดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น (3) จัดให้มีการพิมพ์ในราชกิจจานุเบกษา และตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้ (ก) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้ (ข) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล (ค) ลักษณะการใช้ข้อมูลตามปกติ (ง) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล (จ) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล (ฉ) แหล่งที่มาของข้อมูล

กฎหมาย	มาตรา	รายละเอียด
		(4) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ (5) จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคล ตามความเหมาะสม - หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่นโดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ **เอกสารประวัติศาสตร์** - ข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐไม่ประสงค์จะเก็บรักษาหรือมีอายุครบกำหนด ให้หน่วยงานของรัฐส่งมอบให้แก่หอจดหมายเหตุแห่งชาติกรมศิลปากรหรือหน่วยงานอื่นของรัฐตามที่กำหนดในพระราชกฤษฎีกา เพื่อคัดเลือกไว้ให้ประชาชนได้ศึกษาค้นคว้า
ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544	หมวด 1 หมวด 2	บททั่วไป ■ ให้หัวหน้าหน่วยงานของรัฐมีหน้าที่รักษาข้อมูลข่าวสารลับในหน่วยงานของตน และอาจมอบหมายหน้าที่ดังกล่าวได้ตามความจำเป็นให้ผู้ใต้บังคับบัญชา ■ ชั้นความลับของข้อมูลข่าวสารลับ แบ่งออกเป็น 3 ชั้น คือ 1. ลับที่สุด (TOP SECRET) 2. ลับมาก (SECRET) 3. ลับ (CONFIDENTIAL) การกำหนดชั้นความลับ ■ ให้หัวหน้าหน่วยงานของรัฐมีหน้าที่รับผิดชอบในการกำหนดชั้นความลับพร้อมทั้งให้เหตุผลประกอบ ■ การปรับชั้นความลับ ต้องกระทำโดยผู้มีอำนาจกำหนดชั้นความลับของหน่วยงานเจ้าของเรื่อง

กฎหมาย	มาตรา	รายละเอียด
	หมวด 3	การทะเบียน ■ ให้หัวหน้าหน่วยงานของรัฐแต่งตั้งเจ้าหน้าที่ควบคุมและรับผิดชอบการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ เรียกว่า “นายทะเบียนข้อมูลข่าวสารลับ” ■ ให้หัวหน้าหน่วยงานของรัฐแต่งตั้งคณะกรรมการตรวจสอบทำการตรวจสอบความถูกต้องในการปฏิบัติตามระเบียนนี้และการมีอยู่ของข้อมูลข่าวสารลับ อย่างน้อยทุก 6 เดือน
	หมวด 4	การดำเนินการ ■ การดำเนินการใด ๆ เกี่ยวกับข้อมูลข่าวสารลับในทุกขั้นตอน ให้หัวหน้าหน่วยงานของรัฐกำหนดเจ้าหน้าที่ที่เกี่ยวข้อง และจำกัดให้ทราบเท่าที่จำเป็นเท่านั้น ■ การเก็บรักษาข้อมูลข่าวสารลับ ให้หน่วยงานของรัฐเก็บรักษาไว้ในที่ปลอดภัย และให้กำหนดระเบียบการเก็บรักษาข้อมูลข่าวสารลับ ■ ให้หน่วยงานของรัฐจัดให้มีแผนการปฏิบัติในเวลาฉุกเฉิน โดยมีแผนการเคลื่อนย้าย แผนการพิทักษ์รักษา และแผนการทำลายข้อมูลข่าวสารลับ
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ (ฉบับที่ 2) พ.ศ. 2560	มาตรา 5	ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ
	มาตรา 6	ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

กฎหมาย	มาตรา	รายละเอียด
	มาตรา 7	ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ
	มาตรา 8	ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ
	มาตรา 9	ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมด หรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ
	มาตรา 10	ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่น ถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุก ไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ
	มาตรา 11	ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิด หรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของ บุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท
พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 และ (ฉบับที่ 2) พ.ศ. 2551	มาตรา 25	ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกาให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้

กฎหมาย	มาตรา	รายละเอียด
พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549	มาตรา 5	หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้ (1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (2) การจัดให้มีระบบเทคโนโลยีสารสนเทศและการสื่อสารและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง (3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ
ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550		▪ กำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังต่อไปนี้ ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการต้องเก็บรักษา ปรากฏดังภาคผนวก ข.2 ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงเครือข่าย: User ID, วันเวลาการเข้าใช้งาน, IP Address ของเครื่องที่ใช้, และหมายเลขสายที่เรียกเข้า (เช่น กรณี Modem หรือ ADSL) ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (Email Server): Message ID, Email ของผู้รับและผู้ส่ง, วันเวลา การติดต่อและใช้งาน, IP Address ของเครื่องที่เข้ามาใช้งาน, User ID ของผู้ใช้งาน (ถ้ามี), POP3/IMAP4 Log ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล: วันเวลาการเข้าใช้งาน, IP Address ของเครื่องผู้ใช้งาน, User ID (ถ้ามี), path และ file name

กฎหมาย	มาตรา	รายละเอียด
		ง. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ: วันเวลาการติดต่อ, IP Address ของเครื่องผู้ใช้งาน, คำสั่งการใช้งานเว็บ, URI (หน้าเว็บที่เรียกใช้) จ. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet): บันทึกการเข้าถึงเครือข่าย, วันและเวลาการติดต่อ, หมายเลข Port, ชื่อเครื่อง และลำดับข้อความ (ถ้าองค์กรไม่มีบริการ Usenet สามารถตัดหัวข้อนี้ได้) ฉ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น IRC หรือ IM : วันเวลาการติดต่อ, IP Address ของผู้ใช้งาน ■ จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ■ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย มีระบบในการจัดเก็บ เช่น การเก็บไว้ใน Centralized Log Server และไม่ถูกเปลี่ยนแปลงได้จากผู้ใช้งานและผู้ดูแลระบบ การเข้าถึงข้อมูล (แต่ห้ามเปลี่ยนแปลง) จะกระทำได้โดยผู้ที่ได้รับมอบหมายเท่านั้น
พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553	มาตรา 7	วิธีการแบบปลอดภัยตามมาตรา 4 ในแต่ละระดับ ให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด โดยมาตรฐานดังกล่าวสำหรับวิธีการแบบปลอดภัยในแต่ละระดับนั้นอาจมีการกำหนดหลักเกณฑ์ที่แตกต่างกันตามความจำเป็น แต่อย่างน้อยต้องมีการกำหนดเกี่ยวกับหลักเกณฑ์ ดังต่อไปนี้ (1) การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ (2) การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารในส่วนการบริหารจัดการความมั่นคง

กฎหมาย	มาตรา	รายละเอียด
		ปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารทั้งภายในและภายนอกหน่วยงานหรือองค์กร (3) การบริหารจัดการทรัพย์สินสารสนเทศ (4) การสร้างความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารด้านบุคลากร (5) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร (7) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร สารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (8) การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร (9) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (10)การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง (11)การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร
ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง	ข้อ 2 ข้อ 3	หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศของหน่วยงาน

กฎหมาย	มาตรา	รายละเอียด
แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และ (ฉบับที่ 2) พ.ศ. 2556	ข้อ 4	ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ 5-15
	ข้อ 5	ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)
	ข้อ 6	ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย
	ข้อ 7	ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต
	ข้อ 8	ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือ การลักลอบทำสำเนาสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ
	ข้อ 9	ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต
	ข้อ 10	ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต
	ข้อ 11	ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control)
	ข้อ 12	หน่วยงานของรัฐที่มีระบบเทคโนโลยีสารสนเทศและการสื่อสารต้องจัดทำระบบสำรอง

กฎหมาย	มาตรา	รายละเอียด
	ข้อ 13	หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
	ข้อ 14	หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น
	ข้อ 15	หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่าข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า
ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555	ข้อ 2	ในกรณีที่จะต้องปฏิบัติให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน ให้หน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่กำหนดในแนบท้ายประกาศฉบับนี้ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นมาตรการสำหรับใช้ในการควบคุมให้ระบบสารสนเทศมีความมั่นคงปลอดภัย ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและสารสนเทศในระบบ นั้น โดยการทำธุรกรรมทางอิเล็กทรอนิกส์ด้วยระบบสารสนเทศ ต้องดำเนินการตามมาตรการที่เกี่ยวข้องตามบัญชีแนบท้ายนี้ และต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน ทั้งนี้ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ แบ่งออกเป็น 11 ข้อ ได้แก่

กฎหมาย	มาตรา	รายละเอียด
		1. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ 2. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร 3. การบริหารจัดการทรัพย์สินสารสนเทศ 4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร 5. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม 6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 7. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ 8. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 9. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด 10. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง 11. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

กฎหมาย	มาตรา	รายละเอียด
ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559	ข้อ 3	ให้หน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่มีรายชื่อแนบท้ายประกาศฉบับนี้ ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัดตามพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 แนบท้าย ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559 ว่าด้วยรายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กร **<u>ส่วนราชการ</u>** **3. กระทรวงการคลัง** เฉพาะ (2) กรมบัญชีกลาง
ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต	ข้อ 2 ข้อ 3	ผู้ใช้บริการบาทเนตต้องดำเนินการให้คอมพิวเตอร์ลูกข่ายบาทเนตผ่านการตรวจรับรองมาตรฐาน ISO/IEC 27001 ตามแนวทางใดแนวทางหนึ่ง ดังนี้ (1) ผ่านการตรวจรับรองมาตรฐานภายในปี 2560 (2) ผ่านการตรวจประเมินภายในปี 2560 และผ่านการตรวจรับรองมาตรฐานภายในปี 2561 ผู้ใช้บริการบาทเนตต้องรักษาสถานภาพการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 อย่างต่อเนื่อง
พระราชบัญญัติ การรักษาความมั่นคง	มาตรา ๕๘	ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือ

กฎหมาย	มาตรา	รายละเอียด
ปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒		หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของ หน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงาน ควบคุมหรือกำกับดูแลของตนโดยเร็ว
	มาตรา ๖๐	การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้ (๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยง อย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลง (๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้น อย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมาย เพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือ โครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือ ให้บริการได้

กฎหมาย	มาตรา	รายละเอียด
		(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ที่มีลักษณะ ดังต่อไปนี้ (ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของ หน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยา ตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยัง โครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบ คอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ (ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือ การสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุข ของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัด หรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง ทั้งนี้ รายละเอียดของลักษณะภัยคุกคามทางไซเบอร์

กฎหมาย	มาตรา	รายละเอียด
		มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ให้คณะกรรมการเป็นผู้ประกาศกำหนด
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	มาตรา ๑๙	ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติ แห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้ การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้ ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้ง วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้น ต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้ง ใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้ ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึง อย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่าย เช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือ สัญญา

กฎหมาย	มาตรา	รายละเอียด
		ที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบตามที่กำหนดไว้ในหมวดนี้ ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุม ข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในหมวดนี้ ไม่มีผล ผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้
	มาตรา ๒๑	ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่ (๑) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อน เก็บรวบรวม ใช้ หรือเปิดเผยแล้ว (๒) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้
	มาตรา ๔๐	ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้ (๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับ จากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ (๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้ง แจ้งให้ผู้

กฎหมาย	มาตรา	รายละเอียด
		ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น (๓) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด