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