

## การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)

### ขอบเขตการดำเนินการตามภาคผนวกนี้

1. ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ระดับปานกลาง หรือระดับสูง ให้ดำเนินการตามที่กำหนดในภาคผนวกนี้
2. ผู้ประกอบธุรกิจขนาดเล็ก ให้ดำเนินการรักษาความมั่นคงปลอดภัยด้าน IT ขั้นต้น อย่างน้อยในเรื่องดังนี้
  - 2.1 ส่วนที่ 2 การบริหารจัดการบุคลากร และบุคคลภายนอก ข้อ 2.2 บุคคลภายนอก
  - 2.2 ส่วนที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control) ข้อ 5.3 กำหนดมาตรการควบคุมจำกัด และติดตามการใช้งานบัญชี privileged user (privileged user management)
  - 2.3 ส่วนที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security) ดังนี้
    - ข้อ 8.1 การบริหารจัดการการตั้งค่าระบบ (system configuration management)
    - ข้อ 8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint)
    - ข้อ 8.5 การกำหนดนโยบายและมาตรการรักษาความปลอดภัยสำหรับการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD)
    - ข้อ 8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment)
    - ข้อ 8.10 การทดสอบการเจาะระบบงาน (penetration test)
    - ข้อ 8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)
  - 2.4 ส่วนที่ 11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management) ข้อ 11.3 รายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลกระทบต่อทรัพย์สินของผู้ใช้งานเสียหายอันเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT

### การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT

ส่วนที่ 1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security)

ผู้ประกอบธุรกิจต้องดำเนินการจัดให้มีโครงสร้างดังกล่าว โดยมีลักษณะอย่างน้อยดังนี้

- 1.1 กำหนดโครงสร้างภายในองค์กร (organizational structure) ในการปฏิบัติงานด้าน IT โดยมีรายละเอียดหน้าที่และความรับผิดชอบของบุคลากรเป็นลายลักษณ์อักษร
- 1.2 มีการสอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบ IT ที่อาจเกิดขึ้นในการปฏิบัติงาน

ส่วนที่ 2 การบริหารจัดการบุคลากร และบุคคลภายนอก

บุคลากรหรือบุคคลภายนอก	การบริหารจัดการ
<p>2.1 บุคลากรที่เกี่ยวข้องหรือที่ใช้ระบบ IT ปฏิบัติงาน</p>	<p>ผู้ประกอบการธุรกิจต้องบริหารจัดการบุคลากรตามข้อ 2.1 อย่างเหมาะสม โดยดำเนินการอย่างน้อยดังนี้</p> <ol style="list-style-type: none"> <li>(1) มีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่ดังนี้               <ol style="list-style-type: none"> <li>(1.1) คำนึงถึงความรู้ ความสามารถ และความเพียงพอในการปฏิบัติงาน</li> <li>(1.2) มีการตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอ และสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ</li> </ol> </li> <li>(2) มีข้อกำหนดให้บุคลากรทำความเข้าใจ รับทราบ และลงนามยอมรับในเรื่องดังนี้               <ol style="list-style-type: none"> <li>(2.1) บทบาทหน้าที่และความรับผิดชอบของบุคลการดังกล่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT</li> <li>(2.2) non-disclosure agreement</li> </ol> </li> <li>(3) สร้างความตระหนักรู้ถึงความเสี่ยงด้าน IT ให้แก่บุคลากรที่ปฏิบัติงาน ซึ่งสามารถเข้าถึงข้อมูลหรือระบบงานภายในองค์กร เพื่อให้บุคลากรดังกล่าวสามารถใช้งานระบบ IT ได้อย่างปลอดภัย</li> <li>(4) กำหนดให้บุคลการงดเว้นการใช้งานระบบ IT ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ประกอบการธุรกิจ ตลาดทุนโดยรวม หรือที่เป็น การกระทำผิดกฎหมาย หรือข้อกำหนดและจรรยาบรรณที่ผู้ประกอบการ กำหนดไว้ (ถ้ามี)</li> <li>(5) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT</li> <li>(6) กำหนดขั้นตอนปฏิบัติเมื่อสิ้นสุดการจ้างงาน หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน เพื่อป้องกันการละเมิดหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT</li> </ol>
<p>2.2 บุคคลภายนอก ในกรณีที่ผู้ประกอบการมีการดำเนินการอย่างใดอย่างหนึ่งดังนี้</p>	<p>ผู้ประกอบการธุรกิจต้องบริหารจัดการบุคคลภายนอกตามข้อ 2.2.1 , 2.2.2 หรือ 2.2.3 ดังนี้</p> <ol style="list-style-type: none"> <li>(1) ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูล</li> </ol>

บุคลากรหรือบุคคลภายนอก	การบริหารจัดการ
<p>2.2.1 ใช้บริการงานด้าน IT จากบุคคลภายนอก</p> <p>2.2.2 เชื่อมต่อระบบ IT กับบุคคลภายนอก</p> <p>2.2.3 อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยผู้ประกอบธุรกิจได้</p>	<p>จากบุคคลภายนอก รวมถึงผู้รับดำเนินการช่วง (subcontract) จากบุคคลภายนอก (ถ้ามี)</p> <p>(2) กำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอก</p> <p>(3) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ประกอบธุรกิจและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร</p> <p>(4) กรณีบุคคลภายนอกซึ่งเป็นผู้ให้บริการงานด้าน IT รายที่มีนัยสำคัญตามผลการประเมินความเสี่ยงในข้อ 2.2 (1) ข้อตกลงหรือสัญญาการให้บริการต้องระบุสิทธิให้ผู้ประกอบธุรกิจ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากผู้ประกอบธุรกิจหรือสำนักงาน สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกดังกล่าวได้</p> <p>หากมีเหตุจำเป็นทำให้ผู้ประกอบธุรกิจไม่สามารถระบุสิทธิในการเข้าตรวจสอบตามวรรคหนึ่งไว้ในข้อตกลงหรือสัญญา ผู้ประกอบธุรกิจต้องมีมาตรการประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอสอดคล้องกับความเสี่ยงและควมมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล</p> <p>(5) มี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้า</p> <p>(6) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยต้องสอดคล้องกับระดับความเสี่ยงและระดับความมีนัยสำคัญของบุคคลภายนอก</p> <p>(7) รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจ</p> <p>(8) เตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้าน 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)

ผู้ประกอบการควรจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน และมีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับของข้อมูลได้อย่างเหมาะสม 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 การควบคุมการเข้ารหัส (cryptographic control)

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

6.1 กำหนดวิธีการเข้ารหัสที่ปลอดภัย

6.2 กำหนดการบริหารจัดการกุญแจเข้ารหัส โดยจัดให้มีมาตรการการควบคุมตั้งแต่การสร้างและติดตั้งกุญแจเข้ารหัส การจัดเก็บและสำรองกุญแจเข้ารหัส ไปจนถึงการเพิกถอนหรือทำลายกุญแจเข้ารหัส

6.3 กำหนดมาตรการการควบคุมกุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ซึ่งต้องตรวจสอบเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสที่สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคลอื่น

6.4 กำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส

## ส่วนที่ 7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

ผู้ประกอบการธุรกิจต้องจัดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินด้าน IT พร้อมทั้งมีระบบการป้องกัน และกระบวนการบำรุงรักษาฮาร์ดแวร์และระบบสาธารณูปโภค (facilities) ที่เกี่ยวข้องกับ IT เพื่อให้สามารถป้องกันความเสียหายต่อทรัพย์สินด้าน IT ที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และศูนย์คอมพิวเตอร์จากบุคคลภายนอก (co-location)

## ส่วนที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)

ผู้ประกอบการธุรกิจต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT เพื่อให้การปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย โดยต้องครอบคลุมการบริหารจัดการอย่างน้อยในเรื่องดังนี้

8.1 การบริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีกระบวนการในการควบคุมการตั้งค่าระบบ และสอบทานการตั้งค่าระบบอย่างสม่ำเสมอ เพื่อให้การตั้งค่าระบบเป็นไปอย่างถูกต้องและปลอดภัย

8.2 การบริหารจัดการการเปลี่ยนแปลง (change management) อย่างรัดกุมเพียงพอเพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต

8.3 การบริหารจัดการขีดความสามารถของระบบ 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) อย่างครบถ้วนและเพียงพอเพื่อให้สามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ และสามารถติดตามและตรวจสอบการเข้าถึงและใช้งานข้อมูลและระบบ IT ย้อนหลังได้ ตามที่กฎหมายกำหนด

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

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

## 8.10 การทดสอบการเจาะระบบ (penetration test)

### 8.10.1 ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบการเจาะระบบดังนี้

ระบบงาน	การทดสอบ
(1) ระบบงาน (application system) และระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing)	(1.1) อย่างน้อยปีละ 1 ครั้ง และ (1.2) ทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ
(2) ระบบอื่น ๆ นอกจาก (1)	จัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กร เพื่อกำหนดขอบเขตการทดสอบการเจาะระบบและทดสอบการเจาะระบบตามความเหมาะสม

8.10.2 การทดสอบการเจาะระบบข้างต้น ต้องดำเนินการโดยผู้เชี่ยวชาญภายในหรือภายนอกที่เป็นอิสระจากเจ้าของระบบ

8.10.3 ในกรณีที่มีการตรวจพบช่องโหว่ ผู้ประกอบธุรกิจต้องดำเนินการแก้ไข และป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นอย่างทันท่วงที เพื่อขจัดความเสี่ยงจากช่องโหว่ดังกล่าว

8.10.4 ผู้ประกอบธุรกิจต้องจัดเก็บรายงานการดำเนินการตามข้อ 8.10 เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

8.10.5 ผู้ประกอบธุรกิจต้องนำส่งรายงานผลการทดสอบการเจาะระบบโดยไม่ชักช้าเมื่อได้รับการแจ้งจากสำนักงาน

8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management) โดยจัดให้มีกระบวนการควบคุมการติดตั้งโปรแกรมแก้ไขช่องโหว่บนระบบและอุปกรณ์ เพื่อลดความเสี่ยงที่จะถูกโจมตีในอนาคต

## ส่วนที่ 9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)

ผู้ประกอบธุรกิจต้องมีการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสารอย่างเหมาะสม เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมทั้งพร้อมให้บริการได้อย่างต่อเนื่อง

ส่วนที่ 10 การบริหารจัดการโครงการด้าน IT (IT project management) การจัดหา พัฒนา และบำรุงรักษา ระบบ IT (system acquisition, development and maintenance)

ผู้ประกอบการธุรกิจต้องมีการบริหารจัดการโครงการด้าน IT และมีการจัดหา พัฒนา รวมถึงบำรุงรักษา ระบบ IT เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ IT (entire life cycle) ดังนี้

การดำเนินการ	รายละเอียด
10.1 บริหารจัดการโครงการด้าน IT (IT project management)	กำหนดกรอบการบริหารจัดการโครงการ (project management framework) เพื่อให้การบริหารจัดการโครงการด้าน IT ที่มีนัยสำคัญ เป็นไปอย่างมีประสิทธิภาพ สามารถส่งมอบโครงการได้อย่างถูกต้อง ครบถ้วนตามแผนงานและบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้
10.2 จัดหาระบบ IT (system acquisition)	จัดให้มีหลักเกณฑ์ในการจัดหาระบบ IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัย 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> <p>(1) มีการกำหนดรายละเอียดความต้องการของระบบ (requirement) และคุณสมบัติทางเทคนิค (technical specification) ของระบบ ที่พัฒนา ดังนี้</p> <ul style="list-style-type: none"> <li>(1.1) ความมั่นคงปลอดภัย (security)</li> <li>(1.2) สภาพพร้อมใช้งาน (availability)</li> <li>(1.3) ขีดความสามารถที่รองรับ (capacity)</li> </ul> <p>(2) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของ ผู้ที่เกี่ยวข้องในการพัฒนาระบบ เพื่อให้มีการสอบทานก่อนนำระบบ ขึ้นไปให้บริการจริง</p>



การดำเนินการ	รายละเอียด
	<p>(3) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production)</p> <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 เมื่อมีการพัฒนาหรือเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าระบบดังกล่าวสามารถรองรับปริมาณการใช้งานได้สอดคล้องกับความต้องการทางธุรกิจ</p> <p>(9) ในกรณีที่มีการมอบหมายให้บุคคลภายนอกเป็นผู้พัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ผู้ประกอบธุรกิจต้องจัดให้มีการติดตาม และควบคุมการดำเนินการให้เป็นไปตามข้อตกลงในการมอบหมายงาน</p> <p>(10) มีกระบวนการขออนุมัติจากผู้บริหารหรือคณะกรรมการที่ได้รับมอบหมายจากผู้ประกอบธุรกิจ ก่อนนำระบบขึ้นใช้งานจริง</p>
10.4 แก้ไขเปลี่ยนแปลงระบบ IT (system change)	<p>(1) มีการประเมินผลกระทบ และจัดลำดับความสำคัญของการเปลี่ยนแปลง</p> <p>(2) มีกระบวนการขออนุมัติการเปลี่ยนแปลง (change request) โดยต้องได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมแล้ว</p>

การดำเนินการ	รายละเอียด
	(3) มีการทดสอบระบบก่อนนำไปตั้งค่า หรือนำไปติดตั้งบนระบบ ที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น (4) มีกระบวนการขออนุมัติจากผู้บริหารหรือคณะกรรมการที่ได้รับ มอบหมายจากผู้ประกอบธุรกิจ ก่อนนำระบบขึ้นใช้งานจริง (5) มีกระบวนการหรือเครื่องมือควบคุมการเปลี่ยนแปลงรุ่น (version) ของชุดคำสั่งคอมพิวเตอร์ (source code version control) และรองรับการถอยกลับสู่สภาพเดิม (fallback) (6) ปรับปรุงรายละเอียดประกอบระบบงานที่ได้มีการแก้ไข เปลี่ยนแปลง เพื่อให้เป็นปัจจุบัน

### ส่วนที่ 11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management)

ผู้ประกอบธุรกิจต้องมีการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างเหมาะสมและทันทั่วถึง ดังนี้

11.1 จัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้าน IT จากบุคลากร ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง

11.2 กำหนดแผน หรือขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT

11.3 รายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลกระทบต่อทรัพย์สินของผู้ใช้งานเสียหายอันเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว

11.4 วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไข และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

11.5 บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

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

## ส่วนที่ 12 แผนฉุกเฉินด้าน IT (IT contingency plan)

ผู้ประกอบการธุรกิจต้องจัดให้มีแผนฉุกเฉินด้าน IT เพื่อรองรับเหตุการณ์ผิดปกติด้าน IT ซึ่งส่งผลกระทบต่อให้ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง โดยต้องกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ ดังนี้

12.1 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT

12.2 กระบวนการจัดทำแผนฉุกเฉินด้าน IT ต้องครอบคลุมการดำเนินการ ดังนี้

12.2.1 ประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง

12.2.2 วิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากเหตุการณ์ความเสี่ยงตามข้อ 12.2.1 เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ IT (Recovery Time Objective: RTO) ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (Maximum Tolerable Downtime: MTD) อย่างเหมาะสม

12.2.3 จัดทำแผนฉุกเฉินด้าน IT อย่างเป็นลายลักษณ์อักษร ซึ่งได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบการธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบการธุรกิจ

12.3 จัดให้มีระบบ IT สำรอง และทรัพยากรที่จำเป็น เพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมายที่กำหนดไว้

12.4 สื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม

12.5 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว โดยรายงานผลการทบทวนและทดสอบต่อคณะกรรมการของผู้ประกอบการธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบการธุรกิจ

12.6 กำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากรด้าน IT หรือการใช้ประสิทธิภาพของระบบงานเกินขีดจำกัดของตัวชี้วัดที่กำหนดไว้ เช่น การจำกัดการให้บริการบางช่องทาง หรือตัดการเชื่อมต่อกับผู้ให้บริการหรือบุคคลภายนอกที่มีผลกระทบต่อระบบ IT เป็นต้น

12.7 จัดให้มีรายละเอียดในการติดต่อ ดังนี้ เพื่อให้สามารถประสานงานในการรายงานเหตุการณ์ผิดปกติด้าน IT หรือขอความช่วยเหลือจากหน่วยงานภายนอกที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ โดยต้องปรับปรุงข้อมูลดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

12.7.1 รายชื่อหน่วยงานกำกับดูแลและบุคคลภายนอกที่ให้บริการหรือที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบการธุรกิจ

12.7.2 ช่องทางในการติดต่อ และรายชื่อผู้ที่เกี่ยวข้องของหน่วยงานกำกับดูแลหรือบุคคลภายนอกตามข้อ 12.7.1