



ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์

โดยที่เป็นการสมควรอธิบายภาพรวมของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ มีแนวทางในการให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย และช่วยสร้างความมั่นใจให้กับผู้ส่งข้อมูลและผู้รับข้อมูลที่ใช้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ว่าข้อมูลได้รับการปกป้องจากความเสี่ยงของการสูญหาย การโจรกรรม ความเสียหาย หรือการเปลี่ยนแปลงใด ๆ โดยไม่ได้รับอนุญาต

อาศัยอำนาจตามความในมาตรา ๕ แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์ เลขที่ ชมธอ. ๓๕-๒๕๖๖ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๑๙ เมษายน พ.ศ. ๒๕๖๖

๑.๑๕

(นายศักดิ์ เสกขุนทด)

ที่ปรึกษา รักษาการในตำแหน่งรองผู้อำนวยการ
ปฏิบัติการแทนผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์



ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ
และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard
for Electronic Transactions

ชมธอ. 35-2566

ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์

ELECTRONIC DELIVERY SERVICE

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์

ชมธอ. 35-2566

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ 19 เมษายน พ.ศ. 2566

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์ฉบับนี้ จัดทำขึ้นเพื่ออธิบายภาพรวมของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ มีแนวทางในการให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย และช่วยสร้างความมั่นใจให้กับผู้ส่งข้อมูลและผู้รับข้อมูลที่ใช้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ว่าข้อมูลได้รับการปกป้องจากความเสี่ยงของการสูญหาย การโจรกรรม ความเสียหาย หรือการเปลี่ยนแปลงใด ๆ โดยไม่ได้รับอนุญาต

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อเสนอแนะ ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์ฉบับนี้ จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ โนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22 เลขที่ 33/4 ถนนพระราม 9

แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310

โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200

อีเมล: estandard.center@etda.or.th

เว็บไซต์: www.etda.or.th

คำนำ

ปัจจุบันธุรกรรมทางอิเล็กทรอนิกส์มีบทบาทสำคัญในการดำเนินธุรกิจในระบบเศรษฐกิจยุคใหม่ ทำให้ผู้ประกอบการต่าง ๆ ต้องพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ ให้มีความสะดวก รวดเร็ว และมีประสิทธิภาพ แต่เนื่องจากในการพัฒนานั้นมีระยะเวลาและต้นทุนที่สูง ผู้ประกอบการหลายรายจึงมีแนวคิดที่จะลดระยะเวลาและต้นทุนในการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ จึงหันมาใช้บริการจาก “ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์” หรือ “ผู้ให้บริการ” ซึ่งทำหน้าที่ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ระหว่างผู้ประกอบการกับหน่วยงานภาครัฐหรือกับผู้ประกอบการรายอื่น ผู้ให้บริการดังกล่าวจึงมีบทบาทสำคัญต่อการสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ให้มีการเชื่อมโยงเครือข่ายเข้าด้วยกัน มีการใช้ทรัพยากรร่วมกัน มีการประมวลผลและกระจายข้อมูลไปตามหน่วยงานต่าง ๆ ทำให้ต้องมีการรักษาความมั่นคงปลอดภัยสารสนเทศและข้อมูลอิเล็กทรอนิกส์ให้มีความถูกต้องครบถ้วน พร้อมใช้งาน และน่าเชื่อถือ

ด้วยเหตุนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำข้อเสนอแนะมาตรฐานฯ ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์ เพื่ออธิบายภาพรวมของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ มีแนวทางในการให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย และช่วยสร้างความมั่นใจให้กับผู้ส่งข้อมูลและผู้รับข้อมูลที่ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ โดยข้อเสนอแนะมาตรฐานฉบับนี้สามารถใช้ได้กับบริการนำส่งข้อมูลอิเล็กทรอนิกส์ให้กับกรมสรรพากร บริการนำส่งข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงานที่เชื่อมต่อกับระบบ National Single Window (NSW) หรือบริการนำส่งข้อมูลอิเล็กทรอนิกส์อื่น ๆ ที่ต้องการความน่าเชื่อถือในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์

สารบัญ

	หน้า
1. ขอบข่าย	1
2. บทนิยาม	1
3. ภาพรวมของบริการนำส่งข้อมูลอิเล็กทรอนิกส์	2
3.1 การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 3-corner model	2
3.2 การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 4-corner model	3
4. ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์	5
4.1 การใช้ช่องทางการสื่อสารที่มีความมั่นคงปลอดภัย (protected channel)	6
4.2 การเข้ารหัสลับของข้อมูล (message encryption)	6
4.3 การระบุตัวผู้ส่งข้อมูลต้นทาง (sender identification)	7
4.4 การระบุตัวผู้รับข้อมูลปลายทาง (recipient identification)	7
4.5 การอ้างอิงเวลา (time reference)	8
4.6 หลักฐานการส่งและการรับข้อมูล (evidence of sending and receiving)	9
5. ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ	10
5.1 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ	10
5.2 มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ	10
5.2.1 มาตรการควบคุมด้านองค์กร (organizational controls)	11
5.2.2 มาตรการควบคุมด้านกายภาพ (physical controls)	17
5.2.3 มาตรการควบคุมด้านบุคลากร (people controls)	19
5.2.4 มาตรการควบคุมด้านเทคโนโลยี (technological controls)	20
บรรณานุกรม	25

สารบัญรูป

	หน้า
รูปที่ 1 การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 3-corner model	3
รูปที่ 2 การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 4-corner model	4

สารบัญตาราง

	หน้า
ตารางที่ 1 ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์	6

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้อธิบายภาพรวมของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ มีแนวทางในการให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย และช่วยสร้างความมั่นใจให้กับผู้ส่งข้อมูลและผู้รับข้อมูลที่ใช้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ว่าข้อมูลได้รับการปกป้องจากความเสี่ยงของการสูญหาย การโจรกรรม ความเสียหาย หรือการเปลี่ยนแปลงใด ๆ โดยไม่ได้รับอนุญาต

ข้อเสนอแนะมาตรฐานฉบับนี้สามารถใช้ได้กับหน่วยงานที่เป็นผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ เช่น

- ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ให้กับกรมสรรพากร
- ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงานที่เชื่อมต่อกับระบบ National Single Window (NSW)
- ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์อื่น ๆ ที่ต้องการความน่าเชื่อถือในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์

อย่างไรก็ตาม บริการนำส่งข้อมูลอิเล็กทรอนิกส์ตามข้อเสนอแนะมาตรฐานฉบับนี้ไม่ได้ระบุเฉพาะเจาะจงให้ใช้วิธีการใดวิธีการหนึ่ง เช่น รูปแบบของการนำส่งข้อมูลอิเล็กทรอนิกส์ (message delivery model) เกณฑ์วิธีการรับส่งข้อมูล (messaging protocol) รูปแบบของข้อมูล (message format) หรือรูปแบบของหลักฐานการส่งและการรับข้อมูล (evidence format) ดังนั้น ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์สามารถใช้วิธีการที่แตกต่างกันตามหลักเกณฑ์ที่กำหนดไว้โดยหน่วยงานกำกับดูแลหรือหน่วยงานที่เกี่ยวข้องกับบริการนำส่งข้อมูลอิเล็กทรอนิกส์

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

- 2.1 บริการนำส่งข้อมูลอิเล็กทรอนิกส์ (electronic delivery service) หมายถึง บริการที่ช่วยให้ผู้ส่งข้อมูลและผู้รับข้อมูลสามารถรับส่งข้อมูลด้วยวิธีการทางอิเล็กทรอนิกส์ รวมถึงช่วยบันทึกหลักฐานการส่งและการรับข้อมูล และช่วยปกป้องข้อมูลจากความเสี่ยงของการสูญหาย การโจรกรรม ความเสียหาย หรือการเปลี่ยนแปลงใด ๆ โดยไม่ได้รับอนุญาต
- 2.2 ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ (electronic delivery service provider) หรือ ผู้ให้บริการ (service provider) หมายถึง หน่วยงานที่ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์
- 2.3 ผู้ส่งข้อมูลต้นทาง (original sender) หมายถึง บุคคลซึ่งเป็นผู้ส่งข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีการที่ผู้นั้นกำหนด โดยบุคคลนั้นอาจจะส่งข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้อีก ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์

- 2.4 ผู้รับข้อมูลปลายทาง (final recipient) หมายถึง บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้ และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์

3. ภาพรวมของบริการนำส่งข้อมูลอิเล็กทรอนิกส์

บริการนำส่งข้อมูลอิเล็กทรอนิกส์ (electronic delivery service) เป็นการรับส่งข้อมูลระหว่างผู้ส่งข้อมูลต้นทาง (original sender) กับผู้รับข้อมูลปลายทาง (final recipient) ผ่านผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ โดยผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์จะทำหน้าที่จัดทำหลักฐานการส่งและการรับข้อมูลเพื่อยืนยันเหตุการณ์ที่เกิดขึ้นระหว่างการรับส่งข้อมูล (เช่น หลักฐานที่ยืนยันว่าผู้ให้บริการได้รับข้อมูลต้นฉบับจากผู้ส่งข้อมูลแล้ว หลักฐานที่ยืนยันว่าผู้ให้บริการได้ส่งข้อมูลไปยังผู้รับข้อมูลแล้ว) ซึ่งมีลักษณะคล้ายกับบริการไปรษณีย์ลงทะเบียนที่ใช้สำหรับการส่งเอกสารกระดาษที่เป็นหลักฐานสำคัญ ทั้งนี้ หลักฐานการส่งและการรับข้อมูลสามารถใช้เพื่อพิสูจน์ว่า การทำธุรกรรมรับส่งข้อมูลเกิดขึ้นระหว่างผู้ส่งข้อมูลกับผู้รับข้อมูลที่เกี่ยวข้อง และเกิดขึ้น ณ เวลาตามที่ปรากฏในหลักฐานดังกล่าว

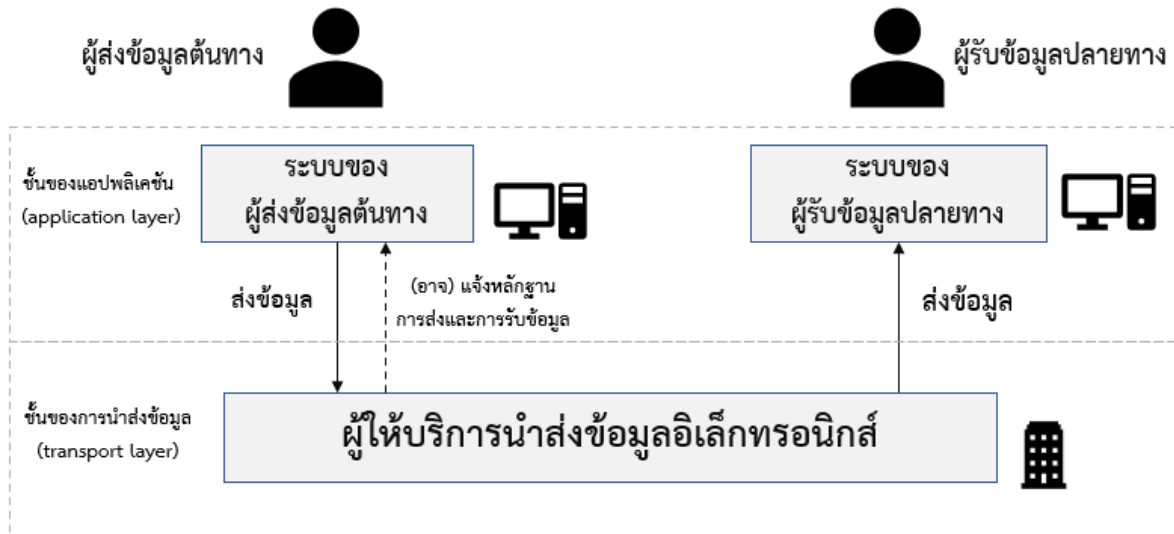
บริการนำส่งข้อมูลอิเล็กทรอนิกส์อาจมีรูปแบบของการนำส่งข้อมูลอิเล็กทรอนิกส์ (message delivery model) ที่แตกต่างกัน แต่จะไม่รวมถึงกรณีที่ผู้ส่งข้อมูลต้นทางส่งข้อมูลไปยังผู้รับข้อมูลปลายทางโดยตรง เช่น การส่งข้อมูลจากเครื่องเซิร์ฟเวอร์ของผู้ส่งข้อมูลต้นทางไปยังเครื่องเซิร์ฟเวอร์ของผู้รับข้อมูลปลายทาง

รูปแบบโดยทั่วไปของการนำส่งข้อมูลทางอิเล็กทรอนิกส์สามารถอธิบายรายละเอียด ดังนี้

3.1 การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 3-corner model

การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 3-corner model (ตามรูปที่ 1) เป็นการรับส่งข้อมูลระหว่างผู้ส่งข้อมูลต้นทางกับผู้รับข้อมูลปลายทาง ผ่านผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ โดยระบบ (user agent) ของผู้ส่งข้อมูลต้นทางและผู้รับข้อมูลปลายทางเป็นแอปพลิเคชันที่โต้ตอบโดยตรงกับผู้ใช้งานที่เป็นบุคคล (เช่น แอปพลิเคชันบนเว็บ หรือแอปพลิเคชันบนอุปกรณ์เคลื่อนที่) หรือแอปพลิเคชันระดับองค์กร (enterprise application) (เช่น ระบบบริหารจัดการทรัพยากรองค์กร) ซึ่งอาจมีหรือไม่มีผู้ใช้งานที่เป็นบุคคลเข้ามามีส่วนร่วม

ระบบ (user agent) ของผู้ส่งข้อมูลต้นทางทำหน้าที่เตรียมข้อมูลต้นฉบับและส่งไปยังผู้ให้บริการ รวมถึงอาจรองรับการใช้ลายมือชื่อดิจิทัลประกอบกับข้อมูลต้นฉบับ หรือการเข้ารหัสลับข้อมูล (end-to-end encryption) ระหว่างผู้ส่งข้อมูลต้นทางและผู้รับข้อมูลปลายทาง [1] โดยผู้ส่งข้อมูลต้นทางหรือผู้รับข้อมูลปลายทางอาจเป็นผู้พัฒนาระบบดังกล่าวเอง หรือใช้บริการด้านซอฟต์แวร์จากหน่วยงานภายนอกที่เป็นผู้ให้บริการแอปพลิเคชัน (application service provider) ก็ได้



รูปที่ 1 การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 3-corner model

การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 3-corner model มีขั้นตอนทั่วไป ดังนี้

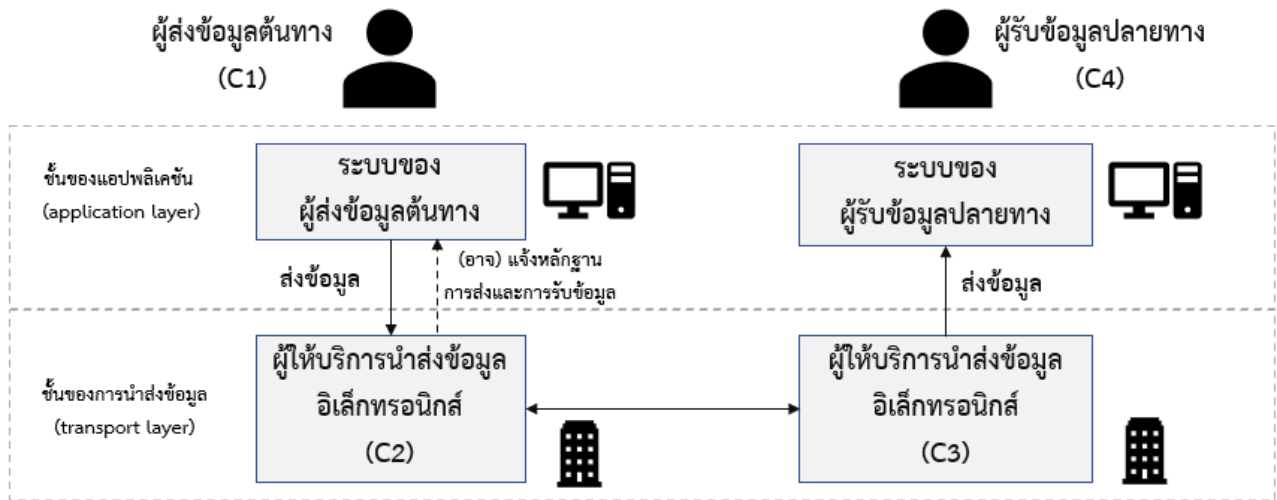
- (1) ผู้ส่งข้อมูลต้นทางยืนยันตัวตนเพื่อเข้าใช้บริการนำส่งข้อมูลอิเล็กทรอนิกส์
- (2) ผู้ส่งข้อมูลต้นทางหรือระบบของผู้ส่งข้อมูลต้นทางเตรียมข้อมูลต้นฉบับ ทั้งนี้ ข้อมูลต้นฉบับอาจประกอบด้วยลายมือชื่อดิจิทัลซึ่งใช้ระบุและยืนยันตัวผู้ส่งข้อมูลต้นทาง
- (3) ระบบของผู้ส่งข้อมูลต้นทางส่งข้อมูลต้นฉบับไปยังผู้ให้บริการ
- (4) ผู้ให้บริการจัดทำหลักฐานเพื่อยืนยันว่าผู้ให้บริการได้รับข้อมูลต้นฉบับแล้ว ทั้งนี้ ผู้ให้บริการอาจส่งหลักฐานนั้นให้ผู้ส่งข้อมูลต้นทาง หรือจัดเก็บหลักฐานนั้นเป็นระยะเวลาหนึ่งเพื่อให้ผู้ที่เกี่ยวข้องเข้าถึงได้ในภายหลัง
- (5) ผู้ให้บริการส่งข้อมูลไปยังระบบของผู้รับข้อมูลปลายทาง
- (6) ผู้ให้บริการจัดทำหลักฐานเพื่อยืนยันว่าผู้ให้บริการได้ส่งข้อมูลไปยังผู้รับข้อมูลปลายทางแล้ว ทั้งนี้ ผู้ให้บริการอาจส่งหลักฐานนั้นให้ผู้ส่งข้อมูลต้นทาง หรือจัดเก็บหลักฐานนั้นเป็นระยะเวลาหนึ่งเพื่อให้ผู้ที่เกี่ยวข้องเข้าถึงได้ในภายหลัง
- (7) ผู้รับข้อมูลปลายทางยืนยันตัวตนเพื่อเข้าใช้บริการนำส่งข้อมูลอิเล็กทรอนิกส์
- (8) ผู้รับข้อมูลปลายทางหรือระบบของผู้รับข้อมูลปลายทางเข้าถึงข้อมูลจากบริการนำส่งอิเล็กทรอนิกส์

3.2 การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 4-corner model

การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 4-corner model (ตามรูปที่ 2) เป็นการรับส่งข้อมูลระหว่างผู้ส่งข้อมูลต้นทาง (C1) กับผู้รับข้อมูลปลายทาง (C4) ผ่านผู้ให้บริการฝั่งผู้ส่งข้อมูลต้นทาง (C2) และผู้ให้บริการฝั่งผู้รับข้อมูลปลายทาง (C3) ตามลำดับ เนื่องจากผู้ส่งข้อมูลต้นทางและผู้รับข้อมูลปลายทางอาจจะสมัครใช้บริการหรือเชื่อมต่อกับผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ที่แตกต่างกัน ทั้งนี้ รูปแบบ 4-corner model จะระบุผู้ส่งข้อมูลต้นทาง ผู้ให้บริการฝั่งผู้ส่งข้อมูลต้นทาง ผู้ให้บริการฝั่งผู้รับข้อมูลปลายทาง และผู้รับข้อมูลปลายทาง ด้วย C1, C2, C3 และ C4 ตามลำดับ

นอกจากนี้ ผู้ให้บริการฝั่งผู้ส่งข้อมูลต้นทางและผู้ให้บริการฝั่งผู้รับข้อมูลปลายทางจะมีการกำหนดข้อตกลงที่จำเป็นในด้านต่าง ๆ เพื่อให้เกิดการทำงานร่วมกันอย่างมีประสิทธิภาพ เช่น ความน่าเชื่อถือของ

ระบบที่ให้บริการ เหนือวิธีของการรับส่งข้อมูล (messaging protocol) รูปแบบของข้อมูล (message format) รูปแบบของหลักฐานการส่งและการรับข้อมูล (evidence format) หรือค่าธรรมเนียมที่อาจเกิดขึ้น



รูปที่ 2 การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 4-corner model

การนำส่งข้อมูลอิเล็กทรอนิกส์ตามแบบ 4-corner model มีขั้นตอนทั่วไป ดังนี้

- (1) C1 ยืนยันตัวตนเพื่อเข้าใช้บริการนำส่งข้อมูลอิเล็กทรอนิกส์
- (2) C1 และระบบของ C1 เตรียมข้อมูลต้นฉบับ ทั้งนี้ ข้อมูลต้นฉบับอาจประกอบด้วยลายมือชื่อดิจิทัล ซึ่งใช้ระบุและยืนยันตัวตน C1
- (3) ระบบของ C1 ส่งข้อมูลต้นฉบับไปยัง C2
- (4) C2 จัดทำหลักฐานเพื่อยืนยันว่า C2 ได้รับข้อมูลต้นฉบับแล้ว ทั้งนี้ C2 อาจส่งหลักฐานนั้นให้ C1 หรือจัดเก็บหลักฐานนั้นเป็นระยะเวลาหนึ่งเพื่อให้ผู้ที่เกี่ยวข้องเข้าถึงได้ในภายหลัง
- (5) C2 ส่งต่อข้อมูลไปยัง C3 ตามข้อตกลงของการรับส่งข้อมูล
- (6) C3 จัดทำหลักฐานเพื่อยืนยันว่า C3 ได้รับข้อมูลจาก C2 แล้ว ทั้งนี้ C3 อาจส่งหลักฐานนั้นให้ C2 หรือจัดเก็บหลักฐานนั้นเป็นระยะเวลาหนึ่งเพื่อให้ผู้ที่เกี่ยวข้องเข้าถึงได้ในภายหลัง จากนั้น C2 อาจส่งหลักฐานนั้นต่อให้ C1
- (7) C3 ส่งข้อมูลไปยังระบบของ C4
- (8) C3 จัดทำหลักฐานเพื่อยืนยันว่า C3 ได้ส่งข้อมูลไปยัง C4 แล้ว ทั้งนี้ C3 อาจส่งหลักฐานนั้นให้ C2 หรือจัดเก็บหลักฐานนั้นเป็นระยะเวลาหนึ่งเพื่อให้ผู้ที่เกี่ยวข้องเข้าถึงได้ในภายหลัง จากนั้น C2 อาจส่งหลักฐานนั้นต่อให้ C1
- (9) C4 ยืนยันตัวตนเพื่อเข้าใช้บริการนำส่งข้อมูลอิเล็กทรอนิกส์
- (10) C4 และระบบของ C4 เข้าถึงข้อมูลจากบริการนำส่งอิเล็กทรอนิกส์

ในบางกรณี การนำส่งข้อมูลอิเล็กทรอนิกส์อาจมีผู้ให้บริการหนึ่งหรือหลายราย (เช่น C5) อยู่ระหว่างผู้ให้บริการ C2 และ C3 ซึ่งเพิ่มเติมจากแบบ 4-corner model เป็นแบบ extended model ทั้งนี้ ในกรณีดังกล่าวผู้ให้บริการทั้งหมด (เช่น C5) ที่อยู่ระหว่าง C2 และ C3 จะต้องปฏิบัติตามข้อตกลงที่จำเป็นในด้านต่าง ๆ เพื่อให้เกิดการทำงานร่วมกันอย่างมีประสิทธิภาพ เช่นเดียวกับกับ C2 และ C3

4. ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์

ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์มีจำนวน 6 ข้อ ดังนี้

- (1) การใช้ช่องทางการสื่อสารที่มีความมั่นคงปลอดภัย (protected channel) เพื่อให้มีการรักษาความถูกต้องครบถ้วนและการรักษาความลับของข้อมูลระหว่างการนำส่ง
- (2) การเข้ารหัสลับของข้อมูล (message encryption) เพื่อให้ผู้รับข้อมูลปลายทางเท่านั้นที่สามารถเข้าถึงข้อมูลได้
- (3) การระบุตัวผู้ส่งข้อมูลต้นทาง (sender identification) เพื่อตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ส่งข้อมูลต้นทาง
- (4) การระบุตัวผู้รับข้อมูลปลายทาง (recipient identification) เพื่อตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้รับข้อมูลปลายทางก่อนการนำส่งข้อมูล
- (5) การอ้างอิงเวลา (time reference) เพื่อระบุวันเวลาที่ส่งข้อมูลและรับข้อมูล
- (6) หลักฐานการส่งและการรับข้อมูล (evidence of sending and receiving) เพื่อให้ผู้ส่งข้อมูลต้นทางและผู้รับข้อมูลปลายทางมีหลักฐานของการส่งข้อมูลและการรับข้อมูล

ทั้งนี้ รายละเอียดของข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ เป็นไปตามตารางที่ 1 ซึ่งอ้างอิงจากการนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 4-corner model ในกรณีการนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 3-corner model นั้น ผู้ให้บริการต้องปฏิบัติตามข้อกำหนดของทั้ง C2 และ C3

ตารางที่ 1 ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์

ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์	ผู้ส่งข้อมูล ต้นทาง (C1)	ผู้ให้บริการฝั่ง ผู้ส่งข้อมูลต้นทาง (C2)	ผู้ให้บริการฝั่งผู้รับ ข้อมูลปลายทาง (C3)	ผู้รับข้อมูล ปลายทาง (C4)
<p>4.1 การใช้ช่องทางการสื่อสารที่มีความมั่นคงปลอดภัย (protected channel)</p>				
<p>(1) C1, C2, C3 และ C4 ต้องใช้ช่องทางการสื่อสารที่มีความมั่นคงปลอดภัยผ่านเกณฑ์วิธี Transport Layer Security (TLS) เช่น TLS 1.2 หรือเวอร์ชันที่สูงกว่า ซึ่งช่วยให้มีการรักษาความถูกต้องครบถ้วนและการรักษาความลับของข้อมูลด้วยการเข้ารหัสลับ (symmetric-key encryption) ในการนำส่งข้อมูลอิเล็กทรอนิกส์ ทั้งนี้ C2 และ C3 อาจจัดเตรียมช่องทางการสื่อสารดังกล่าวให้กับ C1 และ C4 ตามลำดับ</p> <p>ในกรณีการนำส่งข้อมูลอิเล็กทรอนิกส์แบบ extended model นั้น ผู้ให้บริการทั้งหมด (เช่น C5) ต้องใช้ช่องทางการสื่อสารที่มีความมั่นคงปลอดภัยเช่นเดียวกัน</p> <p>หมายเหตุ: เกณฑ์วิธี Secure Sockets Layer (SSL) และ Transport Layer Security (TLS) ในเวอร์ชันที่ต่ำกว่า TLS 1.2 ถูกประกาศยกเลิกใช้งานเนื่องจากเหตุผลด้านความมั่นคงปลอดภัย ดังนี้</p> <ul style="list-style-type: none"> — SSL 2.0 ถูกประกาศยกเลิกใช้งาน โดย RFC 6176 [1] — SSL 3.0 ถูกประกาศยกเลิกใช้งาน โดย RFC 7568 [2] — TLS 1.0 และ TLS 1.1 ถูกประกาศยกเลิกใช้งาน โดย RFC 8996 [3] 	✓	✓	✓	✓
<p>4.2 การเข้ารหัสลับของข้อมูล (message encryption)</p>				
<p>(1) หากข้อมูลที่จะส่งเป็นข้อมูลส่วนบุคคลที่อ่อนไหว (sensitive data) หรือ C1 ประสงค์จะให้ C4 เท่านั้นที่สามารถเข้าถึงข้อมูลได้ C1 สามารถดำเนินการเข้ารหัสลับข้อมูล (end-to-end encryption) ด้วยกุญแจสาธารณะของ C4</p>	✓			

ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์	ผู้ส่งข้อมูล ต้นทาง (C1)	ผู้ให้บริการฝั่ง ผู้ส่งข้อมูลต้นทาง (C2)	ผู้ให้บริการฝั่งผู้รับ ข้อมูลปลายทาง (C3)	ผู้รับข้อมูล ปลายทาง (C4)
4.3 การระบุตัวผู้ส่งข้อมูลต้นทาง (sender identification)				
<p>(1) C2 ต้องยืนยันตัวตน C1 ซึ่งสามารถทำผ่านเกณฑ์วิธี TLS ด้วยวิธีใดวิธีหนึ่ง ดังนี้</p> <p>(1.1) กรณีใช้ one-way TLS นั้น C2 ยืนยันตัวตน C1 จากการใช้สิ่งที่ใช้ยืนยันตัวตนของ C1 เช่น บัญชีผู้ใช้และรหัสผ่าน</p> <p>(1.2) กรณีใช้ two-way TLS นั้น C2 ยืนยันตัวตน C1 จากการตรวจสอบใบรับรองของ C1 (client certificate) ซึ่งเป็นการยืนยันตัวตนทั้งสองฝ่าย (mutual authentication) โดยทั้งสองกรณี C1 สามารถยืนยันตัวตน C2 จากการตรวจสอบใบรับรองของ C2 (server certificate)</p> <p>(2) หาก C1 ลงลายมือชื่อดิจิทัลประกอบด้วยข้อมูลต้นฉบับ C2 สามารถยืนยันตัวตน C1 จากการตรวจสอบใบรับรองของ C1 โดย C2 และ C3 (รวมถึงผู้ให้บริการทั้งหมด ถ้ามี เช่น C5) ไม่จำเป็นต้องลงลายมือชื่อดิจิทัลประกอบด้วยข้อมูลนั้น อย่างไรก็ตาม C2 สามารถลงลายมือชื่อประกอบด้วยข้อมูลต้นฉบับแทน C1 เพื่อรักษาความถูกต้องครบถ้วนของข้อมูลต้นฉบับ (message integrity) ให้กับ C1 ได้ หาก C1 และ C2 มีข้อตกลงระหว่างกัน</p>		✓		
4.4 การระบุตัวผู้รับข้อมูลปลายทาง (recipient identification)				
<p>(1) C3 ต้องยืนยันตัวตน C4 ก่อนอนุญาตให้ C4 รับข้อมูล ซึ่งสามารถทำผ่านเกณฑ์วิธี TLS ด้วยวิธีใดวิธีหนึ่ง ดังนี้</p> <p>(1.1) กรณีใช้ one-way TLS นั้น C3 ยืนยันตัวตน C4 จากการใช้สิ่งที่ใช้ยืนยันตัวตนของ C4 เช่น บัญชีผู้ใช้และรหัสผ่าน สำหรับใช้ยืนยันตัวตน</p> <p>(1.2) กรณีใช้ two-way TLS นั้น C3 ยืนยันตัวตน C4 จากการตรวจสอบใบรับรองของ C4 (client certificate) ซึ่งเป็นการยืนยันตัวตนทั้งสองฝ่าย (mutual authentication) โดยทั้งสองกรณี C4 สามารถยืนยันตัวตน C3 จากการตรวจสอบใบรับรองของ C3 (server certificate)</p>			✓	

ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์	ผู้ส่งข้อมูล ต้นทาง (C1)	ผู้ให้บริการฝั่ง ผู้ส่งข้อมูลต้นทาง (C2)	ผู้ให้บริการฝั่งผู้รับ ข้อมูลปลายทาง (C3)	ผู้รับข้อมูล ปลายทาง (C4)
4.5 การอ้างอิงเวลา (time reference)				
(1) C2 และ C3 (รวมถึงผู้ให้บริการทั้งหมด ถ้ามี เช่น C5) <u>ต้อง</u> ใช้การอ้างอิงวันเวลาที่น่าเชื่อถือ ในการจัดทำหลักฐานการส่งและการรับข้อมูลเพื่อยืนยันเหตุการณ์ที่เกิดขึ้น ณ เวลานั้น ๆ ตามที่ปรากฏในหลักฐาน โดยสามารถอ้างอิงวันเวลาจากระบบภายใน (system clock) หรือจากบริการประทับเวลา (time-stamping service) ของผู้ให้บริการประทับเวลา (time-stamping authority: TSA) ¹		✓	✓	

¹ รายละเอียดของบริการประทับเวลา (time-stamping service) เป็นไปตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยการประทับเวลาอิเล็กทรอนิกส์ เลขที่ ชมธอ. 33

ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์	ผู้ส่งข้อมูล ต้นทาง (C1)	ผู้ให้บริการฝั่ง ผู้ส่งข้อมูลต้นทาง (C2)	ผู้ให้บริการฝั่งผู้รับ ข้อมูลปลายทาง (C3)	ผู้รับข้อมูล ปลายทาง (C4)
4.6 หลักฐานการส่งและการรับข้อมูล (evidence of sending and receiving)				
<p>(1) C2 และ C3 (รวมถึงผู้ให้บริการทั้งหมด ถ้ามี เช่น C5) ต้องจัดเก็บหลักฐานที่เกี่ยวข้องกับการรับส่งข้อมูลอย่างน้อย ดังนี้</p> <ul style="list-style-type: none"> — ข้อมูลระบุตัวตนหรือข้อมูลยืนยันตัวตน ของผู้ใช้งานที่เกี่ยวข้อง — หลักฐานที่แสดงว่ามีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ส่งข้อมูลต้นทาง — หลักฐานที่แสดงว่ามีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้รับข้อมูลปลายทาง — หลักฐานที่แสดงว่าข้อมูลต้นฉบับไม่มีการแก้ไขเปลี่ยนแปลงระหว่างการนำส่งข้อมูล เช่น แมสเสจไดเจสต์ (message digest) ของข้อมูลต้นฉบับ — บันทึกเหตุการณ์ (log) ของเหตุการณ์ที่เกิดขึ้นระหว่างการรับส่งข้อมูล (ตัวอย่างของเหตุการณ์² เช่น ผู้ให้บริการได้รับข้อมูลต้นฉบับแล้ว ผู้ให้บริการได้รับข้อมูลจากผู้ให้บริการลำดับก่อนหน้าแล้ว ผู้ให้บริการได้ส่งข้อมูลไปยังผู้รับข้อมูลปลายทางแล้ว) <p>(2) C2 และ C3 (รวมถึงผู้ให้บริการทั้งหมด ถ้ามี เช่น C5) ต้องจัดเก็บหลักฐานตามระยะเวลาที่กำหนดเพื่อให้ผู้ที่เกี่ยวข้องเข้าถึงได้ และอาจส่งหลักฐานของเหตุการณ์ที่เกิดขึ้นระหว่างการรับส่งข้อมูลให้ผู้ที่เกี่ยวข้อง</p>		✓	✓	

² ตัวอย่างของเหตุการณ์ (event) ที่เกิดขึ้นระหว่างการรับส่งข้อมูล สามารถอ้างอิงจาก ETSI EN 319 522-1 ข้อ 6. ERDS events and evidence set [5]

5. ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ ประกอบด้วย การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ

5.1 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

- (1) ผู้ให้บริการต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (information security risk assessment) ของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ ดังนี้
 - การกำหนดเกณฑ์ความเสี่ยง ซึ่งประกอบด้วย เกณฑ์การยอมรับความเสี่ยง (risk acceptance criteria) และเกณฑ์การประเมินความเสี่ยง (risk assessment criteria)
 - การระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (risk identification) ได้แก่ การใช้กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อระบุความเสี่ยงที่เกี่ยวข้องกับการถูกเปิดเผยข้อมูล ความถูกต้องครบถ้วน และความพร้อมใช้งานของสารสนเทศภายในขอบเขตของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ รวมถึงการระบุผู้เป็นเจ้าของความเสี่ยง
 - การวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (risk analysis) โดยการประเมินผลกระทบและโอกาสที่อาจเกิดขึ้นจากความเสี่ยง รวมถึงการกำหนดระดับค่าความเสี่ยง
 - การเปรียบเทียบผลลัพธ์จากการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยง และการจัดลำดับความเสี่ยงเพื่อการจัดการความเสี่ยง (risk treatment)
- (2) ผู้ให้บริการต้องกำหนดแผนจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (information security risk treatment plan) และต้องเก็บรักษาเอกสารแสดงผลลัพธ์จากการจัดการความเสี่ยง
- (3) ผู้ให้บริการต้องทบทวนการประเมินความเสี่ยงและการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของบริการนำส่งข้อมูลอิเล็กทรอนิกส์อย่างสม่ำเสมอ

5.2 มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ อ้างอิง มาตรการควบคุม (control) และแนวปฏิบัติ (guidance) จากมาตรฐาน ISO/IEC 27002:2022 [4] ทั้งนี้ มาตรฐาน ISO/IEC 27002:2022 ประกอบด้วยมาตรการควบคุมจำนวน 93 ข้อ ซึ่งแบ่งออกเป็น 4 ด้าน ดังนี้

- (1) มาตรการควบคุมด้านองค์กร (organizational controls)
- (2) มาตรการควบคุมด้านบุคลากร (people controls)
- (3) มาตรการควบคุมด้านกายภาพ (physical controls)
- (4) มาตรการควบคุมด้านเทคโนโลยี (technological controls)

อย่างไรก็ตาม ข้อเสนอแนะมาตรฐานฉบับนี้ นำมาตรการควบคุมทั้งหมดของมาตรฐาน ISO/IEC 27002:2022 มาวิเคราะห์ตามบริบทและประเด็นที่เกี่ยวข้องกับบริการนำส่งข้อมูลอิเล็กทรอนิกส์ และแบ่ง มาตรการควบคุมตามระดับความจำเป็น ดังนี้

- (1) มาตรการควบคุมที่จำเป็น (mandatory controls) จำนวน 50 ข้อ

- (2) มาตรการควบคุมที่เป็นทางเลือก (optional controls) จำนวน 33 ข้อ
- (3) มาตรการควบคุมที่เฉพาะกรณี (conditional controls) จำนวน 10 ข้อ

ทั้งนี้ เพื่อให้สอดคล้องตามข้อเสนอแนะมาตรฐานฉบับนี้ ผู้ให้บริการต้องปฏิบัติตามมาตรการควบคุมที่จำเป็น (mandatory controls) ทุกข้อ และปฏิบัติตามมาตรการควบคุมที่เฉพาะกรณี (conditional controls) หากระบบของผู้ให้บริการเป็นไปตามเงื่อนไขที่ระบุไว้ในข้อนั้น ๆ เช่น กรณีที่ให้หน่วยงานภายนอกทำหน้าที่ให้บริการแทน กรณีที่ใช้บริการคลาวด์ หรือกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง

นอกจากนี้ ผู้ให้บริการสามารถพิจารณาปฏิบัติตามมาตรการควบคุมที่เป็นทางเลือก (optional controls) เพิ่มเติม เพื่อให้สอดคล้องกับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และหลักเกณฑ์ของหน่วยงานที่กำกับดูแลการนำส่งข้อมูลอิเล็กทรอนิกส์แต่ละประเภท

5.2.1 มาตรการควบคุมด้านองค์กร (organizational controls)

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
1	นโยบายความมั่นคงปลอดภัยสารสนเทศ (policies for information security) ผู้ให้บริการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศและนโยบายเฉพาะเรื่องด้านความมั่นคงปลอดภัยซึ่งได้รับการอนุมัติโดยผู้บริหาร รวมถึงเผยแพร่และสื่อสารให้บุคลากรที่เกี่ยวข้องรับทราบ นอกจากนี้ ผู้ให้บริการมีการทบทวนนโยบายความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงการดำเนินงานใด ๆ ภายในองค์กร	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.1
2	การกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (information security roles and responsibilities) ผู้ให้บริการกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ และจัดสรรให้มีความเหมาะสมตามความต้องการของหน่วยงาน	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.2
3	การแบ่งแยกหน้าที่ความรับผิดชอบ (segregation of duties) ผู้ให้บริการแบ่งแยกหน้าที่หรือส่วนงานที่รับผิดชอบที่อาจมีการขัดต่อการปฏิบัติงานออกจากกัน	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.3
4	การจัดการความรับผิดชอบ (management responsibilities) ผู้บริหารของผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์กำหนดให้บุคลากรทั้งหมดปฏิบัติตามการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยเป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศ นโยบายเฉพาะเรื่องด้านความมั่นคงปลอดภัยสารสนเทศ และขั้นตอนการปฏิบัติงานขององค์กร	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.4

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
5	การติดต่อกับหน่วยงานผู้มีอำนาจ (contact with authorities) ผู้ให้บริการจัดตั้งและรักษาช่องทางการติดต่อสื่อสารกับหน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.5
6	การติดต่อกับกลุ่มผลประโยชน์พิเศษ (contact with special interest groups) ผู้ให้บริการจัดตั้งและรักษาช่องทางติดต่อสื่อสารกับกลุ่มผลประโยชน์พิเศษ กลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศและสมาคมวิชาชีพอื่น ๆ	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.6
7	ศูนย์รวมข้อมูลภัยคุกคาม (threat intelligence) ผู้ให้บริการรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับภัยคุกคามเพื่อให้มีศูนย์รวมข้อมูลภัยคุกคาม (threat intelligence)	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.7
8	ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (information security in project management) ผู้ให้บริการบูรณาการความมั่นคงปลอดภัยสารสนเทศเข้ากับการบริหารจัดการโครงการ	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.8
9	บัญชีของข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ (inventory of information and other associated assets) ผู้ให้บริการจัดทำและเก็บรักษาบัญชีของข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ซึ่งรวมถึง ข้อมูลระบุเจ้าของทรัพย์สิน	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.9
10	การใช้ข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ อย่างเหมาะสม (acceptable use of information and other associated assets) ผู้ให้บริการกำหนดกฎเกณฑ์การใช้และขั้นตอนการจัดการกับข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ รวมถึงจัดทำเป็นเอกสารและนำไปปฏิบัติอย่างเหมาะสม	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.10
11	การคืนทรัพย์สิน (return of assets) ผู้ให้บริการกำหนดให้บุคลากรและผู้มีส่วนได้ส่วนเสีย (interested party) อื่น ๆ คืนทรัพย์สินทั้งหมดขององค์กรที่ตนถือครองเมื่อสิ้นสุดการจ้างงาน สิ้นสุดสัญญา หรือข้อตกลงการจ้างงาน	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.11
12	ชั้นความลับของข้อมูล (classification of information) ผู้ให้บริการจำแนกข้อมูลตามความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยเป็นไปตามข้อกำหนดการรักษาความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.12

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
13	การทำป้ายบ่งชี้สารสนเทศ (labelling of information) ผู้ให้บริการกำหนดขั้นตอนการทำป้ายบ่งชี้สารสนเทศอย่างเหมาะสมและนำไปปฏิบัติให้สอดคล้องกับวิธีการจัดชั้นความลับของข้อมูลที่องค์กรกำหนดไว้	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.13
14	การถ่ายโอนสารสนเทศ (information transfer) ผู้ให้บริการมีการกำหนดกฎเกณฑ์ ขั้นตอนการปฏิบัติงาน หรือข้อตกลงเกี่ยวกับเครื่องมือหรืออุปกรณ์ในการถ่ายโอนสารสนเทศทุกประเภท ทั้งการถ่ายโอนภายในองค์กร และการถ่ายโอนระหว่างองค์กรกับหน่วยงานภายนอก	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.14
15	การควบคุมการเข้าถึง (access control) ผู้ให้บริการมีการกำหนดกฎเกณฑ์การเข้าถึงข้อมูลและทรัพย์สินอื่น ๆ ทั้งการเข้าถึงทางกายภาพ (physical access) และการเข้าถึงเชิงตรรกะ (logical access) และนำไปปฏิบัติโดยคำนึงถึงข้อกำหนดทางธุรกิจและด้านความมั่นคงปลอดภัยสารสนเทศ	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.15
16	การจัดการข้อมูลเกี่ยวกับอัตลักษณ์ (identity management) ผู้ให้บริการมีการจัดการข้อมูลเกี่ยวกับอัตลักษณ์ที่แท้จริง	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.16
17	ข้อมูลการยืนยันตัวตน (authentication information) ผู้ให้บริการควบคุมการจัดสรรและการบริหารจัดการข้อมูลการยืนยันตัวตนผ่านกระบวนการจัดการ รวมถึงการให้คำแนะนำแก่บุคลากรในการจัดการข้อมูลการยืนยันตัวตนอย่างเหมาะสม	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.17
18	สิทธิการเข้าถึง (access rights) ผู้ให้บริการมีการจัดเตรียม ทบทวน แก้ไข หรือลบสิทธิการเข้าถึงข้อมูล และสินทรัพย์ที่เกี่ยวข้องอื่น ๆ ตามนโยบายเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศและกฎระเบียบขององค์กร	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.18
19	ความมั่นคงปลอดภัยสารสนเทศเกี่ยวกับความสัมพันธ์กับผู้ให้บริการภายนอก (information security in supplier relationships) ผู้ให้บริการมีการกำหนดและดำเนินการตามกระบวนการและขั้นตอนการปฏิบัติงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์หรือบริการของผู้ให้บริการภายนอก	conditional (ในกรณีที่ให้หน่วยงานภายนอกทำหน้าที่ให้บริการแทน)	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.19

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
20	<p>การระบุความมั่นคงปลอดภัยสารสนเทศในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (addressing information security within supplier agreements)</p> <p>ผู้ให้บริการมีการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง และตกลงกับผู้ให้บริการภายนอกแต่ละรายตามประเภทของความสัมพันธ์กับผู้ให้บริการภายนอก</p>	conditional (ในกรณีที่ให้หน่วยงานภายนอกทำหน้าที่ให้บริการแทน)	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.20
21	<p>การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานด้านเทคโนโลยีสารสนเทศและการสื่อสาร (managing information security in the ICT supply chain)</p> <p>ผู้ให้บริการมีการกำหนดและดำเนินการตามกระบวนการและขั้นตอนการปฏิบัติงาน เพื่อจัดการความเสี่ยงด้านความมั่นคงปลอดภัยในห่วงโซ่อุปทานด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology: ICT)</p>	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.21
22	<p>การติดตาม การทบทวน และการจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (monitoring, review and change management of supplier services)</p> <p>ผู้ให้บริการมีการติดตาม ทบทวน ประเมิน และบริหารจัดการการเปลี่ยนแปลงในแนวทางปฏิบัติด้านความมั่นคงปลอดภัยและการส่งมอบบริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ</p>	conditional (ในกรณีที่ให้หน่วยงานภายนอกทำหน้าที่ให้บริการแทน)	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.22
23	<p>ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (information security for use of cloud services)</p> <p>ผู้ให้บริการมีการกำหนดกระบวนการการได้มา การใช้บริการ การบริหารจัดการ และการยกเลิกบริการคลาวด์ที่เป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร</p>	conditional (ในกรณีที่ใช้บริการคลาวด์)	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.23
24	<p>การวางแผนและเตรียมการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (information security incident management planning and preparation)</p> <p>ผู้ให้บริการมีการวางแผนและเตรียมการสำหรับการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (information security incident) โดยมีการกำหนดและสื่อสารกระบวนการจัดการ บทบาทและหน้าที่ความรับผิดชอบสำหรับการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ</p>	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.24

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
25	<p>การประเมินและตัดสินใจต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (assessment and decision on information security events)</p> <p>ผู้ให้บริการประเมินเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (information security event) และตัดสินใจว่าเหตุการณ์นั้นจัดเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่</p>	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.25
26	<p>การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (response to information security incidents)</p> <p>ผู้ให้บริการมีการตอบสนองและจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศตามขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร</p>	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.26
27	<p>การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (learning from information security incidents)</p> <p>ผู้ให้บริการนำความรู้ที่ได้รับจากสถานการณ์ความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ในการเสริมสร้างความแข็งแกร่งและปรับปรุงมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ (information security control)</p>	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.27
28	<p>การเก็บรวบรวมหลักฐาน (collection of evidence)</p> <p>ผู้ให้บริการกำหนดและดำเนินการตามขั้นตอนการปฏิบัติงานในการระบุ การรวบรวม การได้มา และการเก็บรักษาหลักฐานที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ</p>	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.28
29	<p>ความมั่นคงปลอดภัยสารสนเทศในระหว่างการหยุดชะงัก (information security during disruption)</p> <p>ผู้ให้บริการวางแผนการรักษาความมั่นคงปลอดภัยสารสนเทศให้อยู่ในระดับที่เหมาะสมในระหว่างการหยุดชะงัก</p>	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.29
30	<p>ความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศและการสื่อสารเพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)</p> <p>ผู้ให้บริการมีการวางแผน ดำเนินการ บำรุงรักษา และทดสอบความพร้อมใช้งานด้านเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นไปตามวัตถุประสงค์ด้านความต่อเนื่องทางธุรกิจและข้อกำหนดด้านความพร้อมใช้งานของระบบ ICT</p>	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.30

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
31	ข้อกำหนดทางกฎหมาย ข้อบังคับและสัญญา (legal, statutory, regulatory and contractual requirements) ผู้ให้บริการจัดทำเอกสารข้อกำหนดทางกฎหมาย ข้อบังคับ และสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ รวมถึงแนวทางขององค์กรในการปฏิบัติตามข้อกำหนด ทั้งนี้ ข้อกำหนดทางกฎหมาย ข้อบังคับ และสัญญาควรมีการปรับปรุงให้เป็นปัจจุบัน	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.31
32	สิทธิในทรัพย์สินทางปัญญา (intellectual property rights) ผู้ให้บริการดำเนินการตามขั้นตอนการปฏิบัติงานที่มีความเหมาะสมเพื่อปกป้องสิทธิในทรัพย์สินทางปัญญา	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.32
33	การป้องกันข้อมูล (protection of records) ผู้ให้บริการป้องกันข้อมูลจากการสูญหาย การถูกทำลาย การปลอมแปลง และการเข้าถึงหรือเผยแพร่โดยไม่ได้รับอนุญาต	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.33
34	การรักษาความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (privacy and protection of PII (personal identifiable information)) ผู้ให้บริการระบุและปฏิบัติตามข้อกำหนดเกี่ยวกับการรักษาความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคลที่เป็นไปตามกฎหมายที่ใช้บังคับ ระเบียบข้อบังคับ และข้อกำหนดในสัญญา	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.34
35	การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (independent review of information security) ผู้ให้บริการมีการทบทวนอย่างอิสระในด้านความมั่นคงปลอดภัยสารสนเทศ เช่น ตรวจสอบการจัดการและการดำเนินงานที่เกี่ยวข้องกับบุคลากร กระบวนการทำงาน เทคโนโลยี โดยมีการทบทวนตามช่วงเวลาที่วางแผนไว้ หรือเมื่อมีการเปลี่ยนแปลงสำคัญเกิดขึ้น	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.35
36	การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ (compliance with policies, rules and standards for information security) ผู้ให้บริการมีการทบทวนการปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.36

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
37	เอกสารขั้นตอนการปฏิบัติงาน (documented operating procedures) ผู้ให้บริการจัดทำเอกสารขั้นตอนการปฏิบัติงานของอุปกรณ์ประมวลผลสารสนเทศ และเอกสารขั้นตอนการปฏิบัติงานนี้ควรเข้าถึงได้โดยบุคลากรที่มีความจำเป็นต้องใช้งาน	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 5.37

5.2.2 มาตรการควบคุมด้านกายภาพ (physical controls)

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
38	ขอบเขตความมั่นคงปลอดภัยทางกายภาพ (physical security perimeters) ผู้ให้บริการกำหนดขอบเขตหรือบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยเพื่อปกป้องข้อมูลและทรัพย์สินอื่น ๆ ที่เกี่ยวข้อง	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.1
39	การเข้าออกทางกายภาพ (physical entry) ผู้ให้บริการมีการควบคุมการเข้าออกทางกายภาพของพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.2
40	การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และอุปกรณ์ (securing offices, rooms and facilities) ผู้ให้บริการออกแบบและดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และอุปกรณ์	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.3
41	การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ (physical security monitoring) ผู้ให้บริการเฝ้าติดตามสถานที่เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.4
42	การป้องกันภัยคุกคามด้านกายภาพและสิ่งแวดล้อม (protecting against physical and environmental threats) ผู้ให้บริการออกแบบและดำเนินการป้องกันภัยคุกคามด้านกายภาพและสิ่งแวดล้อม เช่น ภัยธรรมชาติ และภัยคุกคามทางกายภาพอื่น ๆ ต่อโครงสร้างทางกายภาพทั้งโดยเจตนาหรือไม่เจตนา	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.5
43	การปฏิบัติงานในพื้นที่ที่มีความมั่นคงปลอดภัย (working in secure areas) ผู้ให้บริการออกแบบและดำเนินการเกี่ยวกับมาตรการด้านความมั่นคงปลอดภัยสำหรับการปฏิบัติงานในพื้นที่ที่มีความมั่นคงปลอดภัย	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.6

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
44	<p>กฎเกณฑ์โต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (clear desk and clear screen)</p> <p>ผู้ให้บริการมีการกำหนดและบังคับใช้กฎเกณฑ์อย่างเหมาะสมเกี่ยวกับโต๊ะทำงานปลอดเอกสารทั้งรูปแบบกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ รวมถึงกฎเกณฑ์การป้องกันหน้าจอคอมพิวเตอร์สำหรับอุปกรณ์ประมวลผลข้อมูล</p>	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.7
45	<p>การจัดตั้งและการป้องกันอุปกรณ์ (equipment siting and protection)</p> <p>ผู้ให้บริการมีการจัดตั้งและป้องกันอุปกรณ์ให้มีความมั่นคงปลอดภัย</p>	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.8
46	<p>ความมั่นคงปลอดภัยของอุปกรณ์และสินทรัพย์ที่ใช้งานอยู่ภายนอกองค์กร (security of assets off-premises)</p> <p>ผู้ให้บริการปกป้องทรัพย์สินที่ใช้งานอยู่ภายนอกองค์กรให้มีความมั่นคงปลอดภัย</p>	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.9
47	<p>การจัดเก็บสื่อบันทึกข้อมูล (storage media)</p> <p>ผู้ให้บริการมีการจัดการสื่อบันทึกข้อมูลตลอดวงจรการใช้งาน เช่น การจัดหา การใช้ การขนส่ง การกำจัดสื่อบันทึกตามรูปแบบการจัดหมวดหมู่และข้อกำหนดในการจัดการขององค์กร</p>	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.10
48	<p>ระบบและอุปกรณ์สนับสนุนการทำงาน (supporting utilities)</p> <p>ผู้ให้บริการมีการปกป้องระบบและอุปกรณ์ประมวลผลข้อมูลจากไฟฟ้าขัดข้องและการหยุดชะงักอื่น ๆ ที่เกิดจากความล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงาน</p>	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.11
49	<p>ความมั่นคงปลอดภัยของการเดินสายสัญญาณและการสื่อสาร (cabling security)</p> <p>ผู้ให้บริการมีการปกป้องการเดินสายสัญญาณนำไฟฟ้า ข้อมูล หรือบริการที่สนับสนุนข้อมูลจากการดักจับสัญญาณ การแทรกแซงสัญญาณ หรือการทำให้สายสัญญาณเสียหาย</p>	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.12
50	<p>การบำรุงรักษาอุปกรณ์ (equipment maintenance)</p> <p>ผู้ให้บริการมีการบำรุงรักษาอุปกรณ์อย่างถูกต้องเพื่อให้มีสภาพพร้อมใช้งาน รักษาความถูกต้องครบถ้วนและมีการรักษาความลับของข้อมูล</p>	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.13

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
51	<p>การกำจัดหรือนำอุปกรณ์มาใช้ใหม่อย่างปลอดภัย (secure disposal or re-use of equipment)</p> <p>ผู้ให้บริการมีการตรวจสอบรายการของอุปกรณ์ที่มีสื่อบันทึกข้อมูล เพื่อให้แน่ใจว่าข้อมูลสำคัญและซอฟต์แวร์ที่มีใบอนุญาตได้ถูกลบออก หรือเขียนทับอย่างมั่นคงปลอดภัยก่อนมีการกำจัดทิ้งหรือนำอุปกรณ์มาใช้ใหม่</p>	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 7.14

5.2.3 มาตรการควบคุมด้านบุคลากร (people controls)

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
52	<p>การคัดเลือกบุคลากร (screening)</p> <p>ผู้ให้บริการตรวจสอบประวัติผู้สมัครงานทุกคนก่อนมีการว่าจ้างเพื่อเป็นบุคลากรของหน่วยงาน โดยการตรวจสอบประวัติควรดำเนินการให้มีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และดำเนินการในระดับที่เหมาะสมกับความต้องการของธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง</p>	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 6.1
53	<p>ข้อตกลงและเงื่อนไขการจ้างงาน (terms and conditions of employment)</p> <p>ผู้ให้บริการระบุความรับผิดชอบของบุคลากรและองค์กรด้านความมั่นคงปลอดภัยสารสนเทศในข้อตกลงและเงื่อนไขการจ้างงาน</p>	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 6.2
54	<p>การสร้างความตระหนัก การศึกษา และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (information security awareness, education and training)</p> <p>บุคลากรของผู้ให้บริการและผู้ที่เกี่ยวข้องได้รับการสร้างความตระหนัก ได้รับการศึกษาและการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศที่เหมาะสม รวมถึงได้รับรู้ถึงนโยบายความมั่นคงปลอดภัยสารสนเทศ และนโยบายเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบ ที่มีความเป็นปัจจุบันอย่างสม่ำเสมอ</p>	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 6.3
55	<p>กระบวนการทางวินัย (disciplinary process)</p> <p>ผู้ให้บริการมีการกำหนดและสื่อสารกระบวนการทางวินัยอย่างเป็นทางการและมีการสื่อสารให้บุคลากรและผู้ที่มีส่วนเกี่ยวข้องทราบเพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศขององค์กร</p>	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 6.4

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
56	การสิ้นสุดหรือการเปลี่ยนแปลงหน้าที่ความรับผิดชอบของการจ้างงาน (responsibilities after termination or change of employment) ผู้ให้บริการมีการกำหนด บังคับใช้ สื่อสารต่อบุคลากรและผู้ที่มีส่วนเกี่ยวข้องถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่ยังมีผลบังคับใช้หลังจากการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 6.5
57	ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (confidentiality or non-disclosure agreements) ผู้ให้บริการมีการระบุและจัดทำเอกสารข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับที่สะท้อนถึงความจำเป็นขององค์กรในการปกป้องข้อมูลสารสนเทศ โดยข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับควรมีการทบทวนและลงนามโดยบุคลากรและผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 6.6
58	การทำงานจากระยะไกล (remote working) ผู้ให้บริการมีมาตรการด้านความมั่นคงปลอดภัยสารสนเทศเมื่อบุคลากรทำงานจากระยะไกลเพื่อป้องกันการเข้าถึง การประมวลผล หรือการจัดเก็บข้อมูลนอกสถานที่ขององค์กร	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 6.7
59	การรายงานสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (information security event reporting) ผู้ให้บริการจัดให้มีกลไกสำหรับบุคลากรในการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่สังเกตพบหรือสงสัยผ่านช่องทางที่เหมาะสมอย่างทันที่	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 6.8

5.2.4 มาตรการควบคุมด้านเทคโนโลยี (technological controls)

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
60	อุปกรณ์ปลายทางของผู้ใช้ (user endpoint devices) ผู้ให้บริการมีการจัดการเพื่อให้มั่นใจว่าข้อมูลที่จัดเก็บ ประมวลผล หรือเข้าถึงผ่านอุปกรณ์ปลายทางของผู้ใช้ได้รับการปกป้อง	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.1
61	สิทธิการเข้าถึงของสิทธิระดับสูง (privileged access rights) ผู้ให้บริการมีการจัดสรรและจำกัดการเข้าถึงของสิทธิระดับสูง	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.2

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
62	การจำกัดการเข้าถึงข้อมูลสารสนเทศ (information access restriction) ผู้ให้บริการมีการจำกัดการเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ให้สอดคล้องกับนโยบายควบคุมการเข้าถึง	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.3
63	การเข้าถึงซอร์สโค้ดของโปรแกรม (access to source code) ผู้ให้บริการมีการจัดการอย่างเหมาะสมในการเข้าถึง การอ่าน และการเขียนซอร์สโค้ด เครื่องมือการพัฒนา และซอฟต์แวร์ไลบรารี	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.4
64	การยืนยันตัวตนอย่างปลอดภัย (secure authentication) ผู้ให้บริการมีการใช้เทคโนโลยีและกระบวนการยืนยันตัวตนที่มีความมั่นคงปลอดภัย โดยสอดคล้องกับข้อจำกัดการเข้าถึงข้อมูลและนโยบายควบคุมการเข้าถึง	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.5
65	การจัดการขีดความสามารถของระบบ (capacity management) ผู้ให้บริการตรวจสอบการใช้ทรัพยากรและปรับให้มีความสอดคล้องกับข้อกำหนดในปัจจุบันและข้อกำหนดที่คาดหวังเกี่ยวกับการจัดการขีดความสามารถของระบบ	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.6
66	การป้องกันมัลแวร์ (protection against malware) ผู้ให้บริการมีการดำเนินการป้องกันมัลแวร์อย่างเหมาะสมโดยผู้ใช้งานมีความตระหนักในการป้องกันมัลแวร์	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.7
67	การจัดการช่องโหว่ทางเทคนิค (management of technical vulnerabilities) ผู้ให้บริการมีข้อมูลช่องโหว่ทางเทคนิคของระบบสารสนเทศที่ใช้งาน โดยผู้ให้บริการมีการประเมินความเสี่ยงต่อช่องโหว่ทางเทคนิคดังกล่าว และใช้มาตรการที่เหมาะสม	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.8
68	การจัดการการตั้งค่า (configuration management) ผู้ให้บริการมีการจัดการการตั้งค่า ซึ่งรวมถึงกำหนดค่าความมั่นคงปลอดภัยของฮาร์ดแวร์ ซอฟต์แวร์ บริการต่าง ๆ และระบบเครือข่าย โดยมีการจัดทำเป็นเอกสาร ตรวจสอบติดตามและมีการทบทวนอย่างสม่ำเสมอ	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.9
69	การลบข้อมูล (information deletion) ผู้ให้บริการมีการลบข้อมูลที่จัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์ หรือสื่อบันทึกข้อมูลอื่น ๆ เมื่อไม่มีความต้องการใช้อีกต่อไป	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.10

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
70	การปกปิดข้อมูลเพื่อจำกัดการเห็นข้อมูลทั้งหมด (data masking) ผู้ให้บริการดำเนินการเกี่ยวกับการปกปิดข้อมูลเพื่อจำกัดการเห็นข้อมูลทั้งหมด (data masking) ที่เป็นไปตามนโยบายการควบคุมการเข้าถึงและนโยบายเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง รวมถึงคำนึงถึงข้อกำหนดทางธุรกิจและกฎหมายที่เกี่ยวข้อง	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.11
71	การป้องกันการรั่วไหลของข้อมูล (data leakage prevention) ผู้ให้บริการมีมาตรการป้องกันการรั่วไหลของข้อมูลที่ใช้กับระบบสารสนเทศ ระบบเครือข่าย และอุปกรณ์ประมวลผลอื่น ๆ ที่จัดเก็บหรือส่งข้อมูลที่ละเอียดอ่อน	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.12
72	การสำรองข้อมูล (information backup) ผู้ให้บริการมีการบำรุงรักษาและทดสอบการสำรองข้อมูล ซอฟต์แวร์ และระบบสารสนเทศอย่างสม่ำเสมอโดยเป็นไปตามนโยบายการสำรองข้อมูล	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.13
73	การเตรียมการอุปกรณ์ประมวลผลข้อมูลสำรอง (redundancy of information processing facilities) ผู้ให้บริการมีการเตรียมการอุปกรณ์ประมวลผลข้อมูลสำรองให้เพียงพอและเป็นไปตามข้อกำหนดด้านความพร้อมใช้งาน	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.14
74	การบันทึกข้อมูลเหตุการณ์ (logging) ผู้ให้บริการมีการสร้าง การจัดเก็บ การป้องกัน และการวิเคราะห์บันทึกข้อมูลเหตุการณ์ (logging) ข้อยกเว้น (exceptions) ข้อผิดพลาด (faults) และเหตุการณ์ที่เกี่ยวข้องอื่น ๆ	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.15
75	การเฝ้าติดตามเหตุการณ์ (monitoring activities) ผู้ให้บริการตรวจสอบระบบเครือข่าย ระบบสารสนเทศ และแอปพลิเคชันเพื่อหาพฤติกรรมที่ผิดปกติและดำเนินการอย่างเหมาะสมในการประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.16
76	การตั้งค่าเทียบเวลา (clock synchronization) ผู้ให้บริการตั้งค่าเทียบเวลาระบบประมวลผลที่องค์กรใช้ให้สอดคล้องกับแหล่งเวลาที่น่าเชื่อถือ	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.17
77	การใช้โปรแกรมอรรถประโยชน์ที่ได้รับสิทธิพิเศษ (use of privileged utility programs) ผู้ให้บริการจำกัดและควบคุมอย่างเข้มงวดในการใช้โปรแกรมอรรถประโยชน์ที่สามารถลบหรือเปลี่ยนแปลงการควบคุมระบบสารสนเทศและแอปพลิเคชัน	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.18

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
78	การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ (installation of software on operational systems) ผู้ให้บริการมีกระบวนการหรือมาตรการในการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการให้มีความมั่นคงปลอดภัย	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.19
79	ความมั่นคงปลอดภัยของระบบเครือข่าย (networks security) ผู้ให้บริการมีการจัดการ ควบคุม และรักษาความมั่นคงปลอดภัยระบบเครือข่ายและอุปกรณ์เครือข่าย เพื่อปกป้องข้อมูลในระบบสารสนเทศและแอปพลิเคชัน	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.20
80	ความมั่นคงปลอดภัยของบริการเครือข่าย (security of network services) ผู้ให้บริการมีการดำเนินการและติดตามตรวจสอบมาตรการรักษาความมั่นคงปลอดภัยของระบบเครือข่าย ระดับของบริการและข้อกำหนดของบริการระบบเครือข่าย	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.21
81	การแบ่งแยกเครือข่าย (segregation of networks) ผู้ให้บริการแบ่งแยกกลุ่มการบริการข้อมูล กลุ่มผู้ใช้ และกลุ่มของระบบสารสนเทศในระบบเครือข่ายขององค์กร	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.22
82	การกรองเว็บ (web filtering) ผู้ให้บริการมีการจัดการการเข้าถึงเว็บไซต์ภายนอกเพื่อลดความเสี่ยงการเข้าถึงเนื้อหาที่เป็นอันตราย	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.23
83	การใช้การเข้ารหัสลับ (use of cryptography) ผู้ให้บริการมีการกำหนดและดำเนินการเกี่ยวกับกฎเกณฑ์การเข้ารหัสลับอย่างมีประสิทธิภาพ ซึ่งรวมถึงการบริหารจัดการกุญแจเข้ารหัส	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.24
84	วงจรการพัฒนาอย่างปลอดภัย (secure development life cycle) ผู้ให้บริการมีการจัดทำและประยุกต์ใช้กฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบอย่างปลอดภัย	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.25
85	ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (application security requirements) ผู้ให้บริการมีการระบุและอนุมัติข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศเมื่อมีการพัฒนาหรือใช้แอปพลิเคชันที่ได้รับมา	Optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.26

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ (guidance)
86	ความมั่นคงปลอดภัยของสถาปัตยกรรมของระบบและหลักการทางวิศวกรรม (secure system architecture and engineering principles) ผู้ให้บริการมีการใช้หลักการระบบความมั่นคงปลอดภัยทางวิศวกรรม โดยควรจัดทำเป็นเอกสาร มีการบำรุงรักษา และนำไปประยุกต์ใช้กับกิจกรรมการพัฒนาระบบสารสนเทศ	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.27
87	การเขียนโปรแกรมที่มีความมั่นคงปลอดภัย (secure coding) ผู้ให้บริการใช้หลักการเขียนโปรแกรมที่มีความมั่นคงปลอดภัย ในการพัฒนาซอฟต์แวร์	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.28
88	การทดสอบความมั่นคงปลอดภัยในการพัฒนาและรับรองระบบ (security testing in development and acceptance) ผู้ให้บริการมีการกำหนดและดำเนินการเกี่ยวกับการทดสอบความมั่นคงปลอดภัยในวงจรการพัฒนาระบบ	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.29
89	การจ้างหน่วยงานภายนอกพัฒนาระบบ (outsourced development) ผู้ให้บริการติดตาม กำกับดูแล และทบทวนกิจกรรมที่เกี่ยวข้องกับการพัฒนาระบบโดยหน่วยงานภายนอก	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.30
90	การแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการให้บริการออกจากกัน (separation of development, test and production environments) ผู้ให้บริการมีการแยกสภาพแวดล้อมและรักษาความมั่นคงปลอดภัยในสภาพแวดล้อมของการพัฒนา การทดสอบ และการให้บริการ	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.31
91	การบริหารจัดการการเปลี่ยนแปลง (change management) ผู้ให้บริการจัดการต่อการเปลี่ยนแปลงระบบสารสนเทศและอุปกรณ์ ประมวลผลข้อมูลให้เป็นไปตามกระบวนการจัดการการเปลี่ยนแปลง	mandatory	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.32
92	ข้อมูลการทดสอบ (test information) ผู้ให้บริการมีการคัดเลือก การป้องกัน และการจัดการข้อมูลสำหรับการทดสอบอย่างเหมาะสม	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.33
93	การป้องกันระบบสารสนเทศระหว่างการตรวจสอบระบบ (protection of information systems during audit testing) ผู้ให้บริการมีการวางแผนและตกลงร่วมกันระหว่างผู้ทดสอบระบบและผู้บริหารที่เกี่ยวข้องในการตรวจสอบระบบและกิจกรรมการประกันความมั่นคงปลอดภัยอื่นๆ ที่เกี่ยวข้องกับระบบปฏิบัติการ	optional	รายละเอียดเป็นไปตาม ISO/IEC 27002:2022 ข้อ 8.34

บรรณานุกรม

- [1] Internet Engineering Task Force, "RFC 6176: Prohibiting Secure Sockets Layer (SSL) Version 2.0", March 2011. Available: <https://www.rfc-editor.org/rfc/rfc6176>.
- [2] Internet Engineering Task Force, "RFC 7568: Deprecating Secure Sockets Layer Version 3.0", June 2015. Available: <https://www.rfc-editor.org/rfc/rfc7568>.
- [3] Internet Engineering Task Force, "RFC 8996: Deprecating TLS 1.0 and TLS 1.1", March 2021. Available: <https://datatracker.ietf.org/doc/html/rfc8996>.
- [4] International Organization for Standardization, "ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls", March 2022.
- [5] European Telecommunications Standards Institute, "ETSI EN 319 522-1 V1.1.1 – Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture", September 2018.
- [6] European Telecommunications Standards Institute, "ETSI EN 319 521 V1.1.1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers", February 2019.
- [7] European Commission, "eDelivery Building Block, Security Controls, Linking eIDAS (Q)ERDS & eDelivery", Version 1.20, April 2022.
- [8] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม.