

การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)

ขอบเขตการดำเนินการตามภาคผนวกนี้

1. ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ระดับปานกลาง หรือระดับสูง ให้ดำเนินการตามที่กำหนดในภาคผนวกนี้
2. ผู้ประกอบธุรกิจขนาดเล็ก ให้ดำเนินการอย่างน้อยในเรื่องดังนี้

2.1 การดำเนินการตามส่วนที่ 2 การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT หรือบุคคลภายนอก ข้อ 2.3 บุคคลภายนอก

2.2 การดำเนินการตามส่วนที่ 5 การกำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชี privileged user (privileged user management)

2.3 การดำเนินการตามส่วนที่ 8 มาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security) ดังนี้

ข้อ 8.1 การตั้งค่าระบบ (system configuration management)

ข้อ 8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint)

ข้อ 8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment)

ข้อ 8.10 ทดสอบเจาะระบบงาน (penetration test)

ข้อ 8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)

การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT

ส่วนที่ 1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security)

ผู้ประกอบธุรกิจต้องดำเนินการจัดให้มีโครงสร้างดังกล่าว โดยมีลักษณะอย่างน้อยดังนี้

1.1 กำหนดโครงสร้างภายในองค์กร (organizational structure) ในการปฏิบัติงานด้าน IT โดยมีรายละเอียดหน้าที่และความรับผิดชอบของบุคลากรเป็นลายลักษณ์อักษร

1.2 แบ่งแยกหน้าที่ในการปฏิบัติงานที่เกี่ยวกับความมั่นคงปลอดภัยของระบบ IT เพื่อให้มีการสอบทาน การปฏิบัติงาน และลดโอกาสในการแก้ไขเปลี่ยนแปลงหรือใช้งานทรัพยากรสินด้าน IT โดยมีชอบหรือไม่ได้รับอนุญาต

ส่วนที่ 2 การบริหารจัดการบุคลากรที่ปฏิบัติงานด้าน IT หรือบุคคลภายนอก

บุคลากรหรือบุคคลภายนอก	การบริหารจัดการ
<p>2.1 บุคลากรที่มีหน้าที่ดังนี้</p> <p>2.1.1 การปฏิบัติงานด้าน IT</p> <p>2.1.2 การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง</p> <p>2.1.3 การตรวจสอบด้าน IT</p> <p>2.2 บุคลากรอื่นนอกจาก 2.1 ที่ใช้ระบบ IT ในการปฏิบัติงาน</p>	<p>ผู้ประกอบการธุรกิจต้องบริหารจัดการบุคลากรตาม 2.1 หรือ 2.2 อย่างเหมาะสม โดยดำเนินการอย่างน้อยดังนี้</p> <p>(1) มีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่ ดังนี้</p> <p>(1.1) คำนึงถึงความรู้ ความสามารถ และความเพียงพอในการปฏิบัติงาน</p> <p>(1.2) มีการตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอ และสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ</p> <p>(2) มีการกำหนดเรื่องดังนี้ ไว้ในข้อตกลงการจ้างงานเพื่อป้องกันการละเมิดหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT ของผู้ประกอบการธุรกิจ</p> <p>(2.1) บทบาทหน้าที่และความรับผิดชอบของบุคลากรดังกล่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT</p> <p>(2.2) non-disclosure agreement</p> <p>(3) สร้างความตระหนักรู้เกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบ IT ให้แก่บุคลากรที่ปฏิบัติงานโดยมีการเข้าถึงข้อมูลหรือระบบงานภายในองค์กร เพื่อให้บุคลากรดังกล่าวสามารถปฏิบัติหน้าที่ได้ตามนโยบายและมาตรการที่กำหนด</p> <p>(4) กำหนดให้บุคลากรดังกล่าวงดเว้นการใช้งานระบบ IT ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ประกอบการธุรกิจ ตลาดทุนโดยรวม หรือที่เป็นการกระทำผิดกฎหมาย หรือข้อกำหนดและจรรยาบรรณที่ผู้ประกอบการธุรกิจกำหนดไว้ (ถ้ามี)</p> <p>(5) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT</p> <p>(6) กำหนดขั้นตอนปฏิบัติเมื่อสิ้นสุดการจ้างงาน หรือยกเลิกข้อตกลงการจ้างบุคลากร เพื่อป้องกันการละเมิดหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT</p>
<p>2.3 บุคคลภายนอก ในกรณีที่ผู้ประกอบการธุรกิจมีการดำเนินการอย่างใดอย่างหนึ่งดังนี้</p>	<p>ผู้ประกอบการธุรกิจต้องบริหารจัดการบุคคลภายนอกตาม 2.3.1 , 2.3.2 หรือ 2.3.3 ดังนี้</p> <p>(1) ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูล</p>

บุคลากรหรือบุคคลภายนอก	การบริหารจัดการ
<p>2.3.1 ใช้บริการงานด้าน IT จากบุคคลภายนอก</p> <p>2.3.2 เชื่อมต่อกับระบบ IT ของบุคคลภายนอก</p> <p>2.3.3 อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้ำที่ควบคุมดูแลโดยผู้ประกอบธุรกิจได้</p>	<p>จากบุคคลภายนอก รวมถึงผู้รับดำเนินการช่วง (subcontract) จากบุคคลภายนอก (ถ้ามี)</p> <p>(2) กำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอก</p> <p>(3) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ประกอบธุรกิจและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร</p> <p>(4) กรณีเป็นบุคคลภายนอกรายที่มีนัยสำคัญตามผลการประเมินความเสี่ยงใน 2.3 (1) ข้อตกลงหรือสัญญาการให้บริการต้องระบุสิทธิให้ผู้ประกอบธุรกิจ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ประกอบธุรกิจหรือสำนักงาน สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกดังกล่าว ในส่วนที่เกี่ยวข้องกับการให้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของผู้ประกอบธุรกิจจากบุคคลภายนอก</p> <p>หากมีเหตุจำเป็นทำให้ผู้ประกอบธุรกิจไม่สามารถระบุสิทธิในการเข้าตรวจสอบตามวรรคหนึ่งไว้ในข้อตกลงหรือสัญญา ผู้ประกอบธุรกิจต้องมีมาตรการประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอสอดคล้องกับความเสี่ยงและควมมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล</p> <p>(5) มี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้ำ</p> <p>(6) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยต้องสอดคล้องกับระดับความเสี่ยงและระดับความมีนัยสำคัญของบุคคลภายนอก</p> <p>(7) รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจ</p> <p>(8) เตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง</p>

ส่วนที่ 3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management)

ผู้ประกอบการควรจัดให้มีการบริหารจัดการทรัพย์สินด้าน IT เพื่อนำไปใช้ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT ได้อย่างเหมาะสม ครบถ้วนและเป็นปัจจุบัน ดังนี้

- 3.1 จัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ ซอฟต์แวร์ รวมถึงสิทธิในการใช้งาน ฮาร์ดแวร์และซอฟต์แวร์
- 3.2 กำหนดบุคคลหรือหน่วยงานซึ่งรับผิดชอบทรัพย์สินด้าน IT แต่ละรายการ
- 3.3 จัดให้มีการบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอ

ส่วนที่ 4 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

ผู้ประกอบการควรจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างถูกต้อง ครบถ้วน มีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับและคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม ดังนี้

- 4.1 การกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล
- 4.2 การจัดชั้นความลับของข้อมูล (data classification) และแนวทางการรักษาความปลอดภัยของข้อมูลที่สอดคล้องตามชั้นความลับ โดยครอบคลุมข้อมูลดังนี้
 - 4.2.1 ข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint)
 - 4.2.2 ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit)
 - 4.2.3 ข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest)
- 4.3 การจัดให้มีแนวทางในการนำเข้า ประมวลผล และทำลายข้อมูลอย่างปลอดภัย
- 4.4 การจัดทำทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน

ส่วนที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)

ผู้ประกอบการควรจัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบ IT อย่างมีประสิทธิภาพ เพื่อให้สามารถป้องกันการเข้าถึง และเปลี่ยนแปลงแก้ไขโดยผู้ไม่มีสิทธิหรือไม่ได้รับอนุญาต ดังนี้

- 5.1 จัดให้มีแนวทางการบริหารจัดการบัญชีผู้ใช้งานและสิทธิการเข้าถึง โดยมีการทบทวนปรับปรุงสิทธิให้เหมาะสมอย่างสม่ำเสมอ สอดคล้องกับหน้าที่ความรับผิดชอบ รวมถึงมีกระบวนการเพิกถอนสิทธิเมื่อสิ้นสุดความจำเป็นต้องใช้งาน
- 5.2 จัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมกับความเสี่ยง และป้องกันการปฏิเสธความรับผิดชอบ
- 5.3 กำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชี privileged user (privileged user management) ดังนี้

5.3.1 มี MFA เมื่อเข้าใช้งานและเปลี่ยนรหัสผ่าน สำหรับระบบปฏิบัติการและระบบฐานข้อมูลที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ

5.3.2 กรณีผู้ประกอบการธุรกิจมีข้อจำกัดสำหรับ MFA สามารถใช้วิธีการอื่นใดที่เทียบเท่าทดแทน และจัดให้มีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงก่อนดำเนินการเพื่อขออนุมัติยกเว้น (exception)

5.3.3 มีการควบคุมและติดตามตรวจสอบการใช้งานบัญชี privileged user อย่างเข้มงวด

ส่วนที่ 6 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

ผู้ประกอบการธุรกิจต้องจัดให้มีการควบคุมการเข้ารหัสที่เชื่อถือได้และเป็นไปตามมาตรฐานสากล โดยกำหนดวิธีการเข้ารหัสข้อมูล (encryption) และการบริหารจัดการกุญแจเข้ารหัส (key management) อย่างปลอดภัยเพื่อให้มั่นใจได้ว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และความถูกต้องแท้จริง (authenticity) ของข้อมูลมีความเหมาะสมและมีประสิทธิภาพ ดังนี้

6.1 กำหนดวิธีการเข้ารหัสที่ปลอดภัย

6.2 กำหนดการบริหารจัดการกุญแจเข้ารหัสโดยกำหนดให้มีมาตรการการควบคุมตั้งแต่การสร้างและติดตั้งกุญแจเข้ารหัส การจัดเก็บและสำรอง ไปจนถึงการเพิกถอนหรือทำลายกุญแจเข้ารหัส

6.3 กำหนดมาตรการการควบคุมกุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ซึ่งต้องตรวจสอบเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสที่สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคลอื่น

6.4 กำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส

ส่วนที่ 7 การสร้างความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

ผู้ประกอบการธุรกิจต้องจัดให้มีการสร้างความมั่นคงปลอดภัย รวมทั้งมีระบบการป้องกันและกระบวนการในการบำรุงรักษาฮาร์ดแวร์ และระบบสาธารณูปโภค (facilities) ทางกายภาพและสภาพแวดล้อม ที่เกี่ยวข้องกับ IT อย่างเหมาะสม เพื่อให้สามารถป้องกันการเข้าถึง และป้องกันการสร้างความเสียหายต่อทรัพย์สินด้าน IT ที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และศูนย์คอมพิวเตอร์จากบุคคลภายนอก (co-location) ตลอดจนมีการป้องกันความปลอดภัยทางกายภาพของอุปกรณ์ IT อื่น ๆ

ส่วนที่ 8 มาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)

ผู้ประกอบการธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT เพื่อให้การปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย โดยต้องครอบคลุมการบริหารจัดการอย่างน้อยในเรื่องดังนี้

8.1 การตั้งค่าระบบ (system configuration management) โดยมีกระบวนการในการควบคุมการตั้งค่าของระบบที่ใช้งานจริง และมีการสอบทานการตั้งค่าเพื่อให้การตั้งค่าระบบ IT เป็นไปอย่างถูกต้อง และปลอดภัย

8.2 การเปลี่ยนแปลงด้าน IT (change management) อย่างรัดกุมเพียงพอเพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต

8.3 การคำนึงถึงขีดความสามารถของระบบ IT (capacity management) โดยจัดให้มีมาตรฐานและวิธีปฏิบัติเรื่องการจัดการขีดความสามารถ การติดตามประสิทธิภาพการทำงานของระบบ และการประเมินแนวโน้มการใช้ทรัพยากรด้าน IT เพื่อให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และสามารถวางแผนการจัดสรรทรัพยากรให้รองรับการใช้งานในอนาคตได้อย่างมีประสิทธิภาพ

8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) เพื่อไม่ให้ถูกใช้เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหล หรือมีการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต

8.5 การกำหนดนโยบายและมาตรการรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และรวมถึงการใช้งานอุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD) โดยพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมอย่างเหมาะสม

8.6 การสำรองข้อมูล (data backup) ที่สำคัญด้วยวิธีการและความถี่ที่เหมาะสม เพื่อให้ข้อมูลสำรองมีสภาพพร้อมใช้งานสอดคล้องกับเป้าหมายการกู้คืนระบบ IT ในกรณีที่ระบบ IT และข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย โดยต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง

8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log) อย่างครบถ้วนและเพียงพอ เพื่อให้สามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ และสามารถติดตามและตรวจสอบการเข้าถึงและใช้งานข้อมูลและระบบ IT ตามที่กฎหมายกำหนด

8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT โปรแกรมไม่ประสงค์ดี (malware) หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ

8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) ของระบบ IT ที่เหมาะสมกับระดับความเสี่ยงเพื่อให้ทราบถึงช่องโหว่ และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันท่วงที โดยการประเมินช่องโหว่ทางเทคนิคครอบคลุมระบบ IT ที่มีนัยสำคัญ และระบบ IT ที่เชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) ทุกระบบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญของระบบดังกล่าว เช่น การเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ IT หรือการเพิ่มเติมฟังก์ชันสำคัญของระบบ IT เป็นต้น

8.10 การทดสอบเจาะระบบงาน (penetration test)

8.10.1 ต้องจัดให้มีการทดสอบการเจาะระบบงานดังนี้

ระบบงาน	การทดสอบ
(1) ระบบงาน (application system) และระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing)	(1.1) อย่างน้อยปีละ 1 ครั้ง และ (1.2) ทุกครั้งที่มีการเปลี่ยนแปลงระบบงานดังกล่าว อย่างมีนัยสำคัญ
(2) ระบบงานอื่น ๆ นอกจาก (1)	จัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตการทดสอบเจาะระบบและทดสอบเจาะระบบตามความเหมาะสม

8.10.2 การทดสอบการเจาะระบบงานข้างต้น ต้องดำเนินการโดยผู้เชี่ยวชาญภายในหรือภายนอกที่เป็นอิสระจากเจ้าของระบบ

8.10.3 ในกรณีที่มีการตรวจพบช่องโหว่ ผู้ประกอบธุรกิจต้องดำเนินการแก้ไข และป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นอย่างทันท่วงที เพื่อขจัดความเสี่ยงจากช่องโหว่ดังกล่าว

8.10.4 จัดเก็บรายงานการดำเนินการตาม 8.10 เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

8.10.5 นำส่งรายงานผลการเจาะระบบโดยไม่ชักช้าเมื่อได้รับการแจ้งจากสำนักงาน ตามวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน

8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management) โดยจัดให้มีกระบวนการควบคุมการติดตั้งโปรแกรมแก้ไขช่องโหว่บนระบบที่ใช้งานจริง เพื่อลดความเสี่ยงที่ระบบ IT อาจถูกโจมตีในอนาคต

ส่วนที่ 9 มาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)

ผู้ประกอบธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสารอย่างเหมาะสม เพื่อรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสาร

ส่วนที่ 10 การบริหารจัดการโครงการด้าน IT (IT project management) และมาตรการการจัดหา พัฒนา รวมถึงบำรุงรักษาระบบ IT (system acquisition, development and maintenance)

ผู้ประกอบธุรกิจต้องมีการบริหารจัดการโครงการด้าน IT และมีมาตรการการจัดหา พัฒนา รวมถึงบำรุงรักษาระบบ IT เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ IT (entire life cycle) ดังนี้

การดำเนินการ	รายละเอียด
10.1 บริหารจัดการโครงการด้าน IT (IT project management)	กำหนดกรอบการบริหารจัดการโครงการ (project management framework) เพื่อให้การบริหารจัดการโครงการที่มีนัยสำคัญเป็นไปอย่างมีประสิทธิภาพ สามารถส่งมอบโครงการได้อย่างถูกต้อง ครบถ้วนตามแผนงานและบรรลุมิติวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้
10.2 จัดหาระบบ IT (system acquisition)	จัดให้มีหลักเกณฑ์ในการจัดหาระบบ IT และผู้ให้บริการ เพื่อมั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัย IT โดยคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี รวมถึงการเปลี่ยนแปลงต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจอย่างมีนัยสำคัญ
10.3 พัฒนาระบบ IT (system development)	<p>จัดให้มีมาตรการควบคุมเกี่ยวกับการพัฒนาระบบ IT ในการออกแบบ พัฒนา ทดสอบระบบ และนำระบบขึ้นใช้งานจริง เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอจะรองรับการใช้งานได้ สอดคล้องกับแผนการดำเนินธุรกิจ โดยต้องดำเนินการอย่างน้อยดังนี้</p> <ol style="list-style-type: none"> (1) มีการกำหนดรายละเอียดความต้องการของระบบ (requirement) และคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนา ดังนี้ <ol style="list-style-type: none"> (1.1) ความมั่นคงปลอดภัย (security) (1.2) ความเป็นส่วนตัว (privacy) (1.3) สภาพพร้อมใช้งาน (availability) (1.4) ขีดความสามารถที่รองรับ (capacity) (2) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง (3) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production)

การดำเนินการ	รายละเอียด
	<p>(4) มีกระบวนการหรือเครื่องมือควบคุมการพัฒนาชุดคำสั่งคอมพิวเตอร์ให้มีความปลอดภัย</p> <p>(5) มีการทดสอบระบบ IT ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถประมวลผลได้อย่างถูกต้อง ครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน</p> <p>(6) มีมาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion)</p> <p>(7) มีมาตรการรักษาความมั่นคงปลอดภัย และความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ</p> <p>(8) มีการทดสอบประสิทธิภาพ (performance test) ของระบบที่เกี่ยวข้องกับการให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์ เมื่อมีการพัฒนาหรือเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าระบบดังกล่าวสามารถรองรับปริมาณการใช้งานได้สอดคล้องกับความต้องการทางธุรกิจ</p> <p>(9) ในกรณีที่มีการมอบให้มอบหมายให้บุคคลภายนอกเป็นผู้พัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ผู้ประกอบธุรกิจต้องจัดให้มีการติดตาม และควบคุมการดำเนินการให้ไปตามข้อตกลงในการมอบหมายงาน</p> <p>(10) มีกระบวนการขออนุมัติจากผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายจากผู้ประกอบธุรกิจ ก่อนนำระบบขึ้นใช้งานจริง</p>
<p>10.4 แก้ไขเปลี่ยนแปลงระบบ IT (system change)</p>	<p>(1) มีการประเมินผลกระทบ และจัดลำดับความสำคัญของการเปลี่ยนแปลง</p> <p>(2) มีกระบวนการอนุมัติการเปลี่ยนแปลง (change request) โดยต้องได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่าการขอเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมแล้ว</p> <p>(3) มีการทดสอบระบบภายหลังจากการเปลี่ยนแปลง</p> <p>(4) มีกระบวนการขออนุมัติจากผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายจากผู้ประกอบธุรกิจ ก่อนนำระบบขึ้นใช้งานจริง</p>

การดำเนินการ	รายละเอียด
	(5) มีกระบวนการหรือเครื่องมือควบคุมการเปลี่ยนแปลงรุ่น (version) ของชุดคำสั่งคอมพิวเตอร์ (source code version control) และรองรับการถอยกลับสู่สภาพเดิม (fallback) (6) ปรับปรุงรายละเอียดประกอบระบบงานที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้เป็นปัจจุบัน

ส่วนที่ 11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT (IT incident management)

ผู้ประกอบการต้องมีการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT อย่างเหมาะสมและทันท่วงที ดังนี้

11.1 จัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้าน IT จากบุคลากร ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง

11.2 กำหนดแผน หรือขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT

11.3 รายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลให้ทรัพย์สินด้าน IT ของผู้ใช้งานเสียหายอันเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยระบบ IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว

11.4 วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อหาแนวทางการแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

11.5 บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

11.6 ทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และปัญหาด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยต้องครอบคลุมถึงการทดสอบการบริหารจัดการเหตุการณ์ด้านภัยคุกคามทางไซเบอร์ (cyber security drill) และจัดให้มีการรายงานผลการทดสอบและทบทวนต่อคณะกรรมการของผู้ประกอบการหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบการ

ส่วนที่ 12 แผนฉุกเฉินด้าน IT (IT contingency plan)

ผู้ประกอบการต้องจัดให้มีแผนฉุกเฉินด้าน IT อย่างเป็นลายลักษณ์อักษร โดยต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบการหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบการ เพื่อรองรับเหตุการณ์ผิดปกติด้าน IT ในกรณีที่ระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินการธุรกิจอย่างต่อเนื่อง โดยต้องกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ โดยแผนฉุกเฉินด้าน IT ต้องมีลักษณะดังนี้

- 12.1 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT
- 12.2 ประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง
- 12.3 วิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากเหตุการณ์ความเสี่ยงตาม 12.2 เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ IT (Recovery Time Objective: RTO) ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (Maximum Tolerable Downtime: MTD) อย่างเหมาะสม
- 12.4 จัดให้มีระบบ IT สำรอง และทรัพยากรที่จำเป็น เพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมายที่กำหนดไว้
- 12.5 สื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม
- 12.6 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว โดยรายงานผลการทบทวนและทดสอบต่อคณะกรรมการของผู้ประกอบธุรกิจหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ
- 12.7 กำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากรด้าน IT หรือการใช้ประสิทธิภาพของระบบงานเกินขีดจำกัดของตัวชี้วัดที่กำหนดไว้ เช่น การจำกัดการให้บริการบางช่องทาง หรือตัดการเชื่อมต่อกับผู้ให้บริการหรือบุคคลภายนอกที่มีผลกระทบต่อระบบ IT เป็นต้น
- 12.8 จัดให้มีรายละเอียดในการติดต่อ ดังนี้ เพื่อให้สามารถประสานงานในการรายงานเหตุการณ์ผิดปกติด้าน IT หรือขอความช่วยเหลือจากหน่วยงานภายนอกที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ โดยต้องปรับปรุงข้อมูลดังกล่าวให้เป็นปัจจุบันอยู่เสมอ
- 12.8.1 รายชื่อหน่วยงานกำกับดูแลและบุคคลภายนอกที่ให้บริการหรือที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบธุรกิจ
- 12.8.2 ช่องทางในการติดต่อ และรายชื่อผู้ที่เกี่ยวข้องของหน่วยงานกำกับดูแลหรือบุคคลภายนอกตาม 12.8.1