ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. [x-xxxx]

ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์

ELECTRONIC DELIVERY SERVICE

เวอร์ชัน 0.3

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์

ขมธอ. [x-xxxx]

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 กรุณาเลือกวันที่ประกาศ

คณะทำงานจัดทำร่างข้อเสนอแนะมาตรฐานเกี่ยวกับธุรกิจบริการ
ด้านการทำธุรกรรมทางอิเล็กทรอนิกส์

ที่ปรึกษาคณะทำงาน

นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงาน

นางสาวสำรวย นุ่มศรี	กรมศุลกากร
นายกำชัย จัตตานนท์	
นายนิรันดร์ ประจวบเหมาะ	กรมสรรพากร
นางสุภิดา บรรเทาทุกข์	
นายคงฤทธิ์ จันทริก	สภาผู้ส่งสินค้าทางเรือแห่งประเทศไทย
นายภาวุธ พงษ์วิทยภานุ	สมาคมผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ไทย
นายธานินทร์ ตันกิติบุตร	สมาคมผู้ให้บริการอินเทอร์เน็ตและคลาวด์ไทย
นายวรพจน์ ธาราศิริสกุล	สมาคมฟินเทคประเทศไทย
นายปกรณ์ ลี้สกุล	สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
นายสันติ สิทธิเลิศพิศาล	สำนักมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นางสาวธิดารัธ ธนภรรคภวิน	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายอิศร์ เตาลานนท์	
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายพงษ์พันธ์ ศรีปาน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงานและเลขานุการ

นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายวีรศักดิ์ ดีอ่ำ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์ฉบับนี้ จัดทำขึ้นเพื่ออธิบายภาพรวมของการนำส่งข้อมูลอิเล็กทรอนิกส์ ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ และมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ เพื่อให้ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ มีแนวทางในการให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย และช่วยสร้างความมั่นใจให้กับผู้ส่งข้อมูลและผู้รับข้อมูลที่ใช้บริการนำส่งข้อมูลอิเล็กทรอนิกส์

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์ฉบับนี้ จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ 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 ต้องพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความสะดวก รวดเร็ว และมีประสิทธิภาพ แต่เนื่องจากในการพัฒนานั้นมีระยะเวลาและต้นทุนที่สูง ผู้ประกอบการหลายรายจึงมีแนวคิดที่จะลดระยะเวลาและต้นทุนในการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ จึงหันมาใช้บริการจาก “ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์” หรือ “ผู้ให้บริการ” ที่ทำหน้าที่เป็นจุดรับส่ง (access point) ในการนำส่งข้อมูลอิเล็กทรอนิกส์ระหว่างผู้ประกอบการกับหน่วยงานภาครัฐหรือกับผู้ประกอบการรายอื่น ผู้ให้บริการดังกล่าวจึงมีบทบาทสำคัญต่อการสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ให้มีการเชื่อมโยงเครือข่ายเข้าด้วยกัน มีการใช้ทรัพยากรร่วมกัน มีการประมวลผลและกระจายข้อมูลไปตามหน่วยงานต่าง ๆ ทำให้ต้องมีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและข้อมูลอิเล็กทรอนิกส์ให้มีความถูกต้องครบถ้วน พร้อมใช้งาน และน่าเชื่อถือ

ด้วยเหตุนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำข้อเสนอแนะมาตรฐานฯ ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์ เพื่ออธิบายภาพรวมของการนำส่งข้อมูลอิเล็กทรอนิกส์ ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ และมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ เพื่อให้ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ มีแนวทางในการให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัยและช่วยสร้างความมั่นใจให้กับผู้ส่งข้อมูลและผู้รับข้อมูลที่ใช้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ โดยข้อเสนอแนะมาตรฐานฉบับนี้สามารถใช้ได้กับบริการนำส่งข้อมูลอิเล็กทรอนิกส์ให้กับกรมสรรพากร บริการนำส่งข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงานที่เชื่อมต่อกับระบบ National Single Window (NSW) หรือบริการนำส่งข้อมูลอิเล็กทรอนิกส์อื่น ๆ ที่ต้องการความน่าเชื่อถือในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์

สารบัญ

สารบัญรูป

สารบัญตาราง

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยบริการนำส่งข้อมูลอิเล็กทรอนิกส์

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้อธิบายภาพรวมของการนำส่งข้อมูลอิเล็กทรอนิกส์ ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ และมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ เพื่อให้ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ ซึ่งทำหน้าที่เป็นจุดรับส่ง (access point) ระหว่างผู้ส่งข้อมูลกับผู้รับข้อมูล มีแนวทางในการให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย และช่วยสร้างความมั่นใจให้กับผู้ส่งข้อมูลและผู้รับข้อมูลที่ใช้บริการนำส่งข้อมูลอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานฉบับนี้สามารถใช้ได้กับหน่วยงานที่เป็นผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ เช่น

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

อย่างไรก็ตาม หน่วยงานที่เกี่ยวข้องอาจจะมีข้อกำหนดอื่น ๆ ตามหลักเกณฑ์ที่กำหนดไว้เป็นการเฉพาะ เช่น เกณฑ์วิธี (protocol) ของการรับส่งข้อมูล โครงสร้างข้อมูลของข้อมูลที่จะส่ง ดังนั้น ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ควรดำเนินการตามข้อกำหนดอื่น ๆ ที่เกี่ยวข้องด้วย

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 บริการนำส่งข้อมูลอิเล็กทรอนิกส์ (electronic delivery service) หมายถึง บริการที่ช่วยให้ผู้ส่งข้อมูลและผู้รับข้อมูลสามารถรับส่งข้อมูลด้วยวิธีการทางอิเล็กทรอนิกส์ รวมถึงช่วยบันทึกหลักฐานเกี่ยวกับการจัดการข้อมูล หลักฐานการส่งและรับข้อมูล และช่วยปกป้องข้อมูลจากความเสี่ยงจากการสูญหาย การโจรกรรม ความเสียหาย หรือการเปลี่ยนแปลงใด ๆ โดยไม่ได้รับอนุญาต

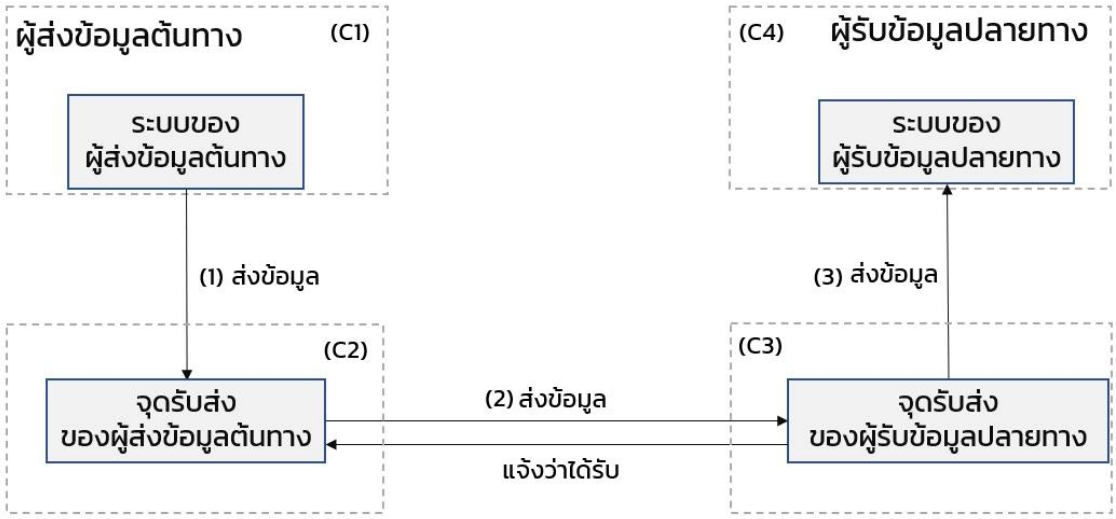
2.2 ผู้ส่งข้อมูลต้นทาง (original sender) หมายถึง บุคคลซึ่งเป็นผู้ส่งข้อมูลอิเล็กทรอนิกส์ก่อนจะมีการเก็บรักษาข้อมูลเพื่อส่งไปตามวิธีการที่ผู้นั้นกำหนด โดยบุคคลนั้นอาจจะส่งข้อมูลอิเล็กทรอนิกส์ด้วยตนเอง หรือมีการส่งข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนบุคคลนั้นก็ได้ ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

2.3 ผู้รับข้อมูลปลายทาง (final recipient) หมายถึง บุคคลซึ่งผู้ส่งข้อมูลประสงค์จะส่งข้อมูลอิเล็กทรอนิกส์ให้และได้รับข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลางสำหรับข้อมูลอิเล็กทรอนิกส์นั้น

2.4 ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ (electronic delivery service provider) หรือ ผู้ให้บริการ (service provider) หมายถึง บุคคลที่ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ โดยมีการส่งข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนผู้ส่งข้อมูลต้นทาง หรือมีการรับข้อมูลอิเล็กทรอนิกส์ในนามหรือแทนผู้รับข้อมูลปลายทาง

3. ภาพรวมของการนำส่งข้อมูลอิเล็กทรอนิกส์

รูปแบบการเชื่อมต่อ (topology) ของการนำส่งข้อมูลอิเล็กทรอนิกส์ โดยทั่วไปจะเป็นรูปแบบ 4-corner model (ตามรูปที่ 1) ซึ่งประกอบด้วย ผู้ส่งข้อมูลต้นทาง (original sender: C1) ผู้รับข้อมูลปลายทาง (final recipient: C4) จุดรับส่งของผู้ส่งข้อมูลต้นทาง (original sender's access point: C2) และจุดรับส่งของผู้รับข้อมูลปลายทาง (final recipient's access point: C3) ทั้งนี้ จุดรับส่ง (access point) จะเป็นระบบที่เชื่อมต่อกับผู้ส่งข้อมูลหรือผู้รับข้อมูล เพื่อช่วยให้ผู้ส่งข้อมูลและผู้รับข้อมูลซึ่งอาจมีระบบที่แตกต่างกัน สามารถรับส่งข้อมูลอิเล็กทรอนิกส์ระหว่างกันตามเกณฑ์วิธี (protocol) ที่กำหนด



รูปที่ 1 รูปแบบการเชื่อมต่อแบบ 4-corner model

การนำส่งข้อมูลอิเล็กทรอนิกส์ตามรูปแบบการเชื่อมต่อแบบ 4-corner model มีขั้นตอนทั่วไป ดังนี้

(1) ผู้ส่งข้อมูลต้นทาง (C1) สร้างและส่งข้อมูล (submit) ไปยังจุดรับส่งของผู้ส่งข้อมูลต้นทาง (C2) ด้วยระบบของ C1 ที่เชื่อมต่อกับ C2

(2) จุดรับส่งของผู้ส่งข้อมูลต้นทาง (C2) และจุดรับส่งของผู้รับข้อมูลปลายทาง (C3) รับส่งข้อมูลอิเล็กทรอนิกส์ระหว่างกันตามเกณฑ์วิธี (protocol) ที่ตกลงกัน

(3) จุดรับส่งของผู้รับข้อมูลปลายทาง (C3) ส่งต่อข้อมูล (deliver) ไปยังผู้รับข้อมูลปลายทาง (C4) เพื่อให้ระบบของ C4 ที่เชื่อมต่อกับ C3 นำข้อมูลที่ได้รับมาไปประมวลผล

ทั้งนี้ ระบบสนับสนุน (backend system) ของผู้ส่งข้อมูลต้นทาง (C1) หรือผู้รับข้อมูลปลายทาง (C4) อาจเป็นระบบที่ให้บริการโดยจุดรับส่งของผู้ส่งข้อมูลต้นทาง (C2) หรือจุดรับส่งของผู้รับข้อมูลปลายทาง (C3) ก็ได้

4. ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์

ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ตามรูปแบบการเชื่อมต่อแบบ 4-corner model มีจำนวน 6 ข้อ ดังนี้

(1) การใช้ช่องทางการสื่อสารที่มีความปลอดภัย (protected channel) เพื่อให้มีการรักษาความครบถ้วนและการรักษาความลับของข้อมูลระหว่างการนำส่ง

(2) การเข้ารหัสลับของข้อมูล (message encryption) เพื่อให้ผู้รับข้อมูลปลายทางเท่านั้นที่สามารถเข้าถึงข้อมูลได้

(3) การระบุตัวผู้ส่งข้อมูลต้นทาง (sender identification) เพื่อตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ส่งข้อมูลต้นทาง

(4) การระบุตัวผู้รับข้อมูลปลายทาง (recipient identification) เพื่อตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้รับข้อมูลปลายทางก่อนการนำส่งข้อมูล

(5) การอ้างอิงเวลา (time reference) เพื่อระบุวันเวลาที่ส่งข้อมูลและรับข้อมูล

(6) หลักฐานการส่งข้อมูลและการรับข้อมูล (proof of send and receive) เพื่อให้ผู้ส่งข้อมูลต้นทางและผู้รับข้อมูลปลายทางมีหลักฐานของการส่งข้อมูลและการรับข้อมูล

ทั้งนี้ รายละเอียดของข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ เป็นไปตามตารางที่ 1

ตารางที่ 1 ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์

ข้อกำหนด	ผู้ส่งข้อมูลต้นทาง (C1)	จุดรับส่งของผู้ส่งข้อมูลต้นทาง (C2)	จุดรับส่งของผู้รับข้อมูลปลายทาง (C3)	ผู้รับข้อมูลปลายทาง (C4)
4.1 การใช้ช่องทางการสื่อสารที่มีความปลอดภัย (protected channel)				
(1) ผู้ส่งข้อมูลต้นทาง (C1) ผู้รับข้อมูลปลายทาง (C4) จุดรับส่งของผู้ส่งข้อมูลต้นทาง (C2) และจุดรับส่งของผู้รับข้อมูลปลายทาง (C3) ต้องใช้ช่องทางการสื่อสารที่มีความปลอดภัยผ่านเกณฑ์วิธี Transport Layer Security (TLS) protocol ในระดับที่มีความมั่นคงปลอดภัย เช่น TLS 1.2 หรือเวอร์ชันที่สูงกว่า ซึ่งช่วยให้มีการรักษาความครบถ้วนและการรักษาความลับของข้อมูลด้วยการเข้ารหัสลับ (symmetric-key encryption) ระหว่างการนำส่งระหว่าง C1 กับ C2, C2 กับ C3 และ C3 กับ C4	✓	✓	✓	✓
4.2 การเข้ารหัสลับของข้อมูล				
(1) หากข้อมูลที่จะส่งเป็นข้อมูลส่วนบุคคลที่อ่อนไหว (sensitive data) หรือประสงค์จะให้ผู้รับข้อมูลปลายทางเท่านั้นที่สามารถเข้าถึงข้อมูลได้ ผู้ส่งข้อมูลต้นทางสามารถดำเนินการเข้ารหัสลับข้อมูล (public-key encryption) ด้วยกุญแจสารธารณะของผู้รับข้อมูลปลายทาง	✓			
4.3 การระบุตัวผู้ส่งข้อมูลต้นทาง				
(1) จุดรับส่งของผู้ส่งข้อมูลต้นทางอาจทำหน้าที่ระบุตัวตนของผู้ส่งข้อมูลต้นทางก่อนการนำส่งข้อมูล โดยจุดรับส่งของผู้ส่งข้อมูลต้นทางเป็นเจ้าของใบรับรองในการสนับสนุนตราประทับอิเล็กทรอนิกส์ (e-seal) ทั้งนี้ การระบุตัวตนอาจมีรายละเอียดเบื้องต้นดังนี้ — ผู้ส่งข้อมูลต้นทางยืนยันตัวตนกับจุดรับส่งของผู้ส่งข้อมูลต้นทางด้วยวิธีการใดวิธีการหนึ่งดังนี้ - การตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของผู้ส่งข้อมูลต้นทาง เช่น บัญชีผู้ใช้และรหัสผ่าน (username and password) สำหรับใช้ยืนยันตัวตน - การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ส่งข้อมูลต้นทางจากใบรับรองของผู้ส่งข้อมูล		✓		

ข้อกำหนด	ผู้ส่งข้อมูลต้นทาง (C1)	จุดรับส่งของผู้ส่งข้อมูลต้นทาง (C2)	จุดรับส่งของผู้รับข้อมูลปลายทาง (C3)	ผู้รับข้อมูลปลายทาง (C4)
ต้นทาง ด้วยการยืนยันตัวตนทั้งสองฝ่าย (mutual authentication) ของเกณฑ์วิธี TLS — จุดรับส่งของผู้ส่งข้อมูลต้นทางนำส่งข้อมูลระบุตัวตนของผู้ส่งข้อมูลต้นทางรวมกับข้อมูลที่จะส่ง เพื่อให้ผู้รับข้อมูลปลายทางสามารถระบุตัวผู้ส่งข้อมูลต้นทาง — กรณีนี้เหมาะกับ ผู้ส่งข้อมูลต้นทางเป็นหน่วยงานที่มีข้อจำกัดในการจัดหาใบรับรองมาใช้งาน จึงได้มอบหมายจุดรับส่งของผู้ส่งข้อมูลต้นทางให้จัดการแทน ทั้งนี้ ผู้ส่งข้อมูลต้นทางและจุดส่งต่อของผู้ส่งข้อมูลต้นทางควรมีข้อตกลงทางกฎหมายระหว่างกัน				
(2) กรณีที่ผู้ส่งข้อมูลต้นทางเป็นเจ้าของใบรับรอง ผู้ส่งข้อมูลต้นทางอาจทำหน้าที่เป็นผู้สร้างตราประทับอิเล็กทรอนิกส์หรือลายมือชื่ออิเล็กทรอนิกส์ประกอบกับข้อมูลที่จะส่ง โดยผู้ที่เกี่ยวข้องสามารถระบุตัวตนผู้ส่งข้อมูลต้นทางได้จากข้อมูลอัตลักษณ์ในใบรับรองของผู้ส่งข้อมูลต้นทาง ทั้งนี้ จุดรับส่งข้อมูลไม่จำเป็นต้องสร้างตราประทับอิเล็กทรอนิกส์เพิ่มเติม	✓			
4.4 การระบุตัวผู้รับข้อมูลปลายทาง				
(1) จุดรับส่งของผู้รับข้อมูลปลายทางต้องระบุตัวตนของผู้รับข้อมูลปลายทางก่อนการนำส่งข้อมูล ด้วยวิธีการใดวิธีการหนึ่งดังนี้ — การตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของผู้ส่งข้อมูลต้นทาง เช่น บัญชีผู้ใช้และรหัสผ่าน (username and password) สำหรับใช้ยืนยันตัวตน — การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ส่งข้อมูลต้นทางจากใบรับรอง (digital certificate) ของผู้ส่งข้อมูลต้นทาง จากการยืนยันตัวตนทั้งสองฝ่าย (mutual authentication) ของเกณฑ์วิธี TLS			✓	

ข้อกำหนด	ผู้ส่งข้อมูลต้นทาง (C1)	จุดรับส่งของผู้ส่งข้อมูลต้นทาง (C2)	จุดรับส่งของผู้รับข้อมูลปลายทาง (C3)	ผู้รับข้อมูลปลายทาง (C4)
4.5 การอ้างอิงเวลา				
(1) จุดรับส่งของผู้ส่งข้อมูลต้นทางและจุดรับส่งของผู้รับข้อมูลปลายทางต้องใช้การระบุวันเวลาที่น่าเชื่อถือ เพื่อสร้างหลักฐานยืนยันการส่งข้อมูลและการรับข้อมูล ณ เวลานั้น ๆ โดยสามารถใช้เวลาอ้างอิงจากระบบภายใน (system clock) หรือบริการประทับเวลาของผู้ให้บริการประทับเวลา (time-stamping authority: TSA)		✓	✓	
4.6 หลักฐานการส่งและการรับข้อมูล				
(1) จุดรับส่งของผู้ส่งข้อมูลต้นทางและจุดรับส่งของผู้รับข้อมูลปลายทางต้องจัดทำหลักฐานที่เกี่ยวข้องกับการนำส่งข้อมูลอิเล็กทรอนิกส์ ให้กับผู้ส่งข้อมูลต้นทางและผู้รับข้อมูลปลายทาง โดยมีรายละเอียดอย่างน้อย ดังนี้ — ข้อมูลระบุตัวผู้ส่งข้อมูลต้นทางและผู้รับข้อมูลปลายทาง — หลักฐานที่แสดงว่าผู้ส่งข้อมูลต้นทางได้รับการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์แล้ว — หลักฐานที่แสดงว่าผู้รับข้อมูลปลายทางได้รับการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ก่อนการนำส่งข้อมูลอิเล็กทรอนิกส์ — บันทึกเหตุการณ์ (log) ของการส่งและรับข้อมูล การตรวจสอบอัตลักษณ์ของผู้ส่งข้อมูลต้นทางและผู้รับข้อมูลปลายทาง — วิธีการที่แสดงว่าข้อมูลไม่มีการแก้ไขเปลี่ยนแปลงระหว่างการส่ง เช่น การมีช่องทางให้เข้าถึงข้อมูลต้นฉบับ หรือการส่งข้อมูล digest ของข้อมูลต้นฉบับไปด้วย ทั้งนี้ หลักฐานการส่งข้อมูลและรับข้อมูลต้องเชื่อมโยงกับวันเวลาที่น่าเชื่อถือซึ่งแสดงการส่งหรือรับข้อมูล		✓	✓	

ข้อกำหนด	ผู้ส่งข้อมูลต้นทาง (C1)	จุดรับส่งของผู้ส่งข้อมูลต้นทาง (C2)	จุดรับส่งของผู้รับข้อมูลปลายทาง (C3)	ผู้รับข้อมูลปลายทาง (C4)
(2) ในการสร้างข้อมูลแจ้งเตือนการรับข้อมูล จุดรับส่งของผู้รับข้อมูลปลายทางต้องสร้างตราประทับอิเล็กทรอนิกส์ประกอบกับหลักฐานการรับข้อมูล ก่อนส่งกลับให้จุดรับส่งของผู้ส่งข้อมูลต้นทางเพื่อยืนยันว่าได้รับข้อมูลแล้ว			✓	

67

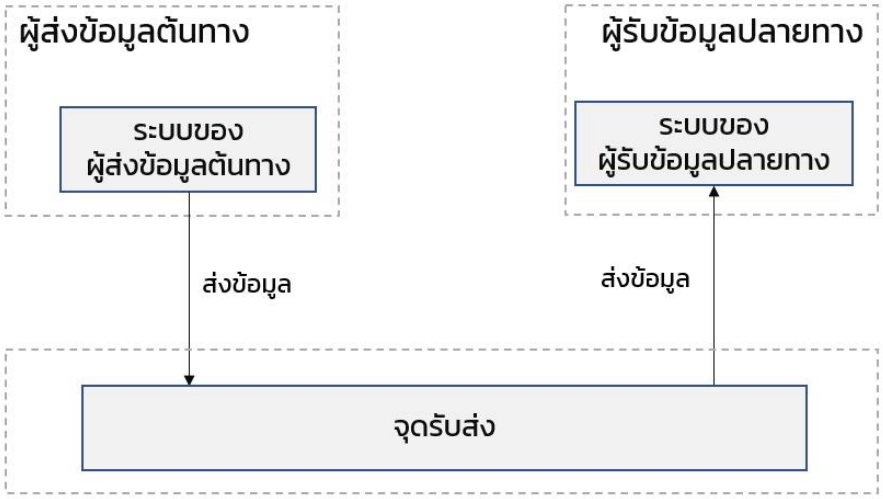
นอกจากรูปแบบการเชื่อมต่อแบบ 4-corner model แล้ว ข้อกำหนดข้างต้นสามารถนำมาพิจารณากับรูปแบบการเชื่อมต่อที่อาจเป็นไปได้ ดังนี้

(1) ในกรณีที่รูปแบบการเชื่อมต่อแบบ 4-corner model มีจุดรับส่งเพิ่มเติมระหว่างจุดรับส่งของผู้ส่งข้อมูลต้นทาง (C2) และจุดรับส่งของผู้รับข้อมูลปลายทาง (C3) จุดรับส่งเพิ่มเติมเหล่านั้นต้องนำส่งข้อมูลอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยทางสารสนเทศด้วย โดยอย่างน้อยต้องใช้ช่องทางการสื่อสารที่มีความปลอดภัย

(2) รูปแบบการเชื่อมต่อแบบ 3-corner model

ผู้ส่งข้อมูลต้นทางส่งข้อมูลให้ผู้รับข้อมูลปลายทางผ่านจุดรับส่งข้อมูล ซึ่งเป็นผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ที่เป็นหน่วยงานเดียวกัน

จุดรับส่งข้อมูลควรปฏิบัติตามข้อกำหนดในข้อเสนอแนะมาตรฐานฉบับนี้ด้วย



รูปที่ 2 รูปแบบการเชื่อมต่อแบบ 3-corner model

(3) รูปแบบการเชื่อมต่อแบบ 2-corner model

ผู้ส่งข้อมูลต้นทางส่งข้อมูลให้ผู้รับข้อมูลปลายทางโดยตรง โดยไม่ผ่านจุดรับส่งข้อมูล เช่น การส่งข้อมูลจากเครื่องเซิร์ฟเวอร์ของผู้ส่งข้อมูลต้นทางไปยังเครื่องเซิร์ฟเวอร์ของผู้รับข้อมูลปลายทาง

ข้อกำหนดในข้อเสนอแนะมาตรฐานฉบับนี้ จะไม่ครอบคลุมรูปแบบการเชื่อมต่อแบบ 2-corner model เนื่องจากไม่มีผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์

รูปที่ 3 รูปแบบการเชื่อมต่อแบบ 2-corner model

5. มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริการนำส่งข้อมูลอิเล็กทรอนิกส์

มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ อ้างอิงมาตรการควบคุม (control) และแนวปฏิบัติ (guidance) ที่เกี่ยวข้องตามมาตรฐาน ISO/IEC 27002:2022 [2] 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 ได้พิจารณามาตรการควบคุมทั้งหมดของ ISO/IEC 27002:2022 ตามบริบทและประเด็นที่เกี่ยวข้องกับบริการนำส่งข้อมูลอิเล็กทรอนิกส์ และแบ่งมาตรการควบคุมออกเป็น 3 กลุ่มตามระดับความจำเป็น ดังนี้

(1) มาตรการควบคุมที่จำเป็น (mandatory controls) จำนวน 50 ข้อ
(2) มาตรการควบคุมที่เป็นทางเลือก (optional controls) จำนวน 33 ข้อ
(3) มาตรการควบคุมที่เฉพาะกรณี (conditional controls) จำนวน 10 ข้อ

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

นอกจากนี้ ผู้ให้บริการสามารถเลือกปฏิบัติตามมาตรการควบคุมที่เป็นทางเลือก (optional controls) เพิ่มเติม โดยพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน และหลักเกณฑ์ของหน่วยงานที่กำกับดูแลบริการนำส่งข้อมูลอิเล็กทรอนิกส์แต่ละประเภท

5.1 มาตรการควบคุมด้านองค์กร (organizational controls)

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
1	**นโยบายความมั่นคงปลอดภัยสารสนเทศ (policies for information security)** หน่วยงานควรกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศและนโยบายเฉพาะเรื่องด้านความมั่นคงปลอดภัยซึ่งได้รับการอนุมัติโดยผู้บริหาร รวมถึงเผยแพร่และสื่อสารให้บุคลากรที่เกี่ยวข้องรับทราบ นอกจากนี้ หน่วยงานควรมีการทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงการดำเนินงานใด ๆ ภายในองค์กร	mandatory	ข้อ 5.1

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
2	**การกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (information security roles and responsibilities)** หน่วยงานควรกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ และจัดสรรให้มีความเหมาะสมตามความต้องการของหน่วยงาน	mandatory	ข้อ 5.2
3	**การแบ่งแยกหน้าที่ความรับผิดชอบ (segregation of duties)** หน่วยงานควรแบ่งแยกหน้าที่หรือส่วนงานที่รับผิดชอบที่อาจมีการขัดต่อการปฏิบัติงานออกจากกัน	optional	ข้อ 5.3
4	**การจัดการความรับผิดชอบ (management responsibilities)** ผู้บริหารของหน่วยงานควรกำหนดให้บุคลากรทั้งหมดปฏิบัติตามการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยเป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศ นโยบายเฉพาะเรื่องด้านความมั่นคงปลอดภัยสารสนเทศ และขั้นตอนการปฏิบัติงานขององค์กร	optional	ข้อ 5.4
5	**การติดต่อกับหน่วยงานผู้มีอำนาจ (contact with authorities)** หน่วยงานควรจัดตั้งและรักษาช่องการติดต่อสื่อสารกับหน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ	mandatory	ข้อ 5.5
6	**การติดต่อกับกลุ่มผลประโยชน์พิเศษ (contact with special interest groups)** หน่วยงานควรจัดตั้งและรักษาช่องทางติดต่อสื่อสารกับกลุ่มผลประโยชน์พิเศษ กลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และสมาคมวิชาชีพอื่น ๆ	optional	ข้อ 5.6
7	**ศูนย์รวมข้อมูลภัยคุกคาม (threat intelligence)** หน่วยงานควรรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับภัยคุกคามเพื่อให้มีศูนย์รวมข้อมูลภัยคุกคาม (threat intelligence)	optional	ข้อ 5.7
8	**ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (information security in project management)** หน่วยงานควรบูรณาการความมั่นคงปลอดภัยสารสนเทศเข้ากับการบริหารจัดการโครงการ	optional	ข้อ 5.8

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
9	**บัญชีของข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ (inventory of information and other associated assets)** หน่วยงานควรจัดทำและเก็บรักษาบัญชีของข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ซึ่งรวมถึง ข้อมูลระบุเจ้าของทรัพย์สิน	mandatory	ข้อ 5.9
10	**การใช้ข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ อย่างเหมาะสม (acceptable use of information and other associated assets)** หน่วยงานควรมีการกำหนด จัดทำเอกสาร และนำกฎและขั้นตอนเกี่ยวกับการใช้ข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ไปปฏิบัติอย่างเหมาะสม	optional	ข้อ 5.10
11	**การคืนทรัพย์สิน (return of assets)** หน่วยงานควรกำหนดให้บุคลากรและผู้ที่มีส่วนเกี่ยวข้องอื่น ๆ คืนทรัพย์สินทั้งหมดขององค์กรที่ตนถือครองเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงของการจ้างงาน	optional	ข้อ 5.11
12	**ชั้นความลับของข้อมูล (classification of information)** หน่วยงานควรจำแนกข้อมูลตามความมั่นคงปลอดภัยสารสนเทศขององค์กรโดยเป็นไปตามข้อกำหนดการรักษาความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง	mandatory	ข้อ 5.12
13	**การทำป้ายบ่งชี้สารสนเทศ (labelling of information)** หน่วยงานควรกำหนดขั้นตอนการทำป้ายบ่งชี้สารสนเทศอย่างเหมาะสม และนำไปปฏิบัติให้สอดคล้องกับวิธีการจัดชั้นความลับของข้อมูลที่องค์กรกำหนดไว้	optional	ข้อ 5.13
14	**การถ่ายโอนสารสนเทศ (information transfer)** หน่วยงานควรมีการกำหนดกฎเกณฑ์ ขั้นตอนการปฏิบัติ หรือข้อตกลงในการถ่ายโอนสารสนเทศทุกประเภทภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอก	mandatory	ข้อ 5.14
15	**การควบคุมการเข้าถึง (access control)**	mandatory	ข้อ 5.15

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
	หน่วยงานควรมีการกำหนดกฎเกณฑ์การเข้าถึงข้อมูลและทรัพย์สินอื่น ๆ ทางกายภาพ (physical access) และการเข้าถึงเชิงตรรกะ (logical access) โดยคำนึงถึงข้อกำหนดทางธุรกิจและด้านความมั่นคงปลอดภัยสารสนเทศ		
16	**การจัดการข้อมูลเกี่ยวกับอัตลักษณ์ (identity management)** หน่วยงานควรมีการจัดการข้อมูลเกี่ยวกับอัตลักษณ์ทั้งวงจร	mandatory	ข้อ 5.16
17	**ข้อมูลการยืนยันตัวตน (authentication information)** หน่วยงานควรมีการควบคุมกระบวนการการจัดการและการจัดสรรข้อมูลการยืนยันตัวตน และให้คำแนะนำแก่บุคลากรในการจัดการข้อมูลการยืนยันตัวตน	mandatory	ข้อ 5.17
18	**สิทธิการเข้าถึง (access rights)** หน่วยงานควรมีการจัดเตรียม ทบทวน แก้ไข หรือลบสิทธิการเข้าถึงข้อมูลและสินทรัพย์ที่เกี่ยวข้องอื่น ๆ ตามนโยบายเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศและกฎระเบียบขององค์กร	mandatory	ข้อ 5.18
19	**ความมั่นคงปลอดภัยสารสนเทศเกี่ยวกับความสัมพันธ์กับผู้ให้บริการภายนอก (information security in supplier relationships)** หน่วยงานควรมีการกำหนดกระบวนการและดำเนินการเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์หรือบริการของผู้ให้บริการภายนอก	conditional (ในกรณีที่ให้หน่วยงานภายนอกทำหน้าที่ให้บริการแทน)	ข้อ 5.19
20	**การระบุความมั่นคงปลอดภัยสารสนเทศในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (addressing information security within supplier agreements)** หน่วยงานควรมีการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง และตกลงกับผู้ให้บริการภายนอกแต่ละรายตามประเภทของความสัมพันธ์กับผู้ให้บริการภายนอก	conditional (ในกรณีที่ให้หน่วยงานภายนอกทำหน้าที่ให้บริการแทน)	ข้อ 5.20
21	**การจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานระบบสารสนเทศ (managing information security in the ICT supply chain)** หน่วยงานควรมีการกำหนดกระบวนการและแนวทางปฏิบัติเพื่อใช้ในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยในห่วงโซ่อุปทานระบบสารสนเทศ	optional	ข้อ 5.21

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
22	**การติดตาม การทบทวน และการจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (monitoring, review and change management of supplier services)** หน่วยงานควรมีการติดตาม ทบทวน ประเมิน และจัดการการเปลี่ยนแปลงในแนวทางปฏิบัติด้านความมั่นคงปลอดภัยและการส่งมอบบริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ	conditional (ในกรณีที่ให้หน่วยงานภายนอกทำหน้าที่ให้บริการแทน)	ข้อ 5.22
23	**ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (information security for use of cloud services)** หน่วยงานควรมีการกำหนดกระบวนการได้มาซึ่ง การใช้บริการ การจัดการ และการยกเลิกบริการคลาวด์ที่เป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	conditional (ในกรณีที่ใช้บริการคลาวด์)	ข้อ 5.23
24	**การวางแผนและเตรียมการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (information security incident management planning and preparation)** หน่วยงานควรมีการวางแผนและเตรียมการสำหรับการจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ โดยผู้ให้บริการควรมีการกำหนดกระบวนการจัดการ บทบาทและหน้าที่ความรับผิดชอบของบุคลากร และสื่อสารกระบวนการจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ	mandatory	ข้อ 5.24
25	**การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (assessment and decision on information security events)** หน่วยงานควรประเมินสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและตัดสินใจว่าเหตุการณ์นั้นจัดเป็นสถานการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่	mandatory	ข้อ 5.25
26	**การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (response to information security incidents)** หน่วยงานควรมีการตอบสนองและจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศตามแนวทางปฏิบัติที่เป็นลายลักษณ์อักษร	mandatory	ข้อ 5.26
27	**การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (learning from information security incidents)**	mandatory	ข้อ 5.27

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
	หน่วยงานควรนำความรู้ที่ได้รับจากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศเพื่อใช้ในการเสริมสร้างความแข็งแกร่งและปรับปรุงข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร		
28	**การเก็บรวบรวมหลักฐาน (collection of evidence)** หน่วยงานควรกำหนดขั้นตอนและดำเนินการตามขั้นตอนในการระบุ การรวบรวม การได้มา และการเก็บรักษาหลักฐานที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	mandatory	ข้อ 5.28
29	**ความมั่นคงปลอดภัยสารสนเทศในระหว่างการหยุดชะงัก (information security during disruption)** หน่วยงานควรวางแผนการรักษาความมั่นคงปลอดภัยสารสนเทศให้มีระดับที่เหมาะสมในระหว่างการหยุดชะงัก	mandatory	ข้อ 5.29
30	**ความพร้อมใช้งานของระบบสารสนเทศเพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)** หน่วยงานควรมีการวางแผน การดำเนินการ การบำรุงรักษา และการทดสอบความพร้อมใช้งานของระบบสารเทศที่เป็นไปตามวัตถุประสงค์และข้อกำหนดของความพร้อมใช้งานระบบสารสนเทศเพื่อความต่อเนื่องทางธุรกิจ	mandatory	ข้อ 5.30
31	**ข้อกำหนดทางกฎหมาย ข้อบังคับและสัญญา (legal, statutory, regulatory and contractual requirements)** หน่วยงานควรจัดทำเอกสารข้อกำหนดทางกฎหมาย ข้อบังคับ และสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ รวมถึงแนวทางขององค์กรในการปฏิบัติตามข้อกำหนด ทั้งนี้ ข้อกำหนดทางกฎหมาย ข้อบังคับ และสัญญาควรมีการปรับปรุงให้เป็นปัจจุบัน	mandatory	ข้อ 5.31
32	**สิทธิในทรัพย์สินทางปัญญา (intellectual property rights)** หน่วยงานควรมีแนวทางปฏิบัติที่มีความเหมาะสมเพื่อปกป้องสิทธิในทรัพย์สินทางปัญญา	optional	ข้อ 5.32
33	**การป้องกันข้อมูล (protection of records)** หน่วยงานควรป้องกันบันทึกจากการสูญหาย การถูกทำลาย การปลอมแปลง และการเข้าถึงหรือเผยแพร่โดยไม่ได้รับอนุญาต	mandatory	ข้อ 5.33

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
34	**การรักษาความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (privacy and protection of PII)** หน่วยงานควรระบุและปฏิบัติตามข้อกำหนดเกี่ยวกับการรักษาความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคลที่เป็นไปตามกฎหมาย ระเบียบข้อบังคับ และข้อกำหนดในสัญญา	optional	ข้อ 5.34
35	**การตรวจสอบอย่างอิสระด้านความมั่นคงปลอดภัย (independent review of information security)** หน่วยงานควรมีการตรวจสอบอย่างอิสระในด้านความมั่นคงปลอดภัยสารสนเทศ เช่น ตรวจสอบการจัดการและการดำเนินงานที่เกี่ยวข้องกับบุคลากร กระบวนการทำงาน เทคโนโลยี โดยการตรวจสอบนี้ควรได้รับการทบทวนตามช่วงเวลาที่วางแผนไว้ หรือเมื่อมีการเปลี่ยนแปลงสำคัญเกิดขึ้น	optional	ข้อ 5.35
36	**การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัย (compliance with policies, rules and standards for information security)** หน่วยงานควรมีการทบทวนการปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ	mandatory	ข้อ 5.36
37	**เอกสารขั้นตอนการปฏิบัติงาน (documented operating procedures)** หน่วยงานควรจัดทำเอกสารขั้นตอนการปฏิบัติงานของอุปกรณ์ประมวลผลสารสนเทศ และเอกสารขั้นตอนการปฏิบัติงานนี้ควรเข้าถึงได้โดยบุคลากรที่เกี่ยวข้อง	mandatory	ข้อ 5.37

110 **5.2 มาตรการควบคุมด้านกายภาพ (physical controls)**

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
38	**ขอบเขตความมั่นคงปลอดภัยทางกายภาพ (physical security perimeters)** หน่วยงานควรกำหนดขอบเขตหรือบริเวณที่ต้องการรักษาความมั่นคงปลอดภัยเพื่อปกป้องข้อมูลและทรัพย์สินอื่น ๆ ที่เกี่ยวข้อง	mandatory	ข้อ 7.1
39	**การเข้าออกทางกายภาพ (physical entry)**	mandatory	ข้อ 7.2

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
	หน่วยงานควรมีการควบคุมการเข้าออกทางกายภาพของพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย		
40	**การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และอุปกรณ์ (securing offices, rooms and facilities)** หน่วยงานควรออกแบบและดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และอุปกรณ์	mandatory	ข้อ 7.3
41	**การเฝ้าติดตามความปลอดภัยทางกายภาพ (physical security monitoring)** หน่วยงานควรเฝ้าติดตามสถานที่ทางกายภาพเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต	mandatory	ข้อ 7.4
42	**การป้องกันภัยคุกคามด้านกายภาพและสิ่งแวดล้อม (protecting against physical and environmental threats)** หน่วยงานควรออกแบบและดำเนินการป้องกันภัยคุกคามด้านกายภาพและสิ่งแวดล้อม เช่น ภัยธรรมชาติ และภัยคุกคามทางกายภาพอื่น ๆ ต่อโครงสร้างทางกายภาพทั้งโดยเจตนาหรือไม่เจตนา	mandatory	ข้อ 7.5
43	**การปฏิบัติงานในพื้นที่ที่มีความมั่นคงปลอดภัย (working in secure areas)** หน่วยงานควรออกแบบและดำเนินการเกี่ยวกับมาตรการด้านความมั่นคงปลอดภัยสำหรับการปฏิบัติงานในพื้นที่ที่มีความมั่นคงปลอดภัย	mandatory	ข้อ 7.6
44	**กฎเกณฑ์โต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (clear desk and clear screen)** หน่วยงานควรมีการกำหนดและบังคับใช้กฎเกณฑ์อย่างเหมาะสมเกี่ยวกับโต๊ะทำงานปลอดเอกสารสำหรับกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ รวมถึงกฎเกณฑ์การป้องกันหน้าจอคอมพิวเตอร์สำหรับอุปกรณ์ประมวลผลข้อมูล	optional	ข้อ 7.7
45	**การจัดตั้งและการป้องกันอุปกรณ์ (equipment siting and protection)** หน่วยงานควรมีการจัดตั้งและป้องกันอุปกรณ์ให้มีความมั่นคงปลอดภัย	optional	ข้อ 7.8
46	**ความมั่นคงปลอดภัยของอุปกรณ์และสินทรัพย์ที่ใช้งานอยู่ภายนอกสำนักงาน (security of assets off-premises)**	optional	ข้อ 7.9

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
	หน่วยงานควรปกป้องทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานให้มีความมั่นคงปลอดภัย		
47	**การจัดเก็บสื่อบันทึกข้อมูล (storage media)** หน่วยงานควรมีการจัดการสื่อบันทึกข้อมูลผ่านวงจรการจัดการ เช่น การจัดหา การใช้ การขนส่ง การกำจัดสื่อบันทึกตามรูปแบบการจัดหมวดหมู่และข้อกำหนดในการจัดการขององค์กร	mandatory	ข้อ 7.10
48	**ระบบและอุปกรณ์สนับสนุนการทำงาน (supporting utilities)** หน่วยงานควรมีการปกป้องระบบอุปกรณ์ประมวลผลข้อมูลให้ได้รับการป้องกันจากไฟฟ้าขัดข้องและการหยุดชะงักอื่น ๆ ที่เกิดจากความล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงาน	optional	ข้อ 7.11
49	**ความมั่นคงปลอดภัยของการเดินสายสัญญาณและการสื่อสาร (cabling security)** หน่วยงานควรมีการปกป้องการเดินสายสัญญาณนำไฟฟ้า ข้อมูล หรือบริการที่สนับสนุนข้อมูลจากการดักจับสัญญาณ การแทรกแซงสัญญาณ หรือการทำให้สายสัญญาณเสียหาย	optional	ข้อ 7.12
50	**การบำรุงรักษาอุปกรณ์ (equipment maintenance)** หน่วยงานควรมีการบำรุงรักษาอุปกรณ์อย่างถูกต้องเพื่อให้มีสภาพพร้อมใช้งาน รักษาความถูกต้องครบถ้วนและมีการรักษาความลับของข้อมูล	mandatory	ข้อ 7.13
51	**การกำจัดหรือนำอุปกรณ์มาใช้ใหม่อย่างปลอดภัย (secure disposal or re-use of equipment)** หน่วยงานควรมีการตรวจสอบรายการของอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อให้แน่ใจว่าข้อมูลสำคัญและซอฟต์แวร์ที่มีใบอนุญาตได้ถูกลบออกหรือเขียนทับอย่างมั่นคงปลอดภัยก่อนมีการกำจัดทิ้งหรือนำอุปกรณ์มาใช้ใหม่	optional	ข้อ 7.14

111 **5.3 มาตรการควบคุมด้านบุคลากร (people controls)**

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
52	**การคัดเลือกบุคลากร (screening)** หน่วยงานควรตรวจสอบประวัติผู้สมัครทุกคนก่อนมีการว่าจ้างเพื่อเป็นบุคคลากรของหน่วยงาน โดยการตรวจสอบประวัติควรดำเนินการให้มี	optional	ข้อ 6.1

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
	ความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับความต้องการของธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง		
53	**ข้อตกลงและเงื่อนไขการจ้างงาน (terms and conditions of employment)** หน่วยงานควรระบุความรับผิดชอบของบุคลากรและองค์กรด้านความมั่นคงปลอดภัยสารสนเทศในข้อตกลงและเงื่อนไขการจ้างงาน	optional	ข้อ 6.2
54	**การสร้างความตระหนัก การศึกษา และการฝึกอบรมด้านความมั่นคงปลอดภัย (information security awareness, education and training)** บุคลากรของหน่วยงานและผู้ที่เกี่ยวข้องควรได้รับการสร้างความตระหนัก ได้รับการศึกษาและการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศที่เหมาะสม รวมถึงได้รับรู้ถึงนโยบายความมั่นคงปลอดภัยสารสนเทศ และนโยบายเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบ ที่มีความเป็นปัจจุบันอย่างสม่ำเสมอ	mandatory	ข้อ 6.3
55	**กระบวนการทางวินัย (disciplinary process)** หน่วยงานควรมีการกำหนดและสื่อสารกระบวนการทางวินัยอย่างเป็นทางการและมีการสื่อสารให้บุคลากรและผู้ที่มีส่วนเกี่ยวข้องทราบเพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศขององค์กร	optional	ข้อ 6.4
56	**การสิ้นสุดหรือการเปลี่ยนแปลงหน้าที่ความรับผิดชอบของการจ้างงาน (responsibilities after termination or change of employment)** หน่วยงานควรมีการกำหนด บังคับใช้ สื่อสารต่อบุคลากรและผู้ที่มีส่วนเกี่ยวข้องถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่ยังมีผลบังคับใช้หลังจากการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน	optional	ข้อ 6.5
57	**ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (confidentiality or non-disclosure agreements)**	optional	ข้อ 6.6

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
	หน่วยงานควรมีการระบุและจัดทำเอกสารข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับที่สะท้อนถึงความจำเป็นขององค์กรในการปกป้องข้อมูลสารสนเทศ โดยข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับควรมีการทบทวนและลงนามโดยบุคลากรและผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ		
58	**การทำงานจากระยะไกล (remote working)** หน่วยงานควรมีมาตรการด้านความปลอดภัยสารสนเทศเมื่อบุคลากรทำงานจากระยะไกลเพื่อป้องกันการเข้าถึง การประมวลผล หรือการจัดเก็บข้อมูลนอกสถานที่ขององค์กร	mandatory	ข้อ 6.7
59	**การรายงานสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (information security event reporting)** หน่วยงานควรจัดให้มีกลไกสำหรับบุคลากรในการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่สังเกตพบหรือสงสัยผ่านช่องทางที่เหมาะสมอย่างทันท่วงที	optional	ข้อ 6.8

112 **5.4 มาตรการควบคุมด้านเทคโนโลยี (technological controls)**

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
60	**อุปกรณ์ปลายทางของผู้ใช้ (user endpoint devices)** หน่วยงานควรมีการจัดการเพื่อให้มั่นใจว่าข้อมูลที่จัดเก็บ ประมวลผล หรือเข้าถึงผ่านอุปกรณ์ปลายทางของผู้ใช้ได้รับการปกป้อง	mandatory	ข้อ 8.1
61	**สิทธิการเข้าถึงของสิทธิระดับสูง (privileged access rights)** หน่วยงานควรมีการจัดสรรและจำกัดการเข้าถึงของสิทธิระดับสูง	mandatory	ข้อ 8.2
62	**การจำกัดการเข้าถึงข้อมูลสารสนเทศ (information access restriction)** หน่วยงานควรมีการจำกัดการเข้าถึงข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ ให้สอดคล้องกับนโยบายควบคุมการเข้าถึง	mandatory	ข้อ 8.3
63	**การเข้าถึงซอร์สโค้ดของโปรแกรม (access to source code)** หน่วยงานควรมีการจัดการอย่างเหมาะสมในการเข้าถึง การอ่าน และการเขียนซอร์สโค้ด เครื่องมือการพัฒนา และซอฟต์แวร์ไลบรารี	optional	ข้อ 8.4

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
64	**การยืนยันตัวตนอย่างปลอดภัย (secure authentication)** หน่วยงานควรมีการใช้เทคโนโลยีและกระบวนการยืนยันตัวตนที่มีความปลอดภัย โดยสอดคล้องกับข้อจำกัดการเข้าถึงข้อมูลและนโยบายควบคุมการเข้าถึง	mandatory	ข้อ 8.5
65	**การจัดการขีดความสามารถของระบบ (capacity management)** หน่วยงานควรตรวจสอบการใช้ทรัพยากรและปรับให้มีความสอดคล้องกับข้อกำหนดในปัจจุบันและข้อกำหนดที่คาดหวังเกี่ยวกับการจัดการขีดความสามารถของระบบ	mandatory	ข้อ 8.6
66	**การป้องกันมัลแวร์ (protection against malware)** หน่วยงานควรมีการดำเนินการป้องกันมัลแวร์อย่างเหมาะสมโดยผู้ใช้งานมีความตระหนักในการป้องกันมัลแวร์	mandatory	ข้อ 8.7
67	**การจัดการช่องโหว่ทางเทคนิค (management of technical vulnerabilities)** หน่วยงานควรมีข้อมูลช่องโหว่ทางเทคนิคของระบบสารสนเทศที่ใช้งาน โดยหน่วยงานควรมีการประเมินความเสี่ยงต่อช่องโหว่ทางเทคนิคดังกล่าวและใช้มาตรการที่เหมาะสม	mandatory	ข้อ 8.8
68	**การจัดการการตั้งค่า (configuration management)** หน่วยงานควรมีการจัดการการตั้งค่า ซึ่งรวมถึงกำหนดค่าความปลอดภัยของฮาร์ดแวร์ ซอฟต์แวร์ บริการต่าง ๆ และระบบเครือข่าย โดยควรมีการจัดทำเป็นเอกสาร ตรวจสอบติดตามและมีการทบทวนอย่างสม่ำเสมอ	mandatory	ข้อ 8.9
69	**การลบข้อมูล (information deletion)** หน่วยงานควรมีการลบข้อมูลที่จัดเก็บไว้ในระบบสารสนเทศ อุปกรณ์หรือสื่อบันทึกข้อมูลอื่น ๆ เมื่อไม่มีความต้องการใช้อีกต่อไป	mandatory	ข้อ 8.10
70	**การปกปิดข้อมูลเพื่อจำกัดการเห็นขอมูลทั้งหมด (data masking)** หน่วยงานควรดำเนินการเกี่ยวกับการปกปิดข้อมูลเพื่อจำกัดการเห็นข้อมูลทั้งหมด (data masking) ที่เป็นไปตามนโยบายการควบคุมการเข้าถึง และนโยบายเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง รวมถึงคำนึงถึงข้อกำหนดทางธุรกิจและกฎหมายที่เกี่ยวข้อง	optional	ข้อ 8.11
71	**การป้องกันการรั่วไหลของข้อมูล (data leakage prevention)**	optional	ข้อ 8.12

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
	หน่วยงานควรมีมาตรการป้องกันการรั่วไหลของข้อมูลที่ใช้กับระบบสารสนเทศ ระบบเครือข่าย และอุปกรณ์ประมวลผลอื่น ๆ ที่จัดเก็บหรือส่งข้อมูลที่ละเอียดอ่อน		
72	**การสำรองข้อมูล (information backup)** หน่วยงานควรมีการบำรุงรักษาและทดสอบการสำรองข้อมูล ซอฟต์แวร์ และระบบสารสนเทศอย่างสม่ำเสมอโดยเป็นไปตามนโยบายการสำรองข้อมูล	mandatory	ข้อ 8.13
73	**การเตรียมการอุปกรณ์ประมวลผลข้อมูลสำรอง (redundancy of information processing facilities)** หน่วยงานควรมีการเตรียมการอุปกรณ์ประมวลผลข้อมูลสำรองให้เพียงพอและเป็นไปตามข้อกำหนดด้านความพร้อมใช้งาน	mandatory	ข้อ 8.14
74	**การบันทึกข้อมูลเหตุการณ์ (logging)** หน่วยงานควรมีการสร้าง การจัดเก็บ การป้องกัน และการวิเคราะห์บันทึกข้อมูลเหตุการณ์ (logging) ข้อยกเว้น (exceptions) ข้อผิดพลาด (faults) และเหตุการณ์ที่เกี่ยวข้องอื่น ๆ	mandatory	ข้อ 8.15
75	**การเฝ้าติดตามเหตุการณ์ (monitoring activities)** หน่วยงานควรตรวจสอบระบบเครือข่าย ระบบสารสนเทศ และแอปพลิเคชันเพื่อหาพฤติกรรมที่ผิดปกติและดำเนินการอย่างเหมาะสมในการประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น	mandatory	ข้อ 8.16
76	**การตั้งค่าเทียบเวลา (clock synchronization)** หน่วยงานควรตั้งค่าเทียบเวลาระบบประมวลผลที่องค์กรใช้ให้สอดคล้องกับแหล่งเวลาที่น่าเชื่อถือ	mandatory	ข้อ 8.17
77	**การใช้โปรแกรมอรรถประโยชน์ที่ได้รับสิทธิพิเศษ (use of privileged utility programs)** หน่วยงานควรจำกัดและควบคุมอย่างเข้มงวดในการใช้โปรแกรมอรรถประโยชน์ที่สามารถลบหรือเปลี่ยนแปลงการควบคุมระบบสารสนเทศและแอปพลิเคชัน	optional	ข้อ 8.18
78	**การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ (installation of software on operational systems)**	optional	ข้อ 8.19

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
	หน่วยงานควรมีกระบวนการหรือมาตรการในการติดตั้งซอฟต์แวร์บนระบบปฏิบัติการให้มีความปลอดภัย		
79	**ความมั่นคงปลอดภัยของระบบเครือข่าย (networks security)** หน่วยงานควรมีการจัดการ ควบคุม และรักษาความปลอดภัยระบบเครือข่ายและอุปกรณ์เครือข่ายเพื่อปกป้องข้อมูลในระบบสารสนเทศและแอปพลิเคชัน	mandatory	ข้อ 8.20
80	**ความมั่นคงปลอดภัยของบริการเครือข่าย (security of network services)** หน่วยงานควรมีการดำเนินการและติดตามตรวจสอบกลไกการรักษาความปลอดภัยของระบบเครือข่าย ระดับของบริการและข้อกำหนดของบริการระบบเครือข่าย	mandatory	ข้อ 8.21
81	**การแบ่งแยกเครือข่าย (segregation of networks)** หน่วยงานควรแบ่งแยกกลุ่มการบริการข้อมูล กลุ่มผู้ใช้ และกลุ่มของระบบสารสนเทศในระบบเครือข่ายขององค์กร	mandatory	ข้อ 8.22
82	**การกรองเว็บ (web filtering)** หน่วยงานควรมีการจัดการการเข้าถึงเว็บไซต์ภายนอกเพื่อลดความเสี่ยงการเข้าถึงเนื้อหาที่เป็นอันตราย	optional	ข้อ 8.23
83	**การใช้การเข้ารหัสลับ (use of cryptography)** หน่วยงานควรมีการกำหนดและดำเนินการเกี่ยวกับกฎเกณฑ์การเข้ารหัสลับอย่างมีประสิทธิภาพ ซึ่งรวมถึงการบริหารจัดการกุญแจการเข้ารหัสลับ	mandatory	ข้อ 8.24
84	**วงจรการพัฒนาระบบอย่างปลอดภัย (secure development life cycle)** หน่วยงานควรมีการจัดทำและประยุกต์ใช้กฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบอย่างปลอดภัย	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	ข้อ 8.25
85	**ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (application security requirements)** หน่วยงานควรมีการระบุและอนุมัติข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศเมื่อมีการพัฒนาหรือใช้แอปพลิเคชันที่ได้รับมา	Optional	ข้อ 8.26

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
86	**ความมั่นคงปลอดภัยของสถาปัตยกรรมของระบบและหลักการทางวิศวกรรม (secure system architecture and engineering principles)** หน่วยงานควรมีการใช้หลักการระบบความมั่นคงปลอดภัยทางวิศวกรรม โดยควรจัดทำเป็นเอกสาร มีการบำรุงรักษา และนำไปประยุกต์ใช้กับกิจกรรมการพัฒนาระบบสารสนเทศ	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	ข้อ 8.27
87	**การเขียนโปรแกรมที่มีความปลอดภัย (secure coding)** หน่วยงานควรใช้หลักการเขียนโปรแกรมที่มีความปลอดภัยในการพัฒนาซอฟต์แวร์	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	ข้อ 8.28
88	**การทดสอบความมั่นคงปลอดภัยในการพัฒนาและรับรองระบบ (security testing in development and acceptance)** หน่วยงานควรมีการกำหนดและดำเนินการเกี่ยวกับการทดสอบความมั่นคงปลอดภัยในวงจรการพัฒนาระบบ	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	ข้อ 8.29
89	**การจ้างหน่วยงานภายนอกพัฒนาระบบ (outsourced development)** หน่วยงานควรติดตาม กำกับดูแล และทบทวนกิจกรรมที่เกี่ยวข้องกับการพัฒนาระบบโดยหน่วยงานภายนอก	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	ข้อ 8.30
90	**การแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการให้บริการออกจากกัน (separation of development, test and production environments)** หน่วยงานควรมีการแยกสภาพแวดล้อมและรักษาความปลอดภัยในสภาพแวดล้อมของการพัฒนา การทดสอบ และการให้บริการ	conditional (ในกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง)	ข้อ 8.31
91	**การบริหารจัดการการเปลี่ยนแปลง (change management)** หน่วยงานควรจัดการต่อการเปลี่ยนแปลงระบบสารสนเทศและอุปกรณ์ประมวลผลข้อมูลให้เป็นไปตามกระบวนการการจัดการการเปลี่ยนแปลง	mandatory	ข้อ 8.32
92	**ข้อมูลการทดสอบ (test information)** หน่วยงานควรมีการคัดเลือก การป้องกัน และการจัดการข้อมูลสำหรับการทดสอบอย่างเหมาะสม	optional	ข้อ 8.33

ข้อ	มาตรการควบคุม (control)	ความจำเป็น	แนวปฏิบัติ ตาม ISO/IEC 27002:2022
93	**การป้องกันระบบสารสนเทศระหว่างการตรวจสอบระบบ (protection of information systems during audit testing)** หน่วยงานควรมีการวางแผนและตกลงร่วมกันระหว่างผู้ทดสอบระบบและผู้บริหารที่เกี่ยวข้องในการตรวจสอบระบบและกิจกรรมการการประกันความมั่นคงปลอดภัยอื่นๆ ที่เกี่ยวข้องกับระบบปฏิบัติการ	optional	ข้อ 8.34

113

114 **บรรณานุกรม**

115

[1] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม.

[2] International Organization for Standardization, “ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements”, October 2022.

[3] International Organization for Standardization, “ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls”, March 2022.

[4] European Commission, "eDelivery Building Block, Security Controls, Linking eIDAS (Q)ERDS & eDelivery", Version 1.20, April 2022.

[5] European Telecommunications Standards Institute, "ETSI EN 319 401 V2.3.1 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers", May 2021.

[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.

116