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 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 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 ความล้มเหลวหรือ

การหยุดชะงักใด 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