แนวทางการตรวจประเมิน
ตามประกาศหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

ศูนย์กำกับดูแลและตรวจสอบธุรกิจ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เวอร์ชัน 1.0 | มิถุนายน 2566

ETDA

Version History

Version	Date	Description	Revised By
1.0	มิ.ย. 2566	แนวทางการตรวจประเมินตาม ประกาศ สพธอ. ที่ ธพส. 1/2566 เรื่อง หลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต	ศูนย์กำกับดูแลและตรวจสอบธุรกิจ สพธอ.

สารบัญ

วัตถุประสงค์

ตามที่ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่ ธพส. 1/2566 เรื่อง หลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต มีการกำหนดหลักเกณฑ์การควบคุมดูแลตามลักษณะของการให้บริการในลักษณะของข้อกำหนดแนบท้ายประกาศ ซึ่งผู้ประกอบธุรกิจบริการแต่ละลักษณะต้องปฏิบัติให้สอดคล้องตามหลักเกณฑ์ดังกล่าว โดยการจัดให้มีนโยบายและมาตรการที่จำเป็น รวมถึงมีการกำกับดูแลและดำเนินการให้สอดคล้องตามมาตรการต่างๆ นั้น

สำนักงานจึงจัดทำเอกสารฉบับนี้ขึ้นเพื่อเป็นแนวทางสำหรับให้ผู้ประกอบธุรกิจบริการและผู้ตรวจประเมิน สามารถประยุกต์ใช้กับการดำเนินงานหรือการตรวจประเมินให้เหมาะสมตามลักษณะการให้บริการ ขอบเขตบริการ และระดับความเสี่ยงของการดำเนินธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

ขอบเขตการตรวจประเมิน

ในการพิจารณาเพื่อกำหนดขอบเขตการตรวจประเมินตามหลักเกณฑ์การควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต ต้องพิจารณาให้ครอบคลุมถึงกระบวนการควบคุมภายในขององค์กร เช่น นโยบายระเบียบ แนวปฏิบัติ หรือคู่มือการทำงานที่ควบคุมกิจกรรมขององค์กร กระบวนการทำงานของระบบงานที่เกี่ยวข้องทั้งหมดที่มีความเชื่อมโยงกับระบบการให้บริการ โดยสามารถอาศัยการไหลของข้อมูล (Data Flow) รวมถึงการปฏิบัติงานที่สำคัญของพนักงานที่เกี่ยวข้อง เช่น การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล และการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล เป็นแนวทางในการกำหนดขอบการตรวจประเมินโดยพิจารณาควบคู่กับลักษณะของการประกอบธุรกิจบริการ

ทั้งนี้ ผู้ตรวจสอบสามารถใช้ดุลยพินิจกำหนดขนาดกลุ่มตัวอย่างในการตรวจสอบได้ตามความเหมาะสม โดยพิจารณา ตามปัจจัยต่าง ๆ เช่น ความสำคัญของระบบงานที่นำมาใช้ ความเสี่ยงที่อาจจะเกิดขึ้น ความซับซ้อนของระบบงาน เหตุการณ์ไม่พึงประสงค์ที่อาจเกิดขึ้น รวมถึงสามารถใช้หลักเกณฑ์หรือแนวปฏิบัติที่ดี (Best Practice) ในการสุ่มตัวอย่างได้

คู่มือการใช้งาน

1. ลักษณะบริการตามมาตรา 7 แห่ง พ.ร.ฎ.ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565 มีการใช้คำแทนด้วยอักษรย่อ ดังนี้

ลักษณะบริการ	อักษรย่อ
(1) **บริการพิสูจน์ตัวตน**	IdP 1
(2) **บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน**	IdP 2
(3) **บริการยืนยันตัวตน**	IdP 3
(4) **บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล**	Ex.

2. แนวทางการตรวจประเมินตามข้อกำหนดแนบท้ายประกาศ สพธอ. จัดทำในรูปแบบตาราง ประกอบด้วยข้อมูล ดังนี้
   2.1 การระบุข้อกำหนดแนบท้ายประกาศ สพธอ. พร้อมรายละเอียดแนวทางการตรวจประเมินสำหรับแต่ละข้อกำหนด ทั้งนี้ ในบางข้อกำหนดอาจไม่ได้กำหนดรายละเอียดแนวทางการตรวจประเมินเพิ่มเติม เนื่องจากข้อกำหนดนั้นมีรายละเอียดที่เพียงพอ
   2.2 การพิจารณาข้อกำหนดที่ต้องดำเนินการสำหรับผู้ประกอบธุรกิจตามแต่ละลักษณะบริการ สามารถตรวจสอบได้จากสัญลักษณ์ X ในตารางด้านหน้า
   2.3 สำหรับข้อกำหนดบางส่วนเป็นกรณีที่ต้องปฏิบัติตาม แต่มีข้อสังเกตเพิ่มเติมเกี่ยวกับการนำมาพิจารณาประกอบการตรวจประเมิน เช่น กรณีที่นำมาใช้ประกอบการตรวจประเมินสำหรับบางกิจกรรม หรือกรณีมีข้อสังเกตเกี่ยวกับการดำเนินการตามข้อกำหนดเพิ่มเติม สำนักงานจะระบุเป็นรายละเอียดเพิ่มเติมไว้ในช่องแนวทางการประเมิน

ตัวอย่างตาราง

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X				-- รายละเอียดตามข้อกำหนดแนบท้ายประกาศ --	-- คำอธิบาย --
X	X	X		-- รายละเอียดตามข้อกำหนดแนบท้ายประกาศ --	-- คำอธิบาย --
X	X	X	X	-- รายละเอียดตามข้อกำหนดแนบท้ายประกาศ --	**ใช้ในกรณีการตรวจประเมินความพร้อมสำหรับการขอเริ่มประกอบธุรกิจ**
			X	-- รายละเอียดตามข้อกำหนดแนบท้ายประกาศ --	-- คำอธิบาย --

การตรวจสอบข้อกำหนดที่ต้องดำเนินการ

กรณีที่ต้องปฏิบัติตามข้อกำหนด แต่มีข้อสังเกตเพิ่มเติมเกี่ยวกับการนำมาพิจารณาประกอบการตรวจประเมิน

แนวทางการตรวจประเมินตามข้อกำหนดแนบท้ายประกาศ สพธอ.

ฉบับที่ 2 หลักเกณฑ์การบริหารและจัดการความเสี่ยงในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ฉบับที่ 3 หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ

ฉบับที่ 4 หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

ฉบับที่ 5 หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ

ฉบับที่ 6 หลักเกณฑ์ตามลักษณะของการให้บริการ

ฉบับที่ 7 หลักเกณฑ์การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ

ฉบับที่ 8 หลักเกณฑ์การใช้บริการจากผู้รับดำเนินการแทน

ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 2

หลักเกณฑ์การบริหารและจัดการความเสี่ยงในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	1. ผู้รับใบอนุญาตต้องจัดให้มีนโยบายและมาตรการบริหารจัดการความเสี่ยงซึ่งครอบคลุมความเสี่ยงที่เกี่ยวข้องกับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อประเมินฐานะและผลการดำเนินงาน โดยคำนึงถึงผลกระทบจากความเสี่ยงของการให้บริการเพื่อกำหนดมาตรการและแผนการบรรเทาผลกระทบที่อาจจะเกิดขึ้นอย่างทันท่วงที	1. มีนโยบายที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงสำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งสอดคล้องกับลักษณะการให้บริการ และมีการกำหนดมาตรการที่สอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงดังกล่าว 2. นโยบายได้รับการอนุมัติจากผู้บริหารขององค์กรหรือบุคลากรที่ได้รับมอบหมายหรือคณะกรรมการที่เกี่ยวข้อง 3. มีการสื่อสารนโยบายและมาตรการให้บุคลากรได้รับทราบ 4. มีการทบทวนนโยบายและมาตรการบริการจัดการความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
X	X	X	X	2. ผู้รับใบอนุญาตต้องเข้าใจและตระหนักถึงความเสี่ยงสำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ส่งผลกระทบต่อผู้ที่เกี่ยวข้อง รวมถึงบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมกระบวนการในการบริหารจัดการความเสี่ยง ดังนี้	1. มีการกำหนดบุคลากรผู้รับผิดชอบในการกำกับดูแลการบริหารจัดการความเสี่ยงอย่างชัดเจน และมีการกำหนดหน้าที่ความรับผิดชอบสอดคล้องตามหลักเกณฑ์ที่กำหนด

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				2.1 การระบุความเสี่ยงที่เกี่ยวข้องกับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (risk identification) ตามลักษณะการให้บริการ 2.2 การประเมินความเสี่ยง (risk assessment) ซึ่งครอบคลุมการประเมินความเสี่ยงตั้งต้นและการตรวจสอบความสามารถในการบริหารจัดการความเสี่ยง 2.3 การวัดผลความเสี่ยงกับเกณฑ์การประเมินความเสี่ยง (risk evaluation) 2.4 การลดความเสี่ยงหลังจากการประเมินความเสี่ยงเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (risk treatment) 2.5 การติดตามและรายงานผลความเสี่ยงอย่างต่อเนื่อง (risk monitoring and reporting)	
X	X	X	X	3. ในการระบุความเสี่ยงที่เกี่ยวข้องกับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ต้องดำเนินการให้ครอบคลุมความเสี่ยง 5 ด้าน ได้แก่ 3.1 ความเสี่ยงด้านกลยุทธ์ (strategic risk) หมายถึง ความเสี่ยงของการสูญเสียที่เกิดขึ้นจากการตัดสินใจทางธุรกิจที่ไม่พึงประสงค์ การตัดสินใจทางธุรกิจที่ไม่ดี หรือการไม่ตอบสนองต่อการเปลี่ยนแปลงในอุตสาหกรรมและสภาพแวดล้อมในการดำเนินงาน ทั้งนี้ ความเสี่ยงด้านกลยุทธ์สำหรับผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความคล้ายคลึงกับความเสี่ยงขององค์กรทั่วไป โดยมีปัจจัย	**หมายเหตุ** - สามารถพิจารณากำหนดความเสี่ยงได้ตามความเหมาะสมของลักษณะการประกอบธุรกิจ แต่อย่างน้อยต้องประกอบด้วยความเสี่ยง 5 ด้าน ตามข้อกำหนด

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ที่ต้องคำนึงถึง เช่น นโยบาย แผนกลยุทธ์ และการจัดสรรงบประมาณ อิทธิพลในการตัดสินใจเชิงกลยุทธ์ การบริหารความเสี่ยงในระดับองค์กร 3.2 ความเสี่ยงด้านการปฏิบัติการ (operational risk) หมายถึง ความเสี่ยงที่จะเกิดความเสียหายต่าง ๆ อันเนื่องมาจากความไม่เพียงพอหรือความบกพร่องของกระบวนการควบคุมภายใน บุคลากร และระบบงาน หรือจากเหตุการณ์ภายนอก เช่น ความเสี่ยงจากการฉ้อโกงโดยบุคคลภายในและบุคคลภายนอก ความเสี่ยงจากการขัดข้องหรือหยุดชะงักของระบบงาน ความเสี่ยงจากแนวปฏิบัติเกี่ยวกับผู้ใช้บริการการให้บริการและดำเนินธุรกิจ 3.3 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (information technology risk) หมายถึง ความเสี่ยงของผลลัพธ์ที่ไม่พึงประสงค์ ความเสียหาย การสูญเสีย การละเมิด ความล้มเหลวหรือการหยุดชะงักใด ๆ ที่อาจเกิดขึ้นจากการใช้หรือการพึ่งพาฮาร์ดแวร์คอมพิวเตอร์ ซอฟต์แวร์ อุปกรณ์ ระบบ แอปพลิเคชันและเครือข่าย ความเสี่ยงนี้มักเกี่ยวข้องกับข้อบกพร่องของระบบ ข้อผิดพลาดในการประมวลผล ข้อบกพร่องของซอฟต์แวร์ ข้อผิดพลาดในการทำงาน ความล้มเหลวของฮาร์ดแวร์ ความล้มเหลวของระบบ ความไม่เพียงพอของความจุ ช่องโหว่ของเครือข่าย จุดอ่อนในการควบคุม ข้อบกพร่องด้านความปลอดภัย การโจมตีที่เป็นอันตราย เหตุการณ์การเจาะ	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ระบบ โดยทั่วไปความเสี่ยงด้านเทคโนโลยีสารสนเทศสำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการบริการพิสูจน์และยืนยันตัวตนทางดิจิทัล เช่น ภัยคุกคามทางไซเบอร์ การรั่วไหลของข้อมูล รวมถึงข้อมูลอ่อนไหวซึ่งมักเป็นองค์ประกอบสำคัญในการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล 3.4 ความเสี่ยงด้านชื่อเสียงขององค์กร (reputation risk) หมายถึง ความเสี่ยงที่ทำให้การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้รับผลกระทบทางลบจากสังคม ส่งผลให้สูญเสียชื่อเสียงและความน่าเชื่อถือในการให้บริการ เช่น การเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้ตั้งใจ 3.5 ความเสี่ยงด้านการปฏิบัติตามหลักเกณฑ์ (compliance risk) หมายถึง ความเสี่ยงที่เกิดจากการที่ผู้รับใบอนุญาตไม่สามารถปฏิบัติงานสอดคล้องตามที่กฎหมาย กฎระเบียบหรือมาตรฐานที่เกี่ยวข้องกับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลกำหนด ทั้งนี้รวมถึงมาตรฐานสากลที่กฎหมายหรือกฎระเบียบอ้างถึงด้วย เช่น การไม่ปฏิบัติตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต	
X	X	X	X	4. ผู้รับใบอนุญาตต้องดำเนินการให้สอดคล้องตามแนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของสำนักงาน พร้อมจัดส่งผลการประเมินต่อ	**หมายเหตุ** - รายละเอียดเป็นไปตามหลักเกณฑ์เกี่ยวกับการนำส่งรายงานผลการตรวจประเมินฯ ที่สำนักงานกำหนด

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				สำนักงานตามรูปแบบและระยะเวลาที่สำนักงานกำหนด โดยผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับรองผลการประเมินตนเองก่อนนำส่งต่อสำนักงาน	
X	X	X	X	5. ผู้รับใบอนุญาตต้องจัดให้มีการทบทวนนโยบายและมาตรการบริหารจัดการความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				หมวด 1 **ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ**	
X	X	X	X	1. ผู้รับใบอนุญาตต้องเข้าใจและตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อผู้ที่เกี่ยวข้อง รวมทั้งมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงที่เกี่ยวข้องให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ ซึ่งอย่างน้อยต้องครอบคลุมการดำเนินการและการดูแลด้านต่าง ๆ ดังนี้ 1.1 การพิจารณาเลือกใช้เทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์การประกอบธุรกิจ 1.2 จัดให้มีนโยบายและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ 1.3 กำกับดูแลให้มีการปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการในระบบการให้บริการของตน	1. มีการกำหนดโครงสร้างและบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแลความเสี่ยงเทคโนโลยีสารสนเทศอย่างเหมาะสม โดยสอดคล้องตามหลักการถ่วงดุล (check and balance) และการแบ่งแยกหน้าที่ความรับผิดชอบอย่างชัดเจนระหว่างการทำหน้าที่ดังต่อไปนี้ - การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือคณะกรรมการที่ได้รับมอบหมาย - การกำกับดูแลและบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น คณะกรรมการบริหารความเสี่ยง คณะกรรมการบริหารความเสี่ยงด้านปฏิบัติการ คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือคณะกรรมการที่ได้รับมอบหมาย - การกำกับดูแลการตรวจสอบด้านเทคโนโลยีสารสนเทศ เช่น คณะกรรมการตรวจสอบ หรือคณะกรรมการที่ได้รับมอบหมาย ซึ่งต้องมีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
X	X	X	X	2. ผู้รับใบอนุญาตต้องจัดให้มีโครงสร้างและบทบาทหน้าที่ตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (three lines of defense) สำหรับการทำหน้าที่ดังนี้	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ระดับ 1 : การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ระดับ 2 : การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ระดับ 3 : การตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยมีบุคลากรระดับสูงทำหน้าที่ในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องตามลักษณะของการให้บริการ ปริมาณธุรกรรม และความซับซ้อนทางเทคโนโลยีอย่างมีประสิทธิภาพ ซึ่งบุคคลดังกล่าวต้อง 2.1 เป็นผู้มีความรู้ ประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ 2.2 มีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศของระบบการให้บริการ	2. มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ นโยบายการบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก นโยบายคุ้มครองข้อมูลส่วนบุคคล 3. มีนโยบาย/แนวทางในการพิจารณาเลือกใช้เทคโนโลยีเทคโนโลยีสารสนเทศที่สอดคล้องกับกลยุทธ์การประกอบธุรกิจ และระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ 4. มีการพิจารณาแต่งตั้งบุคลากรผู้รับผิดชอบในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศซึ่งมีคุณสมบัติที่เหมาะสม และมีการกำหนดหน้าที่ความรับผิดชอบสอดคล้องตามหลักเกณฑ์ที่กำหนด
X	X	X	X	3. บุคลากรผู้รับผิดชอบกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมีหน้าที่และความรับผิดชอบอย่างน้อยในเรื่องดังต่อไปนี้ 3.1 จัดให้มีนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งกำกับดูแลให้มีการปฏิบัติตามนโยบายและมาตรการดังกล่าว	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				3.2 จัดให้มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture) ของระบบการให้บริการ 3.3 จัดให้มีนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) รวมถึงบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงขององค์กร 3.4 ดูแลและดำเนินการให้องค์กรมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ 3.5 รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยระบบสารสนเทศและภัยคุกคามทางไซเบอร์ตามที่กฎหมายกำหนด 3.6 ดูแลและส่งเสริมให้บุคลากรในองค์กรมีความรู้และตระหนักรู้เรื่องการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์	
X	X	X	X	4. ผู้รับใบอนุญาตต้องมีการบริหารจัดการบุคลากรที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบการให้บริการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ การกำกับดูแลการปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง และตรวจสอบด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอย่างเหมาะสม โดยต้องมีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้	1. มีกระบวนการคัดเลือก และการบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (human resource security) ตั้งแต่ก่อนบรรจุเป็นพนักงานจนถึงการสิ้นสุดการว่าจ้าง โดยเฉพาะกับบุคลากรที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ 2. มีหลักเกณฑ์ในการคัดเลือกเพื่อบรรจุเป็นพนักงาน โดยเฉพาะกับบุคลากรที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				4.1 ข้อกำหนดหรือเงื่อนไขในการจ้างบุคลากรควรระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอย่างชัดเจน 4.2 มีการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับระบบการให้บริการให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน หรือสิ้นสุดการจ้างงาน รวมทั้งต้องสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงดังกล่าว 4.3 จัดให้มีการฝึกอบรมหรือสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบและการบรรเทาผลกระทบอย่างสม่ำเสมอ	3. มีข้อกำหนดหรือสัญญาจ้างงานเรื่องความรับผิดชอบเกี่ยวกับการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการ รวมถึงสอบทานกฎระเบียบ หรือข้อบังคับระหว่างการปฏิบัติงานของพนักงาน 4. มีการจัดอบรม เพื่อพัฒนาความรู้ความเชี่ยวชาญครอบคลุมพนักงานทั่วทั้งองค์กร ในเรื่อง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง โดยพิจารณาตามความเหมาะสมของพนักงานในแต่ละระดับ 5. มีการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน โดยต้องมีการทบทวนและปรับปรุงข้อมูลให้เป็นปัจจุบันเสมอ และต้องสื่อสารให้ผู้เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลง 6. มีการเสริมสร้างความตระหนัก (awareness program) ให้กับบุคลากรของผู้ให้บริการตั้งแต่ระดับกรรมการผู้บริหาร และพนักงานทุกระดับเกี่ยวกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์
X	X	X	X	5. ผู้รับใบอนุญาตต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการในเรื่องดังต่อไปนี้ 5.1 นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security policy) โดยคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณ	1. มีการจัดทำนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ทั้ง 3 นโยบาย ได้แก่ นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security policy), นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง รวมทั้งความเสี่ยงจากการใช้เทคโนโลยีภายในองค์กร และความเสี่ยงจากกรณีมีการใช้บริการเชื่อมต่อ หรือเข้าถึงข้อมูลจากบุคคลภายนอก 5.2 นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยพิจารณาถึงความเหมาะสมของมาตรการควบคุมที่มีอยู่ในปัจจุบัน และการตอบสนองและการจัดการการเปลี่ยนแปลงที่สำคัญต่อความเสี่ยง ภัยคุกคาม และสภาพแวดล้อมในการปฏิบัติงาน 5.3 นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล (privacy policy)	policy) และ นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล (privacy policy) 2. มีการดำเนินการดังนี้ (1) มีการประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (2) มีการอนุมัติจากผู้บริหาร คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย (3) ช่องทางการสื่อสารนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศว่าสามารถสื่อสารได้ทั่วถึงพนักงานทุกคนและมีประสิทธิภาพ อาทิเช่น สื่อสารผ่านทางอีเมลหรือ Intranet (4) มีการทบทวนและปรับปรุงให้เป็นปัจจุบันอย่างน้อยทุกหนึ่งปี หรือเมื่อมีการปรับเปลี่ยนที่สำคัญ (5) มีการรายงานนโยบายฯ ให้กับผู้บริหารขององค์กรรวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องทราบ 3. มีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security policy) ที่ต้องเผยแพร่นโยบายดังกล่าวสู่สาธารณะ ควรจะครอบคลุม ระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) และระบบเครือข่าย (network system) รวมถึงอุปกรณ์เครือข่าย ตามข้อกำหนด ฉ.3 ข้อ 8

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					4. มีการจัดทำนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) ที่ต้องเผยแพร่นโยบายดังกล่าวสู่สาธารณะ ควรจะประกอบไปด้วย (1) มีการกำหนดประเภทความเสี่ยง และ/หรือรายการความเสี่ยงที่อาจเกิดขึ้นก่อนการนำเทคโนโลยีมาใช้ จากเทคโนโลยีภายในองค์กร จากผู้ให้บริการภายนอก การระบุความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยี และแนวทางการจัดการความเสี่ยง (2) มีการกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สอดคล้องตามหลัก three lines of defense (3) มีกระบวนการหรือขั้นตอนการประเมินและจัดการความเสี่ยงอย่างน้อยครอบคลุมถึงเรื่อง การประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามและทบทวนความเสี่ยง การรายงานผลการบริหารความเสี่ยง (4) มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite) และการอนุมัติระดับความเสี่ยงที่ยอมรับได้จากผู้บริหาร คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายอย่างเป็นลายลักษณอักษร (5) มีการกำหนดรายละเอียดของแต่ละระดับผลกระทบ และโอกาสเกิดเหตุการณ์ (6) มีแนวทางการจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง และระยะเวลาในการจัดการของแต่ละระดับค่าความเสี่ยง

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					(7) มีการกำหนดดัชนีชี้วัดความเสี่ยง รอบการติดตาม และรายงานผลดัชนีชี้วัดความเสี่ยงต่อผู้บริหาร คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย 5. ผู้ตรวจสอบตรวจสอบว่าผู้ให้บริการมีการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล (data privacy policy) ที่ต้องเผยแพร่นโยบายดังกล่าวสู่สาธารณะ ควรจะประกอบไปด้วย (1) ประเภทของข้อมูลส่วนบุคคลที่ผู้ให้บริการเก็บรวบรวม (2) วิธีการได้มาซึ่งข้อมูลส่วนบุคคล (3) วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (4) วิธีการที่ผู้ใช้บริการสามารถเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน รวมทั้งวิธีการในการปรับปรุงหรือแก้ไขข้อมูลส่วนบุคคลดังกล่าว (5) ช่องทางการร้องเรียนและการจัดการเรื่องร้องเรียนกรณีผู้ให้บริการฝ่าฝืนหลักเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคล
X	X	X	X	6. ผู้รับใบอนุญาตต้องสื่อสารและสร้างความตระหนักให้แก่บุคลากรผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่เกี่ยวข้องกับระบบการให้บริการในการปฏิบัติงานประจำวันอย่างเพียงพอและเหมาะสม เพื่อให้บุคลากรเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีอย่างปลอดภัย	1. มีการสื่อสารและสร้างความตระหนักให้แก่บุคลากรผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่เกี่ยวข้องกับระบบให้บริการเกี่ยวกับความเสี่ยงด้านเทคโนโลยีสารสนเทศและการใช้เทคโนโลยีอย่างปลอดภัย

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	7. ผู้รับใบอนุญาตต้องจัดให้มีการทบทวนนโยบายและมาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อการดำเนินการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	1. มีแนวปฏิบัติ/ข้อกำหนดเกี่ยวกับการทบทวนนโยบายฯ ที่ได้กำหนดไว้อย่างน้อยปีละหนึ่งครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
				หมวด 2 **การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (IT security)**	
X	X	X	X	8. ผู้รับใบอนุญาตต้องจัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ซึ่งครอบคลุม ระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) และระบบเครือข่าย (network system) รวมถึงอุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญให้ชัดเจนเป็นลายลักษณ์อักษร ภายใต้หลักการดังต่อไปนี้ 8.1 การรักษาความลับของข้อมูล 8.2 ความถูกต้องเชื่อถือได้ของระบบสารสนเทศ 8.3 การรักษาสภาพความพร้อมใช้งานของระบบการให้บริการ	1. มีการประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ครอบคลุมระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่รองรับระบบงานสำคัญให้ชัดเจนเป็นลายลักษณ์อักษร 2. เนื้อหาของนโยบายจะต้องครอบคลุมหลักการการรักษาความลับข้อมูล ความถูกต้องเชื่อถือได้ของระบบสารสนเทศ และการรักษาสภาพความพร้อมใช้งานของการให้บริการ 3. นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศได้รับการอนุมัติจากผู้บริหารขององค์กร และมีการทบทวนปรับปรุงนโยบายอย่างสม่ำเสมอ
				9. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยครอบคลุมหัวข้ออย่างน้อยดังต่อไปนี้	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	9.1 การบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศ (IT asset management) ผู้รับใบอนุญาตต้องบริหารจัดการสินทรัพย์ด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การบำรุงรักษาทรัพย์สินอย่างสม่ำเสมอ การยกเลิกและเรียกคืนทรัพย์สิน โดยอย่างน้อยทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศต้องมีการระบุฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลที่ถือครอง รวมถึงการจัดประเภทและระดับความสำคัญของข้อมูล และเจ้าของทรัพย์สิน นอกจากนี้ ต้องมีการวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดอายุการใช้งาน หรือสิ้นสุดการให้บริการจากผู้ผลิตด้วย	1.มีการจัดทำทะเบียนทรัพย์สินสารสนเทศ โดยต้องมีทบทวนและอัพเดทอย่างสม่ำเสมอ 2.มีการกำหนดเจ้าของทรัพย์สินในทะเบียนทรัพย์สินสารสนเทศ และผู้รับผิดชอบทรัพย์สิน 3.มีการระบุทรัพย์สินประเภท (hardware) และ ซอฟต์แวร์ (software) 4.มีการจัดประเภทและกำหนดระดับความสำคัญของข้อมูล 5.มีกระบวนการยกเลิกและเรียกคืนทรัพย์สิน 6.มีการบำรุงรักษาทรัพย์สินสารสนเทศอย่างสม่ำเสมอ 7.มีการวางแผนรองรับการใช้ทรัพย์สินสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (end-of- life) หรือสิ้นสุดการให้บริการ (end-of-support)
X	X	X	X	9.2 การรักษาความมั่นคงปลอดภัยของข้อมูล (information security) ผู้รับใบอนุญาตต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล โดยครอบคลุมหัวข้อดังต่อไปนี้ 9.2.1 หลักเกณฑ์การจัดประเภทและระดับความสำคัญของข้อมูล 9.2.2 แนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลที่สอดคล้องตามระดับความสำคัญซึ่งครอบคลุมถึงการ	**Data classification** 1.มีแนวปฏิบัติการจัดชั้นสารสนเทศ (information classification) ที่เหมาะสมตามชั้นความลับและความสำคัญของสารสนเทศขององค์กร โดยต้องสามารถระบุชั้นความลับของข้อมูลได้อย่างชัดเจน 2.มีแนวทางการรักษาความมั่นคงปลอดภัยที่สอดคล้องตามชั้นความลับ ซึ่งรวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูล ระหว่างการรับส่งข้อมูลผ่านเครือข่ายสื่อสาร การจัดเก็บข้อมูลในระบบงานหรือสื่อบันทึกข้อมูลต่าง ๆ 3.มีแนวทางการทำลายข้อมูลที่เหมาะสมกับชั้นความลับ โดยกำหนดหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องในการทำลายข้อมูล

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				กำหนดสิทธิผู้เข้าถึงข้อมูล วิธีการรับส่ง การประมวลผล และการจัดเก็บข้อมูล และการทำลายข้อมูล 9.2.3 การเข้ารหัสลับข้อมูลตามระดับความสำคัญของข้อมูล รวมถึงวิธีการเข้ารหัสข้อมูล และการบริหารจัดการกุญแจเข้ารหัสลับ โดยครอบคลุมทุกขั้นตอนของวงจรการบริหารจัดการกุญแจเข้ารหัสลับ ตลอดจนกระบวน การสร้าง แจกจ่าย จัดเก็บ ใช้งาน การสำรอง เพิกถอน การต่ออายุ รวมถึงการบันทึกและตรวจสอบกิจกรรมที่สำคัญ	4.มีการจัดทำทะเบียนการทำลายข้อมูลสำคัญ โดยระบุผู้รับผิดชอบในการทำลายข้อมูล วันที่ เวลา ชนิดของสื่อบันทึกข้อมูล serial number และวิธีการที่ใช้ทำลายข้อมูล **Cryptography** 1. มีมาตรฐานหรือแนวปฏิบัติการเข้ารหัสข้อมูล (cryptography) ในการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสมตามชั้นความลับและความสำคัญของข้อมูลสารสนเทศ ที่ครอบคลุมถึงขอบเขตความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง วิธีการเข้ารหัสข้อมูล ที่สอดคล้องตามระดับความสำคัญของข้อมูล และการบริหารจัดการกุญแจเข้ารหัส (key management) มาตรฐานการเข้ารหัสที่เชื่อถือได้และเป็นมาตรฐานสากล 2. กำหนดให้มีการเข้ารหัสข้อมูลและช่องทางการสื่อสารที่ใช้รับ-ส่งข้อมูลสำคัญกับหน่วยงานภายนอก 3. มีการบริหารจัดการกุญแจเข้ารหัส โดยมีกระบวนการที่รัดกุมปลอดภัย ครอบคลุมตั้งแต่การสร้าง การติดตั้ง การจัดเก็บ และการยกเลิกกุญแจเข้ารหัสที่ต้องมั่นใจได้ว่าไม่สามารถนำกุญแจกลับมาใช้งานได้อีก 4. มีการทบทวนประสิทธิภาพของวิธีการเข้ารหัสข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานยังคงมีความแข็งแรงเพียงพอในการรักษาความมั่นคงปลอดภัยของข้อมูล
X	X	X	X	9.3 การควบคุมการเข้าถึงสารสนเทศ (access to information)	1. กำหนดนโยบายการเข้าถึงหรือเข้าใช้งานข้อมูล ทรัพย์สินด้านเทคโนโลยีสารสนเทศ และการใช้บริการเครือข่ายสื่อสารขององค์กร

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				9.3.1 ผู้รับใบอนุญาตต้องมีการควบคุมการเข้าถึงสารสนเทศอย่างเหมาะสม โดยอย่างน้อยต้องมีการควบคุมดังต่อไปนี้ (1) จำกัดการเข้าถึงสารสนเทศที่มีความสำคัญ ข้อมูลอัตลักษณ์ และทรัพยากรที่เกี่ยวข้องกับระบบการให้บริการเฉพาะบุคคลที่จำเป็นเท่านั้น (2) ต้องมีกลไกควบคุมและจัดการสิทธิการเข้าถึงระบบปฏิบัติการ ระบบงาน ระบบฐานข้อมูล และระบบเครือข่าย รวมถึงอุปกรณ์ที่เกี่ยวข้องกับระบบการให้บริการ โดยพิจารณาตามความจำเป็น ระดับความเสี่ยง และเป็นไปตามหลักการแบ่งแยกหน้าที่ที่ดี 9.3.2 ในการจัดการการเข้าถึงระบบสารสนเทศซึ่งจัดเก็บสารสนเทศที่มีความสำคัญ ผู้รับใบอนุญาตต้องมีกลไกในการระบุตัวตนที่สามารถแยกแยะผู้ใช้งาน การยืนยันตัวตน และการให้สิทธิในการอนุญาตให้เข้าถึงระบบ 9.3.3 ผู้รับใบอนุญาตต้องจัดให้มีการบันทึกกิจกรรมการเข้าถึงสารสนเทศซึ่งสามารถแยกแยะผู้ใช้งานและสิทธิในการเข้าถึง	โดยกำหนดหน้าที่และความรับผิดชอบของผู้มีสิทธิเข้าใช้งานระบบที่ชัดเจนรวมถึงการกำหนดสิทธิให้แก่บุคคลภายนอกอย่างเป็นลายลักษณ์อักษรให้สอดคล้องและเป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ผู้ให้บริการกำหนด และสอดคล้องตามข้อกำหนดการดำเนินธุรกิจ 2. การเข้าถึงระบบงานขององค์กร ต้องได้รับการตรวจพิสูจน์ตัวตนของผู้ใช้งานก่อนเสมอ และพิจารณาอนุญาตให้ใช้งานระบบเท่าที่จำเป็นดังนี้ (1) การควบคุมการเข้าถึงระบบงานขององค์กร ต้องพิจารณาอนุมัติการเข้าถึงเฉพาะระบบที่มีความจำเป็นต่อผู้ใช้งาน(least privilege) และเป็นไปตามหลักการแบ่งแยกหน้าที่ที่ดี (segregation of duty)เท่านั้น (2) ต้องจัดทำ access matrix ที่เหมาะสมกับความต้องการทางธุรกิจ ความจำเป็นในการใช้งาน และความจำเป็นในการรักษาความมั่นคงปลอดภัยข้อมูล เพื่อเป็นเกณฑ์มาตรฐานในการควบคุมการเข้าใช้งานระบบงานขององค์กร ทั้งนี้ access matrix ต้องได้รับการพิจารณาอนุมัติโดยเจ้าของข้อมูล/ระบบ และ/หรือ ผู้บริหาร และต้องได้รับการทบทวนและปรับปรุงให้ทันสมัยอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบ เช่น การปรับเปลี่ยนเวอร์ชันของระบบ 3. มีการบันทึกกิจกรรมการการเข้าถึงสารสนเทศที่แยกแยะผู้ใช้งานและสิทธิการเข้าถึง

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	9.4 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) ผู้รับใบอนุญาตต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของระบบการให้บริการ บุคลากร และสินทรัพย์ที่เกี่ยวข้อง โดยอย่างน้อยต้องครอบคลุมกรณีดังต่อไปนี้ 9.4.1 การปกป้องทรัพยากรที่สอดคล้องกับระดับการประเมินผลกระทบทางธุรกิจอันเกิดจากการละเมิด การสูญเสีย หรือความเสียหาย โดยการกระทำของมนุษย์ ความขัดข้องของระบบสาธารณูปโภค สภาพแวดล้อมที่ไม่เหมาะสม หรือภัยพิบัติทางธรรมชาติ 9.4.2 การประเมินความเสี่ยงด้านความมั่นคงปลอดภัย การเลือกใช้อุปกรณ์จัดเก็บและพื้นที่มั่นคงปลอดภัย 9.4.3 การควบคุมการเข้าถึงสถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ โดยควรควบคุมให้เข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตตามสิทธิที่ได้รับมอบหมายเท่านั้น 9.4.4 การทำลายทรัพย์สินทางกายภาพอย่างมั่นคงปลอดภัย	1. ตรวจสอบระบบโครงสร้างพื้นฐานหลักที่ให้บริการพิสูจน์และยืนยันตัวตนสำคัญ อย่างน้อยต้องครอบคลุมการดำเนินการดังนี้ 1.1 ความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ พื้นที่ที่เกี่ยวข้องกับเทคโนโลยรสารสนเทศที่สำคัญ 1.2 ตรวจสอบทรัพย์สินสำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย อุปกรณ์รักษาความปลอดภัยเครือข่าย และพื้นที่มั่นคงปลอดภัยถูกจำกัดการเข้าถึงทางกายภาพโดยพิจารณาหัวข้อ ดังนี้ (ก) ประตูและหน้าต่าง (ข) การตรวจตราพื้นที่ (ค) รั้วหรือกำแพง (ง) บันทึกการเข้าออกพื้นที่ (จ) การประกบตามบุคคลจากภายนอก (visitor escort) 2. ตรวจสอบนโยบายและขั้นตอนปฏิบัติ เพื่อตรวจสอบว่าการเข้าถึงพื้นที่สำคัญอนุญาตให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น 3. การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยและเลือกใช้อุปกรณ์จัดเก็บและพื้นที่มั่นคงปลอดภัย 4. ตรวจสอบมาตรการเกี่ยวกับการทำลายทรัพย์สินทางกายภาพอย่างมั่นคงปลอดภัย
X	X	X	X	9.5 การรักษาความมั่นคงปลอดภัยของการสื่อสาร (communications security)	1. มีการจำแนกโซนเครือข่ายสื่อสาร โดยมีการจัดแบ่งเครือข่ายอย่างเหมาะสม คำนึงถึงระดับความสำคัญของระบบงาน ระดับความสำคัญของข้อมูลที่ประมวลผล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่นๆหรือจากภายนอกองค์กร

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ผู้รับใบอนุญาตต้องรักษาความมั่นคงปลอดภัยของการสื่อสารข้อมูล เพื่อให้ข้อมูลที่รับส่งผ่านเครือข่ายมีความมั่นคงปลอดภัย โดยอย่างน้อยต้องมีการดำเนินการ ดังนี้ 9.5.1 การออกแบบเครือข่ายอย่างมั่นคงปลอดภัย 9.5.2 การป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต 9.5.3 การป้องกันการดักรับข้อมูล 9.5.4 การรักษาความถูกต้องของข้อมูลที่รับส่งบนเครือข่าย 9.5.5 การควบคุมและจัดการสิทธิการใช้ระบบสารสนเทศระยะไกล 9.5.6 มาตรการป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก	2. มีการควบคุม และจำกัดให้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงระบบเครือข่ายได้ 3. ฮาร์ดแวร์ที่มีการเชื่อมต่อกับเครือข่าย ควรมีการออกแบบและตั้งค่า firewall โดยแบ่งตามบริการหรือแบ่งตามหน่วยงานที่ใช้บริการ เพื่อให้สามารถตรวจสอบหรือแก้ไขได้ง่ายเพื่อป้องกัน และลดความเสี่ยงที่อาจเกิดขึ้นกับระบบและข้อมูลได้ 4. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล 5. มีการบริหารจัดการบัญชีผู้ใช้งานที่สามารถใช้ระบบสารสนเทศระยะไกล 6. มีมาตรการป้องกันการเชื่อมต่อกับระบบเครือข่ายภายนอก
				9.6 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation security) ผู้รับใบอนุญาตต้องรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศโดยต้องครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้	
X	X	X	X	9.6.1 มีกระบวนการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศอย่างรัดกุม (change management)	1. มีกระบวนการในการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงอย่างรัดกุมและเพียงพอที่เป็นลายลักษณ์อักษร ทั้งการนำระบบขึ้นใช้งานจริง (system deployment) การตั้งค่าระบบ (system configuration)

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					2. มีการควบคุมการเปลี่ยนแปลงอย่างเป็นขั้นตอน มีการแบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) ของผู้ที่เกี่ยวข้องในกระบวนการบริหารจัดการเปลี่ยนแปลง 3. ในการอนุมัติการเปลี่ยนแปลงทุกครั้งต้องจัดทำเป็นลายลักษณ์อักษร ที่รวมถึงการอนุมัติผ่านระบบหรือทางอีเมล โดยผู้ให้บริการต้องจัดเก็บเอกสารหรือหลักฐานที่ทำให้ทราบว่าการเปลี่ยนแปลง (change) ที่เกิดขึ้นได้ผ่านการอนุมัติจากผู้ที่มีอำนาจในการพิจารณาตามสิทธิที่ผู้ให้บริการกำหนด
X	X	X	X	9.6.2 การบริหารจัดการขีดความสามารถของระบบ (capacity management) อย่างเหมาะสม เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอต่อการรองรับการให้บริการ หรือดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต	1.มีกระบวนการบริหารจัดการขีดความสามารถของระบบ (capacity management) ที่เป็นลายลักษณ์อักษร 2.มีการบริหารจัดการขีดความสามารถของระบบ และระบบสาธารณูปโภค ให้สามารถบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอ สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และในอนาคตได้อย่างมีประสิทธิภาพ
X	X	X	X	9.6.3 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยี (endpoint) โดยอย่างน้อยต้องจัดให้มีการควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ การติดตั้งเครื่องมือสำหรับป้องกันภัยจากมัลแวร์ รวมทั้งติดตามให้มีการ	1. มีการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint) โดยควรมีการติดตั้งโปรแกรมป้องกันไวรัส หรือระบบตรวจจับการแฝงตัวของโปรแกรมไม่ประสงค์ดี (malware) หรือการโจมตีด้วยรูปแบบต่างๆ เพื่อป้องกันการรั่วไหลของข้อมูลหรือการเข้าใช้งานจากผู้ที่ไม่ได้รับอนุญาต โดยควรจัดให้มีการปฏิบัติดังนี้

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ปรับปรุงให้เป็นปัจจุบันและเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ	(1) ติดตั้งและเปิดใช้งานโปรแกรมป้องกันมัลแวร์บนระบบปฏิบัติการทั้งหมดที่เสี่ยงต่อการติดมัลแวร์ เช่น window (2) จำกัดไม่ให้ผู้ใช้งานสามารถปิดการทำงานของโปรแกรมได้ (3) ปรับปรุงฐานข้อมูลมัลแวร์ให้เป็นปัจจุบัน อย่างสม่ำเสมอ (4) ตั้งค่าโปรแกรมให้สแกนแบบเรียลไทม์ และ/หรือสแกนอย่างสม่ำเสมอ เช่น อย่างน้อยสัปดาห์ละครั้งสำหรับคอมพิวเตอร์ของผู้ใช้, อย่างน้อยเดือนละครั้งสำหรับเครื่องแม่ข่าย (5) ตั้งค่าโปรแกรมให้สแกนสื่อบันทึกข้อมูลแบบถอดได้โดยอัตโนมัติเมื่อเชื่อมต่อ (6) ใช้งานโปรแกรมป้องกันมัลแวร์ที่สามารถตรวจจับจากพฤติกรรมการใช้งาน (behavior-based) (7) บริหารจัดการโปรแกรมป้องกันมัลแวร์โดยใช้ระบบที่ศูนย์กลาง (8) ติดตามสถานะการปรับปรุงฐานข้อมูลมัลแวร์สำหรับเครื่องแม่ข่ายและคอมพิวเตอร์ (9) มีการควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ โดยพิจาณาจากการจัดทำ system configuration ของ server และ endpoint 2. มีขั้นตอนการจัดการอุปกรณ์สารสนเทศขององค์กร อุปกรณ์ส่วนตัว (bring-your-own-device: BYOD) ที่นำมาใช้ในองค์กร รวมไปถึงอุปกรณ์จัดเก็บข้อมูลแบบพกพา (external hard disk/flash drive) 3. มีมาตรการด้านความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์อื่นๆ เช่น อุปกรณ์ส่วนตัว (bring-your-own-device:

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					BYOD) อุปกรณ์จัดเก็บข้อมูลแบบพกพา (external hard disk/flash drive)
X	X	X	X	9.6.4 การสำรองข้อมูล (data backup) ด้วยวิธีการ เทคโนโลยี และระยะเวลาที่เหมาะสม	1. กำหนดวิธีการ รูปแบบเทคโนโลยี และความถี่ ที่ใช้ในการสำรองข้อมูลที่มีความสอดคล้องกับระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหายตามที่กำหนด (recovery point objective: RPO) รวมทั้งลักษณะและความซับซ้อนของการดำเนินงาน ความต้องการในการใช้งาน 2. มีรายการข้อมูลที่ดำเนินการสำรองข้อมูล 3. แผนปฏิบัติงานการสำรองข้อมูล (data backup) ที่ได้รับอนุมัติจากผู้บริหาร 4. จัดให้มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งาน 5. มีการรายงานผลการสำรองข้อมูล และผลการทดสอบการเรียกคืนชุดข้อมูลที่ได้สำรองไว้
X	X	X	X	9.6.5 การจัดเก็บประวัติกิจกรรม (log) เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการใช้งานระบบหรือข้อมูล	1. มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging) ของเครื่องแม่ข่าย ระบบงาน และอุปกรณ์เครือข่ายที่สำคัญโดยมีระยะเวลาจัดเก็บตามกฎหมายที่เกี่ยวข้องได้กำหนดไว้ และมีการจัดเก็บรักษาความมั่นคงปลอดภัยของข้อมูลบันทึกเหตุการณ์อย่างรัดกุมเพียงพอ ในการป้องกันการเปลี่ยนแปลง แก้ไขหรือทำลาย โดยประเภทขอบ log ที่ควรจัดเก็บมีดังต่อไปนี้ (1) บันทึกของการเข้าถึง และความพยายามทั้งหมดในการเข้าถึง (access log)

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					(2) บันทึกเหตุการณ์ (event log) ซึ่งครอบคลุมกิจกรรมของผู้ใช้ (user activity) เหตุการณ์ด้านความมั่นคงปลอดภัย (security event) ความล้มเหลวหรือผิดพลาดของระบบ (fault and error) (3) จัดเก็บบันทึกกิจกรรมของบัญชีที่มีสิทธิ์ระดับผู้ดูแลระบบ (admin activity log) 2. มีการสอบทานบันทึกการเข้าถึงระบบ (access Log) และบันทึกการดำเนินงาน (activity log) อย่างสม่ำเสมอ เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการใช้งานระบบหรือข้อมูล โดยมีรายละเอียดที่เพียงพอเพื่อสามารถใช้เป็นหลักฐานในการตรวจสอบและระบุตัวผู้กระทำได้
X	X	X	X	9.6.6 การตั้งค่าเทียบเวลา (clock synchronization) ให้ตรงกับแหล่งเทียบเวลาอ้างอิงที่เป็นมาตรฐานสากลในระดับเดียวกันทั้งระบบ	1. ข้อกำหนดภายนอกและภายในสำหรับการซิงโครไนซ์เวลาที่เชื่อถือได้และความถูกต้องควรได้รับการจัดทำเป็นเอกสารและมีการดำเนินการ 2. ควรกำหนดและพิจารณาเวลาอ้างอิงมาตรฐานสำหรับใช้ภายในองค์กรในทุกระบบรวมถึงระบบการจัดการอาคาร ระบบเข้า/ออก และอื่น ๆ ควรใช้แหล่งนาฬิกาที่เชื่อถือได้เพื่อนำมาอ้างอิงสำหรับระบบบันทึก
X	X	X	X	9.6.7 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการและเครื่องมือตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เพื่อให้สามารถ	1. มีมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที	2. มีผู้รับผิดชอบในการประสานงานและแลกเปลี่ยนข้อมูลภัยคุกคามระหว่างหน่วยงานที่เกี่ยวข้องรวมทั้งมีกระบวนการและช่องทางในการรายงาน แลกเปลี่ยน ติดตาม เพื่อป้องกัน รับมือ และแก้ไขภัยคุกคาม 3. มีการติดตามดูแลระบบและการเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติ หรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันท่วงที 4. มีกระบวนการหรือเครื่องมือในการค้นหาหรือรับข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้ เพื่อวิเคราะห์และประเมินภัยคุกคามที่อาจจะเกิดขึ้น โดยครอบคลุมรูปแบบของการโจมตี ความเป็นไปได้ที่จะเกิดเหตุการณ์ภัยคุกคาม รวมถึงวิธีการรับมือหรือป้องกันเพื่อใช้สนับสนุนการรับมือต่อภัยคุกคามทางไซเบอร์
X	X	X	X	9.6.8 การบริหารจัดการช่องโหว่ของระบบ (vulnerability management) ที่เหมาะสม โดยมีการประเมินช่องโหว่ การรายงานผลไปยังผู้รับผิดชอบ ติดตามและจัดการกับช่องโหว่ให้ได้รับการแก้ไขอย่างเพียงพอ โดยขอบเขตการประเมินช่องโหว่ต้องครอบคลุม การประเมินความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรม สำหรับทุกระบบงานตามระดับความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ	1. มีการประเมินช่องโหว่ทางเทคนิคที่เหมาะสมกับระดับความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง 2. ข้อมูลที่ใช้สำหรับการพิจารณาเกี่ยวกับการประเมินช่องโหว่ (1) ขอบเขตการประเมินช่องโหว่ซึ่งครอบคลุมระบบการให้บริการ (2) วิธีการและรายละเอียดสำหรับแต่ละสถานการณ์ของการประเมิน เช่น การทดสอบผ่าน internet การทดสอบผ่านเครือข่ายภายใน (3) เครื่องมือที่ใช้สำหรับการประเมินช่องโหว่ (4) ช่วงเวลาที่ทำการประเมินช่องโหว่

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					(5) มีการกำหนดเกณฑ์การประเมินช่องโหว่ (6) มีกระบวนการหรือเครื่องมือในการประเมินช่องโหว่ ซึ่งมีวัตถุประสงค์และการตั้งค่าเครื่องมือที่เหมาะสมสำหรับการประเมินช่องโหว่ รวมถึงมีการเปรียบเทียบช่องโหว่กับฐานข้อมูลภัยคุกคามสากล เช่น OWASP web security, Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE) เพื่อวิเคราะห์และประเมินภัยคุกคามที่อาจจะเกิดขึ้น (7) ผลการประเมินช่องโหว่ พร้อมคำแนะนำในการแก้ไข (8) มีกระบวนการติดตามและแก้ไขช่องโหว่ของระบบซึ่งสอดคล้องตามเกณฑ์การประเมินช่องโหว่ (9) มีการรายงานในระดับผู้บริหาร คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย ให้พิจารณาและรับทราบถึงเกณฑ์การประเมินช่องโหว่และพิจารณาระดับความรุนแรงของช่องโหว่ที่ยอมรับได้ ผลการประเมิน การติดตามและการแก้ไขที่สอดคล้องตามเกณฑ์การประเมินช่องโหว่
X	X	X	X	9.6.9 การทดสอบการเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญภายในหรือภายนอกที่เป็นอิสระอย่างน้อยปีละหนึ่งครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งมีการรายงานผลไปยังผู้รับผิดชอบติดตามและจัดการกับช่องโหว่ให้ได้รับการแก้ไขอย่างเพียงพอ โดยควรพิจารณาขอบเขตของการทดสอบเจาะ	1. มีการทดสอบเจาะระบบโดยผู้เชี่ยวชาญจากภายในและภายนอก โดยเฉพาะระบบงาน (application) และระบบเครือข่าย (network) ที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (Internet facing) อย่างสม่ำเสมอหรือทุกครั้งที่มีการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ระบบให้ครอบคลุมการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของระบบการให้บริการ โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง ทั้งนี้ ในกรณีที่สำนักงานเห็นว่าผลการทดสอบเจาะระบบมีข้อมูลรายงานหรือวิธีการทดสอบการเจาะระบบไม่ครอบคลุมช่องโหว่สำคัญที่เป็นความเสี่ยงที่ได้รับการยอมรับโดยทั่วไป หรือในกรณีที่สำนักงานเห็นว่าจำเป็นหรือสมควร สำนักงานอาจสั่งให้แต่งตั้งผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระดำเนินการทดสอบเจาะระบบเพิ่มเติมได้	2. มีการรายงานผลไปยังผู้รับผิดชอบ เพื่อติดตามและจัดการช่องโหว่ให้ได้รับการแก้ไขอย่างเพียงพอ 3. ข้อมูลที่ใช้สำหรับการพิจารณาเกี่ยวกับการทดสอบเจาะระบบ (1) บุคลากรผู้ทำการทดสอบการเจาะระบบควรผ่านการรับรองและมีวุฒิบัตรหรือได้รับประกาศนียบัตรที่เกี่ยวข้องกับการทดสอบเจาะระบบ เช่น CISSP (Certified Information Systems Security Professional), CEH(Certified Ethical Hacker), OPST (OSSTMM Professional Security Tester), GIAC Penetration Tester (GPEN), GIAC Security Expert (GSE), Offensive Security Certified Professional (OSCP) (2) ขอบเขตการทดสอบเจาะระบบมีการตั้งเป้าหมายการทดสอบ (scope target) ครอบคลุมการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของระบบการให้บริการ (3) วิธีการและรายละเอียดสำหรับแต่ละสถานการณ์ของการทดสอบ (4) เครื่องมือที่ใช้สำหรับการทดสอบเจาะระบบ ซึ่งมีวัตถุประสงค์และคุณสมบัติในการใช้งานสอดคล้องกับลักษณะการดำเนินการทดสอบ เช่น ตรวจสอบเว็บไซต์ ตรวจสอบ application รวมถึงมีการตั้งค่าเครื่องมือที่เหมาะสมกับการดำเนินการในแต่ละประเภทของการทดสอบ (5) ช่วงเวลาที่ทำการทดสอบ (6) เกณฑ์การทดสอบเจาะระบบ (7) Raw data จากเครื่องมือที่ใช้ในการตรวจสอบ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					(8) ผลลัพธ์ของการทดสอบ พร้อมข้อแนะนำในการแก้ไข (9) มีการสื่อสารหรือรายงานในระดับผู้บริหาร คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย เพื่อพิจารณาและรับทราบผลการดำเนินการทดสอบเจาะระบบ ผลการแก้ไขหรือการยอมรับแนวทางการแก้ไขที่สอดคล้องตามเกณฑ์การทดสอบ
X	X	X	X	9.6.10 การบริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีการกำหนดมาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัยสำหรับระบบ ปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่าย มีกระบวนการควบคุมการตั้งค่าของระบบที่ใช้งานจริง มีการสอบทานการใช้มาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ และมีการทบทวนมาตรฐานการตั้งค่าขั้นต่ำด้านความมั่นคงปลอดภัยอย่างน้อยปีละหนึ่งครั้ง	1.การกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย(security baseline configuration standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ โดยครอบคลุมองค์ประกอบของระบบอย่างน้อย ดังนี้ (1) ระบบปฏิบัติการบนเครื่องแม่ข่ายและเครื่องลูกข่าย เช่น Window, Unix (2) โปรแกรมมิดเดิลแวร์ (middleware) บนเครื่องแม่ข่าย เช่น WebSphere, JBoss, WebLogic, Tomcat, IIS, Nginx (3) โปรแกรมฐานข้อมูลบนเครื่องแม่ข่าย เช่น MS SQL, MySQL, Oracle DB (4) อุปกรณ์เครือข่าย เช่น firewall, switch, router (5) Hypervisor (e.g. VMware ESXi), Containers (e.g. Docker, Kubernetes), Cloud components (e.g. Amazon, Azure, Google, Office365) 2.ตรวจสอบว่ามาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัยคำนึงถึงหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังนี้ (1) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (least access privilege)

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					(2) การแบ่งแยกหน้าที่ (separation of duties) (3) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน (4) การลบบัญชีที่ไม่ได้ใช้ (5) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (removal of compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (vendor support application) รวมถึงการให้บริการเข้าถึงผ่านเว็บที่ไม่จำเป็น (6) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน (7) การป้องกันมัลแวร์ (malware) (8) การปรับปรุงซอฟต์แวร์และแพตช์ (patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม (9) มีการสอบทานการตั้งค่าอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง 3.กรณีมีความจำเป็นต้องตั้งค่าที่ไม่เป็นไปตามเอกสาร minimum baseline standard ควรผ่านกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ
X	X	X	X	9.6.11 การบริหารจัดการการติดตั้งโปรแกรมสำหรับแก้ไขข้อบกพร่อง (patch management) โดยมีกระบวนการควบคุมการติดตั้ง patch ของระบบที่ใช้งานจริง เพื่อให้สามารถติดตั้ง patch ที่สำคัญในการรักษาความมั่นคงปลอดภัยได้อย่างทันการณ์และเหมาะสมตามระดับความเสี่ยง	1.มีการบริหารจัดการ patch (patch management) ของเครื่องแม่ข่ายโดยมีกระบวนการควบคุมการติดตั้ง patch ของระบบที่ใช้งานจริง เพื่อให้สามารถติดตั้ง patch ที่สำคัญในการรักษาความมั่นคงปลอดภัยได้อย่างทันการณ์ ดังนี้ (1) มีการจัดลำดับความสำคัญของช่องโหว่ที่ได้รับการรายงาน เพื่อพิจารณากำหนดระยะเวลาในการแก้ไขที่เหมาะสมสำหรับแต่ละ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					ช่วงโหว่ เช่น ช่องโหว่บนระบบสารสนเทศที่มีความเสี่ยงระดับ critical ต้องแก้ไขภายใน 30 วัน (2) ลำดับความสำคัญของช่องโหว่ อาจพิจารณาจากความเสี่ยงที่มีหรือความรุนแรงของช่องโหว่ เป็นต้น (3) ช่องโหว่และลำดับความสำคัญ (หรือระยะเวลาในการแก้ไข) ได้รับการรายงานไปยังผู้รับผิดชอบในการแก้ไข (สุ่มตรวจหลักฐานการลำดับความสำคัญของช่องโหว่ ว่ามีการดำเนินการตามแนวทางที่องค์กรกำหนด) 2. ตรวจสอบว่ามีการรับข้อมูลช่องโหว่จากช่องทางอย่างน้อย ดังนี้ (1) ผลการประเมินช่องโหว่ (2) ผลการทดสอบเจาะระบบ (3) การรับข่าวสารด้านภัยคุกคามทางไซเบอร์และช่องโหว่ จากแหล่งที่น่าเชื่อถือ 3.ตรวจสอบว่ามีการรับข่าวสารด้านภัยคุกคามทางไซเบอร์และช่องโหว่จากแหล่งที่น่าเชื่อถือ เช่น US-CERT, THAICERT, product vendor, information security forum 4.ตรวจสอบว่ามีขั้นตอนปฏิบัติในการสื่อสารข้อมูลภัยคุกคามทางไซเบอร์และช่องโหว่ใหม่ ๆ ให้ผู้เกี่ยวข้องรับทราบ เพื่อจัดการความเสี่ยงอย่างเหมาะสม 5.ตรวจสอบว่ามีการกำหนดหน้าที่ความรับผิดชอบในการติดตามข่าวสารด้านภัยคุกคามทางไซเบอร์และช่องโหว่ใหม่ ๆ และการสื่อสารให้ผู้เกี่ยวข้องรับทราบ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					6. ตรวจสอบว่ามีการจัดการกับช่องโหว่ให้ได้รับการแก้ไข ด้วยการปิดช่องโหว่ ใช้มาตรการควบคุมทดแทน หรือยอมรับความเสี่ยงพร้อมระบุเหตุผลความจำเป็นอย่างเป็นลายลักษณ์อักษร สำหรับทั้งช่องโหว่บนระบบสารสนเทศและช่องโหว่บนแอปพลิเคชัน 7. ตรวจสอบว่ามีการติดตามการแก้ไขช่องโหว่อย่างเพียงพอ โดย (1) มีกระบวนการติดตามการแก้ไขช่องโหว่ให้เป็นไปตามระยะเวลาที่กำหนด (2) พิจารณากำหนดตัวชี้วัดประสิทธิภาพในการดำเนินการแก้ไขช่องโหว่ 8. สุ่มตรวจหลักฐานการแก้ไขช่องโหว่ ใช้มาตรการควบคุมทดแทน (เช่น change request, rescan report, re-visit pentest report) ว่ามีการดำเนินการภายในระยะเวลาที่เหมาะสมตามนโยบายขององค์กร 9. ตรวจสอบว่ามีขั้นตอนการวิเคราะห์เพื่อระบุสาเหตุ (root cause analysis) ของช่องโหว่ที่เกิดจากโค้ดที่พัฒนา เพื่อการปรับปรุงอย่างต่อเนื่องของทีมพัฒนาระบบ
X	X	X	X	9.7 การพัฒนาระบบ (system development) ผู้รับใบอนุญาตต้องนำมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศไปใช้ตลอดวงจรการพัฒนาระบบ โดยอย่างน้อยมีการดำเนินการดังต่อไปนี้ 9.7.1 มีเอกสารรายละเอียดคุณสมบัติทางเทคนิค ซึ่งครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ 9.7.2 มีกระบวนการควบคุมเวอร์ชันของการพัฒนาระบบ	1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างเป็นลายลักษณ์อักษร โดยคำนึงถึงการรักษาความมั่นคงปลอดภัย ครอบคลุมกระบวนการตั้งแต่จัดทำความต้องการ (requirement) การออกแบบ การพัฒนา และการทดสอบระบบก่อนใช้งานจริง

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				9.7.3 มีการแบ่งแยกบาทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ 9.7.4 มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา และการทดสอบออกจากระบบงานที่ให้บริการจริง 9.7.5 มีแนวทางการควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ 9.7.6 ทดสอบระบบก่อนการใช้งานจริง โดยอย่างน้อยต้องครอบคลุมการทดสอบตามความต้องการของหน่วยงานธุรกิจ ในด้านประสิทธิภาพ และด้านความมั่นคงปลอดภัยเป็นอย่างน้อย 9.7.7 การจัดการข้อผิดพลาดหรือข้อบกพร่องของระบบที่พบในการทดสอบหรือเมื่อนำไปใช้งานจริง 9.7.8 มีการสร้างความตระหนักและให้ความรู้กับผู้พัฒนาโปรแกรมอย่างสม่ำเสมอ เพื่อเสริมสร้างทักษะ ในด้านการออกแบบและพัฒนาโปรแกรมอย่างปลอดภัย	2. มีการสร้างความตระหนักและให้ความรู้กับผู้พัฒนาโปรแกรมอย่างสม่ำเสมอ เพื่อเสริมสร้างทักษะในด้านการออกแบบและพัฒนาโปรแกรมอย่างปลอดภัย (secure software development) 3. กำหนดให้หน่วยงานธุรกิจที่เกี่ยวข้องสอบทานความถูกต้องครบถ้วนตามความต้องการของหน่วยงานธุรกิจ (business requirement) โดยครอบคลุมการรักษาความปลอดภัยตามนโยบายหรือมาตรฐานที่กำหนด (security requirement) และ sign off ก่อนเริ่มออกแบบระบบ 4. ในการออกแบบระบบมีการจัดทำเอกสารรายละเอียดคุณสมบัติทางเทคนิค (technical specification) โดยครอบคลุมการรักษาความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่กำหนด (security specification) รวมทั้งจัดให้มีการสอบทานความถูกต้องครบถ้วนและ sign off จากผู้ที่เกี่ยวข้องก่อนเริ่มพัฒนาระบบ 5. ในการทดสอบการออกแบบระบบมีการจัดทำขอบเขตการทดสอบให้ครอบคลุมฟังก์ชันและเงื่อนไขต่าง ๆ ด้านประสิทธิภาพ ตามความต้องการของหน่วยงานธุรกิจ (business requirement) รวมถึงการควบคุมความมั่นคงปลอดภัยตามนโยบายหรือมาตรฐานที่กำหนด เพื่อเป็นแนวทางการพัฒนาระบบและสอบทานผลการทดสอบก่อนที่จะออกใช้งานจริง (exit criteria) 6. การพัฒนาระบบ (1) มีกระบวนการควบคุมเวอร์ชันของการพัฒนาระบบ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					(2) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ (3) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) (4) มีแนวทางการควบคุมการรักษาความมั่นคงปลอดภัยและความลับของข้อมูลสำคัญที่นำไปใช้ทดสอบระบบ 7. การทดสอบระบบ (1) บทบาทหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในกระบวนการพัฒนาระบบควรเป็นไปตามหลักการ แบ่งแยกหน้าที่อย่างเหมาะสม (segregation of duties) เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่ต้นจนจบกระบวนการ เช่น ควรแยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง (2) มีการทดสอบบนสภาพแวดล้อมใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงของการเปลี่ยนแปลงบนระบบที่ให้บริการจริง (3) การทดสอบระบบที่ได้รับการพัฒนาหรือเปลี่ยนแปลง ควรครอบคลุม การทดสอบ unit test, system and integration test, user acceptance test, performance test, security test ตาม security specification และควรจัดให้มีกระบวนการและเอกสารการ sign off ผลการทดสอบระบบจากฝ่ายงานที่เกี่ยวข้อง (4) มีกระบวนการสอบทาน test scenario หรือ test case

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					(5) มีการสอบทานคำสั่งในการเขียนโปรแกรม (source code review) อย่างเป็นอิสระทุกครั้ง (6) มีกระบวนการในการจัดการข้อผิดพลาดหรือข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ เพื่อพิจารณาแนวทางปรับปรุงหรือลดความเสี่ยงหรือผลกระทบของข้อผิดพลาดหรือข้อบกพร่องที่มีต่อความปลอดภัย ความถูกต้องเชื่อถือได้ และความพร้อมใช้ของระบบ (7) มีการจัดทำคู่มือและอบรมผู้ใช้งานระบบ เพื่อให้มีความเข้าใจฟังก์ชันการทำงานและมีการใช้งานระบบ อย่างปลอดภัย รวมถึงจัดให้มีคู่มือการดูแลระบบและอบรมผู้ดูแลระบบ เพื่อสามารถตรวจสอบและจัดการแก้ไขปัญหาได้ (8) หลังจากนำระบบขึ้นใช้งานจริง สง. ควรพิจารณาจัดให้มีการทดสอบจริงในวงจำกัด (pilot test) สำหรับฟังก์ชันการทำงานที่สำคัญ (9) ไม่อนุญาตให้นำข้อมูลจริงของผู้ใช้บริการมาใช้งานในการทดสอบการนำระบบขึ้นใช้งานจริง (system deployment) (10)การนำระบบขึ้นใช้งานจริง ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่กำหนดเพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน (11)มีการจัดเก็บการเปลี่ยนแปลง (version control) ของระบบงานขึ้นใช้งานจริงทั้งหมด โดยมีการรักษาความปลอดภัยที่รัดกุมเพียงพอ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					(12)ระบบงานสำรองควรปรับปรุงให้มีความเป็นปัจจุบัน เพื่อให้มีความพร้อมใช้งานเมื่อเกิดเหตุฉุกเฉิน 8. กรณีว่าจ้างบุคลลหรือหน่วยงานภายนอกพัฒนาซอฟต์แวร์ให้ ต้องพิจารณาจัดทำหลักเกณฑ์การพิจารณาคัดเลือกระบบและผู้ให้บริการเพื่อใช้เป็นแนวทางในการปฏิบัติงาน
X	X	X	X	9.8 การบริหารจัดการเหตุการณ์ไม่พึงประสงค์ (incident management) ผู้รับใบอนุญาตต้องมีการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์อย่างเหมาะสมและทันท่วงที โดยมีขั้นตอนสำหรับบุคลากรและผู้ใช้งานในการบริหารจัดการเหตุการณ์ไม่พึงประสงค์ซึ่งจะครอบคลุมขั้นตอนการตรวจพบเหตุการณ์ การแจ้งเหตุ การพิสูจน์เหตุการณ์ การรายงานเหตุการณ์ การตอบสนองต่อเหตุการณ์ รวมถึงการรวบรวมและจัดเก็บหลักฐานเพื่อการสืบสวน นอกจากนี้ ต้องวิเคราะห์สาเหตุที่แท้จริงของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริงและป้องกันไม่ให้เกิดเหตุการณ์ไม่พึงประสงค์ซ้ำในอนาคต	1. มีแนวทางในการบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management) ที่เกิดจากการใช้เทคโนโลยีสารสนเทศ โดยจัดให้มีวิธีปฏิบัติ ขั้นตอนปฏิบัติ หรือแผนรองรับการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ ครอบคลุมขั้นตอนการตรวจพบเหตุการณ์ การแจ้งเหตุ การพิสูจน์เหตุการณ์ การรายงานเหตุการณ์ การตอบสนองต่อเหตุการณ์ รวมถึงการรวบรวมและจัดเก็บหลักฐานเพื่อการสืบสวน 2. มีการบันทึกและวิเคราะห์เหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศ โดยผู้ให้บริการควรวิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ที่เกิดขึ้น 3. มีการรายงานเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศรวมถึงเหตุการณ์ผิดปกติเสนอต่อคณะกรรมการผู้ให้บริการ หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย โดยควรพิจารณาลักษณะของเหตุการณ์ที่ควรรายงานจากระดับของผลกระทบที่เกิดขึ้น

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					4. มีแนวทางในการส่งต่อเหตุการณ์ผิดปกติ (escalation) และรายงานความคืบหน้าเหตุการณ์ผิดปกติให้ผู้เกี่ยวข้อง ผู้บริหารระดับสูง คณะกรรมการชุดย่อยที่ได้รับมอบหมายหรือเกี่ยวข้อง หรือคณะกรรมการผู้ให้บริการโดยพิจารณาให้เหมาะสมสอดคล้องกับระดับความรุนแรงของเหตุการณ์ที่เกิดขึ้น 5. จัดให้มีศูนย์รับแจ้งเหตุหรือบุคลากรที่ทำหน้าที่รับแจ้งเหตุหรือรับรายงานด้านเทคโนโลยีสารสนเทศจากผู้ที่พบหรือสงสัยว่ามีเหตุภัยคุกคามเกิดขึ้นภายในองค์กร และจัดให้มีช่องทางในการรายงาน เช่น อีเมล โทรศัพท์ แบบฟอร์มบนเว็บไซต์ เป็นต้น 6. มีแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติที่แสดงถึงวิธีปฏิบัติเพื่อตอบสนองเมื่อเกิดเหตุการณ์ผิดปกติสอดคล้องและเชื่อมโยงกับแผน BCP ของผู้ให้บริการ ครอบคลุมระบบงานด้านเทคโนโลยีสารสนเทศที่สำคัญ โดยควรได้รับอนุมัติจากคณะกรรมการผู้ให้บริการหรือ คณะกรรมการชุดย่อยที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ 7. มีแผนการสื่อสารภาวะวิกฤต (crisis communication plan) ครอบคลุมการสื่อสารไปยังผู้ที่เกี่ยวข้อง (call tree) รวมทั้งลูกค้าประชาชนที่ได้รับผลกระทบ
X	X	X	X	9.9 การจัดทำแผนการกู้คืนเมื่อเกิดภัยพิบัติ (disaster recovery plan) และการบริหารความต่อเนื่องทางธุรกิจ (business continuity management)	มีการกำหนดแผนการกู้คืนเมื่อเกิดภัยพิบัติ (disaster recovery plan) และแผนการบริหารความต่อเนื่องทางธุรกิจ (business continuity

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				9.9.1 ผู้รับใบอนุญาตต้องจัดทำแผนการกู้คืนเมื่อเกิดภัยพิบัติและแผนการบริหารความต่อเนื่องทางธุรกิจสำหรับระบบการให้บริการโดยคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง ซึ่งครอบคลุมเนื้อหาอย่างน้อยดังต่อไปนี้ (1) การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis - BIA) (2) การกำหนดระยะเวลาในการกู้คืนระบบ (recovery time objective : RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (recovery point objective : RPO) ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (maximum tolerance period of disruption : MTPD) เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (3) แผนและขั้นตอนการกู้คืนระบบ (4) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan : BCP) 9.9.2 ต้องจัดทำคู่มือหรือเอกสารประกอบการดำเนินการตามแผนการกู้คืนเมื่อเกิดภัยพิบัติ และการบริหารความต่อเนื่องทางธุรกิจ รวมทั้งประชาสัมพันธ์และฝึกอบรม	management) สำหรับระบบให้บริการ identity system โดยมีการดำเนินการดังนี้ 1. มีการวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis - BIA) 2. มีการกำหนดระยะเวลาในการกู้คืนระบบ (recovery time objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (recovery point objective: RPO) ที่สอดคล้องกับความสำคัญของระบบ รวมทั้งการกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (maximum tolerance period of disruption : MTPD) 3. มีการกำหนดวิธีการ รูปแบบเทคโนโลยีที่ใช้ในการสำรองข้อมูล และความถี่ในการสำรองข้อมูลสอดคล้องกับเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหายได้ (recovery point objective: RPO) ตามที่กำหนด disaster recovery plan 4. จัดทำแผนการกู้คืนเมื่อเกิดภัยพิบัติ (disaster recovery plan) และแผนการบริหารความต่อเนื่องทางธุรกิจ (business continuity management) ประกอบด้วย (1) ชื่อแผน วัตถุประสงค์ ขอบเขต และความสัมพันธ์กับแผนอื่น ๆ ที่เกี่ยวข้อง (2) ผังโครงสร้างของการบังคับบัญชาในการดำเนินงานตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบ (3) รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม แผนภาพระบบเครือข่ายสื่อสาร เป็นต้น

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				บุคลากรที่เกี่ยวข้องให้มีความเข้าใจและสามารถปฏิบัติตามแผนดังกล่าวได้ 9.9.3 ต้องทบทวนและทดสอบการปฏิบัติตามแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจอย่างน้อยปีละหนึ่งครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ พร้อมทั้งจัดทำรายงานผลการทดสอบ 9.9.4 ต้องจัดให้มีระบบสำรองที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อระบบหลักหยุดชะงัก โดยระบบสำรองควรแยกออกจากระบบหลักในการให้บริการเพียงพอที่จะมิให้เกิดปัญหาหรือได้รับผลกระทบในลักษณะเดียวกันในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง	(4) ขั้นตอนในการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศการตอบสนองต่อเหตุการณ์ ฉุกเฉินและแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบ (5) ขั้นตอนในการดำเนินการกู้คืนระบบ โดยควรระบุรายละเอียดอย่างชัดเจนและเพียงพอ เพื่อให้สามารถใช้เป็น checklist ควบคุมไม่ให้มีการข้ามหรือละเลยขั้นตอนที่กำหนดไว้ (6) ขั้นตอนในการกลับคืนสู่ภาวะปกติ (return to normal) และการประกาศยกเลิกแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (7) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ พร้อมเอกสารประกอบการทำงานภายใต้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรจัดเก็บไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้ในสถานที่ปฏิบัติงานหลักและสำรอง 5. จัดทำคู่มือหรือเอกสารประกอบการดำเนินการตามแผน พร้อมกับประชาสัมพันธ์และฝึกอบรมบุคลากรที่เกี่ยวข้องรับทราบ 6. มีการทบทวนและทดสอบการปฏิบัติตามแผนการกู้คืนเมื่อเกิดภัยพิบัติและการบริหารความต่อเนื่องทางธุรกิจ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญพร้อมทั้งจัดทำรายงานผลการทดสอบ
				10. การจัดเก็บประวัติกิจกรรม (log)	
X	X	X	X	10.1 ผู้รับใบอนุญาตต้องจัดเก็บประวัติกิจกรรมเพื่อประโยชน์ในการตรวจสอบในกรณีอย่างน้อยดังต่อไปนี้	มีการจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์สำหรับกิจกรรมต่างๆ ในกรณีอย่างน้อยดังต่อไปนี้

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				10.1.1 การใช้สิทธิพิเศษของบุคลากรทั้งในกรณีที่ดำเนินการสำเร็จและไม่สำเร็จ 10.1.2 การบริหารจัดการสิทธิผู้ใช้งาน ทั้งในการเพิ่มบัญชีและกลุ่มผู้ใช้งาน การลบ และการแก้ไขสิทธิ 10.1.3 การแจ้งเตือนด้านความมั่นคงปลอดภัยและความผิดพลาด เช่น การปฏิเสธความพยายามเข้าสู่ระบบ การแจ้งเตือนความผิดพลาด 10.1.4 การพยายามเข้าถึงระบบโดยไม่ได้รับอนุญาต	1. การใช้สิทธิพิเศษของบุคลากรทั้งในกรณีที่ดำเนินการสำเร็จและไม่สำเร็จ 2. การบริหารจัดการสิทธิผู้ใช้งาน ทั้งในการเพิ่มบัญชีและกลุ่มผู้ใช้งาน การลบ และการแก้ไขสิทธิ 3. การแจ้งเตือนด้านความมั่นคงปลอดภัยและความผิดพลาด เช่น การปฏิเสธความพยายามเข้าสู่ระบบ การแจ้งเตือนความผิดพลาด 4. การพยายามเข้าถึงระบบและไฟล์ข้อมูลที่มีความสำคัญโดยไม่ได้รับอนุญาต 5. สำหรับการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ต้องจัดเก็บประวัติกิจกรรมเกี่ยวกับการเชื่อมโยงข้อมูลอัตลักษณ์กับอัตลักษณ์ดิจิทัล
X	X	X	X	10.2 ประวัติกิจกรรมที่จัดเก็บสำหรับแต่ละเหตุการณ์ต้องประกอบด้วยข้อมูลเบื้องต้นอย่างน้อยดังต่อไปนี้ 10.2.1 วันที่และเวลาของเหตุการณ์ 10.2.2 ผู้ใช้งาน หรือรหัสบ่งชี้ (identifier) หรือขั้นตอนที่เกี่ยวข้อง 10.2.3 ระบุเฉพาะ (unique identifier) สำหรับแต่ละกิจกรรม 10.2.4 รายละเอียดของเหตุการณ์ 10.2.5 ข้อมูลอื่นอันเป็นประโยชน์ เช่น อุปกรณ์ที่เกี่ยวข้อง	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X				10.3 การจัดเก็บประวัติกิจกรรมสำหรับการพิสูจน์ตัวตนต้องมีการจัดเก็บข้อมูลเพิ่มเติม ได้แก่ ระดับความน่าเชื่อถือของการพิสูจน์ตัวตนในแต่ละกิจกรรม	
	X			10.4 การจัดเก็บประวัติกิจกรรมสำหรับการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนในแต่ละกิจกรรมต้องมีการจัดเก็บข้อมูลเพิ่มเติมดังนี้ 10.4.1 ประเภทของสิ่งที่ใช้ยืนยันตัวตน 10.4.2 ระดับความน่าเชื่อถือของการยืนยันตัวตน 10.4.3 วันที่และเวลาที่ทำการเชื่อมโยงข้อมูลเพื่อออกสิ่งที่ใช้ยืนยันตัวตน	
		X		10.5 การจัดเก็บประวัติกิจกรรมสำหรับการยืนยันตัวตนต้องมีการจัดเก็บข้อมูลเพิ่มเติมดังนี้ 10.5.1 หมายเลขไอพีต้นทางของอุปกรณ์ที่ผ่านการยืนยันตัวตนเข้ามาในระบบการให้บริการ 10.5.2 หมายเลขพอร์ตต้นทางที่ถูกใช้ในการยืนยันตัวตน 10.5.3 หมายเลขไอพีปลายทางที่ถูกใช้ในการยืนยันตัวตน 10.5.4 หมายเลขพอร์ตปลายทางที่ถูกใช้ในการยืนยันตัวตน 10.5.5 user agent string ในกรณีที่มีการใช้งานผ่าน browser	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
			X	10.6 การจัดเก็บประวัติกิจกรรมสำหรับการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลต้องมีการจัดเก็บข้อมูลเพิ่มเติม ดังนี้ 10.6.1 ประเภทของการโต้ตอบ (interaction) 10.6.2 ตัวระบุเฉพาะของการโต้ตอบ (unique interaction identifier) 10.6.3 ชื่อผู้เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตน 10.6.4 ประเภทของข้อมูลอัตลักษณ์ตามคำขอและการตอบกลับ 10.6.5 ระดับความน่าเชื่อถือที่ใช้ในการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามคำขอและการตอบกลับ	
X	X	X	X	10.7 ผู้รับใบอนุญาตต้องทำให้มั่นใจได้ว่าในการจัดเก็บประวัติกิจกรรมต้องดำเนินการให้ครอบคลุมในเรื่องดังต่อไปนี้ 10.7.1 มีการจัดเก็บอย่างมั่นคงปลอดภัยและมีความถูกต้องครบถ้วน 10.7.2 ปราศจากการเข้าถึง การแก้ไข และการลบ โดยไม่ได้รับอนุญาต 10.7.3 จัดเก็บไม่น้อยกว่าหนึ่งปีนับแต่วันที่มีการดำเนินการ 10.7.4 ประวัติกิจกรรมที่จัดเก็บต้องไม่มีข้อมูลชีวมิติ	
				11. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ (Cyber Security Incident)	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	11.1 ผู้รับใบอนุญาตต้องจัดให้มีกลไกหรือกระบวนการในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์อย่างน้อยดังนี้ 11.1.1 ต้องมีกลไกในการตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ รวมถึงจัดให้มีช่องทางที่เป็นการรักษาความลับสำหรับบุคลากรและผู้ใช้งานในการแจ้งเหตุการณ์ที่น่าสงสัยเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ 11.1.2 ต้องจัดให้มีกลไกการเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ ที่มีลักษณะคล้ายกับเหตุการณ์ที่ตรวจพบ หรือที่เกี่ยวข้องกับเหตุการณ์ที่ตรวจพบ และนำข้อมูลที่เกี่ยวกับเหตุการณ์ที่พบมาตรวจสอบกับการลงทะเบียนใหม่และการปรับปรุงข้อมูลของผู้ใช้งานเดิมด้วย โดยจะต้องไม่อนุญาตให้มีการลงทะเบียนใหม่หรือมีการปรับปรุงข้อมูล หากกลไกการควบคุมระบุหรือบ่งชี้ว่าการลงทะเบียนหรือการปรับปรุงข้อมูลดังกล่าวจะก่อให้เกิดเหตุการณ์ด้านความปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ 11.1.3 ต้องมีกระบวนการกำหนดหลักเกณฑ์เกี่ยวกับการตัดสินใจในช่วงที่สำคัญ (critical stage) เพื่อการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์	**หมายเหตุ** - ไม่มีการกำหนดรูปแบบหรือวิธีการไว้เป็นการเฉพาะ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				11.1.4 ต้องมีขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ และมาตรการบรรเทาผลกระทบใด ๆ ให้กับบุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบ เช่น ผู้ใช้บริการ บุคคลภายนอกที่เกี่ยวกับระบบการให้บริการ เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้	
X	X	X	X	11.2 ผู้รับใบอนุญาตต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ และดำเนินการฝึกซ้อม ทบทวน และปรับปรุงแผนอย่างน้อยปีละหนึ่งครั้งเพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤต	1. มีการจัดทำแผนการสื่อสารแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ที่แสดงถึงแผนการสื่อสารภาวะวิกฤต (crisis communication plan) ครอบคลุมการสื่อสารไปยังผู้ที่เกี่ยวข้อง (call tree) รวมทั้งลูกค้าประชาชนที่ได้รับผลกระทบ และวิธีปฏิบัติเพื่อตอบสนองเมื่อเกิดเหตุการณ์ผิดปกติทางไซเบอร์สอดคล้องและเชื่อมโยงกับแผน BCP ของผู้ให้บริการ โดยครอบคลุมระบบงานด้านเทคโนโลยีสารสนเทศที่สำคัญ 2. แผนมีการพิจารณาอนุมัติจากผู้ที่ได้รับมอบหมาย และได้รับฝึกซ้อมทบทวนอย่างเหมาะสม
X	X	X	X	11.3 ผู้รับใบอนุญาตต้องรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี ซึ่งอย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้ 11.3.1 วันที่และเวลาของเหตุการณ์ 11.3.2 จำนวนเหตุการณ์และระดับความรุนแรง	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				11.3.3 มาตรการในการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น	
X	X	X	X	11.4 ในกรณีที่เกิดหรือคาดว่าจะเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีซึ่งส่งผลกระทบต่อระบบการให้บริการ และเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย ผู้รับใบอนุญาตต้องรายงานมายังสำนักงานเมื่อเกิดหรือรับทราบปัญหาหรือเหตุการณ์ดังกล่าวโดยเร็ว และให้แจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง	1. มีกระบวนการบันทึกปัญหาหรือเหตุการณ์ที่มีนัยสำคัญในการใช้เทคโนโลยีที่คาดว่าจะเกิดขึ้นและส่งผลกระทบต่อการให้บริการหรือระบบงาน 2. มีกระบวนการรายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญ หรือเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์ที่คาดว่าจะเกิด เสนอต่อคณะกรรมการผู้ให้บริการ หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย
X	X	X	X	11.5 ผู้รับใบอนุญาตต้องมีกลไกหรือกระบวนรับแจ้งเหตุอันน่าสงสัยเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์	1. มีศูนย์รับแจ้งเหตุหรือบุคลากรที่ทำหน้าที่รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ไม่พึงประสงค์จากผู้ที่พบหรือสงสัยว่ามีเหตุภัยคุกคามเกิดขึ้น 2. จัดให้มีช่องทางในการรายงาน เช่น อีเมล โทรศัพท์ แบบฟอร์มบนเว็บไซต์ โดยอย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้ 1) วันที่และเวลาของเหตุการณ์ 2) จำนวนเหตุการณ์และระดับความรุนแรง 3) มาตรการในการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น 3. มีการสรุปเหตุภัยคุกคามที่น่าสงสัยเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ และมีการรายงานเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ที่ไม่พึงประสงค์ให้กับผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องรับทราบ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					หมายเหตุ - ไม่มีการกำหนดรูปแบบหรือวิธีการไว้เป็นการเฉพาะ
X	X	X	X	11.6 ในกรณีที่เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ก่อให้เกิดผลกระทบกับผู้ใช้บริการ ผู้รับใบอนุญาตต้องมีกระบวนการที่เหมาะสมสำหรับการพิสูจน์ยืนยันตัวตนบุคคลที่เป็นเจ้าของอัตลักษณ์ดิจิทัลหรือสิ่งที่ใช้ยืนยันตัวตนที่อยู่ภายใต้เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ และมีเทคโนโลยีที่เหมาะสมซึ่งสามารถบ่งชี้ถึงการละเมิดอัตลักษณ์ดิจิทัลหรือสิ่งที่ใช้ยืนยันตัวตน	1. มีกระบวนการที่เหมาะสมสำหรับการพิสูจน์ยืนยันตัวตนบุคคลที่เป็นเจ้าของอัตลักษณ์ดิจิทัล หรือสิ่งที่ใช้ยืนยันตัวตน ที่อยู่ภายใต้เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ (cyber security incident) และมีเทคโนโลยีที่เหมาะสมซึ่งสามารถบ่งชี้ถึงการละเมิดอัตลักษณ์ดิจิทัล หรือสิ่งที่ใช้ยืนยันตัวตน 2. มีการป้องกันไม่ให้มีการใช้อัตลักษณ์ดิจิทัล หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการต่อไป ในกรณีที่มีเหตุอันควรสงสัยว่ามีเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ เช่น การใช้เครื่องมือ SIEM เพื่อช่วยให้ทีมรักษาความปลอดภัยกำหนดภัยคุกคามและสร้างการแจ้งเตือนได้ 3. ในกรณีที่ระบุได้ว่าบุคคลใดเป็นผู้ถูกละเมิดภายใต้เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ 1) ผู้ให้บริการพิสูจน์ตัวตน ต้องจัดให้มีการพิสูจน์ซ้ำด้วยการพิสูจน์ยืนยันตัวตนในระดับสูงสุดที่ได้ดำเนินการมาก่อน 2) ผู้ให้บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ต้องจัดให้มีการ verify สิ่งที่ใช้ยืนยันตัวตนในระดับสูงสุดที่ได้ดำเนินการมาก่อน 3) ผู้ให้บริการยืนยันตัวตน ต้องมีการ verify เจ้าของอัตลักษณ์ดิจิทัลหรือสิ่งที่ใช้ยืนยันตัวตนซ้ำ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				12. การบริหารจัดการบุคคลภายนอก (third party management)	
X	X	X	X	12.1 ในกรณีที่ผู้รับใบอนุญาตมีการดำเนินการดังต่อไปนี้ 12.1.1 ใช้บริการจากผู้ให้บริการด้านเทคโนโลยีสารสนเทศ (IT outsourcing) 12.1.2 เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก 12.1.3 ให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญ หรือเข้าถึงข้อมูลผู้ใช้บริการของระบบการให้บริการ ผู้รับใบอนุญาตต้องกำกับดูแลกระบวนการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบุคคลภายนอกให้อยู่ในระดับที่สอดคล้องกับระดับความเสี่ยงของการดำเนินงานของผู้รับใบอนุญาต โดยพิจารณาตามแนวปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยงจากบุคคลภายนอกของสำนักงาน ทั้งนี้ สามารถพิจารณาประยุกต์ใช้ให้เหมาะสมและสอดคล้องตามขอบเขต ระดับความเสี่ยงและนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของบุคคลภายนอก	1. จัดให้มีการกำกับดูแลและการบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก โดยกำหนดนโยบายการบริหารจัดการความเสี่ยง ให้ครอบคลุมความเสี่ยงจากการใช้บริการเป็นลายลักษณ์อักษร และสอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงโดยรวมของผู้ให้บริการ และนโยบายอื่นที่เกี่ยวข้อง เช่น นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) คำนึงถึงขนาด ปริมาณธุรกรรมความซับซ้อนของงานเทคโนโลยีสารสนเทศที่ใช้บริการและความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการ 2. นโยบายดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการผู้ให้บริการหรือคณะกรรมการที่ได้รับมอบหมายและได้รับการทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ 3. มีการสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและควบคุมดูแลให้ปฏิบัติตามนโยบาย 4. ดำเนินการตามแนวปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยงบุคคลภายนอก
X	X	X	X	12.2 ในการบริหารจัดการบุคคลภายนอกเพื่อควบคุมให้มีการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่เหมาะสม ต้องมีการดำเนินการอย่างน้อย ดังนี้	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				12.2.1 ระบุและประเมินความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลหรือระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมต่อกับบุคคลภายนอกหรือบุคคลภายนอกสามารถเข้าถึงได้ และกำหนดแนวทางการจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยง 12.2.2 การรักษาความมั่นคงปลอดภัยระบบสารเทศของบุคคลภายนอกต้องสอดคล้องกับมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของผู้รับใบอนุญาต 12.2.3 ระบุข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รวมถึงข้อกำหนดการไม่เปิดเผยข้อมูลในข้อตกลงการให้บริการหรือเงื่อนไขของสัญญากับบุคคลภายนอก เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึง กระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของบุคคลภายนอก 12.2.4 มีกระบวนการติดตาม ประเมิน และทบทวนผลการปฏิบัติงานของบุคคลภายนอก 12.2.5 มีการสื่อสารหรือการฝึกอบรมบุคคลภายนอกที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบการให้บริการ โดยเฉพาะอย่างยิ่งบุคคลภายนอกที่สามารถเข้าถึงระบบสารสนเทศ อย่างน้อยดังนี้	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				(1) เผยแพร่หรืออบรมนโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้อง (2) มีการฝึกอบรมหรือสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบอย่างสม่ำเสมอ	
X	X	X	X	12.3 ในกรณีที่ผู้รับใบอนุญาตมีการใช้บริการจากผู้รับดำเนินการแทนในการดำเนินการเกี่ยวกับระบบการให้บริการให้ผู้รับใบอนุญาตปฏิบัติตามหลักเกณฑ์การใช้บริการจากผู้รับดำเนินการแทนด้วย	**หมายเหตุ** - พิจารณาตามข้อกำหนดแนบท้ายประกาศ สพธอ. ฉบับที่ 8
				หมวด 3 **การบริหารและการจัดการความเสี่ยงของระบบการให้บริการ** **(IT risk management)**	
X	X	X	X	13. เพื่อให้การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมกระบวนการอย่างน้อยในเรื่องดังต่อไปนี้ 13.1 การประเมินความเสี่ยง (risk assessment) 13.1.1 ระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจจะเกิดขึ้น โดยอย่างน้อยต้องระบุปัจจัยและสาเหตุของ	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ความเสี่ยง ประเภทของความเสี่ยง ผลกระทบต่อการประกอบธุรกิจ 13.1.2 การวิเคราะห์ความเสี่ยงเพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม โดยอย่างน้อยต้องระบุเจ้าของความเสี่ยง การควบคุมที่มีอยู่ในปัจจุบันและวิเคราะห์ผลกระทบที่อาจจะเกิดขึ้น 13.1.3 ประเมินค่าความเสี่ยงโดยกำหนดเกณฑ์การประเมินความเสี่ยงด้านโอกาสและผลกระทบ กำหนดระดับความเสี่ยงที่ยอมรับได้ ประเมินโอกาสของการเกิดความเสี่ยง และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ และนำมาจัดลำดับในการบริหารความเสี่ยง 13.2 การจัดการความเสี่ยง (risk treatment) มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ อยู่ในระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ 13.3 การติดตามและทบทวนความเสี่ยง (risk monitoring and review) มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ โดยกำหนดมาตรการควบคุมด้านการรักษา	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ความมั่นคงปลอดภัยระบบสารสนเทศที่มีอยู่และการจัดการความเสี่ยงอย่างเพียงพอ รวมถึงการตอบสนองและการจัดการการเปลี่ยนแปลงที่สำคัญต่อความเสี่ยงและสภาพแวดล้อมของการปฏิบัติงาน และกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (key risk indicator: KRI) เพื่อใช้ติดตามและทบทวนความเสี่ยง 13.4 การรายงานความเสี่ยง (risk reporting) ต้องมีการรายงานระดับความเสี่ยงและผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย	
X	X	X	X	14. ผู้รับใบอนุญาตต้องจัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญที่อาจส่งผลกระทบต่อการดำเนินการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	
X	X	X	X	15. ในกรณีที่เกิดเหตุการณ์ซึ่งส่งผลกระทบหรือขัดขวางความสามารถของผู้รับใบอนุญาตในการปฏิบัติตามหลักเกณฑ์ที่กำหนด ผู้รับใบอนุญาตต้องดำเนินการดังต่อไปนี้ 15.1 แจ้งให้สำนักงานทราบถึงเหตุการณ์ซึ่งส่งผลให้ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดโดยเร็ว 15.2 บันทึกการตัดสินใจเกี่ยวกับการดำเนินมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่เปลี่ยนแปลงไป และ	1. มีการกำหนดแนวทางหรือกลไกการดำเนินการรองรับ เช่น การกำหนดบุคคลผู้มีอำนาจตัดสินใจในการปรับเปลี่ยนมาตรการ ขั้นตอนการดำเนินการหากมีการปรับเปลี่ยนมาตรการ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				การแก้ไขหรือเยียวยา (ถ้ามี) และนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี 15.3 ผู้รับใบอนุญาตอาจเปลี่ยนแปลงมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศได้ภายในระยะเวลาจำกัดเพื่อรับมือเหตุการณ์ที่เกิดขึ้น ทั้งนี้ การเปลี่ยนแปลงดังกล่าวต้องไม่ทำให้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศสูงกว่าระดับความเสี่ยงที่ยอมรับได้	
				หมวด 4 **การคุ้มครองข้อมูลส่วนบุคคล**	
X	X	X	X	16. ผู้รับใบอนุญาตต้องจัดให้มีนโยบายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ซึ่งสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต โดยต้องมีการเผยแพร่เป็นการทั่วไป	1. องค์กรมีนโยบาย การกำหนดโครงสร้าง และการมอบหมาย แต่งตั้ง หรือกำหนดบุคลากรผู้รับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล 2. มีการสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและควบคุมดูแลให้ปฏิบัติตามนโยบาย
X	X	X	X	17. ผู้รับใบอนุญาตต้องกำหนดบุคลากรที่ทำหน้าที่ในการกำกับดูแลและจัดให้มีการดำเนินงานตามนโยบายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคล	1. มีการแต่งตั้ง/มอบหมายบุคลากรผู้รับผิดชอบในการกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล โดยบุคคลดังกล่าวควรมีประสบการณ์เพียงพอต่อการปฏิบัติงาน 2. พิจารณาบทบาทหน้าที่ของบุคลากรผู้รับผิดชอบ
X	X	X	X	18. นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลต้องมีข้อมูลที่ชัดเจน และประกอบด้วยรายละเอียดอย่างน้อยดังต่อไปนี้ 18.1 ประเภทของข้อมูลส่วนบุคคลที่ผู้รับใบอนุญาตเก็บรวบรวม	1. องค์กรควรที่จะมีการปรับปรุงนโยบายดังกล่าวให้เป็นปัจจุบันอยู่เสมอ และมีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				18.2 วิธีการได้มาซึ่งข้อมูลส่วนบุคคล 18.3 วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล 18.4 วิธีการที่ผู้ใช้บริการสามารถเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน รวมทั้งวิธีการในการปรับปรุงหรือแก้ไขข้อมูลส่วนบุคคลดังกล่าว 18.5 ช่องทางการร้องเรียนและการจัดการเรื่องร้องเรียนกรณีผู้รับใบอนุญาตฝ่าฝืนหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล	2. มีการสื่อสารนโยบายให้ผู้เกี่ยวข้องได้รับทราบอย่างทั่วถึงและควบคุมดูแลให้ปฏิบัติตามนโยบายอย่างเหมาะสม
X	X	X	X	19. ผู้รับใบอนุญาตต้องจัดให้มีการฝึกอบรมหรือสร้างความตระหนักด้านการคุ้มครองข้อมูลส่วนบุคคลแก่บุคลากรที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบการให้บริการก่อนเริ่มปฏิบัติงาน และอย่างน้อยปีละหนึ่งครั้ง ซึ่งครอบคลุมหลักเกณฑ์ของกฎหมายที่เกี่ยวข้อง และนโยบายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้รับใบอนุญาต	1. จัดให้มีทรัพยากรที่เพียงพอเพื่อให้บุคลากรผู้รับผิดชอบ และบุคลากรที่ทำหน้าที่หรือปฏิบัติงานเกี่ยวกับระบบให้บริการ รักษาและพัฒนาความรูความสามารถและความเชี่ยวชาญ อย่างน้อยควรสนับสนุนให้เขารวมประชุม สัมมนา อบรมตาง ๆ โดนเนื้อหาอย่างน้อยต้องครอบคลุมหลักเกณฑ์ของกฎหมายที่เกี่ยวข้อง และนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลของผู้ให้บริการ 2. จัดให้มีการอบรม ให้ความรู้ และความตระหนักถึงความเป็นส่วนตัวแก่บุคลากรในองค์กรทั้งหมดอย่างน้อยปีละ 1 ครั้ง
X	X	X	X	20. ในการจัดทำรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจ ผู้รับใบอนุญาตต้องมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลที่อาจเกิดขึ้นจากระบบการให้บริการ และกำหนดแนวทางในการบริหารจัดการ	1. จัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลนำส่งพร้อมกับการจัดทำรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					ใช้ในกรณีการตรวจประเมินความพร้อม สำหรับการขอเริ่มประกอบธุรกิจ หรือกรณีที่มีการเปลี่ยนแปลงที่สำคัญ ซึ่งต้องประเมินผลกระทบใหม่
X	X	X	X	21. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้ 21.1 ระบุขั้นตอน กระบวนการ กิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในระบบการให้บริการ 21.2 วิเคราะห์ความเสี่ยงของการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต 21.3 วิเคราะห์ผลกระทบของขั้นตอน กระบวนการ กิจกรรมที่ส่งผลต่อการคุ้มครองข้อมูลส่วนบุคคล 21.4 กำหนดแนวทางการจัดการ ควบคุม และป้องกันที่เหมาะสม	1. การระบุขั้นตอน กระบวนการ กิจกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในระบบให้บริการ โดยควรอธิบายรายละเอียดของกระบวนการประมวลผลขอมูลสวนบุคคลอย่างน้อยควรประกอบด้วย การอธิบายขอบเขต วัตถุประสงค์ และวิธีการประมวลผลข้อมูล และการบริหารจัดการข้อมูล 2. วิเคราะห์ความเสี่ยงของการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและหลักเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคล 3. วิเคราะห์ผลกระทบของขั้นตอน กระบวนการ กิจกรรมที่ส่งผลต่อการคุ้มครองข้อมูลส่วนบุคคล ต้องพิจารณาให้สอดคล้องตามระดับความเสี่ยงของการไม่ปฏิบัติตามหลักเกณฑ์ที่เกี่ยวข้อง โดยคำนึงถึงความน่าจะเป็น (likelihood) และความร้ายแรง (severity) ประกอบกัน โดยสามารถออกแบบระดับและความหมายแต่ละระดับได้เองตามความเหมาะสมขององค์กร เช่น ความเสี่ยงสูงเกิดจากการที่ผลกระทบมีความร้ายแรงมาก และมีความน่าจะเป็นที่จะเกิดขึ้นสูงด้วย ทั้งนี้ เป้าหมายหลักการประเมินความเสี่ยงของผลกระทบคือสามารถระบุ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					ถึงความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลที่มีผลต่อผู้ใช้บริการทั้งในเชิงร่างกาย จิตใจ และทรัพย์สิน 4. กำหนดแนวทางการจัดการ ควบคุม และป้องกันที่เหมาะสม โดยควรจะระบุมาตรการเพื่อลดความเสี่ยงดังกลาว โดยควรระบุวามาตรการดังกลาวสามารถลดหรือกำจัดความเสี่ยงไดหรือไม อย่างไร ขอดีและข้อเสียของแตละมาตรการที่เลือกใช และควรไดรับคำปรึกษาจากผู้เชี่ยวชาญ ตัวอย่างเช่น การไมจัดเก็บข่อมูลบางประเภท การเพิ่มมาตรการทางเทคโนโลยีเพื่อความปลอดภัย การแฝงข้อมูลหรือการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ *ใช้ในกรณีการตรวจประเมินความพร้อมสำหรับการขอเริ่มประกอบธุรกิจ หรือกรณีที่มีการเปลี่ยนแปลงที่สำคัญซึ่งต้องประเมินผลกระทบใหม่*
X	X	X	X	22. กรณีที่มีการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อระบบการให้บริการภายหลังจากเริ่มประกอบธุรกิจ ผู้รับใบอนุญาตต้องจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลและนำส่งผลการประเมินพร้อมการแจ้งการเปลี่ยนแปลงต่อสำนักงาน	*ใช้ในกรณีที่มีการเปลี่ยนแปลงที่สำคัญซึ่งต้องประเมินผลกระทบใหม่* **หมายเหตุ** - รายละเอียดเป็นไปตามหลักเกณฑ์เกี่ยวกับการแจ้งการเปลี่ยนแปลงที่สำคัญตามที่สำนักงานประกาศกำหนด

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	23. ผู้รับใบอนุญาตต้องจัดให้มีแผนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคล ซึ่งอย่างน้อยต้องประกอบด้วย 23.1 ขั้นตอนการปฏิบัติเมื่อเกิดหรือสงสัยว่าจะเกิดเหตุการละเมิดข้อมูลส่วนบุคคล การตรวจพบ หรือการรายงาน 23.2 การกำหนดบทบาทหน้าที่และความรับผิดชอบของบุคลากรตามแผนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคล 23.3 แนวทางการสื่อสารข้อมูลเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ซึ่งครอบคลุมการสื่อสารภายใน การแจ้งเตือนผู้ได้รับผลกระทบ และการแจ้งเตือนหรือการรายงานตามกฎหมายที่เกี่ยวข้อง 23.4 แผนการตอบสนองต่อเหตุการละเมิดข้อมูลส่วนบุคคลต้องสอดคล้องกับมาตรการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ และมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	1. มีการจัดเตรียมแผนตอบสนองตอเหตุการณ (incident response plan: IRP) รวมทั้งรายละเอียดของแผน เพื่อให้สามารถตอบสนองตอเหตุการการละเมิดข้อมูลสวนบุคคลได้อย่างเหมาะสม เปนไปตามลำดับขั้นตอนที่กำหนด 2. มีการกำหนดผู้รับผิดชอบ (incident response team) รวมถึงการระบุประเภทหรือลักษณะของเหตุการณ์ดังกล่าวว่ามีการฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัยอย่างไร 3. มีขั้นตอน/กลไกการรายงานเหตุการณ์ที่เกิดขึ้นไปยังบุคคลที่เกี่ยวข้อง ในกรณีที่มีข้อมูลส่วนบุคคลรั่วไหลหรือถูกละเมิดจะต้องพิจารณาหน้าที่แจ้งตามกฎหมาย 4. มีกระบวนการ/กลไกในการประเมินความเสียหายและหาแนวทางที่จะดำเนินการแก้ไขต่อไป การตัดสินใจเพื่อเลือกมาตรการที่จะใช้รับมือเหตุการณ์ดังกล่าว รวมถึงการพิจารณาทบทวนเพื่อปรับปรุงมาตรการ/แนวทางการรักษาความมั่นคงปลอดภัยที่รัดกุมขึ้น 5. มีการจัดทำแผนตอบสนองตอเหตุการณ (incident response plan: IRP) รวมทั้งรายละเอียดของแผน ต้องมีความสอดคล้องกับมาตรการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ (fraud control) และมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ (security control)
X	X	X	X	24. ผู้รับใบอนุญาตจะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเกี่ยวกับพฤติกรรมการใช้งานระบบการให้บริการได้เฉพาะเพื่อวัตถุประสงค์ดังต่อไปนี้	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				24.1 เพื่อการตรวจสอบไอเดนติตี้ของผู้ใช้บริการ และอำนวยความสะดวกให้กับผู้ใช้บริการ 24.2 เพื่อสนับสนุนการจัดการเหตุการณ์การทุจริตหรือฉ้อโกงในระบบการให้บริการ 24.3 เพื่อพัฒนาประสิทธิภาพหรือความสามารถในการให้บริการของระบบการให้บริการ 24.4 เป็นการปฏิบัติตามกฎหมาย	
X	X	X	X	25. ห้ามมิให้ผู้รับใบอนุญาตนำข้อมูลเกี่ยวกับพฤติกรรมการใช้งานตามข้อ 24 ไปขายให้กับบุคคลอื่น	
X	X	X	X	26. ในกรณีที่ผู้รับใบอนุญาตมีการเก็บรวบรวมข้อมูลชีวมิติ ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล โดยเจ้าของข้อมูลได้รับแจ้งถึงวัตถุประสงค์ของการเก็บรวบรวมและใช้งานข้อมูลชีวมิติอย่างชัดเจน	1. มีกระบวนการขอความยินยอมโดยชัดแจ้ง และผู้ใช้บริการได้รับทราบและให้ความยินยอมด้วยตนเอง 2. มีการแจ้งวัตถุประสงค์ให้ผู้ใช้บริการได้รับทราบอย่างชัดเจน
X	X	X	X	27. ผู้รับใบอนุญาตจะจัดเก็บข้อมูลชีวมิติได้เฉพาะเพื่อวัตถุประสงค์ดังต่อไปนี้ 27.1 เพื่อประโยชน์ในการใช้บริการระบบการให้บริการ 27.2 เพื่อการปรับปรุง พัฒนา และทดสอบสมรรถนะของระบบการให้บริการ เว้นแต่เป็นกรณีที่ผู้รับใบอนุญาตต้องปฏิบัติตามที่กฎหมายกำหนด	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	28. ในการจัดเก็บข้อมูลชีวมิติ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยข้อมูลชีวมิติที่ชัดเจน โดยครอบคลุมกระบวนการอย่างน้อย ดังนี้ 28.1 มีการเข้ารหัสข้อมูลชีวมิติ 28.2 จัดเก็บข้อมูลชีวมิติแยกออกจากการเก็บเทมเพลตชีวมิติและข้อมูลเกี่ยวกับอัตลักษณ์ 28.3 จัดเก็บบนเครือข่ายที่มั่นคงปลอดภัย และรับส่งข้อมูลชีวมิติผ่านช่องทางที่มั่นคงปลอดภัย 28.4 จำกัดการเข้าถึงข้อมูลชีวมิติเฉพาะบุคลากรผู้รับผิดชอบ	
X	X	X	X	29. กรณีที่ต้องมีการแลกเปลี่ยนข้อมูลชีวมิติเพื่อประโยชน์ในการใช้งานระบบการให้บริการ ผู้ให้บริการต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล โดยต้องมีการเข้ารหัสข้อมูลและจัดให้มีการแลกเปลี่ยนข้อมูลผ่านช่องทางที่มีความมั่นคงปลอดภัย	1. การแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงาน ควรอยู่ในรูปแบบมาตรฐานสากล ซึ่งกำหนดอยู่ในมาตรฐาน ISO/IEC 19785-1:2020 การแลกเปลี่ยนข้อมูลต้องผ่านช่องทางที่มีความปลอดภัย 2. เมื่อมีการแลกเปลี่ยนข้อมูลชีวมิติระหว่างหน่วยงาน ข้อมูลตัวอย่างชีวมิติต้องถูกเข้ารหัส และข้อมูลที่เข้ารหัสแล้วต้องแยกส่วนกับข้อมูลส่วนบุคคลอื่น ๆ โดยส่งข้อมูลเหล่านี้แยกกันไม่รวมกัน เพื่อป้องกันข้อมูลตัวอย่างชีวมิติใน กรณีที่ข้อมูลอยู่ในระหว่างนำส่งหรือในกรณีที่มีการดักจับข้อมูลระหว่างหน่วยงาน 3. ผู้รับผิดชอบจะเข้าถึงข้อมูลส่วนนี้ได้จะต้องได้รับกุญแจในการถอดรหัสในช่องทางที่มีการรักษาความปลอดภัยข้อมูลสูงสุด
X	X	X	X	30. ผู้รับใบอนุญาตต้องทำลายข้อมูลชีวมิติเมื่อมีการเพิกถอนความยินยอมหรือยกเลิกการใช้บริการ โดยต้องดำเนินการให้ครอบคลุมทุก	1. มีการทำลายข้อมูลชีวมิติเมื่อมีการเพิกถอนความยินยอมหรือยกเลิก โดยต้องดำเนินการลบหรือทำลายข้อมูลอัตลักษณ์ทั้งหมดรวมทั้ง

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				กระบวนการที่มีการเก็บรวบรวม ซึ่งรวมถึงกรณีที่มีการว่าจ้างบุคคลภายนอกให้ดำเนินการด้วย เช่น การทำสำเนา การจัดเก็บชั่วคราวในฐานข้อมูล เว้นแต่เป็นกรณีที่ผู้รับใบอนุญาตต้องปฏิบัติตามที่กฎหมายกำหนด	ข้อมูลชีวมิติ หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
X	X	X	X	31. ผู้รับใบอนุญาตต้องมีการบันทึกหรือจัดเก็บหลักฐานการทำลายข้อมูลชีวมิติเพื่อประโยชน์ในการตรวจสอบ	1. มีการจัดเก็บบันทึกเหตุการณ์ (log) ที่เกี่ยวข้องกับการทำลายข้อมูลชีวมิติ ด้วยวิธีการที่มีความปลอดภัยและมีความเพียงพอต่อการสอบทานย้อนหลัง การตรวจสอบในกรณีเกิดเหตุการณ์ผิดปกติ และการใช้เป็นหลักฐานทางกฎหมาย
X	X	X	X	32. ผู้รับใบอนุญาตต้องได้รับความยินยอมโดยชัดแจ้งจากผู้ใช้บริการก่อนการเปิดเผยข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลดังกล่าวแก่ผู้ที่เกี่ยวข้องกับการใช้งานระบบการให้บริการ	1. มีกระบวนการขอความยินยอมโดยชัดแจ้ง และผู้ใช้บริการได้รับทราบและให้ความยินยอมด้วยตนเอง 2. มีการแจ้งวัตถุประสงค์ให้ผู้ใช้บริการได้รับทราบอย่างชัดเจน
X	X	X	X	33. ผู้รับใบอนุญาตต้องจัดเก็บประวัติกิจกรรม (log) ที่แสดงถึงการได้ความยินยอมโดยชัดแจ้งจากผู้ใช้บริการ รวมถึงข้อมูลดังต่อไปนี้ 33.1 วันที่และวิธีการได้มาซึ่งความยินยอม 33.2 ระยะเวลาของความยินยอม 33.3 เงื่อนไขการให้ความยินยอม 33.4 การถอน หรือการสิ้นอายุความยินยอม	
X	X	X	X	34. การเข้าถึงข้อมูล 34.1 ผู้รับใบอนุญาตต้องจัดให้มีวิธีการที่ให้ผู้ใช้บริการสามารถเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้โดยไม่เสียค่าใช้จ่าย	1. มีขั้นตอนสำหรับการปฏิบัติหนาที่ของผู้ให้บริการเมื่อเจาของขอมูลรองขอ โดยควรประกอบด้วยขั้นตอนอย่างน้อย ดังนี้ สามารถสรุปพอสังเขปไดดังนี้ 1) มีการตรวจสอบตัวตนของผูยื่นคำรองขอ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				34.2 ผู้รับใบอนุญาตต้องตอบรับคำขอเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการภายในสามสิบวันนับแต่ได้รับคำขอ หากผู้รับใบอนุญาตปฏิเสธคำขอ ต้องดำเนินการให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล	2) พิจารณาสิทธิของผู้ขอและความถูกต่องของคำขอ 3) การพิจารณาดำเนินการตามสิทธิที่รองขอ 4) แจงผลการพิจารณาดำเนินการตามสิทธิที่รองขอ 5) มีการจัดเก็บหลักฐานเกี่ยวกับการดำเนินการต่างๆ 2. ต้องจัดหาช่องทางในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยการเข้าถึงนั้นต้องไม่ละเมิดสิทธิความเป็นส่วนตัวของผู้ใช้บริการรายอื่นๆและต้องไม่มีการเรียกเก็บค่าใช้จ่ายใดๆ ต่อผู้ใช้บริการ 3. มีการดำเนินการภายใน 30 วัน นับแต่ได้รับคำขอ หากผู้ให้บริการปฏิเสธคำขอ ต้องดำเนินการให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
X	X	X	X	35. การแก้ไขปรับปรุงข้อมูล 35.1 ผู้รับใบอนุญาตต้องจัดให้ผู้ใช้บริการสามารถแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้ด้วยวิธีการที่เข้าถึงได้โดยง่าย 35.2 ผู้รับใบอนุญาตต้องจัดให้มีคู่มือหรือคำอธิบายสำหรับผู้ใช้บริการเกี่ยวกับวิธีการในการแก้ไขหรือปรับปรุงข้อมูล	1. จะต้องดำเนินการให้ข้อมูลส่วนบุคคลของผู้ใช้บริการถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด โดยอาจกำหนดหลักเกณฑ์ให้ผู้ใช้บริการนำหลักฐานหรือเอกสารที่เกี่ยวข้องมาเพื่อพิสูจน์ยืนยันตัวตน ทั้งนี้ผู้ให้บริการควรดำเนินการอย่างน้อยดังต่อไปนี้ 1) จัดให้ผู้ใช้บริการสามารถแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้ด้วยวิธีการที่เข้าถึงได้โดยง่าย 2) ในกรณีที่ผู้ใช้บริการร้องขอให้ตรวจสอบข้อมูลส่วนบุคคลนั้น ควรจะต้องระงับการประมวลผลข้อมูลดังกล่าว ในระหว่างการตรวจสอบข้อมูลส่วนบุคคล ไม่ว่าผู้ใช้บริการจะใช้สิทธิในการห้ามมิให้ประมวลผลแล้วหรือไม่ก็ตาม

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					3) จัดให้มีระบบหรือขั้นตอนในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลตั้งแต่ขณะที่ได้รับข้อมูลดังกล่าว หรือตรวจสอบในช่วงเวลาอื่นๆ แม้จะยังมิได้มีการร้องขอจากผู้ใช้บริการก็ตาม 4) จัดให้มีบันทึกการร้องขอให้มีการแก้ไขหรือตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลนั้น พร้อมด้วยเหตุผลขอผู้ใช้บริการประกอบ 2. มีการจัดทำคู่มือ/ขั้นตอนสำหรับการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลรองขอในการปรับปรุงข้อมูลส่วนบุคคลที่เกี่ยวกับตนให้เป็นปัจจุบัน และมีการสื่อสาร/อบรมให้บุคลากรที่เกี่ยวข้องรับทราบและปฏิบัติได้อย่างถูกต้อง
X	X	X	X	36. การดูแลคุณภาพของข้อมูลส่วนบุคคล 36.1 ผู้รับใบอนุญาตต้องมีการทบทวนข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยตรวจทานและปรับปรุงข้อมูลที่ใช้สำหรับการพิสูจน์และยืนยันตัวตนให้เป็นปัจจุบัน และดำเนินการอย่างสม่ำเสมอ 36.2 หากผู้รับใบอนุญาตได้จัดให้มีการทบทวนข้อมูลของผู้ใช้บริการแล้ว แต่ไม่สามารถติดต่อผู้ใช้บริการได้ ให้กำหนดมาตรการที่สามารถทบทวนข้อมูลผู้ใช้บริการให้เป็นปัจจุบัน เมื่อผู้ใช้บริการมาทำธุรกรรม หรือในโอกาสแรกที่สามารถติดต่อผู้ใช้บริการได้	1. มีกลไก/มาตรการในการตรวจสอบความถูกต้องและการสอบทานเพื่อปรับปรุงข้อมูลให้เป็นปัจจุบัน ทั้งนี้ จัดให้มีระบบหรือขั้นตอนในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลตั้งแต่ขณะที่ได้รับข้อมูลดังกล่าว หรือตรวจสอบในช่วงเวลาอื่นๆ แม้จะยังมิได้มีการร้องขอ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	37. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการหรือกลไกในการจัดการเรื่องร้องเรียนเกี่ยวกับข้อมูลส่วนบุคคล โดยมีลักษณะอย่างน้อยดังนี้ 37.1 ผู้ใช้บริการสามารถเข้าถึงได้ง่าย มีข้อมูลการติดต่อที่ชัดเจน 37.2 มีกระบวนการจัดการด้วยความเป็นธรรม มีความเป็นกลางและโปร่งใส 37.3 มีขั้นตอนที่ชัดเจน ดำเนินการอย่างทันท่วงที และมีการบรรเทาความเสียหายอย่างเหมาะสม 37.4 มีบุคลากรที่มีความรู้ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการจัดการเรื่องร้องเรียน 37.5 มีกลไกที่สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล	1. มีกระบวนการ/ขั้นตอน/แนวปฏิบัติสำหรับการรับเรื่องร้องเรียน และกรอบระยะเวลาในการดำเนินการตามขั้นตอนต่าง ๆ 2. มีการสื่อสารอย่างชัดเจนถึงวิธีการติดต่อและให้ความช่วยเหลือ เช่น จัดให้มีลิงก์ไปยังคุณลักษณะการบริการตนเองแบบออนไลน์ เซสชันการแชท และหมายเลขโทรศัพท์ของฝ่ายช่วยเหลือ และรับข้อร้องเรียน 3. มีช่องทางที่ผู้ใช้บริการสามารถติดต่อได้ตามวัตถุประสงค์ที่หลักเกณฑ์กำหนด โดยเป็นช่องทางที่มีการแจ้งให้ผู้ใช้บริการทราบเป็นการทั่วไป และช่องทางดังกล่าวต้องสามารถติดต่อสื่อสารกับบุคลากรของผู้รับใบอนุญาตเพื่อขอรับความช่วยเหลือหรือคำแนะนำในการใช้บริการได้ 4. มีระบบบันทึกรายการเกี่ยวกับคำรองขอ เช่น วันที่ได้รับ ผู้ขอ ผู้รับเรื่อง เป็นต้น โดยอาจพิจารณาจัดทำระบบการบันทึกรายการเกี่ยวกับคำรองขอ เช่น การบันทึกให้อยู่ในไฟล์เดียวกับตัวข้อมูลที่ผู้ใช้บริการรองขอ หรือจัดทำเป็นเอกสารหรือระบบการบันทึกแยกจากข้อมูลที่ผู้ใช้บริการองขอ 5. จัดให้มีกลไกในการประสานงานและจัดการข้อร้องเรียน 6. มีคู่มือหรือแนวทางสำหรับบุคลากรเพื่อให้คำแนะนำหรือความช่วยเหลือแก่ผู้ใช้บริการ 7. มีบุคลากรต้องมีความรู้ความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการจัดการเรื่องร้องเรียน

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				หมวด 5 **การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง (IT compliance)**	
X	X	X	X	38. ผู้รับใบอนุญาตต้องปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันการฝ่าฝืนหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง	
				หมวด 6 **การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)**	
X	X	X	X	39. ผู้รับใบอนุญาตต้องจัดให้มีการตรวจสอบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการอย่างน้อยปีละหนึ่งครั้ง รวมทั้งต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเพียงพอ	1. มีการกำหนดบทบาทหน้าที่และแผนงานในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ให้มีผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบของผู้ให้บริการต้องมีความรู้ ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ 2. ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศต้องมีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 4

หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	1. ผู้รับใบอนุญาตต้องมีการกำหนดบุคลากรที่ทำหน้าที่ในการกำกับดูแลการดำเนินงานเกี่ยวกับการควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ รวมถึงรับผิดชอบในการจัดให้มีและดำเนินการตามแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ	1. สอบทานนโยบาย การกำหนดโครงสร้าง และการมอบหมาย แต่งตั้ง หรือกำหนดบุคลากรผู้รับผิดชอบ 2. พิจารณาบทบาทหน้าที่ของบุคลากรผู้รับผิดชอบ
X	X	X	X	2. ผู้รับใบอนุญาตต้องจัดให้มีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้ 2.1 จัดให้มีแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ 2.2 กำหนดระดับความเสี่ยงที่ยอมรับได้สำหรับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ 2.3 จัดให้มีการบริหารความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ 2.4 จัดให้มีมาตรการที่เหมาะสมในการป้องกัน การตรวจจับ และจัดการกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ และดูแลให้มีการดำเนินการตามมาตรการดังกล่าว	1. มีนโยบายซึ่งครอบคลุมเรื่องการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ และมีหลักฐานแสดงให้เห็นถึงการรับทราบ/อนุมัติจากผู้บริหาร 2. มีการบริการจัดการความเสี่ยง และจัดทำแผนป้องกันที่สอดคล้องกับแนวทางการบริหารจัดการความเสี่ยง ซึ่งมีเนื้อหาครอบคลุมเป้าหมาย วัตถุประสงค์ การบริหารจัดการความเสี่ยงการฉ้อโกง และบทบาทหน้าที่ต่าง ๆ 3. สอบทานมาตรการ/แนวปฏิบัติขององค์กรที่เกี่ยวกับการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ 4. การจัดการปัญหาการทุจริตหรือการฉ้อโกงสอดคล้องกับมาตการ/แนวปฏิบัติขององค์กร
X	X	X	X	3. การจัดทำแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบต้องสอดคล้องกับลักษณะการให้บริการและความเสี่ยงของระบบการให้บริการ โดยประกอบด้วยข้อมูลอย่างน้อยดังนี้	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				3.1 เป้าหมายและวัตถุประสงค์ 3.2 กลยุทธ์ในการบริหารจัดการความเสี่ยงจากการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ 3.3 ระดับความเสี่ยงที่ยอมรับได้ 3.4 การระบุภัยคุกคาม ความเสี่ยง และช่องโหว่ที่เกี่ยวข้อง 3.5 ความพร้อมและความสามารถของบุคลากรที่เหมาะสมกับการบริหารจัดการความเสี่ยง 3.6 มาตรการในการควบคุมและจัดการภัยคุกคาม ความเสี่ยง และช่องโหว่ 3.7 การสร้างความตระหนักให้กับบุคลากรที่เกี่ยวข้อง 3.8 การบริหารจัดการ การตรวจสอบ และการรายงานเหตุการณ์ที่เกี่ยวข้องกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ 3.9 การกำหนดโครงสร้าง บทบาท หน้าที่ และความรับผิดชอบของบุคลากรที่เกี่ยวข้องในการดำเนินการตามแผน	
X	X	X	X	4. ผู้รับใบอนุญาตต้องมีการทบทวนแผนการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยยะสำคัญ โดยคำนึงถึงความเหมาะสมของมาตรการที่มีอยู่ในปัจจุบันและความเสี่ยงหรือสภาพแวดล้อมการให้บริการที่เปลี่ยนแปลงไป	1. มีกระบวนการทบทวนแผน/มาตรการป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ 2. มีผลการทบทวน แก้ไข และปรับปรุงแผน/มาตรการฯ ซึ่งได้รับอนุมัติจากผู้บริหาร

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	5. ผู้รับใบอนุญาตต้องมีการบริหารจัดการบุคลากรอย่างเหมาะสม โดยต้องมีการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้ 5.1 จัดให้มีบุคลากรที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและควบคุมการทุจริตหรือฉ้อโกงซึ่งมีคุณสมบัติเหมาะสม โดยมีกระบวนการคัดเลือกบุคคลที่มีความรู้หรือประสบการณ์ที่เหมาะสม และมีปริมาณบุคลากรที่เพียงพอสอดคล้องกับลักษณะการประกอบธุรกิจ 5.2 มีการส่งเสริมและสร้างความตระหนักให้กับบุคลากรที่เกี่ยวข้องให้มีความเข้าใจและตระหนักถึงความเสี่ยงเกี่ยวกับการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ 5.3 จัดให้มีคู่มือหรือขั้นตอนการปฏิบัติงานสำหรับบุคลากรที่เกี่ยวข้อง ในการป้องกัน การตรวจจับ การรายงานและการจัดการกับเหตุการณ์การทุจริตหรือการฉ้อโกง 5.4 มีการอบรมให้ความรู้ที่จำเป็นแก่บุคลากรในองค์กรเกี่ยวกับการป้องกันและควบคุมการทุจริตหรือการฉ้อโกงทั้งก่อนการเริ่มปฏิบัติงานและอย่างน้อยปีละหนึ่งครั้ง	1. การกำหนดโครงสร้างและคุณสมบัติของบุคลากรที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและควบคุมการทุจริตหรือการฉ้อโกงอย่างเหมาะสม 2. มีกระบวนการหรือกลไกในการตรวจสอบทักษะ คุณสมบัติบุคลากรที่สอดคล้องกับความเสี่ยงทางธุรกิจ และตำแหน่งงานที่ได้รับมอบหมาย 3. มีแผนการฝึกอบรมหรือแนวทางการส่งเสริมพัฒนาบุคลากรที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและควบคุมการทุจริตหรือการฉ้อโกง 4. มีคู่มือ/ขั้นตอนการปฏิบัติงานสำหรับบุคลากรที่ปฏิบัติงานเกี่ยวกับการป้องกันและควบคุมการทุจริตหรือการฉ้อโกง และต้องมีการฝึกอบรมก่อนปฏิบัติงาน 5. มีแผนการพัฒนาหรือฝึกอบรมบุคลากรในองค์กรเกี่ยวกับการป้องกันและควบคุมการทุจริตหรือการฉ้อโกง
X	X	X	X	6. ผู้รับใบอนุญาตต้องจัดให้มีคำแนะนำแก่ผู้ใช้บริการอย่างน้อยในเรื่องดังต่อไปนี้ 6.1 การดูแลอัตลักษณ์และข้อมูลคุณลักษณะของตน เพื่อป้องกันการทุจริตหรือการฉ้อโกงที่อาจเกิดขึ้นจากการใช้งานระบบ 6.2 คำแนะนำแก่ผู้ใช้บริการเพื่อหลีกเลี่ยงการหลอกลวงทางอินเทอร์เน็ตอันทำให้ได้ไปซึ่งข้อมูลเกี่ยวกับอัตลักษณ์	1. มีคู่มือ/คำแนะนำเกี่ยวกับวิธีการดูแลข้อมูล การป้องกันตนจากการถูกหลอกลวง ซึ่งรวมถึงการจัดการหรือการรับมือหากข้อมูลรั่วไหล ซึ่งมีการเปิดเผยหรือประชาสัมพันธ์ให้ผู้ใช้บริการทราบ 2. มีช่องทางการติดต่อที่ผู้ใช้บริการสามารถสอบถามหรือขอรับคำแนะนำได้อย่างชัดเจน **หมายเหตุ**

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					- คำแนะนำ/คู่มือ/ช่องทางการติดต่อ สอดคล้องกับข้อกำหนดแนบท้ายประกาศ สพธอ. ฉบับที่ 5 และ 7
X	X	X	X	7. ผู้รับใบอนุญาตต้องมีกลไกในการตรวจจับและเฝ้าระวังเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบอย่างน้อยดังนี้ 7.1 มีกลไกในการตรวจจับเหตุการณ์การทุจริตหรือการฉ้อโกงหรือเหตุที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง รวมถึงจัดให้มีช่องทางที่เป็นการรักษาความลับสำหรับบุคลากรและผู้ใช้งานในการแจ้งเหตุดังกล่าว 7.2 ต้องจัดให้มีกลไกในการเฝ้าระวังเหตุการณ์ที่มีลักษณะคล้ายกับเหตุการณ์ที่ตรวจพบ หรือที่เกี่ยวข้องกับเหตุการณ์ที่ตรวจพบ และนำมาตรวจสอบกับการลงทะเบียนใหม่และการปรับปรุงข้อมูลของผู้ใช้งานเดิม โดยระบบจะต้องไม่อนุญาตให้มีการลงทะเบียนใหม่หรือมีการปรับปรุงข้อมูล หากพบว่าการลงทะเบียนหรือการปรับปรุงข้อมูลมีลักษณะสุ่มเสี่ยงจะก่อให้เกิดเหตุการณ์ทุจริตหรือฉ้อโกง	1. มีกระบวนการ/ขั้นตอนการทำงาน หรือระบบที่นำมาใช้ในการตรวจสอบ/ตรวจจับ/เฝ้าระวัง และจัดการเหตุการณ์ทุจริตหรือฉ้อโกง 2. มีช่องทางสำหรับการรับแจ้งเหตุซึ่งเพียงพอที่จะรักษาความลับสำหรับผู้แจ้งเหตุ และมีการบันทึก/เก็บหลักฐานในการรับแจ้ง 3. ระบบการให้บริการมีกลไกหรือมีความสามารถในการป้องกันการลงทะเบียนใหม่หรือการปรับปรุงข้อมูลหากมีการตรวจพบว่ามีการแจ้งเตือนเกี่ยวกับความผิดปกติของชุดข้อมูลดังกล่าว **หมายเหตุ** - ไม่มีการกำหนดรูปแบบหรือวิธีการไว้เป็นการเฉพาะ
X	X	X	X	8. ผู้รับใบอนุญาตต้องจัดให้มีกลไกในการจัดการเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกงอย่างเหมาะสมและทันท่วงที โดยมีกระบวนการอย่างน้อยดังนี้ 8.1 มีกลไกในการตรวจสอบเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				8.2 ในกรณีที่เกิดเหตุการณ์การทุจริตหรือการฉ้อโกง ต้องมีการบรรเทาผลกระทบจากเหตุการณ์ดังกล่าวอย่างเหมาะสม และพิจารณาจัดการความเสี่ยงที่อาจทำให้เกิดเหตุการณ์ในลักษณะเดียวกันเพื่อไม่ให้เกิดซ้ำ 8.3 มีขั้นตอนการปฏิบัติงานที่กำหนดหลักเกณฑ์การตัดสินใจในช่วงที่สำคัญ (critical stage) เพื่อจัดการเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง 8.4 มีการบันทึกการตัดสินใจเกี่ยวกับการตอบสนอง การดำเนินการหรือกรณีที่ไม่มีการดำเนินการกับเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง 8.5 ต้องมีการรายงานเหตุการณ์การทุจริตหรือการฉ้อโกง หรือเหตุที่น่าจะสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี ซึ่งควรประกอบด้วยข้อมูลอย่างน้อย ดังนี้ 8.5.1 จำนวนเหตุการณ์ 8.5.2 ประเภทและระดับความรุนแรงของเหตุการณ์ 8.5.3 การตัดสินใจเกี่ยวกับการตอบสนอง การดำเนินการ หรือกรณีที่ไม่มีการดำเนินการกับเหตุการณ์ที่น่าสงสัยว่าจะเกิดการทุจริตหรือการฉ้อโกง 8.5.4 การให้ความช่วยเหลือเยียวยาแก่ผู้ที่ได้รับผลกระทบหรืออาจได้รับผลกระทบจากการทุจริตหรือการฉ้อโกง	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	9. ในกรณีที่เกิดหรือคาดว่าจะเกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญที่เกี่ยวกับการทุจริตหรือการฉ้อโกงในระบบให้บริการและเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย ให้ผู้รับใบอนุญาตรายงานมายังสำนักงานเมื่อเกิดหรือรับทราบปัญหาหรือเหตุการณ์ดังกล่าวโดยเร็ว และให้แจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง	1. มีแนวทางการกำหนดระดับความสำคัญของปัญหาที่ต้องรายงานต่อผู้บริหารสูงสุด คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย 2. มีคู่มือ/แนวปฏิบัติในการรายงานต่อผู้บริหารสูงสุด คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย และการแจ้งสำนักงาน
X	X	X	X	10. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการ ช่องทาง และการให้ความช่วยเหลือ เยียวยาแก่ผู้ที่ได้รับผลกระทบหรืออาจได้รับผลกระทบจากการทุจริตหรือการฉ้อโกง อย่างน้อยดังนี้ 10.1 มีช่องทางในการแจ้งเหตุในกรณีที่มีข้อสงสัยว่าอัตลักษณ์ หรือสิ่งที่ใช้ยืนยันตัวตน ของผู้ใช้บริการถูกนำไปใช้งานโดยไม่ชอบ 10.2 ให้ความช่วยเหลือผู้ใช้บริการในกรณีที่อัตลักษณ์ หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการรั่วไหล หรือถูกล่วงรู้โดยบุคคลอื่น 10.3 มีมาตรการป้องกันการใช้งานอัตลักษณ์ และ/หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ เมื่อผู้รับใบอนุญาตมีเหตุสงสัยว่าอาจเกิดการทุจริตหรือการฉ้อโกง 10.4 ในกรณีที่ผู้รับใบอนุญาตตรวจพบหรือผู้เสียหายแจ้งต่อผู้รับใบอนุญาต ว่าบุคคลดังกล่าวเป็นเหยื่อของการทุจริตหรือการฉ้อโกง ผู้รับใบอนุญาตต้องจัดให้มีการพิสูจน์ตัวตนของบุคคลนั้นใหม่ โดยอย่างน้อยต้องใช้ระดับความน่าเชื่อถือในการพิสูจน์ตัวตนที่เทียบเท่าหรือสูงกว่ากระบวนการที่เคยทำไว้	1. มีขั้นตอน/กระบวนการในการรับแจ้ง การจัดการ และการเยียวยาความเสียหาย/ผลกระทบที่เกิดขึ้นกับผู้ใช้บริการ 2. มีช่องทางที่ผู้ใช้บริการสามารถติดต่อได้ตามวัตถุประสงค์ที่หลักเกณฑ์กำหนด โดยเป็นช่องทางที่มีการแจ้งให้ผู้ใช้บริการทราบเป็นการทั่วไป 3. มีเอกสาร/คู่มือ/คำแนะนำสำหรับผู้ใช้บริการ เกี่ยวกับขั้นตอนและวิธีการในการแจ้งเหตุ/การดำเนินการเมื่อเกิดเหตุตามวัตถุประสงค์ที่กำหนด 4. มีการกำหนดแนวปฏิบัติหรือขั้นตอนการดำเนินการในการตรวจสอบตัวตนใหม่ตามระดับความน่าเชื่อถือที่กำหนด

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	11. ในกรณีที่เกิดเหตุการณ์ซึ่งส่งผลกระทบหรือขัดขวางความสามารถของผู้รับใบอนุญาตในการปฏิบัติตามหลักเกณฑ์ที่กำหนด ผู้รับใบอนุญาตต้องพิจารณาดำเนินการดังต่อไปนี้ 11.1 แจ้งให้สำนักงานทราบถึงเหตุการณ์ซึ่งส่งผลให้ไม่สามารถปฏิบัติตามหลักเกณฑ์ที่กำหนดโดยเร็ว 11.2 บันทึกการตัดสินใจเกี่ยวกับการบริหารจัดการการทุจริตหรือฉ้อโกงจากการใช้งานระบบ และการแก้ไขหรือเยียวยา (ถ้ามี) โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี 11.3 ผู้รับใบอนุญาตอาจเปลี่ยนแปลงการบริหารจัดการการทุจริตหรือฉ้อโกงจากการใช้งานระบบได้ภายในระยะเวลาจำกัดเพื่อรับมือเหตุการณ์ที่เกิดขึ้น ทั้งนี้ การเปลี่ยนแปลงดังกล่าวต้องไม่ทำให้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศสูงกว่าระดับความเสี่ยงที่ยอมรับได้	1. มีขั้นตอน/คู่มือ/แนวปฏิบัติในการรายงานต่อผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย 2. มีการบันทึกหลักฐานการพิจารณา/การตัดสินใจเพื่อเปลี่ยนแปลงการบริหารจัดการเหตุ และการบันทึกผลการดำเนินการในกรณีดังกล่าว

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				หมวด 1 **การออกแบบการใช้งานระบบการให้บริการ**	
X	X	X	X	1. ผู้รับใบอนุญาตต้องพิจารณาออกแบบระบบการให้บริการโดยคำนึงถึงเรื่องดังต่อไปนี้ 1.1 การแสดงผลในรูปแบบที่ชัดเจน ด้วยภาษาที่กระชับ เข้าใจได้ง่าย และสามารถเข้าถึงได้ด้วยอุปกรณ์ต่างๆ 1.2 ต้องจัดให้มีช่องทางที่ผู้ใช้บริการสามารถเลือกใช้งานได้ โดยออกแบบให้เข้าใจได้ง่ายและไม่เกิดการทำซ้ำโดยไม่จำเป็น 1.3 ต้องออกแบบการใช้งานให้ง่ายและเหมาะสม โดยเฉพาะผู้ใช้งานที่ขาดทักษะหรือไม่คุ้นเคยกับการใช้งานเทคโนโลยีดิจิทัล 1.4 ต้องออกแบบส่วนต่อประสานกับผู้ใช้งาน (user interface) ให้แสดงผลอย่างเหมาะสม บนอุปกรณ์ของผู้ใช้งาน เช่น อุปกรณ์เคลื่อนที่ แท็บเล็ต คอมพิวเตอร์ตั้งโต๊ะ แล็ปท็อป รวมถึงการแสดงผลผ่านเบราว์เซอร์ทั่วไป หรือซอฟต์แวร์สนับสนุนที่เกี่ยวข้อง	1. ภาษาที่ใช้แสดงในการสื่อสารกับผู้ใช้บริการ มีเนื้อหาในภาษาธรรมดาโดยทั่วไปและหลีกเลี่ยงศัพท์ทางเทคนิค เพื่อหลีกเลี่ยงความสับสน และใช้สัญลักษณ์แสดงหัวข้อย่อยตัวเลขและการจัดรูปแบบตามความเหมาะสมเพื่อช่วยในการอ่านได้ง่ายยิ่งขึ้น 2. มีการแสดงตัวอย่างการใช้งานระบบสำหรับผู้ที่ขาดทักษะหรือไม่เคยใช้งานเทคโนโลยีดิจิทัลหรือไม่ เช่น คู่มือการนำทางการใช้งาน ว่าจะต้องไปที่เมนูใด หรือตัวอย่างในการกรอกข้อมูลต่าง ๆ 3. มีการออกแบบส่วนต่อประสานกับผู้ใช้งานควรคำนึงถึงผู้ใช้งานเป็นหลัก โดยมีแนวทางการพิจารณาประกอบ ดังนี้ - ควรศึกษาความต้องการของผู้ใช้งานมาก่อน เพื่อให้สามารถออกแบบให้ผู้ใช้งานสามารถทำความเข้าใจและใช้งานได้โดยง่าย - หลีกเลี่ยงความซับซ้อนและการทำซ้ำในการทำกิจกรรมต่างๆ บนระบบการให้บริการ - การแสดงผลมีความเหมาะสมกับอุปกรณ์ของผู้ใช้งาน โดยรูปแบบของเนื้อหาที่แสดงผลในระบบการให้บริการควรจัดให้อยู่ภายใต้มาตรฐานการออกแบบเดียวกันตลอดทุกหน้าจอ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					- ควรออกแบบให้การโต้ตอบเป็นไปตามระดับความชำนาญในการใช้งาน โดยควรกำหนดค่าเริ่มต้นการใช้งานที่เหมาะสมกับผู้ใช้งานทั่วไป และมีตัวเลือกอื่นเพื่อให้ผู้ใช้งานสามารถปรับแต่งค่าได้ และสามารถเรียกค่าเริ่มต้นกลับมาได้ด้วย เพื่อให้ผู้ใช้งานสามารถปรับเปลี่ยนส่วนต่อประสานให้เหมาะสมกับความต้องการเฉพาะตัวได้ 4. ประเมินจากผลการสำรวจความพึงพอใจในการใช้งาน หรือผลการทดสอบจากการทดสอบความสามารถของระบบในข้อกำหนด 11.2.2 5. มีช่องทางรับฟังความคิดเห็นเกี่ยวกับปัญหาการใช้งานระบบจากผู้ใช้งาน และมีกระบวนการหรือขั้นตอนที่แสดงให้เห็นถึงการตอบสนองเพื่อนำไปพัฒนาปรับปรุงการให้บริการ
X	X	X	X	2. ผู้รับใบอนุญาตต้องจัดให้มีช่องทางสำหรับการรับฟังความคิดเห็น การให้ความช่วยเหลือ การแก้ปัญหา และการรับข้อร้องเรียนที่เกี่ยวข้องกับการให้บริการ	1. มีช่องทางที่ผู้ใช้บริการสามารถติดต่อได้ตามวัตถุประสงค์ที่หลักเกณฑ์กำหนด โดยเป็นช่องทางที่มีการแจ้งให้ผู้ใช้บริการทราบเป็นการทั่วไป 2. มีการสื่อสารอย่างชัดเจนถึงวิธีการติดต่อและให้ความช่วยเหลือ เช่น จัดให้มีลิงก์ไปยังคุณลักษณะการบริการตนเองแบบออนไลน์ เซสชันการแชท และหมายเลขโทรศัพท์ของฝ่ายช่วยเหลือ และรับข้อร้องเรียน
X	X	X	X	3. ผู้รับใบอนุญาตต้องจัดทำผังขั้นตอนการทำงานของระบบให้บริการซึ่งครอบคลุมกรณีดังต่อไปนี้ 3.1 กระบวนการใช้งานของผู้ใช้บริการตั้งแต่ต้นจนจบ ซึ่งมีการปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ	1. มีการจัดทำผังขั้นตอนการทำงานในกระบวนการใช้งานของผู้ใช้บริการ ซึ่งแสดงขั้นตอน หรือกระบวนการทำงานตั้งแต่ต้นจนจบที่กระชับ เข้าใจง่าย และมีกระบวนการทบทวนและปรับปรุงให้เป็นปัจจุบัน

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				3.2 ผังขั้นตอนที่มีทางเลือกการใช้งานในกรณีที่ผู้ใช้บริการไม่สามารถทำกิจกรรมได้เนื่องจากเทคโนโลยีของอุปกรณ์หรือซอฟต์แวร์ของผู้ใช้บริการไม่รองรับกับระบบการให้บริการ	2. กรณีที่ขั้นตอนการทำงานเป็นรูปแบบของผังงานที่มีเงื่อนไขเลือกตัดสินใจ ควรเตรียมขั้นตอนการทำงานไว้รองรับสำหรับเงื่อนไขหรือทางเลือกนั้นๆ โดยอย่างน้อยควรระบุทางเลือกสำหรับขั้นตอนที่ผู้ใช้บริการไม่สามารถทำกิจกรรมได้เนื่องจากข้อจำกัดทางเทคโนโลยีของอุปกรณ์หรือซอฟต์แวร์ของผู้ใช้บริการที่ใช้งานอยู่ในขณะนั้น 3. ควรมีการสื่อสารหรือเผยแพร่เพื่อให้ผู้ใช้บริการได้รับทราบและเข้าใจภาพรวมของการเข้าใช้งานระบบการให้บริการ
X	X	X	X	4. ผู้รับใบอนุญาตต้องให้ข้อมูลที่จำเป็นแก่ผู้ใช้บริการอย่างน้อย ดังนี้ 4.1 รายละเอียดกระบวนการที่ผู้ใช้บริการต้องดำเนินการในแต่ละขั้นตอน 4.2 ข้อกำหนดทางเทคนิค (technical requirement) ที่จำเป็นสำหรับการใช้งานระบบการให้บริการ เช่น การตั้งค่าการเชื่อมต่ออินเทอร์เน็ต การตั้งค่าอุปกรณ์สำหรับการถ่ายภาพ 4.3 รายการเอกสารหรือหลักฐานที่จำเป็นในขั้นตอนการพิสูจน์ตัวตนและข้อมูลแจ้งเตือนหากผู้ใช้บริการนำส่งเอกสารไม่ครบถ้วน	
X				5. หากมีการออกรหัสหรือชุดตัวเลขให้กับผู้ใช้บริการในขั้นตอนการพิสูจน์ตัวตน ผู้รับใบอนุญาตต้องจัดให้มีการแจ้งให้ทราบล่วงหน้าเกี่ยวกับการได้รับรหัสหรือชุดตัวเลขพร้อมวิธีการดำเนินการในขั้นตอนถัดไป	1. ในกรณีที่การใช้บริการมีขั้นตอนที่ต้องใช้รหัสหรือชุดตัวเลขเพื่อดำเนินการขั้นตอนการพิสูจน์ตัวตน ต้องมีกระบวนการหรือขั้นตอนแจ้งให้ผู้ใช้บริการได้รับทราบ 2. การแจ้งให้ผู้ใช้บริการได้รับทราบขั้นตอนการใช้รหัสหรือชุดตัวเลขต้องดำเนินการก่อนเวลาที่ต้องมีการใช้รหัสหรือชุดตัวเลขนั้น

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					3. มีการแจ้งให้ผู้ใช้บริการทราบถึงวิธีการใช้งานรหัสหรือชุดตัวเลข และวิธีการดำเนินการในขั้นตอนถัดไป
X				6. ผู้รับใบอนุญาตต้องแจ้งให้ผู้ใช้บริการทราบถึงสถานะของผลการพิสูจน์ตัวตนในแต่ละกรณี ดังนี้ 6.1 กรณีดำเนินการพิสูจน์ตัวตนสำเร็จต้องยืนยันผลการพิสูจน์ตัวตนให้ผู้ใช้บริการทราบ พร้อมรายละเอียดการดำเนินการในขั้นตอนถัดไป 6.2 กรณีพิสูจน์ตัวตนสำเร็จบางส่วน (partially complete) เช่น เอกสารหรือข้อมูลไม่ครบถ้วน ผู้ใช้บริการหยุดการดำเนินการ หรือ session timeout ผู้รับใบอนุญาตต้องมีกระบวนการสื่อสารให้ผู้ใช้บริการทราบถึงข้อมูลที่ดำเนินการไม่สำเร็จ 6.3 กรณีพิสูจน์ตัวตนไม่สำเร็จ (unsuccessful) ผู้รับใบอนุญาตต้องให้ข้อมูลช่องทางอื่นที่สามารถดำเนินการแทนได้ เช่น การพิสูจน์ตัวตนที่สำนักงานสาขา	**หมายเหตุ** - ไม่มีการกำหนดรูปแบบหรือวิธีการไว้เป็นการเฉพาะ
X				7. ผู้รับใบอนุญาตต้องจัดให้มีบริการให้ความช่วยเหลือแก่ผู้ใช้บริการในกระบวนการพิสูจน์ตัวตน ซึ่งรวมถึงกรณีที่ผู้ใช้บริการไม่มีความพร้อมด้านเทคโนโลยีหรือความสามารถในการดำเนินการ โดยอย่างน้อยต้องมีช่องทางที่สามารถติดต่อสื่อสารกับบุคลากรของผู้รับใบอนุญาตได้ เช่น เคาน์เตอร์เซอร์วิส call center หรือ VDO call	1. มีช่องทางที่ผู้ใช้บริการสามารถติดต่อได้ตามวัตถุประสงค์ที่หลักเกณฑ์กำหนด โดยเป็นช่องทางที่มีการแจ้งให้ผู้ใช้บริการทราบเป็นการทั่วไป และช่องทางดังกล่าวต้องสามารถติดต่อสื่อสารกับบุคลากรของผู้รับใบอนุญาตเพื่อขอรับความช่วยเหลือหรือคำแนะนำในการใช้บริการได้ 2. มีการสื่อสารอย่างชัดเจนถึงช่องทางหรือวิธีการติดต่อขอรับบริการ 3. มีคู่มือหรือแนวทางสำหรับบุคลากรเพื่อให้คำแนะนำหรือความช่วยเหลือแก่ผู้ใช้บริการ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X				8. ผู้รับใบอนุญาตต้องจัดให้มีคู่มือหรือคำแนะนำสำหรับผู้ใช้บริการในการแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลของตนที่มีการเก็บรวบรวมในขั้นตอนการพิสูจน์ตัวตน	1. มีเอกสาร/คู่มือ/คำแนะนำสำหรับผู้ใช้บริการ เกี่ยวกับขั้นตอนและวิธีการในการแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลของตนเอง 2. ควรแจ้งให้ผู้ใช้บริการรับทราบถึงรายการข้อมูลที่ไม่สามารถขอแก้ไขได้ 3. มีแนวทาง/ช่องทาง/วิธีการสื่อสารเพื่อให้ผู้ใช้บริการได้รับทราบข้อมูลดังกล่าว
	X	X		9. ผู้รับใบอนุญาตต้องจัดให้มีคำแนะนำการใช้งานและดูแลรักษาสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ เช่น ระยะเวลาการใช้งานสิ่งที่ใช้ยืนยันตัวตน การดำเนินการเมื่อสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย หรือเสียหาย	1. มีเอกสาร/คู่มือ/คำแนะนำสำหรับผู้ใช้บริการเกี่ยวกับการใช้งานสิ่งที่ใช้ยืนยันตัวตนที่สอดคล้องตามชนิดของสิ่งที่ใช้ยืนยันตัวตน ซึ่งครอบคลุมเนื้อหาอย่างน้อยดังนี้ - วิธีการใช้งาน - วิธีการจัดเก็บ และดูแลรักษา - ระยะเวลาการใช้งาน หรืออายุการใช้งาน (ถ้ามี) - การดำเนินการกรณีสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย เสียหาย ไม่สามารถใช้งานได้ หรือลืม 2. มีแนวทาง/ช่องทาง/วิธีการสื่อสารเพื่อให้ผู้ใช้บริการได้รับทราบข้อมูลดังกล่าว
	X	X		10. ผู้รับใบอนุญาตต้องจัดให้มีช่องทางสำหรับผู้ใช้บริการในการกู้คืน เปลี่ยนแปลง หรือจัดให้มีสิ่งทดแทนสิ่งที่ใช้ยืนยันตัวตน ในกรณีที่สิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย เสียหาย ไม่สามารถใช้งาน หรือลืม โดยช่องทางดังกล่าวอย่างน้อยต้องเป็นกระบวนการที่มีระดับความน่าเชื่อถือเทียบเท่ากับกระบวนการออกสิ่งที่ใช้ยืนยันตัวตนที่เคยทำไว้	1. มีการกำหนดแนวปฏิบัติหรือขั้นตอนการดำเนินการกรณีสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย เสียหาย หรือไม่สามารถใช้งาน ซึ่งมีรายละเอียดเกี่ยวกับ 1.1 ขั้นตอนและช่องทางการติดต่อ/แจ้งเรื่องการสูญหาย เสียหาย ไม่สามารถใช้งานได้ หรือลืม

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					1.2 แนวทางการจัดการสิ่งที่ใช้ยืนยันตัวตนอันเดิมที่มีการแจ้ง/ทราบการสูญหาย เสียหาย ไม่สามารถใช้งานได้ หรือลืม เช่น การระงับการใช้งาน การยุติการใช้งาน เป็นต้น 1.3 ขั้นตอนการกู้คืน เปลี่ยนแปลง หรือจัดให้มีสิ่งทดแทนสิ่งที่ใช้ยืนยันตัวตนอันเดิม 1.4 การดำเนินการในส่วนที่เกี่ยวข้องกับผู้ใช้บริการ เช่น การตรวจสอบตัวตนของผู้ใช้บริการ การตรวจสอบสิทธิของผู้ขอกรณีได้รับการแจ้งขอกู้คืนสิ่งที่ใช้ยืนยันตัวตน เป็นต้น 2. มีคู่มือหรือแนวปฏิบัติสำหรับบุคลากรผู้ปฏิบัติงานที่เกี่ยวข้องกับขั้นตอนดังกล่าว โดยควรให้รายละเอียดแยกตามประเภทของสิ่งที่ใช้ยืนยันตัวตน 3. มีช่องทางสำหรับผู้ใช้บริการในการกู้คืน เปลี่ยนแปลง หรือจัดให้มีสิ่งทดแทนสิ่งที่ใช้ยืนยันตัวตน (Authenticator) ในกรณีที่สิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย เสียหาย หรือไม่สามารถใช้งานสิ่งที่ใช้ยืนยันตัวตนได้ หรือลืม โดยอย่างน้อยต้องเป็นกระบวนการที่มีความน่าเชื่อถือเทียบเท่ากับกระบวนการออกสิ่งที่ใช้ยืนยันตัวตน 4. มีการสื่อสารอย่างชัดเจนถึงวิธีการที่จะได้รับความช่วยเหลือด้านเทคนิค ตัวอย่างเช่น ให้ข้อมูลแก่ผู้ใช้ เช่น จัดให้มีลิงก์ไปยังคุณลักษณะการบริการตนเองแบบออนไลน์ เซสชันการแชท หรือหมายเลขโทรศัพท์สำหรับฝ่ายสนับสนุนของฝ่ายช่วยเหลือ หลีกเลี่ยงการเปลี่ยนเส้นทางผู้ใช้ไปมาระหว่างฝ่ายที่ทำธุรกรรม (เช่น RPs, IdPs และโบรกเกอร์) เพื่อรับความช่วยเหลือด้านเทคนิค

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	11. ผู้รับใบอนุญาตต้องจัดทำแผนและรายละเอียดการทดสอบระบบ (usability test plans) ซึ่งครอบคลุมตามขอบเขตการให้บริการ โดยอย่างน้อยต้องประกอบด้วย 11.1 วัตถุประสงค์ เป้าหมาย 11.2 วิธีการวัดผลหรือเกณฑ์การทดสอบซึ่งครอบคลุมหัวข้อดังนี้ 11.2.1 ระบบการให้บริการแสดงผลในรูปแบบที่ชัดเจน ด้วยภาษาที่กระชับ เข้าใจได้ง่าย และสามารถเข้าถึงได้ด้วยอุปกรณ์ต่างๆ 11.2.2 ระบบการให้บริการใช้งานง่ายและเหมาะสม โดยเฉพาะผู้ใช้งานที่ขาดทักษะหรือไม่คุ้นเคยกับการใช้งานเทคโนโลยีดิจิทัล 11.2.3 ส่วนต่อประสานกับผู้ใช้งาน (user interface) ของระบบการให้บริการแสดงผลอย่างเหมาะสม (responsive design) บนอุปกรณ์ของผู้ใช้งาน 11.3 จำนวน วิธีการคัดเลือก และการจัดกลุ่มผู้เข้าร่วมการทดสอบตามขอบเขตการให้บริการ เช่น ผู้ใช้งานทั่วไป ผู้พิการ ผู้สูงอายุ ผู้ที่ใช้เทคโนโลยีอำนวยความสะดวก ผู้ที่ขาดความเข้าใจในการใช้งาน ผู้ที่มีความหลากหลายทางวัฒนธรรมและภาษา ผู้ที่มาจากภูมิภาคและพื้นที่ห่างไกล ผู้ที่มีเทคโนโลยีรุ่นเก่าและการเชื่อมต่อแบนด์วิดท์ต่ำ 11.4 แนวทางและวิธีการที่ใช้ในการทดสอบซึ่งแสดงถึงกระบวนการทำงาน ปัญหา และสิ่งที่ต้องปรับปรุง	**หมายเหตุ** - พิจารณารายละเอียดตามประเภทของใบอนุญาต - การกำหนดกลุ่มผู้เข้าร่วมการทดสอบ ขึ้นอยู่กับการกำหนดวัตถุประสงค์และกลุ่มเป้าหมายในการให้บริการ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				11.5 รูปแบบการทดสอบ บนอุปกรณ์ต่างๆ ทั้งในรูปแบบอุปกรณ์ตั้งโต๊ะและอุปกรณ์เคลื่อนที่ 11.6 ผลลัพธ์ของการทดสอบและแนวทางการพัฒนาหรือปรับปรุงระบบการให้บริการ	
X	X	X	X	12. ในการทดสอบความสามารถของระบบ ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อย ดังนี้ 12.1 ต้องทำการทดสอบความสามารถในการใช้งานของระบบที่ครอบคลุมขั้นตอนตั้งแต่ต้นจนจบกระบวนการในสภาพแวดล้อมที่ใกล้เคียงกับการให้บริการจริง ตามกลุ่มของผู้เข้าร่วมการทดสอบ 12.2 ต้องบันทึกผลลัพธ์ของการทดสอบการใช้งานระบบ รวมถึงวิธีการทดสอบ ผลการทดสอบ ข้อสังเกต และข้อเสนอแนะจากการทดสอบ	**หมายเหตุ** - เป็นการทดสอบ load test
X	X	X	X	13. ผู้รับใบอนุญาตต้องจัดทำรายงานผลการทดสอบความสามารถของระบบ ซึ่งประกอบด้วย 13.1 แผนและรายละเอียดการทดสอบ 13.2 บันทึกผลลัพธ์ของการทดสอบ	1. มีรายงานผลการทดสอบความสามารถของระบบ ซึ่งต้องแสดงให้เห็นกระบวนการทดสอบที่ครอบคลุมระบบงานตั้งแต่ต้นจนจบกระบวนการ โดยมีรายละเอียดประกอบด้วย 1.1 แผนและรายละเอียดการทดสอบ - วัตถุประสงค์ เป้าหมายของการทดสอบ - วิธีการวัดผล หรือเกณฑ์การทดสอบ โดยควรต้องมีการกำหนด performance target - รูปแบบ กระบวนการ และวิธีการทดสอบ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					1.2 ผลลัพธ์ของการทดสอบ - ผลการทดสอบ - ข้อสังเกต และข้อเสนอแนะจากการทดสอบ - การปรับปรุงกระบวนการทำงาน (ถ้ามี)
X	X	X	X	14. รายงานผลการทดสอบความสามารถของระบบเป็นส่วนหนึ่งของรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจที่ต้องนำส่งต่อสำนักงาน	
				หมวด 2 **การทดสอบด้านเทคนิคของระบบและซอฟต์แวร์ที่เกี่ยวข้อง** **(technical testing requirement)**	
X	X	X	X	15. ผู้รับใบอนุญาตต้องจัดให้มีแผนการทดสอบและดำเนินการทดสอบด้านเทคนิคของระบบและซอฟต์แวร์ที่ครอบคลุมระบบการให้บริการ	1. มีการจัดทำแผนการทดสอบระบบการให้บริการที่ครอบคลุมรายละเอียดความสอดคล้องในหัวข้อต่างๆ ตามข้อ 16
X	X	X	X	16. ในการทดสอบทางเทคนิคต้องแสดงให้เห็นความสอดคล้องกับข้อกำหนดในเรื่องต่อไปนี้ 16.1 การจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ 16.2 กลไกในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ 16.3 กลไกในการตรวจจับเฝ้าระวังและจัดการเหตุการณ์การทุจริตหรือฉ้อโกงจากการใช้งานระบบ 16.4 วิธีการพิสูจน์ตัวตน และระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)	1. พิจารณาขอบเขตและการดำเนินการทดสอบให้ครอบคลุมหัวข้อตามรายละเอียดข้อกำหนด โดยพิจารณาตามลักษณะของการประกอบธุรกิจที่ขอรับใบอนุญาต ซึ่งสอดคล้องกับหลักเกณฑ์อื่น ดังนี้ 1.1 การจัดเก็บข้อมูลจราจรอิเล็กทรอนิกส์ : 1.2 กลไกในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่พึงประสงค์ 1.3 กลไกในการตรวจจับ เฝ้าระวัง และจัดการเหตุการณ์การทุจริตหรือฉ้อโกงจากการใช้งานระบบ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				16.5 การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน 16.6 วิธีการยืนยันตัวตน และระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) 16.7 การทดสอบความสอดคล้องของโพรโทคอลที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการ	1.4 ขั้นตอน/กระบวนการ/วิธีการพิสูจน์ตัวตน และระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ตามระดับความน่าเชื่อถือที่กำหนดในการให้บริการ 1.5 ขั้นตอน/กระบวนการ/วิธีการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน 1.6 ขั้นตอน/กระบวนการ/วิธีการยืนยันตัวตน และระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) 1.7 การทดสอบความสอดคล้องของโพรโทคอลที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการ
X	X	X	X	17. ผู้รับใบอนุญาตต้องจัดให้มีการทำตารางเปรียบเทียบความสามารถของระบบกับการทดสอบ (requirement traceability matrix) ที่เชื่อมโยงความสอดคล้องของกรณีที่ใช้ในการทดสอบ (test case) กับข้อกำหนดที่ต้องดำเนินการ	1. มีการจัดทำ ตารางเปรียบเทียบความสามารถของระบบกับการทดสอบ (requirement traceability matrix) ซึ่งอย่างน้อยควรครอบคลุมเนื้อหา ดังนี้ 1.1 business requirement 1.2 test level 1.3 test case 1.4 mapping test case 1.5 test run 1.6 issues 1.7 user acceptance test cases 1.8 test result **หมายเหตุ** - พิจารณารายละเอียดตามประเภทของใบอนุญาต
X	X	X	X	18. ก่อนเริ่มการทดสอบผู้รับใบอนุญาตต้องดำเนินการอย่างน้อย ดังนี้ 18.1 ระบุข้อกำหนดที่ใช้ในแผนการทดสอบทางเทคนิค	1. มีการจัดทำแผนการทดสอบซึ่งสอดคล้องกับ ตารางเปรียบเทียบความสามารถของระบบกับการทดสอบ (requirement traceability matrix) โดยมีการกำหนด test case ในทุกกรณี

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				18.2 ข้อกำหนดทุกข้อในแผนการทดสอบทางเทคนิคต้องมีการทดสอบอย่างน้อยหนึ่งกรณี 18.3 ต้องมีเอกสารการบันทึกกรณีที่ใช้ในการทดสอบ และระบุทรัพยากรที่ใช้ในการทดสอบ	2. จำนวน test case ที่กำหนดซึ่งสอดคล้องกับแผนการทดสอบ 3. มีหลักฐานบันทึกกรณีที่ใช้ในการทดสอบ และระบุทรัพยากรที่ใช้ในการทดสอบ
X	X	X	X	19. ผู้รับใบอนุญาตต้องจัดทำรายงานผลการทดสอบทางเทคนิค (technical test report) โดยประกอบด้วยข้อมูลดังต่อไปนี้ 19.1 การทดสอบที่ได้ดำเนินการตามแผนการทดสอบทางเทคนิค 19.2 เกณฑ์การทดสอบ 19.3 สถานะการทดสอบของแต่ละกรณีที่ใช้ในการทดสอบรวมถึงความครอบคลุมของการทดสอบและข้อบกพร่องที่เกิดขึ้น 19.4 ผลของการทดสอบที่ครบถ้วนตามเกณฑ์การทดสอบ 19.5 ถ้าผลการทดสอบไม่ครบถ้วนตามเกณฑ์การทดสอบจะต้องมีการประเมินความเสี่ยงในข้อกำหนดที่ไม่สามารถดำเนินการได้โดยครบถ้วนพร้อมเหตุผลในการพิจารณายอมรับผลการทดสอบดังกล่าว	1. มีการจัดทำรายงานผลการทดสอบทางเทคนิค ซึ่งครอบคลุมรายละเอียดดังนี้ 1.1 ขั้นตอนและวิธีการทดสอบ 1.2 เกณฑ์การทดสอบ 1.3 สถานะการทดสอบ และผลการทดสอบในแต่ละกรณี 1.4 กระบวนการตรวจสอบความถูกต้องของการพัฒนาระบบการให้บริการ 1.5 กระบวนการตรวจสอบผลการพัฒนาระบบการให้บริการเปรียบเทียบกับความต้องการของผู้ใช้งาน 1.6 ข้อบกพร่องที่เกิดขึ้น และการแก้ไขหรือการยอมรับข้อบกพร่อง
X	X	X	X	20. รายงานผลการทดสอบทางเทคนิคถือเป็นส่วนหนึ่งของรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจที่ต้องนำส่งต่อสำนักงาน	**ใช้ในกรณีการตรวจประเมินความพร้อมสำหรับการขอเริ่มประกอบธุรกิจ หรือกรณีที่มีการเปลี่ยนแปลงที่สำคัญซึ่งต้องดำเนินการทดสอบใหม่**
				หมวด 3 **การตรวจประเมินระบบการให้บริการ**	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	21. ภายหลังจากเริ่มประกอบธุรกิจ ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินและจัดทำรายงานผลการตรวจประเมินระบบการให้บริการและรายงานต่อสำนักงานตามหลักเกณฑ์และระยะเวลาที่สำนักงานกำหนด	**หมายเหตุ** - รายละเอียดเป็นไปตามหลักเกณฑ์เกี่ยวกับการนำส่งรายงานผลการตรวจประเมินฯ ที่สำนักงานกำหนด
X	X	X	X	22. ในการตรวจประเมินระบบการให้บริการ ผู้รับใบอนุญาตต้องแสดงให้เห็นได้ว่า 22.1 การตรวจประเมินได้ดำเนินการโดยผู้ตรวจสอบที่เป็นอิสระ ซึ่งมีความรู้ ความสามารถ และประสบการณ์ที่เหมาะสมในการดำเนินการ 22.2 ในกรณีที่เป็นการตรวจประเมินด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบต้องผ่านการรับรองและมีวุฒิบัตรหรือได้รับประกาศนียบัตรด้านความมั่นคงปลอดภัยระดับสากลอย่างหนึ่งอย่างใดดังต่อไปนี้ 22.2.1 certified information system auditor (CISA) 22.2.2 certified information security manager (CISM) 22.2.3 certified information system security professional (CISSP) 22.2.4 ISO/IEC 27001 lead auditor 22.2.5 ใบรับรองอื่นตามที่ประกาศกำหนดเพิ่มเติม	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				22.3 ผู้ตรวจสอบไม่มีความเกี่ยวข้องกับการพัฒนาหรือการดำเนินงานเกี่ยวกับระบบให้บริการที่ทำการตรวจประเมิน 22.4 ผู้ตรวจสอบไม่มีส่วนได้เสียกับการตรวจประเมินระบบให้บริการที่ทำการตรวจประเมิน	
X	X	X	X	23. รายงานผลการตรวจประเมินระบบการให้บริการต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้ 23.1 วัตถุประสงค์และขอบเขตของการตรวจประเมิน 23.2 หลักเกณฑ์ที่นำมาใช้ในการตรวจประเมิน 23.3 วันเวลาในการตรวจประเมิน 23.4 ชื่อ ตำแหน่ง และข้อมูลการติดต่อผู้รับผิดชอบการตรวจประเมินของผู้รับใบอนุญาต 23.5 รายชื่อและคุณสมบัติของผู้ตรวจสอบ 23.6 สถานที่ที่ทำการตรวจประเมิน รวมถึงศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง และที่ตั้งอื่นๆ ที่ใช้ในการควบคุมระบบการให้บริการ 23.7 รายการข้อมูล เอกสาร หลักฐาน หรือบุคคลผู้ให้ข้อมูลประกอบการตรวจประเมิน 23.8 วิธีการที่ใช้ในการตรวจประเมิน 23.9 ผลการทดสอบหรือผลการตรวจประเมิน	**หมายเหตุ** - รายงานผลการตรวจประเมินให้อ้างอิงแบบรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				23.10 ข้อตรวจพบซึ่งรวมถึงรายการความสอดคล้องและไม่สอดคล้องตามหลักเกณฑ์ที่นำมาใช้ในการตรวจประเมิน 23.11 การดำเนินการและการแก้ไขตามข้อตรวจพบ 23.12 ความเห็น ข้อสังเกต หรือข้อเสนอแนะของผู้ตรวจสอบ	
X	X	X	X	24. ผู้รับใบอนุญาตต้องจัดให้มีการรายงานผลการตรวจประเมินระบบการให้บริการ พร้อมทั้งรายงานข้อตรวจพบและผลการปรับปรุงแก้ไข ให้ผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับทราบตามรอบการประเมินและตามรอบการติดตามการปรับปรุงแก้ไขข้อตรวจพบหรือโดยไม่ชักช้าเมื่อพบข้อบกพร่องที่มีนัยสำคัญ	1. มีการจัดทำรายงานผลการตรวจประเมินระบบการให้บริการ ซึ่งมีเนื้อหาครอบคลุมรายละเอียดที่ต้องดำเนินการตามหลักเกณฑ์ที่กำหนด 2. มีหลักฐานแสดงให้เห็นว่าได้มีการนำเสนอรายงานผลการตรวจประเมินให้ผู้บริหารรับทราบ 3. รายงานผลการตรวจประเมินล่าสุดสอดคล้องกับรอบระยะเวลาการตรวจประเมิน หรือรอบการติดตามการปรับปรุงแก้ไขข้อตรวจพบ
X	X	X	X	25. กรณีที่มีการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อระบบการให้บริการภายหลังจากเริ่มประกอบธุรกิจ ผู้รับใบอนุญาตต้องดำเนินการตรวจประเมินระบบในส่วนที่ได้รับผลกระทบจากการเปลี่ยนแปลงดังกล่าวและนำส่งรายงานผลการตรวจประเมินพร้อมการแจ้งการเปลี่ยนแปลงต่อสำนักงาน	**ใช้ในกรณีที่มีการเปลี่ยนแปลงที่สำคัญซึ่งต้องดำเนินการตรวจประเมินส่วนที่ได้รับผลกระทบ** **หมายเหตุ** - รายละเอียดเป็นไปตามหลักเกณฑ์เกี่ยวกับการแจ้งการเปลี่ยนแปลงที่สำคัญตามที่สำนักงานประกาศกำหนด
X	X	X	X	26. ผู้รับใบอนุญาตต้องนำส่งรายงานผลการตรวจประเมินระบบการให้บริการต่อสำนักงานตามระยะเวลาที่สำนักงานประกาศกำหนด และสำนักงานอาจร้องขอข้อมูล เอกสาร หรือหลักฐานเพิ่มเติมเพื่อประกอบการตรวจรายงานผลการตรวจประเมินระบบการให้บริการได้	**หมายเหตุ** - รายละเอียดเป็นไปตามหลักเกณฑ์เกี่ยวกับการนำส่งรายงานผลการตรวจประเมินที่สำนักงานกำหนด

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	27. ในกรณีที่สำนักงานเห็นว่ารายงานผลการตรวจประเมินระบบการให้บริการไม่ครอบคลุมประเด็นสำคัญที่อาจส่งผลกระทบต่อความน่าเชื่อถือและความเสี่ยงของระบบการให้บริการ สำนักงานอาจดำเนินการตรวจประเมินเพิ่มเติมได้	**หมายเหตุ** - สำนักงานอาจเข้าทำการตรวจประเมินเพิ่มเติมเอง หรือสั่งให้ผู้รับใบอนุญาตดำเนินการตรวจประเมินเพิ่มเติมและนำส่งรายงานผลการตรวจประเมินให้สำนักงาน
X	X	X	X	28. ในกรณีที่ผู้รับใบอนุญาตประสงค์จะเลิกประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลต้องจัดให้มีการประเมินผลกระทบและแผนรองรับการเลิกประกอบธุรกิจตามที่คณะกรรมการประกาศกำหนด	**หมายเหตุ** - รายละเอียดเป็นไปตามหลักเกณฑ์เกี่ยวกับวิธีการ เงื่อนไข และระยะเวลาในการเลิกประกอบธุรกิจ ภายใต้ ม.30 ของพระราชกฤษฎีกา
				หมวด 4 **ข้อตกลงการให้บริการ**	
X	X	X	X	29. ผู้รับใบอนุญาตต้องจัดให้มีข้อตกลงในการให้บริการเกี่ยวกับระบบการให้บริการที่มีความชัดเจนและเป็นปัจจุบัน โดยเปิดเผยให้ผู้ใช้บริการได้รับทราบและยอมรับข้อตกลงดังกล่าวก่อนเริ่มใช้บริการ	1. มีเอกสารหรือหลักฐานที่กำหนดรายละเอียดข้อตกลงในการให้บริการทั้งนี้พิจารณาตามลักษณะของการประกอบธุรกิจที่ขอรับใบอนุญาต โดยข้อตกลงในการให้บริการมีเนื้อหาครอบคลุมหัวข้อที่กำหนด ต้องสอดคล้องกับนโยบายและแนวปฏิบัติของหน่วยงาน 2. ข้อตกลงการให้บริการดังกล่าวมีการทบทวนและปรับปรุงให้เป็นปัจจุบัน 3. มีการเปิดเผยหรือมีช่องทางให้ผู้ใช้บริการรับทราบข้อตกลงดังกล่าวอย่างชัดเจนก่อนเข้าใช้บริการ
X	X	X	X	30. ข้อตกลงในการให้บริการต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้ 30.1 รายละเอียดเกี่ยวกับลักษณะของการให้บริการ 30.2 หลักเกณฑ์ เงื่อนไข และวิธีปฏิบัติในการให้บริการ 30.3 สิทธิ หน้าที่และความรับผิดของผู้ใช้บริการ 30.3.1 สิทธิในการเข้าถึงและใช้งานระบบ 30.3.2 หน้าที่ที่เกี่ยวข้องการใช้งาน เช่น การแสดงหรือนำส่งเอกสารหรือหลักฐานตามที่กำหนด การปฏิบัติตามคู่มือผู้ใช้งาน	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				30.3.3 หน้าที่ในการให้ข้อมูลเกี่ยวกับอัตลักษณ์และหลักฐานแสดงตนที่ถูกต้อง 30.3.4 หน้าที่ในการแจ้งให้ผู้รับใบอนุญาตทราบโดยเร็ว เมื่อทราบว่ามีการใช้งานอัตลักษณ์หรือสิ่งที่ใช้ยืนยันตัวตนโดยไม่ได้รับอนุญาต 30.4 สิทธิ หน้าที่ และความรับผิดของผู้รับใบอนุญาต 30.4.1 กรณีที่อาจมีการระงับ ยกเลิก หรือเพิกถอนสิทธิในการเข้าถึงและใช้งานโดยผู้รับใบอนุญาต 30.4.2 การเปลี่ยนแปลงข้อตกลงการให้บริการ 30.4.3 การบริหารจัดการข้อมูลเกี่ยวกับอัตลักษณ์ ข้อมูลส่วนบุคคล หรือสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ เช่น การไม่เปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการต่อบุคคลภายนอก เว้นแต่ได้รับความยินยอมจากผู้ใช้บริการ 30.4.4 ความรับผิดและข้อจำกัดความรับผิดของผู้รับใบอนุญาต (ถ้ามี) 30.5 ช่องทางการติดต่อกับผู้รับใบอนุญาต 30.6 กระบวนการในการระงับข้อพิพาท การแก้ไขปัญหาหรือการจัดการเรื่องร้องเรียน 30.7 การชดใช้หรือเยียวยาความเสียหายของผู้รับใบอนุญาต	
X	X	X	X	31. ผู้รับใบอนุญาตต้องแจ้งให้ผู้ใช้บริการทราบถึงการใช้บริการในส่วนที่ผู้ใช้บริการต้องดำเนินการกับบุคคลภายนอก	1. กรณีที่ผู้ใช้บริการระบบการให้บริการมีขั้นตอนที่ต้องดำเนินการกับบุคคลภายนอก เช่น การดำเนินการยืนยันตัวตนที่จุดยืนยันตัวตน เป็นต้น ต้องมีเอกสารหรือคู่มือที่แสดงรายละเอียดหรือชี้แจงขั้นตอน

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					การดำเนินการดังกล่าว เพื่อให้ผู้ใช้บริการทราบและสามารถดำเนินกิจกรรมได้โดยถูกต้อง โดยอย่างน้อยควรมีรายละเอียดดังนี้ 1.1 ขั้นตอน และวิธีการดำเนินการ 1.2 เอกสาร เครื่องมือ หรืออุปกรณ์ที่ผู้ใช้บริการต้องจัดเตรียม 1.3 ข้อควรทราบอื่นๆ ซึ่งเป็นเงื่อนไขที่จำเป็นในการดำเนินการ 2. ขั้นตอนในส่วนที่ผู้ใช้บริการต้องดำเนินการกับบุคคลภายนอก ต้องสอดคล้องกับกระบวนการทำงานของระบบการให้บริการ และเป็นไปตามหลักเกณฑ์ในส่วนที่เกี่ยวข้อง
X	X	X	X	32. ผู้รับใบอนุญาตต้องเปิดเผยรายละเอียดของค่าธรรมเนียมที่เรียกเก็บจากผู้ใช้บริการระบบ โดยวิธีการที่ทำให้ผู้ใช้บริการสามารถทราบได้อย่างชัดเจน ทั้งนี้ กรณีที่มีการเปลี่ยนแปลงค่าธรรมเนียม ผู้รับใบอนุญาตจะต้องแจ้งให้ผู้ใช้บริการทราบรายละเอียดการเปลี่ยนแปลงดังกล่าวด้วย	1. มีช่องทางในการเปิดเผยรายละเอียดค่าธรรมเนียมที่เรียกเก็บให้ผู้ใช้บริการได้รับทราบ โดยวิธีการที่ทำให้ผู้ใช้บริการสามารถทราบได้อย่างชัดเจน ซึ่งควรมีการระบุรายละเอียดเกี่ยวกับอัตราค่าธรรมเนียมและวิธีการหรือช่องทางการเรียกเก็บค่าธรรมเนียม 2. มีขั้นตอนการแจ้งการเปลี่ยนแปลงค่าธรรมเนียมที่เรียกเก็บซึ่งทำให้ผู้ใช้บริการได้รับทราบอย่างชัดเจน โดยต้องแจ้งให้ผู้ใช้บริการได้รับทราบก่อนดำเนินการเรียกเก็บตามอัตราที่เปลี่ยนแปลง

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				หมวด 1 **บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการยืนยันตัวตน**	
X				1. ผู้รับใบอนุญาตต้องบริหารจัดการกระบวนการพิสูจน์ตัวตนให้สอดคล้องตามลักษณะและระดับความเสี่ยงของธุรกรรมหรือการประกอบธุรกิจ	1. มีการกำหนดนโยบายเกี่ยวกับการให้บริการพิสูจน์ตัวตน และการกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตนต้องมีระดับความน่าเชื่อถือไม่ต่ำกว่าที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกาศกำหนด (IAL2) ทั้งในกรณีที่เป็นการพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า และพบเห็นต่อหน้า (อ้างอิง ขมธอ. 19-2566) 2. ในกรณีที่ผู้รับใบอนุญาตอยู่ภายใต้การกำกับดูแลของหน่วยงานกำกับดูแลที่มีการกำหนดระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน ต้องพิจารณาความสอดคล้องตามระดับความน่าเชื่อถือที่หน่วยงานกำกับดูแลกำหนดด้วย 3. มีขั้นตอนหรือกระบวนการพิสูจน์ตัวตนที่สอดคล้องตามระดับความน่าเชื่อถือในการให้บริการ 3.1 มีกระบวนการพิสูจน์ตัวตนสอดคล้องตามระดับความน่าเชื่อถือ (อ้างอิง ขมธอ. 19-2566) ซึ่งอย่างน้อยต้องมีระดับความน่าเชื่อถือไม่ต่ำกว่า IAL2 ทั้งในกรณีที่เป็นการพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า และพบเห็นต่อหน้า

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					3.2 ในกรณีที่ผู้รับใบอนุญาตอยู่ภายใต้การกำกับดูแลของหน่วยงานกำกับดูแลที่มีการกำหนดระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน ต้องพิจารณาความสอดคล้องตามระดับความน่าเชื่อถือที่หน่วยงานกำกับดูแลกำหนดด้วย 4. ขั้นตอนหรือกระบวนการพิสูจน์ตัวตนต้องครอบคลุมกระบวนการหลัก 3 กระบวนการ ดังนี้ 4.1 กระบวนการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล เช่น การรวบรวมข้อมูลจากบัตรประชาชน การถ่ายภาพใบหน้า 4.2 กระบวนการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลว่ามีความถูกต้อง แท้จริง และความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์ เช่น การตรวจสอบรูปถ่ายของหลักฐานแสดงตน การตรวจสอบลักษณะทางกายภาพของหลักฐานแสดงตนโดยเจ้าหน้าที่ การตรวจสอบข้อมูลบนหลักฐานแสดงตนและตรวจสอบสถานะของหลักฐานแสดงตน 4.3 กระบวนการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์ดังกล่าว เพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริงตามระดับความน่าเชื่อถือที่นำมาใช้ในการพิสูจน์ตัวตน เช่น การเปรียบเทียบภาพใบหน้าของบุคคลกับภาพใบหน้าบนหลักฐานแสดงตน 5. หากมีการใช้งานชีวมิติ (biometric) ในการเปรียบเทียบข้อมูลชีวมิติของบุคคล ต้องมีความสอดคล้องกับแนวทางตามข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					6. กระบวน/ขั้นตอนการดำเนินการมีความสอดคล้องตามหลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ **หมายเหตุ** - แนวทางการประเมินความเสี่ยงเพื่อพิจารณากำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน สามารถอ้างอิงตาม ขมธอ. 18-2566 ข้อ 4
X				2. ในการให้บริการพิสูจน์ตัวตน ผู้รับใบอนุญาตต้องมีกระบวนการที่ครอบคลุมการทำงานอย่างน้อยในเรื่องดังต่อไปนี้ 2.1 ต้องจัดให้ผู้ใช้บริการสามารถปรับปรุงข้อมูลเกี่ยวกับอัตลักษณ์ของตนซึ่งถูกจัดเก็บในกระบวนการพิสูจน์ตัวตนได้ โดยต้องจัดให้มีกระบวนการตรวจสอบที่เกี่ยวข้องอย่างน้อยดังนี้ 2.1.1 ตรวจสอบข้อมูลที่ขอปรับปรุงก่อนที่จะบันทึกการเปลี่ยนแปลงข้อมูลในระบบการให้บริการ รวมถึงกรณีที่มีการเปลี่ยนแปลงสถานะของอัตลักษณ์ดิจิทัลนั้น เช่น การระงับชั่วคราว การใช้งานใหม่ 2.1.2 ในกรณีที่ตรวจพบการทำธุรกรรมที่ผิดปกติต้องมีการตรวจสอบว่าอัตลักษณ์ดิจิทัลนั้น ยังอยู่ภายใต้ความควบคุมของเจ้าของอัตลักษณ์ดิจิทัลที่แท้จริง	**1. การแก้ไขปรับปรุงข้อมูล** • ขั้นตอนการพิสูจน์ตัวตนซึ่งดำเนินการเรียบร้อยแล้ว มีกระบวนการให้ผู้ใช้บริการสามารถตรวจสอบและปรับปรุงข้อมูลเกี่ยวกับอัตลักษณ์ของตนเองที่มีการจัดเก็บและบันทึกไว้ได้ เช่น แก้ไขด้วยตนเองบน application ที่กำลังใช้งาน แจ้งเจ้าหน้าที่ให้ทำการแก้ไข • ก่อนเริ่มการแก้ไขปรับปรุงข้อมูล มีขั้นตอนการตรวจสอบตัวบุคคลผู้ขอแก้ไขปรับปรุงข้อมูล และมีการตรวจสอบสิทธิของบุคคลผู้ขอแก้ไขปรับปรุงข้อมูล • ในกระบวนการปรับปรุงข้อมูล ผู้ใช้บริการสามารถตรวจสอบความถูกต้องของข้อมูลที่แก้ไขก่อนที่จะมีการบันทึกในระบบให้บริการ **2. การขอให้ระงับการใช้งาน/ยุติการใช้งานอัตลักษณ์ดิจิทัล** • มีขั้นตอนการตรวจสอบตัวบุคคลผู้ขอแก้ไขปรับปรุงข้อมูล และมีการตรวจสอบสิทธิของบุคคลผู้ร้องขอว่าเป็นบุคคลผู้มีสิทธิหรือไม่

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				2.2 ในกรณีที่ผู้ใช้บริการร้องขอให้ระงับการใช้งานชั่วคราว หรือยุติการใช้งานอัตลักษณ์ดิจิทัล ผู้รับใบอนุญาตต้องจัดให้มีกระบวนการอย่างน้อยดังนี้ 2.2.1 มีการตรวจสอบความถูกต้องของคำขอก่อนที่จะดำเนินการตามคำขอ 2.2.2 ป้องกันไม่ให้มีการใช้งานอัตลักษณ์ดิจิทัลตามคำขอ 2.2.3 มีการแจ้งให้ผู้ใช้บริการทราบว่าไม่สามารถใช้งานอัตลักษณ์ดิจิทัลได้ พร้อมระบุเหตุผล เช่น ระงับการใช้งานชั่วคราว ยุติการใช้งาน	• มีขั้นตอน/กระบวนการแจ้งผู้ใช้บริการให้ทราบถึงการระงับ/เพิกถอนการใช้งานอัตลักษณ์ดิจิทัลของบุคคลดังกล่าว • มีกระบวนการที่สามารถตรวจพบได้ว่ามีการร้องขอใช้งานอัตลักษณ์ดิจิทัลที่มีการระงับ/เพิกถอน • มีกลไกหรือมาตรการในการปฏิเสธหรือป้องกันการขอใช้งานอัตลักษณ์ดิจิทัลที่ถูกระงับ/เพิกถอน
X				3. กรณีที่ระบบการให้บริการรองรับการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อย ดังนี้ 3.1 ต้องดำเนินการให้สอดคล้องตามข้อกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตนที่สูงกว่าให้ครบถ้วน 3.2 ต้องจัดให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้นก่อนเริ่มกระบวนการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตน 3.3 เมื่อดำเนินการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตนเสร็จสิ้น ต้องส่งการแจ้งเตือนผู้ใช้บริการทราบผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้ยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตนดังกล่าว เช่น การส่งให้ทางอีเมลของผู้ใช้บริการ	1. การยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตน มีขั้นตอนที่สอดคล้องตามมาตรฐาน (อ้างอิง ขมธอ. 19-2566) สำหรับระดับความน่าเชื่อถือที่สูงขึ้น 2. ก่อนดำเนินการมีการตรวจสอบตัวบุคคลด้วยกระบวนการยืนยันตัวตนและตรวจสอบสิทธิของบุคคลผู้ขอ 3. มีขั้นตอน/กระบวนการแจ้งผู้ใช้บริการให้ทราบผลการยกระดับความน่าเชื่อถือ ซึ่งช่องทางในการแจ้งต้องเป็นคนละช่องทางที่ใช้ในการยกระดับความน่าเชื่อถือฯ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X				4. ผู้รับใบอนุญาตจัดมีการดูแลข้อมูลผู้ใช้บริการอย่างน้อย ดังนี้ 4.1 ต้องรวบรวมหรือจัดเก็บข้อมูลเพื่อการพิสูจน์ตัวตนเพียงเท่าที่จำเป็น เหมาะสม และตรงตามวัตถุประสงค์ของการให้บริการ 4.2 ต้องจำกัดการเปิดเผยข้อมูลอัตลักษณ์ของผู้ใช้บริการต่อบุคคลอื่นเพื่อใช้ในการพิสูจน์ตัวตนตามที่ได้รับความยินยอมจากผู้ใช้บริการ เว้นแต่เป็นกรณีที่ผู้รับใบอนุญาตต้องปฏิบัติตามที่กฎหมายกำหนด	1. มีนโยบายหรือแนวปฏิบัติที่เกี่ยวกับการจัดเก็บ/รวบรวมข้อมูลเพื่อการพิสูจน์ตัวตน และการเปิดเผยข้อมูลอัตลักษณ์ของผู้ใช้บริการที่แสดงให้เห็นได้อย่างชัดเจนว่า • มีการกำหนดวัตถุประสงค์ในการจัดเก็บ/รวบรวม และเงื่อนไขการเปิดเผยข้อมูลฯ • มีการกำหนดถึงระยะเวลาในการจัดเก็บข้อมูล • มีขอบเขต/เงื่อนไขที่ระบุเกี่ยวกับการเปิดเผยข้อมูล 2. มีขั้นตอน/กระบวนการเก็บข้อมูลเพื่อการพิสูจน์ตัวตนที่สอดคล้องตามนโยบายหรือแนวปฏิบัติดังกล่าว
	X	X		5.ผู้รับใบอนุญาตต้องบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนและกระบวนการยืนยันตัวตนให้สอดคล้องตามลักษณะและระดับความเสี่ยงของธุรกรรมหรือการประกอบธุรกิจ	1. กรณีการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน: มีแนวทางในการพิจารณาเลือกใช้งานชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สอดคล้องกับระดับความน่าเชื่อถือของการยืนยันตัวตน (อ้างอิง ขมธอ. 20-2566) โดยพิจารณากำหนดระดับความน่าเชื่อถือตามลักษณะและความเสี่ยงของธุรกรรม ทั้งนี้ การกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตน ต้องมีระดับความน่าเชื่อถือไม่ต่ำกว่าที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกาศกำหนด (AAL2) 2. ในกรณีที่ผู้รับใบอนุญาตอยู่ภายใต้การกำกับดูแลของหน่วยงานกำกับดูแลที่มีการกำหนดระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน ต้องพิจารณาความสอดคล้องตามระดับความน่าเชื่อถือที่หน่วยงานกำกับดูแลกำหนดด้วย

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					3. กระบวน/ขั้นตอนการดำเนินการมีความสอดคล้องตามหลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ **หมายเหตุ** - แนวทางการประเมินความเสี่ยงเพื่อพิจารณากำหนดระดับความน่าเชื่อถือของการยืนยันตัวตน สามารถอ้างอิงตาม ขมธอ. 18-2566 ข้อ 4
	X			6. การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ให้พิจารณาตามข้อกำหนดของการยืนยันตัวตน ภายใต้มาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งครอบคลุมกระบวนการอย่างน้อยดังนี้ 6.1 การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน 6.2 การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน 6.3 การหมดอายุและการออกใหม่ 6.4 การเพิกถอน หรือยุติการใช้งาน	การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน อ้างอิงตาม ขมธอ. 20-2566 โดยพิจารณาตามชนิดของสิ่งที่ใช้ยืนยันตัวตน **1. การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน** 1.1 ตรวจสอบว่าบุคคลดังกล่าวผ่านกระบวนการพิสูจน์ตัวตนมาแล้วตามระดับ IAL ที่กำหนด 1.2 ตรวจสอบชนิดของสิ่งที่ใช้ยืนยันตัวตนตามข้อกำหนด AAL แต่ละระดับ 1.3 ต้องเก็บรักษาข้อมูลของสิ่งที่ใช้ยืนยันตัวตนทั้งหมดที่เชื่อมโยงหรือเคยเชื่อมโยงกับอัตลักษณ์ของผู้ใช้บริการ ตลอดอายุการใช้งาน Digital ID อย่างน้อยประกอบด้วย • วันที่และเวลาที่เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนกับบัญชีของผู้ใช้บริการ • ข้อมูลเกี่ยวกับอุปกรณ์ที่ใช้เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน เช่น IP address หรือ หมายเลขประจำอุปกรณ์ (device identifier)

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					1.4 กรณีที่มีการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนเพิ่มเติม หรือนำสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่แล้วเชื่อมโยงเข้ากับ Digital ID ของผู้ใช้บริการ ต้องจัดให้มีการยืนยันตัวตนที่ระดับ AAL ปัจจุบันหรือสูงกว่า ก่อนที่จะทำการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนดังกล่าว และมีขั้นตอนการแจ้งผลการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนอันใหม่ให้ผู้ใช้บริการทราบผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน เช่น email
	X				**2. การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน** **2.1 การสูญหาย ถูกขโมย เสียหาย** • มีขั้นตอนการระงับการใช้งานสิ่งที่ใช้ยืนยันตัวตน ซึ่งควรดำเนินการได้ทันทีหลังจากตรวจพบหรือได้รับแจ้งว่าสิ่งที่ใช้ยืนยันตัวตนสูญหาย/ถูกขโมย/เสียหาย • กรณีที่เป็นการรับแจ้งจากผู้ใช้บริการ ต้องมีขั้นตอนการตรวจสอบตัวบุคคลผู้แจ้ง โดยกำหนดสิ่งที่ใช้ยืนยันตัวตนสำรองด้วยรหัสลับจดจำหรือสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์ หรือวิธีการอื่นเพื่อตรวจสอบตัวบุคคลผู้แจ้ง **2.2 การออกทดแทน** • มีการกำหนดเงื่อนไข หรือวิธีการ หรือขั้นตอนในการออกสิ่งที่ใช้ยืนยันตัวตนเพื่อทดแทนอันที่สูญหาย/ถูกขโมย/เสียหาย • มีกระบวนการพิสูจน์ตัวตนก่อนดำเนินการออกทดแทน

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					• มีขั้นตอนการแจ้งผลการออกทดแทนสำเร็จให้ผู้ใช้บริการทราบผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้ดำเนินการออกทดแทน เช่น email
	X				**3. การหมดอายุและการออกใหม่ (ถ้ามี)** **3.1 การหมดอายุ** • มีกระบวนการตรวจสอบอายุการใช้งานของสิ่งที่ใช้ยืนยันตัวตน • มีการแจ้งเตือนให้ผู้ใช้บริการทราบถึงระยะเวลาการใช้งานสิ่งที่ใช้ยืนยันตัวตนซึ่งใกล้หมดอายุ • มีกระบวนการ/ขั้นตอนแจ้งให้ผู้ใช้บริการทราบหากมีการใช้งานสิ่งที่ใช้ยืนยันตัวตนซึ่งหมดอายุ **3.2 การออกใหม่** • มีกระบวนการ/เงื่อนไขในการออกสิ่งที่ใช้ยืนยันตัวตนใหม่ทดแทนอันเดิมซึ่งหมดอายุ • ก่อนการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนอันใหม่ ควรมีการสอบทานข้อมูลเกี่ยวกับอัตลักษณ์ที่จะนำมาเชื่อมโยงกับสิ่งที่ใช้ยืนยันตัวตน
	X				**4. การเพิกถอน หรือยุติการใช้งาน** 4.1 มีการกำหนดเงื่อนไขของการเพิกถอนหรือยุติการใช้งานสิ่งที่ใช้ยืนยันตัวตน โดยอย่างน้อยต้องกำหนดให้มีการเพิกถอนหรือยุติการใช้งานสิ่งที่ใช้ยืนยันตัวตนโดยเร็วในกรณีดังต่อไปนี้

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					• เมื่อตรวจพบหรือได้รับแจ้งว่าอัตลักษณ์ดิจิทัลนั้นไม่สามารถนำมาใช้กับบุคคลดังกล่าวได้ต่อไป เช่น เสียชีวิต หรือผู้ใช้บริการเป็นตัวปลอม • เมื่อมีการร้องขอจากผู้ใช้บริการ ซึ่งได้ดำเนินการตรวจสอบตัวบุคคลและสิทธิของผู้ขอแล้ว • เมื่อผู้ใช้บริการมีคุณสมบัติไม่ตรงตามเงื่อนไขที่ผู้รับใบอนุญาตกำหนด 4.2 มีกระบวนการเพิกถอนหรือยุติการใช้งานสิ่งที่ใช้ยืนยันตัวตน 4.3 มีขั้นตอน/กระบวนการแจ้งผู้ใช้บริการให้ทราบถึงการเพิกถอนหรือยุติการใช้งานสิ่งที่ใช้ยืนยันตัวตนของบุคคลดังกล่าว 4.4 มีกระบวนการที่สามารถตรวจพบได้ว่าสิ่งที่ใช้ยืนยันตัวตนถูกเพิกถอนหรือยุติการใช้งานแล้ว 4.5 มีกลไกหรือมาตรการในการปฏิเสธหรือป้องกันการขอใช้งานสิ่งที่ใช้ยืนยันตัวตนที่ถูกเพิกถอนหรือยุติการใช้งาน
	X	X		7. ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดเกี่ยวกับสิ่งที่ใช้ยืนยันตัวตน ให้พิจารณาตามข้อกำหนดของการยืนยันตัวตนภายใต้มาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งครอบคลุมหัวข้ออย่างน้อยดังต่อไปนี้ 7.1 ชนิดของสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตนตามระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) 7.2 ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน	**1. การพิจารณาตรวจสอบการเลือกใช้งานชนิดของสิ่งที่ใช้ยืนยันตัวตน** • ระดับความน่าเชื่อถือของการยืนยันตัวตนที่เลือกใช้งาน มีการดำเนินการสอดคล้องตามมาตรฐานที่นำมาพิจารณาอ้างอิง

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					ตารางที่ 1 สรุปข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL ข้อกำหนดของการยืนยันตัวตน: ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้ ระดับ AAL — AAL1: ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้ (1) memorized secret (2) out-of-band device (3) SF OTP device (4) SF crypto software (5) SF crypto device (6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่ระดับ AAL2 และ AAL3 AAL2: ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้ (1) MF OTP device (2) MF crypto software (3) memorized secret + out-of-band device (4) memorized secret + SF OTP device (5) memorized secret + SF crypto software (6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่ระดับ AAL3 AAL3: ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้ (1) MF crypto device (2) SF crypto device + memorized secret (3) MF OTP device + SF crypto device (4) MF OTP device เฉพาะที่เป็นฮาร์ดแวร์ + SF crypto software (5) SF OTP device เฉพาะที่เป็นฮาร์ดแวร์ + MF crypto software (6) SF OTP device เฉพาะที่เป็นฮาร์ดแวร์ + SF crypto software + memorized secret
	X	X		8.ก่อนดำเนินการยืนยันตัวตน ผู้รับใบอนุญาตต้องตรวจสอบสิ่งที่ใช้ยืนยันตัวตนอย่างน้อยดังนี้ 8.1 ตรวจสอบให้แน่ใจว่าสิ่งที่ใช้ยืนยันตัวตนที่แสดงนั้นถูกต้อง ใช้งานได้ และยังไม่หมดอายุหรือถูกเพิกถอน 8.2 ในกรณีที่ตรวจพบการทำธุรกรรมที่ผิดปกติ ต้องมีการตรวจสอบว่าสิ่งที่ใช้ยืนยันตัวตนนั้น ยังอยู่ภายใต้ความควบคุมของเจ้าของอัตลักษณ์ดิจิทัลที่แท้จริง	1. มีการกำหนดขั้นตอน/กระบวนการในการตรวจสอบสิ่งที่ใช้ในการยืนยันตัวตนตามชนิดของสิ่งที่ใช้ยืนยันตัวตนก่อนดำเนินการยืนยันตัวตน โดยต้องตรวจสอบได้ว่าสิ่งที่ใช้ยืนยันตัวตนนั้น • สามารถใช้งานได้ ไม่ถูกระงับ หรือถูกเพิกถอน หรือยุติการใช้งาน • อยู่ในระหว่างอายุการใช้งาน 2. ต้องมีการกำหนด criteria ของการทำธุรกรรมผิดปกติ เช่น มีการ login จากต่างประเทศ โดยกรณีที่มีการตรวจพบหรือแจ้งเตือนว่าพบการทำธุรกรรมผิดปกติ ระบบมีกลไกหรือขั้นตอนที่สามารถเชื่อมโยงให้เชื่อได้ว่าเจ้าของอัตลักษณ์ดิจิทัลเป็นผู้ใช้งานสิ่งที่ใช้ในการยืนยันตัวตน เช่น เพิ่มการยืนยันด้วย OTP
	X	X		9.ในกรณีที่ผู้ใช้บริการร้องขอให้ระงับการใช้งานสิ่งที่ใช้ยืนยันตัวตนชั่วคราว หรือยุติการใช้งานสิ่งที่ใช้ยืนยันตัวตน ผู้รับใบอนุญาตต้องจัดให้มีกระบวนการอย่างน้อย ดังนี้	1. มีขั้นตอนการตรวจสอบตัวบุคคลผู้ขอ และตรวจสอบสิทธิว่าเป็นผู้มีสิทธิขอให้ระงับการใช้งานหรือไม่ 2. มีขั้นตอน/กระบวนการแจ้งผู้ใช้บริการให้ทราบถึงการระงับ/เพิกถอนการใช้งานสิ่งที่ใช้ยืนยันตัวตนของบุคคลดังกล่าว

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				9.1 มีการตรวจสอบความถูกต้องของคำขอก่อนที่จะดำเนินการตามคำขอ 9.2 มีการแจ้งให้ผู้ใช้บริการทราบว่าไม่สามารถใช้งานสิ่งที่ใช้ยืนยันตัวตนได้พร้อมระบุเหตุผล เช่น ระงับการใช้งานชั่วคราว ยุติการใช้งาน	3. มีกระบวนการที่สามารถตรวจพบได้ว่าสิ่งที่ใช้ยืนยันตัวตนถูกระงับการใช้งานแล้ว 4. มีกลไกหรือมาตรการในการปฏิเสธหรือป้องกันการใช้งานสิ่งที่ใช้ยืนยันตัวตนที่ถูกเพิกถอน
	X	X		10. กรณีที่ระบบการให้บริการรองรับการยกระดับความน่าเชื่อถือของการยืนยันตัวตน ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อย ดังนี้ 10.1 ต้องดำเนินการให้สอดคล้องตามข้อกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตนที่สูงกว่าให้ครบถ้วน 10.2 ต้องจัดให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้นก่อนเริ่มกระบวนการยกระดับความน่าเชื่อถือของการยืนยันตัวตน 10.3 เมื่อดำเนินการยกระดับความน่าเชื่อถือของการยืนยันตัวตนเสร็จสิ้น ต้องส่งการแจ้งเตือนผู้ใช้บริการทราบผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้ยกระดับความน่าเชื่อถือของการยืนยันตัวตน เช่น การส่งให้ทางอีเมลของผู้ใช้บริการ	1. การยกระดับความน่าเชื่อถือของการยืนยันตัวตนพิจารณาขั้นตอนที่สอดคล้องตามมาตรฐาน (อ้างอิง ขมธอ. 20-2566) สำหรับระดับความน่าเชื่อถือที่สูงขึ้น 2. ก่อนดำเนินการมีการตรวจสอบตัวบุคคลด้วยกระบวนการยืนยันตัวตนและตรวจสอบสิทธิของบุคคลผู้ขอ 3. มีขั้นตอน/กระบวนการแจ้งผู้ใช้บริการให้ทราบผลการยกระดับความน่าเชื่อถือ ซึ่งช่องทางในการแจ้งต้องเป็นคนละช่องทางที่ใช้ในการยกระดับความน่าเชื่อถือฯ
X	X	X		11. ผู้รับใบอนุญาตต้องกำหนดโพรโทคอลที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการ (communication protocol) สำหรับเชื่อมโยงคำขอและการตอบกลับ โดยต้องสามารถเชื่อมโยงคำขอไปยังปลายทางที่ระบุโดยผู้ส่งคำขอได้และสามารถเชื่อมโยงการตอบกลับไปยังคำขอต้นทางได้ ซึ่งต้องมีการ	1. มีการกำหนดหลักเกณฑ์หรือข้อกำหนดการเชื่อมต่อสำหรับใช้ในการแลกเปลี่ยนข้อมูลการพิสูจน์ยืนยันตัวตน โดยมีรายละเอียดที่เพียงพอให้ผู้เชื่อมต่อสามารถใช้งานได้ 2. ความสามารถของโพรโทคอลที่นำมาใช้งาน • มีกระบวนการรักษาความมั่นคงปลอดภัยของข้อมูล

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				แจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขความสอดคล้องของระบบการให้บริการ	• มีกลไกป้องกันการ replay attack • กรณีที่เป็น Protocol ซึ่งพัฒนาขึ้นเอง ต้องมีการอธิบายหรือแสดงให้เห็นถึงกระบวนการรักษาความมั่นคงปลอดภัยของข้อมูลที่เพียงพอและสอดคล้องตามหลักเกณฑ์ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เช่น มีการรักษาความลับและความครบถ้วนของข้อมูล
X	X	X		12. ผู้รับใบอนุญาตต้องจัดให้มีนโยบายเกี่ยวกับการเปิดเผยข้อมูลอัตลักษณ์ที่สอดคล้องกับหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลและประกาศให้ผู้ที่เกี่ยวข้องได้รับทราบเป็นการทั่วไป	1. สอบทานนโยบายเกี่ยวกับข้อมูลส่วนบุคคล ในส่วนที่เกี่ยวข้องกับการเปิดเผยข้อมูลอัตลักษณ์ ซึ่งสอดคล้องตามหลักเกณฑ์ที่ประกาศกำหนด 2. มีการแจ้ง/ประกาศให้ผู้ที่เกี่ยวข้องรับทราบ ได้แก่ บุคลากรและผู้ปฏิบัติงานที่เกี่ยวข้องกับข้อมูลอัตลักษณ์ และผู้ใช้บริการ
		X		13. ผู้รับใบอนุญาตต้องจัดให้มีรายการข้อมูลอัตลักษณ์ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลในระบบการให้บริการ โดยต้องมีชุดข้อมูลขั้นต่ำที่สามารถระบุตัวผู้ใช้บริการได้อย่างชัดเจน ประกอบด้วย 13.1 เลขประจำตัวประชาชน 13.2 ชื่อ นามสกุล ภาษาไทย 13.3 ชื่อ นามสกุล ภาษาอังกฤษ (ถ้ามี) 13.4 วัน เดือน ปี เกิด 13.5 ที่อยู่ตามบัตรประจำตัวประชาชน	1. มีชุดข้อมูลขั้นต่ำตามที่หลักเกณฑ์กำหนด ซึ่งพร้อมสำหรับการเชื่อมโยงและแลกเปลี่ยนหากผู้อาศัยการพิสูจน์ยืนยันตัวตนร้องขอข้อมูลของผู้ใช้บริการ และเป็นกรณีที่ได้รับความยินยอมจากผู้ใช้บริการ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
		X		14. ในกรณีที่ดำเนินการยืนยันตัวตนสำเร็จและมีการตอบกลับไปยังคำขอต้นทาง ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อยดังนี้ 14.1 ผลการยืนยันตัวตน ประกอบด้วยผลการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน และข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ 14.2 ต้องจัดให้มีการรักษาความลับของผลหรือข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนในกระบวนการดังกล่าว เพื่อให้มั่นใจว่าเฉพาะบุคคลที่เกี่ยวข้องและมีสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลได้ 14.3 ต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย เพื่อรักษาความครบถ้วนของผลหรือข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตน	1. รายละเอียด/รูปแบบของผลการยืนยันตัวตนที่ใช้สำหรับตอบกลับคำขอ มีข้อมูลขั้นต่ำตามที่กำหนดในข้อ 14.1 2. กระบวนการรักษาความมั่นคงปลอดภัย การรักษาความลับและความครบถ้วนของผลการยืนยันตัวตนและ/หรือข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตน 3. การส่งผลการยืนยันตัวตนดำเนินการผ่านช่องทางที่มีความมั่นคงปลอดภัย 4. ตรวจสอบกระบวนการเข้ารหัสข้อมูล และสิทธิในการเข้าถึงข้อมูลตลอดกระบวนการรับส่งข้อมูล **หมายเหตุ** - ไม่กำหนดรูปแบบผลการยืนยันตัวตนเป็นการเฉพาะ
X	X	X		15. ห้ามมิให้ผู้รับใบอนุญาตส่งข้อมูลที่ใช้สำหรับการตรวจสอบสถานะของหลักฐานแสดงตนให้กับบุคคลอื่น โดยข้อมูลดังกล่าวได้แก่ 15.1 เลขคำร้องขอมีบัตรประจำตัวประชาชน 15.2 หมายเลขชิปบัตรประจำตัวประชาชน 15.3 เลขควบคุมหลังบัตรประจำตัวประชาชน (เลเซอร์ ไอดี (laser ID)) เว้นแต่เป็นกรณีที่ผู้รับใบอนุญาตต้องปฏิบัติตามที่กฎหมายกำหนด	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X		16. ในกรณีที่ผู้รับใบอนุญาตมีการใช้งานข้อมูลชีวมิติในกระบวนการพิสูจน์และยืนยันตัวตน ต้องมีการดำเนินการอย่างน้อย ดังนี้ 16.1 ต้องจัดให้มีการกำกับดูแลการใช้งานเทคโนโลยีชีวมิติตามหลักปฏิบัติ ดังนี้ 16.1.1 มีนโยบายและแนวปฏิบัติการนำเทคโนโลยีชีวมิติมาใช้ในระบบการให้บริการอย่างชัดเจน ซึ่งต้องคำนึงถึงการดำเนินงานที่สำคัญอย่างน้อย ดังนี้ (1) การประเมินความเสี่ยงการนำเทคโนโลยีชีวมิติมาใช้ (2) การปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ (3) การรักษาความมั่นคงปลอดภัยข้อมูลชีวมิติ 16.1.2 มีการบริหารจัดการอัตลักษณ์เพื่อการพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมิติที่สอดคล้องตามมาตรฐานการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน 16.1.3 มีการจัดทำคู่มือหรือแนวปฏิบัติสำหรับบุคลากรที่ปฏิบัติงานเกี่ยวกับการใช้งานข้อมูลชีวมิติ 16.1.4 มีการจัดทำคู่มือหรือการให้คำแนะนำผู้ใช้บริการในการใช้งานข้อมูลชีวมิติ 16.2 ต้องจำกัดการเข้าถึงการควบคุมข้อมูลชีวมิติ ให้สามารถเข้าถึงได้เฉพาะบุคลากรที่เกี่ยวข้องซึ่งผ่านการฝึกอบรมอย่างเหมาะสม และมีการสอบทานสิทธิอย่างสม่ำเสมอ	1. มีนโยบายหรือแนวปฏิบัติที่เกี่ยวข้องกับการใช้งานข้อมูลชีวมิติอย่างชัดเจน ซึ่งมีแนวทางสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและข้อกำหนดในการควบคุมดูแลธุรกิจบริการ Digital ID 2. มีหลักเกณฑ์หรือแนวทางในการประเมินความเสี่ยงในการใช้งานเทคโนโลยีชีวมิติ ซึ่งมีการระบุขอบเขตการใช้งานเทคโนโลยีชีวมิติ กระบวนการควบคุมและการติดตามความเสี่ยง 3. มีหลักเกณฑ์หรือแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลชีวมิติ ซึ่งสอดคล้องกับแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ 4. การกำหนดแนวทางการบริหารจัดการข้อมูลชีวมิติควรมีการพิจารณาหัวข้ออย่างน้อย ดังนี้ • แนวทางในการเลือกระบบรู้จำชีวมิติอัตโนมัติ • การเก็บรักษาและบันทึกข้อมูลชีวมิติ • ความแม่นยำในการเปรียบเทียบข้อมูลชีวมิติควรกำหนดอัตราขั้นต่ำดังนี้ - อัตราการยอมรับที่ผิดพลาด (false accept rate: FAR) ไม่เกิน 0.1% - อัตราการปฏิเสธที่ผิดพลาด (false reject rate: FRR) ไม่เกิน 3% • การประเมินคุณภาพข้อมูลชีวมิติ 5. มีแนวทางการปฏิบัติงานสำหรับบุคลากรที่ปฏิบัติงานเกี่ยวกับการใช้งานข้อมูลชีวมิติโดยมีคู่มือหรือแนวปฏิบัติ และต้องมีการฝึกอบรมก่อนปฏิบัติงาน

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
					6. มีกลไก/กระบวนการในการจำกัดและตรวจสอบสิทธิของผู้เข้าถึงข้อมูลชีวมิติ 7. ความแม่นยำในการเปรียบเทียบข้อมูลชีวมิติต้องมีอัตราการเข้าคู่ผิดพลาด (false match rate: FMR) ไม่เกิน 0.01% และอัตราการไม่เข้าคู่ผิดพลาด (false non-match rate: FNMR) ไม่เกิน 3%
		X		17. ให้ผู้รับใบอนุญาตจัดเก็บข้อมูลประวัติการใช้งานเพื่อประโยชน์ในการสอบทานของผู้ใช้บริการ โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้ผู้ใช้บริการเรียกดูข้อมูลย้อนหลังได้เป็นระยะเวลาไม่น้อยกว่าหกเดือน โดยอย่างน้อยควรมีข้อมูล ดังต่อไปนี้ 17.1 ประวัติกิจกรรมของผู้ใช้บริการที่ได้ดำเนินการผ่านระบบการให้บริการของผู้รับใบอนุญาต 17.2 ประวัติการให้ความยินยอมในการเปิดเผยข้อมูลอัตลักษณ์	1. มีช่องทางสำหรับให้ผู้ใช้บริการตรวจสอบประวัติการใช้งานอัตลักษณ์ดิจิทัลที่ผู้ใช้บริการสามารถเข้าถึงหรือติดต่อได้เป็นการทั่วไป 2. ประวัติการใช้งานอย่างน้อยต้องมีข้อมูลที่พร้อมสำหรับการตรวจสอบตามที่หลักเกณฑ์กำหนด 2.1 ประวัติกิจกรรม อย่างน้อยต้องแสดงให้เห็น • ผู้เกี่ยวข้องกับการใช้งานอัตลักษณ์ดิจิทัล • วันที่ และเวลาของการใช้งานอัตลักษณ์ดิจิทัล • วัตถุประสงค์การใช้งานอัตลักษณ์ดิจิทัล 2.2 ประวัติการให้ความยินยอม อย่างน้อยต้องแสดงให้เห็นรายการข้อมูลของผู้ใช้บริการที่มีการเชื่อมโยงและแลกเปลี่ยนกับบุคคลอื่นในกระบวนการพิสูจน์และยืนยันตัวตน 3. ประวัติการใช้งานต้องไม่มีการแสดงข้อมูลส่วนบุคคล **หมายเหตุ** - ไม่จำกัดรูปแบบหรือช่องทางการตรวจสอบประวัติการใช้งาน
		X		18. การแสดงผลการตรวจสอบประวัติการใช้งานต้องไม่มีการแสดงข้อมูลส่วนบุคคลของผู้ใช้บริการ	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				หมวด 2 **บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล**	
			X	19. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการดูแลข้อมูลส่วนบุคคลอย่างน้อยดังนี้ 19.1 ไม่นำข้อมูลส่วนบุคคลของผู้ใช้บริการมาใช้เป็นตัวระบุ (identifier) ผู้ใช้บริการ 19.2 ไม่จัดเก็บหรือคงไว้ซึ่งข้อมูลส่วนบุคคลของผู้ใช้บริการที่มีการส่งจากผู้รับใบอนุญาตไปยังผู้อาศัยการพิสูจน์และยืนยันตัวตน เว้นแต่เป็นการจัดเก็บโดยมั่นคงปลอดภัยในระหว่างเซสชันการพิสูจน์และยืนยันตัวตน และข้อมูลดังกล่าวต้องไม่สามารถเข้าถึงได้โดยบุคลากรของผู้รับใบอนุญาต	1. มีนโยบายหรือแนวปฏิบัติที่เกี่ยวข้องกับการดูแลข้อมูลส่วนบุคคลของผู้ใช้บริการ ซึ่งกำหนดมาตรการที่ชัดเจนตามที่กำหนด 2. แนวปฏิบัติหรือขั้นตอนการทำงานต้องระบุขอบเขตกิจกรรมให้ชัดเจนเกี่ยวกับขั้นตอนหรือการดำเนินการที่ต้องมีการจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการ 3. หากมีการจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการ จำกัดเฉพาะการจัดเก็บระหว่าง session ที่อยู่ระหว่างการใช้งานเพื่อการพิสูจน์และยืนยันตัวตนในขณะนั้น โดยต้องไม่ปรากฏว่ามีการจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการไว้เกินกว่าที่หลักเกณฑ์กำหนด 4. มีแนวปฏิบัติ/มาตรการ ในการบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของผู้ใช้บริการที่มีการจัดเก็บ 5. แนวทางการป้องกันการเข้าถึงข้อมูลส่วนบุคคลที่มีการจัดเก็บในระหว่าง session
			X	20. ผู้รับใบอนุญาตต้องจัดให้มีการบันทึกประวัติกิจกรรม (log) สำหรับบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลไว้เพื่อการตรวจสอบ (audit log) โดยกรณีที่เป็นคำขอเพื่อการยืนยันตัวตนต้องมีการจัดเก็บประวัติกิจกรรมของการโต้ตอบทั้งหมดที่	1. การจัดเก็บ log ต้องมีข้อมูลขั้นต่ำตามที่ระบุในข้อกำหนดด้าน IT security 2. audit log สำหรับคำขอเพื่อการยืนยันตัวตนมีการจัดเก็บประวัติกิจกรรมการโต้ตอบระหว่าง RP และ IDP ทั้งหมด โดยใช้ตัวระบุ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				เกี่ยวข้องกับคำขอเพื่อการยืนยันตัวตนดังกล่าว โดยใช้ตัวระบุเฉพาะของการโต้ตอบเดียวกัน (unique interaction identifier) สำหรับแต่ละเหตุการณ์	เฉพาะเดียวกันในเหตุการณ์นั้นๆ ซึ่งตัวระบุเฉพาะต้องไม่ใช่ข้อมูลส่วนบุคคลของผู้ใช้บริการ
			X	21. ในการกำหนดเงื่อนไขความสอดคล้องของระบบการให้บริการเพื่อให้บุคคลอื่นสามารถเชื่อมต่อได้อย่างมีประสิทธิภาพ ผู้รับใบอนุญาตต้องแจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขความสอดคล้องของระบบการให้บริการอย่างน้อยในเรื่องดังต่อไปนี้ 21.1 ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล (assurance level) ที่สามารถเชื่อมต่อกับระบบการให้บริการ 21.2 โพรโทคอล (protocol) สำหรับเชื่อมโยงคำขอ (request) และการตอบกลับ (response) ในระบบการให้บริการ	1. มีเอกสารหรือข้อมูลแสดงเงื่อนไขในการใช้บริการแลกเปลี่ยนข้อมูล ซึ่งอย่างน้อยต้องกำหนดรายละเอียดเกี่ยวกับ 1.1 ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล (assurance level) ที่สามารถเชื่อมต่อกับระบบการให้บริการ 1.2 การกำหนดโพรโทคอลที่ใช้ในการแลกเปลี่ยนข้อมูลคำขอและการตอบกลับเพื่อการพิสูจน์และยืนยันตัวตน (1) มีการกำหนดหลักเกณฑ์หรือข้อกำหนดการเชื่อมต่อสำหรับใช้ในการแลกเปลี่ยนข้อมูลการพิสูจน์ยืนยันตัวตน โดยมีรายละเอียดที่เพียงพอให้ผู้เชื่อมต่อสามารถใช้งานได้ (2) ความสามารถของโพรโทคอลที่นำมาใช้งาน • มีกระบวนการรักษาความมั่นคงปลอดภัยของข้อมูล • กรณีที่เป็น Protocol ซึ่งพัฒนาขึ้นเอง ต้องมีการอธิบายหรือแสดงให้เห็นถึงกระบวนการรักษาความมั่นคงปลอดภัยของข้อมูลที่เพียงพอและสอดคล้องตามหลักเกณฑ์ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เช่น มีการรักษาความลับของข้อมูล 1.3 รายละเอียดข้อกำหนดทางเทคนิคสำหรับการเชื่อมต่อกับระบบการให้บริการ เช่น เวอร์ชั่นของ library ของระบบ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
			X	22. ในการกำหนดความสอดคล้องของระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล ผู้รับใบอนุญาตต้องพิจารณาดำเนินการอย่างน้อย ดังนี้ 22.1 จัดให้มีรายชื่อและระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนของผู้รับใบอนุญาตที่เชื่อมต่อกับระบบการให้บริการของตน 22.2 จัดให้มีกลไกที่สามารถคัดแยกผู้รับใบอนุญาตที่เชื่อมต่อกับระบบการให้บริการที่มีระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล ในระดับที่สอดคล้องตามคำขอหรือสูงกว่าคำขอของผู้ส่งคำขอได้	1. มีรายละเอียดที่สามารถแสดงรายชื่อของผู้รับใบอนุญาตและระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนที่สามารถให้บริการได้ของผู้ที่เชื่อมต่อกับระบบการให้บริการ 2. จัดให้มีกลไกที่สามารถในการคัดกรอง แยกแยะ หรือจัดกลุ่มผู้รับใบอนุญาตที่เชื่อมต่อกับระบบการให้บริการ เช่น กลไกการติดตามการปรับระดับความน่าเชื่อถือ ทั้งนี้ เพื่อให้ผู้ใช้งานสามารถทราบและเลือกใช้บริการผู้รับใบอนุญาตได้อย่างถูกต้อง **หมายเหตุ** - ไม่จำกัดรูปแบบหรือวิธีการแสดงผล เช่น กำหนดเป็นคุณสมบัติตั้งต้นสำหรับผู้ที่จะเข้าใช้บริการ แสดงข้อมูลบนหน้าเว็บไซต์ หรือแสดงข้อมูลบนแอปพลิเคชัน - กลไกการคัดกรอง แยกแยะ หรือจัดกลุ่มผู้รับใบอนุญาต ไม่จำกัดว่าต้องเป็นกลไกทางเทคนิค
			X	23. การกำหนดโพรโทคอลที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการ (communication protocol) ต้องสามารถเชื่อมโยงคำขอและการตอบกลับ โดยเชื่อมโยงคำขอไปยังปลายทางที่ระบุโดยผู้ส่งคำขอและสามารถเชื่อมโยงการตอบกลับ	1. มี sequence diagram ที่แสดงให้เห็น flow การทำงานของ communication protocol ซึ่งระบุถึงตัวแปรในแต่ละขั้น 2. มีรายละเอียดที่อธิบายการทำงานของแต่ละ function 3. โพรโทคอลที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการมีการทดสอบการใช้งานตามข้อ 24 และ 25

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ไปยังคำขอต้นทางได้ ซึ่งต้องมีการแจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขความสอดคล้องของระบบการให้บริการ	
			X	24. ผู้รับใบอนุญาตต้องกำหนดส่วนต่อประสานโปรแกรมประยุกต์ (application programming interface) ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนในระบบการให้บริการ (ถ้ามี) โดยอย่างน้อยต้องสามารถเชื่อมโยงรายการต่อไปนี้เข้าด้วยกันได้อย่างถูกต้องและครบถ้วน 24.1 รายการข้อมูลที่กำหนดในคำขอและการตอบกลับ 24.2 ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามที่กำหนดในคำขอและการตอบกลับ	
			X	25. ผู้รับใบอนุญาตต้องจัดให้มีแผนการทดสอบ (testing plan) การเชื่อมโยงและแลกเปลี่ยนข้อมูลบนระบบการให้บริการที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยของระบบการให้บริการ โดยแผนการทดสอบดังกล่าวเป็นส่วนหนึ่งของรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจ	1. มีการกำหนดแผนการทดสอบการทำงานของโพรโทคอลที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการ
			X	26. ผู้รับใบอนุญาตต้องจัดให้มีการทดสอบการใช้งานตามแผนการทดสอบร่วมกับผู้ประสงค์จะเชื่อมต่อกับระบบการให้บริการก่อนเริ่มให้บริการแก่บุคคลดังกล่าว	1. มีเอกสาร/ข้อมูลที่แสดงให้เห็นแผนการทดสอบการเชื่อมต่อระหว่างผู้รับใบอนุญาต กับผู้ที่ประสงค์จะเชื่อมต่อกับระบบการให้บริการโดยสอดคล้องกับเงื่อนไขความสอดคล้องของระบบการให้บริการ 2. ตรวจทานให้แน่ชัดว่าผู้ใช้บริการทุกรายมีการทดสอบการใช้งานก่อนเริ่มใช้บริการจริงและมีการจัดทำรายงานผลการทดสอบการใช้งานสำหรับผู้ใช้งานแต่ละราย
			X	27.ห้ามมิให้เปิดให้บริการแก่ผู้ประสงค์จะเชื่อมต่อกับระบบการให้บริการของผู้รับใบอนุญาตที่ไม่สามารถทดสอบการใช้งานร่วมกัน	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				กับผู้รับใบอนุญาตหรือผลการทดสอบไม่สามารถดำเนินการได้โดยสมบูรณ์	3. ผู้ใช้บริการทุกรายจะต้องปรากฏผลการทดสอบการเชื่อมต่อว่าสามารถดำเนินการได้โดยสมบูรณ์

ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 7

หลักเกณฑ์การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการให้บริการ การคุ้มครองผู้ใช้บริการ และมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
X	X	X	X	1. ผู้รับใบอนุญาตต้องเปิดเผยข้อมูลที่สำคัญซึ่งเกี่ยวข้องกับการให้บริการแก่ผู้ใช้บริการอย่างเพียงพอต่อการตัดสินใจเลือกใช้บริการได้ตรงตามความต้องการ	1. ข้อมูลที่สำคัญซึ่งเกี่ยวข้องกับการให้บริการ เช่น ลักษณะการให้บริการ สถานที่หรือช่องทาง การใช้บริการ ค่าธรรมเนียม และเงื่อนไขการใช้บริการ
X	X	X	X	2. ผู้รับใบอนุญาตต้องจัดให้มีช่องทางในการติดต่อสื่อสารกับผู้ใช้บริการในการรับฟังความคิดเห็น การให้ความช่วยเหลือ การแก้ปัญหา และการรับข้อร้องเรียนที่เกี่ยวข้องกับการให้บริการที่ผู้ใช้บริการสามารถติดต่อได้โดยสะดวก โดยมีการควบคุมดูแลและดำเนินการภายในเวลาที่เหมาะสม	1. มีช่องทางที่เปิดให้ผู้ใช้บริการสามารถติดต่อได้โดยง่าย และเป็นช่องทางที่เผยแพร่ให้ผู้ใช้บริการทราบเป็นการทั่วไป
X	X	X	X	3. ผู้รับใบอนุญาตต้องดูแลให้ข้อมูลที่ใช้ในการติดต่อสื่อสารมีความชัดเจน น่าเชื่อถือ และไม่ทำให้ผู้ใช้บริการสำคัญผิด	1. ข้อมูลที่ใช้ในการสื่อสาร เผยแพร่ประชาสัมพันธ์เกี่ยวกับการให้บริการภายในขอบข่ายที่ได้รับอนุญาตตรงต่อความเป็นจริงและไม่ก่อให้เกิดความเข้าใจผิด เช่น ลักษณะการให้บริการตามประเภทที่ได้รับใบอนุญาต
X	X	X	X	4. ในกรณีที่ระบบการให้บริการของงานที่สำคัญหยุดให้บริการชั่วคราว หรือเกิดปัญหา หรือมีความบกพร่องในการให้บริการ ผู้รับใบอนุญาตต้องดำเนินการดังต่อไปนี้ 4.1 กรณีหยุดให้บริการชั่วคราวอันเกิดจากการเตรียมการไว้ล่วงหน้า เช่น การปรับปรุงระบบงานสำคัญ	1. มีขั้นตอนการดำเนินการสำหรับกรณีที่ต้องหยุดให้บริการทั้งในกรณีที่มีการเตรียมการไว้ล่วงหน้า และกรณีที่ไม่มีการเตรียมการไว้ล่วงหน้า ซึ่งครอบคลุมวิธีการแจ้งให้ผู้ใช้บริการทราบ วิธีการแจ้งให้สำนักงานทราบ 2. มีการสื่อสาร/คู่มือ/แนวปฏิบัติเพื่อให้ผู้ที่เกี่ยวข้องรับทราบ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				4.1.1 แจ้งให้สำนักงานทราบล่วงหน้าไม่น้อยกว่าสิบห้าวันก่อนดำเนินการ โดยแจ้งเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ตามที่สำนักงานกำหนด 4.1.2 แจ้งให้ผู้ใช้บริการทราบล่วงหน้าไม่น้อยกว่าเจ็ดวันก่อนดำเนินการ โดยมีรายละเอียดเกี่ยวกับระบบการให้บริการที่หยุดให้บริการชั่วคราว และระยะเวลาหยุดให้บริการเพื่อให้ผู้ใช้บริการทราบได้อย่างชัดเจน 4.2 กรณีหยุดให้บริการชั่วคราวโดยไม่ได้มีการเตรียมการไว้ล่วงหน้า 4.2.1 แจ้งให้สำนักงานทราบโดยเร็วถึงเหตุที่ทำให้งานสำคัญหยุดให้บริการชั่วคราวพร้อมรายละเอียดเป็นหนังสือหรือโดยวิธีการทางอิเล็กทรอนิกส์ตามที่สำนักงานกำหนด 4.2.2 แจ้งให้ผู้ใช้บริการทราบโดยเร็วนับแต่เวลาที่หยุดให้บริการชั่วคราว โดยมีรายละเอียดเกี่ยวกับระบบการให้บริการที่หยุดให้บริการชั่วคราวและระยะเวลาหยุดหรือคาดว่าจะหยุดให้บริการเพื่อให้ผู้ใช้บริการทราบได้อย่างชัดเจน 4.3 กรณีเกิดปัญหาหรือมีความบกพร่องในการให้บริการให้แจ้งสำนักงานทราบเป็นหนังสือหรือด้วยวิธีการทางอิเล็กทรอนิกส์ตามที่สำนักงานกำหนดโดยเร็ว 4.4 เมื่อการหยุดให้บริการชั่วคราวของงานที่สำคัญสิ้นสุดลงแล้ว หรือผู้รับใบอนุญาตแก้ไขปัญหาหรือความบกพร่องเป็นที่เรียบร้อยแล้ว ให้ผู้รับใบอนุญาตแจ้งสำนักงานทราบโดยเร็ว และต้องจัดเก็บ	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				เอกสารหลักฐานที่เกี่ยวข้องกับการดำเนินการเป็นระยะเวลาไม่น้อยกว่าหนึ่งปีนับแต่วันที่จัดทำเอกสารหลักฐานนั้นในลักษณะที่พร้อมให้สำนักงานสามารถตรวจสอบได้เมื่อได้รับการร้องขอ	
X	X	X	X	5. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการใช้งานระบบการให้บริการซึ่งครอบคลุมรายการอย่างน้อยดังต่อไปนี้ 5.1 การกำหนดช่องทางการติดต่อและให้ความช่วยเหลือที่ผู้ใช้บริการสามารถติดต่อสื่อสารได้โดยสะดวก 5.2 การกำหนดขั้นตอนและมาตรการในการแก้ไขปัญหา การชดใช้หรือเยียวยาผู้ได้รับความเสียหาย และกำหนดเป็นมาตรฐานสำหรับปัญหาที่มีลักษณะคล้ายกัน โดยมีรายละเอียดอย่างน้อยดังนี้ 5.2.1 กำหนดกรอบระยะเวลาในการดำเนินการในแต่ละขั้นตอนให้การจัดการเป็นไปด้วยความเหมาะสมและไม่ชักช้า 5.2.2 กำหนดระยะเวลาและปัจจัยในการพิจารณาชดใช้หรือเยียวยาให้เป็นธรรม โดยเฉพาะกรณีที่เป็นความผิดพลาดจากระบบการให้บริการหรือจากบุคลากรของผู้รับใบอนุญาตและปฏิบัติอย่างเท่าเทียมกันในกรณีที่มีลักษณะเดียวกัน 5.2.3 กำหนดรายละเอียดพร้อมวิธีการในการแก้ไขปัญหาและการชดใช้ค่าเสียหายซึ่งครอบคลุมกรณีดังต่อไปนี้เป็นอย่างน้อย (1) ความเสียหายอันเกิดจากความผิดพลาดหรือการหยุดชะงักของระบบการให้บริการ	1. มีกระบวนการ/ขั้นตอน/แนวปฏิบัติสำหรับการจัดการปัญหา การบรรเทาหรือเยียวยาความเสียหาย และกรอบระยะเวลาในการดำเนินการตามขั้นตอนต่าง ๆ 2. มีการสื่อสารอย่างชัดเจนถึงวิธีการติดต่อและให้ความช่วยเหลือ เช่น จัดให้มีลิงก์ไปยังคุณลักษณะการบริการตนเองแบบออนไลน์ เซสชันการแชท และหมายเลขโทรศัพท์ของฝ่ายช่วยเหลือ และรับข้อร้องเรียน 3. มีช่องทางที่ผู้ใช้บริการสามารถติดต่อได้ตามวัตถุประสงค์ที่หลักเกณฑ์กำหนด โดยเป็นช่องทางที่มีการแจ้งให้ผู้ใช้บริการทราบเป็นการทั่วไป และช่องทางดังกล่าวต้องสามารถติดต่อสื่อสารกับบุคลากรของผู้รับใบอนุญาตเพื่อขอรับความช่วยเหลือหรือคำแนะนำในการใช้บริการได้ 4. มีคู่มือหรือแนวทางสำหรับบุคลากรเพื่อให้คำแนะนำหรือความช่วยเหลือแก่ผู้ใช้บริการ

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				(2) ความเสียหายอันเกิดจากความผิดพลาดหรือบกพร่องในการพิสูจน์หรือยืนยันตัวตน (3) ความเสียหายอันเกิดจากการรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคล (4) ความเสียหายอันเกิดจากการตรวจสอบข้อมูลไม่ถูกต้อง 5.3 การกำหนดขั้นตอนการเยียวยาความเสียหายและการแจ้งผลการดำเนินการให้ผู้ได้รับความเสียหายทราบ โดยมีข้อพึงปฏิบัติดังนี้ 5.3.1 ต้องจัดให้มีข้อตกลงกับผู้ใช้บริการเกี่ยวกับความรับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากการให้บริการ 5.3.2 ข้อตกลงตามข้อ 5.3.1 ต้องไม่มีลักษณะเป็นการตัดหรือจำกัดความรับผิดของผู้รับใบอนุญาตเมื่อมีความเสียหายเกิดขึ้น อันเนื่องมาจากการที่ผู้รับใบอนุญาต กรรมการ ผู้บริหาร หรือบุคลากร ไม่ได้ดำเนินธุรกิจหรือปฏิบัติงานให้เป็นไปตามกฎหมาย 5.3.3 มีการแจ้งผลการดำเนินการให้ผู้ได้รับความเสียหายทราบความคืบหน้าเป็นระยะ	
X	X	X	X	6. ผู้รับใบอนุญาตต้องระบุข้อตกลงเกี่ยวกับการชดใช้หรือเยียวยาความเสียหายไว้ในข้อกำหนดของสัญญาหรือเงื่อนไขการให้บริการอย่างชัดเจน	**หมายเหตุ** - โปรดนำส่งสำเนาสัญญาหรือข้อตกลงการใช้บริการมาพร้อมเอกสารแสดงความพร้อมของระบบงาน
X	X	X	X	7. ผู้รับใบอนุญาตต้องจัดให้มีบุคลากรที่ทำหน้าที่รับเรื่องร้องเรียนซึ่งผู้ใช้บริการสามารถติดต่อโดยตรงได้อย่างสะดวก โดยมีการแจ้งให้	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ผู้ใช้บริการทราบถึงช่องทางและวิธีการแจ้งปัญหาหรือร้องเรียนการใช้บริการได้อย่างชัดเจน	
X	X	X	X	8. ผู้รับใบอนุญาตต้องจัดให้มีมาตรการหรือขั้นตอนในการดำเนินการเมื่อมีการร้องเรียนหรือมีข้อโต้แย้งจากผู้ใช้บริการ รวมทั้งกำหนดกรอบเวลาเพื่อหาข้อยุติ ดังนี้ 8.1 จัดให้มีช่องทางและวิธีการสำหรับการรับข้อร้องเรียนจากผู้ใช้บริการ โดยอย่างน้อยต้องจัดให้มีหมายเลขโทรศัพท์และที่อยู่สำหรับติดต่อได้ หรือที่อยู่สำหรับติดต่อทางจดหมายอิเล็กทรอนิกส์ที่สามารถติดต่อได้ 8.2 กำหนดวิธีปฏิบัติเกี่ยวกับขั้นตอนการดำเนินการและกรอบระยะเวลาเพื่อหาข้อยุติเป็นลายลักษณ์อักษร และจัดให้มีการอบรมวิธีปฏิบัติดังกล่าวให้แก่บุคลากรที่เกี่ยวข้อง 8.3 มีกลไกในการตรวจสอบและแจ้งความคืบหน้า รวมทั้งชี้แจงขั้นตอนการดำเนินการและกำหนดระยะเวลาในการแก้ไขข้อร้องเรียนให้ผู้ร้องเรียนทราบภายในเจ็ดวันนับแต่วันที่ได้รับแจ้งการร้องเรียน 8.4 ดำเนินการแก้ไขข้อร้องเรียนให้แล้วเสร็จ และแจ้งผลการดำเนินการให้ผู้ร้องเรียนทราบโดยเร็ว 8.5 ในกรณีที่ผู้ให้บริการไม่สามารถพิจารณาหรือแก้ไขข้อร้องเรียนให้แล้วเสร็จภายในกำหนดระยะเวลาตามข้อ 8.3 ให้แจ้งความคืบหน้าของการดำเนินการให้ผู้ใช้บริการทราบก่อนครบกำหนดระยะเวลา	**หมายเหตุ** - อ้างอิงตามข้อ 5

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ดังกล่าว และรายงานความคืบหน้าให้ผู้ใช้บริการทราบเพิ่มเติมเป็นระยะจนกว่าการดำเนินการจะแล้วเสร็จ	
X	X	X	X	9. ผู้รับใบอนุญาตต้องรายงานการร้องเรียนหรือฟ้องร้องเกี่ยวกับการประกอบธุรกิจให้สำนักงานทราบ โดยนำส่งพร้อมสรุปผลการดำเนินงานเกี่ยวกับการให้บริการประจำปี ซึ่งอย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้ 9.1 จำนวนเรื่องร้องเรียนหรือฟ้องร้อง 9.2 วันที่และเวลาของการร้องเรียนหรือฟ้องร้องแต่ละรายการ 9.3 การดำเนินการเพื่อแก้ไขปัญหาการร้องเรียนหรือฟ้องร้องแต่ละรายการ 9.4 แนวทางการป้องกันปัญหาเพื่อไม่ให้เกิดเหตุการณ์ดังกล่าวซ้ำอีก	**หมายเหตุ** - รายละเอียดเป็นไปตามหลักเกณฑ์เกี่ยวกับการนำส่งข้อมูลประจำปี
X	X	X	X	10. ในกรณีที่เป็นการร้องเรียนหรือฟ้องร้องเกี่ยวกับการประกอบธุรกิจที่มีนัยสำคัญซึ่งส่งผลกระทบต่อการให้บริการและเป็นปัญหาสำคัญที่ผู้รับใบอนุญาตต้องรายงานต่อผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย ผู้รับใบอนุญาตต้องรายงานมายังสำนักงานเมื่อรับทราบการร้องเรียนหรือฟ้องร้องดังกล่าวโดยเร็ว และให้แจ้งผลการดำเนินการแก้ไขปัญหาเพิ่มเติมภายหลัง	**หมายเหตุ** - รายละเอียดเป็นไปตามหลักเกณฑ์/วิธีการ/ช่องทางที่สำนักงานประกาศกำหนด
X	X	X	X	11. ในกรณีที่ผู้ใช้บริการแจ้งข้อร้องเรียนต่อสำนักงานและสำนักงานได้แจ้งให้ผู้รับใบอนุญาตทราบแล้ว ให้ผู้รับใบอนุญาตดำเนินการเกี่ยวกับข้อร้องเรียนดังกล่าวตามหลักเกณฑ์ในข้อ 8 และรายงานผลการดำเนินการให้สำนักงานทราบภายในสามสิบวันนับแต่วันที่ได้รับทราบ	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				ข้อร้องเรียนจากสำนักงาน ทั้งนี้ หากการดำเนินการพิจารณาหรือแก้ไขปัญหาเกี่ยวกับข้อร้องเรียนไม่แล้วเสร็จภายในระยะเวลาดังกล่าว ให้รายงานความคืบหน้าเป็นระยะต่อสำนักงานจนกว่าการดำเนินการจะแล้วเสร็จ เว้นแต่สำนักงานจะกำหนดเป็นอย่างอื่น	

ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. 1/2566 ฉบับที่ 8

หลักเกณฑ์การใช้บริการจากผู้รับดำเนินการแทน

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
x	x	x	x	1. ผู้รับใบอนุญาตสามารถใช้บริการจากผู้รับดำเนินการแทนได้โดยต้องมีแนวทางการบริหารความเสี่ยงและแนวทางการดูแลผู้ใช้บริการที่เหมาะสม เว้นแต่งานหลักที่เกี่ยวข้องกับการตัดสินใจในผลการพิสูจน์และยืนยันตัวตนซึ่งอาจส่งผลกระทบต่อฐานะการดำเนินงานและความเสี่ยงของผู้รับใบอนุญาตหากดำเนินการไม่เหมาะสมไม่สามารถให้ผู้รับดำเนินการแทนดำเนินการได้ ดังต่อไปนี้ 1.1 งานที่เกี่ยวกับการวิเคราะห์เชิงลึก การตรวจสอบหรือการสอบทานในขั้นตอนดังนี้ 1.1.1 การตัดสินใจหรือการนำส่งผลการพิสูจน์ตัวตน หรือ 1.1.2 การเชื่อมโยงอัตลักษณ์ของบุคคลเข้ากับสิ่งที่ใช้ยืนยันตัวตน หรือ 1.1.3 การตัดสินใจหรือการนำส่งผลการยืนยันตัวตน 1.2 งานที่เกี่ยวกับการติดตาม การตรวจสอบ และการสอบทานภายหลังขั้นตอนดังนี้ 1.2.1 การตัดสินใจหรือนำส่งผลการพิสูจน์ตัวตน หรือ 1.2.2 การเชื่อมโยงข้อมูลอัตลักษณ์ของบุคคลเข้ากับสิ่งที่ใช้ยืนยันตัวตน หรือ 1.2.3 การตัดสินใจหรือการนำส่งผลการยืนยันตัวตน	1. มีนโยบาย/แผนงาน/มติที่ประชุม ที่ได้รับอนุมัติหรือได้รับความเห็นชอบสำหรับการใช้บริการจากผู้รับดำเนินการแทน รวมถึงขอบเขตการใช้บริการ 2. มีแนวทางการประเมินและบริหารจัดการความเสี่ยงจากการใช้บริการจากผู้รับดำเนินการแทน และมีการกำหนดรอบการทบทวนการบริหารจัดการความเสี่ยงสำหรับกรณีดังกล่าว

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
x	x	x	x	2. ในกรณีที่ผู้รับใบอนุญาตใช้บริการจากผู้รับดำเนินการแทนในการให้บริการผู้รับใบอนุญาตต้องดูแลให้ผู้รับดำเนินการแทนสามารถให้บริการแก่ผู้ใช้บริการเสมือนผู้รับใบอนุญาตเป็นผู้ดำเนินการเอง และต้องกำหนดแนวทางการใช้บริการจากผู้รับดำเนินการแทนอย่างเหมาะสมโดยอย่างน้อยต้องประกอบด้วย 2.1 การกำหนดขอบเขตและลักษณะการใช้บริการ โดยมีการกำหนดบทบาท หน้าที่ และความรับผิดชอบระหว่างผู้รับใบอนุญาตกับผู้รับดำเนินการแทนอย่างชัดเจนและเป็นลายลักษณ์อักษร และพร้อมสำหรับการตรวจสอบเมื่อสำนักงานร้องขอ 2.2 การกำหนดแนวทางการคัดเลือกผู้รับดำเนินการแทนอย่างเหมาะสมก่อนการทำสัญญาหรือข้อตกลงร่วมกัน หรือการทบทวนเพื่อต่ออายุสัญญาหรือข้อตกลงดังกล่าว ซึ่งครอบคลุมประเด็นสำคัญดังต่อไปนี้ 2.2.1 ความสามารถทางด้านเทคนิค ความเชี่ยวชาญ ประสบการณ์ และความพร้อมในการดำเนินงาน 2.2.2 ชื่อเสียงทางธุรกิจ ประวัติการถูกร้องเรียนหรือการฟ้องร้องดำเนินคดีในเรื่องที่เกี่ยวกับงานที่จะให้ดำเนินการ 2.2.3 มีหลักเกณฑ์ในการพิจารณาการใช้บริการที่มีส่วนเกี่ยวข้องกับกรรมการหรือผู้บริหารระดับสูงของผู้รับใบอนุญาต (conflict of interest)	1. มีนโยบาย/แนวทางในการคัดเลือก การดูแล ติดตาม หรือประเมินการทำงานของผู้รับดำเนินการแทน 2. มีการจัดทำสัญญาการใช้บริการซึ่งครอบคลุมประเด็นต่างๆ ที่หลักเกณฑ์กำหนด 3. มีการจัดเตรียมมาตรการรองรับกรณีที่ผู้รับดำเนินการแทนไม่สามารถปฏิบัติงานได้ หรือระบบการให้บริการหยุดชะงัก **หมายเหตุ** - โปรดนำส่งสำเนาสัญญาการใช้บริการจากผู้รับดำเนินการแทนมาพร้อมเอกสารแสดงความพร้อมของระบบงาน

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				2.2.4 ความเสี่ยงในกรณีที่ผู้รับดำเนินการแทนให้บริการแก่ผู้รับใบอนุญาตรายอื่นหลายรายพร้อมกัน 2.2.5 มีหลักเกณฑ์การพิจารณาคัดเลือกในกรณีที่ผู้รับดำเนินการแทนเป็นผู้ให้บริการต่างประเทศ ซึ่งสอดคล้องตามขอบเขตระดับความเสี่ยงและนัยสำคัญของการใช้บริการ 2.3 การประเมินและบริหารจัดการความเสี่ยงจากการใช้บริการที่เหมาะสมตามระดับความสำคัญและผลกระทบในการให้บริการ โดยมีการทบทวนการบริหารจัดการความเสี่ยงอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ 2.4 กำหนดมาตรการรองรับที่ทำให้สามารถประกอบธุรกิจได้อย่างต่อเนื่อง (business continuity management) ในกรณีที่ผู้รับดำเนินการแทนไม่สามารถดำเนินงานได้หรือการให้บริการหยุดชะงักลง 2.5 การจัดทำสัญญาหรือข้อตกลงกับผู้รับดำเนินการแทนควรครอบคลุมประเด็นสำคัญอย่างน้อยดังต่อไปนี้ 2.5.1 รายละเอียดการใช้บริการ ขอบเขตความรับผิดชอบการบริหารความเสี่ยง 2.5.2 ข้อตกลงการให้บริการเพื่อเป็นมาตรฐานขั้นต่ำที่ต้องปฏิบัติ 2.5.3 แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเพื่อรองรับกรณีการให้บริการมีปัญหาหยุดชะงักและไม่สามารถให้บริการได้อย่างต่อเนื่อง	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
				2.5.4 ขั้นตอนการติดตาม ตรวจสอบ ประเมินประสิทธิภาพการปฏิบัติงาน 2.5.5 ค่าบริการ (ถ้ามี) 2.5.6 อายุสัญญาหรือข้อตกลง และเงื่อนไขเกี่ยวกับการต่ออายุ การแก้ไข และการยกเลิกสัญญา 2.5.7 ขอบเขตความรับผิดชอบในกรณีเกิดปัญหาหรือข้อขัดข้องในการให้บริการ เช่น การให้บริการล่าช้า หรือมีข้อผิดพลาดในการให้บริการ เป็นต้น รวมถึงแนวทางการแก้ไขปัญหาและการชดใช้ค่าเสียหายที่อาจเกิดมีขึ้น 2.5.8 การรักษาความมั่นคงปลอดภัยของข้อมูล การรักษาความลับ และความเป็นส่วนตัวของผู้ใช้บริการและผู้รับใบอนุญาต 2.5.9 การปฏิบัติตามหลักเกณฑ์ที่เกี่ยวข้องกับระบบการให้บริการ 2.5.10 เงื่อนไขอื่นๆ ตามความจำเป็น เช่น การประกันภัย 2.5.11 การกำหนดเงื่อนไขในสัญญาหรือข้อตกลงเกี่ยวกับการให้ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก และสำนักงานมีสิทธิเข้าตรวจสอบการดำเนินการของผู้รับดำเนินการแทน 2.6 การดูแลให้ผู้รับดำเนินการแทนปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง	

ลักษณะบริการ				ข้อกำหนด	แนวทางในการประเมิน
IdP 1	IdP 2	IdP 3	Ex.		
x	x	x	x	3. ผู้รับใบอนุญาตต้องให้สำนักงาน หรือผู้ตรวจสอบ สามารถเข้าตรวจสอบการดำเนินงาน ระบบการควบคุมภายในต่างๆ รวมถึงการเรียกดูข้อมูลที่เกี่ยวกับการตรวจสอบการดำเนินงานของผู้รับดำเนินการแทน รวมถึงการจัดเตรียมข้อมูลที่เกี่ยวข้องกับระบบการให้บริการให้มีความถูกต้องและเป็นปัจจุบันให้สามารถตรวจสอบได้	**ไม่ใช้ในการตรวจประเมิน**
x	x	x	x	4. ในกรณีที่ผู้รับใบอนุญาตใช้บริการจากผู้รับดำเนินการแทนในการเก็บรวบรวมหรือเก็บรักษาข้อมูลเกี่ยวกับระบบการให้บริการ เช่น การเก็บรวบรวมหรือเก็บรักษาข้อมูลผู้ใช้บริการในขั้นตอนการพิสูจน์ตัวตน ผู้รับใบอนุญาตต้องแจ้งให้สำนักงานทราบภายในสิบห้าวันนับแต่วันที่เริ่มใช้บริการตามแบบที่จัดไว้บนเว็บไซต์ของสำนักงาน	**ไม่ใช้ในการตรวจประเมิน** **หมายเหตุ** - รายละเอียดเป็นไปตามหลักเกณฑ์/วิธีการ/ช่องทางที่สำนักงานประกาศกำหนด
x	x	x	x	5. กรณีที่มีการเปลี่ยนแปลงการใช้บริการจากผู้รับดำเนินการแทนซึ่งแตกต่างจากที่แจ้งไว้ตามข้อ 4 ให้ผู้รับใบอนุญาตแจ้งให้สำนักงานทราบภายในสิบห้าวันนับแต่วันที่มีการเปลี่ยนแปลง	**ไม่ใช้ในการตรวจประเมิน** **หมายเหตุ** - รายละเอียดเป็นไปตามหลักเกณฑ์เกี่ยวกับการแจ้งการเปลี่ยนแปลงที่สำคัญตามที่สำนักงานประกาศกำหนด

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 20-22 เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง
เขตห้วยขวาง กรุงเทพฯ 10310
โทรศัพท์ : 02 123 1234 | โทรสาร : 02 123 1200

: ETDA THAILAND