กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

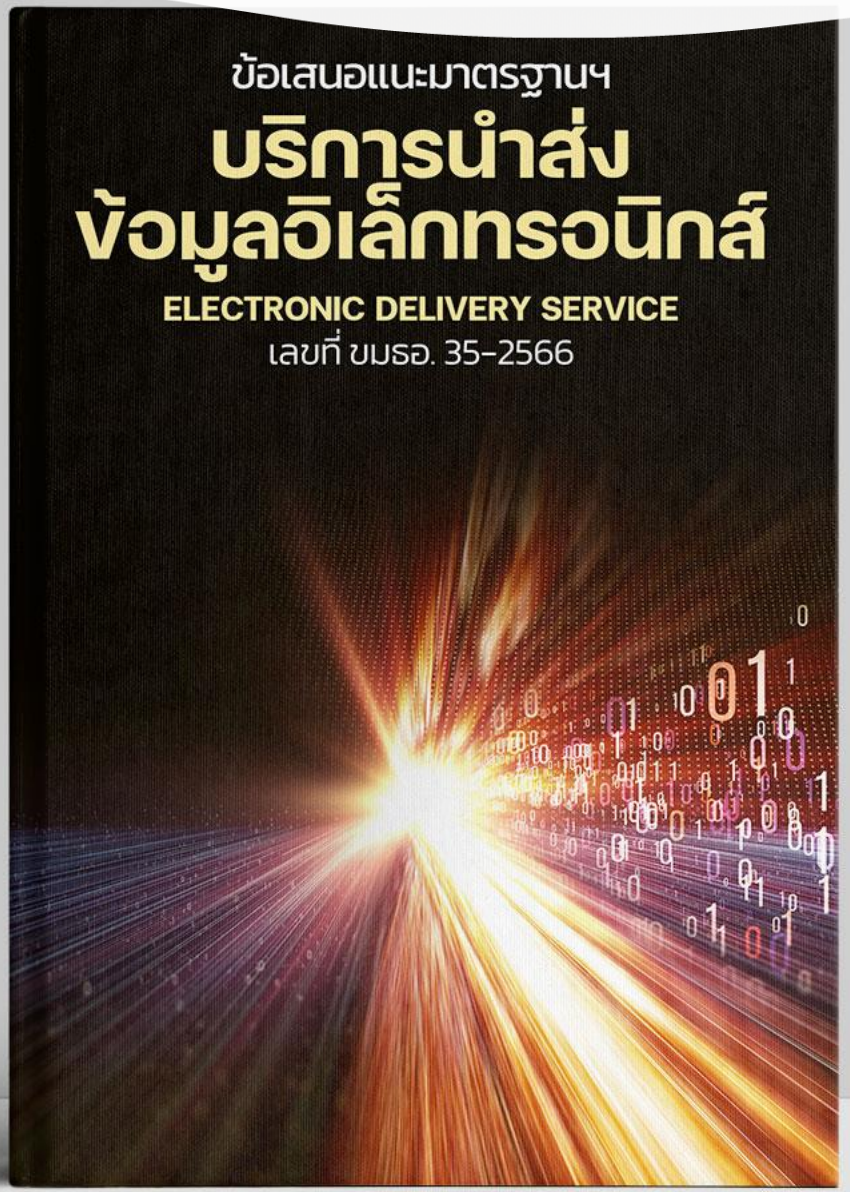
ETDA

ข้อเสนอแนะมาตรฐานฯ

บริการนำส่งข้อมูลอิเล็กทรอนิกส์

ELECTRONIC DELIVERY SERVICE

เลขที่ ขมธอ. 35-2566



บริการนำส่งข้อมูลอิเล็กทรอนิกส์ (Electronic Delivery Service)

บริการนำส่งข้อมูลอิเล็กทรอนิกส์ (electronic delivery service) หมายถึง บริการที่ช่วยให้ผู้ส่งข้อมูลและผู้รับข้อมูลสามารถรับส่งข้อมูลด้วยวิธีการทางอิเล็กทรอนิกส์ รวมถึงช่วยบันทึกหลักฐานการส่งและการรับข้อมูล และช่วยปกป้องข้อมูลจากความเสี่ยงของการสูญหาย การโจรกรรม ความเสียหาย หรือการเปลี่ยนแปลงใด ๆ โดยไม่ได้รับอนุญาต

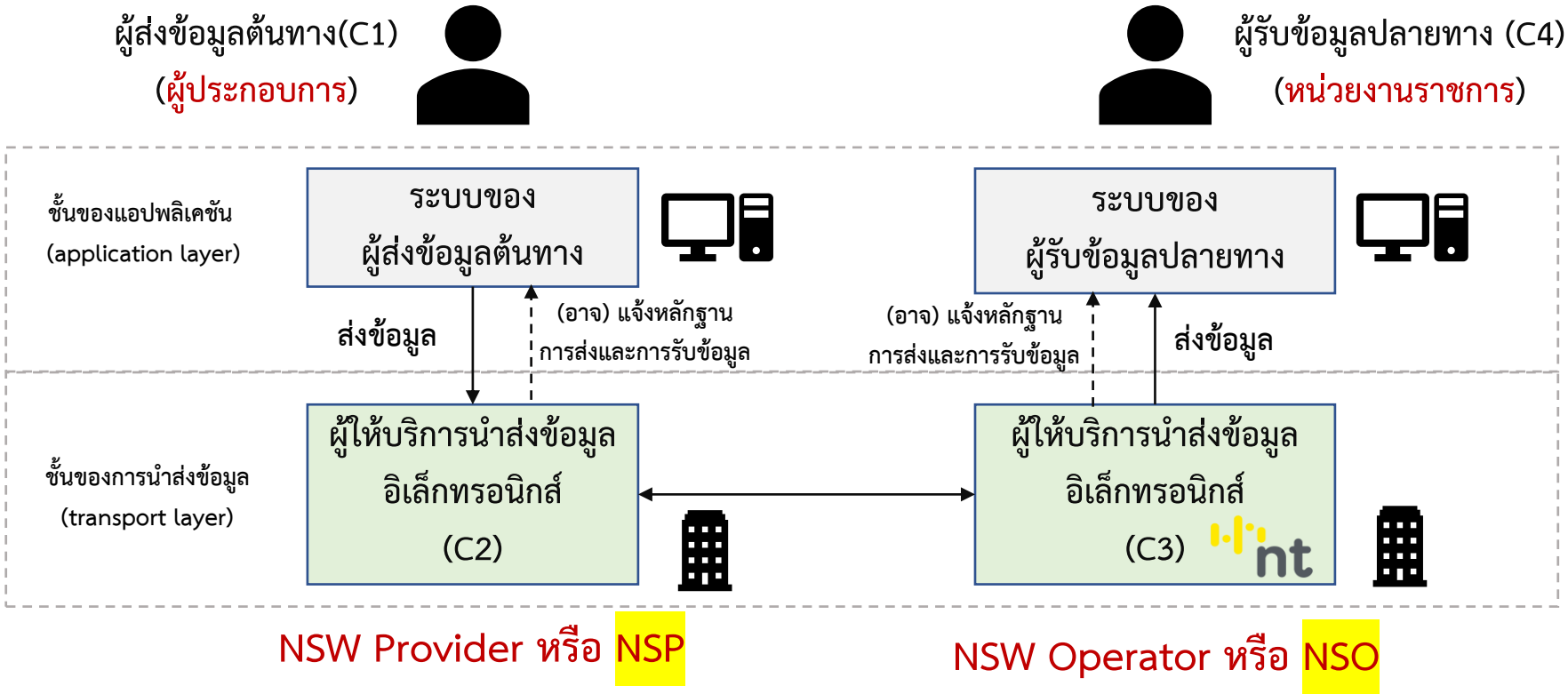
ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ (electronic delivery service provider) หมายถึง หน่วยงานที่ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานฉบับนี้สามารถใช้ได้กับหน่วยงานที่เป็นผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ เช่น

- ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ให้กับกรมสรรพากร
- ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงานที่เชื่อมต่อกับระบบ National Single Window (NSW)
- ผู้ให้บริการอื่น ๆ ที่ต้องการความน่าเชื่อถือในการนำส่งข้อมูลอิเล็กทรอนิกส์

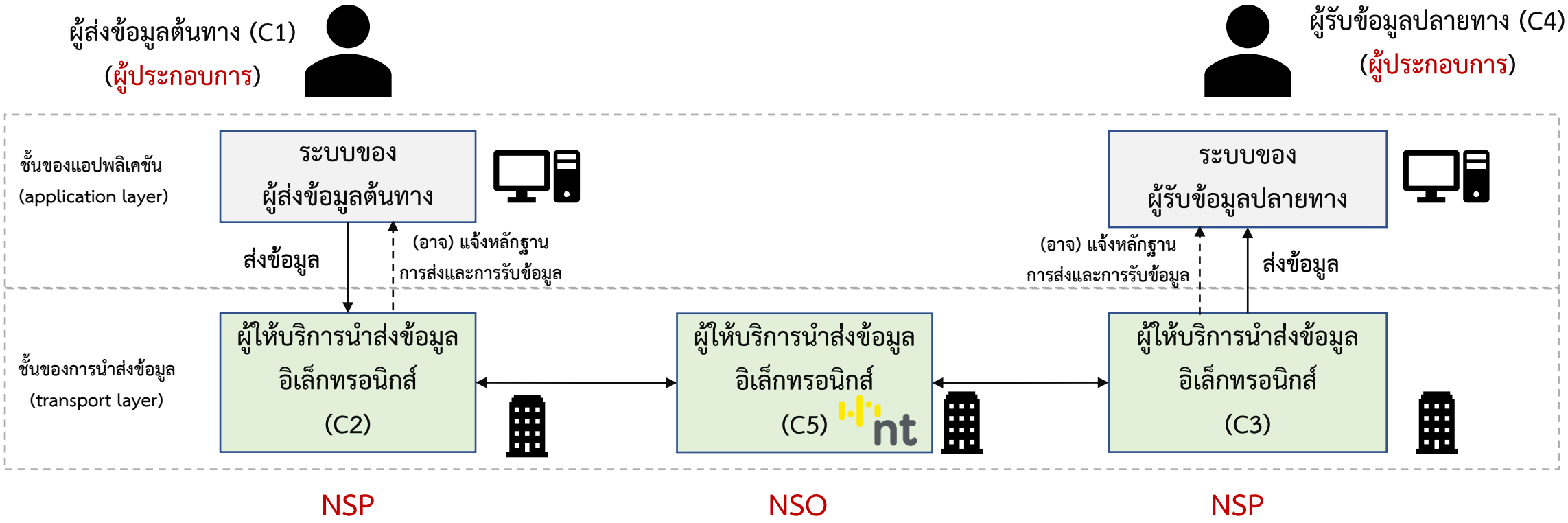
ตัวอย่างการนำส่งข้อมูลอิเล็กทรอนิกส์

ตัวอย่างบริการ : การนำส่งข้อมูลแบบ B2G ของกลุ่ม NSW เช่น การขอใบอนุญาตจากหน่วยงานภาครัฐ



ตัวอย่างการนำส่งข้อมูลอิเล็กทรอนิกส์

ตัวอย่างบริการ : การนำส่งข้อมูลแบบ B2B ของกลุ่ม NSW



โครงสร้างและที่มาของมาตรฐาน

1. ขอบข่าย
2. บทนิยาม
3. ภาพรวมของบริการนำส่งข้อมูลอิเล็กทรอนิกส์
4. ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์
5. ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ
   - 5.1 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
   - 5.2 มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ
     - 5.2.1 มาตรการควบคุมด้านองค์กร (organizational controls)
     - 5.2.2 มาตรการควบคุมด้านบุคลากร (people controls)
     - 5.2.3 มาตรการควบคุมด้านกายภาพ (physical controls)
     - 5.2.4 มาตรการควบคุมด้านเทคโนโลยี (technological controls)

บรรณานุกรม

เป็นข้อกำหนดที่เฉพาะเจาะจงต่อบริการนำส่งข้อมูลอิเล็กทรอนิกส์ โดยวิเคราะห์จากมาตรฐาน eDelivery Building Block Version 1.20, Security Controls Linking eIDAS (Q) ERDS& eDelivery, European Commission

ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ ใช้ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์เป็นหนึ่งในปัจจัยในการพิจารณากำหนดประเภทมาตรการควบคุม (control) จาก ISO/IEC 27002:2022 และสอดคล้องกับ ISO/IEC 27001:2022

Summary of ERDS requirements from the eIDAS regulation.

Requirement	Description	eIDAS reference
REQ1 **Message Integrity**	Messages should be secured against any modification during transmission.	Article 3 (36) Article 19 Article 24 Article 44, (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
REQ2 **Message Confidentiality**	Messages should be encrypted during transmission	Article 5 Article 19 Article 24
REQ3 **Sender Identification**	The identity of the sender should be verified.	Article 24 Article 44 (b) they ensure with a high level of confidence the identification of the sender;
REQ4 **Recipient / Addressee Identification**	Recipient / addressee Identity should be verified before the delivery of the message.	Article 24 Article 44 (c) they ensure the identification of the addressee before the delivery of the data;
REQ5 **Time-Reference**	The date and time of sending and receiving a message should be indicated via a qualified electronic timestamp.	Article 44 (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.
REQ6 **Proof of Send/Receive**	Sender and receiver of the message should be provided with evidence of message recipient and deliver.	Article 3 (36) "... provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data..."

Reference: Electronic Registered Delivery Service (ERDS) and the eIDAS Regulation, 12 September 2016

Control

Summary of security controls

(*) Not exhaustive and it is by no means a guarantee that the system will be granted qualified status under the eIDAS regulation.
For the process of granting the qualified status, please refer to the national supervisory body in the respective country.

Security control	Legal implications
CTR1 **Transport Layer Security (TLS)** TLS protocols ensure authenticity and integrity of the message, by applying host to host cryptographic mechanisms	European General Data Protection Regulation (GDPR), in case of applicability.
CTR2 **Message Encryption** Message encryption ensures confidentiality of the message payload so that only the correct recipient can access it	European General Data Protection Regulation (GDPR), in case of applicability.
CTR3: **Electronic Seal of message** From technical perspective, electronic seal ensures integrity of the message header and payload and authenticity of origin	**Non-qualified**: Ensures integrity and origin of the data, in other words its authentication **Qualified**: eIDAS Regulation, Article 35. "A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data" **Both**: Non-discrimination in legal proceedings
CTR4: **Electronic Seal of evidence** Provides evidence to the sender C1 that the message was sent, delivered to the final recipient C4 and authenticity of destination	
CTR5: **Electronic Timestamp** Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time	**Non-qualified:** Ensures date and time of the data. **Qualified:** eIDAS Regulation, Article 41. "A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound." **Both:** Non-discrimination in legal proceedings

Reference: Electronic Registered Delivery Service (ERDS) and the eIDAS Regulation, 12 September 2016

Mapping of CEF Requirements and CEF Controls

Requirements vs. Controls	CTR1 Transport Layer Security protocol (TLS)	CTR2 Message Encryption	CTR3 Electronic Seal of the message	CTR4 Electronic Seal of the evidence	CTR5 Electronic Time Stamp	CTR6 Electronic Signature of the message
REQ1: Message Integrity	✓		✓			O
REQ2: Message Confidentiality	✓	✓				
REQ3. Sender Identification	O (in case that TLS adds Client authentication)		✓			O
REQ4. Addressee Identification	✓					
REQ5. Time-Reference					✓	
REQ6. Proof of Send/Receive				✓		

✓ : Mandatory

O : Optional

ข้อกำหนดของบริการนำส่งข้อมูลอิเล็กทรอนิกส์

1. **การใช้ช่องทางการสื่อสารที่มีความปลอดภัย (protected channel)** TLS 1.2 หรือที่สูงกว่า
   เพื่อให้มีการรักษาความครบถ้วนและการรักษาความลับของข้อมูลระหว่างการนำส่ง
2. **การเข้ารหัสลับของข้อมูล (message encryption) (optional)**
   เพื่อให้ผู้รับข้อมูลปลายทางเท่านั้นที่สามารถเข้าถึงข้อมูลได้
3. **การระบุตัวผู้ส่งข้อมูลต้นทาง (sender identification)** one-way TLS | two-way TLS | C1 Digital Signature
   เพื่อตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ส่งข้อมูลต้นทาง
4. **การระบุตัวผู้รับข้อมูลปลายทาง (recipient identification)** one-way TLS | two-way TLS
   เพื่อตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้รับข้อมูลปลายทางก่อนการนำส่งข้อมูล
5. **การอ้างอิงเวลา (time reference)**
   เพื่อระบุวันเวลาที่ส่งข้อมูลและรับข้อมูล
6. **หลักฐานการส่งข้อมูลและการรับข้อมูล (proof of send and receive)**
   เพื่อให้ผู้ส่งข้อมูลต้นทางและผู้รับข้อมูลปลายทางมีหลักฐานของการส่งข้อมูลและการรับข้อมูล

การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

(1) ผู้ให้บริการต้อง**ดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ** (information security risk assessment) ของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ ดังนี้

- **การกำหนดเกณฑ์ความเสี่ยง** ซึ่งประกอบด้วย เกณฑ์การยอมรับความเสี่ยง (risk acceptance criteria) และเกณฑ์การประเมินความเสี่ยง (risk assessment criteria)
- **การระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ** (risk identification) ได้แก่ การใช้กระบวนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเพื่อระบุความเสี่ยงที่เกี่ยวกับการถูกเปิดเผยข้อมูล ความถูกต้องครบถ้วน และความพร้อมใช้งานของสารสนเทศภายในขอบเขตของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ รวมถึงการระบุผู้เป็นเจ้าของความเสี่ยง
- **การวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ** (risk analysis) โดยการประเมินผลกระทบและโอกาสที่อาจจะเกิดขึ้นจากความเสี่ยง รวมถึงการกำหนดระดับค่าความเสี่ยง
- **การเปรียบเทียบผลลัพธ์**จากการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยง และการจัดลำดับความเสี่ยงเพื่อการจัดการความเสี่ยง (risk treatment)

(2) ผู้ให้บริการต้องกำหนดแผนจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (information security risk treatment plan) และต้องเก็บรักษาเอกสารแสดงผลลัพธ์จากการจัดการความเสี่ยง

(3) ผู้ให้บริการต้องทบทวนการประเมินความเสี่ยงและการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของบริการนำส่งข้อมูลอิเล็กทรอนิกส์อย่างสม่ำเสมอ

มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ

มาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศของบริการนำส่งข้อมูลอิเล็กทรอนิกส์ **อ้างอิงมาตรการควบคุม (control) และแนวปฏิบัติ (guidance) จากมาตรฐาน ISO/IEC 27002:2022** ทั้งนี้ มาตรฐาน ISO/IEC 27002:2022 ประกอบด้วยมาตรการควบคุมจำนวน **93 ข้อ** ซึ่งแบ่งออกเป็น **4 ด้าน** ดังนี้

- มาตรการควบคุมด้านองค์กร (organizational controls)
- มาตรการควบคุมด้านบุคลากร (people controls)
- มาตรการควบคุมด้านกายภาพ (physical controls)
- มาตรการควบคุมด้านเทคโนโลยี (technological controls)

อย่างไรก็ตาม ข้อเสนอแนะมาตรฐานฉบับนี้ ได้**พิจารณามาตรการควบคุมทั้งหมดของ ISO/IEC 27002:2022 มาวิเคราะห์ตามบริบทและประเด็นที่เกี่ยวข้องกับบริการนำส่งข้อมูลอิเล็กทรอนิกส์** และแบ่งมาตรการควบคุมตามระดับความจำเป็นดังนี้

- มาตรการควบคุมที่จำเป็น (mandatory controls) จำนวน **50** ข้อ
- มาตรการควบคุมที่เป็นทางเลือก (optional controls) จำนวน **33** ข้อ
- มาตรการควบคุมที่เฉพาะกรณี (conditional controls) จำนวน **10** ข้อ

ทั้งนี้ เพื่อให้สอดคล้องตามข้อเสนอแนะมาตรฐานฉบับนี้ **ผู้ให้บริการต้องปฏิบัติตามมาตรการควบคุมที่จำเป็น (mandatory controls) ทุกข้อ** และ **ปฏิบัติตามมาตรการควบคุมที่เฉพาะกรณี (conditional controls) หากระบบของผู้ให้บริการเป็นไปตามเงื่อนไขที่ระบุไว้ในข้อนั้น ๆ** เช่น กรณีที่ให้หน่วยงานภายนอกทำหน้าที่ให้บริการแทน กรณีที่ใช้บริการคลาวด์ หรือกรณีที่หน่วยงานเป็นผู้พัฒนาระบบเอง

นอกจากนี้ **ผู้ให้บริการสามารถพิจารณาปฏิบัติตามมาตรการควบคุมที่เป็นทางเลือก (optional controls) เพิ่มเติม** เพื่อให้สอดคล้องกับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และหลักเกณฑ์ของหน่วยงานที่กำกับดูแลบริการนำส่งข้อมูลอิเล็กทรอนิกส์แต่ละประเภท

ตัวอย่างตารางของมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ

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