# ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ที่ ธพส. ๑/๒๕๖๖

เรื่อง หลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการ
เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

---

เพื่อให้การควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตสามารถให้บริการได้อย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถให้บริการได้อย่างต่อเนื่อง รวมทั้งควบคุมดูแลผู้ประกอบธุรกิจบริการให้มีความน่าเชื่อถือ และมีการคุ้มครองผู้ใช้บริการอย่างเหมาะสม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงได้กำหนดหลักเกณฑ์การควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต เพื่อให้ผู้ประกอบธุรกิจบริการต้องถือปฏิบัติ

อาศัยอำนาจตามความในมาตรา ๑๙ มาตรา ๒๑ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๕ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ๒๕๖๕ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต”

ข้อ ๒ ลักษณะการให้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่มีลักษณะเป็นบริการที่ต้องได้รับใบอนุญาต ตามมาตรา ๗ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ๒๕๖๕ มีรายละเอียดปรากฏตามข้อกำหนดแนบท้ายประกาศ

ข้อ ๓ ในประกาศฉบับนี้และข้อกำหนดแนบท้ายประกาศ ให้ใช้คำนิยามตามที่กำหนด ดังนี้

“ผู้รับใบอนุญาต” หมายความว่า บุคคลที่ได้รับใบอนุญาตให้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

“ผู้ใช้บริการ” หมายความว่า ผู้ขอใช้บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน บริการยืนยันตัวตน หรือบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ประชาชน นิติบุคคลที่มาขอใช้บริการ ทั้งนี้ ขึ้นอยู่กับลักษณะการให้บริการของผู้รับใบอนุญาตแต่ละราย

“ระบบการให้บริการ” หมายความว่า ระบบและเทคโนโลยีที่ใช้สำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่มีลักษณะเป็นบริการที่ต้องได้รับใบอนุญาต และหมายรวมถึงระบบงานที่เกี่ยวข้องกับการประกอบธุรกิจบริการดังกล่าวด้วย

“บุคคลภายนอก” หมายความว่า บุคคลหรือนิติบุคคลภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของผู้รับใบอนุญาต หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลที่สำคัญของผู้รับใบอนุญาตหรือข้อมูลของผู้ใช้บริการของระบบการให้บริการ รวมถึงผู้รับดำเนินการแทนผู้รับใบอนุญาต ทั้งนี้ บุคคลภายนอกไม่ครอบคลุมถึงผู้ใช้บริการซึ่งเป็นผู้ใช้งานระบบการให้บริการของผู้รับใบอนุญาต

“ผู้รับดำเนินการแทน” หมายความว่า บุคคลภายนอกซึ่งเป็นบุคคลธรรมดาหรือนิติบุคคลที่มีการทำสัญญาหรือข้อตกลงร่วมกับผู้รับใบอนุญาตในการดำเนินการแทนผู้รับใบอนุญาตสำหรับการให้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ตัวแทนในการเก็บรวบรวมข้อมูลผู้ใช้บริการซึ่งอาจมีการเชื่อมต่อระบบงานด้านเทคโนโลยีสารสนเทศกับผู้รับใบอนุญาตด้วย

“สำนักงาน” หมายความว่า สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

“คณะกรรมการ” หมายความว่า คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ข้อ ๔ การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่มีลักษณะเป็นบริการที่ต้องได้รับใบอนุญาตต้องปฏิบัติตามหลักเกณฑ์การควบคุมดูแลการประกอบธุรกิจบริการในเรื่อง ดังต่อไปนี้

(๑) หลักเกณฑ์การบริหารและจัดการความเสี่ยงในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(๒) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ

(๓) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

(๔) หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ

(๕) หลักเกณฑ์ตามลักษณะของการให้บริการ

(๖) หลักเกณฑ์การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ การคุ้มครองผู้ใช้บริการและมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ

(๗) หลักเกณฑ์การใช้บริการจากผู้รับดำเนินการแทน ตามข้อกำหนดแนบท้ายประกาศ

ข้อ ๕ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๒๒ มิถุนายน พ.ศ. ๒๕๖๖ เป็นต้นไป

ประกาศ ณ วันที่ ๒๖ พฤษภาคม พ.ศ. ๒๕๖๖
ชัยชนะ มิตรพันธ์
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

**ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. ๑/๒๕๖๖**
**ฉบับที่ ๑**
**ลักษณะการให้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล**
**ที่มีลักษณะเป็นบริการที่ต้องได้รับใบอนุญาต**
---

**๑. บริการพิสูจน์ตัวตน**

บริการพิสูจน์ตัวตนเป็นบริการเกี่ยวกับกระบวนการอันเป็นสาระสำคัญในการพิสูจน์ตัวตน ซึ่งครอบคลุมกระบวนการหลัก ๓ กระบวนการ ดังนี้

๑.๑ กระบวนการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล เช่น การรวบรวมข้อมูลจากบัตรประชาชน การถ่ายภาพใบหน้า

๑.๒ กระบวนการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลว่ามีความถูกต้อง แท้จริง และความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์ เช่น การตรวจสอบรูปถ่ายของหลักฐานแสดงตน การตรวจสอบลักษณะทางกายภาพของหลักฐานแสดงตนโดยเจ้าหน้าที่ การตรวจสอบข้อมูลบนหลักฐานแสดงตนและตรวจสอบสถานะของหลักฐานแสดงตน

๑.๓ กระบวนการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์ดังกล่าวเพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริงตามระดับความน่าเชื่อถือที่นำมาใช้ในการพิสูจน์ตัวตน เช่น การเปรียบเทียบภาพใบหน้าของบุคคลกับภาพใบหน้าบนหลักฐานแสดงตน

**๒. บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน**

บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนครอบคลุมกระบวนการหลัก ดังนี้

๒.๑ กระบวนการออกหรือลงทะเบียนชนิดของสิ่งที่ใช้ในการยืนยันตัวตน เช่น รหัสจดจำ อุปกรณ์ OTP อุปกรณ์เข้ารหัสลับ

๒.๒ กระบวนการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนซึ่งประกอบด้วยกระบวนการสำคัญ ดังนี้

๒.๒.๑ การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนโดยสร้างความเชื่อมโยงระหว่างอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนเข้ากับสิ่งที่ใช้ยืนยันตัวตนเพื่อให้บุคคลดังกล่าวใช้ในการยืนยันตัวตน

๒.๒.๒ การดำเนินการในกรณีสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย หรือเสียหาย รวมถึงการออกสิ่งที่ใช้ยืนยันตัวตนทดแทนอันเดิม (replacement)

๒.๒.๓ การดำเนินการในกรณีสิ่งที่ใช้ยืนยันตัวตนหมดอายุการใช้งาน และการออกสิ่งที่ใช้ยืนยันตัวตนอันใหม่ (renewal)

๒.๒.๔ การดำเนินการในกรณีที่ต้องมีการเพิกถอน (revocation) หรือยุติการใช้งาน (termination) ของสิ่งที่ใช้ยืนยันตัวตน

**๓. บริการยืนยันตัวตน**

บริการยืนยันตัวตนเป็นกระบวนการยืนยันอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้น

**๔. บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล**

บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลเป็นการให้บริการเพื่อการเชื่อมต่อหรือเชื่อมโยงระหว่างผู้รับใบอนุญาตกับผู้ประสงค์จะอาศัยการพิสูจน์และยืนยันตัวตนหรือผู้ที่เกี่ยวข้องเพื่อแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยมีการแจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่สามารถเชื่อมต่อกับระบบการให้บริการ และการบริหารจัดการการเชื่อมต่อในระบบการให้บริการ เช่น การกำหนดโพรโทคอล และเงื่อนไขในการเชื่อมต่อกับระบบการให้บริการ

แต่ทั้งนี้ ไม่รวมถึงผู้ทำหน้าที่เป็นสื่อกลางในการเชื่อมต่อเพื่อรับส่งข้อมูลระหว่างผู้ใช้บริการกับระบบการให้บริการของผู้รับใบอนุญาตซึ่งไม่สามารถเข้าถึงข้อมูลสำหรับการพิสูจน์และยืนยันตัวตนในระบบการให้บริการได้

**ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. ๑/๒๕๖๖**
**ฉบับที่ ๒**
**หลักเกณฑ์การบริหารและจัดการความเสี่ยง**
**ในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล**
---

ข้อ ๑ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายและมาตรการบริหารจัดการความเสี่ยงซึ่งครอบคลุมความเสี่ยงที่เกี่ยวข้องกับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อประเมินฐานะและผลการดำเนินงาน โดยคำนึงถึงผลกระทบจากความเสี่ยงของการให้บริการ เพื่อกำหนดมาตรการและแผนการบรรเทาผลกระทบที่อาจจะเกิดขึ้นอย่างทันท่วงที

ข้อ ๒ ผู้รับใบอนุญาตต้องเข้าใจและตระหนักถึงความเสี่ยงสำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ส่งผลกระทบต่อผู้ที่เกี่ยวข้อง รวมถึงบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมกระบวนการในการบริหารจัดการความเสี่ยง ดังนี้

๒.๑ การระบุความเสี่ยงที่เกี่ยวข้องกับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (risk identification) ตามลักษณะการให้บริการ

๒.๒ การประเมินความเสี่ยง (risk assessment) ซึ่งครอบคลุมการประเมินความเสี่ยงตั้งต้นและการตรวจสอบความสามารถในการบริหารจัดการความเสี่ยง

๒.๓ การวัดผลความเสี่ยงกับเกณฑ์การประเมินความเสี่ยง (risk evaluation)

๒.๔ การลดความเสี่ยงหลังจากการประเมินความเสี่ยงเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (risk treatment)

๒.๕ การติดตามและรายงานผลความเสี่ยงอย่างต่อเนื่อง (risk monitoring and reporting)

ข้อ ๓ ในการระบุความเสี่ยงที่เกี่ยวข้องกับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ต้องดำเนินการให้ครอบคลุมความเสี่ยง ๕ ด้าน ได้แก่

๓.๑ ความเสี่ยงด้านกลยุทธ์ (strategic risk) หมายถึง ความเสี่ยงของการสูญเสียที่เกิดขึ้นจากการตัดสินใจทางธุรกิจที่ไม่พึงประสงค์ การตัดสินใจทางธุรกิจที่ไม่ดี หรือการไม่ตอบสนองต่อการเปลี่ยนแปลงในอุตสาหกรรมและสภาพแวดล้อมในการดำเนินงาน ทั้งนี้ ความเสี่ยงด้านกลยุทธ์สำหรับผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความคล้ายคลึงกับความเสี่ยงขององค์กรทั่วไป โดยมีปัจจัยที่ต้องคำนึงถึง เช่น นโยบาย แผนกลยุทธ์ และการจัดสรรงบประมาณ อิทธิพลในการตัดสินใจเชิงกลยุทธ์ การบริหารความเสี่ยงในระดับองค์กร

๓.๒ ความเสี่ยงด้านการปฏิบัติการ (operational risk) หมายถึง ความเสี่ยงที่จะเกิดความเสียหายต่าง ๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการควบคุมภายใน บุคลากร และระบบงาน หรือจากเหตุการณ์ภายนอก เช่น ความเสี่ยงจากการฉ้อโกงโดยบุคคลภายในและบุคคลภายนอก ความเสี่ยงจากการขัดข้องหรือหยุดชะงักของระบบงาน ความเสี่ยงจากแนวปฏิบัติเกี่ยวกับผู้ใช้บริการ การให้บริการและดำเนินธุรกิจ

๓.๓ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (information technology risk) หมายถึง ความเสี่ยงของผลลัพธ์ที่ไม่พึงประสงค์ ความเสียหาย การสูญเสีย การละเมิด ความล้มเหลวหรือการหยุดชะงักใด ๆ ที่อาจเกิดขึ้นจากการใช้หรือการพึ่งพาฮาร์ดแวร์คอมพิวเตอร์ ซอฟต์แวร์ อุปกรณ์ ระบบ แอปพลิเคชัน และเครือข่าย ความเสี่ยงนี้มักเกี่ยวข้องกับข้อบกพร่องของระบบ ข้อผิดพลาดในการประมวลผล ข้อบกพร่องของซอฟต์แวร์ ข้อผิดพลาดในการทำงาน ความล้มเหลวของฮาร์ดแวร์ ความล้มเหลวของระบบ ความไม่เพียงพอของความจุ ช่องโหว่ของเครือข่าย จุดอ่อนในการควบคุม ข้อบกพร่องด้านความปลอดภัย การโจมตีที่เป็นอันตราย เหตุการณ์การเจาะระบบ โดยทั่วไปความเสี่ยงด้านเทคโนโลยีสารสนเทศสำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ภัยคุกคามทางไซเบอร์ การรั่วไหลของข้อมูล รวมถึงข้อมูลอ่อนไหวซึ่งมักเป็นองค์ประกอบสำคัญในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

๓.๔ ความเสี่ยงด้านชื่อเสียงขององค์กร (reputation risk) หมายถึง ความเสี่ยงที่ทำให้การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้รับผลกระทบทางลบจากสังคม ส่งผลให้สูญเสียชื่อเสียงและความน่าเชื่อถือในการให้บริการ เช่น การเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้ตั้งใจ

๓.๕ ความเสี่ยงด้านการปฏิบัติตามหลักเกณฑ์ (compliance risk) หมายถึง ความเสี่ยงที่เกิดจากการที่ผู้รับใบอนุญาตไม่สามารถปฏิบัติงานสอดคล้องตามที่กฎหมาย กฎระเบียบหรือมาตรฐานที่เกี่ยวข้องกับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลกำหนด ทั้งนี้รวมถึงมาตรฐานสากลที่กฎหมายหรือกฎระเบียบอ้างถึงด้วย เช่น การไม่ปฏิบัติตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

ข้อ ๔ ผู้รับใบอนุญาตต้องดำเนินการให้สอดคล้องตามแนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของสำนักงาน พร้อมจัดส่งผลการประเมินต่อสำนักงานตามรูปแบบและระยะเวลาที่สำนักงานกำหนด โดยผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับรองผลการประเมินตนเองก่อนนำส่งต่อสำนักงาน

ข้อ ๕ ผู้รับใบอนุญาตต้องจัดให้มีการทบทวนนโยบายและมาตรการบริหารจัดการความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

**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

**ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. ๑/๒๕๖๖**
**ฉบับที่ ๔**
**หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ**

---

ข้อ ๑ ผู้รับใบอนุญาตต้องมีการกำหนดบุคลากรที่ทำหน้าที่ในการกำกับดูแลการดำเนินงานเกี่ยวกับการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ รวมถึงรับผิดชอบในการจัดให้มีและดำเนินการตามแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

ข้อ ๒ ผู้รับใบอนุญาตต้องจัดให้มีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๒.๑ จัดให้มีแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๒.๒ กำหนดระดับความเสี่ยงที่ยอมรับได้สำหรับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๒.๓ จัดให้มีการบริหารความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๒.๔ จัดให้มีมาตรการที่เหมาะสมในการป้องกัน การตรวจจับ และจัดการกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ และดูแลให้มีการดำเนินการตามมาตรการดังกล่าว

ข้อ ๓ การจัดทำแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบต้องสอดคล้องกับลักษณะการให้บริการและความเสี่ยงของระบบการให้บริการ โดยประกอบด้วยข้อมูลอย่างน้อยดังนี้

๓.๑ เป้าหมายและวัตถุประสงค์

๓.๒ กลยุทธ์ในการบริหารจัดการความเสี่ยงจากการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๓.๓ ระดับความเสี่ยงที่ยอมรับได้

๓.๔ การระบุภัยคุกคาม ความเสี่ยง และช่องโหว่ที่เกี่ยวข้อง

๓.๕ ความพร้อมและความสามารถของบุคลากรที่เหมาะสมกับการบริหารจัดการความเสี่ยง

๓.๖ มาตรการในการควบคุมและจัดการภัยคุกคาม ความเสี่ยง และช่องโหว่

๓.๗ การสร้างความตระหนักให้กับบุคลากรที่เกี่ยวข้อง

๓.๘ การบริหารจัดการ การตรวจสอบ และการรายงานเหตุการณ์ที่เกี่ยวข้องกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๓.๙ การกำหนดโครงสร้าง บทบาท หน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องในการดำเนินการตามแผน

ข้อ ๔ ผู้รับใบอนุญาตต้องมีการทบทวนแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยคำนึงถึงความเหมาะสมของมาตรการที่มีอยู่ในปัจจุบันและความเสี่ยงหรือสภาพแวดล้อมการให้บริการที่เปลี่ยนแปลงไป

ข้อ ๕ ผู้รับใบอนุญาตต้องมีการบริหารจัดการบุคลากรอย่างเหมาะสม โดยต้องมีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

๕.๑ จัดให้มีบุคลากรที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและควบคุมการทุจริตหรือฉ้อโกงซึ่งมีคุณสมบัติเหมาะสม โดยมีกระบวนการคัดเลือกบุคคลที่มีความรู้หรือประสบการณ์ที่เหมาะสม และมีปริมาณบุคลากรที่เพียงพอสอดคล้องกับลักษณะการประกอบธุรกิจ

๕.๒ มีการส่งเสริมและสร้างความตระหนักให้กับบุคลากรที่เกี่ยวข้อง ให้มีความเข้าใจและตระหนักถึงความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

๕.๓ จัดให้มีคู่มือหรือขั้นตอนการปฏิบัติงานสำหรับบุคลากรที่เกี่ยวข้อง ในการป้องกัน การตรวจจับ การรายงานและการจัดการกับเหตุการณ์การทุจริตหรือการฉ้อโกง

๕.๔ มีการอบรมให้ความรู้ที่จำเป็นแก่บุคลากรในองค์กรเกี่ยวกับการป้องกันและควบคุม การทุจริตหรือการฉ้อโกงทั้งก่อนการเริ่มปฏิบัติงานและอย่างน้อยปีละหนึ่งครั้ง

ข้อ ๖ ผู้รับใบอนุญาตต้องจัดให้มีคำแนะนำแก่ผู้ใช้บริการอย่างน้อยในเรื่องดังต่อไปนี้

๖.๑ การดูแลอัตลักษณ์และข้อมูลคุณลักษณะของตน เพื่อป้องกันการทุจริตหรือการฉ้อโกงที่อาจเกิดขึ้นจากการใช้งานระบบ

๖.๒ คำแนะนำแก่ผู้ใช้บริการเพื่อหลีกเลี่ยงการหลอกลวงทางอินเทอร์เน็ตอันทำให้ได้ไปซึ่งข้อมูลเกี่ยวกับอัตลักษณ์

ข้อ ๗ ผู้รับใบอนุญาตต้องมีกลไกในการตรวจจับและเฝ้าระวังเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบอย่างน้อยดังนี้

๗.๑ มีกลไกในการตรวจจับเหตุการณ์การทุจริตหรือการฉ้อโกงหรือเหตุที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง รวมถึงจัดให้มีช่องทางที่เป็นการรักษาความลับสำหรับบุคลากรและผู้ใช้งานในการแจ้งเหตุดังกล่าว

๗.๒ ต้องจัดให้มีกลไกในการเฝ้าระวังเหตุการณ์ที่มีลักษณะคล้ายกับเหตุการณ์ที่ตรวจพบ หรือที่เกี่ยวข้องกับเหตุการณ์ที่ตรวจพบ และนำมาตรวจสอบกับการลงทะเบียนใหม่และการปรับปรุงข้อมูลของผู้ใช้งานเดิม โดยระบบจะต้องไม่อนุญาตให้มีการลงทะเบียนใหม่หรือมีการปรับปรุงข้อมูลหากพบว่าการลงทะเบียนหรือการปรับปรุงข้อมูลมีลักษณะสุ่มเสี่ยงจะก่อให้เกิดเหตุการณ์ทุจริตหรือฉ้อโกง

ข้อ ๘ ผู้รับใบอนุญาตต้องจัดให้มีกลไกในการจัดการเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกงอย่างเหมาะสมและทันท่วงที โดยมีกระบวนการอย่างน้อยดังนี้

๘.๑ มีกลไกในการตรวจสอบเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

๘.๒ ในกรณีที่เกิดเหตุการณ์การทุจริตหรือการฉ้อโกง ต้องมีการบรรเทาผลกระทบจากเหตุการณ์ดังกล่าวอย่างเหมาะสม และพิจารณาจัดการความเสี่ยงที่อาจทำให้เกิดเหตุการณ์ในลักษณะเดียวกันเพื่อไม่ให้เกิดซ้ำ

๘.๓ มีขั้นตอนการปฏิบัติงานที่กำหนดหลักเกณฑ์การตัดสินใจในช่วงที่สำคัญ (critical stage) เพื่อจัดการเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

๘.๔ มีการบันทึกการตัดสินใจเกี่ยวกับการตอบสนอง การดำเนินการ หรือกรณีที่ไม่มีการดำเนินการกับเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

๘.๕ ต้องมีการรายงานเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุที่น่าจะสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี ซึ่งควรประกอบด้วยข้อมูลอย่างน้อย ดังนี้

๘.๕.๑ จำนวนเหตุการณ์

๘.๕.๒ ประเภทและระดับความรุนแรงของเหตุการณ์

๘.๕.๓ การตัดสินใจเกี่ยวกับการตอบสนอง การดำเนินการ หรือกรณีที่ไม่มีการดำเนินการกับเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง

๘.๕.๔ การให้ความช่วยเหลือเยียวยาแก่ผู้ที่ได้รับผลกระทบหรืออาจได้รับผลกระทบจากการทุจริตหรือการฉ้อโกง

ข้อ ๙ ในกรณีที่เกิดหรือคาดว่าจะเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญที่เกี่ยวกับการทุจริตหรือการฉ้อโกงในระบบให้บริการและเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารระดับสูง คณะกรรมการหรือบุคลากรที่ได้รับมอบหมาย ให้ผู้รับใบอนุญาตรายงานมายังสำนักงานเมื่อเกิดหรือรับทราบปัญหาหรือเหตุการณ์ดังกล่าวโดยเร็ว และให้แจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง

ข้อ ๑๐ ผู้รับใบอนุญาตต้องจัดให้มีมาตรการ ช่องทาง และการให้ความช่วยเหลือ เยียวยาแก่ผู้ที่ได้รับผลกระทบหรืออาจได้รับผลกระทบจากการทุจริตหรือการฉ้อโกง อย่างน้อยดังนี้

๑๐.๑ มีช่องทางในการแจ้งเหตุในกรณีที่มีข้อสงสัยว่าอัตลักษณ์ หรือสิ่งที่ใช้ยืนยันตัวตน ของผู้ใช้บริการถูกนำไปใช้งานโดยไม่ชอบ

๑๐.๒ ให้ความช่วยเหลือผู้ใช้บริการในกรณีที่อัตลักษณ์ หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการรั่วไหล หรือถูกล่วงรู้โดยบุคคลอื่น

๑๐.๓ มีมาตรการป้องกันการใช้งานอัตลักษณ์ และ/หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ เมื่อผู้รับใบอนุญาตมีเหตุสงสัยว่าอาจเกิดการทุจริตหรือการฉ้อโกง

๑๐.๔ ในกรณีที่ผู้รับใบอนุญาตตรวจพบหรือผู้เสียหายแจ้งต่อผู้รับใบอนุญาต ว่าบุคคลดังกล่าวเป็นเหยื่อของการทุจริตหรือการฉ้อโกง ผู้รับใบอนุญาตต้องจัดให้มีการพิสูจน์ตัวตนของบุคคลนั้นใหม่โดยอย่างน้อยต้องใช้ระดับความน่าเชื่อถือในการพิสูจน์ตัวตนที่เทียบเท่าหรือสูงกว่ากระบวนการที่เคยทำไว้

ข้อ ๑๑ ในกรณีที่เกิดเหตุการณ์ซึ่งส่งผลกระทบหรือขัดขวางความสามารถของผู้รับใบอนุญาตในการปฏิบัติตามหลักเกณฑ์ที่กำหนด ผู้รับใบอนุญาตต้องพิจารณาดำเนินการดังต่อไปนี้

๑๑.๑ แจ้งให้สำนักงานทราบถึงเหตุการณ์ซึ่งส่งผลให้ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดโดยเร็ว

๑๑.๒ บันทึกการตัดสินใจเกี่ยวกับการบริหารจัดการการทุจริตหรือฉ้อโกงจากการใช้งานระบบ และการแก้ไขหรือเยียวยา (ถ้ามี) โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี

๑๑.๓ ผู้รับใบอนุญาตอาจเปลี่ยนแปลงการบริหารจัดการการทุจริตหรือฉ้อโกงจากการใช้งานระบบได้ภายในระยะเวลาจำกัดเพื่อรับมือเหตุการณ์ที่เกิดขึ้น ทั้งนี้ การเปลี่ยนแปลงดังกล่าวต้องไม่ทำให้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศสูงกว่าระดับความเสี่ยงที่ยอมรับได้

**ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. ๑/๒๕๖๖**
**ฉบับที่ ๕**
**หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ**
---

## หมวด ๑
## การออกแบบการใช้งานระบบการให้บริการ

**ส่วนที่ ๑ ความสามารถในการใช้งานระบบการให้บริการ (usability requirement)**

ข้อ ๑ ผู้รับใบอนุญาตต้องพิจารณาออกแบบระบบการให้บริการโดยคำนึงถึงเรื่องดังต่อไปนี้

๑.๑ การแสดงผลในรูปแบบที่ชัดเจน ด้วยภาษาที่กระชับ เข้าใจได้ง่าย และสามารถเข้าถึงได้ด้วยอุปกรณ์ต่างๆ

๑.๒ ต้องจัดให้มีช่องทางที่ผู้ใช้บริการสามารถเลือกใช้งานได้ โดยออกแบบให้เข้าใจได้ง่ายและไม่เกิดการทำซ้ำโดยไม่จำเป็น

๑.๓ ต้องออกแบบการใช้งานให้ง่ายและเหมาะสม โดยเฉพาะผู้ใช้งานที่ขาดทักษะหรือไม่คุ้นเคยกับการใช้งานเทคโนโลยีดิจิทัล

๑.๔ ต้องออกแบบส่วนต่อประสานกับผู้ใช้งาน (user interface) ให้แสดงผลอย่างเหมาะสมบนอุปกรณ์ของผู้ใช้งาน เช่น อุปกรณ์เคลื่อนที่ แท็บเล็ต คอมพิวเตอร์ตั้งโต๊ะ แล็ปท็อป รวมถึงการแสดงผลผ่านเบราว์เซอร์ทั่วไป หรือซอฟต์แวร์สนับสนุนที่เกี่ยวข้อง

ข้อ ๒ ผู้รับใบอนุญาตต้องจัดให้มีช่องทางสำหรับการรับฟังความคิดเห็น การให้ความช่วยเหลือ การแก้ปัญหาและการรับข้อร้องเรียนที่เกี่ยวข้องกับการให้บริการ

ข้อ ๓ ผู้รับใบอนุญาตต้องจัดทำผังขั้นตอนการทำงานของระบบให้บริการซึ่งครอบคลุมกรณีดังต่อไปนี้

๓.๑ กระบวนการใช้งานของผู้ใช้บริการตั้งแต่ต้นจนจบ ซึ่งมีการปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

๓.๒ ผังขั้นตอนที่มีทางเลือกการใช้งานในกรณีที่ผู้ใช้บริการไม่สามารถทำกิจกรรมได้เนื่องจากเทคโนโลยีของอุปกรณ์หรือซอฟต์แวร์ของผู้ใช้บริการไม่รองรับกับระบบการให้บริการ

**ส่วนที่ ๒ การออกแบบส่วนต่อประสานและการสร้างประสบการณ์ที่ดีแก่ผู้ใช้บริการในขั้นตอนการพิสูจน์ตัวตน (requirements for the identity verification journey)**

ข้อ ๔ ผู้รับใบอนุญาตต้องให้ข้อมูลที่จำเป็นแก่ผู้ใช้บริการอย่างน้อย ดังนี้

๔.๑ รายละเอียดกระบวนการที่ผู้ใช้บริการต้องดำเนินการในแต่ละขั้นตอน

๔.๒ ข้อกำหนดทางเทคนิค (technical requirement) ที่จำเป็นสำหรับการใช้งานระบบการให้บริการ เช่น การตั้งค่าการเชื่อมต่ออินเทอร์เน็ต การตั้งค่าอุปกรณ์สำหรับการถ่ายภาพ

๔.๓ รายการเอกสารหรือหลักฐานที่จำเป็นในขั้นตอนการพิสูจน์ตัวตนและข้อมูลแจ้งเตือนหากผู้ใช้บริการนำส่งเอกสารไม่ครบถ้วน

ข้อ ๕ หากมีการออกรหัสหรือชุดตัวเลขให้กับผู้ใช้บริการในขั้นตอนการพิสูจน์ตัวตน ผู้รับใบอนุญาตต้องจัดให้มีการแจ้งให้ทราบล่วงหน้าเกี่ยวกับการได้รับรหัสหรือชุดตัวเลขพร้อมวิธีการดำเนินการในขั้นตอนถัดไป

ข้อ ๖ ผู้รับใบอนุญาตต้องแจ้งให้ผู้ใช้บริการทราบถึงสถานะของผลการพิสูจน์ตัวตนในแต่ละกรณี ดังนี้

๖.๑ กรณีดำเนินการพิสูจน์ตัวตนสำเร็จต้องยืนยันผลการพิสูจน์ตัวตนให้ผู้ใช้บริการทราบพร้อมรายละเอียดการดำเนินการในขั้นตอนถัดไป

๖.๒ กรณีพิสูจน์ตัวตนสำเร็จบางส่วน (partially complete) เช่น เอกสารหรือข้อมูลไม่ครบถ้วน ผู้ใช้บริการหยุดการดำเนินการ หรือ session timeout ผู้รับใบอนุญาตต้องมีกระบวนการสื่อสารให้ผู้ใช้บริการทราบถึงข้อมูลที่ดำเนินการไม่สำเร็จ

๖.๓ กรณีพิสูจน์ตัวตนไม่สำเร็จ (unsuccessful) ผู้รับใบอนุญาตต้องให้ข้อมูลช่องทางอื่นที่สามารถดำเนินการแทนได้ เช่น การพิสูจน์ตัวตนที่สำนักงานสาขา

ข้อ ๗ ผู้รับใบอนุญาตต้องจัดให้มีบริการให้ความช่วยเหลือแก่ผู้ใช้บริการในกระบวนการพิสูจน์ตัวตน ซึ่งรวมถึงกรณีที่ผู้ใช้บริการไม่มีความพร้อมด้านเทคโนโลยีหรือความสามารถในการดำเนินการ โดยอย่างน้อยต้องมีช่องทางที่สามารถติดต่อสื่อสารกับบุคลากรของผู้รับใบอนุญาตได้ เช่น เคาน์เตอร์เซอร์วิส call center หรือ VDO call

ข้อ ๘ ผู้รับใบอนุญาตต้องจัดให้มีคู่มือหรือคำแนะนำสำหรับผู้ใช้บริการในการแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลของตนที่มีการเก็บรวบรวมในขั้นตอนการพิสูจน์ตัวตน

**ส่วนที่ ๓ การออกแบบส่วนต่อประสานและการสร้างประสบการณ์ที่ดีแก่ผู้ใช้บริการในขั้นตอนการยืนยันตัวตน (requirements for the authentication journey)**

ข้อ ๙ ผู้รับใบอนุญาตต้องจัดให้มีคำแนะนำการใช้งานและดูแลรักษาสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ เช่น ระยะเวลาการใช้งานสิ่งที่ใช้ยืนยันตัวตน การดำเนินการเมื่อสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย หรือเสียหาย

ข้อ ๑๐ ผู้รับใบอนุญาตต้องจัดให้มีช่องทางสำหรับผู้ใช้บริการในการกู้คืน เปลี่ยนแปลง หรือจัดให้มีสิ่งทดแทนสิ่งที่ใช้ยืนยันตัวตน ในกรณีที่สิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย เสียหาย ไม่สามารถใช้งาน หรือลืม โดยช่องทางดังกล่าวอย่างน้อยต้องเป็นกระบวนการที่มีระดับความน่าเชื่อถือเทียบเท่ากับกระบวนการออกสิ่งที่ใช้ยืนยันตัวตนที่เคยทำไว้

**ส่วนที่ ๔ การทดสอบความสามารถของระบบ**

ข้อ ๑๑ ผู้รับใบอนุญาตต้องจัดทำแผนและรายละเอียดการทดสอบระบบ (usability test plans) ซึ่งครอบคลุมตามขอบเขตการให้บริการ โดยอย่างน้อยต้องประกอบด้วย

๑๑.๑ วัตถุประสงค์ เป้าหมาย

๑๑.๒ วิธีการวัดผลหรือเกณฑ์การทดสอบซึ่งครอบคลุมหัวข้อดังนี้

๑๑.๒.๑ ระบบการให้บริการแสดงผลในรูปแบบที่ชัดเจน ด้วยภาษาที่กระชับ เข้าใจได้ง่าย และสามารถเข้าถึงได้ด้วยอุปกรณ์ต่างๆ

๑๑.๒.๒ ระบบการให้บริการใช้งานง่ายและเหมาะสม โดยเฉพาะผู้ใช้งานที่ขาดทักษะหรือไม่คุ้นเคยกับการใช้งานเทคโนโลยีดิจิทัล

๑๑.๒.๓ ส่วนต่อประสานกับผู้ใช้งาน (user interface) ของระบบการให้บริการแสดงผลอย่างเหมาะสม (responsive design) บนอุปกรณ์ของผู้ใช้งาน

๑๑.๓ จำนวน วิธีการคัดเลือก และการจัดกลุ่มผู้เข้าร่วมการทดสอบตามขอบเขตการให้บริการ เช่น ผู้ใช้งานทั่วไป ผู้พิการ ผู้สูงอายุ ผู้ที่ใช้เทคโนโลยีอำนวยความสะดวก ผู้ที่ขาดความเข้าใจในการใช้งาน ผู้ที่มีความหลากหลายทางวัฒนธรรมและภาษา ผู้ที่มาจากภูมิภาคและพื้นที่ห่างไกล ผู้ที่มีเทคโนโลยีรุ่นเก่าและการเชื่อมต่อแบนด์วิดท์ต่ำ

๑๑.๔ แนวทางและวิธีการที่ใช้ในการทดสอบซึ่งแสดงถึงกระบวนการทำงาน ปัญหา และสิ่งที่ต้องปรับปรุง

๑๑.๕ รูปแบบการทดสอบ บนอุปกรณ์ต่างๆ ทั้งในรูปแบบอุปกรณ์ตั้งโต๊ะและอุปกรณ์เคลื่อนที่

๑๑.๖ ผลลัพธ์ของการทดสอบและแนวทางการพัฒนาหรือปรับปรุงระบบการให้บริการ

ข้อ ๑๒ ในการทดสอบความสามารถของระบบ ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อย ดังนี้

๑๒.๑ ต้องทำการทดสอบความสามารถในการใช้งานของระบบที่ครอบคลุมขั้นตอนตั้งแต่ต้นจนจบกระบวนการในสภาพแวดล้อมที่ใกล้เคียงกับการให้บริการจริง ตามกลุ่มของผู้เข้าร่วมการทดสอบ

๑๒.๒ ต้องบันทึกผลลัพธ์ของการทดสอบการใช้งานระบบ รวมถึงวิธีการทดสอบ ผลการทดสอบ ข้อสังเกต และข้อเสนอแนะจากการทดสอบ

ข้อ ๑๓ ผู้รับใบอนุญาตต้องจัดทำรายงานผลการทดสอบความสามารถของระบบ ซึ่งประกอบด้วย

๑๓.๑ แผนและรายละเอียดการทดสอบ

๑๓.๒ บันทึกผลลัพธ์ของการทดสอบ

ข้อ ๑๔ รายงานผลการทดสอบความสามารถของระบบเป็นส่วนหนึ่งของรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจที่ต้องนำส่งต่อสำนักงาน

## หมวด ๒
## การทดสอบด้านเทคนิคของระบบและซอฟต์แวร์ที่เกี่ยวข้อง
## (technical testing requirement)

ข้อ ๑๕ ผู้รับใบอนุญาตต้องจัดให้มีแผนการทดสอบและดำเนินการทดสอบด้านเทคนิคของระบบและซอฟต์แวร์ที่ครอบคลุมระบบการให้บริการ

ข้อ ๑๖ ในการทดสอบทางเทคนิคต้องแสดงให้เห็นความสอดคล้องกับข้อกำหนดในเรื่องต่อไปนี้

๑๖.๑ การจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์

๑๖.๒ กลไกในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์

๑๖.๓ กลไกในการตรวจจับเฝ้าระวังและจัดการเหตุการณ์การทุจริตหรือฉ้อโกงจากการใช้งานระบบ

๑๖.๔ วิธีการพิสูจน์ตัวตนและระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

๑๖.๕ การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน

๑๖.๖ วิธีการยืนยันตัวตน และระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

๑๖.๗ การทดสอบความสอดคล้องของโพรโทคอลที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการ

ข้อ ๑๗ ผู้รับใบอนุญาตต้องจัดให้มีการทำตารางเปรียบเทียบความสามารถของระบบกับการทดสอบ (requirement traceability matrix) ที่เชื่อมโยงความสอดคล้องของกรณีที่ใช้ในการทดสอบ (test case) กับข้อกำหนดที่ต้องดำเนินการ

ข้อ ๑๘ ก่อนเริ่มการทดสอบผู้รับใบอนุญาตต้องดำเนินการอย่างน้อย ดังนี้

๑๘.๑ ระบุข้อกำหนดที่ใช้ในแผนการทดสอบทางเทคนิค

๑๘.๒ ข้อกำหนดทุกข้อในแผนการทดสอบทางเทคนิคต้องมีการทดสอบอย่างน้อยหนึ่งกรณี

๑๘.๓ ต้องมีเอกสารการบันทึกกรณีที่ใช้ในการทดสอบและระบุทรัพยากรที่ใช้ในการทดสอบ

ข้อ ๑๙ ผู้รับใบอนุญาตต้องจัดทำรายงานผลการทดสอบทางเทคนิค (technical test report) โดยประกอบด้วยข้อมูลดังต่อไปนี้

๑๙.๑ การทดสอบที่ได้ดำเนินการตามแผนการทดสอบทางเทคนิค

๑๙.๒ เกณฑ์การทดสอบ

๑๙.๓ สถานะการทดสอบของแต่ละกรณีที่ใช้ในการทดสอบรวมถึงความครอบคลุมของการทดสอบและข้อบกพร่องที่เกิดขึ้น

๑๙.๔ ผลของการทดสอบที่ครบถ้วนตามเกณฑ์การทดสอบ

๑๙.๕ ถ้าผลการทดสอบไม่ครบถ้วนตามเกณฑ์การทดสอบจะต้องมีการประเมินความเสี่ยงในข้อกำหนดที่ไม่สามารถดำเนินการได้โดยครบถ้วนพร้อมเหตุผลในการพิจารณายอมรับผลการทดสอบดังกล่าว

ข้อ ๒๐ รายงานผลการทดสอบทางเทคนิคถือเป็นส่วนหนึ่งของรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจที่ต้องนำส่งต่อสำนักงาน

## หมวด ๓
## การตรวจประเมินระบบการให้บริการ

ข้อ ๒๑ ภายหลังจากเริ่มประกอบธุรกิจ ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินและจัดทำรายงานผลการตรวจประเมินระบบการให้บริการและรายงานต่อสำนักงานตามหลักเกณฑ์และระยะเวลาที่สำนักงานกำหนด

ข้อ ๒๒ ในการตรวจประเมินระบบการให้บริการผู้รับใบอนุญาตต้องแสดงให้เห็นได้ว่า

๒๒.๑ การตรวจประเมินได้ดำเนินการโดยผู้ตรวจสอบที่เป็นอิสระ ซึ่งมีความรู้ ความสามารถ และประสบการณ์ที่เหมาะสมในการดำเนินการ

๒๒.๒ ในกรณีที่เป็นการตรวจประเมินด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบต้องผ่านการรับรองและมีวุฒิบัตรหรือได้รับประกาศนียบัตรด้านความมั่นคงปลอดภัยระดับสากลอย่างหนึ่งอย่างใดดังต่อไปนี้

๒๒.๒.๑ certified information system auditor (CISA)

๒๒.๒.๒ certified information security manager (CISM)

๒๒.๒.๓ certified information system security professional (CISSP)

๒๒.๒.๔ ISO/IEC 27001 lead auditor

๒๒.๒.๕ ใบรับรองอื่นตามที่ประกาศกำหนดเพิ่มเติม

๒๒.๓ ผู้ตรวจสอบไม่มีความเกี่ยวข้องกับการพัฒนาหรือการดำเนินงานเกี่ยวกับระบบให้บริการที่ทำการตรวจประเมิน

๒๒.๔ ผู้ตรวจสอบไม่มีส่วนได้เสียกับการตรวจประเมินระบบให้บริการที่ทำการตรวจประเมิน

ข้อ ๒๓ รายงานผลการตรวจประเมินระบบการให้บริการต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

๒๓.๑ วัตถุประสงค์และขอบเขตของการตรวจประเมิน

๒๓.๒ หลักเกณฑ์ที่นำมาใช้ในการตรวจประเมิน

๒๓.๓ วันเวลาในการตรวจประเมิน

๒๓.๔ ชื่อ ตำแหน่ง และข้อมูลการติดต่อผู้รับผิดชอบการตรวจประเมินของผู้รับใบอนุญาต

๒๓.๕ รายชื่อและคุณสมบัติของผู้ตรวจสอบ

๒๓.๖ สถานที่ที่ทำการตรวจประเมิน รวมถึงศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรอง และที่ตั้งอื่นๆ ที่ใช้ในการควบคุมระบบการให้บริการ

๒๓.๗ รายการข้อมูล เอกสาร หลักฐาน หรือบุคคลผู้ให้ข้อมูลประกอบการตรวจประเมิน

๒๓.๘ วิธีการที่ใช้ในการตรวจประเมิน

๒๓.๙ ผลการทดสอบหรือผลการตรวจประเมิน

๒๓.๑๐ ข้อตรวจพบซึ่งรวมถึงรายการความสอดคล้องและไม่สอดคล้องตามหลักเกณฑ์ที่นำมาใช้ในการตรวจประเมิน

๒๓.๑๑ การดำเนินการและการแก้ไขตามข้อตรวจพบ

๒๓.๑๒ ความเห็น ข้อสังเกต หรือข้อเสนอแนะของผู้ตรวจสอบ

ข้อ ๒๔ ผู้รับใบอนุญาตต้องจัดให้มีการรายงานผลการตรวจประเมินระบบการให้บริการ พร้อมทั้งรายงานข้อตรวจพบและผลการปรับปรุงแก้ไขให้ผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับทราบตามรอบการประเมินและตามรอบการติดตามการปรับปรุงแก้ไขข้อตรวจพบหรือโดยไม่ชักช้าเมื่อพบข้อบกพร่องที่มีนัยสำคัญ

ข้อ ๒๕ กรณีที่มีการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อระบบการให้บริการภายหลังจากเริ่มประกอบธุรกิจ ผู้รับใบอนุญาตต้องดำเนินการตรวจประเมินระบบในส่วนที่ได้รับผลกระทบจากการเปลี่ยนแปลงดังกล่าวและนำส่งรายงานผลการตรวจประเมินพร้อมการแจ้งการเปลี่ยนแปลงต่อสำนักงาน

ข้อ ๒๖ ผู้รับใบอนุญาตต้องนำส่งรายงานผลการตรวจประเมินระบบการให้บริการต่อสำนักงานตามระยะเวลาที่สำนักงานประกาศกำหนด และสำนักงานอาจร้องขอข้อมูล เอกสาร หรือหลักฐานเพิ่มเติมเพื่อประกอบการตรวจรายงานผลการตรวจประเมินระบบการให้บริการได้

ข้อ ๒๗ ในกรณีที่สำนักงานเห็นว่ารายงานผลการตรวจประเมินระบบการให้บริการไม่ครอบคลุมประเด็นสำคัญที่อาจส่งผลกระทบต่อความน่าเชื่อถือและความเสี่ยงของระบบการให้บริการ สำนักงานอาจดำเนินการตรวจประเมินเพิ่มเติมได้

ข้อ ๒๘ ในกรณีที่ผู้รับใบอนุญาตประสงค์จะเลิกประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลต้องจัดให้มีการประเมินผลกระทบและแผนรองรับการเลิกประกอบธุรกิจตามที่คณะกรรมการประกาศกำหนด

## หมวด ๔
## ข้อตกลงการให้บริการ

ข้อ ๒๙ ผู้รับใบอนุญาตต้องจัดให้มีข้อตกลงในการให้บริการเกี่ยวกับระบบการให้บริการที่มีความชัดเจนและเป็นปัจจุบัน โดยเปิดเผยให้ผู้ใช้บริการได้รับทราบและยอมรับข้อตกลงดังกล่าวก่อนเริ่มใช้บริการ

ข้อ ๓๐ ข้อตกลงในการให้บริการต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

๓๐.๑ รายละเอียดเกี่ยวกับลักษณะของการให้บริการ

๓๐.๒ หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการให้บริการ

๓๐.๓ สิทธิ หน้าที่และความรับผิดของผู้ใช้บริการ

๓๐.๓.๑ สิทธิในการเข้าถึงและใช้งานระบบ

๓๐.๓.๒ หน้าที่ที่เกี่ยวข้องกับการใช้งาน เช่น การแสดงหรือนำส่งเอกสารหรือหลักฐานตามที่กำหนด การปฏิบัติตามคู่มือผู้ใช้งาน

๓๐.๓.๓ หน้าที่ในการให้ข้อมูลเกี่ยวกับอัตลักษณ์และหลักฐานแสดงตนที่ถูกต้อง

๓๐.๓.๔ หน้าที่ในการแจ้งให้ผู้รับใบอนุญาตทราบโดยเร็วเมื่อทราบว่ามีการใช้งานอัตลักษณ์หรือสิ่งที่ใช้ยืนยันตัวตนโดยไม่ได้รับอนุญาต

๓๐.๔ สิทธิ หน้าที่ และความรับผิดของผู้รับใบอนุญาต

๓๐.๔.๑ กรณีที่อาจมีการระงับ ยกเลิก หรือเพิกถอนสิทธิในการเข้าถึงและใช้งานโดยผู้รับใบอนุญาต

๓๐.๔.๒ การเปลี่ยนแปลงข้อตกลงการให้บริการ

๓๐.๔.๓ การบริหารจัดการข้อมูลเกี่ยวกับอัตลักษณ์ ข้อมูลส่วนบุคคล หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ เช่น การไม่เปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการต่อบุคคลภายนอก เว้นแต่ได้รับความยินยอมจากผู้ใช้บริการ

๓๐.๔.๔ ความรับผิดและข้อจำกัดความรับผิดของผู้รับใบอนุญาต (ถ้ามี)

๓๐.๕ ช่องทางการติดต่อกับผู้รับใบอนุญาต

๓๐.๖ กระบวนการในการระงับข้อพิพาท การแก้ไขปัญหาหรือการจัดการเรื่องร้องเรียน

๓๐.๗ การชดใช้หรือเยียวยาความเสียหายของผู้รับใบอนุญาต

ข้อ ๓๑ ผู้รับใบอนุญาตต้องแจ้งให้ผู้ใช้บริการทราบถึงการใช้บริการในส่วนที่ผู้ใช้บริการต้องดำเนินการกับบุคคลภายนอก

ข้อ ๓๒ ผู้รับใบอนุญาตต้องเปิดเผยรายละเอียดของค่าธรรมเนียมที่เรียกเก็บจากผู้ใช้บริการระบบ โดยวิธีการที่ทำให้ผู้ใช้บริการสามารถทราบได้อย่างชัดเจน ทั้งนี้ กรณีที่มีการเปลี่ยนแปลงค่าธรรมเนียม ผู้รับใบอนุญาตจะต้องแจ้งให้ผู้ใช้บริการทราบรายละเอียดการเปลี่ยนแปลงดังกล่าวด้วย

**ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. ๑/๒๕๖๖**
**ฉบับที่ ๖**
**หลักเกณฑ์ตามลักษณะของการให้บริการ**
---

**หมวด ๑**
**บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการยืนยันตัวตน**

**ส่วนที่ ๑ การพิสูจน์ตัวตน**

ข้อ ๑ ผู้รับใบอนุญาตต้องบริหารจัดการกระบวนการพิสูจน์ตัวตนให้สอดคล้องตามลักษณะและระดับความเสี่ยงของธุรกรรมหรือการประกอบธุรกิจ

ข้อ ๒ ในการให้บริการพิสูจน์ตัวตนผู้รับใบอนุญาตต้องมีกระบวนการที่ครอบคลุมการทำงานอย่างน้อยในเรื่องดังต่อไปนี้

๒.๑ ต้องจัดให้ผู้ใช้บริการสามารถปรับปรุงข้อมูลเกี่ยวกับอัตลักษณ์ของตนซึ่งถูกจัดเก็บในกระบวนการพิสูจน์ตัวตนได้ โดยต้องจัดให้มีกระบวนการตรวจสอบที่เกี่ยวข้องอย่างน้อยดังนี้

๒.๑.๑ ตรวจสอบข้อมูลที่ขอปรับปรุงก่อนที่จะบันทึกการเปลี่ยนแปลงข้อมูลในระบบการให้บริการ รวมถึงกรณีที่มีการเปลี่ยนแปลงสถานะของอัตลักษณ์ดิจิทัลนั้น เช่น การระงับชั่วคราว การใช้งานใหม่

๒.๑.๒ ในกรณีที่ตรวจพบการทำธุรกรรมที่ผิดปกติต้องมีการตรวจสอบว่าอัตลักษณ์ดิจิทัลนั้นยังอยู่ภายใต้ความควบคุมของเจ้าของอัตลักษณ์ดิจิทัลที่แท้จริง

๒.๒ ในกรณีที่ผู้ใช้บริการร้องขอให้ระงับการใช้งานชั่วคราว หรือยุติการใช้งานอัตลักษณ์ดิจิทัล ผู้รับใบอนุญาตต้องจัดให้มีกระบวนการอย่างน้อยดังนี้

๒.๒.๑ มีการตรวจสอบความถูกต้องของคำขอก่อนที่จะดำเนินการตามคำขอ

๒.๒.๒ ป้องกันไม่ให้มีการใช้งานอัตลักษณ์ดิจิทัลตามคำขอ

๒.๒.๓ มีการแจ้งให้ผู้ใช้บริการทราบว่าไม่สามารถใช้งานอัตลักษณ์ดิจิทัลได้ พร้อมระบุเหตุผล เช่น ระงับการใช้งานชั่วคราว ยุติการใช้งาน

ข้อ ๓ กรณีที่ระบบการให้บริการรองรับการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อยดังนี้

๓.๑ ต้องดำเนินการให้สอดคล้องตามข้อกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตนที่สูงกว่าให้ครบถ้วน

๓.๒ ต้องจัดให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้นก่อนเริ่มกระบวนการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตน

๓.๓ เมื่อดำเนินการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตนเสร็จสิ้น ต้องส่งการแจ้งเตือนผู้ใช้บริการทราบผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้ยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตนดังกล่าว เช่น การส่งให้ทางอีเมลของผู้ใช้บริการ

ข้อ ๔ ผู้รับใบอนุญาตต้องจัดให้มีมาตรการดูแลข้อมูลผู้ใช้บริการอย่างน้อยดังนี้

๔.๑ ต้องรวบรวมหรือจัดเก็บข้อมูลเพื่อการพิสูจน์ตัวตนเพียงเท่าที่จำเป็น เหมาะสม และตรงตามวัตถุประสงค์ของการให้บริการ

๔.๒ ต้องจำกัดการเปิดเผยข้อมูลอัตลักษณ์ของผู้ใช้บริการต่อบุคคลอื่นเพื่อใช้ในการพิสูจน์ตัวตนตามที่ได้รับความยินยอมจากผู้ใช้บริการ เว้นแต่เป็นกรณีที่ผู้รับใบอนุญาตต้องปฏิบัติตามที่กฎหมายกำหนด

**ส่วนที่ ๒ การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และการยืนยันตัวตน**

ข้อ ๕ ผู้รับใบอนุญาตต้องบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนและกระบวนการยืนยันตัวตนให้สอดคล้องตามลักษณะและระดับความเสี่ยงของธุรกรรมหรือการประกอบธุรกิจ

ข้อ ๖ การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนให้พิจารณาตามข้อกำหนดของการยืนยันตัวตนภายใต้มาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัลซึ่งครอบคลุมกระบวนการอย่างน้อยดังนี้

๖.๑ การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน

๖.๒ การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน

๖.๓ การหมดอายุและการออกใหม่

๖.๔ การเพิกถอน หรือยุติการใช้งาน

ข้อ ๗ ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดเกี่ยวกับสิ่งที่ใช้ยืนยันตัวตนให้พิจารณาตามข้อกำหนดของการยืนยันตัวตนภายใต้มาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัลซึ่งครอบคลุมหัวข้ออย่างน้อยดังนี้

๗.๑ ชนิดของสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตนตามระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

๗.๒ ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน

ข้อ ๘ ก่อนดำเนินการยืนยันตัวตนผู้รับใบอนุญาตต้องตรวจสอบสิ่งที่ใช้ยืนยันตัวตนอย่างน้อยดังนี้

๘.๑ ตรวจสอบให้แน่ใจว่าสิ่งที่ใช้ยืนยันตัวตนที่แสดงนั้นถูกต้อง ใช้งานได้ และยังไม่หมดอายุหรือถูกเพิกถอน

๘.๒ ในกรณีที่ตรวจพบการทำธุรกรรมที่ผิดปกติต้องมีการตรวจสอบว่าสิ่งที่ใช้ยืนยันตัวตนนั้นยังอยู่ภายใต้ความควบคุมของเจ้าของอัตลักษณ์ดิจิทัลที่แท้จริง

ข้อ ๙ ในกรณีที่ผู้ใช้บริการร้องขอให้ระงับการใช้งานสิ่งที่ใช้ยืนยันตัวตนชั่วคราวหรือยุติการใช้งานสิ่งที่ใช้ยืนยันตัวตน ผู้รับใบอนุญาตต้องจัดให้มีกระบวนการอย่างน้อยดังนี้

๙.๑ มีการตรวจสอบความถูกต้องของคำขอก่อนที่จะดำเนินการตามคำขอ

๙.๒ มีการแจ้งให้ผู้ใช้บริการทราบว่าไม่สามารถใช้งานสิ่งที่ใช้ยืนยันตัวตนได้พร้อมระบุเหตุผล เช่น ระงับการใช้งานชั่วคราว ยุติการใช้งาน

ข้อ ๑๐ กรณีที่ระบบการให้บริการรองรับการยกระดับความน่าเชื่อถือของการยืนยันตัวตนผู้รับใบอนุญาตต้องดำเนินการอย่างน้อยดังนี้

๑๐.๑ ต้องดำเนินการให้สอดคล้องตามข้อกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตนที่สูงกว่าให้ครบถ้วน

๑๐.๒ ต้องจัดให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้นก่อนเริ่มกระบวนการยกระดับความน่าเชื่อถือของการยืนยันตัวตน

๑๐.๓ เมื่อดำเนินการยกระดับความน่าเชื่อถือของการยืนยันตัวตนเสร็จสิ้น ต้องส่งการแจ้งเตือนผู้ใช้บริการทราบผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้ยกระดับความน่าเชื่อถือของการยืนยันตัวตน เช่น การส่งให้ทางอีเมลของผู้ใช้บริการ

**ส่วนที่ ๓ การเชื่อมโยงและแลกเปลี่ยนข้อมูล**

ข้อ ๑๑ ผู้รับใบอนุญาตต้องกำหนดโพรโทคอลที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการ (communication protocol) สำหรับเชื่อมโยงคำขอและการตอบกลับ โดยต้องสามารถเชื่อมโยงคำขอไปยังปลายทางที่ระบุโดยผู้ส่งคำขอได้และสามารถเชื่อมโยงการตอบกลับไปยังคำขอต้นทางได้ ซึ่งต้องมีการแจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขความสอดคล้องของระบบการให้บริการ

ข้อ ๑๒ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายเกี่ยวกับการเปิดเผยข้อมูลอัตลักษณ์ที่สอดคล้องกับหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลและประกาศให้ผู้ที่เกี่ยวข้องได้รับทราบเป็นการทั่วไป

ข้อ ๑๓ ผู้รับใบอนุญาตต้องจัดให้มีรายการข้อมูลอัตลักษณ์ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลในระบบการให้บริการ โดยต้องมีชุดข้อมูลขั้นต่ำที่สามารถระบุตัวผู้ใช้บริการได้อย่างชัดเจนประกอบด้วย

๑๓.๑ เลขประจำตัวประชาชน

๑๓.๒ ชื่อ นามสกุล ภาษาไทย

๑๓.๓ ชื่อ นามสกุล ภาษาอังกฤษ (ถ้ามี)

๑๓.๔ วัน เดือน ปี เกิด

๑๓.๕ ที่อยู่ตามบัตรประจำตัวประชาชน

ข้อ ๑๔ ในกรณีที่ดำเนินการยืนยันตัวตนสำเร็จและมีการตอบกลับไปยังคำขอต้นทาง ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อยดังนี้

๑๔.๑ ผลการยืนยันตัวตนประกอบด้วยผลการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนและข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ

๑๔.๒ ต้องจัดให้มีการรักษาความลับของผลหรือข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนในกระบวนการดังกล่าวเพื่อให้มั่นใจว่าเฉพาะบุคคลที่เกี่ยวข้องและมีสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลได้

๑๔.๓ ต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัยเพื่อรักษาความครบถ้วนของผลหรือข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตน

ข้อ ๑๕ ห้ามมิให้ผู้รับใบอนุญาตส่งข้อมูลที่ใช้สำหรับการตรวจสอบสถานะของหลักฐานแสดงตนให้กับบุคคลอื่น โดยข้อมูลดังกล่าวได้แก่

๑๕.๑ เลขคำร้องขอมีบัตรประจำตัวประชาชน

๑๕.๒ หมายเลขชิปบัตรประจำตัวประชาชน

๑๕.๓ เลขควบคุมหลังบัตรประจำตัวประชาชน (เลเซอร์ ไอดี (laser ID))

เว้นแต่เป็นกรณีที่ผู้รับใบอนุญาตต้องปฏิบัติตามที่กฎหมายกำหนด

**ส่วนที่ ๔ การพิสูจน์และยืนยันตัวตนโดยใช้เทคโนโลยีชีวมิติ**

ข้อ ๑๖ ในกรณีที่ผู้รับใบอนุญาตมีการใช้งานข้อมูลชีวมิติในกระบวนการพิสูจน์และยืนยันตัวตนต้องมีการดำเนินการอย่างน้อยดังนี้

๑๖.๑ ต้องจัดให้มีการกำกับดูแลการใช้งานเทคโนโลยีชีวมิติตามหลักปฏิบัติดังนี้

๑๖.๑.๑ มีนโยบายและแนวปฏิบัติการนำเทคโนโลยีชีวมิติมาใช้ในระบบการให้บริการอย่างชัดเจน ซึ่งต้องคำนึงถึงการดำเนินงานที่สำคัญอย่างน้อยดังนี้

(๑) การประเมินความเสี่ยงการนำเทคโนโลยีชีวมิติมาใช้

(๒) การปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ

(๓) การรักษาความมั่นคงปลอดภัยข้อมูลชีวมิติ

๑๖.๑.๒ มีการบริหารจัดการอัตลักษณ์เพื่อการพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมิติที่สอดคล้องตามมาตรฐานการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน

๑๖.๑.๓ มีการจัดทำคู่มือหรือแนวปฏิบัติสำหรับบุคลากรที่ปฏิบัติงานเกี่ยวกับการใช้งานข้อมูลชีวมิติ

๑๖.๑.๔ มีการจัดทำคู่มือหรือการให้คำแนะนำผู้ใช้บริการในการใช้งานข้อมูลชีวมิติ

๑๖.๒ ต้องจำกัดการเข้าถึงการควบคุมข้อมูลชีวมิติให้สามารถเข้าถึงได้เฉพาะบุคลากรที่เกี่ยวข้องซึ่งผ่านการฝึกอบรมอย่างเหมาะสม และมีการสอบทานสิทธิอย่างสม่ำเสมอ

**ส่วนที่ ๕ การตรวจสอบประวัติการใช้งาน**

ข้อ ๑๗ ให้ผู้รับใบอนุญาตจัดเก็บข้อมูลประวัติการใช้งานเพื่อประโยชน์ในการสอบทานของผู้ใช้บริการ โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้ผู้ใช้บริการเรียกดูข้อมูลย้อนหลังได้เป็นระยะเวลาไม่น้อยกว่า หกเดือน โดยอย่างน้อยควรมีข้อมูลดังต่อไปนี้

๑๗.๑ ประวัติกิจกรรมของผู้ใช้บริการที่ได้ดำเนินการผ่านระบบการให้บริการของผู้รับใบอนุญาต

๑๗.๒ ประวัติการให้ความยินยอมในการเปิดเผยข้อมูลอัตลักษณ์

ข้อ ๑๘ การแสดงผลการตรวจสอบประวัติการใช้งานต้องไม่มีการแสดงข้อมูลส่วนบุคคลของผู้ใช้บริการ

## หมวด ๒
## บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล

**ส่วนที่ ๑ ข้อกำหนดทั่วไป**

ข้อ ๑๙ ผู้รับใบอนุญาตต้องจัดให้มีมาตรการดูแลข้อมูลส่วนบุคคลอย่างน้อยดังนี้

๑๙.๑ ไม่นำข้อมูลส่วนบุคคลของผู้ใช้บริการมาใช้เป็นตัวระบุ (identifier) ผู้ใช้บริการ

๑๙.๒ ไม่จัดเก็บหรือคงไว้ซึ่งข้อมูลส่วนบุคคลของผู้ใช้บริการที่มีการส่งจากผู้รับใบอนุญาตไปยังผู้อาศัยการพิสูจน์และยืนยันตัวตน เว้นแต่เป็นการจัดเก็บโดยมั่นคงปลอดภัยในระหว่างเซสชันการพิสูจน์และยืนยันตัวตน และข้อมูลดังกล่าวต้องไม่สามารถเข้าถึงได้โดยบุคลากรของผู้รับใบอนุญาต

ข้อ ๒๐ ผู้รับใบอนุญาตต้องจัดให้มีการบันทึกประวัติกิจกรรม (log) สำหรับบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลไว้เพื่อการตรวจสอบ (audit log) โดยกรณีที่เป็นคำขอเพื่อการยืนยันตัวตนต้องมีการจัดเก็บประวัติกิจกรรมของการโต้ตอบทั้งหมดที่เกี่ยวข้องกับคำขอเพื่อการยืนยันตัวตนดังกล่าว โดยใช้ตัวระบุเฉพาะของการโต้ตอบเดียวกัน (unique interaction identifier) สำหรับแต่ละเหตุการณ์

**ส่วนที่ ๒ ข้อกำหนดด้านความสอดคล้องของระบบการให้บริการ**

ข้อ ๒๑ ในการกำหนดเงื่อนไขความสอดคล้องของระบบการให้บริการเพื่อให้บุคคลอื่นสามารถเชื่อมต่อได้อย่างมีประสิทธิภาพ ผู้รับใบอนุญาตต้องแจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขความสอดคล้องของระบบการให้บริการอย่างน้อยในเรื่องดังต่อไปนี้

๒๑.๑ ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล (assurance level) ที่สามารถเชื่อมต่อกับระบบการให้บริการ

๒๑.๒ โพรโทคอล (protocol) สำหรับเชื่อมโยงคำขอ (request) และการตอบกลับ (response) ในระบบการให้บริการ

ข้อ ๒๒ ในการกำหนดความสอดคล้องของระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล ผู้รับใบอนุญาตต้องพิจารณาดำเนินการอย่างน้อยดังนี้

๒๒.๑ จัดให้มีรายชื่อและระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนของผู้รับใบอนุญาตที่เชื่อมต่อกับระบบการให้บริการของตน

๒๒.๒ จัดให้มีกลไกที่สามารถคัดแยกผู้รับใบอนุญาตที่เชื่อมต่อกับระบบการให้บริการที่มีระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล ในระดับที่สอดคล้องตามคำขอหรือสูงกว่าคำขอของผู้ส่งคำขอได้

ข้อ ๒๓ การกำหนดโพรโทคอลที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการ (communication protocol) ต้องสามารถเชื่อมโยงคำขอและการตอบกลับ โดยเชื่อมโยงคำขอไปยังปลายทางที่ระบุโดยผู้ส่งคำขอและสามารถเชื่อมโยงการตอบกลับไปยังคำขอต้นทางได้ ซึ่งต้องมีการแจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขความสอดคล้องของระบบการให้บริการ

ข้อ ๒๔ ผู้รับใบอนุญาตต้องกำหนดส่วนต่อประสานโปรแกรมประยุกต์ (application programming interface) ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนในระบบการให้บริการ (ถ้ามี) โดยอย่างน้อยต้องสามารถเชื่อมโยงรายการต่อไปนี้เข้าด้วยกันได้อย่างถูกต้องและครบถ้วน

๒๔.๑ รายการข้อมูลที่กำหนดในคำขอและการตอบกลับ

๒๔.๒ ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามที่กำหนดในคำขอและการตอบกลับ

**ส่วนที่ ๓ ข้อกำหนดด้านเทคนิค**

ข้อ ๒๕ ผู้รับใบอนุญาตต้องจัดให้มีแผนการทดสอบ (testing plan) การเชื่อมโยงและแลกเปลี่ยนข้อมูลบนระบบการให้บริการที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยของระบบการให้บริการ โดยแผนการทดสอบดังกล่าวเป็นส่วนหนึ่งของรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจ

ข้อ ๒๖ ผู้รับใบอนุญาตต้องจัดให้มีการทดสอบการใช้งานตามแผนการทดสอบร่วมกับผู้ประสงค์จะเชื่อมต่อกับระบบการให้บริการก่อนเริ่มให้บริการแก่บุคคลดังกล่าว

ข้อ ๒๗ ห้ามมิให้เปิดให้บริการแก่ผู้ประสงค์จะเชื่อมต่อกับระบบการให้บริการของผู้รับใบอนุญาตที่ไม่สามารถทดสอบการใช้งานร่วมกันกับผู้รับใบอนุญาตหรือผลการทดสอบไม่สามารถดำเนินการได้โดยสมบูรณ์

**ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. ๑/๒๕๖๖**
**ฉบับที่ ๗**
**หลักเกณฑ์การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ**
---

**ส่วนที่ ๑ การคุ้มครองผู้ใช้บริการ**

ข้อ ๑ ผู้รับใบอนุญาตต้องเปิดเผยข้อมูลที่สำคัญซึ่งเกี่ยวข้องกับการให้บริการแก่ผู้ใช้บริการอย่างเพียงพอต่อการตัดสินใจเลือกใช้บริการได้ตรงตามความต้องการ

ข้อ ๒ ผู้รับใบอนุญาตต้องจัดให้มีช่องทางในการติดต่อสื่อสารกับผู้ใช้บริการในการรับฟังความคิดเห็น การให้ความช่วยเหลือ การแก้ปัญหา และการรับข้อร้องเรียนที่เกี่ยวข้องกับการให้บริการที่ผู้ใช้บริการสามารถติดต่อได้โดยสะดวก โดยมีการควบคุมดูแลและดำเนินการภายในเวลาที่เหมาะสม

ข้อ ๓ ผู้รับใบอนุญาตต้องดูแลให้ข้อมูลที่ใช้ในการติดต่อสื่อสารมีความชัดเจน น่าเชื่อถือ และไม่ทำให้ผู้ใช้บริการสำคัญผิด

ข้อ ๔ ในกรณีที่ระบบการให้บริการของงานที่สำคัญหยุดให้บริการชั่วคราว หรือเกิดปัญหา หรือมีความบกพร่องในการให้บริการ ผู้รับใบอนุญาตต้องดำเนินการดังต่อไปนี้

๔.๑ กรณีหยุดให้บริการชั่วคราวอันเกิดจากการเตรียมการไว้ล่วงหน้า เช่น การปรับปรุงระบบงานสำคัญ

๔.๑.๑ แจ้งให้สำนักงานทราบล่วงหน้าไม่น้อยกว่าสิบห้าวันก่อนดำเนินการ โดยแจ้งเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ตามที่สำนักงานกำหนด

๔.๑.๒ แจ้งให้ผู้ใช้บริการทราบล่วงหน้าไม่น้อยกว่าเจ็ดวันก่อนดำเนินการ โดยมีรายละเอียดเกี่ยวกับระบบการให้บริการที่หยุดให้บริการชั่วคราว และระยะเวลาหยุดให้บริการเพื่อให้ผู้ใช้บริการทราบได้อย่างชัดเจน

๔.๒ กรณีหยุดให้บริการชั่วคราวโดยไม่ได้มีการเตรียมการไว้ล่วงหน้า

๔.๒.๑ แจ้งให้สำนักงานทราบโดยเร็วถึงเหตุที่ทำให้งานสำคัญหยุดให้บริการชั่วคราว พร้อมรายละเอียดเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ตามที่สำนักงานกำหนด

๔.๒.๒ แจ้งให้ผู้ใช้บริการทราบโดยเร็วนับแต่เวลาที่หยุดให้บริการชั่วคราว โดยมีรายละเอียดเกี่ยวกับระบบการให้บริการที่หยุดให้บริการชั่วคราวและระยะเวลาหยุดหรือคาดว่าจะหยุดให้บริการเพื่อให้ผู้ใช้บริการทราบได้อย่างชัดเจน

๔.๓ กรณีเกิดปัญหาหรือมีความบกพร่องในการให้บริการให้แจ้งสำนักงานทราบเป็นหนังสือหรือด้วยวิธีการทางอิเล็กทรอนิกส์ตามที่สำนักงานกำหนดโดยเร็ว

๔.๔ เมื่อการหยุดให้บริการชั่วคราวของงานที่สำคัญสิ้นสุดลงแล้ว หรือผู้รับใบอนุญาตแก้ไขปัญหาหรือความบกพร่องเป็นที่เรียบร้อยแล้ว ให้ผู้รับใบอนุญาตแจ้งสำนักงานทราบโดยเร็ว และต้องจัดเก็บเอกสารหลักฐานที่เกี่ยวข้องกับการดำเนินการเป็นระยะเวลาไม่น้อยกว่าหนึ่งปีนับแต่วันที่จัดทำเอกสารหลักฐานนั้นในลักษณะที่พร้อมให้สำนักงานสามารถตรวจสอบได้เมื่อได้รับการร้องขอ

**ส่วนที่ ๒ มาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยา**

ข้อ ๕ ผู้รับใบอนุญาตต้องจัดให้มีมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการใช้งานระบบการให้บริการซึ่งครอบคลุมรายการอย่างน้อยดังต่อไปนี้

๕.๑ การกำหนดช่องทางการติดต่อและให้ความช่วยเหลือที่ผู้ใช้บริการสามารถติดต่อสื่อสารได้โดยสะดวก

๕.๒ การกำหนดขั้นตอนและมาตรการในการแก้ไขปัญหา การชดใช้หรือเยียวยาผู้ได้รับความเสียหายและกำหนดเป็นมาตรฐานสำหรับปัญหาที่มีลักษณะคล้ายกัน โดยมีรายละเอียดอย่างน้อยดังนี้

๕.๒.๑ กำหนดกรอบระยะเวลาในการดำเนินการในแต่ละขั้นตอนให้การจัดการเป็นไปด้วยความเหมาะสมและไม่ชักช้า

๕.๒.๒ กำหนดระยะเวลาและปัจจัยในการพิจารณาชดใช้หรือเยียวยาให้เป็นธรรม โดยเฉพาะกรณีที่เป็นความผิดพลาดจากระบบการให้บริการหรือจากบุคลากรของผู้รับใบอนุญาตและปฏิบัติอย่างเท่าเทียมกันในกรณีที่มีลักษณะเดียวกัน

๕.๒.๓ กำหนดรายละเอียดพร้อมวิธีการในการแก้ไขปัญหาและการชดใช้ค่าเสียหายซึ่งครอบคลุมกรณีดังต่อไปนี้เป็นอย่างน้อย

(๑) ความเสียหายอันเกิดจากความผิดพลาดหรือการหยุดชะงักของระบบการให้บริการ

(๒) ความเสียหายอันเกิดจากความผิดพลาดหรือบกพร่องในการพิสูจน์หรือยืนยันตัวตน

(๓) ความเสียหายอันเกิดจากการรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคล

(๔) ความเสียหายอันเกิดจากการตรวจสอบข้อมูลไม่ถูกต้อง

๕.๓ การกำหนดขั้นตอนการเยียวยาความเสียหายและการแจ้งผลการดำเนินการให้ผู้ได้รับความเสียหายทราบ โดยมีข้อพึงปฏิบัติดังนี้

๕.๓.๑ ต้องจัดให้มีข้อตกลงกับผู้ใช้บริการเกี่ยวกับความรับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากการให้บริการ

๕.๓.๒ ข้อตกลงตามข้อ ๕.๓.๑ ต้องไม่มีลักษณะเป็นการตัดหรือจำกัดความรับผิดของผู้รับใบอนุญาตเมื่อมีความเสียหายเกิดขึ้น อันเนื่องมาจากการที่ผู้รับใบอนุญาต กรรมการ ผู้บริหาร หรือบุคลากร ไม่ได้ดำเนินธุรกิจหรือปฏิบัติงานให้เป็นไปตามกฎหมาย

๕.๓.๓ มีการแจ้งผลการดำเนินการให้ผู้ได้รับความเสียหายทราบความคืบหน้าเป็นระยะ

ข้อ ๖ ผู้รับใบอนุญาตต้องระบุข้อตกลงเกี่ยวกับการชดใช้หรือเยียวยาความเสียหายไว้ในข้อกำหนดของสัญญาหรือเงื่อนไขการให้บริการอย่างชัดเจน

**ส่วนที่ ๓ การแก้ไขปัญหาและการจัดการเรื่องร้องเรียน**

ข้อ ๗ ผู้รับใบอนุญาตต้องจัดให้มีบุคลากรที่ทำหน้าที่รับเรื่องร้องเรียนซึ่งผู้ใช้บริการสามารถติดต่อโดยตรงได้อย่างสะดวก โดยมีการแจ้งให้ผู้ใช้บริการทราบถึงช่องทางและวิธีการแจ้งปัญหาหรือร้องเรียนการใช้บริการได้อย่างชัดเจน

ข้อ ๘ ผู้รับใบอนุญาตต้องจัดให้มีมาตรการหรือขั้นตอนในการดำเนินการเมื่อมีการร้องเรียนหรือมีข้อโต้แย้งจากผู้ใช้บริการ รวมทั้งกำหนดกรอบเวลาเพื่อหาข้อยุติ ดังนี้

๘.๑ จัดให้มีช่องทางและวิธีการสำหรับการรับข้อร้องเรียนจากผู้ใช้บริการ โดยอย่างน้อยต้องจัดให้มีหมายเลขโทรศัพท์และที่อยู่สำหรับติดต่อได้ หรือที่อยู่สำหรับติดต่อทางจดหมายอิเล็กทรอนิกส์ที่สามารถติดต่อได้

๘.๒ กำหนดวิธีปฏิบัติเกี่ยวกับขั้นตอนการดำเนินการและกรอบระยะเวลาเพื่อหาข้อยุติเป็นลายลักษณ์อักษร และจัดให้มีการอบรมวิธีปฏิบัติดังกล่าวให้แก่บุคลากรที่เกี่ยวข้อง

๘.๓ มีกลไกในการตรวจสอบและแจ้งความคืบหน้า รวมทั้งชี้แจงขั้นตอนการดำเนินการและกำหนดระยะเวลาในการแก้ไขข้อร้องเรียนให้ผู้ร้องเรียนทราบภายในเจ็ดวันนับแต่วันที่ได้รับแจ้งการร้องเรียน

๘.๔ ดำเนินการแก้ไขข้อร้องเรียนให้แล้วเสร็จ และแจ้งผลการดำเนินการให้ผู้ร้องเรียนทราบโดยเร็ว

๘.๕ ในกรณีที่ผู้ให้บริการไม่สามารถพิจารณาหรือแก้ไขข้อร้องเรียนให้แล้วเสร็จภายในกำหนดระยะเวลาตามข้อ ๘.๓ ให้แจ้งความคืบหน้าของการดำเนินการให้ผู้ใช้บริการทราบก่อนครบกำหนดระยะเวลาดังกล่าว และรายงานความคืบหน้าให้ผู้ใช้บริการทราบเพิ่มเติมเป็นระยะจนกว่าการดำเนินการจะแล้วเสร็จ

ข้อ ๙ ผู้รับใบอนุญาตต้องรายงานการร้องเรียนหรือฟ้องร้องเกี่ยวกับการประกอบธุรกิจให้สำนักงานทราบโดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี ซึ่งอย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้

๙.๑ จำนวนเรื่องร้องเรียนหรือฟ้องร้อง

๙.๒ วันที่และเวลาของการร้องเรียนหรือฟ้องร้องแต่ละรายการ

๙.๓ การดำเนินการเพื่อแก้ไขปัญหาการร้องเรียนหรือฟ้องร้องแต่ละรายการ

๙.๔ แนวทางการป้องกันปัญหาเพื่อไม่ให้เกิดเหตุการณ์ดังกล่าวซ้ำอีก

ข้อ ๑๐ ในกรณีที่เป็นการร้องเรียนหรือฟ้องร้องเกี่ยวกับการประกอบธุรกิจที่มีนัยสำคัญซึ่งส่งผลกระทบต่อการให้บริการและเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารระดับสูง คณะกรรมการหรือบุคลากรที่ได้รับมอบหมาย ผู้รับใบอนุญาตต้องรายงานมายังสำนักงานเมื่อรับทราบการร้องเรียนหรือฟ้องร้องดังกล่าวโดยเร็ว และให้แจ้งผลการดำเนินการแก้ไขปัญหาเพิ่มเติมภายหลัง

ข้อ ๑๑ ในกรณีที่ผู้ใช้บริการแจ้งข้อร้องเรียนต่อสำนักงานและสำนักงานได้แจ้งให้ผู้รับใบอนุญาตทราบแล้ว ให้ผู้รับใบอนุญาตดำเนินการเกี่ยวกับข้อร้องเรียนดังกล่าวตามหลักเกณฑ์ในข้อ ๘ และรายงานผลการดำเนินการให้สำนักงานทราบภายในสามสิบวันนับแต่วันที่ได้รับทราบข้อร้องเรียนจากสำนักงาน ทั้งนี้ หากการดำเนินการพิจารณาหรือแก้ไขปัญหาเกี่ยวกับข้อร้องเรียนไม่แล้วเสร็จภายในระยะเวลาดังกล่าว ให้รายงานความคืบหน้าเป็นระยะต่อสำนักงานจนกว่าการดำเนินการจะแล้วเสร็จ เว้นแต่สำนักงานจะกำหนดเป็นอย่างอื่น

**ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. ๑/๒๕๖๖**
**ฉบับที่ ๘**
**หลักเกณฑ์การใช้บริการจากผู้รับดำเนินการแทน**
---

**ส่วนที่ ๑ การใช้บริการจากผู้รับดำเนินการแทน**

ข้อ ๑ ผู้รับใบอนุญาตสามารถใช้บริการจากผู้รับดำเนินการแทนได้โดยต้องมีแนวทางการบริหารความเสี่ยงและแนวทางการดูแลผู้ใช้บริการที่เหมาะสม เว้นแต่งานหลักที่เกี่ยวข้องกับการตัดสินใจในผลการพิสูจน์และยืนยันตัวตนซึ่งอาจส่งผลกระทบต่อฐานะการดำเนินงานและความเสี่ยงของผู้รับใบอนุญาตหากดำเนินการไม่เหมาะสมไม่สามารถให้ผู้รับดำเนินการแทนดำเนินการได้ดังต่อไปนี้

๑.๑ งานที่เกี่ยวกับการวิเคราะห์เชิงลึก การตรวจสอบหรือการสอบทานในขั้นตอนดังนี้

๑.๑.๑ การตัดสินใจหรือการนำส่งผลการพิสูจน์ตัวตน หรือ

๑.๑.๒ การเชื่อมโยงอัตลักษณ์ของบุคคลเข้ากับสิ่งที่ใช้ยืนยันตัวตน หรือ

๑.๑.๓ การตัดสินใจหรือการนำส่งผลการยืนยันตัวตน

๑.๒ งานที่เกี่ยวกับการติดตาม การตรวจสอบ และการสอบทานภายหลังขั้นตอนดังนี้

๑.๒.๑ การตัดสินใจหรือนำส่งผลการพิสูจน์ตัวตน หรือ

๑.๒.๒ การเชื่อมโยงข้อมูลอัตลักษณ์ของบุคคลเข้ากับสิ่งที่ใช้ยืนยันตัวตน หรือ

๑.๒.๓ การตัดสินใจหรือการนำส่งผลการยืนยันตัวตน

ข้อ ๒ ในกรณีที่ผู้รับใบอนุญาตใช้บริการจากผู้รับดำเนินการแทนในการให้บริการผู้รับใบอนุญาตต้องดูแลให้ผู้รับดำเนินการแทนสามารถให้บริการแก่ผู้ใช้บริการเสมือนผู้รับใบอนุญาตเป็นผู้ดำเนินการเอง และต้องกำหนดแนวทางการใช้บริการจากผู้รับดำเนินการแทนอย่างเหมาะสมโดยอย่างน้อยต้องประกอบด้วย

๒.๑ การกำหนดขอบเขตและลักษณะการใช้บริการ โดยมีการกำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างผู้รับใบอนุญาตกับผู้รับดำเนินการแทนอย่างชัดเจนและเป็นลายลักษณ์อักษรและพร้อมสำหรับการตรวจสอบเมื่อสำนักงานร้องขอ

๒.๒ การกำหนดแนวทางการคัดเลือกผู้รับดำเนินการแทนอย่างเหมาะสมก่อนการทำสัญญาหรือข้อตกลงร่วมกัน หรือการทบทวนเพื่อต่ออายุสัญญาหรือข้อตกลงดังกล่าว ซึ่งครอบคลุมประเด็นสำคัญ ดังต่อไปนี้

๒.๒.๑ ความสามารถทางด้านเทคนิค ความเชี่ยวชาญ ประสบการณ์ และความพร้อมในการดำเนินงาน

๒.๒.๒ ชื่อเสียงทางธุรกิจ ประวัติการถูกร้องเรียนหรือการฟ้องร้องดำเนินคดีในเรื่องที่เกี่ยวกับงานที่จะให้ดำเนินการ

๒.๒.๓ มีหลักเกณฑ์ในการพิจารณาการใช้บริการที่มีส่วนเกี่ยวข้องกับกรรมการหรือผู้บริหารระดับสูงของผู้รับใบอนุญาต (conflict of interest)

๒.๒.๔ ความเสี่ยงในกรณีที่ผู้รับดำเนินการแทนให้บริการแก่ผู้รับใบอนุญาตรายอื่นหลายรายพร้อมกัน

๒.๒.๕ มีหลักเกณฑ์การพิจารณาคัดเลือกในกรณีที่ผู้รับดำเนินการแทนเป็นผู้ให้บริการต่างประเทศ ซึ่งสอดคล้องตามขอบเขต ระดับความเสี่ยงและนัยสำคัญของการใช้บริการ

๒.๓ การประเมินและบริหารจัดการความเสี่ยงจากการใช้บริการที่เหมาะสมตามระดับความสำคัญและผลกระทบในการให้บริการ โดยมีการทบทวนการบริหารจัดการความเสี่ยงอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๒.๔ กำหนดมาตรการรองรับที่ทำให้สามารถประกอบธุรกิจได้อย่างต่อเนื่อง (business continuity management) ในกรณีที่ผู้รับดำเนินการแทนไม่สามารถดำเนินงานได้หรือการให้บริการหยุดชะงักลง

๒.๕ การจัดทำสัญญาหรือข้อตกลงกับผู้รับดำเนินการแทนควรครอบคลุมประเด็นสำคัญอย่างน้อยดังต่อไปนี้

๒.๕.๑ รายละเอียดการใช้บริการ ขอบเขตความรับผิดชอบ การบริหารความเสี่ยง

๒.๕.๒ ข้อตกลงการให้บริการเพื่อเป็นมาตรฐานขั้นต่ำที่ต้องปฏิบัติ

๒.๕.๓ แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเพื่อรองรับกรณีการให้บริการมีปัญหาหยุดชะงักและไม่สามารถให้บริการได้อย่างต่อเนื่อง

๒.๕.๔ ขั้นตอนการติดตาม ตรวจสอบ ประเมินประสิทธิภาพการปฏิบัติงาน

๒.๕.๕ ค่าบริการ (ถ้ามี)

๒.๕.๖ อายุสัญญาหรือข้อตกลง และเงื่อนไขเกี่ยวกับการต่ออายุ การแก้ไข และการยกเลิกสัญญา

๒.๕.๗ ขอบเขตความรับผิดชอบในกรณีเกิดปัญหาหรือข้อขัดข้องในการให้บริการ เช่น การให้บริการล่าช้า หรือมีข้อผิดพลาดในการให้บริการ รวมถึงแนวทางการแก้ไขปัญหาและการชดใช้ค่าเสียหายที่อาจเกิดมีขึ้น

๒.๕.๘ การรักษาความมั่นคงปลอดภัยของข้อมูล การรักษาความลับ และความเป็นส่วนตัวของผู้ใช้บริการและผู้รับใบอนุญาต

๒.๕.๙ การปฏิบัติตามหลักเกณฑ์ที่เกี่ยวข้องกับระบบการให้บริการ

๒.๕.๑๐ เงื่อนไขอื่นๆ ตามความจำเป็น เช่น การประกันภัย

๒.๕.๑๑ การกำหนดเงื่อนไขในสัญญาหรือข้อตกลงเกี่ยวกับการให้ผู้ตรวจสอบภายในผู้ตรวจสอบภายนอก และสำนักงาน มีสิทธิเข้าตรวจสอบการดำเนินการของผู้รับดำเนินการแทน

๒.๖ การดูแลให้ผู้รับดำเนินการแทนปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

ข้อ ๓ ผู้รับใบอนุญาตต้องให้สำนักงาน หรือผู้ตรวจสอบ สามารถเข้าตรวจสอบการดำเนินงาน ระบบการควบคุมภายในต่างๆ รวมถึงการเรียกดูข้อมูลที่เกี่ยวกับการตรวจสอบการดำเนินงานของผู้รับดำเนินการแทน รวมถึงการจัดเตรียมข้อมูลที่เกี่ยวข้องกับระบบการให้บริการให้มีความถูกต้องและเป็นปัจจุบันให้สามารถตรวจสอบได้

**ส่วนที่ ๒ การแจ้งต่อสำนักงาน**

ข้อ ๔ ในกรณีที่ผู้รับใบอนุญาตใช้บริการจากผู้รับดำเนินการแทนในการเก็บรวบรวมหรือเก็บรักษาข้อมูลเกี่ยวกับระบบการให้บริการ เช่น การเก็บรวบรวมหรือเก็บรักษาข้อมูลผู้ใช้บริการในขั้นตอนการพิสูจน์ตัวตน ผู้รับใบอนุญาตต้องแจ้งให้สำนักงานทราบภายในสิบห้าวันนับแต่วันที่เริ่มใช้บริการตามแบบที่จัดไว้บนเว็บไซต์ของสำนักงาน

ข้อ ๕ กรณีที่มีการเปลี่ยนแปลงการใช้บริการจากผู้รับดำเนินการแทนซึ่งแตกต่างจากที่แจ้งไว้ตามข้อ ๔ ให้ผู้รับใบอนุญาตแจ้งให้สำนักงานทราบภายในสิบห้าวันนับแต่วันที่มีการเปลี่ยนแปลง