(ร่าง) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบให้บริการ

<u>เค้าโครงร่างหลักเกณฑ์</u>

หมวด 1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

1. ความตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2. การจัดโครงสร้างองค์กรและบทบาทหน้าที่ความรับผิดชอบ
3. บุคลากรผู้รับผิดชอบกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
4. การบริหารจัดการบุคลากร
5. นโยบายที่สำคัญ
6. การสร้างความตระหนัก
7. การทบทวนนโยบาย

หมวด 2 นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security policy)

8. ขอบเขตของการจัดทำนโยบาย
9. มาตรการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
    - 9.1 การบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ (IT asset management)
    - 9.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)
    - 9.3 การควบคุมการเข้าถึงสารสนเทศ (access to information)
    - 9.4 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)
    - 9.5 การรักษาความมั่นคงปลอดภัยของการสื่อสาร (communications security)
    - 9.6 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation security)
    - 9.7 การพัฒนาระบบ (system development)
    - 9.8 การบริหารจัดการเหตุการณ์ไม่พึงประสงค์ (incident management)
    - 9.9 การจัดทำแผนการกู้คืนเมื่อเกิดภัยพิบัติ (disaster recovery plan) และการบริหารความต่อเนื่องทางธุรกิจ (business continuity management)
10. การจัดเก็บประวัติกิจกรรม (log)
11. การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ (cyber security incident)
12. การบริหารจัดการบุคคลภายนอก (third party management)

หมวด 3 การบริหารและการจัดการความเสี่ยงของระบบให้บริการ

13. นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
14. รอบการประเมินความเสี่ยง
15. การดำเนินการกรณีมีเหตุการณ์ที่กระทบต่อความสามารถในการปฏิบัติตามหลักเกณฑ์

หมวด 4 การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 1 นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล
ส่วนที่ 2 การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
ส่วนที่ 3 การจัดการเหตุการละเมิดข้อมูลส่วนบุคคล
ส่วนที่ 4 ข้อมูลเกี่ยวกับพฤติกรรมการใช้งานระบบ
ส่วนที่ 5 การบริหารจัดการข้อมูลชีวมิติ
ส่วนที่ 6 ความยินยอม
ส่วนที่ 7 การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล
ส่วนที่ 8 การจัดการเรื่องร้องเรียน

หมวด 5 การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง (IT compliance)

หมวด 6 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

(ร่าง) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบให้บริการ

หมวด 1
ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

1. ผู้รับใบอนุญาตต้องเข้าใจและตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อผู้ที่เกี่ยวข้อง รวมทั้งมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้องให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมการดำเนินการและการดูแลด้านต่าง ๆ ดังนี้
   (1.1) การพิจารณาเลือกใช้เทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์การประกอบธุรกิจ
   (1.2) จัดให้มีนโยบายและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
   (1.3) กำกับดูแลให้มีการปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และมาตรการในการดูแลข้อมูลส่วนบุคคลของผู้ใช้บริการในระบบให้บริการของตน
2. ผู้รับใบอนุญาตต้องต้องจัดให้มีโครงสร้างและบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (Three line of defense) สำหรับการทำหน้าที่ดังนี้
   ระดับ 1 : การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
   ระดับ 2 : การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
   ระดับ 3 : การตรวจสอบด้านเทคโนโลยีสารสนเทศ
   โดยมีบุคลากรระดับสูงทำหน้าที่ในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องตามลักษณะการให้บริการ ปริมาณธุรกรรม และความซับซ้อนทางเทคโนโลยีอย่างมีประสิทธิภาพซึ่งบุคคลดังกล่าวต้อง
   (1) เป็นผู้มีความรู้ ประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์
   (2) มีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development)
3. บุคลากรผู้รับผิดชอบกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีหน้าที่และความรับผิดชอบอย่างน้อยในเรื่องดังต่อไปนี้
   (1) จัดให้มีนโยบายและมาตรการการรักษาความปลอดภัยระบบสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งกำกับดูแลให้มีการปฏิบัติตามนโยบายและมาตรการดังกล่าว
   (2) จัดให้มีข้อกำหนดด้านความปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture) ของระบบให้บริการ
   (3) จัดให้มีนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงขององค์กร
   (4) ดูแลและดำเนินการให้องค์กรมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

(5) รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยระบบสารสนเทศและด้านภัยคุกคามทางไซเบอร์ตามที่กฎหมายกำหนด

(6) ดูแลและส่งเสริมให้บุคลากรในองค์กรมีความรู้และตระหนักรู้เรื่องการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์

4. ผู้รับใบอนุญาตต้องมีการบริหารจัดการบุคลากรที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบให้บริการ ในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ การกำกับดูแลการปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง และตรวจสอบด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอย่างเหมาะสม โดยต้องมีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

(1) ข้อกำหนดหรือเงื่อนไขในการจ้างบุคลากรควรระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอย่างชัดเจน

(2) มีการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับระบบให้บริการให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน หรือสิ้นสุดการจ้างงาน รวมทั้งต้องสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงดังกล่าว

(3) จัดให้มีการฝึกอบรมหรือสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ อย่างสม่ำเสมอ

5. ผู้รับใบอนุญาตต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในเรื่องดังต่อไปนี้

5.1 นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security policy) โดยคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีภายในองค์กรและความเสี่ยงจากกรณีมีการใช้บริการเชื่อมต่อ หรือเข้าถึงข้อมูลจากบุคคลภายนอก

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

5.3 นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

6. ผู้รับใบอนุญาตต้องสื่อสารและสร้างความตระหนักให้แก่บุคลากรผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่เกี่ยวข้องกับระบบให้บริการในการปฏิบัติงานประจำวันอย่างเพียงพอและเหมาะสม เพื่อให้บุคลากรเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีอย่างปลอดภัย

7. ผู้รับใบอนุญาตต้องจัดให้มีการทบทวนนโยบายและมาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อการดำเนินการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

หมวดที่ 2
นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security policy)

8. ผู้รับใบอนุญาตต้องจัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ซึ่งครอบคลุมระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) และระบบเครือข่าย (network system) รวมถึงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญให้ชัดเจนเป็นลายลักษณ์อักษร ภายใต้หลักการดังต่อไปนี้
   (1) การรักษาความลับของข้อมูล
   (2) ความถูกต้องเชื่อถือได้ของระบบสารสนเทศ
   (3) การรักษาสภาพความพร้อมใช้งานของระบบให้บริการ
9. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยครอบคลุมหัวข้ออย่างน้อยดังต่อไปนี้
   9.1 การบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ (IT asset management)
   ผู้รับใบอนุญาตต้องบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การบำรุงรักษาทรัพย์สินอย่างสม่ำเสมอ การยกเลิกและเรียกคืนทรัพย์สิน โดยทะเบียนรายการสินทรัพย์ด้านเทคโนโลยีสารสนเทศต้องมีการระบุฮาร์ดแวร์ (hardware) ซอฟต์แวร์ (software) ข้อมูลที่ถือครอง รวมถึงการจัดประเภทและระดับความสำคัญของข้อมูล และเจ้าของทรัพย์สิน (owner) เป็นอย่างน้อย นอกจากนี้ต้องมีการวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support) จากผู้ผลิตด้วย
   9.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (information security)
   ผู้รับใบอนุญาตต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (data in transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest) โดยครอบคลุมหัวข้อดังต่อไปนี้
      (1) หลักเกณฑ์การจัดประเภทและระดับความสำคัญของข้อมูล (data classification)
      (2) แนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลที่สอดคล้องตามระดับความสำคัญ ซึ่งครอบคลุมถึงการกำหนดสิทธิผู้เข้าถึงข้อมูล วิธีการรับส่ง การประมวลผล และการจัดเก็บข้อมูล และการทำลายข้อมูล
      (3) การเข้ารหัสลับข้อมูล (cryptography) ตามระดับความสำคัญของข้อมูล รวมถึงวิธีการเข้ารหัสข้อมูล (cryptographic algorithm) และการบริหารจัดการกุญแจเข้ารหัสลับ (key management) โดยครอบคลุมทุกขั้นตอนของวงจรการบริหารจัดการกุญแจเข้ารหัสลับ (lifecycle of cryptographic keys) ตลอดจนกระบวนการสร้าง แจกจ่าย จัดเก็บ ใช้งาน การสำรอง เพิกถอน การต่ออายุ รวมถึงการบันทึกและตรวจสอบกิจกรรมที่สำคัญ

9.3 การควบคุมการเข้าถึงสารสนเทศ (access to information)

(1) ผู้รับใบอนุญาตต้องมีการควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม โดยอย่างน้อยต้องมีการควบคุมดังต่อไปนี้

(1.1) จำกัดการเข้าถึงสารสนเทศที่มีความสำคัญ (sensitive information) ข้อมูลอัตลักษณ์ และทรัพยากรที่เกี่ยวข้องกับระบบให้บริการเฉพาะบุคคลที่จำเป็นเท่านั้น

(1.2) ต้องมีกลไกควบคุมและจัดการสิทธิการเข้าถึงระบบปฏิบัติการ ระบบงาน ระบบฐานข้อมูล และระบบเครือข่าย รวมถึงอุปกรณ์ที่เกี่ยวข้องกับระบบให้บริการ ตามความจำเป็น (Least Privilege) ระดับความเสี่ยง และเป็นไปตามหลักการแบ่งแยกหน้าที่ที่ดี

(2) ในการจัดการการเข้าถึงระบบสารสนเทศ (information systems) ที่จัดเก็บสารสนเทศที่มีความสำคัญ (sensitive information) ผู้รับใบอนุญาตต้องมีกลไกในการระบุตัวตนที่สามารถแยกแยะผู้ใช้งาน การยืนยันตัวตน และการให้สิทธิในการอนุญาตให้เข้าถึงระบบ

(3) ผู้รับใบอนุญาตต้องจัดให้มีการบันทึกกิจกรรมการเข้าถึงสารสนเทศซึ่งสามารถแยกแยะผู้ใช้งานและสิทธิในการเข้าถึง

9.4 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)

ผู้รับใบอนุญาตต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของระบบให้บริการ บุคลากร และสินทรัพย์ที่เกี่ยวข้อง โดยอย่างน้อยต้องครอบคลุมกรณีดังต่อไปนี้

(1) การปกป้องทรัพยากรที่สอดคล้องกับระดับการประเมินผลกระทบทางธุรกิจอันเกิดจากการละเมิด การสูญเสีย หรือความเสียหาย โดยการกระทำของมนุษย์ ความขัดข้องของระบบสาธารณูปโภค สภาพแวดล้อมที่ไม่เหมาะสม หรือภัยพิบัติทางธรรมชาติ

(2) การประเมินความเสี่ยงด้านความมั่นคงปลอดภัย การเลือกใช้อุปกรณ์จัดเก็บและพื้นที่มั่นคงปลอดภัย

(3) การทำลายทรัพย์สินทางกายภาพอย่างมั่นคงปลอดภัย

9.5 การรักษาความมั่นคงปลอดภัยของการสื่อสาร (communications security)

ผู้รับใบอนุญาตต้องรักษาความมั่นคงปลอดภัยของการสื่อสารข้อมูล เพื่อให้ข้อมูลที่รับส่งผ่านเครือข่ายมีความมั่นคงปลอดภัย โดยอย่างน้อยต้องมีการดำเนินการ ดังนี้

(1) การออกแบบเครือข่ายอย่างมั่นคงปลอดภัย

(2) การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

(3) การป้องกันการดักรับข้อมูล

(4) การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย

(5) การควบคุมและจัดการสิทธิการใช้ระบบสารสนเทศระยะไกล

(6) มาตรการป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก

9.6 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation security)

ผู้รับใบอนุญาตต้องรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศโดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

(1) มีกระบวนการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศอย่างรัดกุม (change management)

(2) การบริหารจัดการขีดความสามารถของระบบ (capacity management) อย่างเหมาะสม เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอต่อการรองรับการให้บริการหรือดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต

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

(4) การสำรองข้อมูล (data backup) ด้วยวิธีการ เทคโนโลยี และระยะเวลาที่เหมาะสม

(5) การจัดเก็บประวัติกิจกรรม (logging) เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการใช้งานระบบหรือข้อมูล

(6) การตั้งค่าเทียบเวลา (clock synchronization) ให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากลในระดับเดียวกันทั้งระบบ

(7) การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการหรือเครื่องมือตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที

(8) การบริหารจัดการช่องโหว่ของระบบ (vulnerability management) ที่เหมาะสม โดยมีการประเมินช่องโหว่ (vulnerability assessment) การรายงานผลไปยังผู้รับผิดชอบ ติดตามและจัดการกับช่องโหว่ให้ได้รับการแก้ไขอย่างเพียงพอ โดยขอบเขตการประเมินช่องโหว่ต้องครอบคลุม การประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม สำหรับทุกระบบงานตามระดับความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(9) การทดสอบการเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญภายในหรือภายนอกที่เป็นอิสระอย่างสม่ำเสมออย่างน้อยปีละหนึ่งครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งมีการรายงานผลไปยังผู้รับผิดชอบ ติดตามและจัดการกับช่องโหว่ให้ได้รับการแก้ไขอย่างเพียงพอ โดยควรพิจารณาขอบเขตของการทดสอบเจาะระบบให้ครอบคลุมการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของระบบให้บริการ โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing) ทั้งนี้ ในกรณีที่สำนักงานเห็นว่าผลการทดสอบเจาะระบบมีข้อมูลรายงานหรือวิธีการทดสอบการเจาะระบบไม่ครอบคลุมช่องโหว่สำคัญที่เป็นความเสี่ยงที่ได้รับการยอมรับโดยทั่วไป หรือในกรณีที่สำนักงานเห็นว่าจำเป็นหรือสมควร สำนักงานอาจสั่งให้แต่งตั้งผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระดำเนินการทดสอบเจาะระบบเพิ่มเติมได้

(10) การบริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีการกำหนดมาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัย (security baseline configuration standards)

สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่าย มีกระบวนการควบคุมการตั้งค่าของระบบที่ใช้งานจริง มีการสอบทานการใช้มาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ และมีการทบทวนมาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัย อย่างน้อยปีละหนึ่งครั้ง

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

9.7 การพัฒนาระบบ (system development)

ผู้รับใบอนุญาตต้องนำมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศไปใช้ตลอดวงจรการพัฒนาระบบ โดยอย่างน้อยมีการดำเนินการดังต่อไปนี้

(1) มีเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) ซึ่งครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

(2) มีกระบวนการควบคุมเวอร์ชันของการพัฒนาระบบ

(3) มีการแบ่งแยกบาทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ

(4) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production)

(5) มีแนวทางการควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ

(6) ทดสอบระบบก่อนการใช้งานจริง โดยครอบคลุมการทดสอบตามความต้องการของหน่วยงานธุรกิจด้านประสิทธิภาพ และด้านความมั่นคงปลอดภัยเป็นอย่างน้อย

(7) การจัดการข้อผิดพลาดหรือข้อบกพร่องของระบบที่พบในการทดสอบหรือเมื่อนำไปใช้งานจริง

(8) มีการสร้างความตระหนักและให้ความรู้กับผู้พัฒนาโปรแกรมอย่างสม่ำเสมอ เพื่อเสริมสร้างทักษะในด้านการออกแบบและพัฒนาโปรแกรมอย่างปลอดภัย

9.8 การบริหารจัดการเหตุการณ์ไม่พึงประสงค์ (incident management)

ผู้รับใบอนุญาตต้องมีการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์อย่างเหมาะสมและทันท่วงที โดยมีขั้นตอนสำหรับบุคลากรและผู้ใช้งานในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ซึ่งจะครอบคลุมขั้นตอนการตรวจพบเหตุการณ์ การแจ้งเหตุ การพิสูจน์เหตุการณ์ การรายงานเหตุการณ์ การตอบสนองต่อเหตุการณ์ รวมถึงการรวบรวมและจัดเก็บหลักฐานเพื่อการสืบสวน นอกจากนี้ ต้องวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ไม่พึงประสงค์ซ้ำในอนาคต

9.9 การจัดทำแผนการกู้คืนเมื่อเกิดภัยพิบัติ (Disaster Recovery Plan) และการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)

(1) ผู้รับใบอนุญาตต้องจัดทำแผนการกู้คืนเมื่อเกิดภัยพิบัติ (Disaster Recovery Plan) และแผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) สำหรับระบบให้บริการ

โดยคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง ซึ่งครอบคลุมเนื้อหาอย่างน้อยดังต่อไปนี้

(1.1) การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis - BIA)

(1.2) การกำหนดระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD) เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

(1.3) แผนและขั้นตอนการกู้คืนระบบ

(1.4) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP)

(2) ต้องจัดทำคู่มือหรือเอกสารประกอบการดำเนินการตามแผนการกู้คืนเมื่อเกิดภัยพิบัติ (Disaster Recovery Plan) และการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) รวมทั้งประชาสัมพันธ์และฝึกอบรมบุคลากรที่เกี่ยวข้องให้มีความเข้าใจและสามารถปฏิบัติตามแผนดังกล่าวได้

(3) ต้องทบทวนและทดสอบการปฏิบัติตามแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจ อย่างน้อยปีละหนึ่งครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ พร้อมทั้งจัดทำรายงานผลการทดสอบ

(4) ต้องจัดให้มีระบบสำรองที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อระบบหลักหยุดชะงัก โดยระบบสำรองควรแยกออกจากระบบหลักในการให้บริการเพียงพอที่จะมิให้เกิดปัญหาหรือได้รับผลกระทบในลักษณะเดียวกันในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง เป็นต้น

10. การจัดเก็บประวัติกิจกรรม (log)

10.1 ผู้รับใบอนุญาตต้องจัดเก็บประวัติกิจกรรมเพื่อประโยชน์ในการตรวจสอบ ในกรณีอย่างน้อยดังต่อไปนี้

(1) การใช้สิทธิพิเศษของบุคลากรทั้งในกรณีที่ดำเนินการสำเร็จและไม่สำเร็จ

(2) การบริหารจัดการสิทธิผู้ใช้งาน ทั้งในการเพิ่มบัญชีและกลุ่มผู้ใช้งาน การลบ และการแก้ไขสิทธิ

(3) การแจ้งเตือนด้านความมั่นคงปลอดภัยและความผิดพลาด เช่น การปฏิเสธความพยายามเข้าสู่ระบบ การแจ้งเตือนความผิดพลาด

(4) การพยายามเข้าถึงระบบโดยไม่ได้รับอนุญาต

(5) สำหรับการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ต้องจัดเก็บประวัติกิจกรรมเกี่ยวกับการเชื่อมโยงข้อมูลอัตลักษณ์กับอัตลักษณ์ดิจิทัล

10.2 ประวัติกิจกรรมที่จัดเก็บต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

(1) วันที่และเวลาของเหตุการณ์

(2) ผู้ใช้งาน รหัสบ่งชี้ (identifier) หรือขั้นตอน ซึ่งแต่ละเหตุการณ์ต้องมีรหัสบ่งชี้เฉพาะ

(3) รายละเอียดของเหตุการณ์

(4) อุปกรณ์ที่เกี่ยวข้อง

(5) หมายเลขไอพีต้นทางของอุปกรณ์ที่ผ่านการยืนยันตัวตนเข้ามาในระบบให้บริการ

(6) หมายเลขพอร์ตต้นทางที่ถูกใช้ในการยืนยันตัวตน
(7) หมายเลขไอพีปลายทางที่ถูกใช้ในการยืนยันตัวตน
(8) หมายเลขพอร์ตปลายทางที่ถูกใช้ในการยืนยันตัวตน
(9) User Agent String ซึ่งระบุ browser และ ระบบปฏิบัติการที่พยายามยืนยันตัวตน

10.3 การจัดเก็บประวัติกิจกรรมสำหรับการพิสูจน์ตัวตน ต้องมีการจัดเก็บระดับของการพิสูจน์ตัวตนในแต่ละกิจกรรม

10.4 การจัดเก็บประวัติกิจกรรมสำหรับการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนในแต่ละกิจกรรม ให้รวมถึง
(1) ประเภทของสิ่งที่ใช้ยืนยันตัวตน
(2) ระดับความน่าเชื่อของการยืนยันตัวตน
(3) วันที่และเวลาที่ทำการเชื่อมโยงข้อมูลเพื่อออกสิ่งที่ใช้ยืนยันตัวตน

10.5 การจัดเก็บประวัติกิจกรรมสำหรับการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล ในแต่ละกิจกรรมต้องประกอบด้วยข้อมูลดังต่อไปนี้
(1) ประเภทของกิจกรรมการโต้ตอบ (interaction)
(2) รหัสบ่งชี้เฉพาะของกิจกรรมการโต้ตอบ
(3) ชื่อผู้เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตน
(4) รหัสบ่งชี้เฉพาะที่ใช้สำหรับกิจกรรมนั้น
(5) ประเภทของข้อมูลอัตลักษณ์ตามคำขอและการตอบกลับ
(6) ระดับความน่าเชื่อถือที่ใช้ในการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามคำขอและการตอบกลับ

10.6 ผู้รับใบอนุญาตต้องทำให้มั่นใจได้ว่าในการจัดเก็บประวัติกิจกรรมต้องดำเนินการให้ครอบคลุมในเรื่องดังต่อไปนี้
(1) มีการจัดเก็บอย่างมั่นคงปลอดภัย และมีความถูกต้องครบถ้วน
(2) ปราศจากการเข้าถึง การแก้ไข และการลบ โดยไม่ได้รับอนุญาต
(3) จัดเก็บไม่ต่ำกว่า 3 ปี นับแต่วันที่มีการดำเนินการ
(4) ประวัติกิจกรรมที่จัดเก็บต้องไม่มีข้อมูลชีวมิติ

11. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ (Cyber Security Incident)

11.1 ผู้รับใบอนุญาตต้องจัดให้มีกลไกหรือกระบวนการในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ (Cyber Security Incident) อย่างน้อย ดังนี้
(1) ต้องมีกลไกในการตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ รวมถึงจัดให้มีช่องทางที่เป็นการรักษาความลับสำหรับบุคลากรและผู้ใช้งานในการแจ้งเหตุการณ์ที่น่าสงสัยเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
(2) ต้องจัดให้มีกลไกการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ไม่พึงประสงค์ ที่มีลักษณะคล้ายกับเหตุการณ์ที่ตรวจพบ หรือที่เกี่ยวข้องกับเหตุการณ์ที่ตรวจพบ และนำข้อมูลที่เกี่ยวกับเหตุการณ์ที่พบมาตรวจสอบกับการลงทะเบียนใหม่และการปรับปรุงข้อมูลของผู้ใช้งานเดิมด้วย โดยจะต้องไม่อนุญาตให้มีการลงทะเบียนใหม่หรือมีการปรับปรุงข้อมูล หากกลไกการควบคุมระบุหรือบ่งชี้ว่าการลงทะเบียนหรือการปรับปรุงจะก่อให้เกิดเหตุการณ์ด้านความปลอดภัยทางไซเบอร์

(3) ต้องมีกระบวนการกำหนดหลักเกณฑ์เกี่ยวกับการตัดสินใจในช่วงที่สำคัญ (critical stage) เพื่อการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์

(4) ต้องมีขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ และมาตรการบรรเทาผลกระทบใด ๆ ให้กับบุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบ เช่น ผู้ใช้บริการ ผู้บุคคลภายนอกที่เกี่ยวกับระบบให้บริการ เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

11.2 ผู้รับใบอนุญาตต้องจัดทำแผนการสื่อสารในภาวะวิกฤต (crisis communication plan) เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ และดำเนินการฝึกซ้อม ทบทวน และปรับปรุงแผนอย่างน้อยปีละหนึ่งครั้งเพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤต

11.3 ผู้รับใบอนุญาตต้องรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี ซึ่งอย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้

(1) วันที่และเวลาของเหตุการณ์

(2) จำนวนเหตุการณ์และระดับความรุนแรง

(3) มาตรการในการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

11.4 ในกรณีที่เกิดหรือคาดว่าจะเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีซึ่งส่งผลกระทบต่อการให้บริการหรือระบบงาน และเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารทราบ ผู้รับใบอนุญาตต้องรายงานมายังสำนักงานทันทีเมื่อเกิดหรือรับทราบปัญหาหรือเหตุการณ์ดังกล่าว และให้แจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

11.5 ผู้รับใบอนุญาตต้องมีกลไกหรือกระบวนรับแจ้งเหตุอันน่าสงสัยเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์

11.6 ในกรณีที่เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ก่อให้เกิดผลกระทบกับผู้ใช้บริการ ผู้รับใบอนุญาตต้องมีกระบวนการที่เหมาะสมสำหรับการพิสูจน์ยืนยันตัวตนบุคคลที่เป็นเจ้าของคุณลักษณะ (Attribute) อัตลักษณ์ดิจิทัล (Digital Identity) หรือสิ่งที่ใช้ยืนยันตัวตน (Credential) ที่อยู่ภายใต้เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ และมีเทคโนโลยีที่เหมาะสมซึ่งสามารถบ่งชี้ถึงการละเมิด คุณลักษณะ (Attribute) อัตลักษณ์ดิจิทัล (Digital Identity) หรือสิ่งที่ใช้ยืนยันตัวตน (Credential)

12. การบริหารจัดการบุคคลภายนอก (Third Party Management)

12.1 ในกรณีที่ผู้รับใบอนุญาตดำเนินการดังต่อไปนี้

(1) ใช้บริการจากผู้ให้บริการด้านเทคโนโลยีสารสนเทศ (IT outsourcing)

(2) เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก

(3) ให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญ หรือเข้าถึงข้อมูลผู้ใช้บริการของระบบให้บริการ

ผู้รับใบอนุญาตต้องกำกับดูแลกระบวนการบริหารความเสี่ยง และการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบุคคลภายนอกให้อยู่ในระดับที่สอดคล้องกับระดับความเสี่ยงของการดำเนินงานของผู้รับใบอนุญาต โดยพิจารณาดำเนินการตามแนวปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยง

บุคคลภายนอกที่สำนักงานจัดทำขึ้น ทั้งนี้ สามารถพิจารณาประยุกต์ใช้ให้เหมาะสมและสอดคล้องตามขอบเขต ระดับความเสี่ยงและนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของบุคคลภายนอก

12.2 ในการบริหารจัดการบุคคลภายนอกเพื่อควบคุมให้มีการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่เหมาะสม ต้องมีการดำเนินการอย่างน้อย ดังนี้

(1) ระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลหรือระบบเทคโนโลยีสารสนเทศที่บุคคลภายนอกสามารถเข้าถึง และกำหนดแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยง

(2) การรักษาความมั่นคงปลอดภัยระบบสารเทศของบุคคลภายนอกต้องสอดคล้องกับมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของผู้รับใบอนุญาต

(3) กำหนดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รวมถึงข้อกำหนดการไม่เปิดเผยข้อมูล เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง กระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของบุคคลภายนอก ในข้อตกลงการให้บริการหรือเงื่อนไขของสัญญากับบุคคลภายนอก

(4) ติดตาม ประเมิน และทบทวนผลการปฏิบัติงานของบุคคลภายนอก

(5) ให้มีการสื่อสารหรือการฝึกอบรมบุคคลภายนอกที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบให้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยเฉพาะอย่างยิ่งบุคคลภายนอกที่สามารถเข้าถึงระบบสารสนเทศ โดยอย่างน้อยต้องมีการดำเนินการ ดังนี้

(4.1) เผยแพร่หรืออบรมนโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้อง

(4.2) ให้มีการฝึกอบรมหรือสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบอย่างสม่ำเสมอ

12.3 ในกรณีที่ผู้รับใบอนุญาตมีการใช้บริการจากผู้ให้บริการภายนอกเพื่อให้ดำเนินการแทนสำหรับกิจกรรมที่สำนักงานประกาศกำหนด ให้ผู้รับใบอนุญาตปฏิบัติตามหลักเกณฑ์ด้านการใช้บริการจากบุคคลภายนอกที่เกี่ยวกับระบบให้บริการด้วย

หมวด 3
การบริหารและการจัดการความเสี่ยงของระบบให้บริการ

13. เพื่อให้การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ซึ่งครอบคลุมกระบวนการอย่างน้อยในเรื่องดังต่อไปนี้

13.1 การประเมินความเสี่ยง (risk assessment)

(1) ระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศ (risk identification) ที่อาจจะเกิดขึ้น โดยอย่างน้อยต้องระบุปัจจัยและสาเหตุของความเสี่ยง ประเภทของความเสี่ยง ผลกระทบต่อการประกอบธุรกิจ

(2) การวิเคราะห์ความเสี่ยง (risk analysis) เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม โดยอย่างน้อยต้องระบุเจ้าของความเสี่ยง (risk owner) การควบคุมที่มีอยู่ในปัจจุบัน (existing control) วิเคราะห์ผลกระทบที่อาจจะเกิดขึ้น

(3) ประเมินค่าความเสี่ยง (risk evaluation) โดยกำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบ กำหนดระดับความเสี่ยงที่ยอมรับได้ (risk appetite) ประเมินโอกาสของการเกิดความเสี่ยง และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ และนำมาจัดลำดับในการบริหารความเสี่ยง

13.2 การจัดการความเสี่ยง (risk treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้

13.3 การติดตามและทบทวนความเสี่ยง (risk monitoring and review)

มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ โดยกำหนดมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่มีอยู่และการจัดการความเสี่ยงอย่างเพียงพอ รวมถึงการตอบสนองและการจัดการการเปลี่ยนแปลงที่สำคัญต่อความเสี่ยงและสภาพแวดล้อมของการปฏิบัติงาน และกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) เพื่อใช้ติดตามและทบทวนความเสี่ยง

13.4 การรายงานความเสี่ยง (risk reporting)

ต้องมีการรายงานระดับความเสี่ยงและผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อผู้บริหารระดับสูงหรือคณะกรรมการที่ได้รับมอบหมาย

14. ผู้รับใบอนุญาตต้องจัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อการดำเนินการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

15. ในกรณีที่เกิดเหตุการณ์ซึ่งส่งผลกระทบหรือขัดขวางความสามารถของผู้รับใบอนุญาตในการปฏิบัติตามหลักเกณฑ์ที่กำหนด ผู้รับใบอนุญาตต้องดำเนินการดังต่อไปนี้

15.1 แจ้งให้สำนักงานทราบถึงเหตุการณ์ซึ่งส่งผลให้ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดโดยเร็ว

15.2 บันทึกการตัดสินใจเกี่ยวกับการดำเนินมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่เปลี่ยนแปลงไป และการแก้ไขหรือเยียวยา (ถ้ามี) และนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี

15.3 ผู้รับใบอนุญาตอาจเปลี่ยนแปลงมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศได้ภายในระยะเวลาจำกัดเพื่อรับมือเหตุการณ์ที่เกิดขึ้น ทั้งนี้ การเปลี่ยนแปลงดังกล่าวต้องไม่ทำให้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศสูงกว่าระดับความเสี่ยงที่ยอมรับได้

หมวด 4
การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 1 นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล

16. ผู้รับใบอนุญาตต้องจัดให้มีนโยบายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ซึ่งสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และหลักเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคลตามที่สำนักงานประกาศ โดยต้องมีการเผยแพร่เป็นการทั่วไป
17. ผู้รับใบอนุญาตต้องกำหนดบุคลากรที่ทำหน้าที่รับผิดชอบในการกำกับดูแลการดำเนินงานตามนโยบายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคล รวมถึงรับผิดชอบและจัดให้มีการดำเนินการตามนโยบายและมาตรการดังกล่าว
18. นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลต้องมีข้อมูลที่ชัดเจน และประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้
    (1) ประเภทของข้อมูลส่วนบุคคลที่ผู้รับใบอนุญาตเก็บรวบรวม
    (2) วิธีการได้มาซึ่งข้อมูลส่วนบุคคล
    (3) วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
    (4) วิธีการที่ผู้ใช้บริการสามารถเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน รวมทั้งวิธีการในการปรับปรุงหรือแก้ไขข้อมูลส่วนบุคคลดังกล่าว
    (5) ช่องทางการร้องเรียนและการจัดการเรื่องร้องเรียนกรณีผู้รับใบอนุญาตฝ่าฝืนหลักเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคล
19. ผู้รับใบอนุญาตต้องจัดให้มีการฝึกอบรมหรือสร้างความตระหนักด้านการคุ้มครองข้อมูลส่วนบุคคลแก่บุคลากรที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบให้บริการก่อนเริ่มปฏิบัติงาน และอย่างน้อยปีละหนึ่งครั้ง ซึ่งครอบคลุมหลักเกณฑ์ของกฎหมายที่เกี่ยวข้อง และนโยบายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้รับใบอนุญาต

ส่วนที่ 2 การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

20. ในการจัดทำรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจ ผู้รับใบอนุญาตต้องมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลที่อาจเกิดขึ้นจากระบบให้บริการ และกำหนดแนวทางในการบริหารจัดการ
21. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้
    (1) ระบุขั้นตอน กระบวนการ กิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในระบบให้บริการ
    (2) วิเคราะห์ความเสี่ยงของการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและหลักเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคล
    (3) วิเคราะห์ผลกระทบของขั้นตอน กระบวนการ กิจกรรมที่ส่งผลต่อการคุ้มครองข้อมูลส่วนบุคคล
    (4) กำหนดแนวทางการจัดการ ควบคุม และป้องกันที่เหมาะสม
22. กรณีที่มีการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการให้บริการ ภายหลังจากเริ่มประกอบธุรกิจ ผู้รับใบอนุญาตต้องจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล และนำส่งพร้อมการแจ้งการเปลี่ยนแปลงต่อสำนักงาน

ส่วนที่ 3 การจัดการเหตุการละเมิดข้อมูลส่วนบุคคล

23. ผู้รับใบอนุญาตต้องจัดให้มีแผนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคล ซึ่งอย่างน้อยต้องประกอบด้วย
    (1) ขั้นตอนการปฏิบัติเมื่อเกิดหรือสงสัยว่าจะเกิดเหตุการละเมิดข้อมูลส่วนบุคคล การตรวจพบ หรือการรายงาน
    (2) การกำหนดบทบาทหน้าที่และความรับผิดชอบของบุคลากรตามแผนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคล
    (3) แนวทางการสื่อสารข้อมูลเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ซึ่งครอบคลุมการสื่อสารภายในการแจ้งเตือนผู้ได้รับผลกระทบ และการแจ้งเตือนหรือการรายงานตามกฎหมายที่เกี่ยวข้อง
    (4) แผนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคลต้องสอดคล้องกับมาตรการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ และมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

ส่วนที่ 4 ข้อมูลเกี่ยวกับพฤติกรรมการใช้งานระบบ

24. ผู้รับใบอนุญาตจะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเกี่ยวกับพฤติกรรมการใช้งานระบบให้บริการของผู้ใช้บริการได้เฉพาะเพื่อวัตถุประสงค์ดังต่อไปนี้
    (1) เพื่อการตรวจสอบไอเดนติตี้ของผู้ใช้บริการ และอำนวยความสะดวกให้กับผู้ใช้บริการ
    (2) เพื่อสนับสนุนจัดการเหตุการณ์การทุจริตหรือฉ้อโกงในระบบให้บริการ
    (3) เพื่อพัฒนาประสิทธิภาพหรือความสามารถในการให้บริการของระบบให้บริการ
    (4) เป็นการปฏิบัติตามกฎหมาย
25. ห้ามมิให้ผู้รับใบอนุญาตนำข้อมูลเกี่ยวกับพฤติกรรมการใช้งานของผู้ใช้บริการตามวรรคหนึ่งไปขายให้กับบุคคลอื่น

ส่วนที่ 5 การบริหารจัดการข้อมูลชีวมิติ

26. ในกรณีที่ผู้รับใบอนุญาตมีการเก็บรวบรวมข้อมูลชีวมิติของผู้ใช้บริการ ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล โดยเจ้าของข้อมูลได้รับแจ้งถึงวัตถุประสงค์ของการเก็บรวบรวมและใช้งานข้อมูลชีวมิติอย่างชัดเจน
27. ผู้รับใบอนุญาตจะจัดเก็บข้อมูลชีวมิติได้เฉพาะเพื่อวัตถุประสงค์ดังต่อไปนี้
    (1) เพื่อประโยชน์ในการใช้บริการระบบให้บริการ
    (2) เพื่อการปรับปรุง พัฒนา และทดสอบสมรรถนะของระบบให้บริการ
28. ในการจัดเก็บข้อมูลชีวมิติ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยข้อมูลชีวมิติที่ชัดเจน โดยครอบคลุมกระบวนการอย่างน้อย ดังนี้
    (1) จัดให้มีการเข้ารหัสข้อมูลชีวมิติ
    (2) จัดเก็บข้อมูลชีวมิติแยกออกจากการเก็บเทมเพลตชีวมิติ และข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ
    (3) จัดเก็บบนเครือข่ายที่มั่นคงปลอดภัย และรับส่งข้อมูลชีวมิติผ่านช่องทางที่มั่นคงปลอดภัย
    (4) จำกัดการเข้าถึงข้อมูลชีวมิติเฉพาะบุคลากรผู้รับผิดชอบ

29. กรณีที่ต้องมีการแลกเปลี่ยนข้อมูลชีวมิติเพื่อประโยชน์ในการให้บริการระบบให้บริการ ผู้ให้บริการต้องได้รับความยินยอมโดยชัดแจ้งจากผู้ใช้บริการ โดยต้องมีการเข้ารหัสข้อมูลและจัดให้มีการแลกเปลี่ยนข้อมูลผ่านช่องทางที่มีความมั่นคงปลอดภัย
30. ผู้รับใบอนุญาตต้องทำลายข้อมูลชีวมิติเมื่อผู้ใช้บริการเพิกถอนความยินยอมหรือยกเลิกการใช้บริการ โดยต้องดำเนินการให้ครอบคลุมทุกกระบวนการที่มีการเก็บรวบรวม เช่น การทำสำเนา แคช การจัดเก็บชั่วคราวในฐานข้อมูล เป็นต้น รวมถึงกรณีที่มีการว่าจ้างบุคคลภายนอกให้ดำเนินการด้วย
31. ผู้รับใบอนุญาตต้องมีการบันทึกหรือจัดเก็บหลักฐานการทำลายข้อมูลชีวมิติเพื่อประโยชน์ในการตรวจสอบ

ส่วนที่ 6 ความยินยอม

32. ผู้รับใบอนุญาตต้องได้รับความยินยอมโดยชัดแจ้งจากผู้ใช้บริการก่อนการเปิดเผยข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการแก่ผู้ที่เกี่ยวข้องกับการใช้งานระบบให้บริการ
33. ผู้รับใบอนุญาตต้องจัดเก็บประวัติกิจกรรม (log) ที่แสดงถึงการได้ความยินยอมโดยชัดแจ้งจากผู้ใช้บริการ รวมถึงข้อมูลดังต่อไปนี้
    (1) วันที่และวิธีการได้มาซึ่งความยินยอม
    (2) ระยะเวลาของความยินยอม
    (3) เงื่อนไขการให้ความยินยอม
    (4) การถอน หรือการสิ้นอายุความยินยอม

ส่วนที่ 7 การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล

34. การเข้าถึงข้อมูล
    34.1 ผู้รับใบอนุญาตต้องจัดให้มีวิธีการที่ให้ผู้ใช้บริการสามารถเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้โดยไม่เสียค่าใช้จ่าย
    34.2 ผู้รับใบอนุญาตต้องตอบรับคำขอเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการภายในสามสิบวันนับแต่ได้รับคำขอ หากผู้รับใบอนุญาตปฏิเสธคำขอ ต้องดำเนินการให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
35. การแก้ไขปรับปรุงข้อมูล
    35.1 ผู้รับใบอนุญาตต้องจัดให้ผู้ใช้บริการสามารถแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้ด้วยวิธีการที่เข้าถึงได้โดยง่าย
    35.2 ผู้รับใบอนุญาตต้องจัดให้มีคู่มือหรือคำอธิบายวิธีการในการแก้ไขหรือปรับปรุงข้อมูลสำหรับผู้ใช้บริการ
36. การดูแลคุณภาพของข้อมูลส่วนบุคคล
    36.1 ผู้รับใบอนุญาตต้องมีการทบทวนข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยตรวจทานและปรับปรุงข้อมูลที่ใช้สำหรับการพิสูจน์และยืนยันตัวตนให้เป็นข้อมูลปัจจุบัน และดำเนินการอย่างสม่ำเสมอ
    36.2 หากผู้รับใบอนุญาตได้จัดให้มีการทบทวนข้อมูลของผู้ใช้บริการแล้ว แต่ไม่สามารถติดต่อผู้ใช้บริการได้ ให้กำหนดมาตรการที่สามารถทบทวนข้อมูลผู้ใช้บริการให้เป็นปัจจุบันเมื่อผู้ใช้บริการมาทำธุรกรรม หรือในโอกาสแรกที่สามารถติดต่อผู้ใช้บริการได้

ส่วนที่ 8 การจัดการเรื่องร้องเรียน

37. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการหรือกลไกในการจัดการเรื่องร้องเรียนเกี่ยวกับข้อมูลส่วนบุคคล โดยมีลักษณะอย่างน้อยดังนี้
    (1) ผู้ใช้บริการสามารถเข้าถึงได้ง่าย มีข้อมูลการติดต่อที่ชัดเจน
    (2) มีกระบวนการจัดการด้วยความเป็นธรรม มีความเป็นกลาง และโปร่งใส
    (3) มีขั้นตอนที่ชัดเจน ดำเนินการอย่างทันท่วงที และมีการบรรเทาความเสียหายอย่างเหมาะสม
    (4) มีบุคลากรที่มีความรู้ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการจัดการเรื่องร้องเรียน
    (5) มีกลไกที่สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

หมวด 5
การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง (IT compliance)

38. ผู้รับใบอนุญาตต้องปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น เพื่อป้องกันการฝ่าฝืนหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

หมวด 6
การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

39. ผู้รับใบอนุญาตต้องจัดให้มีการตรวจสอบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบให้บริการอย่างน้อยปีละหนึ่งครั้ง รวมทั้งต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเพียงพอ