(ร่าง)

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล

เรื่อง มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัล
ว่าด้วย เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มีวัตถุประสงค์เพื่อให้การบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน ให้หน่วยงานของรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล โดยมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคง ปลอดภัยและมีธรรมาภิบาล

เพื่อให้การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลเป็นไปตามวัตถุประสงค์ดังกล่าวข้างต้น โดยที่มาตรา ๑๒ (๒) กำหนดให้หน่วยงานของรัฐจัดทำกระบวนการหรือการดำเนินงานทางดิจิทัลเพื่อการบริหารราชการแผ่นดินและการให้บริการประชาชน กระบวนการหรือการดำเนินงานทางดิจิทัลนั้นต้องทำงานร่วมกันได้ตามมาตรฐาน ข้อกำหนด และหลักเกณฑ์ที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด เพื่อให้มีความสอดคล้องและเชื่อมโยงระหว่างหน่วยงานของรัฐแห่งอื่นได้ ประกอบมาตรา ๑๒ (๔) จัดให้มีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล จึงจำเป็นต้องกำหนดมาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัล ว่าด้วย เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

อาศัยอำนาจตามความในมาตรา ๗ (๓) (๙) มาตรา ๑๒ (๒) (๔) แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ คณะกรรมการพัฒนารัฐบาลดิจิทัล ในคราวการประชุมครั้งที่ .../.... วันที่...เดือน..... พ.ศ. ..... จึงมีมติให้ออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัล ว่าด้วย เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย”

ข้อ ๒ ในประกาศนี้

“บริการภาครัฐ” หมายความว่า การดำเนินการอย่างหนึ่งอย่างใดที่หน่วยงานของรัฐจัดทำหรือจัดให้มีขึ้นหรือที่มอบอำนาจให้เอกชนดำเนินการแทนเพื่ออำนวยความสะดวกหรือตอบสนองความต้องการของประชาชน

“คุณลักษณะ” (Attribute) หมายความว่า ลักษณะหรือคุณสมบัติของบุคคล

“ไอเดนทิตี” (Identity หรือ ID) หมายความว่า คุณลักษณะ หรือชุดของคุณลักษณะที่ใช้ระบุตัวบุคคลในบริบทที่กำหนด

“ดิจิทัลไอดี” (Digital Identity หรือ Digital ID) หมายความว่า คุณลักษณะ หรือชุดของคุณลักษณะที่ถูกรวบรวมและบันทึกในรูปแบบดิจิทัล ซึ่งสามารถใช้ระบุตัวบุคคลในบริบทที่กำหนด และสามารถใช้ทำธุรกรรมอิเล็กทรอนิกส์

“การลงทะเบียน” (Enrolment) หมายความว่า กระบวนการที่ผู้สมัครใช้บริการลงทะเบียนเป็นผู้ใช้บริการของผู้พิสูจน์และยืนยันตัวตน

“การพิสูจน์ตัวตน” (Identity Proofing) หมายความว่า กระบวนการที่ผู้พิสูจน์และยืนยันตัวตนรวบรวมข้อมูลตรวจสอบหลักฐานแสดงตน และตรวจสอบตัวตนของผู้สมัครใช้บริการ

“การยืนยันตัวตน” (Authentication) หมายความว่า กระบวนการที่ผู้ใช้บริการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างด้วยการใช้สิ่งที่ใช้ยืนยันตัวตน

“ผู้ให้บริการภาครัฐ” หมายความว่า หน่วยงานของรัฐที่ให้บริการหรืออนุญาตให้เข้าถึงข้อมูลหรือระบบบริการภาครัฐ โดยอาศัยสิ่งที่ใช้ยืนยันตัวตนและผลการยืนยันตัวตนหรือสิ่งที่ใช้รับรองตัวตนจากผู้พิสูจน์และยืนยันตัวตน

“ผู้พิสูจน์และยืนยันตัวตน” (Identity Provider) หมายความว่า บุคคลหรือหน่วยงานที่น่าเชื่อถือซึ่งทำหน้าที่

(๑) รับลงทะเบียนและพิสูจน์ตัวตน และ

(๒) บริหารจัดการสิ่งที่ใช้รับรองตัวตน ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตนอาจบริหารจัดการสิ่งที่ใช้รับรองตัวตนเพื่อใช้ภายในองค์กรหรือใช้ภายนอกองค์กรก็ได้

“แหล่งให้ข้อมูลที่น่าเชื่อถือ” (Authoritative Source) หมายความว่า หน่วยงานที่มีความน่าเชื่อถือและสามารถเข้าถึงหรือมีข้อมูลที่ถูกต้อง ซึ่งทำหน้าที่

(๑) ตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้ใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน หรือ

(๒) อนุญาตให้ผู้ให้บริการภาครัฐเข้าถึงข้อมูลที่น่าเชื่อถือหรือข้อมูลส่วนบุคคลซึ่งได้รับความยินยอมจากผู้ใช้บริการ

“ผู้สมัครใช้บริการ” (Applicant) หมายความว่า บุคคลที่สมัครใช้บริการพิสูจน์และยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

“ผู้ใช้บริการ” (Subscriber) หมายความว่า ผู้สมัครใช้บริการที่ผ่านการลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน และได้รับสิ่งที่ใช้ยืนยันตัวตนสำหรับใช้ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

“สิ่งที่ใช้ยืนยันตัวตน” (Authenticator) หมายความว่า สิ่งที่ผู้ใช้บริการครอบครองเพื่อใช้ในการยืนยันตัวตนโดยสิ่งที่ใช้ยืนยันตัวตนจะมีปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย

“สิ่งที่ใช้รับรองตัวตน” (Credential) หมายความว่า เอกสาร วัตถุ หรือกลุ่มข้อมูล ที่เชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตน

“เจ้าพนักงาน” หมายความว่า บุคคลซึ่งกฎหมายบัญญัติว่าเป็นเจ้าพนักงานหรือได้รับแต่งตั้งตามกฎหมายให้ปฏิบัติหน้าที่ราชการ ไม่ว่าเป็นประจำหรือครั้งคราว และไม่ว่าจะได้รับค่าตอบแทนหรือไม่

“สำนักงาน” หมายความว่า สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

หมวด ๑
บททั่วไป

ข้อ ๓ เพื่อให้การพิสูจน์และยืนยันตัวทางดิจิทัล มีความน่าเชื่อถือ พร้อมใช้ ตรวจสอบได้ และเป็นไปตามที่กฎหมายกำหนดโดยพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ ให้ผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือดำเนินการ ดังต่อไปนี้

(๑) จัดทำธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงานและดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ

(๒) จัดให้มีมาตรการหรือระบบรักษาความมั่นคงปลอดภัย

(๓) กำหนดข้อตกลงร่วมกันในการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐและปฏิบัติตามข้อตกลงนั้น

(๔) ให้ความสำคัญและบริหารความเสี่ยงให้เหมาะสมกับระดับความเสี่ยงของบริการภาครัฐ โดยพิจารณาถึงผลกระทบที่อาจเกิดขึ้น เพื่อกำหนดวิธีการบรรเทาความเสียหายที่อาจเกิดขึ้น

หมวด ๒

การทำความรู้จักผู้ใช้บริการ

ข้อ ๔ ให้ผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังต่อไปนี้

(๑) กำหนดนโยบายและกระบวนการปฏิบัติงานภายในที่ชัดเจนเป็นลายลักษณ์อักษร โดยต้องทบทวน สื่อสาร ทำความเข้าใจ สร้างความตระหนักให้กับเจ้าพนักงานหรือบุคลากรที่เกี่ยวข้องให้เห็นถึงความสำคัญ และปฏิบัติตามนโยบายและกระบวนการปฏิบัติงานภายในหรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมถึงต้องสื่อสารทำความเข้าใจและให้ความรู้กับผู้ใช้บริการด้วย

(๒) กำหนดรูปแบบการทำความรู้จักผู้ใช้บริการ เพื่อเป็นมาตรการที่ใช้รู้จักและพิสูจน์ตัวตนผู้ใช้บริการว่าเป็นบุคคลรายนั้นจริง เพื่อป้องกันการทุจริตจากการปลอมแปลงหรือใช้ข้อมูลบุคคลอื่น

(๓) จัดให้ผู้ใช้บริการแสดงตนโดยได้รับข้อมูลและเอกสารที่บ่งชี้ถึงตัวผู้ใช้บริการ

(๔) ตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลและเอกสารหลักฐานแสดงตนที่ได้รับจากผู้ใช้บริการ รวมถึงตรวจสอบว่าบุคคลที่มาแสดงตนเป็นบุคคลเดียวกันกับบุคคลในเอกสารหลักฐานการแสดงตน

(๕) เก็บรักษาข้อมูลและเอกสารหลักฐานการแสดงตน รวมถึงภาพและเสียง (ถ้ามี) และการบันทึกเหตุการณ์และรายละเอียดการทำธุรกรรมเกี่ยวกับการทำความรู้จักผู้ใช้บริการในระบบหรือสถานที่ที่มีความมั่นคงปลอดภัย ตั้งแต่วันเริ่มทำการทำความรู้จักผู้ใช้บริการและเก็บรักษาตามระยะเวลาที่กำหนด

หมวด ๓

การพิสูจน์และยืนยันตัวตนทางดิจิทัล

ข้อ ๕ ให้ผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังต่อไปนี้

(๑) กำหนดรูปแบบและจัดสรรบุคลากร ระบบ เทคโนโลยีที่จำเป็นต่อการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล ให้สอดคล้องกับระดับความน่าเชื่อถือของไอเดนทิตี

(๒) ดำเนินการทำความรู้จักผู้ใช้บริการตามที่กำหนดไว้ในประกาศฉบับนี้

(๓) ดำเนินการตามข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลตามกลุ่มการให้บริการภาครัฐดังต่อไปนี้

(ก) การรวบรวมข้อมูลเพื่อระบุตัวตนที่จำเป็นจากผู้สมัครใช้บริการ เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล

(ข) การตรวจสอบหลักฐานแสดงตน เพื่อตรวจสอบความแท้จริง สถานะการใช้งาน และความถูกต้องของหลักฐานแสดงตน และตรวจสอบข้อมูลที่อยู่ในหลักฐานแสดงตนว่าเป็นของบุคคลที่มีตัวตนอยู่จริง

(ค) การตรวจสอบตัวบุคคลที่แสดงหลักฐานแสดงตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยอาจตรวจสอบช่องทางติดต่อของผู้สมัครใช้บริการว่าเป็นเจ้าของช่องทางที่ใช้ในการติดต่อ รวมถึงสามารถติดต่อหรือส่งข้อมูลไปยังผู้สมัครใช้บริการผ่านช่องทางดังกล่าวได้จริง

(๔) ดำเนินการตามข้อกำหนดการยืนยันตัวตนทางดิจิทัลตามกลุ่มการให้บริการภาครัฐ

(๕) ดำเนินการตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๖) ประกาศข้อกำหนดให้ผู้ที่เกี่ยวข้องในกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลทราบโดยทั่วกัน

ข้อ ๖ ให้ผู้ให้บริการภาครัฐดำเนินการ ดังต่อไปนี้

(๑) กำหนดความต้องการและระบบของหน่วยงานที่ต้องการใช้ดิจิทัลไอดี

(๒) ประเมินความเสี่ยงเพื่อพิจารณาถึงผลกระทบ ระดับความรุนแรงและความสูญเสียที่อาจเกิดขึ้นได้หากการพิสูจน์ตัวตนผิดพลาด

(๓) นำผลการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือทั้งระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

(๔) เลือกรูปแบบ และวิธีการลงทะเบียน พิสูจน์ตัวตน และยืนยันตัวตนทางดิจิทัล ให้สอดคล้องตามข้อกำหนดในแต่ละระดับความน่าเชื่อถือ

ข้อ ๗ ให้แหล่งให้ข้อมูลที่น่าเชื่อถือดำเนินการ ดังต่อไปนี้

(๑) ตรวจสอบความยินยอมของผู้สมัครใช้บริการกับผู้พิสูจน์และยืนยันตัวตน

(๒) ตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้ใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน และส่งผลการตรวจสอบข้อมูลกลับไปยังผู้พิสูจน์และยืนยันตัวตน

ข้อ ๘ ให้สำนักงานกำหนดแนวทางหรือข้อกำหนดเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ ให้เป็นไปตามประกาศฉบับนี้

เมื่อสำนักงานประกาศแนวทางหรือข้อกำหนดตามวรรคหนึ่งแล้ว ให้ผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือ ดำเนินการตามแนวทางหรือข้อกำหนดที่สำนักงานกำหนด

ประกาศ ณ วันที่.....

( )

นายกรัฐมนตรี

ประธานกรรมการพัฒนารัฐบาลดิจิทัล