แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
ของผู้ประกอบธุรกิจหลักทรัพย์และสัญญาซื้อขายล่วงหน้า

เพื่อให้ผู้ประกอบธุรกิจสามารถปฏิบัติตามประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ .... เรื่อง การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ได้อย่างมีประสิทธิภาพและมีมาตรฐานในระดับเดียวกัน สำนักงานจึงได้จัดทำแนวทางปฏิบัติฉบับนี้ โดยหากผู้ประกอบธุรกิจสามารถปฏิบัติได้ตามแนวทางปฏิบัติฉบับนี้ สำนักงานจะถือว่าผู้ประกอบธุรกิจได้ปฏิบัติเป็นไปตามประกาศข้างต้นแล้ว อย่างไรก็ดี ผู้ประกอบธุรกิจอาจมีแนวทางปฏิบัติอื่นที่แตกต่างจากแนวปฏิบัตินี้ได้ หากแสดงต่อสำนักงานได้ว่าแนวทางดังกล่าวสามารถป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศได้และมีประสิทธิภาพเพียงพอ ตลอดจนอยู่ในมาตรฐานที่ยอมรับได้สำหรับการควบคุมการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจ

ทั้งนี้ สาระสำคัญของแนวทางปฏิบัติฉบับนี้ ประกอบด้วย

บทนิยาม

“ทรัพย์สินสารสนเทศที่มีความสำคัญ”	หมายถึง	ทรัพย์สินสารสนเทศที่เกี่ยวข้อง หรือจำเป็นต้องใช้ประกอบกับงานที่มีความสำคัญ
“ระบบสารสนเทศที่มีความสำคัญ”	หมายถึง	ระบบสารสนเทศที่รองรับการปฏิบัติงานที่สำคัญ
“งานที่สำคัญ”	หมายถึง	งานที่เกี่ยวกับการให้บริการ การทำธุรกรรม หรืองานอื่น ๆ ของผู้ประกอบธุรกิจ ซึ่งหากมีการหยุดชะงักอาจส่งผลกระทบต่อลูกค้าการดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของผู้ประกอบธุรกิจอย่างมีนัยสำคัญ
“ผู้ให้บริการภายนอก”	หมายถึง	บุคคลจากภายนอกองค์กรซึ่งผู้ประกอบธุรกิจว่าจ้างเพื่อใช้บริการที่เกี่ยวข้องกับระบบสารสนเทศ
“ป้ายชื่อของข้อมูล (information label)”	หมายถึง	รายละเอียดและสิ่งที่บ่งชี้ถึงสิทธิหรือผู้รับผิดชอบไฟล์ข้อมูล ซึ่งแบ่งออกเป็น 1. <u>กลุ่มที่ถูกระบุโดยอัตโนมัติอยู่แล้ว</u> เช่น รายละเอียดการ modify หรือ update ไฟล์ข้อมูล และชื่อผู้เป็นเจ้าของไฟล์ข้อมูล 2. <u>กลุ่มที่แสดงระดับความสำคัญของข้อมูล</u> ซึ่งอาจจัดทำ label ได้โดยการแบ่งกลุ่มไฟล์ที่มีความสำคัญระดับเดียวกันให้อยู่ภายใน folder เดียวกัน หรือโดยการกำหนดสิทธิผู้ที่สามารถเข้าถึงไฟล์ข้อมูลที่สำคัญ เป็นต้น

1. นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

วัตถุประสงค์
เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ โดยผู้ประกอบธุรกิจต้องจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยคำนึงถึงลักษณะ ขนาด และความซับซ้อนของการประกอบธุรกิจ รวมทั้งกฎเกณฑ์ต่าง ๆ ที่เกี่ยวข้อง

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากคณะกรรมการบริษัทหรือคณะกรรมการอื่นที่คณะกรรมการบริษัทมอบหมาย และจัดให้มีการทบทวนหรือปรับปรุงนโยบายดังกล่าวอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงของสภาพแวดล้อมต่าง ๆ ที่มีนัยสำคัญ เช่น สภาพธุรกิจ กฎเกณฑ์กฎหมาย และเทคโนโลยี เป็นต้น นอกจากนี้ ผู้ประกอบธุรกิจต้องเผยแพร่นโยบายดังกล่าวในลักษณะที่ให้ผู้ใช้งานเข้าถึงได้ง่าย เพื่อให้บุคลากรที่เกี่ยวข้องทราบและถือปฏิบัติเป็นไปตามที่นโยบายกำหนด

2. นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ต้องมีเนื้อหาขั้นต่ำครอบคลุมในเรื่องดังต่อไปนี้

2.1 การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ
   (1) การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (access control) [อ้างอิงจากข้อ 5]
   (2) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (physical and environmental security) [อ้างอิงจากข้อ 7]

2.2 การจัดการข้อมูลสารสนเทศและการรักษาความลับ
   (1) การจำแนกประเภทของข้อมูลสารสนเทศ (information classification) เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัย [อ้างอิงจากข้อ 4.2]
   (2) การสำรองข้อมูล (backup) [อ้างอิงจากข้อ 8.3]
   (3) การควบคุมการเข้ารหัสข้อมูล (cryptographic controls) [อ้างอิงจากข้อ 6]
   (4) การป้องกันข้อมูลส่วนบุคคล (privacy and protection of personally identifiable information) [อ้างอิงจากข้อ 14.1 แนวทางปฏิบัติข้อ 4]

2.3 การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

(1) การควบคุมการใช้งานของผู้ใช้งาน (end user) เช่น

- ข้อกำหนดการใช้งานทรัพย์สินสารสนเทศอย่างถูกต้องปลอดภัย (acceptable use of assets) [อ้างอิงจากข้อ 4.1 แนวปฏิบัติข้อ 3]
- มาตรการป้องกันอุปกรณ์สารสนเทศระหว่างที่ไม่มีผู้ใช้งาน (protection of unattended user equipment) [อ้างอิงจากข้อ 7.2 แนวทางปฏิบัติข้อ 6]
- การใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานจากภายนอกบริษัท (mobile device and teleworking) [อ้างอิงจากข้อ 2.2]
- การควบคุมการติดตั้งและใช้งานซอฟต์แวร์ (restriction on software installations and use) [อ้างอิงจากข้อ 8.5]

(2) การควบคุมดูแลผู้ให้บริการภายนอก (supplier relationships) [อ้างอิงจากข้อ 11]

2.4 การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

(1) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ (communications security) [อ้างอิงจากข้อ 9]

(2) การควบคุมการรับส่งข้อมูลสารสนเทศ (information transfer) [อ้างอิงจากข้อ 9.2]

2.5 การป้องกันภัยคุกคามต่อระบบสารสนเทศ

(1) การป้องกันโปรแกรมไม่ประสงค์ดี (protection from malware) [อ้างอิงจากข้อ 8.2]

(2) การบริหารจัดการช่องโหว่ทางเทคนิค (technical vulnerability management) [อ้างอิงจากข้อ 8.6]

2.6 การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (system acquisition, development and maintenance) [อ้างอิงจากข้อ 10]

2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

2.1 การจัดโครงสร้างภายในองค์กร (internal organization)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับส่วนงานต่าง ๆ ภายในองค์กร ให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวทางปฏิบัติ

1. ผู้บริหารระดับสูงต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งจัดสรรหน้าที่ความรับผิดชอบและกำหนดแนวทางในการปฏิบัติหน้าที่ให้กับพนักงาน เพื่อให้มั่นใจได้ว่าบุคคลดังกล่าวสามารถปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างครบถ้วน

2. ผู้บริหารระดับสูงต้องจัดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศออกจากกันอย่างชัดเจนเพื่อให้มีการสอบทานระหว่างกัน และป้องกันความเสี่ยงในการปฏิบัติงานที่อาจเกิดขึ้น เช่น การแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (system administrator) ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (production environment) ทั้งนี้ ในกรณีที่ไม่สามารถแบ่งแยกหน้าที่ความรับผิดชอบเนื่องจากข้อจำกัดทางด้านขนาดของการประกอบธุรกิจ ผู้ประกอบธุรกิจต้องจัดให้มีกระบวนการติดตาม และตรวจสอบการปฏิบัติงานของบุคลากรที่เกี่ยวข้องอย่างใกล้ชิดและสม่ำเสมอเพื่อลดความเสี่ยงที่อาจเกิดขึ้น

3. ผู้ประกอบธุรกิจต้องจัดให้มีรายชื่อและช่องทางสำหรับติดต่อ (contact person) ของหน่วยงานกำกับดูแลและหน่วยงานผู้ให้บริการที่สนับสนุนการทำงานระบบสารสนเทศของบริษัท เพื่อให้สามารถติดต่อประสานงานหรือขอความช่วยเหลือในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

2.2 การใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานจากภายนอกบริษัท (mobile device and teleworking)

วัตถุประสงค์
เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับการปฏิบัติงานขององค์กรจากระยะไกล รวมทั้งการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา

แนวทางปฏิบัติ

1. ในกรณีการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพาสำหรับการปฏิบัติงานที่มีการเชื่อมต่อกับระบบงานภายในองค์กร ทั้งนี้ ไม่รวมถึงระบบ mail service ผู้ประกอบธุรกิจต้องมีมาตรการป้องกันข้อมูลสารสนเทศที่สำคัญ โดยพิจารณาถึงแนวทางดังต่อไปนี้

(1) กำหนดให้มีการลงทะเบียนอุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น ยี่ห้อ รุ่น ระบบปฏิบัติการ รหัสประจำเครื่อง (serial number) และหมายเลขอ้างอิงอุปกรณ์เครือข่าย (MAC address) เป็นต้น อย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนอุปกรณ์ เพื่อให้มั่นใจได้ว่าการใช้งานอุปกรณ์ดังกล่าวมีความสอดคล้องเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(2) มีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) กรณีที่อุปกรณ์คอมพิวเตอร์ประเภทพกพาสูญหาย เช่น การกำหนดให้ใส่รหัสผ่านก่อนใช้งานอุปกรณ์ (lock screen) หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น

(3) กำหนดประเภทบริการการใช้งาน (application service) ที่อนุญาตให้ใช้งานผ่านอุปกรณ์คอมพิวเตอร์ประเภทพกพา และกำหนดมาตรการควบคุมการเข้าถึงบริการการใช้งานดังกล่าวโดยคำนึงถึงความปลอดภัยของการเชื่อมต่อกับเครือข่าย เช่น จำกัดให้เข้าถึงบริการการใช้งานบางประเภทหากเป็นการเชื่อมต่อกับเครือข่ายภายนอก เป็นต้น

(4) จัดให้มีการเข้ารหัสข้อมูลสารสนเทศที่สำคัญบนอุปกรณ์พกพาและที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์

(5) จัดให้มีการอบรมผู้ใช้งานเพื่อตระหนักและทราบถึงความเสี่ยงจากการใช้งาน และแนวทางการควบคุมความเสี่ยงดังกล่าว

(6) ควบคุมให้มีการติดตั้งเฉพาะซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์ และโปรแกรมเพื่อปิดช่องโหว่ (patches) ที่เหมาะสม

(7) กำหนดมาตรการป้องกันโปรแกรมไม่ประสงค์ดี (malware)

(8) จัดให้มีการดำเนินการเพื่อลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลสารสนเทศ เช่น ตัดการเชื่อมต่อโดยทันทีที่ทราบเหตุ เป็นต้น

ทั้งนี้ หากอุปกรณ์คอมพิวเตอร์ประเภทพกพาเป็นทรัพย์สินของพนักงาน ผู้ประกอบธุรกิจต้องพิจารณาแนวทางในข้อ (1) - (5) เป็นขั้นต่ำ พร้อมทั้งจัดให้มีมาตรการควบคุมที่เทียบเคียงหรือทดแทนแนวทาง

ในข้อ (6) - (8) ได้ เช่น กำหนดให้มีการตรวจสอบอุปกรณ์คอมพิวเตอร์ประเภทพกพาอย่างสม่ำเสมอ กำหนดบทลงโทษหรือตัดสิทธิการใช้งาน application service ในกรณีที่พนักงานละเมิดข้อกำหนด เป็นต้น

2. ในกรณีที่มีการปฏิบัติงานขององค์กรจากระยะไกล (teleworking site) ผู้ประกอบธุรกิจต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอสำหรับข้อมูลสารสนเทศที่ถูกเข้าถึง ประมวลผล และจัดเก็บในพื้นที่ปฏิบัติงาน โดยพิจารณาถึง

(1) การกำหนดมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสม รัดกุมเพียงพอ สำหรับพื้นที่ปฏิบัติงานนอกองค์กร
(2) การควบคุมสิทธิการใช้งานและการเข้าถึงข้อมูลสารสนเทศของผู้ใช้งานอย่างเหมาะสม
(3) การรักษาความมั่นคงปลอดภัยกรณีมีการเชื่อมต่อระบบงานที่สำคัญ หรือรับส่งข้อมูลที่เป็นความลับหรือมีความสำคัญจากระยะไกล (remote access)
(4) การป้องกันการรั่วไหลของข้อมูลสารสนเทศในกรณีใช้เทคโนโลยี virtual desktop
(5) การป้องกันการเข้าถึงข้อมูลสารสนเทศจากบุคคลที่ไม่มีสิทธิในการใช้งาน เช่น ญาติพี่น้องและเพื่อน เป็นต้น
(6) มีวิธีการในการตรวจสอบความมั่นคงปลอดภัยของอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานในพื้นที่ปฏิบัติงานนอกองค์กร
(7) การป้องกันโปรแกรมไม่ประสงค์ดี

3. ในกรณีที่ใช้บริการ cloud computing ผู้ประกอบธุรกิจต้องจัดให้มีข้อกำหนดเกี่ยวกับการใช้งาน โดยขั้นต่ำต้องมีรายละเอียด ดังนี้

3.1 ต้องกำหนดนโยบายการใช้งาน cloud computing โดยอย่างน้อยต้องมีเนื้อหา ดังนี้
   (1) ประเมินความเสี่ยงเกี่ยวกับการใช้บริการ
   (2) กำหนดประเภทงานที่จะใช้บริการ
   (3) กำหนดรูปแบบของการใช้บริการ เช่น software as a service (saas), platform as a service (paas) และ infrastructure as a service (iaas)
   (4) กำหนดวิธีการคัดเลือกและประเมินผู้ให้บริการ (due diligence) เช่น ผู้ให้บริการต้องได้รับมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล เช่น ได้รับมาตรฐาน ISO 27001
   (5) กำหนดการทบทวนคุณสมบัติของผู้ให้บริการอย่างสม่ำเสมอ เช่น ฐานะทางการเงิน ความเพียงพอของการให้บริการ (capacity planning) เพื่อประเมินความพร้อมในการให้บริการ
   (6) กำหนดความปลอดภัยของข้อมูลแต่ละประเภทที่จะใช้ใน cloud โดยแบ่งชั้นความลับของข้อมูล และกำหนดวิธีปฏิบัติแต่ละระดับชั้นความลับของข้อมูล
   (7) กำหนดเงื่อนไขสำหรับผู้ให้บริการในการเข้าถึงและเปิดเผยข้อมูลของผู้ใช้บริการ

(8) กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการอย่างชัดเจน เช่น การสำรองข้อมูล การรับเรื่องแก้ไขปัญหา ขั้นตอนและกระบวนการแก้ไขปัญหา รายชื่อและช่องทางสำหรับติดต่อ เป็นต้น

(9) จัดให้มีการเผยแพร่นโยบายเกี่ยวกับการใช้บริการ และจัดอบรมให้ความรู้แก่พนักงานเพื่อให้ตระหนักถึงความมั่นคงปลอดภัยจากการใช้บริการ cloud computing

(10) กำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามการใช้งานแต่ละประเภทเพื่อป้องกันภัยคุกคามและการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

(11) กำหนดให้มีการตรวจสอบบันทึกหลักฐานต่าง ๆ และติดตามปัญหาที่อาจส่งผลต่อการใช้บริการ

3.2 กำหนดข้อตกลงระหว่างผู้ให้บริการและผู้ใช้บริการ โดยมีลักษณะดังนี้

(1) ผู้ใช้บริการถือเป็นเจ้าของข้อมูลสารสนเทศ

(2) กำหนดประเภทบริการที่จะใช้ cloud computing

(3) ต้องกำหนดมาตรฐานความปลอดภัยด้านเครือข่าย เช่น การเข้ารหัสข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ การป้องกันการโจมตีในลักษณะ DDoS (distributed denial of service) การป้องกันการบุกรุกจากโปรแกรมไม่ประสงค์ดี การป้องกันภัยคุกคามในรูปแบบใหม่ (advanced persistent threat) การแบ่งแยกเครือข่าย การเข้ารหัสระหว่างแอพพลิเคชั่น (application) การป้องกันการบุกรุกแบบลำดับชั้น (defense-in-depth) และการสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศ (hardening) เป็นต้น

(4) กำหนดใช้วิธีพิสูจน์ตัวตนแบบ multi-factor authentication

(5) ต้องระบุข้อตกลงในการควบคุมการเข้าถึงข้อมูล เช่น วิธีการเข้าใช้งานระบบ วิธีการกำหนดสิทธิการใช้งาน การติดตามการแก้ปัญหา การรายงานข้อผิดพลาด ประสิทธิภาพ และสภาพโดยรวมของระบบ อย่างชัดเจน

(6) กำหนดบทบาทหน้าที่ความรับผิดชอบของผู้ให้บริการในด้านการสำรองข้อมูล กระบวนการแก้ไขปัญหา ระดับการให้บริการ (service level agreement) ระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ (recovery time objectives : RTO) และกำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (recovery point objective : RPO) อย่างชัดเจน

(7) กำหนดเงื่อนไขความรับผิดชอบในกรณีที่ผู้ให้บริการไม่สามารถให้บริการตามสัญญาที่กำหนด

(8) กำหนดให้มีการลงนามในสัญญาที่เกี่ยวกับนโยบายการป้องกันการรั่วไหลของข้อมูลที่อาจเกิดขึ้นจากผู้ให้บริการ

(9) ผู้ให้บริการต้องไม่มีสิทธิเข้าถึงและเปิดเผยข้อมูลของผู้ใช้บริการ เว้นแต่จะแจ้งและได้รับความยินยอมจากผู้ใช้บริการ หรือแจ้งให้ทราบหากเป็นไปตามกฎหมายของประเทศที่ผู้ให้บริการไปตั้งศูนย์ข้อมูล (cloud server hosting country) หรือเป็นไปตามกฎหมายเกี่ยวกับความมั่นคงของประเทศผู้ให้บริการ (origin country)

(10) ผู้ให้บริการต้องปรับปรุงการปฏิบัติงานให้เป็นไปตามมาตรฐานการรับรองความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากลฉบับปัจจุบันโดยไม่ชักช้า หากมาตรฐานดังกล่าวได้ถูกปรับปรุงให้เป็นปัจจุบัน (update)

(11) ผู้ประกอบธุรกิจต้องมีมาตรการเพื่อให้มั่นใจได้ว่าผู้ให้บริการจัดให้มีการตรวจสอบขั้นตอนการปฏิบัติงานอย่างน้อยปีละ 1 ครั้ง จากผู้ตรวจสอบอิสระ

(12) มีข้อกำหนดเมื่อสิ้นสุดการใช้บริการ (exit plan) เช่น กำหนดระยะเวลารักษาข้อมูลและวิธีการทำลายข้อมูลเพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้

(13) ต้องมีการเปิดเผยขั้นตอนปฏิบัติงาน และเงื่อนไขการใช้บริการ cloud computing ต่อจากผู้ให้บริการรายอื่น (sub cloud) อย่างชัดเจน โดยอย่างน้อยต้องมีเงื่อนไขเป็นไปตามข้อ 3.3

3.3 ในกรณีที่ผู้ให้บริการมีการใช้บริการ cloud computing ต่อจากผู้ให้บริการรายอื่น (sub cloud) ต้องจัดให้มีข้อกำหนดดังนี้

(1) ต้องแจ้งส่วนที่ sub cloud ให้ผู้ใช้บริการทราบ และให้ถือว่าบริการดังกล่าวเป็นส่วนหนึ่งของบริการของผู้ให้บริการด้วย โดยต้องมีคุณสมบัติด้านความปลอดภัยเทียบเท่ากับผู้ให้บริการ

(2) ต้องมีการเข้ารหัสในกรณีที่มีการรับส่งข้อมูลระหว่าง cloud provider กับ sub cloud provider

(3) ต้องมีการกำหนดขั้นตอนปฏิบัติงาน และเงื่อนไขการ sub cloud อย่างชัดเจน

3.4 การติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการ

(1) ต้องติดตามตรวจสอบประสิทธิภาพของการให้บริการ รวมทั้งมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดตามสัญญาต่าง ๆ หรือข้อตกลงในการให้บริการ

(2) ต้องประเมินความเพียงพอของระบบงานของผู้ให้บริการ (capacity planning) อย่างสม่ำเสมอ

(3) ต้องทบทวนเงื่อนไขการบริการในกรณีที่มีการเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าการให้บริการยังคงสอดคล้องกับการใช้งานและนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ประกอบธุรกิจ

(4) ต้องทบทวนคุณสมบัติของผู้ให้บริการอย่างต่อเนื่อง เช่น การตรวจสอบความมั่นคงในฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการปฏิบัติงาน เป็นต้น

3.5 ผู้ใช้บริการต้องกำหนดขั้นตอนการ โอนย้ายข้อมูล (data migration) ไปยังผู้ให้บริการรายใหม่อย่างชัดเจน ในกรณีที่มีการเปลี่ยนผู้ให้บริการ ทั้งนี้ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศยังคงมีความครบถ้วนถูกต้อง และพร้อมใช้งานอยู่เสมอ

3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

วัตถุประสงค์
เพื่อให้พนักงานและผู้ให้บริการภายนอกที่ปฏิบัติงานภายในองค์กรมีความตระหนักรู้ และปฏิบัติงานโดยคำนึงถึงการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการสร้างความตระหนักรู้ (awareness education) เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแก่พนักงานและผู้ให้บริการภายนอกที่ปฏิบัติงานภายในองค์กรอย่างสม่ำเสมอ โดยเนื้อหาต้องสอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และหน้าที่ความรับผิดชอบของบุคลากร

2. ผู้ประกอบธุรกิจต้องสื่อสารให้พนักงานและผู้ให้บริการภายนอกที่ปฏิบัติงานภายในองค์กรระมัดระวังและละเว้นการใช้งานระบบสารสนเทศในลักษณะที่อาจก่อให้เกิดความเสียหายกับผู้ประกอบธุรกิจ ตลาดทุนโดยรวม หรือความมั่นคงของประเทศ เช่น การหมิ่นประมาท การข่มขู่ การปลอมแปลงเป็นบุคคลอื่น การส่งจดหมายอิเล็กทรอนิกส์แบบลูกโซ่ และการเปิดเผยข้อมูลที่เป็นความลับของผู้ประกอบธุรกิจ เป็นต้น

3. ผู้ประกอบธุรกิจต้องสื่อสารให้พนักงานและผู้ให้บริการภายนอกที่ปฏิบัติงานภายในองค์กรตระหนักและสังเกตถึงความผิดปกติใด ๆ ที่อาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (security weaknesses) และรายงานบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งสถานการณ์ (point of contact) ทันทีเมื่อพบความผิดปกติดังกล่าวทุกครั้ง

4. ผู้ประกอบธุรกิจต้องจัดให้มีมาตรการดำเนินการทางวินัยต่อผู้ฝ่าฝืนนโยบายและหลักปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

4. การบริหารจัดการทรัพย์สินสารสนเทศ (Asset Management)

4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ (responsibility for assets)

วัตถุประสงค์
เพื่อให้ทรัพย์สินสารสนเทศที่มีความสำคัญได้รับการป้องกันอย่างเหมาะสม ผู้ประกอบธุรกิจต้องจัดให้มีการระบุและกำหนดหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดทำและเก็บทะเบียนทรัพย์สินสารสนเทศ เช่น อุปกรณ์คอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบและอุปกรณ์เครือข่ายคอมพิวเตอร์ และข้อมูลสารสนเทศ เป็นต้น รวมทั้งตรวจสอบและทบทวนรายการทรัพย์สินอย่างสม่ำเสมอ เพื่อให้เกิดความถูกต้องเป็นปัจจุบัน โดยต้องดำเนินการดังกล่าวอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

2. ผู้ประกอบธุรกิจต้องกำหนดผู้รับผิดชอบทรัพย์สินสารสนเทศแต่ละประเภท เพื่อดูแลความมั่นคงปลอดภัยตลอดอายุการใช้งานของทรัพย์สิน

3. ผู้ประกอบธุรกิจต้องจัดให้มีข้อกำหนดในการใช้งานทรัพย์สินสารสนเทศอย่างเหมาะสม เพื่อให้มั่นใจได้ว่าผู้ใช้งานทรัพย์สินสารสนเทศมีการเข้าถึงและใช้งานอย่างถูกต้องปลอดภัย

4. ผู้ประกอบธุรกิจต้องควบคุมให้พนักงานและผู้ให้บริการภายนอก คืนทรัพย์สินสารสนเทศของผู้ประกอบธุรกิจ ในกรณีที่ลาออก เลิกสัญญาว่าจ้าง หรือเปลี่ยนแปลงหน้าที่ปฏิบัติงาน

4.2 การจำแนกประเภทของทรัพย์สินสารสนเทศ (asset classification)

วัตถุประสงค์
เพื่อให้ข้อมูลและทรัพย์สินสารสนเทศที่มีความสำคัญได้รับการปกป้องในระดับที่เหมาะสมตามระดับความสำคัญ

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องกำหนดให้มีการจำแนกประเภททรัพย์สินสารสนเทศตามระดับชั้นความลับและความสำคัญต่อผู้ประกอบธุรกิจ และทบทวนการจำแนกประเภทดังกล่าวอย่างสม่ำเสมอ

2. ผู้ประกอบธุรกิจต้องจัดทำป้ายชื่อทรัพย์สินสารสนเทศ (labeling) ให้ชัดเจน ทั้งทรัพย์สินประเภทอุปกรณ์คอมพิวเตอร์และทรัพย์สินที่เป็นข้อมูลสารสนเทศ (information labeling) เพื่อให้ทราบถึงผู้รับผิดชอบ รายละเอียดและระดับความสำคัญของทรัพย์สินสารสนเทศ พร้อมทั้งจัดให้มีมาตรการดูแลรักษาความมั่นคงปลอดภัยที่สอดคล้องเหมาะสมกับแต่ละกลุ่มประเภทของทรัพย์สินสารสนเทศ เช่น การควบคุมการเข้าถึง การจัดให้มีการเข้ารหัสข้อมูลที่เป็นความลับหรือต้องการความถูกต้องในระดับสูง เป็นต้น

4.3 การจัดการสื่อบันทึกข้อมูล (media handling)

วัตถุประสงค์

เพื่อป้องกันการเปิดเผย เปลี่ยนแปลงแก้ไข หรือสร้างความเสียหายต่อข้อมูลสารสนเทศสำคัญที่ถูกจัดเก็บในสื่อบันทึกข้อมูล

แนวทางปฏิบัติ

1. กรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูล ผู้ประกอบธุรกิจต้องจัดให้มีกระบวนการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลและไม่ให้สามารถกู้คืนข้อมูลได้

2. ผู้ประกอบธุรกิจต้องจัดให้มีกระบวนการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลที่เป็นความลับหรือมีความสำคัญ

3. กรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน ผู้ประกอบธุรกิจต้องคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่

4. ผู้ประกอบธุรกิจต้องจัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความมั่นคงปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต

5. ผู้ประกอบธุรกิจต้องจัดให้มีกระบวนการดูแลรักษาความปลอดภัยกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูลออกจากพื้นที่ทำการ

5. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

5.1 การควบคุมการเข้าถึงตามข้อกำหนดทางธุรกิจ (business requirements of access control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงข้อมูลและ information processing facilities

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายควบคุมการเข้าถึงข้อมูลและ information processing facilities ต่าง ๆ เช่น อุปกรณ์หรือโปรแกรมประมวลผลข้อมูล ระบบเครือข่ายคอมพิวเตอร์ ขั้นตอนหรือสถานที่ประมวลผลข้อมูลตามที่ผู้ประกอบธุรกิจกำหนด เป็นต้น เพื่อควบคุมการเข้าถึงให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยจัดทำเป็นลายลักษณ์อักษรและทบทวนนโยบายดังกล่าวอย่างสม่ำเสมอ ทั้งนี้ นโยบายดังกล่าวต้องสอดคล้องกับข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยขั้นต่ำต้องครอบคลุมเรื่องดังต่อไปนี้

   (1) การกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ และยกเลิกสิทธิของบุคคลที่ไม่มีความจำเป็นในการเข้าถึงโดยทันที

   (2) การแบ่งแยกบทบาทหน้าที่ของบุคคลที่เกี่ยวข้อง เช่น บุคคลผู้ร้องขอ (access request) บุคคลผู้มีอำนาจอนุมัติ (access authorization) และบุคคลผู้บริหารสิทธิการเข้าถึง (access administration) เป็นต้น

   (3) นโยบายในส่วนของการควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ขั้นต่ำต้องครอบคลุมถึงการระบุประเภทหรือบริการทางเครือข่าย (network services) และบุคคลที่ได้รับอนุญาตให้เข้าถึง กระบวนการควบคุมและป้องกันการเข้าถึง วิธีการเข้าถึงแบบปลอดภัย เทคนิคการระบุตัวตน และการติดตามการใช้งานของบุคคลที่ได้รับอนุญาตให้เข้าถึง

   (4) มีระบบการระบุผู้ใช้งานในระบบเครือข่ายคอมพิวเตอร์ได้อย่างชัดเจน โดยเฉพาะกรณีที่ผู้ประกอบธุรกิจใช้หมายเลขประจำเครื่องแบบพลวัต (dynamic IP address) ผู้ประกอบธุรกิจ ต้องมีข้อมูลที่สามารถระบุผู้ใช้งานหมายเลข IP address ในช่วงเวลาที่ใช้งานได้

5.2 การบริหารจัดการบัญชีผู้ใช้งาน (user access management)

วัตถุประสงค์
เพื่อให้มีการควบคุมสิทธิการใช้งานระบบสารสนเทศอย่างเหมาะสมและป้องกันไม่ให้ผู้ที่ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบสารสนเทศได้

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ (user registration) และยกเลิกบัญชีผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าถึง

2. ในการกำหนดสิทธิการเข้าถึงระดับสูง (privileged access rights) ผู้ประกอบธุรกิจต้องจัดสรรอย่างจำกัดและอยู่ภายใต้การควบคุมอย่างเคร่งครัด

3. ผู้ประกอบธุรกิจต้องจัดให้มีขั้นตอนการบริหารจัดการเรื่องการกำหนดรหัสผ่าน (user password management) อย่างเหมาะสม

4. ผู้ประกอบธุรกิจต้องจัดให้มีการติดตามทบทวนระดับสิทธิการเข้าถึงอย่างสม่ำเสมอ และยกเลิกสิทธิการเข้าถึงโดยทันที เมื่อบุคคลที่ได้รับสิทธิลาออก เลิกสัญญาว่าจ้าง หรือเปลี่ยนแปลงหน้าที่ปฏิบัติงาน

5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

วัตถุประสงค์
เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ สามารถเข้าถึงระบบสารสนเทศได้

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีข้อบังคับให้ผู้ใช้งานดูแลรับผิดชอบบัญชีผู้ใช้งาน (user ID) และรหัสผ่าน (password) รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีการใช้งานระบบได้อย่างมั่นคงปลอดภัย (accountable for safeguard) ตามนโยบายการควบคุมการเข้าถึงที่ได้กำหนดไว้

5.4 การควบคุมการเข้าถึงระบบสารสนเทศและแอพพลิเคชั่น (system and application access control)

วัตถุประสงค์
เพื่อป้องกันการเข้าถึงระบบสารสนเทศและแอพพลิเคชั่นโดยไม่ได้รับอนุญาต

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องควบคุมการเข้าถึงข้อมูลสารสนเทศและฟังก์ชั่นต่าง ๆ ในแอพพลิเคชั่นของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับสิทธิที่ได้รับและนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

2. ผู้ประกอบธุรกิจต้องควบคุมการเข้าใช้งาน (log-on) ระบบสารสนเทศและแอพพลิเคชั่นด้วยวิธีการแบบปลอดภัย เช่น มีการป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) แจ้งเตือนกรณีที่มีความพยายามเข้าใช้งานอย่างไม่เหมาะสม (breach of log-on control) และจัดเก็บหลักฐานดังกล่าว เป็นต้น

3. ผู้ประกอบธุรกิจต้องจัดให้มีระบบการบริหารจัดการรหัสผ่านที่มีความมั่นคงปลอดภัย โดยขั้นต่ำต้องมีกระบวนการดังนี้

(1) กำหนดให้ผู้ใช้งานแต่ละรายต้องรับผิดชอบ (accountable) บัญชีผู้ใช้งาน (user ID) และรหัสผ่าน (password) ของตนเอง
(2) ให้ผู้ใช้งานสามารถตั้งค่าหรือเปลี่ยนแปลงรหัสผ่านได้ด้วยตนเอง และระบบต้องมีขั้นตอนให้ยืนยันความถูกต้อง
(3) บังคับให้ผู้ใช้งานตั้งรหัสผ่านที่ยากต่อการคาดเดา เช่น มีความยาวขั้นต่ำ 6-8 ตัวอักษร โดยอาจมีอักขระพิเศษ (เช่น “#”) ประกอบด้วย
(4) บังคับให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสผ่านครั้งแรก และควรเปลี่ยนรหัสผ่านอย่างน้อยทุก 6 เดือน
(5) ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำกับรหัสที่ใช้งานครั้งล่าสุด
(6) ระหว่างที่ผู้ใช้งานใส่รหัสผ่าน ระบบต้องไม่แสดงให้เห็นค่ารหัสผ่านบนหน้าจอ
(7) ต้องมีระบบการเข้ารหัส (encryption) ข้อมูลรหัสผ่าน เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง รวมทั้งไม่จัดเก็บข้อมูลรหัสผ่านใน folder เดียวกันกับ folder ที่จัดเก็บข้อมูลของแอพพลิเคชั่น
(8) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 10 ครั้ง
(9) ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น

4. ผู้ประกอบธุรกิจต้องจำกัดการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ (utility programs) และจำกัดการเข้าถึงชุดคำสั่งควบคุมการทำงานของโปรแกรม (program source code) อย่างเข้มงวด เพื่อป้องกันการเปลี่ยนแปลงการทำงานของระบบสารสนเทศ

6. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)

วัตถุประสงค์
เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่เป็นความลับหรือมีความสำคัญ

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายควบคุมการใช้งานระบบการเข้ารหัสข้อมูล ที่คำนึงถึงชนิด และขั้นตอนวิธีการเข้ารหัสข้อมูล (algorithm) ที่สอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่เป็นความลับหรือมีความสำคัญ รวมทั้งกำหนดผู้รับผิดชอบในการดำเนินนโยบายและบริหารจัดการกุญแจเพื่อการเข้ารหัสข้อมูล (key management)

2. ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายการบริหารกุญแจเพื่อการเข้ารหัสข้อมูล ตลอดช่วงเวลาการใช้งาน (key management whole life cycle) โดยกำหนดแนวปฏิบัติเพื่อการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของรหัส การใช้งานและการยกเลิกการใช้งานกุญแจเพื่อการเข้ารหัส กระบวนการบริหารจัดการกุญแจเพื่อการเข้ารหัส รวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามนโยบายและแนวทางปฏิบัติดังกล่าวอย่างสม่ำเสมอ

7. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

7.1 พื้นที่หวงห้าม (secure areas)

วัตถุประสงค์

เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงพื้นที่หวงห้าม เช่น ศูนย์คอมพิวเตอร์ (data center) ศูนย์สำรอง (backup site) และพื้นที่ที่ตั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ ได้แก่ floor swith หรือ router ซึ่งอาจก่อให้เกิดความเสียหายต่ออุปกรณ์สารสนเทศหรือมีผลกระทบต่อข้อมูลที่เป็นความลับหรือมีความสำคัญ

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องประเมินความเสี่ยงและกำหนดระดับความสำคัญของทรัพย์สินสารสนเทศให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ พร้อมทั้งกำหนดพื้นที่การจัดวางทรัพย์สินสารสนเทศดังกล่าวที่มีความสำคัญให้เป็นพื้นที่หวงห้าม (physical security perimeter)

2. ผู้ประกอบธุรกิจต้องออกแบบพื้นที่หวงห้ามโดยคำนึงถึงความมั่นคงปลอดภัยจากภัยธรรมชาติและภัยคุกคามจากมนุษย์ และให้มีความมิดชิด รวมทั้งป้องกันมิให้มีการเปิดเผยข้อมูลและรายละเอียดของพื้นที่หวงห้ามต่อสาธารณะ

3. ผู้ประกอบธุรกิจต้องกำหนดสิทธิการเข้าออกพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องภายใต้หลักความจำเป็นในการรู้ข้อมูล (need-to-know basis) รวมทั้งต้องจัดให้มีระบบการควบคุมการเข้าออกอย่างรัดกุม และทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

4. ผู้ประกอบธุรกิจต้องจัดให้มีการรักษาความมั่นคงปลอดภัยให้กับศูนย์คอมพิวเตอร์ เช่น มีระบบกล้องวงจรปิด อุปกรณ์เตือนไฟไหม้ ถังดับเพลิงหรือระบบดับเพลิงแบบอัตโนมัติ ระบบไฟฟ้าสำรอง (uninterrupted power supply) และระบบควบคุมอุณหภูมิและความชื้นที่เหมาะสม เป็นต้น พร้อมทั้งมีการบำรุงรักษาอย่างสม่ำเสมอ

5. ผู้ประกอบธุรกิจต้องติดตามและควบคุมบุคคลภายนอกที่เข้าปฏิบัติงานภายในพื้นที่หวงห้ามอย่างใกล้ชิด

6. ผู้ประกอบธุรกิจต้องแยกพื้นที่จุดรับส่งของ (delivery and loading area) และพื้นที่ส่วนที่ต้องมีการเข้าถึงโดยพนักงานฝ่ายอื่น เช่น ส่วนที่ใช้เก็บรายงานที่ฝ่ายคอมพิวเตอร์ได้จัดพิมพ์ให้หน่วยงานต่าง ๆ และส่วนที่ใช้เป็นที่ตั้งเครื่องบันทึกเทปการสนทนา เป็นต้น ออกจากศูนย์คอมพิวเตอร์

7. ผู้ประกอบธุรกิจต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในพื้นที่หวงห้ามอย่างมั่นคงปลอดภัย

7.2 อุปกรณ์สารสนเทศ (equipment)

วัตถุประสงค์

เพื่อป้องกันอุปกรณ์สารสนเทศมิให้สูญหาย ถูกโจรกรรม ก่อให้เกิดความเสียหาย เข้าถึงหรือถูกใช้งานโดยบุคคลที่ไม่เกี่ยวข้อง รวมทั้งเพื่อให้อุปกรณ์สารสนเทศสามารถทำงานได้อย่างต่อเนื่อง

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการป้องกันอุปกรณ์สารสนเทศที่อาจหยุดชะงักจากการทำงานผิดพลาดของระบบโครงสร้างพื้นฐาน เช่น ระบบไฟฟ้า ระบบโทรคมนาคม ระบบประปา ระบบระบายอากาศ และระบบปรับอากาศ เป็นต้น

2. ผู้ประกอบธุรกิจต้องจัดให้มีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสาร สายไฟ และอุปกรณ์ที่เกี่ยวข้องภายในองค์กร เช่น floor switch และท่อเดินสายเคเบิลและสายไฟ เพื่อมิให้มีการดักรับสัญญาณ (interception) หรือมีความเสียหายเกิดขึ้น

3. ผู้ประกอบธุรกิจต้องจัดให้มีการดูแลและบำรุงรักษาอุปกรณ์สารสนเทศอย่างถูกวิธี เพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

4. ผู้ประกอบธุรกิจต้องควบคุมมิให้มีการอุปกรณ์สารสนเทศออกนอกพื้นที่โดยมิได้รับอนุญาต โดยในกรณีที่ได้รับอนุญาต ผู้ประกอบธุรกิจต้องจัดให้มีการทำทะเบียนคุมและมีกระบวนการรักษาความมั่นคงปลอดภัย โดยให้คำนึงถึงระดับความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานในสถานที่ต่าง ๆ

5. ก่อนการยกเลิกการใช้งานหรือจำหน่ายอุปกรณ์สารสนเทศด้านเครือข่าย เช่น switch, firewall และ router เป็นต้น ผู้ประกอบธุรกิจต้องตรวจสอบอุปกรณ์สารสนเทศนั้นว่าได้มีการลบ ย้าย ทำลายข้อมูลเกี่ยวกับการปรับแต่ง (configuration) ที่สำคัญ หรือปรับค่าดังกล่าวกลับไปสู่ค่าตั้งต้น (restore from factory) ด้วยวิธีการที่ทำให้มั่นใจได้ว่าไม่สามารถกู้คืนได้อีก

6. ผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมป้องกันอุปกรณ์สารสนเทศระหว่างที่ไม่มีผู้ใช้งาน (unattended user equipment) ให้มีความปลอดภัย รวมทั้งต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลต่าง ๆ เช่น thumbdrive และ external harddisk ที่มีข้อมูลสารสนเทศที่จัดเก็บหรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (clear desk) ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) เช่น การตัดออกจากระบบ (session time out) และการล็อคหน้าจอ (lock screen) อัตโนมัติ เป็นต้น

8. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

8.1 หน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (operational procedures and responsibilities)

วัตถุประสงค์
เพื่อให้มั่นใจว่าการปฏิบัติงานด้านระบบสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีวิธีปฏิบัติงานด้านระบบสารสนเทศที่สำคัญเป็นลายลักษณ์อักษรเพื่อให้พนักงานปฏิบัติการคอมพิวเตอร์ (computer operator) สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เช่น ขั้นตอนในการเปิด-ปิดระบบ การประมวลผล การตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และต้องทบทวนวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ รวมทั้งจัดให้วิธีปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้

2. ผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมการปฏิบัติงานอย่างเคร่งครัด โดยเฉพาะในกรณีที่มีการเปลี่ยนแปลงโครงสร้างองค์กร ขั้นตอนการปฏิบัติงาน หรือการทำงานของระบบงานต่าง ๆ ซึ่งอาจกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ตัวอย่างของการควบคุมดังกล่าว เช่น
   - กำหนดขั้นตอนหรือวิธีปฏิบัติที่เป็นลายลักษณ์อักษร ในกรณีการเปลี่ยนแปลงที่มีนัยสำคัญ
   - มีแผนรองรับ และดำเนินการทดสอบภายหลังการเปลี่ยนแปลง
   - มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง
   - มีขั้นตอนการขออนุมัติจากผู้มีอำนาจ
   - มีขั้นตอนการตรวจสอบเพื่อให้มั่นใจว่ากระบวนการเปลี่ยนแปลงดังกล่าวเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ
   - มีการสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง
   - มีกระบวนการถอยกลับสู่สภาพเดิม (fall-back) ของระบบงาน หากเกิดข้อผิดพลาดระหว่างการเปลี่ยนแปลง

3. ผู้ประกอบธุรกิจต้องติดตามประสิทธิภาพการทำงานของระบบงานและอุปกรณ์สารสนเทศที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพและความเพียงพอ (capacity) ของระบบงาน อุปกรณ์สารสนเทศ และบุคลากร เพื่อให้สามารถรองรับแผนการปฏิบัติงานในอนาคตได้อย่างมีประสิทธิภาพด้วย

4. ผู้ประกอบธุรกิจต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) และใช้งานจริง (production environment) ออกจากกัน และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้อง

ในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่แยกไว้ต่างหากภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

8.2 การป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี (protection from malware)

วัตถุประสงค์
เพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการป้องกันภัยคุกคามจากโปรแกรมไม่ประสงค์ดี

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการป้องกันและตรวจสอบโปรแกรมไม่ประสงค์ดี รวมทั้งแก้ไขเพื่อให้ระบบกลับมาใช้งานได้ตามปกติ (recovery) โดยขั้นต่ำต้องกำหนดมาตรการ ดังนี้
   (1) กำหนดนโยบายห้ามใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต
   (2) มีกระบวนการป้องกัน และตรวจสอบการใช้ซอฟต์แวร์ที่ไม่ได้รับอนุญาต และการใช้งานเว็บไซต์ที่อาจมีโปรแกรมไม่ประสงค์ดี
   (3) ติดตั้งซอฟต์แวร์ตรวจสอบโปรแกรมไม่ประสงค์ดี และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ พร้อมทั้งกำหนดผู้มีหน้าที่รับผิดชอบให้รายงานและแก้ไขปัญหากรณีพบภัยคุกคาม
   (4) ตรวจสอบซอฟต์แวร์ระบบงานที่มีความสำคัญอย่างสม่ำเสมอ หากพบการติดตั้งหรือเปลี่ยนแปลงที่ไม่ได้รับอนุญาต ต้องมีการตรวจสอบ
   (5) จัดให้มีการติดตามและกลั่นกรองข่าวสารเกี่ยวกับภัยคุกคาม เพื่อให้ทราบข้อเท็จจริง รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้ตระหนักถึงภัยคุกคามดังกล่าว

8.3 การสำรองข้อมูล (backup)

วัตถุประสงค์
เพื่อป้องกันการสูญหายของข้อมูล

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายสำรองข้อมูลสำคัญทางธุรกิจ รวมถึงระบบปฏิบัติการ (operating system) แอพพลิเคชั่นระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง โดยขั้นต่ำต้องพิจารณา ดังนี้
   (1) กำหนดขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูลเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงาน โดยอย่างน้อยต้องมีรายละเอียดเกี่ยวกับ
      (ก) ข้อมูลที่ต้องสำรอง
      (ข) ความถี่ในการสำรอง
      (ค) ประเภทสื่อบันทึกข้อมูล

(ง) จำนวนที่ต้องสำรอง

(จ) ขั้นตอนและวิธีการสำรองโดยละเอียด

(ฉ) สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล

(ช) กระบวนการกู้คืนข้อมูลในกรณีที่สูญหาย

(2) จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่าง ๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหายตามที่กล่าวในหัวข้อการสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อมด้วย

(3) กำหนดเป้าหมายในการกู้คืนข้อมูล เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (recovery point objective : RPO)

(4) จัดให้มีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลรวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและสามารถใช้งานได้ภายในระยะเวลาที่กำหนด

(5) ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น กรณีที่จัดเก็บข้อมูลในสื่อบันทึกประเภทใด ต้องมีการเก็บอุปกรณ์และโปรแกรมที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

8.4 การบันทึก จัดเก็บหลักฐานและติดตาม (logging and monitoring)

วัตถุประสงค์

เพื่อบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศอย่างครบถ้วนและเพียงพอสำหรับการตรวจสอบการล่วงรู้ข้อมูลภายในระหว่างหน่วยงานและบุคลากร การสอบทานการใช้งานข้อมูลและระบบสารสนเทศตามหน้าที่ที่ผู้ปฏิบัติงานได้รับมอบหมาย การตรวจสอบการเข้าใช้งานระบบสารสนเทศโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง การตรวจสอบและป้องกันการใช้งานระบบสารสนเทศที่มีความผิดปกติหรือไม่เป็นไปตามที่กฎหมายหรือหลักเกณฑ์ของทางการ และการตรวจสอบตัวตนของลูกค้าที่ทำรายการซื้อขายผ่านระบบอินเทอร์เน็ต รวมทั้งเพื่อให้มีการติดตามและวิเคราะห์หลักฐานที่จัดเก็บ

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการบันทึกและจัดเก็บหลักฐาน (logs) ของระบบงานที่มีความสำคัญประเภทต่าง ๆ ดังต่อไปนี้

(1) หลักฐานการเข้าถึงพื้นที่หวงห้าม (physical access log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบุคคลที่เข้าถึง ความพยายามในการเข้าถึง (ถ้ามี) และวันเวลาที่ผ่านเข้าออก โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 6 เดือน

(2) หลักฐานการเข้าถึงระบบปฏิบัติการ ฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ (authentication log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน วันเวลาที่เข้าใช้งาน และความพยายามในการเข้าใช้งาน โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 6 เดือน

(3) หลักฐานการเข้าถึงและใช้งานระบบสารสนเทศ เช่น ระบบซื้อขาย ระบบปฏิบัติการหลักทรัพย์ หรือระบบงานอื่น ๆ ที่ผู้ประกอบธุรกิจกำหนด (application log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน หมายเลขประจำเครื่องที่ใช้งาน (client IP address) (ถ้ามี) วันเวลาที่มีการใช้งาน order ID และ account ID โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 2 ปี ทั้งนี้ หากผู้ประกอบธุรกิจใช้หมายเลขประจำเครื่องแบบพลวัต (dynamic IP address) ผู้ประกอบธุรกิจต้องมีข้อมูลที่สามารถระบุผู้ใช้งานและหมายเลข IP address ในช่วงเวลาที่ใช้งานดังกล่าวได้ด้วย

(4) หลักฐานการบริหารระบบปฏิบัติการ (event log) หลักฐานบันทึกข้อมูลจราจรคอมพิวเตอร์ (traffic log) ของอุปกรณ์เครือข่ายที่สำคัญ และหลักฐานการจัดการบริหารข้อมูล (database log) โดยให้เป็นไปตามการประเมินความเสี่ยงขององค์กรและเพียงพอต่อการตรวจสอบ

(5) หลักฐานการใช้งานแฟ้มข้อมูล (audit log) เช่น read, write, copy และ delete เป็นต้น ตามประกาศว่าด้วยแนวทางปฏิบัติเกี่ยวกับระบบงานในการป้องกันมิให้เกิดการกระทำที่อาจมีความขัดหรือแย้งกับประโยชน์ของลูกค้า โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 6 เดือน

(6) หลักฐานการใช้งานอินเทอร์เน็ตที่เกิดขึ้นจากการใช้งานผ่านเครือข่ายสารสนเทศของผู้ประกอบธุรกิจ (internet access log) โดยขั้นต่ำต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน หมายเลขประจำเครื่องที่ใช้งาน (IP address) หมายเลขอินเทอร์เน็ตของผู้ประกอบธุรกิจ (organization IP address) วันเวลาที่มีการใช้งาน และที่อยู่ของเว็บไซต์ปลายทาง (full URL) โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 2 ปี ทั้งนี้ หากผู้ประกอบธุรกิจใช้หมายเลขประจำเครื่องแบบพลวัต (dynamic IP address) ผู้ประกอบธุรกิจต้องมีข้อมูลที่สามารถระบุผู้ใช้งานและหมายเลข IP address ในช่วงเวลาที่ใช้งานดังกล่าวได้ด้วย

2. ผู้ประกอบธุรกิจต้องจัดเก็บข้อมูลการติดต่อสนทนาผ่านช่องทางอิเล็กทรอนิกส์ (electronic messaging) ตามประกาศว่าด้วยแนวทางปฏิบัติเกี่ยวกับระบบงานในการป้องกันมิให้เกิดการกระทำที่อาจมีความขัดหรือแย้งกับประโยชน์ของลูกค้า โดยให้จัดเก็บเป็นระยะเวลาไม่น้อยกว่า 6 เดือน เช่น จัดเก็บข้อความในจดหมายอิเล็กทรอนิกส์ (email archive) เป็นต้น

3. ผู้ประกอบธุรกิจต้องจัดให้มีการป้องกันข้อมูลและระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศ จากการถูกเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต และมีการตรวจสอบอย่างสม่ำเสมอทั้งกรณีของ system administrator logs และ system operator logs

4. ผู้ประกอบธุรกิจต้องกำหนดระบบเวลาของอุปกรณ์และระบบสารสนเทศที่มีความสำคัญ ให้ตรงกับเวลาอ้างอิงสากล (stratum 0) โดยผิดพลาดไม่เกิน 100 มิลลิวินาที

5. ผู้ประกอบธุรกิจต้องจัดให้มีการติดตามและวิเคราะห์หลักฐานที่ถูกจัดเก็บสำหรับการใช้งานระบบสารสนเทศที่มีความสำคัญ โดยให้สอดคล้องกับการประเมินความเสี่ยงขององค์กร และเป็นไปตามที่กำหนดไว้ในนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

8.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน (installation of software on operational systems)

วัตถุประสงค์
เพื่อควบคุมให้ระบบงานทำงานโดยมีความถูกต้อง ครบถ้วน และน่าเชื่อถือ (integrity of operational system)

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีขั้นตอนเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน รวมทั้งจัดให้มีมาตรการเพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน

8.6 การบริหารจัดการช่องโหว่ทางเทคนิค (technical vulnerability management)

วัตถุประสงค์
เพื่อป้องกันภัยคุกคามจากช่องโหว่ทางเทคนิค

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจเป็นความเสี่ยงต่อระบบสารสนเทศของผู้ประกอบธุรกิจอย่างทันต่อเหตุการณ์ รวมทั้งต้องจัดให้มีการตรวจสอบหาช่องโหว่ดังกล่าวและมีมาตรการดำเนินการเพื่อปิดช่องโหว่หรือกำหนดแผนรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ดังกล่าว โดยขั้นต่ำต้องกำหนดแนวทางดำเนินการดังนี้
   (1) กำหนดผู้มีหน้าที่รับผิดชอบในการจัดการเกี่ยวกับช่องโหว่ทางเทคนิค โดยครอบคลุมถึงการประเมินความเสี่ยงของทรัพย์สินสารสนเทศที่เกี่ยวข้องซึ่งอาจได้รับผลกระทบจากช่องโหว่ดังกล่าว โดยเฉพาะทรัพย์สินสารสนเทศที่มีความเสี่ยงสูง การดำเนินการเพื่อปิดช่องโหว่ (patching) และการประสานงานกับบุคคลที่เกี่ยวข้อง
   (2) มีการประเมินความเสี่ยงของโปรแกรมเพื่อปิดช่องโหว่ (patches) โดยก่อนการติดตั้งโปรแกรมต้องมีการทดสอบและประเมินผลกระทบที่อาจเกิดจากการติดตั้งโปรแกรมดังกล่าว ทั้งนี้ กรณีที่ไม่มีโปรแกรมเพื่อปิดช่องโหว่ ให้ปฏิบัติตามคำแนะนำของบริษัทผู้ผลิตทรัพย์สินสารสนเทศที่เกี่ยวข้อง

(3) มีการทดสอบการบุกรุกระบบ (penetration test) กับระบบงานที่มีความสำคัญทุกระบบ โดยผู้ประกอบธุรกิจอาจพิจารณาเลือกจัดทำการทดสอบกับบางระบบงานตามการวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) ได้ โดยต้องจัดทำการทดสอบอย่างน้อยทุก 3 ปี และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ อย่างไรก็ดี ผู้ประกอบธุรกิจยังคงต้องจัดให้มีการทดสอบกับระบบงานที่มีความสำคัญอื่น ๆ ให้ครบถ้วน อย่างน้อยทุก 6 ปี

(4) กระบวนการจัดการช่องโหว่ด้านเทคนิคต้องสอดคล้องกับกระบวนการจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident management) เพื่อเตรียมความพร้อมรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ ทั้งนี้ ให้รวมถึงกรณีที่ตรวจพบช่องโหว่แต่ยังไม่สามารถหาวิธีปิดช่องโหว่ได้

(5) มีการบันทึกและจัดเก็บหลักฐานเพื่อการตรวจสอบในการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ทางเทคนิค

8.7 การตรวจสอบระบบสารสนเทศ (information systems audit)

วัตถุประสงค์

เพื่อจัดให้มีการวางแผนการตรวจสอบระบบสารสนเทศอย่างเพียงพอเหมาะสม โดยการตรวจสอบดังกล่าวต้องส่งผลกระทบต่อการปฏิบัติงานน้อยที่สุด

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการวางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

2. ผู้ประกอบธุรกิจต้องกำหนดขอบเขตการตรวจสอบทางเทคนิค (technical audit test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญ และต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ

3. ในกรณีที่การตรวจสอบระบบสารสนเทศมีโอกาสกระทบต่อความพร้อมใช้งานของระบบ (system availability) ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบนอกเวลาทำการ

9. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

9.1 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (network security management)

วัตถุประสงค์
เพื่อป้องกันการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายคอมพิวเตอร์

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคงปลอดภัย โดยขั้นต่ำควรมีการดำเนินการดังนี้
   (1) แบ่งแยกหน้าที่ความรับผิดชอบระหว่าง network administrator และ computer administrator ออกจากกัน พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบและขั้นตอนในการบริหารจัดการระบบและอุปกรณ์เครือข่ายให้ชัดเจน
   (2) จำกัดการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างเครือข่าย เช่น จำกัดการใช้งานจุดเชื่อมต่อระบบเครือข่าย (port outlet)
   (3) เปิดใช้งาน service port ที่เชื่อมต่อตามความจำเป็น พร้อมทั้งมีวิธีการเพื่อระบุถึงอุปกรณ์ที่เชื่อมต่อ (authenticate) อย่างชัดเจน เช่น IP address และประเภทของอุปกรณ์ เป็นต้น
   (4) มีการควบคุมการเชื่อมต่อกับระบบเครือข่ายสาธารณะ (public network) และระบบเครือข่ายไร้สาย (wireless network) อย่างรัดกุม เพื่อป้องกันการรั่วไหลหรือเปลี่ยนแปลงแก้ไขข้อมูลที่ส่งผ่านระบบเครือข่ายดังกล่าว รวมทั้งเพื่อป้องกันระบบที่เชื่อมต่อและแอพพลิเคชั่นที่ใช้งาน เช่น การเข้ารหัสเครือข่าย หรือการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ออกจากกัน เป็นต้น นอกจากนี้ จะต้องจัดให้มีการควบคุมเป็นพิเศษเพื่อให้ระบบเครือข่ายดังกล่าวอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ เช่น จัดให้มีระบบเครือข่ายคอมพิวเตอร์ที่ใช้งานทดแทนกันได้ (network load balance) เป็นต้น
   (5) มีการบันทึกและจัดเก็บหลักฐาน (logs) เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้องหรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

2. ผู้ประกอบธุรกิจต้องจัดทำข้อตกลงการใช้บริการระบบเครือข่ายคอมพิวเตอร์ (network services agreements) กับผู้ให้บริการภายนอก โดยมีเนื้อหาครอบคลุมถึงวิธีการบริหารจัดการ คุณภาพการให้บริการ รวมทั้งกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ ทั้งนี้ ในกรณีการใช้บริการจากผู้ให้บริการภายในองค์กร ให้ผู้ประกอบธุรกิจจัดให้เป็นไปตามนโยบายด้านระบบสารสนเทศขององค์กร

3. ผู้ประกอบธุรกิจต้องจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขต (domain) ของระบบเครือข่ายย่อยอย่างชัดเจน และจัดให้มีกระบวนการควบคุมการเข้าถึงขอบเขตดังกล่าวโดยสอดคล้องเหมาะสมกับระดับความต้องการด้านการรักษาความมั่นคงปลอดภัยของแต่ละขอบเขตที่ถูกจัดแบ่ง

9.2 การควบคุมการรับส่งข้อมูลสารสนเทศ (information transfer)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างระบบเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอก

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายและหลักปฏิบัติเพื่อปกป้องข้อมูลสารสนเทศที่รับส่งผ่านระบบและอุปกรณ์ในการสื่อสารทุกประเภท โดยมีเนื้อหาขั้นต่ำครอบคลุมถึง
   (1) แนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่าง ๆ
   (2) กระบวนการป้องกันการรับส่งข้อมูลสารสนเทศนอกเส้นทางที่ได้กำหนดไว้ (mis-routing) การดักรับสัญญาณ การเปลี่ยนแปลงแก้ไขหรือทำความเสียหายกับข้อมูล และโปรแกรมไม่ประสงค์ดีที่ถูกส่งผ่านช่องทางการสื่อสาร
   (3) กระบวนการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) และการส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกองค์กร
   (4) การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารบางประเภทที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ cloud computing เป็นต้น

2. ในการใช้งานระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (electronic messaging) ผู้ประกอบธุรกิจต้องคำนึงถึงความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านช่องทางดังกล่าว โดยต้องจัดให้มีมาตรการป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และมีกระบวนการตรวจสอบผู้ใช้งานอย่างเข้มงวดในกรณีที่ใช้งานผ่านเครือข่ายสาธารณะรวมทั้งต้องจัดการและควบคุมให้ระบบทำงานรับส่งข้อมูลได้อย่างถูกต้องและพร้อมใช้งานอยู่เสมอ ทั้งนี้ การใช้งานระบบส่งข้อความผ่านทางอิเล็กทรอกนิกส์ที่ให้บริการโดยบุคคลภายนอก เช่น โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (instant messaging) ระบบเครือข่ายสังคมออนไลน์ (social networking) หรือโปรแกรมเรียกใช้แฟ้มข้อมูลร่วมกัน (file sharing) ผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมดูแลอย่างเหมาะสมเพียงพอ เช่น มีการขออนุมัติก่อนการใช้งาน รวมทั้งต้องปฏิบัติตามกฎหมายและหลักเกณฑ์ของทางการอย่างเคร่งครัด

3. ผู้ประกอบธุรกิจต้องจัดให้พนักงานและผู้ให้บริการภายนอก มีการทำสัญญารักษาความลับหรือไม่เปิดเผยข้อมูลที่มีความสำคัญ โดยขั้นต่ำต้องมีเนื้อหาครอบคลุมถึง

(1) การระบุความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และวิธีป้องกันการรั่วไหลของข้อมูล

(2) การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ต้องจัดให้มีการลงนามโดยผู้รับผิดชอบ

(3) การกำหนดขั้นตอนการขออนุญาตเข้าถึงข้อมูลหรือกำหนดสิทธิการเข้าถึงข้อมูลตามที่ได้ลงนาม

(4) การกำหนดสิทธิการเข้าถึงข้อมูลเพื่อตรวจสอบหรือติดตามการใช้งานข้อมูลที่มีความสำคัญ

(5) การกำหนดกระบวนการแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

(6) การกำหนดมาตรการดำเนินการกรณีละเมิดหรือยกเลิกสัญญา รวมทั้งข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดสัญญา

10. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

10.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (security requirements of information systems)

วัตถุประสงค์
เพื่อกำหนดให้กระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของระบบสารสนเทศของทั้งภายในองค์กรและที่เกี่ยวข้องกับการให้บริการภายนอกผ่านเครือข่ายสาธารณะ ตลอดช่วงอายุการใช้งานระบบสารสนเทศ (entire life cycle) ได้แก่ กระบวนการจัดหา กระบวนการพัฒนาระบบ (system development life cycle) การใช้งาน และการดูแลรักษา

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องระบุข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศไว้เป็นส่วนหนึ่งเมื่อจัดให้มีระบบสารสนเทศใหม่หรือเมื่อปรับปรุงระบบเก่า

2. ผู้ประกอบธุรกิจต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการการใช้งาน (application service) ทั้งในกรณีทั่วไปและกรณีที่ผ่านเครือข่ายสาธารณะ เพื่อป้องกันการกระทำผิดในลักษณะทุจริต (fraudulent activities) การทำธุรกรรมที่ไม่สมบูรณ์หรือผิดพลาด (incomplete transmission or mis-routing) หรือการเปิดเผย คัดลอก หรือเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

10.2 การรักษาความมั่นคงปลอดภัยในกระบวนการพัฒนาระบบสารสนเทศ (security in development and support process)

วัตถุประสงค์
เพื่อจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตลอดช่วงการพัฒนาระบบสารสนเทศ (system development life cycle)

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้ เช่น
   (1) มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง
   (2) มีการกำหนดวิธีปฏิบัติให้คำขอให้แก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิและอนุมัติคำขอโดยผู้มีอำนาจ ต้องควบคุมผลข้างเคียงที่อาจเกิดขึ้นเนื่องจากมีการแก้ไข มีการตรวจรับจากผู้มีอำนาจ

ภายหลังการแก้ไขหรือพัฒนาแล้วเสร็จก่อนโอนย้ายระบบงาน รวมทั้งมีการจัดเก็บรายละเอียดของคำขอไว้ เป็นต้น

(3) กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจทุกครั้ง

(4) ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

(5) จัดเก็บโปรแกรม version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับสู่สภาพเดิม (fall-back) ของระบบงาน ในกรณีระบบงานผิดพลาดหรือไม่สามารถใช้งานได้

(6) มีการสื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

(7) บันทึกและจัดเก็บหลักฐานทั้งหมด (audit trail) ที่เกี่ยวข้องกับการเปลี่ยนแปลง เพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

2. ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (business continuity plan) ให้สอดคล้องกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศดังกล่าว

3. ผู้ประกอบธุรกิจต้องควบคุมสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ (development environment) ซึ่งได้แก่ บุคลากรผู้พัฒนาระบบ ขั้นตอนการพัฒนาระบบ และเทคโนโลยีสำหรับการพัฒนาระบบให้มีความมั่นคงปลอดภัยตลอดขั้นตอนการพัฒนาระบบ โดยคำนึงถึง

(1) การรักษาความลับของข้อมูลที่นำมาประมวลผล จัดเก็บ และส่งผ่านระบบ และการควบคุมการนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา

(2) การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม

(3) การติดตามหากมีการเปลี่ยนแปลงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ

(4) มีการจัดเก็บข้อมูลสำรองในพื้นที่นอกองค์กรที่มีความมั่นคงปลอดภัย

4. ผู้ประกอบธุรกิจต้องจัดให้มีการดูแล ติดตาม และควบคุมการปฏิบัติงานของผู้ให้บริการพัฒนาระบบงานสารสนเทศจากภายนอก (outsourced system development) ให้เป็นไปตามนโยบายการพัฒนาระบบงานสารสนเทศของบริษัท ภายใต้ข้อตกลงที่ให้สิทธิผู้ประกอบธุรกิจสามารถเข้าตรวจสอบการปฏิบัติงานดังกล่าวได้

5. ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบการทำงานของระบบที่ได้รับการพัฒนาโดยผู้ใช้งาน หรือผู้ทดสอบอื่นที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว เพื่อให้มั่นใจได้ว่าระบบที่ได้รับการพัฒนาดังกล่าวสามารถทำงานได้ถูกต้องตรงความต้องการของผู้ใช้งาน และเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งนี้ ผู้ประกอบธุรกิจควรระมัดระวังโดยจัดให้มีแนวทางควบคุมและป้องกันการรั่วไหลของข้อมูลที่ใช้ในการทดสอบ หากข้อมูลดังกล่าวเป็นความลับหรือมีความสำคัญ

11. การควบคุมดูแลผู้ให้บริการภายนอก (Supplier Relationship)

11.1 การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจากผู้ให้บริการภายนอก (information security in supplier relationships)

วัตถุประสงค์
เพื่อป้องกันทรัพย์สินสารสนเทศของผู้ประกอบธุรกิจจากการเข้าถึงโดยผู้ให้บริการภายนอกอย่างไม่เหมาะสม

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายในการควบคุมดูแลผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร เพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศของผู้ประกอบธุรกิจอย่างไม่เหมาะสม ทั้งนี้ นโยบายดังกล่าวต้องมีเนื้อหาขั้นต่ำครอบคลุมประเด็นดังต่อไปนี้

(1) กำหนดข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและกระบวนการควบคุมอย่างเป็นลายลักษณ์อักษร และมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและผู้ให้บริการภายนอก

(2) กำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอก

(3) ระบุประเภทข้อมูลสารสนเทศที่อนุญาตให้ผู้บริการภายนอกเข้าถึง เพื่อให้การกำหนดมาตรการควบคุมและติดตามการเข้าถึงข้อมูลเป็นไปอย่างเหมาะสม ภายใต้หลักความจำเป็นในการรู้ข้อมูล (need-to-know basis)

(4) จัดให้มีขั้นตอนและกระบวนการติดตามควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม

(5) มีการควบคุมความครบถ้วนถูกต้องของข้อมูลและการประมวลผลข้อมูลที่ได้รับจากผู้ให้บริการภายนอก

(6) กำหนดกระบวนการควบคุมอย่างเป็นมาตรฐานเพื่อติดตามการทำงานของผู้ให้บริการภายนอก

(7) ผู้ให้บริการภายนอกต้องกำหนดแผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy) ให้สอดคล้องกับแผนของผู้ประกอบธุรกิจ รวมทั้งกำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกในการกู้คืนระบบงานให้เป็นไปตามข้อตกลงที่ได้กำหนดไว้ เพื่อให้ข้อมูลและการประมวลผลข้อมูลอยู่ในสภาพที่พร้อมใช้งานเสมอ

(8) มีการจัดอบรมให้กับบุคคลที่เกี่ยวข้องกับการจัดหาผู้ให้บริการภายนอก เพื่อให้ทราบถึงนโยบาย ขั้นตอน และกระบวนการ

(9) มีการรักษาความมั่นคงปลอดภัยในกรณีที่มีการเคลื่อนย้ายหรือถ่ายโอนข้อมูลสารสนเทศ

2. ข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ต้องมีเนื้อหาขั้นต่ำดังนี้
   (1) รายละเอียดของข้อมูลที่จำเป็นต้องใช้หรือเข้าถึงโดยผู้ให้บริการภายนอก รวมทั้งวิธีการเข้าถึงข้อมูลดังกล่าว
   (2) การจัดแบ่งประเภทข้อมูลโดยต้องสอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
   (3) มีมาตรการดำเนินการเพื่อให้มั่นใจได้ว่าข้อมูลที่เป็นความลับหรือมีความสำคัญ ทรัพย์สินทางปัญญาและลิขสิทธิ์ของผู้ประกอบธุรกิจได้รับการคุ้มครองอย่างปลอดภัยตามกฎหมายและหลักเกณฑ์ของทางการที่เกี่ยวข้อง
   (4) กำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกในการปฏิบัติงานภายใต้การควบคุมต่าง ๆ เช่น กำหนดเงื่อนไขการเข้าถึงข้อมูลของผู้ใช้บริการ ติดตามตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอกให้เป็นไปตามข้อตกลงของผู้ใช้บริการ กำหนดให้ผู้ให้บริการภายนอกรายงานผลการปฏิบัติงานให้ผู้ใช้บริการทราบเมื่อร้องขอ การแก้ไขปัญหาต่าง ๆ ภายในระยะเวลาที่กำหนด รวมทั้งการปฏิบัติงานให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ใช้บริการ
   (5) แนวทางการใช้งานข้อมูลสารสนเทศอย่างถูกต้องเหมาะสม
   (6) แนวทางการแก้ไขปัญหากรณีที่เกิดข้อผิดพลาดจากการปฏิบัติหน้าที่
   (7) แผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (incident response policy)
   (8) รายชื่อและช่องทางสำหรับติดต่อบุคคลหรือหน่วยงานอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งบุคคลหรือหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
   (9) สิทธิในการเข้าตรวจสอบกระบวนการปฏิบัติงานของผู้ให้บริการภายนอก รวมทั้งควบคุมให้มีการปฏิบัติงานเป็นไปตามข้อตกลงที่ได้กำหนดไว้ ทั้งนี้ ในกรณีที่ผู้ให้บริการภายนอกประกอบธุรกิจในต่างประเทศและมีข้อจำกัดในการเข้าตรวจสอบการปฏิบัติงานดังกล่าว ผู้ประกอบธุรกิจควรมีมาตรการเพื่อให้มั่นใจได้ว่ามีการควบคุมผู้ให้บริการภายนอกให้ปฏิบัติงานเป็นไปตามข้อตกลงที่ได้กำหนดไว้อย่างเหมาะสม
   (10) ข้อกำหนดเพิ่มเติมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีที่ผู้ให้บริการภายนอกมอบหมายการปฏิบัติงานให้กับบุคคลอื่นต่อ (sub-contracting to another supplier)

11.2 การควบคุมการส่งมอบงานของผู้ให้บริการ (Supplier Service Delivery Management)

วัตถุประสงค์
เพื่อควบคุมผู้ให้บริการภายนอกส่งมอบงานให้เป็นไปตามข้อตกลงที่จัดทำไว้กับผู้ประกอบธุรกิจ

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการติดตาม ทบทวน และตรวจสอบผู้ให้บริการภายนอกอย่างสม่ำเสมอ ทั้งในด้านฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการให้บริการ

2. ในกรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน รวมถึงการเปลี่ยนแปลงผู้ให้บริการภายนอก ผู้ประกอบธุรกิจต้องจัดให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว และกำหนดกระบวนการบริหารจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสม

12. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถและประสบการณ์ โดยขั้นต่ำต้องมีการกำหนดขั้นตอนและกระบวนการดังต่อไปนี้

(1) การกำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร

(2) การประเมินเหตุการณ์หรือจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(3) จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) และรายงานเหตุการณ์ต่อคณะผู้บริหารหรือผู้เกี่ยวข้องให้ทราบและดำเนินการต่อไป (escalation)

(4) การดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติอย่างรวดเร็ว

(5) การรวบรวมและจัดเก็บหลักฐานทันทีที่เกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญอย่างมีนัยสำคัญ เช่น ก่อให้เกิดความเสียหายกับข้อมูลหรือทรัพย์สินของลูกค้า โดยคำนึงถึงประเด็นสำคัญต่าง ๆ เช่น มีกระบวนการการจัดเก็บอย่างมั่นคงปลอดภัย การกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง การคัดเลือกบุคคลที่มีความรู้ความสามารถหรือมีประสบการณ์ด้านการรวบรวมและจัดเก็บหลักฐาน เพื่อวิเคราะห์ตรวจสอบและจัดทำเอกสารสรุปนำเสนอต่อบุคคลที่มีหน้าที่รับผิดชอบ เป็นต้น ทั้งนี้ การรวบรวม จัดเก็บ และนำเสนอหลักฐานต้องสอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ

(6) การบันทึกและจัดเก็บหลักฐานการบริหารจัดการทุกขั้นตอน

(7) การรายงานให้สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์รับทราบถึงสถานการณ์และผลการบริหารจัดการ

(8) การตรวจหา ติดตาม วิเคราะห์ และรายงานเหตุการณ์ ทั้งนี้ ให้รวมถึงการวิเคราะห์ภายหลังเหตุการณ์ยุติแล้ว เพื่อระบุถึงสาเหตุของเหตุการณ์และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต

2. ผู้ประกอบธุรกิจต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ ผ่านบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) โดยให้ดำเนินการดังนี้

(1) จัดทำแบบฟอร์มที่เป็นมาตรฐานเพื่อรองรับการรายงานสถานการณ์ และสร้างความเข้าใจให้กับผู้รายงานเกี่ยวกับการดำเนินการต่าง ๆ ที่จำเป็นในกรณีที่เกิดเหตุการณ์ ทั้งนี้ เนื้อหาขั้นต่ำต้องประกอบด้วย วันเวลา เหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น การดำเนินการแก้ไข ผลการแก้ไข ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางการป้องกันในอนาคต

(2) รายงานคณะผู้บริหารขององค์กรเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น พบช่องโหว่ในการควบคุมความมั่นคงปลอดภัย (ineffective security control) เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศ ข้อผิดพลาดจากการปฏิบัติงาน (human errors) การบุกรุกด้านกายภาพ (breaches of physical security arrangements) การปฏิบัติงานที่ไม่เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (non-compliances with policies) การเปลี่ยนแปลงระบบปฏิบัติการหรือชุดคำสั่งที่ควบคุมระบบงานโดยไม่ได้รับอนุญาต (uncontrolled system changes) การทำงานผิดพลาดของโปรแกรมและอุปกรณ์คอมพิวเตอร์ (malfunctions of software or hardware) และการเข้าถึงโดยไม่ได้รับอนุญาต (access violations)

(3) รายงานสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญ ประเภทดังต่อไปนี้

(ก) ระบบหยุดชะงัก (system disruption)

(ข) มีการบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised)

(ค) ส่งผลกระทบต่อชื่อเสียงของผู้ประกอบธุรกิจ (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement)

โดยให้รายงาน ดังนี้

- รายงานทันทีเมื่อทราบเหตุการณ์ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบ ที่คาดว่าจะเกิดขึ้น ทั้งนี้ อาจแจ้งโดยวาจาหรือผ่านระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (electronic messaging) ตามความเหมาะสม
- รายงานภายในวันทำการถัดไปหลังทราบเหตุการณ์ เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา และความคืบหน้าในการแก้ไขปัญหา
- รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต

(4) แจ้งบุคคลที่เกี่ยวข้อง เช่น ลูกค้า และตลาดหลักทรัพย์ รับทราบโดยไม่ชักช้า ในกรณีที่เหตุการณ์ส่งผลกระทบต่อบุคคลดังกล่าว

(5) จัดให้มีการรายงานความคืบหน้าในการบริหารจัดการสถานการณ์และผลการบริหารจัดการเป็นระยะ และเมื่อเหตุการณ์ยุติแล้ว

13. การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจ (business continuity management) ของผู้ประกอบธุรกิจ ทั้งนี้ เพื่อให้ระบบสารสนเทศอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องคำนึงถึงความมั่นคงปลอดภัยของระบบสารสนเทศเมื่อเกิดสถานการณ์ที่ไม่พึงประสงค์หรือไม่คาดคิด

2. ผู้ประกอบธุรกิจต้องจัดให้มีขั้นตอน กระบวนการดำเนินการ และการควบคุมด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้มั่นใจได้ว่ามีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ (business continuity management) โดยขั้นต่ำต้องมีรายละเอียด ดังนี้

   (1) กำหนดขั้นตอนดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้น (incident response process) ให้เป็นไปตามนโยบายการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

   (2) มีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละเหตุการณ์

   (3) มีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นของเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (specification) ขั้นต่ำ ข้อมูลเกี่ยวกับการปรับแต่ง (configuration) และอุปกรณ์เครือข่ายคอมพิวเตอร์ เป็นต้น

   (4) ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น

3. ผู้ประกอบธุรกิจต้องกำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ (recovery time objectives : RTO) พร้อมทั้งจัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญทุกระบบให้เหมาะสมกับผลกระทบที่อาจเกิดขึ้น ทั้งนี้ ระยะเวลาในการกู้คืนดังกล่าวต้องปฏิบัติได้อย่างมีประสิทธิภาพ

4. ผู้ประกอบธุรกิจควรจัดให้มีการสำรองระบบสารสนเทศ เพื่อให้อยู่ในสภาพพร้อมใช้งานหรือสอดคล้องกับ recovery time objectives ที่กำหนด

14. การควบคุมกระบวนการทำงานให้เป็นไปตามข้อกำหนด (Compliance)

14.1 การปฏิบัติให้เป็นไปตามกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญา (compliance with legal and contractual requirements)

วัตถุประสงค์

เพื่อป้องกันการละเมิดกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องระบุกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยจัดทำเป็นเอกสารและปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

2. ผู้ประกอบธุรกิจต้องกำหนดขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าในการใช้งานข้อมูลสารสนเทศที่อาจถือเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ที่พัฒนาโดยผู้ประกอบธุรกิจมีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ

3. ผู้ประกอบธุรกิจต้องป้องกันมิให้ข้อมูลบันทึกหลักฐาน (logs) ต่าง ๆ เกิดความเสียหาย สูญหาย เปลี่ยนแปลงแก้ไข เข้าถึงหรือเผยแพร่โดยไม่ได้รับอนุญาต โดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ และความต้องการทางธุรกิจ

4. ผู้ประกอบธุรกิจต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่าง ๆ

5. ผู้ประกอบธุรกิจต้องควบคุมการเข้ารหัสข้อมูลให้สอดคล้องกับกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่าง ๆ

14.2 การทบทวนมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security reviews)

วัตถุประสงค์
เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศเป็นไปตามนโยบายและหลักปฏิบัติของผู้ประกอบธุรกิจ รวมทั้งมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวทางปฏิบัติ

1. ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบขั้นตอนและการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยผู้ตรวจสอบที่เป็นอิสระจากการบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศ ซึ่งอาจเป็นหน่วยงานตรวจสอบภายในของผู้ประกอบธุรกิจ หรือผู้ตรวจสอบภายนอก อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์ที่มีนัยสำคัญ

2. ผู้ประกอบธุรกิจต้องจัดให้มีการทบทวนและปรับปรุงขั้นตอนและการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และสอดคล้องกับมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

3. ผู้ประกอบธุรกิจต้องจัดให้มีการทบทวนระบบสารสนเทศในด้านเทคนิค เช่น การทดสอบการบุกรุกระบบ (penetration test) อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ