กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม ETDA

การประชุม
เพื่อรับฟังความคิดเห็นต่อ

ร่างหลักเกณฑ์ลำดับรอง ประกอบการควบคุมดูแลการประกอบธุรกิจบริการ เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตน ทางดิจิทัลที่ต้องได้รับใบอนุญาต

วันศุกร์ที่ 11 พฤศจิกายน พ.ศ. 2565
เวลา 13.00 – 15.00 น.

AGENDA

เวลา	กำหนดการ
13.00 – 13.15 น.	**เปิดลงทะเบียน**
13.15 – 13.30 น.	**ที่มาและวัตถุประสงค์**
13.30 – 14.30 น.	**นำเสนอร่างหลักเกณฑ์ลำดับรองประกอบการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต** • (ร่าง) หลักเกณฑ์การบริหารและจัดการความเสี่ยงในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล • (ร่าง) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ • (ร่าง) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบให้บริการ • (ร่าง) หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ • (ร่าง) หลักเกณฑ์ตามลักษณะของการให้บริการ • (ร่าง) หลักเกณฑ์การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ • (ร่าง) หลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจที่เกี่ยวกับระบบให้บริการ
14.30 – 15.00 น.	Q & A

วัตถุประสงค์การจัดกิจกรรม

เพื่อเป็นการเตรียมความพร้อมสำหรับผู้ประกอบธุรกิจเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่เข้าข่ายตามลักษณะการให้บริการที่ต้องขอรับใบอนุญาตภายใต้ร่างกฎหมาย Digital ID และเพื่อให้การจัดทำร่างหลักเกณฑ์ลำดับรองภายใต้ร่างกฎหมายดังกล่าว มีความเหมาะสม เป็นที่ยอมรับ และสามารถปฏิบัติได้

11 พ.ย. 65
- นำเสนอร่างหลักเกณฑ์

11-18 พ.ย. 65
- เปิดรับฟังความคิดเห็นเป็นการทั่วไป

22-23 พ.ย. 65
- หารือกลุ่มย่อยตามลักษณะการให้บริการ

กิจกรรมที่ผ่านมา

1 ก.ย. 64
- ประชุมรับฟังความคิดเห็นครั้งที่ 1
- หัวข้อการรับฟังความคิดเห็น
(1) ร่างหลักเกณฑ์การตรวจประเมินธุรกิจบริการ 10 หัวข้อ

17-22 มี.ค. 65
- ประชุมกลุ่มย่อย เพื่อรับฟังความคิดเห็น ครั้งที่ 2
- หัวข้อการรับฟังความคิดเห็น
(1) ข้อเสนอแนะแนวทางการบริหารจัดการและการประเมินความเสี่ยง
(2) ร่างหลักเกณฑ์การตรวจประเมินธุรกิจบริการ 10 หัวข้อ

7-8 ก.ค. 65
- ประชุมรับฟังความคิดเห็นครั้งที่ 3
- หัวข้อการรับฟังความคิดเห็น
(1) (ร่าง) แนวทางการบริหารจัดการความเสี่ยง
(2) (ร่าง) หลักเกณฑ์การตรวจประเมินธุรกิจบริการ 10 หัวข้อ

19-27 ก.ค. 65
- ประชุมรายย่อยเพื่อรวบรวมประเด็นและข้อสังเกตเพิ่มเติม รวมถึงทำความเข้าใจรายละเอียดแต่ละบริการ

หัวข้อการนำเสนอ

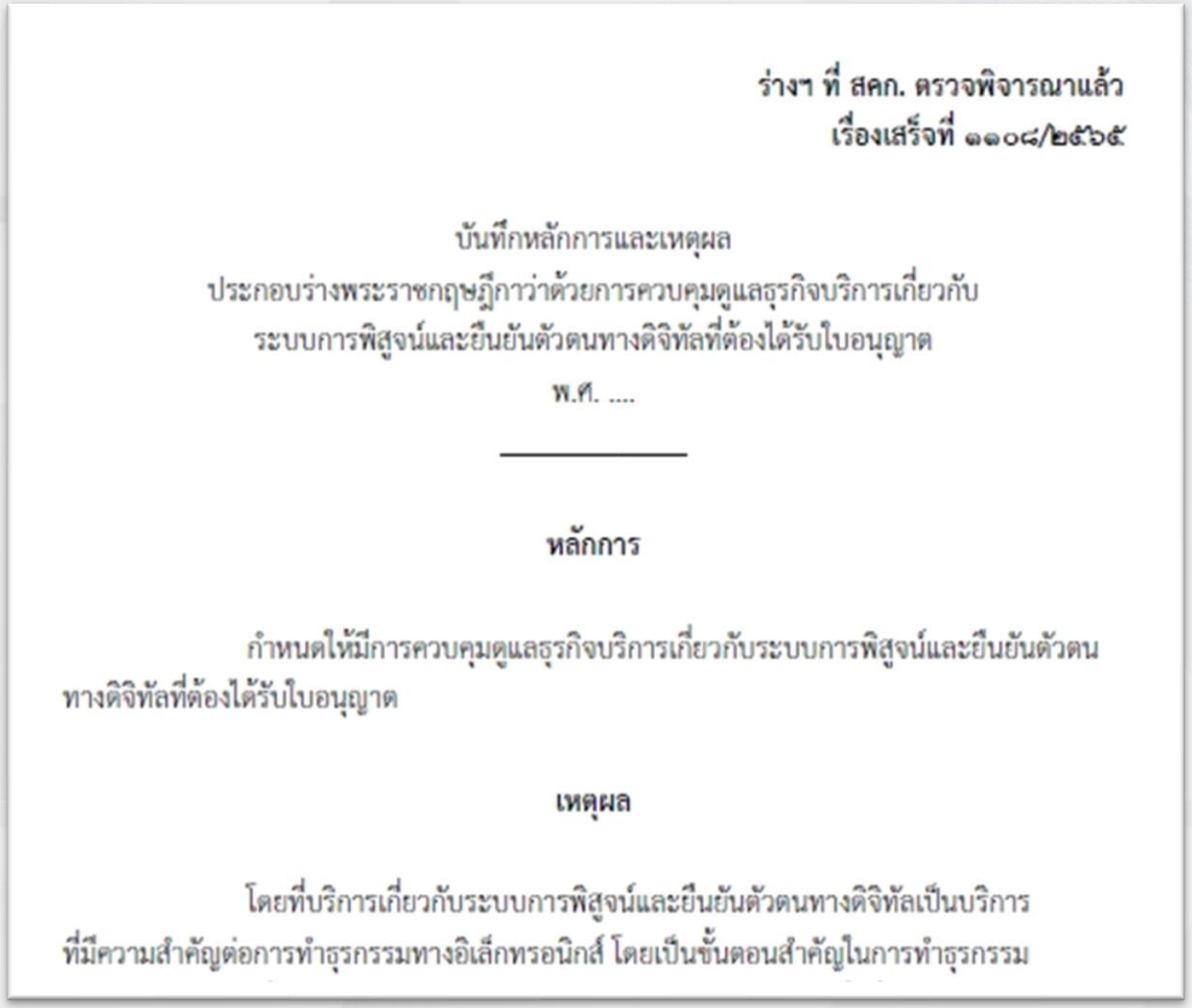
- ร่าง พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. .... (ร่างกฎหมาย Digital ID)
- ร่างหลักเกณฑ์ลำดับรอง ภายใต้ร่างกฎหมาย Digital ID
- แผนเตรียมการรองรับการยื่นคำขอรับใบอนุญาต

ร่าง พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ....

ร่าง พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ....

เหตุผลจำเป็นที่ต้องกำกับดูแล

1. การพิสูจน์และยืนยันตัวตนทางดิจิทัลของบุคคล เป็นกระบวนการสำคัญก่อนทำธุรกรรมออนไลน์โดยเฉพาะธุรกรรมที่มีความเสี่ยง
2. เพื่อให้ธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล มีมาตรฐานการให้บริการที่สอดคล้องกัน ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการปลอมแปลงตัวตน การหลอกลวงหรือฉ้อโกง
3. เพื่อดูแลให้ผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีธรรมาภิบาลและมาตรฐานในการประกอบธุรกิจที่ดีตลอดทั้งกระบวนการ



ร่างฯ ที่ สคก. ตรวจพิจารณาแล้ว
เรื่องเสร็จที่ ๑๑๐๘/๒๕๖๕

บันทึกหลักการและเหตุผล
ประกอบร่างพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับ
ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต
พ.ศ. ....

หลักการ

กำหนดให้มีการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตน
ทางดิจิทัลที่ต้องได้รับใบอนุญาต

เหตุผล

โดยที่บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลเป็นบริการ
ที่มีความสำคัญต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยเป็นขั้นตอนสำคัญในการทำธุรกรรม

Digital ID

- ก.ย. 63 — ครม. มีมติรับหลักการ
- ก.ย. 65 — สคก. ตรวจพิจารณาแล้ว เรื่องเสร็จที่ 1108/2565
- ต.ค. 65 — **เสนอทูลเกล้าฯ**
- มีผลใช้บังคับ 180 วัน นับแต่ประกาศในราชกิจจานุเบกษา

ธุรกิจบริการ Digital ID ภายใต้การกำกับดูแล

ธุรกิจบริการที่กำกับดูแล

1. บริการ**พิสูจน์ตัวตน**
2. บริการ**ออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน**
3. บริการ**ยืนยันตัวตน**
4. บริการ**แลกเปลี่ยนข้อมูล**เพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ธุรกิจบริการที่ได้รับยกเว้น

1. บริการพิสูจน์และยืนยันตัวตน โดยผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมฯ **(Certification Authority: CA)**
2. บริการพิสูจน์และยืนยันตัวตน ที่บุคคลใช้**เพื่อประโยชน์ภายในกิจการ**ของบุคคลหรือนิติบุคคลนั้น **โดยไม่ได้ให้บริการแก่บุคคลภายนอก**
3. **บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในกิจกรรมที่ คธอ. ประกาศกำหนด**

สาระสำคัญ ร่าง พ.ร.ฎ.ฯ

รัฐมนตรีรักษาการ รมว. DE

หมวด 1 การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

- กำหนดประเภทบริการที่ต้องขออนุญาต และไม่ต้องขออนุญาต
- กำหนดคุณสมบัติและลักษณะต้องห้ามของผู้ประกอบธุรกิจ

หมวด 2 การขออนุญาตและการอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

- ขั้นตอนการขออนุญาตและการยื่นเอกสารประกอบ
- การตรวจประเมินความพร้อมของผู้ขอรับใบอนุญาตก่อนเริ่มประกอบธุรกิจ

หมวด 3 หน้าที่ของผู้รับใบอนุญาต

- ลักษณะต้องห้ามของผู้ทำหน้าที่กรรมการ/ผู้จัดการ/ผู้รับผิดชอบในการดำเนินงานของผู้รับใบอนุญาต
- เงื่อนไขการใช้บริการจากบุคคลภายนอกเพื่อเก็บรวบรวมหรือเก็บรักษาข้อมูลเกี่ยวกับบริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- การแจ้งการเปลี่ยนแปลงในเรื่องสำคัญ / เรื่องร้องเรียน
- การจัดเก็บข้อมูลเพื่อประโยชน์ในการตรวจสอบ
- การตรวจประเมินระบบอย่างสม่ำเสมอ

หมวด 4 การควบคุมดูแลการประกอบธุรกิจบริการ

- กำหนดหลักเกณฑ์ตามลักษณะของการให้บริการ
  1) มาตรการการบริหารและการจัดการความเสี่ยง
  2) มาตรการการรักษาความมั่นคงปลอดภัย
  3) มาตรการการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกง จากการใช้งานระบบ
  4) มาตรฐานการให้บริการซึ่งรวมถึงการจัดการและจัดเก็บข้อมูล
  5) การคุ้มครองผู้ใช้บริการและมาตรการการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ
  6) การใช้บริการจากบุคคลภายนอกที่เกี่ยวกับระบบการให้บริการ
  7) การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ
- การนำส่งงบการเงินและสรุปผลการดำเนินงานเกี่ยวกับการให้บริการ อย่างน้อยปีละ 1 ครั้ง
- อำนาจพนักงานเจ้าหน้าที่ในการเรียกให้ส่งรายงานหรือข้อมูลเพิ่มเติม

หมวด 5 การเลิกประกอบธุรกิจ

- ขั้นตอนการขอเลิกประกอบธุรกิจและการยื่นเอกสารประกอบ ที่ผู้ประกอบธุรกิจต้องดำเนินการ
- หลักเกณฑ์ วิธีการ เงื่อนไข และระยะเวลาในการเลิกประกอบธุรกิจ

หมวด 6 การพักใช้และเพิกถอนใบอนุญาต

- เหตุแห่งการเพิกถอน
- ผลของการเพิกถอน

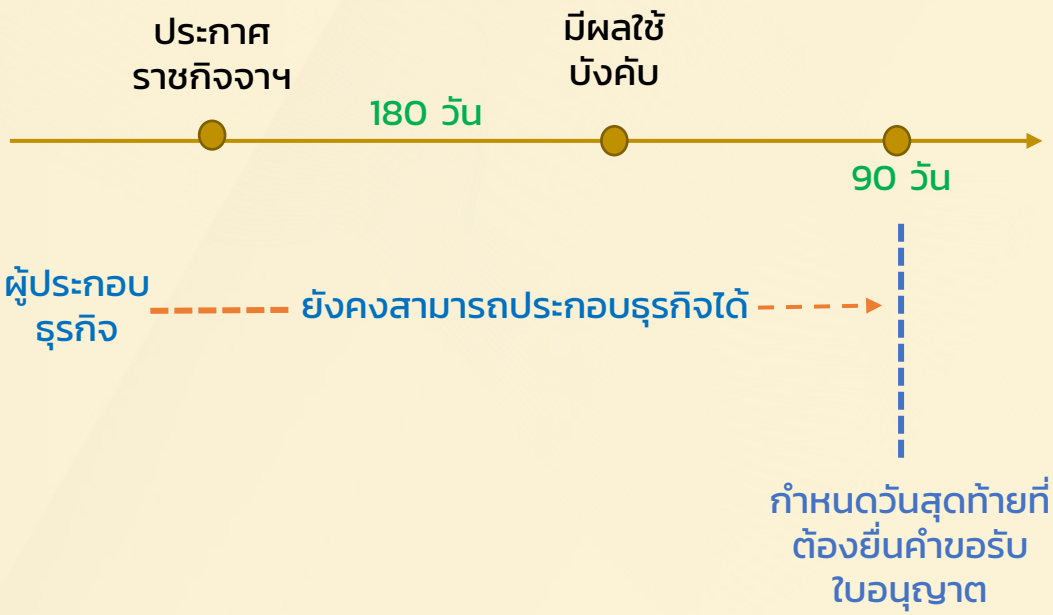
บทเฉพาะกาล

- ผู้ที่ประกอบธุรกิจอยู่แล้วก่อนกฎหมายใช้บังคับให้ยื่นคำขอรับอนุญาตภายใน 90 วัน นับแต่กฎหมายมีผลใช้บังคับ

กลไกทางกฎหมายเพื่อรองรับผู้ประกอบธุรกิจที่ดำเนินการอยู่ในปัจจุบัน

บทเฉพาะกาล

มาตรา 37 ให้**ผู้ประกอบธุรกิจ**บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตตามพระราชกฤษฎีกานี้**ซึ่งได้ประกอบธุรกิจอยู่ในวันก่อนวันที่พระราชกฤษฎีกานี้ใช้บังคับ ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลต่อไปได้** โดย**ให้ยื่นคำขอรับใบอนุญาตพร้อมด้วยรายงานผลการตรวจประเมินความพร้อม**ในการประกอบธุรกิจ**ภายในเก้าสิบวันนับแต่วันที่พระราชกฤษฎีกานี้มีผลใช้บังคับ** และ**เมื่อได้ยื่นคำขอรับใบอนุญาตแล้วให้ดำเนินกิจการต่อไปได้จนกว่าคณะกรรมการจะมีคำสั่งไม่อนุญาต**



หาก**ไม่ยื่นคำขอภายใน 90 วัน** และยัง**ประกอบธุรกิจต่อไป**
ถือว่า **ประกอบธุรกิจโดยไม่ได้รับอนุญาต**
ตาม พ.ร.บ.ธุรกรรมฯ มาตรา 45/1

(ร่าง) หลักเกณฑ์ลำดับรอง ภายใต้ร่างกฎหมาย Digital ID

ร่างหลักเกณฑ์ลำดับรองตามลักษณะของการให้บริการ

มาตรา 24 ให้สำนักงานโดยความเห็นชอบของคณะกรรมการมีอำนาจประกาศกำหนดหลักเกณฑ์ในเรื่องดังต่อไปนี้ โดยกำหนดตามลักษณะของการให้บริการ

ร่าง พ.ร.ฎ.	ร่างลำดับรอง	Control
(1) มาตรการบริหารและการจัดการความเสี่ยงของระบบการให้บริการ	• **(ร่าง) หลักเกณฑ์การบริหารและจัดการความเสี่ยง**ในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล	• **Risk** Management
(2) มาตรการรักษาความมั่นคงปลอดภัยของระบบการให้บริการและการตรวจสอบ	• **(ร่าง) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ**ของระบบให้บริการ	• **Security** Control • **Privacy** Control
(3) มาตรการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ	• **(ร่าง) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกง**จากการใช้งานระบบให้บริการ	• **Fraud** Control
(4) มาตรฐานการให้บริการที่รวมถึงการจัดการและจัดเก็บข้อมูล	• **(ร่าง) หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ**	• **User Experience** • **Technical Test** • **Functional Assessment** • **User term**
	• **(ร่าง) หลักเกณฑ์ตามลักษณะของการให้บริการ**	• Role Requirement – **IDP** – **Exchange**
(5) การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ	• **(ร่าง) หลักเกณฑ์การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยา**ผู้ได้รับความเสียหายจากการประกอบธุรกิจ	• **User Protection** • **Mitigation**
(6) การใช้บริการจากบุคคลภายนอกที่เกี่ยวกับระบบการให้บริการ	• **(ร่าง) หลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจ**ที่เกี่ยวกับระบบให้บริการ	• **Business partner**
(7) การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ	* รวมอยู่ใน (ร่าง) หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ *	

Supervisory framework

Inherent Risk

Quality of Risk Management

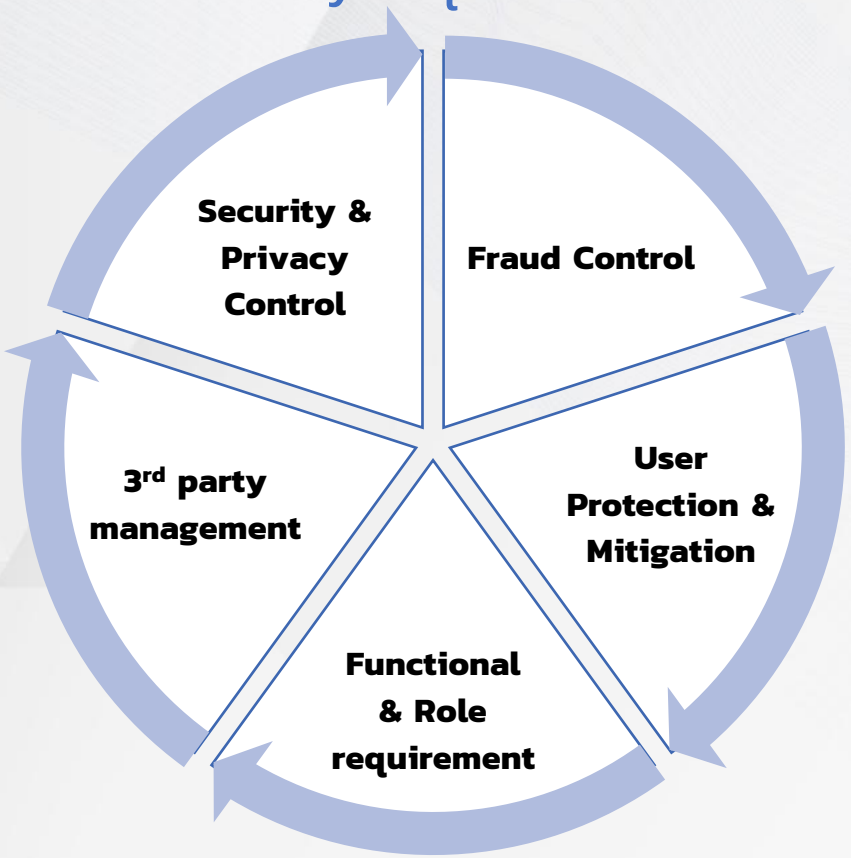
: Risk Factor

- Strategic risk
- Operational risk
- Information Technology risk
- Reputation risk
- Compliance risk

+

Capability Management

: Key requirements



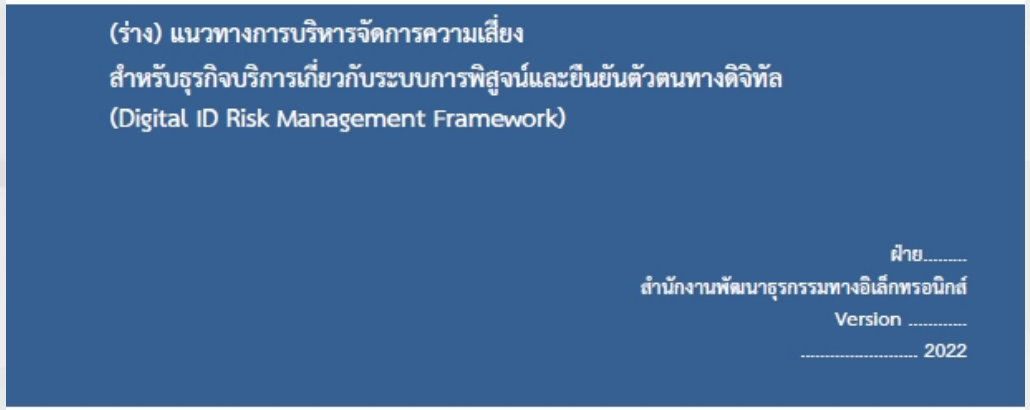
ม.24 (1) มาตรการบริหารและการจัดการความเสี่ยงของระบบการให้บริการ

(ร่าง) หลักเกณฑ์การบริหารและจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ภาพรวม

กำหนดหน้าที่ของผู้รับใบอนุญาตในการบริหารจัดการความเสี่ยง ดังนี้

1. จัดให้มี**นโยบายและมาตรการ**บริหารจัดการความเสี่ยง เพื่อประเมินฐานะและผลการดำเนินงาน
2. **การกำกับดูแล**ความเสี่ยง และกระบวนการบริหารจัดการความเสี่ยง ซึ่งต้อง**ครอบคลุมกระบวนการ** ดังนี้
   1) การ**ระบุความเสี่ยง** (Risk identification)
   2) การ**ประเมินความเสี่ยง** (Risk assessment)
   3) การ**วัดผลความเสี่ยง**กับเกณฑ์ประเมินความเสี่ยง (Risk evaluation)
   4) การ**ลดความเสี่ยง**หลังจากการประเมิน (Risk treatment)
   5) การ**ติดตามและรายงานผล**ความเสี่ยงอย่างต่อเนื่อง (Risk monitoring and reporting)
3. **การระบุความเสี่ยง**ที่เกี่ยวข้องกับระบบฯ โดย**ครอบคลุมความเสี่ยง 5 ด้าน**
   1) ความเสี่ยงด้าน**กลยุทธ์** (Strategic Risk)
   2) ความเสี่ยงด้าน**การปฏิบัติการ** (Operational Risk)
   3) ความเสี่ยงด้าน**เทคโนโลยีสารสนเทศ** (Information Technology Risk)
   4) ความเสี่ยงด้าน**ชื่อเสียง**ขององค์กร (Reputation Risk)
   5) ความเสี่ยงด้าน**การปฏิบัติตามหลักเกณฑ์** (Compliance Risk)
4. การประเมินการปฏิบัติตามแนวทางการบริหารจัดการความเสี่ยง
5. การทบทวนการประเมินความเสี่ยงประจำปี และในกรณีมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ



(ร่าง) แนวทางการบริหารจัดการความเสี่ยง สำหรับธุรกิจบริการ เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

Digital ID Role

ผู้ให้บริการ

- บริการพิสูจน์ตัวตน (Identity Proofing Service)
- บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (Authenticator Management Service)
- บริการยืนยันตัวตน (Authentication Service)
- บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service)

Risk Assessment Process

Self assessment

Inherent risk

สูง	ปานกลาง	ต่ำ

ผลลัพธ์มาจากการประเมินผ่านแบบประเมินความเสี่ยงตั้งต้นขององค์กรผู้ให้บริการธุรกิจที่เกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัล

- เน้นไปที่สภาพแวดล้อมในการดำเนินงานและความเสี่ยงที่ธุรกิจเกี่ยวข้องกับการพิสูจน์และยืนยันตนทางดิจิทัลจะต้องพบเจอ
- อ้างอิงจากหลักฐานที่ดำเนินการจริงขององค์กร

Audit process

Risk management capability

อ่อน	พอใช้	ดี

ผลลัพธ์มาจากการตรวจสอบตามหลักเกณฑ์การตรวจประเมินธุรกิจบริการเกี่ยวกับระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล

- Security & Privacy Control
- Fraud Control
- Functional
- Role requirement
- User Protection & Mitigation
- 3rd party management

Result

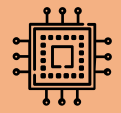
Net risk

- Net risk by risk factor
- Overall net risk

Risk factor

Strategic risk

Operational risk



Technology risk

Reputation risk

Compliance risk

Criteria

IR	RMC: ดี (1)	RMC: พอใช้ (2)	RMC: อ่อน (3)
สูง (3)	ปานกลาง	ค่อนข้างสูง	สูง
ปานกลาง (2)	ค่อนข้างต่ำ	ปานกลาง	ค่อนข้างสูง
ต่ำ (1)	ต่ำ	ค่อนข้างต่ำ	ปานกลาง

Monitor risk

ต่ำ	ค่อนข้างต่ำ
ปานกลาง	

Reduce risk

ค่อนข้างสูง	สูง

ประเด็นที่มีการปรับปรุง

- **ปรับปรุงถ้อยคำ**
  - เพื่อไม่เป็นการบังคับรูปแบบการจัดทำนโยบาย
    "ผู้รับใบอนุญาตต้อง~~กำหนด~~จัดให้มีนโยบายและมาตรการบริหารจัดการความเสี่ยงซึ่งครอบคลุมความเสี่ยงที่เกี่ยวข้องกับ~~สำหรับ~~บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล "

- **ปรับปรุงตัวอย่างของ ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) เพื่อให้ชัดเจนมากขึ้น**
  - ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) หมายถึง ความเสี่ยงที่จะเกิดความเสียหายต่าง ๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการควบคุมภายใน บุคลากร และระบบงาน หรือจากเหตุการณ์ภายนอก เช่น ความเสี่ยงจากการฉ้อโกงโดยบุคคลภายใน และบุคคลภายนอก ความเสี่ยงจากการขัดข้อง หรือหยุดชะงักของระบบงาน ความเสี่ยงจากแนวปฏิบัติเกี่ยวกับผู้ใช้บริการ การให้บริการและดำเนินธุรกิจ

- **เพิ่มเติมกรอบเวลาในการนำส่งผลการประเมินความเสี่ยง**
  - การจัดส่งผลการประเมินให้เป็นไปตามรูปแบบ และระยะเวลาที่สำนักงานกำหนด
    ซึ่งร่าง พ.ร.ฎ. มาตรา 23 ให้ สพธอ. กำหนดหลักเกณฑ์ วิธีการ และระยะเวลานำส่งรายงานการตรวจประเมินระบบ

(ร่าง) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบให้บริการ

หมวด 1	ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ
หมวด 2	นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security policy)
หมวด 3	การบริหารและการจัดการความเสี่ยงของระบบการให้บริการ
หมวด 4	การคุ้มครองข้อมูลส่วนบุคคล
หมวด 5	การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง (IT compliance)
หมวด 6	การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)

ภาพรวม

หมวด 1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

- ความตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- กำหนดโครงสร้าง และผู้รับผิดชอบ
- การบริหารจัดการบุคลากร
- จัดให้มีนโยบายที่สำคัญ ได้แก่
  1. นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
  2. นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
  3. นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล

โดยทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยยะสำคัญ

หมวด 2 นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

- มีนโยบายและมาตรการที่ครอบคลุมหลักการ C.I.A. เช่น การรักษาความมั่นคงปลอดภัยของข้อมูล การควบคุมการเข้าถึง ความมั่นคงปลอดภัยของการสื่อสาร การจัดทำ DRP/BCM
- การดำเนินการสำคัญที่รองรับตามลักษณะการให้บริการ
  - การเก็บ log
  - การจัดการเหตุการณ์ไม่พึงประสงค์
  - การบริหารจัดการบุคคลภายนอก

หมวด 3 การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ

- มีนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ครอบคลุมกระบวนการบริหารจัดการความเสี่ยง
- ต้องมีการประเมินความเสี่ยงด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยยะสำคัญ
- กรณีเกิดเหตุการณ์ที่ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนด ต้องแจ้งให้สำนักงานทราบ และมีการบันทึกการดำเนินการที่แตกต่างจากแผนการบริหารความเสี่ยง โดยนำส่งพร้อมกับสรุปผลการดำเนินการประจำปี

ภาพรวม (ต่อ)

หมวด 4 การคุ้มครองข้อมูลส่วนบุคคล

- **ส่วนที่ 1** นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล
- **ส่วนที่ 2** การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy Impact Assessment) ในขั้นตอนการนำส่งรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจ และกรณีมีการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการให้บริการภายหลังจากเริ่มประกอบธุรกิจ
- **ส่วนที่ 3** การจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- **ส่วนที่ 4** การรวบรวมข้อมูลพฤติกรรมการใช้งาน : จำกัด
- **ส่วนที่ 5 การบริหารจัดการข้อมูลชีวมิติ**
- **ส่วนที่ 6 ความยินยอม :** เปิดเผยข้อมูลอัตลักษณ์ได้ต่อเมื่อได้รับความยินยอม และเก็บ log การให้ความยินยอม
- **ส่วนที่ 7 การดำเนินการที่เกี่ยวข้อง** : การแก้ไขและการเข้าถึงข้อมูลส่วนบุคคล การดูแลคุณภาพของข้อมูล
- **ส่วนที่ 8 การจัดการเรื่องร้องเรียน** : ต้องมีมาตรการ/กลไกการจัดการเรื่องร้องเรียนที่ชัดเจน เข้าถึงได้ง่าย ผู้รับเรื่องมีความรู้ความเข้าใจในการรับเรื่องและจัดการ

หมวด 5 การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

- ต้องปฏิบัติตามกฎหมาย และหลักเกณฑ์ที่เกี่ยวข้อง เช่น
  - กม.ธุรกรรมทางอิเล็กทรอนิกส์
  - กม.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
  - กม.คุ้มครองข้อมูลส่วนบุคคล
  - กม.การรักษาความมั่นคงปลอดภัยไซเบอร์

หมวด 6 IT audit

- ต้องมีการตรวจสอบการรักษาความมั่นคงปลอดภัยของระบบอย่างน้อยปีละ 1 ครั้ง
- ต้องติดตามปรับปรุงประเด็นจากการตรวจสอบ

ประเด็นที่มีการปรับปรุง

หมวด 1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

- เพิ่มเติมการกำหนดบทบาทหน้าที่และความรับผิดชอบของบุคลากรภายในองค์กรของผู้ให้บริการ โดย**ให้กำหนดโครงสร้างการกำกับดูแลองค์กรตามหลัก Three lines of defense**

หมวด 2 นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

(1) ปรับปรุงและเพิ่มเติมรายละเอียดมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

- มาตรการที่กำหนดในแต่ละเรื่องควรสัมพันธ์กับระดับความเสี่ยง
- Asset management
  : การบำรุงรักษาทรัพย์สิน
  : การวางแผนรองรับสินทรัพย์ที่ใกล้จะสิ้นสุดอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support)
- Communications security
  : การออกแบบเครือข่ายอย่างมั่นคงปลอดภัย
- System development
  : การแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้พัฒนาระบบ และควบคุมการใช้งานข้อมูลในการทดสอบ
- Incident management
  : เพิ่มเติมเรื่องการวิเคราะห์สาเหตุที่แท้จริง (root course) ของปัญหาในกระบวนการจัดการเหตุการณ์ไม่พึงประสงค์

ประเด็นที่มีการปรับปรุง (ต่อ)

หมวด 2 นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ต่อ)

(2) การจัดเก็บ log

- หน้าที่ของ Authenticator Management
  : เพิ่มเติมการจัดเก็บวันที่และเวลาที่ทำการเชื่อมโยงข้อมูลเพื่อออกสิ่งที่ใช้ยืนยันตัวตน
- กำหนดระยะเวลาจัดเก็บ log
  : จัดเก็บไม่ต่ำกว่า 3 ปี เพื่อประโยชน์ในการสอบทานกิจกรรม รวมถึงกรณีที่เกิดข้อพิพาทภายหลังการยกเลิกหรือยุติการใช้งาน Digital ID

(3) Incident Management

- เพิ่มเติมหน้าที่รายงานเหตุ
  : กรณีเกิดเหตุการณ์สำคัญซึ่งส่งผลกระทบต่อการให้บริการและเป็นปัญหาที่ต้องรายงานผู้บริหาร จะต้องรายงานสำนักงานทันที

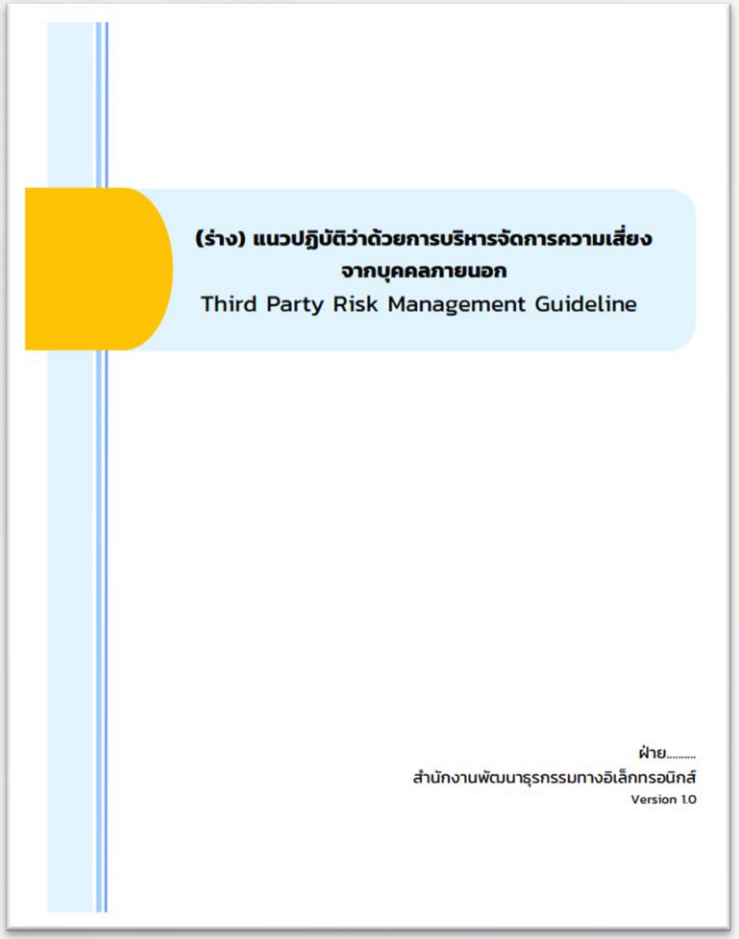
ประเด็นที่มีการปรับปรุง (ต่อ)

หมวด 2 นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (ต่อ)

(4) ปรับปรุงเรื่อง**การบริหารจัดการบุคคลภายนอก** ให้มีความชัดเจนและครอบคลุมในทุกมิติ

- เพิ่มเติมขอบเขตคำว่าบุคคลภายนอกให้ครอบคลุมกรณีดังนี้
  - (1) การใช้บริการจากผู้ให้บริการด้านเทคโนโลยีสารสนเทศ (IT outsourcing)
  - (2) การเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก
  - (3) การให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญ หรือเข้าถึงข้อมูลผู้ใช้บริการของระบบให้บริการ
- ดำเนินการตาม**แนวปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยงบุคคลภายนอก** โดยพิจารณาประยุกต์ใช้ให้เหมาะสมและสอดคล้องตามขอบเขต ระดับความเสี่ยงและนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของบุคคลภายนอก
- ต้องควบคุมให้บุคคลภายนอกมี**มาตรฐานการรักษาความมั่นคงปลอดภัยในระดับที่เทียบเท่า**

- สาระสำคัญของ**ร่างแนวปฏิบัติ**
  - บุคคลภายนอก ไม่รวมถึงผู้ใช้บริการระบบให้บริการ
  - ดูแลเรื่อง Risk Governance
    - บทบาทหน้าที่ความรับผิดชอบ และการจัดโครงสร้างองค์กรตามหลัก 3 line of Defense
    - การจัดการบุคลากร
    - การคุ้มครองผู้ใช้บริการ
    - นโยบายการบริหารจัดการความเสี่ยง
    - การตรวจสอบ
  - Third party risk management
    - การประเมินความเสี่ยง
    - การคัดเลือกบุคคลภายนอก
    - การทำสัญญาหรือข้อตกลง
    - การติดตามผลการปฏิบัติงาน
    - การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง
    - การรักษาความมั่นคงปลอดภัยสารสนเทศ



ประเด็นที่มีการปรับปรุง (ต่อ)

หมวด 4 การคุ้มครองข้อมูลส่วนบุคคล

- **การบริหารจัดการข้อมูลชีวมิติ**
  - เพิ่มเติมเรื่อง**ความยินยอม** โดยหากมีการจัดเก็บและใช้งาน ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล
  - **จำกัดวัตถุประสงค์**ในการจัดเก็บ
    (1) เพื่อประโยชน์ในการใช้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
    (2) เพื่อการปรับปรุง พัฒนา และทดสอบสมรรถนะของการให้บริการ
  - ต้อง**มีกระบวนการดูแลข้อมูลชีวมิติอย่างเข้มงวด** โดยอย่างน้อยต้องดำเนินการดังนี้
    (1) มีการเข้ารหัสข้อมูล
    (2) จัดเก็บบนเครือข่ายที่มั่นคงปลอดภัย
    (3) รับส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย
    (4) จำกัดการเข้าถึงเฉพาะผู้รับผิดชอบ
  - ต้อง**ทำลายเมื่อผู้ใช้บริการเพิกถอนความยินยอมหรือยกเลิกการใช้บริการ**

ม.24 (3) มาตรการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

(ร่าง) หลักเกณฑ์การควบคุมดูแลและป้องกัน
การทุจริตหรือการฉ้อโกงจากการใช้งานระบบให้บริการ

ภาพรวม

- มีการ**กำหนดบุคลากรที่รับผิดชอบ**การดำเนินการตามหลักเกณฑ์
- ต้อง**จัดทำแผนป้องกันการทุจริตหรือการฉ้อโกง**ที่สอดคล้องกับลักษณะการให้บริการ และความเสี่ยงของระบบให้บริการ
- ต้อง**มีการทบทวนแผน**ป้องกันการทุจริตหรือการฉ้อโกง อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงในสาระสำคัญ
- มีการ**บริหารจัดการบุคลากร**อย่างเหมาะสม สร้างความตระหนัก และมีคู่มือการทำงาน
- ต้อง**มีคำแนะนำ**แก่ผู้ใช้บริการสำหรับการดูแลข้อมูลของตน และเพื่อหลีกเลี่ยงการถูกหลอกลวง

- ต้องมี**กลไกในการติดตาม เฝ้าระวังเหตุการณ์ทุจริตหรือฉ้อโกง**
  - มีการบรรเทาผลกระทบอย่างเหมาะสม
  - มีขั้นตอนปฏิบัติงาน การตัดสินใจในช่วงสำคัญ
  - มีการรายงานเหตุ โดยนำส่งพร้อมรายงานประจำปี
- ต้อง**มีมาตรการช่วยเหลือผู้ใช้บริการ**
  - ช่องทางรับแจ้งเหตุ
  - มีการให้ความช่วยเหลือหากข้อมูลรั่วไหล รวมถึงมาตรการป้องกันการใช้งานข้อมูลหากสงสัยว่าจะมีการฉ้อโกงหรือทุจริต
- ถ้าเกิดเหตุที่**ไม่สามารถปฏิบัติตามหลักเกณฑ์**ได้ **ต้องแจ้งสำนักงาน**โดยเร็ว และมีการบันทึกการดำเนินการไว้โดยนำส่งพร้อมรายงานประจำปี

ประเด็นที่มีการปรับปรุง

- **เพิ่มเติมหน้าที่รายงานเหตุ**
  - กรณีเกิดเหตุการณ์สำคัญซึ่งส่งผลกระทบต่อการให้บริการและเป็นปัญหาที่ต้องรายงานผู้บริหาร จะต้องรายงานสำนักงานทันที

ม.24 (4) มาตรฐานการให้บริการที่รวมถึงการจัดการและจัดเก็บข้อมูล
ม.24 (7) การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ

(ร่าง) หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ

หมวด 1	การออกแบบการใช้งานระบบ
หมวด 2	การทดสอบด้านเทคนิคของระบบและซอฟต์แวร์ที่เกี่ยวข้อง (Technical testing requirement)
หมวด 3	การตรวจประเมินระบบให้บริการ
หมวด 4	ข้อตกลงการให้บริการ

ภาพรวมและประเด็นปรับปรุง

หมวด 1 การออกแบบการใช้งานระบบ

- **ส่วนที่ 1 เกณฑ์ทั่วไป :** การออกแบบคำนึงถึงผู้ใช้งาน ซึ่งมีการแสดงผลที่ชัดเจน เข้าใจง่าย และเหมาะสมกับอุปกรณ์
- **ส่วนที่ 2 การออกแบบสำหรับขั้นตอนการพิสูจน์ตัวตน :** มีการแจ้งข้อมูลที่จำเป็น และขั้นตอนต่างๆ ให้ผู้ใช้บริการได้รับทราบ และมีช่องทางให้ความช่วยเหลือ หรือติดต่อสอบถาม
- **ส่วนที่ 3 การออกแบบสำหรับขั้นตอนการยืนยันตัวตน** : มีคู่มือการใช้งานและการรักษา Authenticator รวมถึงช่องทางในการกู้คืนหรือเปลี่ยนแปลงกรณีเกิดการสูญหาย/ไม่สามารถใช้งาน
- **ส่วนที่ 4 การทดสอบความสามารถของระบบ** : มีแผนและดำเนินการทดสอบให้ครอบคลุมขอบเขตการให้บริการ โดยนำส่งผลการทดสอบในขั้นตอนขอเริ่มประกอบธุรกิจ

หมวด 2 การทดสอบด้านเทคนิคของระบบและซอฟต์แวร์ที่เกี่ยวข้อง

- มีแผนการทดสอบ และดำเนินการทดสอบให้ครอบคลุมระบบให้บริการ โดยต้องมีความสอดคล้องตามกลไกที่กำหนด เช่น การเฝ้าระวัง incident การทดสอบโพรโทคอล เป็นต้น
- มี Requirement traceability matrix ที่สอดคล้องกับ test case
- ส่งผลการทดสอบในขั้นตอนขอเริ่มประกอบธุรกิจ

หมวด 3 การตรวจประเมินระบบให้บริการ

- มีการตรวจประเมินต้องทำอย่างน้อยปีละ 1 ครั้ง ครอบคลุมเรื่องสำคัญ ได้แก่
  (1) Security & Privacy
  (2) Fraud
  (3) Role requirement
- ดำเนินการโดยผู้ตรวจสอบอิสระ ที่มีความรู้ความสามารถ และไม่มีส่วนได้เสียกับระบบให้บริการ
- ต้องรายงานผลตรวจให้ผู้บริหารรับทราบ และนำส่งสำนักงานตามระยะเวลาที่กำหนด

หมวด 4 ข้อตกลงการให้บริการ

- มีข้อตกลงในการให้บริการ ให้ผู้ใช้บริการทราบและยอมรับ โดยมีรายละเอียดขั้นต่ำตามที่กำหนด
- ถ้ามีกรณีที่ผู้ใช้บริการต้องดำเนินการกับบุคคลภายนอกที่เกี่ยวกับระบบให้บริการ ต้องแจ้งให้ผู้ใช้บริการทราบด้วย
- แจ้งให้ทราบรายละเอียดค่าธรรมเนียมการใช้บริการ
- **เพิ่มเติมข้อกำหนดรองรับการเลิกประกอบธุรกิจ :** ต้องมีการประเมินความเสี่ยงก่อนการเลิกประกอบธุรกิจและจัดทำแผนรองรับตามที่คณะกรรมการประกาศกำหนด (ร่างหลักเกณฑ์ที่จะดำเนินการจัดทำในระยะที่ 3)

ม.24 (4) มาตรฐานการให้บริการที่รวมถึงการจัดการและจัดเก็บข้อมูล

(ร่าง) หลักเกณฑ์ตามลักษณะของการให้บริการ

หมวด 1	**บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการยืนยันตัวตน** ส่วนที่ 1 การพิสูจน์ตัวตน ส่วนที่ 2 การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และการยืนยันตัวตน ส่วนที่ 3 การเชื่อมโยงและแลกเปลี่ยนข้อมูล ส่วนที่ 4 การพิสูจน์และยืนยันตัวตนโดยใช้เทคโนโลยีชีวมิติ ส่วนที่ 5 การตรวจสอบประวัติการใช้งาน (User Dashboard)
หมวด 2	**บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล** ส่วนที่ 1 ข้อกำหนดทั่วไป ส่วนที่ 2 ข้อกำหนดด้านความสอดคล้องของระบบ ส่วนที่ 3 ข้อกำหนดด้านเทคนิค

ภาพรวม

หมวด 1 บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการยืนยันตัวตน

- **ส่วนที่ 1 การพิสูจน์ตัวตน**
  - ต้องดำเนินการให้สอดคล้องตามมาตรฐาน IAL
  - มีกระบวนการที่ครอบคลุมกิจกรรมสำคัญ ได้แก่
    - การปรับปรุงข้อมูลอัตลักษณ์
    - การระงับการใช้งาน Digital Identity ชั่วคราว
  - กรณีรองรับการยกระดับ IAL ต้องดำเนินการดังนี้
    - กระบวนการสอดคล้องตามมาตรฐาน IAL
    - ยืนยันตัวตนด้วย Authenticator ปัจจุบันก่อน
    - ต้องแจ้งผลเมื่อดำเนินการสำเร็จ
  - ต้องมีการดูแลข้อมูลส่วนบุคคล

- **ส่วนที่ 2 การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และการยืนยันตัวตน**
  - ต้องดำเนินการให้สอดคล้องตามมาตรฐาน AAL
  - ก่อนยืนยันตัวตนต้องมีการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อให้แน่ใจว่าถูกต้อง ใช้งานได้
  - กรณีขอให้ระงับการใช้งานสิ่งที่ใช้ยืนยันตัวตนต้องมีการตรวจสอบ และแจ้งให้ผู้ใช้บริการทราบ
  - การส่งผลการยืนยันตัวตนต้องดูแลเรื่องการรักษาความลับ และความครบถ้วนของข้อมูล
  - หากมีการยกระดับความน่าเชื่อถือของการยืนยันตัวตน ต้องมีการตรวจสอบและแจ้งผลการยกระดับ

ประเด็นที่มีการปรับปรุง

- **ส่วนที่ 3 การเชื่อมโยงและแลกเปลี่ยนข้อมูล**
  - ต้องกำหนด Protocol ที่ใช้งาน และวิธีการเชื่อมต่อเพื่อให้สามารถเชื่อมโยงกันได้ โดยอย่างน้อยต้องสามารถ mapping รายการข้อมูล และระดับความน่าเชื่อถือตามคำขอ
  - ต้องมีรายการข้อมูลอัตลักษณ์ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยน
  - ต้องมีนโยบายการเปิดเผยข้อมูลอัตลักษณ์ที่สอดคล้องกับหลักเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคล

- เพิ่มเติมรายละเอียดชุดข้อมูลที่สามารถระบุตัวผู้ใช้บริการ และข้อมูลที่ห้ามมิให้มีการส่งต่อ
  - ผู้ใช้บริการ**ควรมีชุดข้อมูลขั้นต่ำ**ที่สามารถระบุตัวผู้ใช้บริการได้อย่างชัดเจน ประกอบด้วย
    (1) เลขบัตรประจำตัวประชาชน
    (2) ชื่อ นามสกุล ภาษาไทย
    (3) ชื่อ นามสกุล ภาษาอังกฤษ (ถ้ามี)
    (4) วัน เดือน ปี เกิด
    (5) ที่อยู่
  - **ห้ามมิให้ส่งข้อมูลที่ใช้สำหรับการตรวจสอบสถานะของหลักฐานแสดงตน** ได้แก่
    (1) เลขคำร้องขอมีบัตรประจำตัวประชาชน
    (2) หมายเลขชิปบัตรประจำตัวประชาชน
    (3) เลขควบคุมหลังบัตรประชาขน (เลเซอร์ ไอดี (Laser ID))

หมวด 1 บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการยืนยันตัวตน (ต่อ)

- **ส่วนที่ 4 กรณีที่มีการใช้งานข้อมูลชีวมิติ**
  - ต้องดำเนินการให้สอดคล้องหลักปฏิบัติสำหรับการใช้งานเทคโนโลยีชีวมิติ
    - มีนโยบายและแนวปฏิบัติที่ชัดเจน
    - มีการบริหารจัดการอัตลักษณ์ที่สอดคล้องตามมาตรฐาน
    - มีคู่มือการใช้งานสำหรับผู้ปฏิบัติงาน และผู้ใช้บริการ
  - ต้องจำกัดการเข้าถึงข้อมูลเฉพาะผู้ที่เกี่ยวข้องและได้รับการฝึกอบรมอย่างเหมาะสม

- **ส่วนที่ 5 การตรวจสอบประวัติการใช้งาน**
  - อาจจัดให้มีวิธีการหรือช่องทางเพื่อให้ผู้ใช้บริการตรวจสอบประวัติการใช้งานได้ ปรับปรุงหน้าที่ในการจัดเก็บประวัติการใช้งานเพื่อให้ผู้ใช้บริการสามารถสอบทานการใช้ข้อมูลของตนเองได้
    - ต้องจัดเก็บไว้ในลักษณะที่พร้อมให้ผู้ใช้บริการเรียกดูข้อมูลย้อนหลังได้ทันที
    - ระยะเวลาการจัดเก็บไม่น้อยกว่า 6 เดือน
  - อย่างน้อยควรให้ผู้ใช้บริการสามารถตรวจสอบเกี่ยวกับ
    - ประวัติกิจกรรม
    - ประวัติการให้ความยินยอม
  - ประวัติการใช้งาน ต้องไม่มีการแสดงข้อมูลส่วนบุคคล

หมวด 2 บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล

- **ส่วนที่ 1 เกณฑ์ทั่วไป**
  - ต้องจัดให้มีมาตรการดูแลข้อมูลส่วนบุคคล
    - ไม่นำข้อมูลส่วนบุคคลมาใช้เป็น Identifier
    - ไม่จัดเก็บข้อมูลส่วนบุคคลที่มีการรับส่งในระบบ เว้นแต่จัดเก็บในsession การยืนยันตัวตน
  - ต้องมีการจัดเก็บ log โดยอย่างน้อย
    - กำหนด Uniqueaudit ID สำหรับคำขอเพื่อยืนยันตัวตน และใช้สำหรับการบันทึก log
    - บันทึกรายการสำคัญ ได้แก่ เวลา, ชื่อผู้ร้องขอ/ผู้ให้ข้อมูล, identifier ของผู้ร้องขอ/ผู้ให้ข้อมูล
- **ส่วนที่ 2 ความสอดคล้องของระบบ**
  - ต้องกำหนดเงื่อนไขความสอดคล้องและแจ้งให้ผู้ใช้บริการทราบ อย่างน้อยในเรื่องดังนี้
    - ระดับความน่าเชื่อถือที่สามารถเชื่อมต่อกับระบบบริการ
    - Protocol ที่ใช้งาน
  - การกำหนดระดับความน่าเชื่อถือ
    - ต้องมีรายชื่อผู้ให้บริการและระดับความน่าเชื่อถือที่สามารถให้บริการได้
    - มีกลไกคัดแยกผู้ให้บริการตามระดับความน่าเชื่อถือ
  - ต้องกำหนด Protocol ที่ใช้งาน และวิธีการเชื่อมต่อเพื่อให้สามารถเชื่อมโยงกันได้ โดยอย่างน้อยต้องสามารถ mapping รายการข้อมูล และระดับความน่าเชื่อถือตามคำขอ
  - มีรายการข้อมูลอัตลักษณ์สำหรับการเชื่อมโยงและแลกเปลี่ยน
  - ต้องมีนโยบายการเปิดเผยข้อมูลอัตลักษณ์ ที่สอดคล้องกับหลักเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคล
- **ส่วนที่ 3 ด้านเทคนิค**
  - ต้องมีแผนการทดสอบการเชื่อมโยงและแลกเปลี่ยนข้อมูล
  - ต้องมีการทดสอบการใช้งานตามแผนการทดสอบร่วมกับผู้ประสงค์จะเชื่อมต่อ
  - ถ้าผู้ประสงค์จะเชื่อมต่อไม่สามารถทดสอบได้ หรือผลไม่สมบูรณ์ ห้ามให้บริการแก่ผู้นั้น

ม.24 (5) การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ

ม.21 การแจ้งให้สำนักงานทราบเมื่อได้รับการร้องเรียนหรือฟ้องร้องเกี่ยวกับการประกอบธุรกิจ

(ร่าง) หลักเกณฑ์การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ

ส่วนที่ 1 การคุ้มครองผู้ใช้บริการ

1. การเปิดเผยข้อมูลการให้บริการอย่างเพียงพอต่อการตัดสินใจเลือกใช้บริการ
2. การจัดช่องทางในการติดต่อสื่อสาร ให้สามารถติดต่อได้โดยสะดวก มีการดูแลอย่างเหมาะสม
3. การดูแลข้อมูลที่ใช้ในการติดต่อสื่อสารไม่ให้เกิดความสำคัญผิด
4. การดำเนินการกรณีระบบให้บริการของงานที่สำคัญหยุดให้บริการชั่วคราว หรือเกิดปัญหา หรือมีความบกพร่องในการให้บริการ
   - กรณีหยุดให้บริการชั่วคราว
     - มีการเตรียมการไว้ล่วงหน้า – แจ้งสำนักงาน / แจ้งผู้ใช้บริการ ตามเวลาที่กำหนด และแจ้งระยะเวลาหยุดให้บริการให้ผู้ใช้บริการทราบ
     - ไม่ได้มีการเตรียมการไว้ล่วงหน้า – แจ้งสำนักงาน / แจ้งผู้ใช้บริการ โดยเร็วนับแต่เวลาที่หยุดให้บริการ และแจ้งระยะเวลาหยุดให้บริการให้ผู้ใช้บริการทราบ
   - กรณีเกิดปัญหาหรือความบกพร่องในการให้บริการ
     - ให้แจ้งสำนักงานทราบโดยเร็ว
     - ต้องแจ้งผลการดำเนินการให้สำนักงานทราบ และเก็บหลักฐานไว้เพื่อการตรวจสอบ

ส่วนที่ 2 การกำหนดมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยา

5. การจัดทำมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยา
   - ต้องครอบคลุมช่องทางการติดต่อ ขั้นตอน ระยะเวลาและปัจจัยในการพิจารณาชดใช้หรือเยียวยา
   - ต้องมีการแจ้งผลการดำเนินการให้ผู้ใช้บริการทราบ
   - ต้องมีข้อตกลงเกี่ยวกับความรับผิดชอบต่อความเสียหายที่อาจเกิดจากการให้บริการ
6. การระบุข้อตกลงเกี่ยวกับการชดใช้หรือเยียวยาไว้ในข้อกำหนดของสัญญาหรือเงื่อนไขการใช้บริการอย่างชัดเจน

ส่วนที่ 3 การแก้ไขปัญหาและการจัดการเรื่องร้องเรียน

7. การจัดให้มีบุคลากรดูแลรับเรื่องร้องเรียน
8. จัดให้มีมาตรการหรือขั้นตอนในการดำเนินการเมื่อมีการร้องเรียนหรือมีข้อโต้แย้งจากผู้ใช้บริการ รวมทั้งกำหนดกรอบเวลาเพื่อหาข้อยุติ
   - มีช่องทาง/วิธีการรับเรื่องร้องเรียน
   - มีวิธีปฏิบัติ และกรอบเวลา
   - มีการตรวจสอบและแจ้งความคืบหน้า/ผลการดำเนินการ
9. การรายงานเรื่องร้องเรียนให้สำนักงานทราบ
   - เรื่องร้องเรียนทั่วไป ให้รายงานพร้อมสรุปผลการดำเนินงานประจำปี
   - กรณีที่มีนัยสำคัญซึ่งส่งผลกระทบและต้องรายงานผู้บริหารทราบ ให้รายงานสำนักงานทันที และแจ้งผลการแก้ไขภายหลัง
   - ถ้าเป็นกรณีที่ได้รับแจ้งเรื่องร้องเรียนจากสำนักงาน ต้องแจ้งผลการดำเนินการให้สำนักงานทราบภายในระยะเวลาที่กำหนด

ม.24 (6) การใช้บริการจากบุคคลภายนอกที่เกี่ยวกับระบบการให้บริการ
ม.19 การใช้บริการจากบุคคลภายนอกเพื่อเก็บรวบรวมหรือเก็บรักษาข้อมูลเกี่ยวกับการให้บริการ

(ร่าง) หลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจที่เกี่ยวกับระบบให้บริการ

แนวทางการกำกับดูแล

การใช้บริการบุคคลภายนอกซึ่งมีการดำเนินการดังต่อไปนี้
(1) การใช้บริการจากผู้ให้บริการด้านเทคโนโลยีสารสนเทศ (IT outsourcing)
(2) การเชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก
(3) การให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญ หรือเข้าถึงข้อมูลผู้ใช้บริการของระบบให้บริการ

บุคคลภายนอก

IT Outsourcing

ผู้ให้บริการด้านเทคโนโลยีสารสนเทศ เช่น Cloud Computing, Software เป็นต้น

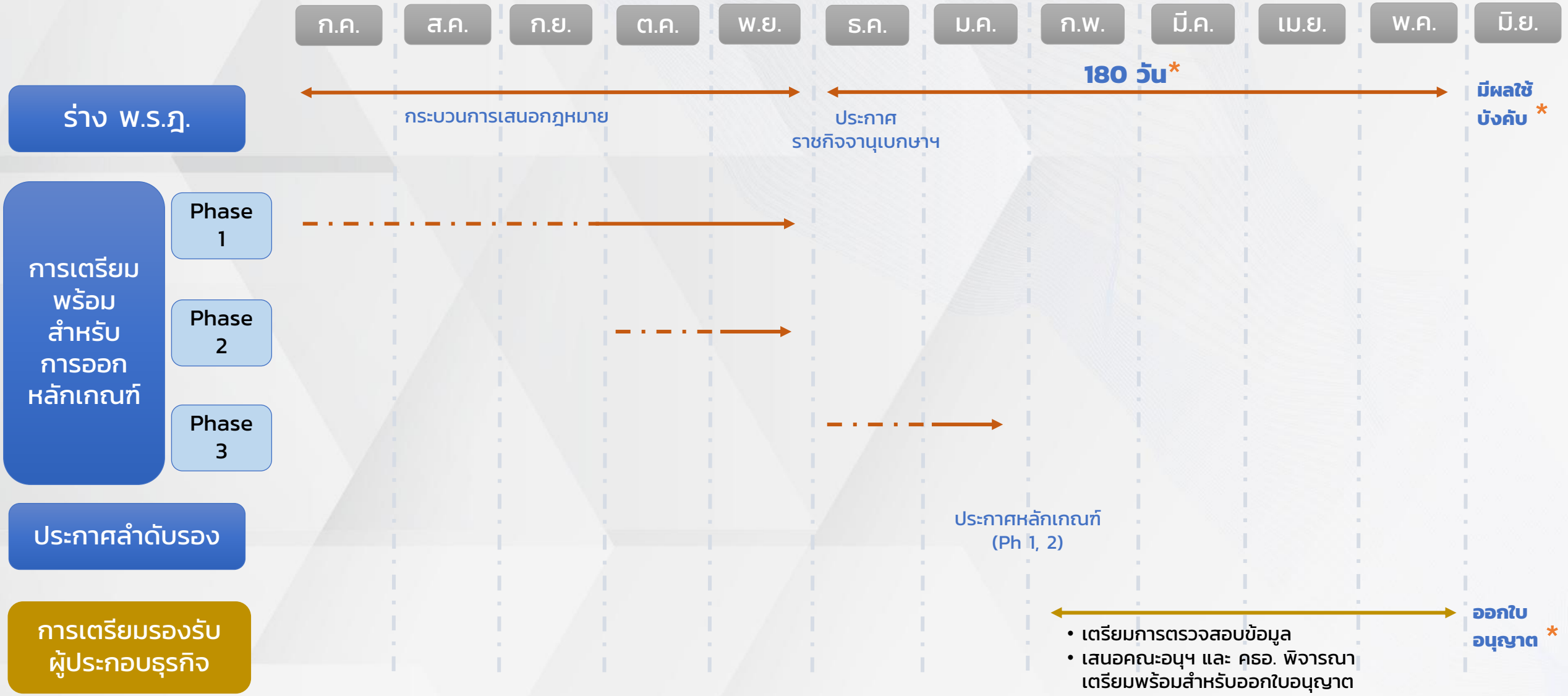
Business Partner

บุคคลธรรมดาหรือนิติบุคคลที่มี**การทำสัญญาหรือข้อตกลงร่วมกับผู้รับใบอนุญาตในการดำเนินการแทนผู้รับใบอนุญาต**สำหรับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ตัวแทนในการเก็บรวบรวมข้อมูลผู้ใช้บริการ เป็นต้น ซึ่งอาจมีการเชื่อมต่อระบบงานด้านเทคโนโลยีสารสนเทศกับผู้รับใบอนุญาตด้วย

(ร่าง) หลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจ ที่เกี่ยวกับระบบให้บริการ

- **การใช้บริการจากพันธมิตรทางธุรกิจ (business partner)**
  - สามารใช้บริการได้ ยกเว้น
    - งานที่เกี่ยวกับการวิเคราะห์เชิงลึก การตรวจสอบหรือการสอบทานในขั้นตอนสุดท้ายก่อนการตัดสินใจหรือนำส่งผลการพิสูจน์ตัวตน การเชื่อมโยงอัตลักษณ์ของบุคคลเข้ากับสิ่งที่ใช้ยืนยันตัวตน หรือนำส่งผลการยืนยันตัวตน
    - งานที่เกี่ยวกับการติดตาม การตรวจสอบ และการสอบทานภายหลังการตัดสินใจหรือนำส่งผลการพิสูจน์ตัวตน การเชื่อมโยงข้อมูลอัตลักษณ์ของบุคคลเข้ากับสิ่งที่ใช้ยืนยันตัวตนหรือผลการยืนยันตัวตน ซึ่งอาจส่งผลกระทบต่อฐานะการดำเนินงานและความเสี่ยงของผู้รับใบอนุญาตหากดำเนินการไม่เหมาะสม
  - ต้องดูแลให้พันธมิตรทางธุรกิจสามารถให้บริการแก่ผู้ใช้บริการเสมือนผู้รับใบอนุญาตเป็นผู้ดำเนินการเอง และต้องกำหนดแนวทางการใช้บริการจากพันธมิตรทางธุรกิจ
  - แนวทางการใช้บริการพันธมิตรทางธุรกิจ
    - กำหนดขอบเขต ลักษณะการใช้บริการ และบทบาทหน้าที่ระหว่างกันอย่างชัดเจน
    - กำหนดแนวทางการคัดเลือกก่อนทำสัญญา
    - มีการประเมินและบริหารจัดการความเสี่ยงอย่างเหมาะสม
    - กำหนดมาตรการ BCP
    - การดูแลให้พันธมิตรทางธุรกิจปฏิบัติให้สอดคล้องตามกฎหมายและให้สำนักงานสามารถเข้าตรวจสอบการทำงานได้
  - กรณีที่ต้องมีการแจ้งต่อสำนักงาน
    - การใช้บริการจากพันธมิตรทางธุรกิจในการเก็บรวบรวมหรือเก็บรักษาข้อมูลเกี่ยวกับการให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (ร่าง พ.ร.ฎ. มาตรา 19)

แผนเตรียมการ
รองรับการยื่นคำขอรับใบอนุญาต



* ปรับปรุงระยะเวลาตามกระบวนการและสถานะล่าสุดของร่าง พ.ร.ฎ.

ร่างพ.ร.ฎ. มาตรา 11 รายการข้อมูล/เอกสาร/หลักฐาน ประกอบคำขอรับใบอนุญาต*

รายการข้อมูล เอกสาร หรือหลักฐาน*	ร่าง พ.ร.ฎ.
1. ชื่อและเลขทะเบียนนิติบุคคล พร้อมด้วยคำยินยอมให้เข้าถึงข้อมูล	ม. 11 (1), (9)
2. หนังสือมอบอำนาจ	ม. 11 (2)
3. รายชื่อกรรมการ ผู้จัดการ หรือผู้ซึ่งรับผิดชอบในการดำเนินงาน พร้อมทั้งหนังสือรับรองคุณสมบัติ และเอกสารที่แสดงถึงการไม่มีลักษณะต้องห้าม	ม. 18
4. รายละเอียดเกี่ยวกับระบบและเทคโนโลยีที่ใช้ในการให้บริการ	ม. 11 (3)
5. แผนการบริหารความเสี่ยงและการประเมินและบริหารจัดการความเสี่ยง	ม. 11 (4)
6. แผนการคุ้มครองข้อมูลส่วนบุคคล	ม. 11 (5)
7. แผนและมาตรการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ	ม. 11 (6)
8. แผนและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ	ม. 11 (7)
9. แผนและมาตรการคุ้มครองผู้ใช้บริการ	ม. 11 (8)
10. แผนการใช้บริการจากพันธมิตรทางธุรกิจเพื่อเก็บรวบรวมหรือเก็บรักษาข้อมูลเกี่ยวกับการให้บริการ (ถ้ามี)	ม. 19

- ข้อมูลประกอบการยื่นคำขอรับใบอนุญาตตาม (4) – (10) ต้องมีรายละเอียดสอดคล้องกับมาตรา 24 ของร่าง พ.ร.ฎ. (หลักเกณฑ์ตามลักษณะของการให้บริการ)
- การยื่นคำขอให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานกำหนด (ร่างพ.ร.ฎ. ม.17 ประกอบ ม.5)

หมายเหตุ

* ข้อมูลเบื้องต้นประกอบการนำเสนอ ซึ่งรายละเอียดอยู่ระหว่างการปรับปรุงเพื่อให้สอดคล้องตามร่างกฎหมายและร่างหลักเกณฑ์ที่จะมีผลบังคับใช้ต่อไป

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม ETDA

อ่านรายละเอียดเพิ่มเติมและแสดงความคิดเห็นได้ที่

https://bit.ly/3hoolRy

สามารถติดตามข่าวสารประชาสัมพันธ์ได้ที่

ETDA THAILAND @ETDA_THAILAND ETDA CHANNEL WWW.ETDA.OR.TH