**แบบสำรวจความคิดเห็น**

**(ร่าง) หลักเกณฑ์ลำดับรองประกอบการควบคุมดูแลการประกอบธุรกิจบริการ  
เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต**

**ชื่อ หน่วยงาน/บริษัท**....................................................................................................................................................

**ชื่อผู้ติดต่อ/ผู้ประสานงาน**………………………………………………**นามสกุล**…….…………………………………………………………

**ตำแหน่ง**………………………………………………………………………………………………………………………………………………………

**โทรศัพท์/มือถือ**……………………………………………………………….**อีเมล**….………………………………………………………………

**คำชี้แจง:**

ตามที่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ได้ดำเนินการจัดทำร่างหลักเกณฑ์ลำดับรอง ภายใต้ (ร่าง) พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. … เพื่อเตรียมการรองรับการประกาศบังคับใช้กฎหมายฉบับดังกล่าว นั้น

ในการนี้ เพื่อให้หลักเกณฑ์ที่จัดทำขึ้นมีความชัดเจนและผู้ที่เกี่ยวข้องสามารถนำมาปฏิบัติได้อย่างเหมาะสมจึงได้จัดให้มีการประชุมเพื่อรับฟังความคิดเห็นเกี่ยวกับร่างหลักเกณฑ์ลำดับรองภายใต้ร่างพระราชกฤษฎีกาฉบับดังกล่าวขึ้น ซึ่ง (ร่าง) หลักเกณฑ์ลำดับรองประกอบการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตประกอบด้วย

1. (ร่าง) หลักเกณฑ์การบริหารและจัดการความเสี่ยงในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
2. (ร่าง) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบให้บริการ
3. (ร่าง) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบให้บริการ
4. (ร่าง) หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ
5. (ร่าง) หลักเกณฑ์ตามลักษณะของการให้บริการ
6. (ร่าง) หลักเกณฑ์การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ
7. (ร่าง) หลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจที่เกี่ยวกับระบบให้บริการ

**โปรดส่งแบบสำรวจความคิดเห็นของท่านมาที่**

**อีเมล:** [**suchayapim@etda.or.th**](mailto:suchayapim@etda.or.th) **และ** [**natcha@etda.or.th**](mailto:natcha@etda.or.th) **ภายในวันที่ 18 พฤศจิกายน 2565**

สอบถามข้อมูลเพิ่มเติม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

โทรศัพท์: 0 2123 1234 ต่อ 90602 (สุฉายพิมพ์) อีเมล: suchayapim@etda.or.th

โทรศัพท์: 0 2123 1234 ต่อ 91411 (ณัชชา) อีเมล: natcha@etda.or.th

**ส่วนที่ 1 : (ร่าง) หลักเกณฑ์ลำดับรองฉบับที่ 1 ถึง 5**

ด้วย (ร่าง) หลักเกณฑ์ลำดับรองฉบับที่ 1 ถึง 5 ซึ่งผ่านการประชุมเพื่อรับฟังความเห็นเมื่อวันที่ 7 – 8 กรกฎาคม 2565 แล้ว ได้มีการปรับปรุงเพิ่มเติมเนื้อหาบางส่วน   
*จึงขอรับฟังความเห็นในส่วนที่แก้ไขเพิ่มเติม*

* **เห็นด้วยตามร่างฯ โดยไม่มีข้อคิดเห็น**
* **เห็นด้วยตามร่างฯ โดยมีข้อคิดเห็น/ข้อเสนอแนะเพิ่มเติม**

| 1. **(ร่าง) หลักเกณฑ์การบริหารจัดการความเสี่ยง ในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล** | |
| --- | --- |
| **รายละเอียดหลักเกณฑ์** | **ข้อคิดเห็น/ข้อเสนอแนะ** |
| * 1. ผู้รับใบอนุญาตต้องจัดให้มีนโยบายและมาตรการบริหารจัดการความเสี่ยงซึ่งครอบคลุมความเสี่ยงที่เกี่ยวข้องกับบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อประเมินฐานะและผลการดำเนินงาน โดยคำนึงถึงผลกระทบจากความเสี่ยงของการให้บริการเพื่อกำหนดมาตรการและแผนการบรรเทาผลกระทบที่อาจจะเกิดขึ้นอย่างทันท่วงที |  |
| 3. ในการระบุความเสี่ยงที่เกี่ยวข้องกับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล  ต้องดำเนินการให้ครอบคลุมความเสี่ยง 5 ด้าน ได้แก่  (1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ..........  (3) ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) หมายถึง ความเสี่ยงที่จะเกิดความเสียหายต่าง ๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการควบคุมภายใน บุคลากร และระบบงาน หรือจากเหตุการณ์ภายนอก เช่น ความเสี่ยงจากการฉ้อโกงโดยบุคคลภายในและบุคคลภายนอก ความเสี่ยงจากการขัดข้องหรือหยุดชะงักของระบบงาน ความเสี่ยงจากแนวปฏิบัติเกี่ยวกับผู้ใช้บริการ การให้บริการและดำเนินธุรกิจ เป็นต้น |  |

| * 1. **(ร่าง) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบให้บริการ** | |
| --- | --- |
| **รายละเอียดหลักเกณฑ์** | **ข้อคิดเห็น/ข้อเสนอแนะ** |
| **หมวดที่ 1**  **ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ**  2. ผู้รับใบอนุญาตต้องต้องจัดให้มีโครงสร้างและบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และสอดคล้องตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (Three line of defense) สำหรับการทำหน้าที่ดังนี้  ระดับ 1 : การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ  ระดับ 2 : การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ  ระดับ 3 : การตรวจสอบด้านเทคโนโลยีสารสนเทศ  โดยมีบุคลากรระดับสูงทำหน้าที่ในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องตามลักษณะการให้บริการ ปริมาณธุรกรรม และความซับซ้อนทางเทคโนโลยีอย่างมีประสิทธิภาพ ... |  |
| **หมวดที่ 2**  **นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security policy)**   1. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยครอบคลุมหัวข้ออย่างน้อยดังต่อไปนี้    1. การบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ (IT asset management)   ผู้รับใบอนุญาตต้องบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม ครอบคลุม การจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การบำรุงรักษาทรัพย์สินอย่างสม่ำเสมอ การยกเลิกและเรียกคืนทรัพย์สิน โดยทะเบียนรายการสินทรัพย์ด้านเทคโนโลยีสารสนเทศต้องมีการระบุฮาร์ดแวร์ (hardware) ซอฟต์แวร์ (software) ข้อมูลที่ถือครอง รวมถึงการจัดประเภทและระดับความสำคัญของข้อมูล และเจ้าของทรัพย์สิน (owner) เป็นอย่างน้อย นอกจากนี้ ต้องมีการวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support) จากผู้ผลิตด้วย |  |
| * 1. การพัฒนาระบบ (system development)   ผู้รับใบอนุญาตต้องนำมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศไปใช้ตลอดวงจรการพัฒนาระบบ โดยอย่างน้อยมีการดำเนินการดังต่อไปนี้   * + - 1. มีเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) ซึ่งครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ       2. มีกระบวนการควบคุมเวอร์ชันของการพัฒนาระบบ       3. มีการแบ่งแยกบาทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ       4. มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และ การทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production)       5. มีแนวทางการควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ       6. ทดสอบระบบก่อนการใช้งานจริง โดยครอบคลุมการทดสอบตามความต้องการของหน่วยงานธุรกิจ ด้านประสิทธิภาพ และด้านความมั่นคงปลอดภัยเป็นอย่างน้อย       7. การจัดการข้อผิดพลาดหรือข้อบกพร่องของระบบที่พบในการทดสอบหรือเมื่อนำไปใช้งานจริง       8. มีการสร้างความตระหนักและให้ความรู้กับผู้พัฒนาโปรแกรมอย่างสม่ำเสมอ เพื่อเสริมสร้างทักษะ ในด้านการออกแบบและพัฒนาโปรแกรมอย่างปลอดภัย |  |
| * 1. การบริหารจัดการเหตุการณ์ไม่พึงประสงค์ (incident management)   ผู้รับใบอนุญาตต้องมีการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์อย่างเหมาะสมและทันท่วงที โดยมีขั้นตอนสำหรับบุคลากรและผู้ใช้งานในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ซึ่งจะครอบคลุมขั้นตอนการตรวจพบเหตุการณ์ การแจ้งเหตุ การพิสูจน์เหตุการณ์ การรายงานเหตุการณ์ การตอบสนองต่อเหตุการณ์ รวมถึงการรวบรวมและจัดเก็บหลักฐานเพื่อการสืบสวน นอกจากนี้ ต้องวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ไม่พึงประสงค์ซ้ำในอนาคต |  |
| 1. การจัดเก็บประวัติกิจกรรม (log)    1. การจัดเก็บประวัติกิจกรรมสำหรับการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนในแต่ละกิจกรรม ให้รวมถึง 2. ประเภทของสิ่งที่ใช้ยืนยันตัวตน 3. ระดับความน่าเชื่อของการยืนยันตัวตน 4. วันที่และเวลาที่ทำการเชื่อมโยงข้อมูลเพื่อออกสิ่งที่ใช้ยืนยันตัวตน |  |
| 10.6 ผู้รับใบอนุญาตต้องทำให้มั่นใจได้ว่าในการจัดเก็บประวัติกิจกรรมต้องดำเนินการให้ครอบคลุมในเรื่องดังต่อไปนี้   * 1. มีการจัดเก็บอย่างมั่นคงปลอดภัย และมีความถูกต้องครบถ้วน   2. ปราศจากการเข้าถึง การแก้ไข และการลบ โดยไม่ได้รับอนุญาต   3. จัดเก็บไม่ต่ำกว่า 3 ปี นับแต่วันที่มีการดำเนินการ   4. ประวัติกิจกรรมที่จัดเก็บต้องไม่มีข้อมูลชีวมิติ |  |
| 1. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ (Cyber Security Incident)    1. ในกรณีที่เกิดหรือคาดว่าจะเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีซึ่งส่งผลกระทบต่อการให้บริการหรือระบบงาน และเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารทราบ ผู้รับใบอนุญาตต้องรายงานมายังสำนักงานทันทีเมื่อเกิดหรือรับทราบปัญหาหรือเหตุการณ์ดังกล่าว และให้แจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง |  |
| 1. การบริหารจัดการบุคคลภายนอก (Third Party Management)    1. ในกรณีที่ผู้รับใบอนุญาตดำเนินการดังต่อไปนี้   (1) ใช้บริการจากผู้ให้บริการด้านเทคโนโลยีสารสนเทศ (IT outsourcing)  (2) เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก  (3) ให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญ หรือเข้าถึงข้อมูลผู้ใช้บริการของระบบให้บริการ  ผู้รับใบอนุญาตต้องกำกับดูแลกระบวนการบริหารความเสี่ยง และการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบุคคลภายนอกให้อยู่ในระดับที่สอดคล้องกับระดับความเสี่ยงของการดำเนินงานของผู้รับใบอนุญาต โดยพิจารณาดำเนินการตามแนวปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยงบุคคลภายนอกที่สำนักงานจัดทำขึ้น ทั้งนี้ สามารถพิจารณาประยุกต์ใช้ให้เหมาะสมและสอดคล้องตามขอบเขต ระดับความเสี่ยงและนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของบุคคลภายนอก   * 1. ในการบริหารจัดการบุคคลภายนอกเพื่อควบคุมให้มีการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่เหมาะสม ต้องมีการดำเนินการอย่างน้อย ดังนี้  1. ระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลหรือระบบเทคโนโลยีสารสนเทศที่บุคคลภายนอกสามารถเข้าถึง และกำหนดแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยง 2. การรักษาความมั่นคงปลอดภัยระบบสารเทศของบุคคลภายนอกต้องสอดคล้องกับมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของผู้รับใบอนุญาต 3. กำหนดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รวมถึงข้อกำหนด การไม่เปิดเผยข้อมูล เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง กระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของบุคคลภายนอก ในข้อตกลงการให้บริการหรือเงื่อนไขของสัญญากับบุคคลภายนอก 4. ติดตาม ประเมิน และทบทวนผลการปฏิบัติงานของบุคคลภายนอก 5. ให้มีการสื่อสารหรือการฝึกอบรมบุคคลภายนอกที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบให้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยเฉพาะอย่างยิ่งบุคคลภายนอกที่สามารถเข้าถึงระบบสารสนเทศ โดยอย่างน้อยต้องมีการดำเนินการ ดังนี้   (4.1) เผยแพร่หรืออบรมนโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้อง  (4.2) ให้มีการฝึกอบรมหรือสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบอย่างสม่ำเสมอ  12.3 ในกรณีที่ผู้รับใบอนุญาตมีการใช้บริการจากผู้ให้บริการภายนอกเพื่อให้ดำเนินการแทนสำหรับกิจกรรมที่สำนักงานประกาศกำหนด ให้ผู้รับใบอนุญาตปฏิบัติตามหลักเกณฑ์ด้านการใช้บริการจากบุคคลภายนอกที่เกี่ยวกับระบบให้บริการด้วย |  |
| **หมวด 4**  **การคุ้มครองข้อมูลส่วนบุคคล**  **ส่วนที่ 5 การบริหารจัดการข้อมูลชีวมิติ**   * + 1. ในกรณีที่ผู้รับใบอนุญาตมีการเก็บรวบรวมข้อมูลชีวมิติของผู้ใช้บริการ ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล โดยเจ้าของข้อมูลได้รับแจ้งถึงวัตถุประสงค์ของการเก็บรวบรวมและใช้งานข้อมูลชีวมิติอย่างชัดเจน     2. ผู้รับใบอนุญาตจะจัดเก็บข้อมูลชีวมิติได้เฉพาะเพื่อวัตถุประสงค์ดังต่อไปนี้   1. เพื่อประโยชน์ในการใช้บริการระบบให้บริการ   2. เพื่อการปรับปรุง พัฒนา และทดสอบสมรรถนะของระบบให้บริการ      1. ในการจัดเก็บข้อมูลชีวมิติ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยข้อมูลชีวมิติที่ชัดเจน โดยครอบคลุมกระบวนการอย่างน้อย ดังนี้  1. จัดให้มีการเข้ารหัสข้อมูลชีวมิติ 2. จัดเก็บข้อมูลชีวมิติแยกออกจากการเก็บเทมเพลตชีวมิติ และข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ 3. จัดเก็บบนเครือข่ายที่มั่นคงปลอดภัย และรับส่งข้อมูลชีวมิติผ่านช่องทางที่มั่นคงปลอดภัย 4. จำกัดการเข้าถึงข้อมูลชีวมิติเฉพาะบุคลากรผู้รับผิดชอบ    * 1. กรณีที่ต้องมีการแลกเปลี่ยนข้อมูลชีวมิติเพื่อประโยชน์ในการให้บริการระบบให้บริการ ผู้ให้บริการต้องได้รับความยินยอมโดยชัดแจ้งจากผู้ใช้บริการ โดยต้องมีการเข้ารหัสข้อมูลและจัดให้มีการแลกเปลี่ยนข้อมูลผ่านช่องทางที่มีความมั่นคงปลอดภัย      2. ผู้รับใบอนุญาตต้องทำลายข้อมูลชีวมิติเมื่อผู้ใช้บริการเพิกถอนความยินยอมหรือยกเลิกการใช้บริการ โดยต้องดำเนินการให้ครอบคลุมทุกกระบวนการที่มีการเก็บรวบรวม เช่น การทำสำเนา แคช การจัดเก็บชั่วคราวในฐานข้อมูล เป็นต้น รวมถึงกรณีที่มีการว่าจ้างบุคคลภายนอกให้ดำเนินการด้วย      3. ผู้รับใบอนุญาตต้องมีการบันทึกหรือจัดเก็บหลักฐานการทำลายข้อมูลชีวมิติเพื่อประโยชน์ในการตรวจสอบ |  |

| * 1. **(ร่าง) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบให้บริการ** | |
| --- | --- |
| **รายละเอียดหลักเกณฑ์** | **ข้อคิดเห็น/ข้อเสนอแนะ** |
| * + 1. ในกรณีที่เกิดหรือคาดว่าจะเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญที่เกี่ยวกับการทุจริตหรือการฉ้อโกงในระบบให้บริการและเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารทราบ ให้ผู้รับใบอนุญาตรายงานมายังสำนักงานทันทีเมื่อเกิดหรือรับทราบปัญหาหรือเหตุการณ์ดังกล่าว และให้แจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง |  |

| * 1. **(ร่าง) หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ** | |
| --- | --- |
| **รายละเอียดหลักเกณฑ์** | **ข้อคิดเห็น/ข้อเสนอแนะ** |
| **หมวด 3**  **การตรวจประเมินระบบให้บริการ**   1. ภายหลังจากเริ่มประกอบธุรกิจ ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบให้บริการ อย่างน้อยปีละหนึ่งครั้ง ซึ่งครอบคลุมเรื่องดังต่อไปนี้   ~~21.1 หลักเกณฑ์การบริหารและจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล~~   * 1. หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบให้บริการ   2. หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบให้บริการ   3. หลักเกณฑ์ตามลักษณะของการให้บริการ |  |
| 26. ผู้รับใบอนุญาตต้องนำส่งรายงานผลการตรวจประเมินระบบให้บริการต่อสำนักงานตามระยะเวลาที่สำนักงานประกาศกำหนด และสำนักงานอาจร้องขอข้อมูล เอกสาร หรือหลักฐานเพิ่มเติมเพื่อประกอบการตรวจรายงานผลการตรวจประเมินระบบให้บริการได้ |  |
| 1. ในกรณีที่ผู้รับใบอนุญาตประสงค์จะเลิกประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ต้องจัดให้มีการประเมินความเสี่ยงและแผนรองรับการเลิกประกอบธุรกิจ ตามที่คณะกรรมการประกาศกำหนด |  |

| * 1. **(ร่าง) หลักเกณฑ์ตามลักษณะของการให้บริการ** | |
| --- | --- |
| **รายละเอียดหลักเกณฑ์** | **ข้อคิดเห็น/ข้อเสนอแนะ** |
| **หมวด 1**  **บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการยืนยันตัวตน**  **ส่วนที่ 3 การเชื่อมโยงและแลกเปลี่ยนข้อมูล**  12. ผู้รับใบอนุญาตต้องจัดให้มีรายการข้อมูลอัตลักษณ์ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลในระบบให้บริการ โดยต้องมีชุดข้อมูลขั้นต่ำที่สามารถระบุตัวผู้ใช้บริการได้อย่างชัดเจน ประกอบด้วย   1. เลขประจำตัวประชาชน 2. ชื่อ นามสกุล ภาษาไทย 3. ชื่อ นามสกุล ภาษาอังกฤษ (ถ้ามี) 4. วัน เดือน ปี เกิด 5. ที่อยู่ตามบัตรประชาชน |  |
| 14. ห้ามมิให้ผู้รับใบอนุญาตส่งข้อมูลที่ใช้สำหรับการตรวจสอบสถานะของหลักฐานแสดงตนให้กับบุคคลอื่น โดยข้อมูลดังกล่าวได้แก่  (1) เลขคำร้องขอมีบัตรประจำตัวประชาชน  (2) หมายเลขชิปบัตรประจำตัวประชาชน  (3) เลขควบคุมหลังบัตรประชาขน (เลเซอร์ ไอดี (Laser ID)) |  |
| **ส่วนที่ 5 การตรวจสอบประวัติการใช้งาน**   1. ให้ผู้รับใบอนุญาตจัดเก็บข้อมูลประวัติการใช้งานเพื่อประโยชน์ในการสอบทานของผู้ใช้บริการ โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้ผู้ใช้บริการเรียกดูข้อมูลย้อนหลังได้ทันที เป็นระยะเวลาไม่น้อยกว่าหกเดือน โดยอย่างน้อยควรมีข้อมูลที่ผู้ใช้บริการสามารถตรวจสอบได้ ดังต่อไปนี้ 2. ประวัติกิจกรรมของผู้ใช้บริการที่ได้ดำเนินการผ่านบริการของผู้รับใบอนุญาต 3. ประวัติการให้ความยินยอมในการเปิดเผยข้อมูลอัตลักษณ์ |  |

**ส่วนที่ 2 : (ร่าง) หลักเกณฑ์ลำดับรอง ฉบับที่ 6 และ 7**

สำหรับร่างหลักเกณฑ์ลำดับรอง ฉบับที่ 6 และ 7 เป็นร่างหลักเกณฑ์ที่จัดทำเพิ่มเติม ภายใต้ร่างมาตรา 24 แห่ง (ร่าง) พ.ร.ฎ.ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. … จึงขอรับฟังความคิดเห็นและข้อเสนอแนะ ดังนี้

* **เห็นด้วยตามร่างฯ โดยไม่มีข้อคิดเห็น**
* **เห็นด้วยตามร่างฯ โดยมีข้อคิดเห็น/ข้อเสนอแนะเพิ่มเติม**

| * 1. **(ร่าง) หลักเกณฑ์การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหาย และการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ** | |
| --- | --- |
| **รายละเอียดหลักเกณฑ์** | **ข้อคิดเห็น/ข้อเสนอแนะ** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

| * 1. **(ร่าง) หลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจที่เกี่ยวกับระบบให้บริการ** | |
| --- | --- |
| **รายละเอียดหลักเกณฑ์** | **ข้อคิดเห็น/ข้อเสนอแนะ** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |