(ร่าง)

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง หลักเกณฑ์การประกอบธุรกิจบริการการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(Identity Provider Service)

พ.ศ. ....

.....

.....

.....

.....

.....

.....

.....

.....

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์การประกอบธุรกิจบริการการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Identity Provider Service) พ.ศ. ....”

ข้อ ๒ ในประกาศนี้

“ผู้ประกอบธุรกิจ” หมายความว่า ผู้ให้บริการการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Identity Provider Service) ตามพระราชกฤษฎีกา

ข้อ ๓ ให้ผู้ให้บริการจัดทำแนวนโยบายและแนวปฏิบัติเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ชัดเจน ซึ่งรวมถึงกระบวนการพิสูจน์และยืนยันตัวตนด้วยวิธีการอื่นในกรณีที่มีเหตุขัดข้องชั่วคราวหรือมีเหตุที่ผู้ประกอบธุรกิจไม่สามารถปฏิบัติตามกระบวนการหลักที่กำหนดได้ โดยมีมาตรการบริหารความเสี่ยงซึ่งต้องมีระดับความน่าเชื่อถือเทียบเคียงกับระดับความน่าเชื่อถือที่ให้บริการ

ข้อ ๔ ในการพิสูจน์ตัวตน ผู้ให้บริการต้องมีกระบวนการและเทคโนโลยีที่สอดคล้องกับเงื่อนไขเกี่ยวกับความน่าเชื่อถือที่กำหนด และมีกระบวนการที่ครอบคลุมการทำงานในเรื่องดังต่อไปนี้

(๑) สามารถจำแนกไอเดนติตี้ของผู้ใช้บริการจากผู้ใช้บริการรายอื่นในบริบทของการให้บริการของผู้ให้บริการได้

(๒) สามารถยืนยันความถูกต้องและแท้จริงของไอเดนติตี้ของผู้ใช้บริการที่มีการสร้างขึ้น

(๓) สามารถยืนยันความถูกต้องในการเชื่อมโยงของไอเดนติตี้กับผู้ใช้บริการ เพื่อยืนยันว่าผู้ใช้บริการเป็นเจ้าของไอเดนติตี้ดังกล่าว

(๔) สามารถยืนยันว่าไอเดนติตี้นั้นไม่ถูกปลอมหรือถูกใช้สำหรับฉ้อโกงหรือทุจริต หรือเคยถูกปลอมหรือถูกใช้สำหรับฉ้อโกงหรือทุจริต

ข้อ ๕ ในการยืนยันตัวตน ผู้ให้บริการต้องมีกระบวนการและเทคโนโลยีในการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ที่สอดคล้องกับเงื่อนไขเกี่ยวกับความน่าเชื่อถือที่กำหนด และมีกระบวนการตรวจสอบว่าสิ่งที่ใช้ยืนยันตัวตนถูกต้อง ใช้งานได้ และยังไม่หมดอายุหรือถูกเพิกถอน ก่อนมีการยืนยันตัวตนของผู้ใช้บริการ

ข้อ ๖ ในการพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมิติแบบไม่พบเห็นต่อหน้า (online biometric binding) ให้ดำเนินการด้วยวิธีการดังต่อไปนี้

(๑) การเปรียบเทียบข้อมูลชีวมิติกับข้อมูลต้นทาง (source biometric matching) ให้ถ่ายภาพบุคคลและส่งภาพที่ได้มาไปยังแหล่งข้อมูลที่น่าเชื่อถือ (Authoritative Source) ของเอกสารแสดงตน เพื่อเปรียบเทียบข้อมูลชีวมิติกับข้อมูลต้นทาง (source biometric matching) หรือ

(๒) การเปรียบเทียบข้อมูลชีวมิติกับเอกสาร (document biometric matching) ให้ถ่ายภาพบุคคลและดำเนินการเปรียบเทียบข้อมูลชีวมิติของภาพที่ได้มากับภาพที่ประมวลผลโดยตรงจากชิปของเอกสารแสดงตน โดยมีกระบวนการตรวจสอบความถูกต้องของภาพที่อ่านจากชิปของเอกสารแสดงตน ตามคำแนะนำของหน่วยงานที่ออกเอกสารแสดงตน

ในกรณีที่เอกสารแสดงตนที่ใช้มีชิปที่ใช้งานได้ ผู้ประกอบธุรกิจต้องทำการเปรียบเทียบข้อมูลชีวมิติของภาพที่ได้มากับภาพที่อ่านโดยตรงจากชิปของเอกสารแสดงตนเท่านั้น เว้นแต่เป็นกรณีที่เอกสารแสดงตนไม่มีชิปหรือชิปใช้งานไม่ได้ ผู้ประกอบธุรกิจต้องดำเนินการตรวจสอบด้วยเอกสารแสดงตนที่น่าเชื่อถืออื่น และห้ามมิให้ใช้ภาพจากการแสกนหรือภาพที่ถ่ายจากเอกสารแสดงตนในการเปรียบเทียบข้อมูลชีวมิติ

การเปรียบเทียบข้อมูลชีวมิติให้ดำเนินการเปรียบเทียบแบบหนึ่งต่อหนึ่ง (one-to-one verification matching) ระหว่างภาพที่ได้มากับภาพที่ได้จากเอกสารแสดงตน โดยไม่ทำการเปรียบเทียบแบบหนึ่งต่อกลุ่ม (one-to-many matching) กับฐานข้อมูลของภาพอ้างอิง

ข้อ ๗ ผู้ให้บริการต้องมีกระบวนการดูแลคุณภาพของภาพที่ได้มาสำหรับการเปรียบเทียบข้อมูลชีวมิติ โดยภาพที่ได้มาต้องมีคุณภาพที่สอดคล้องกับมาตรฐาน ISO 29794-5 และมีกระบวนการในการควบคุมคุณภาพของภาพซึ่งได้มาจากผู้ใช้บริการ พร้อมคำแนะนำผู้ใช้งานในการถ่ายภาพให้ตรงตามคุณภาพของภาพที่กำหนด

ข้อ ๘ ผู้ให้บริการต้องมีกระบวนและมาตรการในการรักษาความปลอดภัยของข้อมูลชีวมิติ โดยต้องจำกัดการเข้าถึงสิทธิในการควบคุมระบบที่เกี่ยวข้องกับข้อมูลชีวมิติ และมีการบันทึกผลลัพธ์ของการเปรียบเทียบข้อมูลชีวมิติในระบบการประมวลผลที่เชื่อถือได้

ข้อ ๙ ผู้ให้บริการต้องมีกระบวนการในการทดสอบเทคโนโลยีการเปรียบเทียบข้อมูลชีวมิติโดยผู้เชี่ยวชาญที่มีประสบการณ์ เพื่อตรวจสอบอัตราความผิดพลาดในการลงทะเบียน (failure to enrol rate) (ถ้ามี) อัตราความผิดพลาดในการได้มาของภาพ (failure to acquire rate) อัตราการตรงกันที่ผิดพลาด (false match rate) และอัตราการไม่ตรงกันที่ผิดพลาด (false non-match rate) ของเทคโนโลยีที่ใช้ ซึ่งต้องสอดคล้องหรือเทียบเคียงได้ตามมาตรฐานสากล (ISO 19795)

การทดสอบต้องดำเนินการภายใต้สภาพการใช้งานที่เสมือนการใช้งานจริง และครอบคลุมการทดสอบกับการให้บริการจริงในทุกกรณี และต้องมีผู้เข้าร่วมทดสอบในปริมาณและความหลากหลายที่เพียงพอ พร้อมมีผลการทดสอบที่สอดคล้องหรือเทียบเคียงได้กับมาตรฐานสากล

ข้อ ๑๐ ผู้ให้บริการต้องมีกระบวนการในการป้องกันการปลอมแปลงข้อมูลชีวมิติในกระบวนการเชื่อมโยงไอเดนตินี้ด้วยข้อมูลชีวมิติ ซึ่งต้องดำเนินการให้เสร็จสิ้นในกระบวนการเดียวกันกับการถ่ายภาพบุคคล ทั้งนี้ เพื่อป้องกันการปลอมแปลงที่อาศัยการแยกกันของกระบวนการ

ในการป้องกันการปลอมแปลงข้อมูลชีวมิติโดยไม่พบเห็นต่อหน้า ผู้ให้บริการต้องจัดให้มีเทคโนโลยีในการตรวจสอบภาพถ่ายที่ได้มาว่าเป็นการถ่ายภาพจากผู้ใช้บริการจริง ณ เวลาที่มีการถ่ายภาพ และมีเทคโนโลยีเพื่อพิสูจน์ความเป็นบุคคลและสังเกตพฤติกรรมผู้ใช้บริการ

กระบวนการในการป้องกันการปลอมแปลงข้อมูลชีวมิติต้องดำเนินการให้สอดคล้องหรือเทียบเคียงได้กับมาตรฐานสากล (ISO 30107-1)

ข้อ ๑๑ ผู้ให้บริการต้องมีกระบวนการในการทดสอบความสามารถของเทคโนโลยีที่ใช้ในการป้องกันการปลอมแปลงข้อมูลชีวมิติโดยผู้เชี่ยวชาญที่มีประสบการณ์ เพื่อตรวจสอบว่าเทคโนโลยีในการป้องกันการปลอมแปลงข้อมูลชีวมิติมีความสอดคล้องหรือเทียบเคียงได้กับมาตรฐานสากล (ISO 30107-1) โดยครอบคลุมการปลอมแปลงข้อมูลชีวมิติในรูปแบบต่างๆ พร้อมรายงานผลการทดสอบต่อสำนักงาน

การทดสอบต้องดำเนินการในสภาพแวดล้อมในการประมวลผลที่เชื่อถือได้ โดยการทดสอบต้องครอบคลุมระบบที่ใช้ให้บริการ ไม่ว่าฮาร์ดแวร์หรือซอฟต์แวร์ที่เกี่ยวข้องกับกระบวนการเชื่อมโยงไอเดนตินี้ด้วยข้อมูลชีวมิติและการป้องกันการปลอมแปลงข้อมูลชีวมิติ

ข้อ ๑๒ ผู้ให้บริการต้องไม่จัดเก็บข้อมูลชีวมิติตั้งต้น (Biometric Sample) ทั้งในบันทึกเหตุการณ์ (log) อุปกรณ์หรือระบบที่จัดเก็บข้อมูลชีวมิติตั้งต้น (Biometric Sample) รวมทั้งต้องไม่เก็บข้อมูลส่วนบุคคลใด ๆ ที่บันทึกไว้ในกระบวนการเชื่อมโยงชีวมิติกับข้อมูลชีวมิติที่รวบรวม และดูแลให้มีการทำลายข้อมูลชีวมิติตั้งต้น

(Biometric Sample) ซึ่งรวมถึงข้อมูลในสำเนา แคช (cache) ระบบของผู้ให้บริการจากภายนอก เว้นแต่เป็นการปฏิบัติตามกฎหมาย

การทำลายข้อมูลชีวมิติตั้งต้น (Biometric Sample) ต้องมีกระบวนการและมีการบันทึกการดำเนินการเพื่อประโยชน์ในการตรวจสอบ (audit log) และให้ทำลายภาพที่ได้มาตามหลักเกณฑ์ที่กำหนดใน Privacy Control

ข้อ ๑๓ ผู้ให้บริการต้องเก็บรักษาข้อมูลและเอกสารหลักฐานในขั้นตอนการพิสูจน์ตัวตน โดยจัดทำรายละเอียดของข้อมูลและเอกสารหลักฐาน ที่สอดคล้องกับกระบวนการและเทคโนโลยีที่ใช้ในการพิสูจน์ตัวตนที่ให้บริการ รวมทั้งจัดเก็บรักษาข้อมูลที่เกี่ยวข้องกับการทำธุรกรรมที่เกี่ยวกับกระบวนการพิสูจน์และยืนยันตัวตน รวมถึงบันทึกเหตุการณ์ (log) ที่เกี่ยวข้องกับการทำธุรกรรม โดยจัดเก็บด้วยวิธีการที่มีความมั่นคงปลอดภัยและมีความเพียงพอในการตรวจสอบและการใช้เป็นพยานหลักฐานตามกฎหมาย

ข้อ ๑๔ ผู้ให้บริการต้องมีกระบวนในการตรวจสอบหรือสอบทานความถูกต้องของกระบวนการดำเนินงานในการพิสูจน์และยืนยันตัวตน เพื่อให้มั่นใจว่าได้ปฏิบัติตามแนวนโยบาย แนวปฏิบัติ และกระบวนการที่กำหนด

ข้อ ๑๕ ผู้ให้บริการต้องมีกระบวนในการตรวจสอบและวิเคราะห์ธุรกรรมผิดปกติที่เกิดหรืออาจเกิดขึ้น (Unusual Transaction) และมีกลไกในการตรวจสอบและแจ้งเตือนผู้ใช้บริการที่เป็นเจ้าของไอเดนติตี้ในกรณีที่พบธุรกรรมผิดปกติ (Unusual Transaction) เพื่อให้มั่นใจไอเดนติตี้นั้นอยู่ภายใต้การควบคุมดูแลของผู้ใช้บริการที่เป็นเจ้าของ

ข้อ ๑๖ ผู้ให้บริการต้องจัดให้มีวิธีการที่ผู้ใช้บริการสามารถปรับปรุงข้อมูลเกี่ยวกับไอเดนติตี้ของตน เพื่อให้เป็นปัจจุบันและสมบูรณ์ได้

ผู้ให้บริการต้องจัดให้มีช่องทางที่ผู้ใช้บริการสามารถแจ้งการระงับการใช้งานไอเดนติตี้ของตน

การดำเนินการตามคำขอของผู้ใช้บริการตามวรรคหนึ่ง ต้องมีกระบวนการตรวจสอบคำขอและมีการยืนยันตัวตนผู้ใช้บริการตามเงื่อนไขเกี่ยวกับความน่าเชื่อถือในระดับเดียวกันก่อนดำเนินการปรับปรุงหรือเปลี่ยนแปลงข้อมูลเกี่ยวกับไอเดนติตี้ หรือระงับการใช้งานไอเดนติตี้ พร้อมแจ้งให้ผู้ใช้บริการทราบถึงสถานะ

ประกาศ ณ วันที่ .. .. พ.ศ. ๒๕๖๔

(.....)

ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์