ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. ๑/๒๕๖๖
ฉบับที่ ๓
หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ

หมวด ๑
ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

ข้อ ๑ ผู้รับใบอนุญาตต้องเข้าใจและตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อผู้ที่เกี่ยวข้อง รวมทั้งมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงที่เกี่ยวข้องให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมการดำเนินการและการดูแลด้านต่าง ๆ ดังนี้

๑.๑ การพิจารณาเลือกใช้เทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์การประกอบธุรกิจ

๑.๒ จัดให้มีนโยบายและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑.๓ กำกับดูแลให้มีการปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการในระบบการให้บริการของตน

ข้อ ๒ ผู้รับใบอนุญาตต้องจัดให้มีโครงสร้างและบทบาทหน้าที่ตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ ๓ ระดับ (three lines of defense) สำหรับการทำหน้าที่ดังนี้

ระดับ ๑ : การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

ระดับ ๒ : การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ระดับ ๓ : การตรวจสอบด้านเทคโนโลยีสารสนเทศ

โดยมีบุคลากรระดับสูงทำหน้าที่ในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องตามลักษณะของการให้บริการ ปริมาณธุรกรรม และความซับซ้อนทางเทคโนโลยีอย่างมีประสิทธิภาพ ซึ่งบุคคลดังกล่าวต้อง

๒.๑ เป็นผู้มีความรู้ ประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์

๒.๒ มีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศของระบบการให้บริการ

ข้อ ๓ บุคลากรผู้รับผิดชอบกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมีหน้าที่และความรับผิดชอบอย่างน้อยในเรื่องดังต่อไปนี้

๓.๑ จัดให้มีนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งกำกับดูแลให้มีการปฏิบัติตามนโยบายและมาตรการดังกล่าว

๓.๒ จัดให้มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture) ของระบบการให้บริการ

๓.๓ จัดให้มีนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) รวมถึงบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงขององค์กร

๓.๔ ดูแลและดำเนินการให้องค์กรมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๓.๕ รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยระบบสารสนเทศและภัยคุกคามทางไซเบอร์ตามที่กฎหมายกำหนด

๓.๖ ดูแลและส่งเสริมให้บุคลากรในองค์กรมีความรู้และตระหนักรู้เรื่องการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์

ข้อ ๔ ผู้รับใบอนุญาตต้องมีการบริหารจัดการบุคลากรที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบการให้บริการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ การกำกับดูแลการปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง และตรวจสอบด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอย่างเหมาะสม โดยต้องมีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๔.๑ ข้อกำหนดหรือเงื่อนไขในการจ้างบุคลากรควรระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอย่างชัดเจน

๔.๒ มีการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับระบบการให้บริการให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้งต้องสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงดังกล่าว

๔.๓ จัดให้มีการฝึกอบรมหรือสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ ผลกระทบและการบรรเทาผลกระทบอย่างสม่ำเสมอ

ข้อ ๕ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการในเรื่องดังต่อไปนี้

๕.๑ นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security policy) โดยคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีภายในองค์กรและความเสี่ยงจากกรณีมีการใช้บริการเชื่อมต่อหรือเข้าถึงข้อมูลจากบุคคลภายนอก

๕.๒ นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยพิจารณาถึงความเหมาะสมของมาตรการควบคุมที่มีอยู่ในปัจจุบัน และการตอบสนองและการจัดการการเปลี่ยนแปลงที่สำคัญต่อความเสี่ยง ภัยคุกคาม และสภาพแวดล้อมในการปฏิบัติงาน

๕.๓ นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล (privacy policy)

ข้อ ๖ ผู้รับใบอนุญาตต้องสื่อสารและสร้างความตระหนักให้แก่บุคลากรผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่เกี่ยวข้องกับระบบการให้บริการในการปฏิบัติงานประจำวันอย่างเพียงพอและเหมาะสม เพื่อให้บุคลากรเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีอย่างปลอดภัย

ข้อ ๗ ผู้รับใบอนุญาตต้องจัดให้มีการทบทวนนโยบายและมาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อการดำเนินการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

หมวด ๒
การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security)

ข้อ ๘ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ซึ่งครอบคลุมระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) และระบบเครือข่าย (network system) รวมถึงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญให้ชัดเจนเป็นลายลักษณ์อักษร ภายใต้หลักการดังต่อไปนี้

๘.๑ การรักษาความลับของข้อมูล

๘.๒ ความถูกต้องเชื่อถือได้ของระบบสารสนเทศ

๘.๓ การรักษาสภาพความพร้อมใช้งานของระบบการให้บริการ

ข้อ ๙ ผู้รับใบอนุญาตต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยครอบคลุมหัวข้ออย่างน้อยดังต่อไปนี้

๙.๑ การบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ (IT asset management)
ผู้รับใบอนุญาตต้องบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การบำรุงรักษาทรัพย์สินอย่างสม่ำเสมอ การยกเลิกและเรียกคืนทรัพย์สิน โดยอย่างน้อยทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศต้องมีการระบุฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลที่ถือครอง รวมถึงการจัดประเภทและระดับความสำคัญของข้อมูล และเจ้าของทรัพย์สิน นอกจากนี้ ต้องมีการวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดอายุการใช้งาน หรือสิ้นสุดการให้บริการจากผู้ผลิตด้วย

๙.๒ การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)
ผู้รับใบอนุญาตต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล โดยครอบคลุมหัวข้อดังต่อไปนี้

๙.๒.๑ หลักเกณฑ์การจัดประเภทและระดับความสำคัญของข้อมูล

๙.๒.๒ แนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลที่สอดคล้องตามระดับความสำคัญ ซึ่งครอบคลุมถึงการกำหนดสิทธิผู้เข้าถึงข้อมูล วิธีการรับส่ง การประมวลผล และการจัดเก็บข้อมูล และการทำลายข้อมูล

๙.๒.๓ การเข้ารหัสลับข้อมูลตามระดับความสำคัญของข้อมูล รวมถึงวิธีการเข้ารหัสข้อมูล และการบริหารจัดการกุญแจเข้ารหัสลับ โดยครอบคลุมทุกขั้นตอนของวงจรการบริหารจัดการกุญแจเข้ารหัสลับ ตลอดจนกระบวนการสร้าง แจกจ่าย จัดเก็บ ใช้งาน การสำรอง เพิกถอน การต่ออายุ รวมถึงการบันทึกและตรวจสอบกิจกรรมที่สำคัญ

๙.๓ การควบคุมการเข้าถึงสารสนเทศ (access to information)

๙.๓.๑ ผู้รับใบอนุญาตต้องมีการควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม โดยอย่างน้อยต้องมีการควบคุมดังต่อไปนี้

(๑) จำกัดการเข้าถึงสารสนเทศที่มีความสำคัญ ข้อมูลอัตลักษณ์และทรัพยากรที่เกี่ยวข้องกับระบบการให้บริการเฉพาะบุคคลที่จำเป็นเท่านั้น

(๒) ต้องมีกลไกควบคุมและจัดการสิทธิการเข้าถึงระบบปฏิบัติการ ระบบงาน ระบบฐานข้อมูล และระบบเครือข่าย รวมถึงอุปกรณ์ที่เกี่ยวข้องกับระบบการให้บริการ โดยพิจารณาตามความจำเป็น ระดับความเสี่ยง และเป็นไปตามหลักการแบ่งแยกหน้าที่ที่ดี

๙.๓.๒ ในการจัดการการเข้าถึงระบบสารสนเทศซึ่งจัดเก็บสารสนเทศที่มีความสำคัญ ผู้รับใบอนุญาตต้องมีกลไกในการระบุตัวตนที่สามารถแยกแยะผู้ใช้งาน การยืนยันตัวตน และการให้สิทธิในการอนุญาตให้เข้าถึงระบบ

๙.๓.๓ ผู้รับใบอนุญาตต้องจัดให้มีการบันทึกกิจกรรมการเข้าถึงสารสนเทศซึ่งสามารถแยกแยะผู้ใช้งานและสิทธิในการเข้าถึง

๙.๔ การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

ผู้รับใบอนุญาตต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของระบบการให้บริการ บุคลากร และสินทรัพย์ที่เกี่ยวข้อง โดยอย่างน้อยต้องครอบคลุมกรณีดังต่อไปนี้

๙.๔.๑ การปกป้องทรัพยากรที่สอดคล้องกับระดับการประเมินผลกระทบทางธุรกิจอันเกิดจากการละเมิด การสูญเสีย หรือความเสียหาย โดยการกระทำของมนุษย์ ความขัดข้องของระบบสาธารณูปโภค สภาพแวดล้อมที่ไม่เหมาะสม หรือภัยพิบัติทางธรรมชาติ

๙.๔.๒ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัย การเลือกใช้อุปกรณ์จัดเก็บและพื้นที่มั่นคงปลอดภัย

๙.๔.๓ การควบคุมการเข้าถึงสถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ โดยควรควบคุมให้เข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตตามสิทธิที่ได้รับมอบหมายเท่านั้น

๙.๔.๔ การทำลายทรัพย์สินทางกายภาพอย่างมั่นคงปลอดภัย

๙.๕ การรักษาความมั่นคงปลอดภัยของการสื่อสาร (communications security)

ผู้รับใบอนุญาตต้องรักษาความมั่นคงปลอดภัยของการสื่อสารข้อมูลเพื่อให้ข้อมูลที่รับส่งผ่านเครือข่ายมีความมั่นคงปลอดภัย โดยอย่างน้อยต้องมีการดำเนินการดังนี้

๙.๕.๑ การออกแบบเครือข่ายอย่างมั่นคงปลอดภัย

๙.๕.๒ การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

๙.๕.๓ การป้องกันการดักรับข้อมูล

๙.๕.๔ การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย

๙.๕.๕ การควบคุมและจัดการสิทธิการใช้ระบบสารสนเทศระยะไกล

๙.๕.๖ มาตรการป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก

๙.๖ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation security)

ผู้รับใบอนุญาตต้องรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ โดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

๙.๖.๑ มีกระบวนการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศอย่างรัดกุม (change management)

๙.๖.๒ การบริหารจัดการขีดความสามารถของระบบ (capacity management) อย่างเหมาะสม เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอต่อการรองรับการให้บริการหรือดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

๙.๖.๓ การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยี (endpoint) โดยอย่างน้อยต้องจัดให้มีการควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ การติดตั้งเครื่องมือสำหรับป้องกันภัยจากมัลแวร์ รวมทั้งติดตามให้มีการปรับปรุงให้เป็นปัจจุบันและเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ

๙.๖.๔ การสำรองข้อมูล (data backup) ด้วยวิธีการ เทคโนโลยี และระยะเวลาที่เหมาะสม

๙.๖.๕ การจัดเก็บประวัติกิจกรรม (log) เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการใช้งานระบบหรือข้อมูล

๙.๖.๖ การตั้งค่าเทียบเวลา (clock synchronization) ให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากลในระดับเดียวกันทั้งระบบ

๙.๖.๗ การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการและเครื่องมือตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

๙.๖.๘ การบริหารจัดการช่องโหว่ของระบบ (vulnerability management) ที่เหมาะสม โดยมีการประเมินช่องโหว่ การรายงานผลไปยังผู้รับผิดชอบ ติดตามและจัดการกับช่องโหว่ให้ได้รับการแก้ไขอย่างเพียงพอ โดยขอบเขตการประเมินช่องโหว่ต้องครอบคลุมการประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม สำหรับทุกระบบงานตามระดับความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๙.๖.๙ การทดสอบการเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญภายในหรือภายนอกที่เป็นอิสระอย่างน้อยปีละหนึ่งครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งมีการรายงานผลไปยังผู้รับผิดชอบ ติดตามและจัดการกับช่องโหว่ให้ได้รับการแก้ไขอย่างเพียงพอ โดยควรพิจารณาขอบเขตของการทดสอบเจาะระบบให้ครอบคลุมการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของระบบการให้บริการโดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง ทั้งนี้ ในกรณีที่สำนักงานเห็นว่าผลการทดสอบเจาะระบบมีข้อมูลรายงานหรือวิธีการทดสอบการเจาะระบบไม่ครอบคลุมช่องโหว่สำคัญที่เป็นความเสี่ยงที่ได้รับการยอมรับโดยทั่วไป หรือในกรณีที่สำนักงานเห็นว่าจำเป็นหรือสมควร สำนักงานอาจสั่งให้แต่งตั้งผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระดำเนินการทดสอบเจาะระบบเพิ่มเติมได้

๙.๖.๑๐ การบริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีการกำหนดมาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัยสำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่าย มีกระบวนการควบคุมการตั้งค่าของระบบที่ใช้งานจริง มีการสอบทานการใช้มาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคง

ปลอดภัยอย่างสม่ำเสมอ และมีการทบทวนมาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัยอย่างน้อยปีละหนึ่งครั้ง

๙.๖.๑๑ การบริหารจัดการการติดตั้งโปรแกรมสำหรับแก้ไขข้อบกพร่อง (patch management) โดยมีกระบวนการควบคุมการติดตั้ง patch ของระบบที่ใช้งานจริง เพื่อให้สามารถติดตั้ง patch ที่สำคัญในการรักษาความมั่นคงปลอดภัยได้อย่างทันการณ์และเหมาะสมตามระดับความเสี่ยง

๙.๗ การพัฒนาระบบ (system development)

ผู้รับใบอนุญาตต้องนำมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศไปใช้ตลอดวงจรการพัฒนาระบบ โดยอย่างน้อยมีการดำเนินการดังต่อไปนี้

๙.๗.๑ มีเอกสารรายละเอียดคุณสมบัติทางเทคนิคซึ่งครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๙.๗.๒ มีกระบวนการควบคุมเวอร์ชันของการพัฒนาระบบ

๙.๗.๓ มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ

๙.๗.๔ มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนาและการทดสอบออกจากระบบงานที่ให้บริการจริง

๙.๗.๕ มีแนวทางการควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ

๙.๗.๖ ทดสอบระบบก่อนการใช้งานจริง โดยอย่างน้อยต้องครอบคลุมการทดสอบตามความต้องการของหน่วยงานธุรกิจในด้านประสิทธิภาพและด้านความมั่นคงปลอดภัย

๙.๗.๗ การจัดการข้อผิดพลาดหรือข้อบกพร่องของระบบที่พบในการทดสอบหรือเมื่อนำไปใช้งานจริง

๙.๗.๘ มีการสร้างความตระหนักและให้ความรู้กับผู้พัฒนาโปรแกรมอย่างสม่ำเสมอเพื่อเสริมสร้างทักษะในด้านการออกแบบและพัฒนาโปรแกรมอย่างปลอดภัย

๙.๘ การบริหารจัดการเหตุการณ์ไม่พึงประสงค์ (incident management)

ผู้รับใบอนุญาตต้องมีการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์อย่างเหมาะสมและทันท่วงที โดยมีขั้นตอนสำหรับบุคลากรและผู้ใช้งานในการบริหารจัดการเหตุการณ์ไม่พึงประสงค์ซึ่งจะครอบคลุมขั้นตอนการตรวจพบเหตุการณ์ การแจ้งเหตุ การพิสูจน์เหตุการณ์ การรายงานเหตุการณ์ การตอบสนองต่อเหตุการณ์ รวมถึงการรวบรวมและจัดเก็บหลักฐานเพื่อการสืบสวน นอกจากนี้ ต้องวิเคราะห์สาเหตุที่แท้จริงของปัญหาเพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ไม่พึงประสงค์ซ้ำในอนาคต

๙.๙ การจัดทำแผนการกู้คืนเมื่อเกิดภัยพิบัติ (disaster recovery plan) และการบริหารความต่อเนื่องทางธุรกิจ (business continuity management)

๙.๙.๑ ผู้รับใบอนุญาตต้องจัดทำแผนการกู้คืนเมื่อเกิดภัยพิบัติ และแผนการบริหารความต่อเนื่องทางธุรกิจสำหรับระบบการให้บริการโดยคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยด้าน

เทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง ซึ่งครอบคลุมเนื้อหาอย่างน้อยดังต่อไปนี้

(๑) การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis - BIA)

(๒) การกำหนดระยะเวลาในการกู้คืนระบบ (recovery time objective : RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (recovery point objective : RPO) ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (maximum tolerance period of disruption : MTPD) เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

(๓) แผนและขั้นตอนการกู้คืนระบบ

(๔) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan : BCP)

๙.๙.๒ ต้องจัดทำคู่มือหรือเอกสารประกอบการดำเนินการตามแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจ รวมทั้งประชาสัมพันธ์และฝึกอบรมบุคลากรที่เกี่ยวข้องให้มีความเข้าใจและสามารถปฏิบัติตามแผนดังกล่าวได้

๙.๙.๓ ต้องทบทวนและทดสอบการปฏิบัติตามแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจอย่างน้อยปีละหนึ่งครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ พร้อมทั้งจัดทำรายงานผลการทดสอบ

๙.๙.๔ ต้องจัดให้มีระบบสำรองที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อระบบหลักหยุดชะงัก โดยระบบสำรองควรแยกออกจากระบบหลักในการให้บริการเพียงพอที่จะมิให้เกิดปัญหาหรือได้รับผลกระทบในลักษณะเดียวกันในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง

ข้อ ๑๐ การจัดเก็บประวัติกิจกรรม (log)

๑๐.๑ ผู้รับใบอนุญาตต้องจัดเก็บประวัติกิจกรรมเพื่อประโยชน์ในการตรวจสอบในกรณีอย่างน้อยดังต่อไปนี้

๑๐.๑.๑ การใช้สิทธิพิเศษของบุคลากรทั้งในกรณีที่ดำเนินการสำเร็จและไม่สำเร็จ

๑๐.๑.๒ การบริหารจัดการสิทธิผู้ใช้งาน ทั้งในการเพิ่มบัญชีและกลุ่มผู้ใช้งาน การลบ และการแก้ไขสิทธิ

๑๐.๑.๓ การแจ้งเตือนด้านความมั่นคงปลอดภัยและความผิดพลาด เช่น การปฏิเสธความพยายามเข้าสู่ระบบ การแจ้งเตือนความผิดพลาด

๑๐.๑.๔ การพยายามเข้าถึงระบบโดยไม่ได้รับอนุญาต

๑๐.๒ ประวัติกิจกรรมที่จัดเก็บสำหรับแต่ละเหตุการณ์ต้องประกอบด้วยข้อมูลเบื้องต้นอย่างน้อยดังต่อไปนี้

๑๐.๒.๑ วันที่และเวลาของเหตุการณ์

๑๐.๒.๒ ผู้ใช้งาน หรือรหัสบ่งชี้ (identifier) หรือขั้นตอนที่เกี่ยวข้อง

๑๐.๒.๓ ระบุเฉพาะ (unique identifier) สำหรับแต่ละกิจกรรม

๑๐.๒.๔ รายละเอียดของเหตุการณ์

๑๐.๒.๕ ข้อมูลอื่นอันเป็นประโยชน์ เช่น อุปกรณ์ที่เกี่ยวข้อง

๑๐.๓ การจัดเก็บประวัติกิจกรรมสำหรับการพิสูจน์ตัวตนต้องมีการจัดเก็บข้อมูลเพิ่มเติม ได้แก่ ระดับความน่าเชื่อถือของการพิสูจน์ตัวตนในแต่ละกิจกรรม

๑๐.๔ การจัดเก็บประวัติกิจกรรมสำหรับการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนในแต่ละกิจกรรมต้องมีการจัดเก็บข้อมูลเพิ่มเติม ดังนี้

๑๐.๔.๑ ประเภทของสิ่งที่ใช้ยืนยันตัวตน

๑๐.๔.๒ ระดับความน่าเชื่อถือของการยืนยันตัวตน

๑๐.๔.๓ วันที่และเวลาที่ทำการเชื่อมโยงข้อมูลเพื่อออกสิ่งที่ใช้ยืนยันตัวตน

๑๐.๕ การจัดเก็บประวัติกิจกรรมสำหรับการยืนยันตัวตนต้องมีการจัดเก็บข้อมูลเพิ่มเติมดังนี้

๑๐.๕.๑ หมายเลขไอพีต้นทางของอุปกรณ์ที่ผ่านการยืนยันตัวตนเข้ามาในระบบการให้บริการ

๑๐.๕.๒ หมายเลขพอร์ตต้นทางที่ถูกใช้ในการยืนยันตัวตน

๑๐.๕.๓ หมายเลขไอพีปลายทางที่ถูกใช้ในการยืนยันตัวตน

๑๐.๕.๔ หมายเลขพอร์ตปลายทางที่ถูกใช้ในการยืนยันตัวตน

๑๐.๕.๕ user agent string ในกรณีที่มีการใช้งานผ่าน browser

๑๐.๖ การจัดเก็บประวัติกิจกรรมสำหรับการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลต้องมีการจัดเก็บข้อมูลเพิ่มเติม ดังนี้

๑๐.๖.๑ ประเภทของการโต้ตอบ (interaction)

๑๐.๖.๒ ตัวระบุเฉพาะของการโต้ตอบ (unique interaction identifier)

๑๐.๖.๓ ชื่อผู้เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตน

๑๐.๖.๔ ประเภทของข้อมูลอัตลักษณ์ตามคำขอและการตอบกลับ

๑๐.๖.๕ ระดับความน่าเชื่อถือที่ใช้ในการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามคำขอและการตอบกลับ

๑๐.๗ ผู้รับใบอนุญาตต้องทำให้มั่นใจได้ว่าในการจัดเก็บประวัติกิจกรรมต้องดำเนินการให้ครอบคลุมในเรื่องดังต่อไปนี้

๑๐.๗.๑ มีการจัดเก็บอย่างมั่นคงปลอดภัยและมีความถูกต้องครบถ้วน

๑๐.๗.๒ ปราศจากการเข้าถึง การแก้ไข และการลบ โดยไม่ได้รับอนุญาต

๑๐.๗.๓ จัดเก็บไม่น้อยกว่าหนึ่งปีนับแต่วันที่มีการดำเนินการ

๑๐.๗.๔ ประวัติกิจกรรมที่จัดเก็บต้องไม่มีข้อมูลชีวมิติ

ข้อ ๑๑ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ (cyber security incident)

๑๑.๑ ผู้รับใบอนุญาตต้องจัดให้มีกลไกหรือกระบวนการในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์อย่างน้อยดังนี้

๑๑.๑.๑ ต้องมีกลไกในการตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ รวมถึงจัดให้มีช่องทางที่เป็นการรักษาความลับสำหรับบุคลากรและผู้ใช้งานในการแจ้งเหตุการณ์ที่น่าสงสัยเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๑๑.๑.๒ ต้องจัดให้มีกลไกการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ ที่มีลักษณะคล้ายกับเหตุการณ์ที่ตรวจพบ หรือที่เกี่ยวข้องกับเหตุการณ์ที่ตรวจพบ และนำข้อมูลที่เกี่ยวกับเหตุการณ์ที่พบมาตรวจสอบกับการลงทะเบียนใหม่และการปรับปรุงข้อมูลของผู้ใช้งานเดิมด้วย โดยจะต้องไม่อนุญาตให้มีการลงทะเบียนใหม่หรือมีการปรับปรุงข้อมูล หากกลไกการควบคุมระบุหรือบ่งชี้ว่าการ

ลงทะเบียนหรือการปรับปรุงข้อมูลดังกล่าวจะก่อให้เกิดเหตุการณ์ด้านความปลอดภัยไซเบอร์ที่ไม่พึงประสงค์

๑๑.๑.๓ ต้องมีกระบวนการกำหนดหลักเกณฑ์เกี่ยวกับการตัดสินใจในช่วงที่สำคัญ (critical stage) เพื่อการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์

๑๑.๑.๔ ต้องมีขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ และมาตรการบรรเทาผลกระทบใด ๆ ให้กับบุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบ เช่น ผู้ใช้บริการ บุคคลภายนอกที่เกี่ยวกับระบบการให้บริการ เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

๑๑.๒ ผู้รับใบอนุญาตต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ และดำเนินการฝึกซ้อม ทบทวน และปรับปรุงแผนอย่างน้อยปีละหนึ่งครั้งเพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤต

๑๑.๓ ผู้รับใบอนุญาตต้องรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี ซึ่งอย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้

๑๑.๓.๑ วันที่และเวลาของเหตุการณ์

๑๑.๓.๒ จำนวนเหตุการณ์และระดับความรุนแรง

๑๑.๓.๓ มาตรการในการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

๑๑.๔ ในกรณีที่เกิดหรือคาดว่าจะเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีซึ่งส่งผลกระทบต่อระบบการให้บริการ และเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย ผู้รับใบอนุญาตต้องรายงานมายังสำนักงานเมื่อเกิดหรือรับทราบปัญหาหรือเหตุการณ์ดังกล่าวโดยเร็ว และให้แจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

๑๑.๕ ผู้รับใบอนุญาตต้องมีกลไกหรือกระบวนรับแจ้งเหตุอันน่าสงสัยเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์

๑๑.๖ ในกรณีที่เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ก่อให้เกิดผลกระทบกับผู้ใช้บริการ ผู้รับใบอนุญาตต้องมีกระบวนการที่เหมาะสมสำหรับการพิสูจน์ยืนยันตัวตนบุคคลที่เป็นเจ้าของอัตลักษณ์ดิจิทัลหรือสิ่งที่ใช้ยืนยันตัวตนที่อยู่ภายใต้เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ และมีเทคโนโลยีที่เหมาะสมซึ่งสามารถบ่งชี้ถึงการละเมิดอัตลักษณ์ดิจิทัลหรือสิ่งที่ใช้ยืนยันตัวตน

ข้อ ๑๒ การบริหารจัดการบุคคลภายนอก (third party management)

๑๒.๑ ในกรณีที่ผู้รับใบอนุญาตมีการดำเนินการดังต่อไปนี้

๑๒.๑.๑ ใช้บริการจากผู้ให้บริการด้านเทคโนโลยีสารสนเทศ (IT outsourcing)

๑๒.๑.๒ เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก

๑๒.๑.๓ บุคคลภายนอกสามารถเข้าถึงข้อมูลที่สำคัญ หรือเข้าถึงข้อมูลผู้ใช้บริการของระบบการให้บริการ

ผู้รับใบอนุญาตต้องกำกับดูแลกระบวนการบริหารความเสี่ยง และการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบุคคลภายนอกให้อยู่ในระดับที่สอดคล้องกับระดับความเสี่ยง

ของการดำเนินงานของผู้รับใบอนุญาต โดยพิจารณาตามแนวปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยงจากบุคคลภายนอกของสำนักงาน ทั้งนี้ สามารถพิจารณาประยุกต์ใช้ให้เหมาะสมและสอดคล้องตามขอบเขต ระดับความเสี่ยงและนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของบุคคลภายนอก

๑๒.๒ ในการบริหารจัดการบุคคลภายนอกเพื่อควบคุมให้มีการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่เหมาะสม ต้องมีการดำเนินการอย่างน้อย ดังนี้

๑๒.๒.๑ ระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลหรือระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมต่อกับบุคคลภายนอกหรือบุคคลภายนอกสามารถเข้าถึงได้ และกำหนดแนวทางการจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยง

๑๒.๒.๒ การรักษาความมั่นคงปลอดภัยระบบสารเทศของบุคคลภายนอกต้องสอดคล้องกับมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของผู้รับใบอนุญาต

๑๒.๒.๓ ระบุข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รวมถึงข้อกำหนดการไม่เปิดเผยข้อมูลในข้อตกลงการให้บริการหรือเงื่อนไขของสัญญากับบุคคลภายนอกเพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง กระบวนการจัดเก็บการสื่อสาร และการดำเนินการของบุคคลภายนอก

๑๒.๒.๔ มีกระบวนการติดตาม ประเมิน และทบทวนผลการปฏิบัติงานของบุคคลภายนอก

๑๒.๒.๕ มีการสื่อสารหรือการฝึกอบรมบุคคลภายนอกที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบการให้บริการ โดยเฉพาะอย่างยิ่งบุคคลภายนอกที่สามารถเข้าถึงระบบสารสนเทศอย่างน้อยดังนี้

(๑) เผยแพร่หรืออบรมนโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้อง

(๒) มีการฝึกอบรมหรือสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบอย่างสม่ำเสมอ

๑๒.๓ ในกรณีที่ผู้รับใบอนุญาตมีการใช้บริการจากผู้รับดำเนินการแทนในการดำเนินการเกี่ยวกับระบบการให้บริการให้ผู้รับใบอนุญาตปฏิบัติตามหลักเกณฑ์การใช้บริการจากผู้รับดำเนินการแทนด้วย

หมวด ๓
การบริหารและการจัดการความเสี่ยงของระบบการให้บริการ (IT risk management)

ข้อ ๑๓ เพื่อให้การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมกระบวนการอย่างน้อยในเรื่องดังต่อไปนี้

๑๓.๑ การประเมินความเสี่ยง (risk assessment)

๑๓.๑.๑ ระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้น โดยอย่างน้อยต้องระบุปัจจัยและสาเหตุของความเสี่ยง ประเภทของความเสี่ยง ผลกระทบต่อการประกอบธุรกิจ

๑๓.๑.๒ การวิเคราะห์ความเสี่ยงเพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม โดยอย่างน้อยต้องระบุเจ้าของความเสี่ยง การควบคุมที่มีอยู่ในปัจจุบันและวิเคราะห์ผลกระทบที่อาจจะเกิดขึ้น

๑๓.๑.๓ ประเมินค่าความเสี่ยงโดยกำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบ กำหนดระดับความเสี่ยงที่ยอมรับได้ ประเมินโอกาสของการเกิดความเสี่ยงและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์และนำมาจัดลำดับในการบริหารความเสี่ยง

๑๓.๒ การจัดการความเสี่ยง (risk treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อให้ความเสี่ยงที่เหลืออยู่อยู่ในระดับความเสี่ยงที่ยอมรับได้

๑๓.๓ การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ โดยกำหนดมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่มีอยู่และการจัดการความเสี่ยงอย่างเพียงพอ รวมถึงการตอบสนองและการจัดการการเปลี่ยนแปลงที่สำคัญต่อความเสี่ยงและสภาพแวดล้อมของการปฏิบัติงาน และกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (key risk indicator: KRI) เพื่อใช้ติดตามและทบทวนความเสี่ยง

๑๓.๔ การรายงานความเสี่ยง (risk reporting)

ต้องมีการรายงานระดับความเสี่ยงและผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย

ข้อ ๑๔ ผู้รับใบอนุญาตต้องจัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อการดำเนินการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อ ๑๕ ในกรณีที่เกิดเหตุการณ์ซึ่งส่งผลกระทบหรือขัดขวางความสามารถของผู้รับใบอนุญาตในการปฏิบัติตามหลักเกณฑ์ที่กำหนด ผู้รับใบอนุญาตต้องดำเนินการดังต่อไปนี้

๑๕.๑ แจ้งให้สำนักงานทราบถึงเหตุการณ์ซึ่งส่งผลให้ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดโดยเร็ว

๑๕.๒ บันทึกการตัดสินใจเกี่ยวกับการดำเนินมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่เปลี่ยนแปลงไป และการแก้ไขหรือเยียวยา (ถ้ามี) และนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี

๑๕.๓ ผู้รับใบอนุญาตอาจเปลี่ยนแปลงมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศได้ภายในระยะเวลาจำกัดเพื่อรับมือเหตุการณ์ที่เกิดขึ้น ทั้งนี้ การเปลี่ยนแปลงดังกล่าวต้องไม่ทำให้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศสูงกว่าระดับความเสี่ยงที่ยอมรับได้

หมวด ๔
การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๑ นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๑๖ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ซึ่งสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต โดยต้องมีการเผยแพร่เป็นการทั่วไป

ข้อ ๑๗ ผู้รับใบอนุญาตต้องกำหนดบุคลากรที่ทำหน้าที่ในการกำกับดูแลและจัดให้มีการดำเนินงานตามนโยบายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๑๘ นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลต้องมีข้อมูลที่ชัดเจน และประกอบด้วยรายละเอียดอย่างน้อยดังต่อไปนี้

๑๘.๑ ประเภทของข้อมูลส่วนบุคคลที่ผู้รับใบอนุญาตเก็บรวบรวม

๑๘.๒ วิธีการได้มาซึ่งข้อมูลส่วนบุคคล

๑๘.๓ วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๑๘.๔ วิธีการที่ผู้ใช้บริการสามารถเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน รวมทั้งวิธีการในการปรับปรุงหรือแก้ไขข้อมูลส่วนบุคคลดังกล่าว

๑๘.๕ ช่องทางการร้องเรียนและการจัดการเรื่องร้องเรียนกรณีผู้รับใบอนุญาตฝ่าฝืนหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๑๙ ผู้รับใบอนุญาตต้องจัดให้มีการฝึกอบรมหรือสร้างความตระหนักด้านการคุ้มครองข้อมูลส่วนบุคคลแก่บุคลากรที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบการให้บริการก่อนเริ่มปฏิบัติงาน และอย่างน้อยปีละหนึ่งครั้ง ซึ่งครอบคลุมหลักเกณฑ์ของกฎหมายที่เกี่ยวข้องและนโยบายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้รับใบอนุญาต

ส่วนที่ ๒ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๒๐ ในการจัดทำรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจ ผู้รับใบอนุญาตต้องมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลที่อาจเกิดขึ้นจากระบบการให้บริการ และกำหนดแนวทางในการบริหารจัดการ

ข้อ ๒๑ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

๒๑.๑ ระบุขั้นตอน กระบวนการ กิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในระบบการให้บริการ

๒๑.๒ วิเคราะห์ความเสี่ยงของการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

๒๑.๓ วิเคราะห์ผลกระทบของขั้นตอน กระบวนการ กิจกรรมที่ส่งผลต่อการคุ้มครองข้อมูลส่วนบุคคล

๒๑.๔ กำหนดแนวทางการจัดการ ควบคุม และป้องกันที่เหมาะสม

ข้อ ๒๒ กรณีที่มีการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อระบบการให้บริการภายหลังจากเริ่มประกอบธุรกิจ ผู้รับใบอนุญาตต้องจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลและนำส่งผลการประเมินพร้อมการแจ้งการเปลี่ยนแปลงต่อสำนักงาน

ส่วนที่ ๓ การจัดการเหตุการละเมิดข้อมูลส่วนบุคคล

ข้อ ๒๓ ผู้รับใบอนุญาตต้องจัดให้มีแผนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคล ซึ่งอย่างน้อยต้องประกอบด้วย

๒๓.๑ ขั้นตอนการปฏิบัติเมื่อเกิดหรือสงสัยว่าจะเกิดเหตุการละเมิดข้อมูลส่วนบุคคล การตรวจพบหรือการรายงาน

๒๓.๒ การกำหนดบทบาทหน้าที่และความรับผิดชอบของบุคลากรตามแผนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคล

๒๓.๓ แนวทางการสื่อสารข้อมูลเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ซึ่งครอบคลุมการสื่อสารภายในการแจ้งเตือนผู้ได้รับผลกระทบและการแจ้งเตือนหรือการรายงานตามกฎหมายที่เกี่ยวข้อง

๒๓.๔ แผนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคลต้องสอดคล้องกับมาตรการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ และมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

ส่วนที่ ๔ ข้อมูลเกี่ยวกับพฤติกรรมการใช้งานระบบ

ข้อ ๒๔ ผู้รับใบอนุญาตจะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเกี่ยวกับพฤติกรรมการใช้งานระบบการให้บริการได้เฉพาะเพื่อวัตถุประสงค์ดังต่อไปนี้

๒๔.๑ เพื่อการตรวจสอบไอเดนติตี้ของผู้ใช้บริการ และอำนวยความสะดวกให้กับผู้ใช้บริการ

๒๔.๒ เพื่อสนับสนุนการจัดการเหตุการณ์การทุจริตหรือฉ้อโกงในระบบการให้บริการ

๒๔.๓ เพื่อพัฒนาประสิทธิภาพหรือความสามารถในการให้บริการของระบบการให้บริการ

๒๔.๔ เป็นการปฏิบัติตามกฎหมาย

ข้อ ๒๕ ห้ามมิให้ผู้รับใบอนุญาตนำข้อมูลเกี่ยวกับพฤติกรรมการใช้งานตามข้อ ๒๔ ไปขายให้กับบุคคลอื่น

ส่วนที่ ๕ การบริหารจัดการข้อมูลชีวมิติ

ข้อ ๒๖ ในกรณีที่ผู้รับใบอนุญาตมีการเก็บรวบรวมข้อมูลชีวมิติต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล โดยเจ้าของข้อมูลได้รับแจ้งถึงวัตถุประสงค์ของการเก็บรวบรวมและใช้งานข้อมูลชีวมิติอย่างชัดเจน

ข้อ ๒๗ ผู้รับใบอนุญาตจะจัดเก็บข้อมูลชีวมิติได้เฉพาะเพื่อวัตถุประสงค์ดังต่อไปนี้

๒๗.๑ เพื่อประโยชน์ในการใช้บริการระบบการให้บริการ

๒๗.๒ เพื่อการปรับปรุง พัฒนา และทดสอบสมรรถนะของระบบการให้บริการ

เว้นแต่เป็นกรณีที่ผู้รับใบอนุญาตต้องปฏิบัติตามที่กฎหมายกำหนด

ข้อ ๒๘ ในการจัดเก็บข้อมูลชีวมิติผู้รับใบอนุญาตต้องจัดให้มีนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยข้อมูลชีวมิติที่ชัดเจน โดยครอบคลุมกระบวนการอย่างน้อยดังนี้

๒๘.๑ มีการเข้ารหัสข้อมูลชีวมิติ

๒๘.๒ จัดเก็บข้อมูลชีวมิติแยกออกจากการเก็บเทมเพลตชีวมิติและข้อมูลเกี่ยวกับอัตลักษณ์

๒๘.๓ จัดเก็บบนเครือข่ายที่มั่นคงปลอดภัยและรับส่งข้อมูลชีวมิติผ่านช่องทางที่มั่นคงปลอดภัย

๒๘.๔ จำกัดการเข้าถึงข้อมูลชีวมิติเฉพาะบุคลากรผู้รับผิดชอบ

ข้อ ๒๙ กรณีที่ต้องมีการแลกเปลี่ยนข้อมูลชีวมิติเพื่อประโยชน์ในการใช้งานระบบการให้บริการ ผู้ให้บริการต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลโดยต้องมีการเข้ารหัสข้อมูลและจัดให้มีการแลกเปลี่ยนข้อมูลผ่านช่องทางที่มีความมั่นคงปลอดภัย

ข้อ ๓๐ ผู้รับใบอนุญาตต้องทำลายข้อมูลชีวมิติเมื่อมีการเพิกถอนความยินยอมหรือยกเลิกการใช้บริการโดยต้องดำเนินการให้ครอบคลุมทุกกระบวนการที่มีการเก็บรวบรวม ซึ่งรวมถึงกรณีที่มีการว่าจ้างบุคคลภายนอกให้ดำเนินการด้วย เช่น การทำสำเนา การจัดเก็บชั่วคราวในฐานข้อมูล เว้นแต่เป็นกรณีที่ผู้รับใบอนุญาตต้องปฏิบัติตามที่กฎหมายกำหนด

ข้อ ๓๑ ผู้รับใบอนุญาตต้องมีการบันทึกหรือจัดเก็บหลักฐานการทำลายข้อมูลชีวมิติเพื่อประโยชน์ในการตรวจสอบ

ส่วนที่ ๖ ความยินยอม

ข้อ ๓๒ ผู้รับใบอนุญาตต้องได้รับความยินยอมโดยชัดแจ้งจากผู้ใช้บริการก่อนการเปิดเผยข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลดังกล่าวแก่ผู้ที่เกี่ยวข้องกับการใช้งานระบบการให้บริการ

ข้อ ๓๓ ผู้รับใบอนุญาตต้องจัดเก็บประวัติกิจกรรม (log) ที่แสดงถึงการได้ความยินยอมโดยชัดแจ้งจากผู้ใช้บริการ รวมถึงข้อมูลดังต่อไปนี้

๓๓.๑ วันที่และวิธีการได้มาซึ่งความยินยอม

๓๓.๒ ระยะเวลาของความยินยอม

๓๓.๓ เงื่อนไขการให้ความยินยอม

๓๓.๔ การถอน หรือการสิ้นอายุความยินยอม

ส่วนที่ ๗ การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล

ข้อ ๓๔ การเข้าถึงข้อมูล

๓๔.๑ ผู้รับใบอนุญาตต้องจัดให้มีวิธีการที่ให้ผู้ใช้บริการสามารถเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้โดยไม่เสียค่าใช้จ่าย

๓๔.๒ ผู้รับใบอนุญาตต้องตอบรับคำขอเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการภายในสามสิบวันนับแต่ได้รับคำขอ หากผู้รับใบอนุญาตปฏิเสธคำขอต้องดำเนินการให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๓๕ การแก้ไขปรับปรุงข้อมูล

๓๕.๑ ผู้รับใบอนุญาตต้องจัดให้ผู้ใช้บริการสามารถแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้ด้วยวิธีการที่เข้าถึงได้โดยง่าย

๓๕.๒ ผู้รับใบอนุญาตต้องจัดให้มีคู่มือหรือคำอธิบายสำหรับผู้ใช้บริการเกี่ยวกับวิธีการในการแก้ไขหรือปรับปรุงข้อมูล

ข้อ ๓๖ การดูแลคุณภาพของข้อมูลส่วนบุคคล

๓๖.๑ ผู้รับใบอนุญาตต้องมีการทบทวนข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยตรวจทานและปรับปรุงข้อมูลที่ใช้สำหรับการพิสูจน์และยืนยันตัวตนให้เป็นปัจจุบันและดำเนินการอย่างสม่ำเสมอ

๓๖.๒ หากผู้รับใบอนุญาตได้จัดให้มีการทบทวนข้อมูลของผู้ใช้บริการแล้วแต่ไม่สามารถติดต่อผู้ใช้บริการได้ ให้กำหนดมาตรการที่สามารถทบทวนข้อมูลผู้ใช้บริการให้เป็นปัจจุบันเมื่อผู้ใช้บริการมาทำธุรกรรมหรือในโอกาสแรกที่สามารถติดต่อผู้ใช้บริการได้

ส่วนที่ ๘ การจัดการเรื่องร้องเรียน

ข้อ ๓๗ ผู้รับใบอนุญาตต้องจัดให้มีมาตรการหรือกลไกในการจัดการเรื่องร้องเรียนเกี่ยวกับข้อมูลส่วนบุคคล โดยมีลักษณะอย่างน้อยดังนี้

๓๗.๑ ผู้ใช้บริการสามารถเข้าถึงได้ง่าย มีข้อมูลการติดต่อที่ชัดเจน

๓๗.๒ มีกระบวนการจัดการด้วยความเป็นธรรม มีความเป็นกลาง และโปร่งใส

๓๗.๓ มีขั้นตอนที่ชัดเจน ดำเนินการอย่างทันท่วงที และมีการบรรเทาความเสียหายอย่างเหมาะสม

๓๗.๔ มีบุคลากรที่มีความรู้ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการจัดการเรื่องร้องเรียน

๓๗.๕ มีกลไกที่สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

หมวด ๕
การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง (IT compliance)

ข้อ ๓๘ ผู้รับใบอนุญาตต้องปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันการฝ่าฝืนหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

หมวด ๖
การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

ข้อ ๓๙ ผู้รับใบอนุญาตต้องจัดให้มีการตรวจสอบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการอย่างน้อยปีละหนึ่งครั้ง รวมทั้งต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเพียงพอ