มาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับธุรกรรมภาษีทางอิเล็กทรอนิกส์

ว่าด้วยความมั่นคงปลอดภัยสารสนเทศ

RD ICT Standard for Electronic Tax Transactions

: Information Security

RD STD. [01-2566]

กรมสรรพากร

Version 01.00.0000

คำนำ

อ้างถึง กฎกระทรวงฉบับที่ 384 (พ.ศ. 2565) ออกตามความในประมวลรัษฎากรว่าด้วยการดำเนินการเกี่ยวกับเอกสารหลักฐานหรือหนังสือด้วยกระบวนการทางอิเล็กทรอนิกส์ หมวด 2 เอกสารหลักฐานหรือหนังสือที่ใช้ในการติดต่อกับกรมสรรพากร ข้อ 6 ผู้เสียภาษีอากรผู้ใดประสงค์จะยื่นหรือส่งเอกสารหลักฐานหรือหนังสือแก่กรมสรรพากรโดยการเชื่อมต่อระบบอิเล็กทรอนิกส์ของตนกับระบบอิเล็กทรอนิกส์ของกรมสรรพากร ให้ยื่นคำขออนุญาตเชื่อมระบบอิเล็กทรอนิกส์ต่ออธิบดี โดยผู้เสียภาษีอากรนั้นต้องมีระบบอิเล็กทรอนิกส์ที่มีลักษณะ ดังต่อไปนี้

(1) มีกระบวนการการพิสูจน์และยืนยันตัวตนของผู้เสียภาษีอากร ผู้ประกอบการจดทะเบียน ผู้มีหน้าที่ออกใบรับ หรือบุคคลใด ซึ่งติดต่อกับกรมสรรพากร โดยอย่างน้อยต้องมีมาตรฐานตามที่กำหนดในกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(2) มีวิธีการที่ทำให้สามารถระบุตัวเจ้าของลายมือชื่ออิเล็กทรอนิกส์ ประเภท ลักษณะ หรือรูปแบบลายมือชื่ออิเล็กทรอนิกส์ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์

(3) มีกระบวนการที่ทำให้เอกสารหลักฐานหรือหนังสือที่กรมสรรพากรได้รับอยู่ในรูปแบบที่เหมาะสม โดยสามารถแสดงหรืออ้างอิงเพื่อใช้ในภายหลัง และยังคงความครบถ้วนของข้อความในเอกสารหลักฐานหรือหนังสือนั้น

(4) มีความมั่นคงปลอดภัยด้านสารสนเทศตามประกาศอธิบดีกรมสรรพากร (ฉบับที่ 48) เรื่อง กำหนดมาตรฐานเกี่ยวกับรูปแบบ วิธีการส่ง การเก็บรักษา เอกสารหลักฐานหรือหนังสือ และความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับการดำเนินการที่เกี่ยวข้องกับกระบวนการทางอิเล็กทรอนิกส์ ได้กำหนดมาตรฐานเกี่ยวกับรูปแบบ วิธีการส่ง การเก็บรักษา เอกสารหลักฐานหรือหนังสือ และความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการดำเนินการที่เกี่ยวข้องกับกระบวนการทางอิเล็กทรอนิกส์ ดังต่อไปนี้

“ข้อ 1 ผู้เสียภาษีอากรหรือบุคคลใดที่ประสงค์จะยื่นคำขออนุญาตเชื่อมต่อระบบอิเล็กทรอนิกส์ของตนกับระบบอิเล็กทรอนิกส์ของกรมสรรพากร เพื่อยื่นหรือส่งเอกสารหลักฐานหรือหนังสือต้องเป็นผู้ได้รับอนุญาตให้ใช้บริการภาษีผ่านระบบอิเล็กทรอนิกส์ของกรมสรรพากร และต้องมีระบบความมั่นคงปลอดภัยด้านสารสนเทศตามที่ประกาศบนเว็บไซต์ของกรมสรรพากร”

เพื่อให้ผู้เสียภาษีอากรหรือบุคคลใดที่ประสงค์จะยื่นหรือส่งเอกสารหลักฐานหรือหนังสือแก่กรมสรรพากรโดยการเชื่อมต่อระบบอิเล็กทรอนิกส์ของตนกับระบบอิเล็กทรอนิกส์ของกรมสรรพากร ทราบถึงมาตรฐานของระบบความมั่นคงปลอดภัยด้านสารสนเทศ จึงได้จัดทำมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขั้นพื้นฐานที่จำเป็นสำหรับเกี่ยวกับ รูปแบบ วิธีการส่งเอกสารหลักฐานหรือหนังสืออิเล็กทรอนิกส์ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือ ได้รับให้ปรากฏอย่างถูกต้องได้ วิธีการที่เชื่อถือได้ในการเก็บรักษา

ความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์และสามารถแสดงข้อความนั้นในภายหลังได้ โดยสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง และข้อกำหนดด้านความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการดำเนินการที่เกี่ยวข้องกับกระบวนการทางอิเล็กทรอนิกส์

ทั้งนี้ มาตรฐานด้านความมั่นปลอดภัยสารสนเทศนี้ ได้มีการอ้างอิงตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ETDA Recommendation on ICT Standard for Electronic Transactions) ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์ ฉบับ ขมธอ. 21-2562 เวอร์ชัน 1.0 จากผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2022 (Annex A: Information Security Controls Reference) และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27002:2022 โดยมีข้อกำหนดตามจำนวน 93 ข้อ ครอบคลุมความมั่นคงปลอดภัยสารสนเทศทั้งหมด 4 ด้าน เพื่อนำขึ้นเผยแพร่บนเว็บไซต์ของกรมสรรพากร ดังนี้

1. ด้านองค์กร (Organizational Controls)
2. ด้านบุคลากร (People Controls)
3. ด้านกายภาพ (Physical Controls)
4. ด้านเทคโนโลยี (Technological Controls)

มาตรฐานฉบับนี้ได้ระบุข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขั้นพื้นฐานที่จำเป็นสำหรับหน่วยงานที่ทำหน้าที่นำส่งข้อมูลอิเล็กทรอนิกส์ ซึ่งได้พิจารณาถึงรูปแบบการรักษาความมั่นคงปลอดภัยที่เหมาะสมกับลักษณะการนำส่งข้อมูลอิเล็กทรอนิกส์ และการรักษาความมั่นคงปลอดภัยสารสนเทศโดยทั่วไป

ประวัติการปรับปรุงเอกสาร

Version	รายละเอียด	วันที่
01.00.0000	เวอร์ชันแรก	23 สิงหาคม 2566

สารบัญ

เรื่อง **หน้าที่**

สารบัญ (ต่อ)

เรื่อง **หน้าที่**

1. คำนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

1.1 ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ของกรมสรรพากร หมายถึง ผู้เสียภาษีอากร หรือหน่วยงานหรือองค์กร หรือบุคคลใด ที่ประสงค์จะยื่นหรือส่งเอกสารหลักฐานหรือหนังสือแก่กรมสรรพากร โดยการเชื่อมต่อระบบอิเล็กทรอนิกส์ของตนกับระบบอิเล็กทรอนิกส์ของกรมสรรพากร

1.2 ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

1.3 บุคลากรหลัก หมายถึง บุคคลที่มีบทบาทสำคัญเกี่ยวกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยที่อยู่ภายใต้ขอบเขตการยื่นหรือส่งเอกสารหลักฐานหรือหนังสือแก่กรมสรรพากรโดยการเชื่อมต่อระบบอิเล็กทรอนิกส์ของตนกับระบบอิเล็กทรอนิกส์ของกรมสรรพากร เช่น ผู้บริหารระดับสูง ผู้จัดการความต่อเนื่องทางธุรกิจ ผู้ดูแลระบบของระบบสารสนเทศที่สำคัญ หรือบุคคลที่สามที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศที่สำคัญ เป็นต้น

1.4 บุคลากรที่เกี่ยวข้อง หมายถึง บุคคลที่เกี่ยวกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยในองค์กรทุกคนและบุคคลที่สามที่อยู่ภายใต้ขอบเขตการยื่นหรือส่งเอกสารหลักฐานหรือหนังสือแก่กรมสรรพากรโดยการเชื่อมต่อระบบอิเล็กทรอนิกส์ของตนกับระบบอิเล็กทรอนิกส์ของกรมสรรพากร

2. ข้อกำหนดด้านความมั่นคงปลอดภัย (Security Requirements)

ข้อกำหนดด้านความมั่นคงปลอดภัยที่อยู่ภายใต้วัตถุประสงค์ด้านความมั่นคงปลอดภัยแต่ละวัตถุประสงค์ที่ผู้เชื่อมต่อบริการของกรมสรรพากร ควรนำมาปฏิบัติเพื่อให้บรรลุวัตถุประสงค์ที่กำหนดไว้ ซึ่งแต่ละข้อกำหนดมี ดังนี้

2.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Policies for Information Security)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ของกรมสรรพากร ควรมีนโยบายความมั่นคงปลอดภัยสารสนเทศและนโยบายเฉพาะเรื่องด้านความมั่นคงปลอดภัยซึ่งได้รับการอนุมัติโดยผู้บริหาร รวมถึงเผยแพร่และสื่อสารให้บุคลากรที่เกี่ยวข้องรับทราบ นอกจากนี้ ควรมีการทบทวนนโยบายความมั่นคงปลอดภัยด้านสารสนเทศตามระยะเวลาที่กำหนด หรือเมื่อมีการเปลี่ยนแปลงการดำเนินงานใด ๆ ภายในองค์กรเพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรให้สอดคล้องกับวัตถุประสงค์ กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง ซึ่งนโยบายความมั่นคงปลอดภัยด้านสารสนเทศต้องได้รับการอนุมัติก่อนนำไปใช้งาน พร้อมสร้างความตระหนักและเผยแพร่ให้มีการรับทราบนโยบายความมั่นคงปลอดภัยด้วยประกอบด้วยหัวข้อ ดังนี้

1) การบริหารจัดการบุคคลที่สาม
2) การเปลี่ยนแปลงบุคลากร
3) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
4) ความมั่นคงปลอดภัยของระบบสนับสนุนการดำเนินงาน
5) การควบคุมการเข้าถึง
6) การบริหารจัดการระบบเครือข่าย
7) การบริหารจัดการสินทรัพย์
8) การตรวจพบและการตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย
9) การเฝ้าติดตามและบันทึกเหตุการณ์
10) การทดสอบระบบ
11) การประเมินผลและการทดสอบความมั่นคงปลอดภัย
12) การปฏิบัติตามข้อกำหนด
13) การเข้ารหัสลับ
14) การบริหารจัดการข้อมูลที่จัดเก็บ
15) ความมั่นคงปลอดภัยของส่วนเชื่อมต่อบริการ
16) ความมั่นคงปลอดภัยของการพัฒนาซอฟต์แวร์
17) สร้างความตระหนักให้แก่บุคลากรหลักทราบถึงหน้าที่ความรับผิดชอบของตนเองและนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

3. การกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ของกรมสรรพากร ควรกำหนดบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศให้แก่บุคลากรที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัยขององค์กรและจัดสรรตามความเหมาะสมและความต้องการขององค์กร โดยจัดทำรายการหน้าที่ความรับผิดชอบของแต่ละหน้าที่ และข้อมูลการติดต่อให้กับบุคลากรที่ควรจัดทำรายชื่อบุคลากรที่เกี่ยวข้องที่ได้รับการแต่งตั้ง และอธิบายรายละเอียดเกี่ยวกับบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย เช่น ผู้บริหารระดับสูงด้านความมั่นคงปลอดภัย (Chief Information Security Officer : CISO) ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) ผู้จัดการความต่อเนื่องทางธุรกิจ สร้างความตระหนักถึงบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย และช่องทางการติดต่อบุคคล หรือหน่วยงานที่เกี่ยวกับด้านความมั่นคงปลอดภัยให้แก่บุคลากรที่เกี่ยวข้องทราบ ทบทวนบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอหรือเมื่อมีการเปลี่ยนแปลงใด ๆ ต่อการดำเนินงานภายในองค์กร

4. ความมั่นคงปลอดภัยสารสนเทศเกี่ยวกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationships)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ของกรมสรรพากร ควรมีการกำหนดกระบวนการและดำเนินการเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้ผลิตภัณฑ์หรือบริการของผู้ให้บริการภายนอก เพื่อให้เกิดความมั่นคงปลอดภัยในการทำสัญญากับบุคคลที่สาม เช่น การระบุข้อตกลงระดับการให้บริการ (Service-Level Agreement : SLA) การระบุข้อกำหนดด้านความมั่นคงปลอดภัยภายในสัญญา และการจัดทำสัญญาเมื่อจ้างงานกับบุคคลที่สาม เพื่อให้มั่นใจว่าการใช้บริการจากบุคคลที่สามและความเสี่ยงที่เหลือ (Residual Risks) จะไม่ส่งผลกระทบหรือส่งผลเสียต่อการให้บริการ โดยมีข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับการให้บริการระบุไว้ภายในข้อตกลงที่จัดทำขึ้นกับบุคคลที่สาม ซึ่งควรประกอบด้วยหัวข้อ ดังนี้

1) รายละเอียดของการให้บริการ
2) ข้อกำหนดด้านความมั่นคงปลอดภัย เช่น ระบบพิสูจน์ตัวตนที่นำมาใช้ในการปฏิบัติงาน การพัฒนาซอฟต์แวร์และขั้นตอนการปฏิบัติงานต่าง ๆ ของบริการที่มีให้แก่องค์กร
3) ข้อตกลงการไม่เปิดเผยข้อมูลหรือความลับขององค์กร (Non-Disclosure Agreement : NDA)
4) บทบาท และหน้าที่ความรับผิดชอบ
5) ข้อตกลงระดับการให้บริการ (Service-Level Agreement : SLA)
6) ช่องทางการติดต่อประสานงานและรายงานผลการดำเนินงาน
7) ข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

การกำหนดสิทธิไว้ในข้อตกลงกับบุคคลที่สาม เพื่อให้ผู้ตรวจสอบสามารถเข้าดำเนินการตรวจสอบในกรณีที่พบประเด็น หรือข้อสงสัยที่มีนัยสำคัญ มีการกำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการบำรุงรักษาอุปกรณ์การปฏิบัติงาน และความเป็นเจ้าของทรัพย์สินสารสนเทศที่ระบุในข้อตกลง เช่น การจัดหาอุปกรณ์สารสนเทศ การให้บริการด้านเทคโนโลยีสารสนเทศการมอบหมายงานขององค์กรให้บุคคลที่สามรับผิดชอบการให้คำแนะนำ หรือความช่วยเหลือในการปฏิบัติงาน (Help Desk) ศูนย์กลางการให้บริการข้อมูล (Call Center) การเชื่อมต่อระบบเครือข่ายเข้าด้วยกัน การใช้สิ่งอำนวยความสะดวกร่วมกัน (Shared Facilities) เป็นต้น

5. การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with Authorities)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ของกรมสรรพากร ควรจัดตั้งและรักษาช่องการติดต่อสื่อสารกับหน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อความถูกต้อง ตรวจสอบกฎหมาย ข้อกำหนดด้านกฎระเบียบและสัญญา หรือมีการออกคำสั่งด้านความปลอดภัยใหม่ โดยมีการจัดทำเอกสารแผนดำเนินการ

6. บัญชีของข้อมูลและทรัพย์สินอื่น ๆ ที่เกี่ยวข้อง (Inventory of Information and Other Associated Assets)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ของกรมสรรพากร ควรกำหนดให้มีการบริหารจัดการสินทรัพย์และการควบคุมการกำหนดค่าของระบบเครือข่ายและระบบสารสนเทศที่สำคัญ รวมถึงการระบุทรัพย์สินสารสนเทศและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินสารสนเทศที่เหมาะสม จัดทำบัญชีทรัพย์สินสารสนเทศที่สำคัญขององค์กร รวมถึงสินทรัพย์ที่สำคัญ เช่น บุคลากร (บุคลากรหลักและบุคลากรที่เกี่ยวข้อง) เป็นต้น ควรมีการดำเนินการ ดังนี้

6.1 การจัดทำเอกสารกำหนดค่าความมั่นคงปลอดภัยพื้นฐานของระบบเครือข่ายและระบบสารสนเทศ ที่มีคุณสมบัติอย่างน้อย ดังนี้

1) ขีดความสามารถสำคัญในการดำเนินงาน
2) ข้อจำกัดการใช้งาน
3) กำหนดค่าความมั่นคงปลอดภัยเริ่มต้น
4) พอร์ต โพรโทคอล และ/หรือบริการที่ได้รับการอนุญาต

6.2 การกำหนดนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการทรัพย์สินสารสนเทศ ประกอบด้วยหัวข้ออย่างน้อย ดังนี้

1) บทบาทหน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ
2) การกำหนดค่าความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ
3) การใช้งานทรัพย์สินสารสนเทศ ตัวอย่างเช่น การใช้งานจดหมายอิเล็กทรอนิกส์ อินเทอร์เน็ต เครื่องคอมพิวเตอร์ และอุปกรณ์พกพาอื่น ๆ เป็นต้น

6.3 ควรให้บุคลากรที่เกี่ยวข้องและผู้ใช้งานภายนอกที่มีสิทธิเข้าถึงระบบสารสนเทศขององค์กรได้รับทราบถึงข้อกำหนดการใช้งานทรัพย์สินสารสนเทศที่กำหนดไว้

6.4 ควรจัดทำรายการการควบคุมการกำหนดค่าความมั่นคงปลอดภัยของระบบเครือข่ายและระบบสารสนเทศที่สำคัญ

6.5 ควรระบุผู้รับผิดชอบของทรัพย์สินสารสนเทศแต่ละรายการในบัญชีทรัพย์สินสารสนเทศและความผูกพันระหว่างทรัพย์สินสารสนเทศ

6.6 ควรทบทวนนโยบายหรือขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการสินทรัพย์และการควบคุมการกำหนด ค่าความมั่นคงปลอดภัยอย่างสม่ำเสมอ โดยคำนึงถึงการเปลี่ยนแปลงใด ๆ ที่มีผลต่อการดำเนินงานขององค์กร

6.7 ควรจำแนกประเภททรัพย์สินสารสนเทศตามข้อกำหนดทางกฎหมาย มูลค่า ความสำคัญ และความอ่อนไหว ต่อการถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

7. การจำแนกข้อมูล (Classification of Information)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ของกรมสรรพากร ควรจำแนกข้อมูลตามความมั่นคงปลอดภัยสารสนเทศขององค์กรโดยเป็นไปตามข้อกำหนดเกี่ยวกับความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง เพื่อให้สารสนเทศได้รับการปกป้องที่เหมาะสม โดยสอดคล้องกับความสำคัญของสารสนเทศนั้น ๆ ที่มีต่อผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ โดยควรมีพิจารณาถึงการกำหนดชั้นความลับของสารสนเทศ อย่างน้อย ดังนี้

7.1 การจัดระดับชั้นความลับต้องพิจารณาถึงข้อกำหนดทางด้านกฎหมาย คุณค่าระดับความสำคัญ และระดับความอ่อนไหวเพื่อป้องกันมิให้ข้อมูลถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต โดยให้ปฏิบัติอย่างเหมาะสมตามระดับชั้นความลับของข้อมูล

7.2 การกำหนดประเภทของข้อมูล ระดับความสำคัญ ลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง และช่องทางการเข้าถึง เป็นลายลักษณ์อักษรและมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ

7.3 แนวทางการแบ่งประเภทของข้อมูล

1) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรอง ข้อมูลบุคลากร และข้อมูลงบประมาณการเงินและบัญชี

2) ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลบริการต่าง ๆ ข้อมูลสารสนเทศต่าง ๆ

7.4 แนวทางการจัดแบ่งระดับชั้นการเข้าถึง

1) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

2) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

3) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

4) ข้อมูลใช้ภายใน หมายถึง ข้อมูลที่ใช้เฉพาะภายในระบบของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ เท่านั้น

5) ข้อมูลสาธารณะ หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่แก่สาธารณะได้

7.5 จัดแบ่งระดับชั้นการเข้าถึง

1) การเข้าถึงและการใช้งานข้อมูลลับที่สุด บุคลากรที่เกี่ยวข้องที่เป็นเจ้าของข้อมูลข่าวสารเป็นผู้กำหนดสิทธิในการเข้าถึงและใช้งานข้อมูล โดยผ่านการอนุมัติเป็นลายลักษณ์อักษรจากบุคลากรหลัก และต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

2) การเข้าถึงและการใช้งานข้อมูลลับมาก บุคลากรที่เกี่ยวข้องที่เป็นเจ้าของข้อมูลข่าวสารเป็นผู้กำหนดสิทธิในการเข้าถึงและใช้งานข้อมูล โดยผ่านการอนุมัติจากบุคลากรหลักที่เป็นเจ้าของข้อมูล ต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรองการเข้าถึงและการใช้งานข้อมูลลับ บุคลากรที่เกี่ยวข้องที่เป็นเจ้าของข้อมูลข่าวสารเป็นผู้กำหนดสิทธิในการเข้าถึงและใช้งานข้อมูล และต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

3) การเข้าถึงและการใช้งานกลุ่มข้อมูลใช้ภายใน บุคลากรที่เกี่ยวข้องของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ สามารถเข้าถึงและใช้งานข้อมูลได้

4) การเข้าถึงและการใช้งานข้อมูลสาธารณะ บุคคลทั่วไป สามารถเข้าถึงและใช้งานข้อมูลได้

7.6 การบ่งชี้สารสนเทศ (Labeling of Information) ควรมีการจัดทำการบ่งชี้สารสนเทศ มีการสื่อสาร และปฏิบัติตามที่สอดคล้องกับขั้นตอนการปฏิบัติที่ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์กำหนดไว้ และให้เหมาะสมกับชั้นความลับที่กำหนดไว้

8. การถ่ายโอนสารสนเทศ (Information Transfer)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรมีการกำหนดกฎเกณฑ์ ขั้นตอนการปฏิบัติ หรือข้อตกลงในการถ่ายโอนสารสนเทศทุกประเภทภายในองค์กรของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ และระหว่างองค์กรของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ กับหน่วยงานภายนอก เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในระบบของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ และระหว่างระบบเครือข่ายภายในผู้เชื่อมต่อระบบอิเล็กทรอนิกส์กับระบบเครือข่ายภายนอก โดยประกอบไปด้วยเรื่องดังต่อไปนี้

8.1 การควบคุมการรับส่งข้อมูลสารสนเทศ (Information Transfer Control) เพื่อให้มีการควบคุมเพื่อป้องกันปัญหาของการรับส่งข้อมูลสารสนเทศภายในระบบของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ และระหว่างระบบของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ กับหน่วยงานภายนอก โดยผ่านช่องทางการสื่อสารทุกชนิดควรมีการควบคุม ดังนี้

1) ควรมีการควบคุมการรับส่งข้อมูลสารสนเทศให้สอดคล้องกับระดับความมั่นคงปลอดภัยของสารสนเทศ

2) ควรมีการป้องกันการดักจับข้อมูลที่รับส่ง การทำสำเนา การเปลี่ยนแปลงแก้ไข การส่งผิดเส้นทาง (Mis-Routing) และการถูกทำลาย

3) ควรมีการตรวจจับและป้องกันโปรแกรมที่ไม่ประสงค์ดี

4) ควรมีการป้องกันข้อมูลที่สำคัญในรูปสื่ออิเล็กทรอนิกส์ที่ส่งผ่านในรูปแบบของเอกสารแนบ และการควบคุมการส่งต่อ เช่น การส่งต่อจดหมายอิเล็กทรอนิกส์ภายในผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ไปจดหมายอิเล็กทรอนิกส์ภายนอกโดยอัตโนมัติ

5) ควรมีการควบคุมในช่องทางการสื่อสารแบบไร้สาย โดยจะต้องคำนึงถึงความเสี่ยงเฉพาะด้านที่เกี่ยวข้อง

6) ควรมีการกำกับดูแลหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของพนักงาน ลูกจ้าง หน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ และนักศึกษาฝึกงาน

7) ควรมีการควบคุมการใช้เทคนิคการเข้ารหัส เพื่อป้องกันสารสนเทศที่เป็นความลับและเพื่อให้สารสนเทศมีความถูกต้องและระบุตัวตนได้

8) ควรมีการเก็บรักษาและทำลายเอกสารเพื่อให้เป็นไปตามข้อกำหนดที่มีผลทางกฎหมาย

9) ควรมีการป้องกันอุปกรณ์ประมวลผลสารสนเทศที่ไม่มีผู้ดูแล

8.2 ข้อตกลงในการรับส่งข้อมูลสารสนเทศ (Transfer Agreement) เพื่อจัดทำข้อตกลงในการรับส่งข้อมูลสารสนเทศและซอฟต์แวร์ระหว่างองค์กรของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ กับหน่วยงานภายนอก อย่างเป็นลายลักษณ์อักษร โดยการรับส่งข้อมูลสารสนเทศและซอฟต์แวร์ขององค์กรของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ กับหน่วยงานภายนอก ต้องได้รับการอนุมัติจากบุคลากรหลัก และควรจัดให้มีการทำข้อตกลงหรือสัญญากับหน่วยงานภายนอกเมื่อมีการรับส่งข้อมูลสารสนเทศและซอฟต์แวร์ ควรพิจารณาข้อกำหนดหรือเงื่อนไขอย่างเหมาะสมและอย่างน้อยดังต่อไปนี้

1) การรักษาความลับของสารสนเทศและซอฟต์แวร์

2) ข้อตกลงในการฝากข้อมูล หรือ Source Code ไว้ที่หน่วยงานภายนอก ซึ่งไม่ใช่คู่สัญญาเพื่อให้ระบบของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ สามารถเข้าถึงข้อมูลดังกล่าวได้ในกรณีที่หน่วยงานคู่สัญญาหรือหน่วยงานที่ได้รับการว่าจ้างให้พัฒนาซอฟต์แวร์ไม่สามารถให้บริการได้ (Escrow Agreement)

3) การระบุถึงหน้าที่ความรับผิดชอบของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ และคู่สัญญาในการควบคุมสารสนเทศและซอฟต์แวร์ระหว่างการส่งผ่าน (Transmission) การกระจายต่อ (Dispatch) และการได้รับ (Receipt) สารสนเทศ

4) การระบุถึงความรับผิดชอบ และการใช้ เมื่อสารสนเทศสูญหาย ถูกแก้ไข หรือถูกเปิดเผยโดยมิชอบ

5) การระบุถึงกรรมสิทธิ์ การป้องกันสิทธิและทรัพย์สินทางปัญญาของสารสนเทศและซอฟต์แวร์

6) ข้อกำหนดข้อตกลงร่วมกันในการจัดทำป้ายชื่อ ตามระดับความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้มีความเข้าใจตรงกันและสามารถดำเนินการป้องกันได้อย่างเหมาะสม

7) มาตรฐานทางเทคนิคอื่น ๆ สำหรับรูปแบบของข้อมูล การจัดเก็บ การประมวลผล และการส่งสารสนเทศที่มีการรับส่งข้อมูล

8) ขั้นตอนปฏิบัติงานสำหรับการรับส่งข้อมูลสารสนเทศกระบวนการติดตาม (Traceability) และป้องกันการปฏิเสธความรับผิด (Non-Repudiation)

8.3 การรับส่งสื่อบันทึกข้อมูล (Physical Media in Transit) เพื่อป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยมิได้รับอนุญาต การใช้งานผิดวัตถุประสงค์และการทำให้ข้อมูลเกิดความเสียหาย ควรพิจารณาข้อกำหนดหรือเงื่อนไขอย่างเหมาะสมและอย่างน้อยดังต่อไปนี้

1) ต้องมีการใช้บริการผู้จัดส่งที่มีความน่าเชื่อถือ

2) กำหนดให้มีกระบวนการในการระบุตัวตนเพื่อให้สามารถติดตามเจ้าหน้าที่ผู้จัดส่งได้

3) มีการบรรจุหีบห่อสื่อบันทึกข้อมูลอย่างเหมาะสมและเป็นไปตามคำแนะนำของผู้ผลิต เพื่อป้องกันความเสียหายทางกายภาพ ที่อาจเกิดขึ้นในช่วงขนส่ง เช่น การถูกความร้อน ความชื้น หรือคลื่นแม่เหล็กไฟฟ้า เป็นต้น

4) มีการป้องกันการเปิดเผยหรือดัดแปลงสารสนเทศอย่างเหมาะสม เช่น การเปิดผนึกและลงนามกำกับ การใช้บรรจุภัณฑ์ที่สามารถล็อคได้ และการส่งมอบด้วยตนเอง เป็นต้น

5) บุคลากรหลักของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ต้องจัดให้มีกระบวนการรับส่งที่เหมาะสมเพื่อให้มั่นใจว่าผู้รับได้รับของถูกต้องครบถ้วน โดยพิจารณาตามระดับความมั่นคงปลอดภัยของสารสนเทศ

8.4 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information System) เพื่อป้องกันสารสนเทศที่มีการรับส่งข้อมูลระหว่างระบบ หรือ แอปพลิเคชันทางธุรกิจของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรพิจารณาข้อกำหนดหรือเงื่อนไขอย่างเหมาะสมและอย่างน้อยดังต่อไปนี้

1) ควรมีการควบคุมทางกายภาพ เพื่อป้องกันการเข้าถึงอุปกรณ์ที่ให้บริการข้อความทางอิเล็กทรอนิกส์โดยได้รับอนุญาต

2) ควรมีการบริหารจัดการการเข้าถึงของผู้ใช้อย่างเหมาะสม เพื่อควบคุมการเข้าถึงระบบเฉพาะผู้ที่ได้รับอนุญาต

3) ควรทำหลักเกณฑ์การใช้งานแอปพลิเคชันทางธุรกิจ และทำการสื่อสารให้บุคลากรที่เกี่ยวข้องทราบ เรื่องการรับส่งข้อมูลสารสนเทศระหว่างแอปพลิเคชัน

4) ควรจัดให้มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งาน และมีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอ

5) ควรมีการปฏิบัติตามข้อกำหนดที่มีผลทางกฎหมาย เช่น การสำรองข้อมูล การควบคุมการเปลี่ยนแปลง และการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ เป็นต้น

6) ต้องมีการเข้ารหัสเพื่อรักษาความลับของข้อมูล ตามระดับความมั่นคงปลอดภัยของสารสนเทศ

7) ต้องจัดให้มีการยืนยันและพิสูจน์ตัวตนของแหล่งที่มาของสารสนเทศและพิสูจน์ความถูกต้องครบถ้วนของสารสนเทศที่ส่งระหว่างแอปพลิเคชัน ตามระดับความมั่นคงปลอดภัยของสารสนเทศ

9. การควบคุมการเข้าถึง (Access Control)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรมีการกำหนดกฎเกณฑ์การเข้าถึงข้อมูลและทรัพย์สินอื่น ๆ ทางกายภาพ (Physical Access) และการเข้าถึงเชิงตรรกะ (Logical Access) โดยคำนึงถึงข้อกำหนดทางธุรกิจและด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อกำหนดนโยบายและข้อกำหนดสำหรับการเข้าถึงแหล่งข้อมูลขององค์กรของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ เช่น ระบบเครือข่าย ระบบบริหารจัดการชื่อผู้ใช้ ระบบการตรวจสอบผู้ใช้งาน ระบบควบคุมการเข้าถึง รวมถึงมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบเครือข่าย มาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร การป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก เพื่อทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ได้อย่างถูกต้อง โดยมีการระบุข้อมูลผู้ใช้งานที่แตกต่างกัน (Unique Identifier) และตรวจสอบสิทธิก่อนเข้าใช้งานระบบสารสนเทศหรือบริการ ดังนี้

9.1 ควรมีขั้นตอนการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ เมื่อมีผู้ขอใช้งานระบบสารสนเทศขององค์กร

9.2 ควรกำหนดบัญชีผู้ใช้งานที่ไม่ซ้ำกัน เพื่อเป็นการระบุตัวตนและเชื่อมโยงไปถึงความรับผิดชอบต่อการกระทำของตนได้

9.3 ควรกำหนดให้มีการเพิกถอนบัญชีผู้ใช้งานทันทีเมื่อผู้ใช้งานนั้นพ้นสภาพการเป็นพนักงาน หรือ เปลี่ยนตำแหน่งงาน

9.4 ควรทบทวนบัญชีผู้ใช้งานเป็นประจำ เพื่อลบหรือปิดการใช้งานบัญชีผู้ใช้ที่มีความซ้ำซ้อน ผู้ให้บริการต้องกำหนดกลไกควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ เพื่ออนุญาตให้เฉพาะผู้ใช้งานที่ได้รับสิทธิแล้วเท่านั้น ดังนี้

9.5 ควรกำหนดวิธีการหรือกลไกสำหรับการควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศประกอบด้วย

1) ผู้ใช้งานควรดูแลรักษาอุปกรณ์สารสนเทศที่อยู่ภายใต้ความรับผิดชอบในระหว่างที่ไม่มีการใช้งาน

2) ไม่มีการแสดงตัวหรือระบุชื่อระบบสารสนเทศจนกว่าจะเข้าสู่ระบบได้สำเร็จ

3) แสดงคำเตือนให้ทราบว่าคอมพิวเตอร์ควรเข้าถึงได้เฉพาะผู้มีอำนาจเท่านั้น

4) ไม่ควรแสดงข้อความหรือวิธีการช่วยเหลือใด ๆ ขณะอยู่ในขั้นตอนการเข้าสู่ระบบ

5) มีการตรวจสอบข้อมูลการเข้าสู่ระบบ และหากเกิดความผิดพลาดขณะเข้าสู่ระบบไม่ควรมีข้อความแสดงว่าความผิดพลาดนั้นเกิดขึ้นจากที่ใด

6) กำหนดจำนวนครั้งของความผิดพลาดในขั้นตอนการเข้าสู่ระบบ เช่น กรอกรหัสผิดพลาดได้ไม่เกินสามครั้ง เป็นต้น

7) ไม่แสดงรหัสผ่านที่ป้อนระหว่างขั้นตอนการเข้าสู่ระบบ

8) จำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่สำคัญ

9) ยุติการใช้งานระบบหากไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนดไว้

10) จำกัดจำนวนผู้ใช้งานที่สามารถเข้าถึงระบบเครือข่ายได้จากภายนอก

11) กำหนดคุณสมบัติของรหัสผ่านให้มีความซับซ้อนยากต่อการคาดเดา

9.6 มีการจัดทำนโยบายควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ ประกอบด้วย

1) การกำหนดกฎเกณฑ์ข้อกำหนดที่เกี่ยวข้องและข้อปฏิบัติที่ผู้ใช้งานต้องปฏิบัติตาม

2) การกำหนดมาตรการในการควบคุมการเข้าถึงระบบเครือข่าย และระบบสารสนเทศและระบบปฏิบัติการ

3) การควบคุมการเข้าถึงให้เหมาะสมกับชั้นความลับและความสำคัญต่อข้อมูลในระบบ

4) การแบ่งแยกระบบเครือข่าย

5) การควบคุมการเข้าถึงทรัพย์สินสารสนเทศที่สำคัญให้มีความมั่นคงปลอดภัย และหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏอยู่ขณะที่ไม่ใช้งาน (Clear Desk and Clear Screen)

6) การอนุมัติการเข้าถึงระบบเครือข่าย และระบบสารสนเทศตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน

7) การจำกัดการเข้าถึงโปรแกรมอรรถประโยชน์ (Utility Program)

8) การทบทวน หรือเพิกถอนสิทธิการเข้าถึงระบบเครือข่ายและระบบสารสนเทศ

9) การกำหนดประเภทของการเชื่อมต่อเพื่อเข้าสู่ระบบเครือข่าย และระบบสารสนเทศ เช่น การเชื่อมต่อจากระยะไกล การเชื่อมต่อผ่านระบบเครือข่ายไร้สาย เป็นต้น

10) การกำหนดให้บุคคลที่สามตระหนัก เข้าใจ และปฏิบัติตามนโยบายควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศขององค์กร

11) การจัดเก็บบันทึกข้อมูลการเข้าถึงของผู้ใช้งาน

12) การเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลของผู้ใช้งานต้องเลือกกลไกสำหรับตรวจสอบและการยืนยันตัวตนของผู้ใช้งานจากผลของการวิเคราะห์ความเสี่ยง โดยกำหนดกลไกยืนยันตัวตนผู้ใช้งานที่แตกต่างกัน เช่น วิธีการยืนยันตัวตนแบบปัจจัยเดียว (Single-Sign-On) วิธีการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) และการยืนตัวตนจากระยะไกล (Teleworking Authentication)

9.7 ติดตามตรวจสอบการเข้าถึงระบบเครือข่าย และระบบสารสนเทศโดยกำหนดกระบวนการอนุมัติและลงทะเบียน เพื่อป้องกัน การละเมิดการเข้าถึงและเข้าใช้งานโดยไม่ได้รับอนุญาต ดังนี้

1) ควรเก็บบันทึกข้อมูลขณะเข้าสู่ระบบได้สำเร็จ หรือไม่สำเร็จ

2) ควรกำหนดให้ผู้ใช้งานสามารถเข้าถึงได้เฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

3) ควรจัดทำรายชื่อของผู้ที่มีสิทธิเข้าถึงระบบเครือข่ายและระบบสารสนเทศ

4) ควรบันทึกข้อมูลการใช้งานสิทธิระดับสูง

9.8 จำกัดจำนวนผู้ใช้งานที่เข้าถึงฟังก์ชันด้านความมั่นคงปลอดภัยให้กับผู้ที่มีความจำเป็นเพื่อให้มีความมั่นคงปลอดภัยของระบบข้อมูล ดังนี้

1) ควรจัดทำรายชื่อของผู้ใช้ที่มีสิทธิเข้าถึงฟังก์ชันด้านความมั่นคงปลอดภัยของระบบเครือข่าย และระบบสารสนเทศ

2) ควรแบ่งเมนูการใช้งานเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชันต่าง ๆ ของระบบเครือข่าย และระบบสารสนเทศ

3) ควรควบคุมสิทธิของผู้ใช้ เช่น สิทธิในการ อ่าน เขียนและลบข้อมูล เป็นต้น

9.9 มีกระบวนการตรวจสอบการใช้งานสิทธิระดับสูง (Privileged Account) โดยพิจารณาตั้งแต่กระบวนการสร้างบัญชีผู้ใช้งานการรับรองสิทธิผู้ใช้งาน และการทบทวนสิทธิผู้ใช้งาน ดังนี้

1) ควรติดตามตรวจสอบการใช้งานสิทธิระดับสูงอย่างสม่ำเสมอ เช่น ดูจากการบันทึกเหตุการณ์การเข้าใช้งานระบบเครือข่าย และระบบสารสนเทศ

2) ควรเพิ่มความถี่สำหรับตรวจสอบสิทธิของบุคลากรที่มีสิทธิระดับสูงให้มากกว่าสิทธิของผู้ใช้งานทั่วไป

9.10 แบ่งแยกระบบเครือข่าย และระบบสารสนเทศตามข้อกำหนดด้านความมั่นคงปลอดภัยด้านสารสนเทศ

1) ควรแบ่งแยกระบบเครือข่ายเพื่อให้จำกัดผลกระทบจากการโจมตีของโปรแกรมไม่พึงประสงค์ (Malware)

2) ควรแบ่งแยกระบบเครือข่ายออกเป็นระบบเครือข่ายภายในและระบบเครือข่ายภายนอก

3) ควรมีข้อกำหนด เพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศของระบบเครือข่าย เช่น ติดตั้งอุปกรณ์ไฟร์วอลล์ เพื่อป้องกันการบุกรุกหรือเข้าถึงโดยไม่ได้รับอนุญาต

4) ควรมีข้อมูลแสดงความสัมพันธ์ของการแบ่งแยกหน้าที่ (Segregation of duties Control Matrix)

10. การบริหารจัดการข้อมูลอัตลักษณ์ สิทธิการเข้าถึง และข้อมูลการยืนยันตัวตน (Identity and Access Management)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรมีการจัดการข้อมูลเกี่ยวกับอัตลักษณ์ทั้งวงจร โดยมีการระบุข้อมูลที่แตกต่างกัน (Unique Identifier) เพื่อใช้ในการระบุตัวตนผู้ใช้งานได้ เช่น กำหนดเลขที่หรือรหัสประจำตัว หรือชื่อผู้ใช้บริการ (ภาษาอังกฤษ) หรือชื่ออื่น ๆ ที่ระบบรองรับได้ และสามารถสื่อความหมายถึงข้อมูลผู้ใช้งานได้อย่างชัดเจน โดยมีการควบคุมกระบวนการการจัดการและการจัดสรรข้อมูลการยืนยันตัวตน และให้คำแนะนำแก่บุคลากรในการจัดการข้อมูลการยืนยันตัวตน และจัดเตรียม ทบทวน แก้ไข หรือลบสิทธิการเข้าถึงข้อมูลและสินทรัพย์ที่เกี่ยวข้องอื่น ๆ ตามนโยบายเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศและกฎระเบียบขององค์กร

11. การวางแผนเตรียมการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management Planning and Response)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรมีการวางแผนและเตรียมการสำหรับการจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีการกำหนดกระบวนการจัดการ บทบาท และหน้าที่ความรับผิดชอบของบุคลากร และการสื่อสารกระบวนการจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมทั้งควรมีการประเมินสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและตัดสินใจว่าเหตุการณ์นั้นจัดเป็นสถานการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่ โดยการจัดแยกกลุ่มเหตุการณ์ หรือจุดอ่อนด้านความมั่นคงปลอดภัยและจัดลำดับความสำคัญ และควรมีกลไกการตอบสนองและจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ควรมีการดำเนินการ ดังนี้

11.1 การเตรียมการเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Response Planning)

1) การวางแผนการรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ควรมีการดำเนินการ ดังนี้

- ควรจัดทำแผน มาตรฐาน และระเบียบวิธีปฏิบัติในการรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ซึ่งรวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital (Digital Forensics) ไว้อย่างชัดเจน

- ควรมีการจัดทำแผนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) สำหรับภัยไซเบอร์สำคัญที่ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์มีโอกาสเผชิญ โดยการจัดทำแผนมีการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบ เพื่อให้สามารถใช้อ้างอิงในการรับมือภัยคุกคาม ตอบสนองต่อเหตุการณ์ และกู้คืนระบบและข้อมูลได้อย่างรวดเร็วและทันการณ์

- ควรมีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) ที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์และเชื่อมโยงกับแผนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยการจัดทำอย่างน้อยครอบคลุมกระบวนการ ดังนี้ การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) การประเมินความเสี่ยง (Risk Analysis) การวางกลยุทธ์สำหรับแผนฉุกเฉิน การจัดทำแผนฉุกเฉิน การสื่อสารและฝึกอบรมให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอก การทดสอบ ปรับปรุง และสอบทานแผนฉุกเฉิน เป็นต้น

- ควรจัดทำแผนฉุกเฉินดังกล่าวให้อ้างอิงตามแนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Implementation Guideline)

- ควรมีแผนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) สอดคล้องและเชื่อมโยงกับแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Disaster Recovery Plan : IT DRP) และแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP)

- ควรปรับปรุงแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ แผน IT DRP และแผน BCP

- ควรทบทวนแผนฉุกเฉินที่รองรับภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยคำนึงถึงเหตุการณ์ความเสียหายครอบคลุมสถานการณ์จำลองต่าง ๆ ที่อาจเกิดขึ้น รวมถึงเหตุการณ์จากภัยไซเบอร์ที่อาจส่งผลกระทบรุนแรง อย่างน้อยครอบคลุมเหตุการณ์ ดังนี้ ระบบงานสำคัญที่ศูนย์คอมพิวเตอร์หลัก และศูนย์สำรองไม่สามารถใช้งานได้พร้อมกัน หรือ ข้อมูลจริงและข้อมูลชุดสำรองไม่สามารถใช้งานได้

- การเปลี่ยนแปลงกระบวนการทำงาน ระบบงาน หรือสิทธิผู้ใช้งาน ที่เกี่ยวข้องกับการจัดการเหตุการณ์ผิดปกติทางไซเบอร์ต้องได้รับการอนุมัติก่อนนำไปใช้ปฏิบัติงานจริง

- ควรประเมินประสิทธิภาพ ความพร้อมและศักยภาพของเครื่องมือ บุคลากร และบริการของบุคคลภายนอก ผู้เชี่ยวชาญ หรือ ที่ปรึกษา (Due Diligence) อย่างสม่ำเสมอ เพื่อให้มั่นใจในความพร้อมของการให้บริการเมื่อมีเหตุการณ์ผิดปกติทางไซเบอร์เกิดขึ้น

2) การทดสอบความพร้อมรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ควรมีการดำเนินการ ดังนี้

- ควรทดสอบความสามารถในการกู้คืนข้อมูลจากชุดข้อมูลสำรอง และความถูกต้องของการประมวลผลระบบงานและข้อมูลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าข้อมูลสำรองมีความครบถ้วนถูกต้องสามารถนำมาใช้งานได้เมื่อมีเหตุการณ์ผิดปกติทางไซเบอร์เกิดขึ้นจริง
- ควรมีการทดสอบแผนในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) ที่ครอบคลุมระบบงานด้านเทคโนโลยีสารสนเทศที่สำคัญของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์
- ควรจัดให้มีการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT DRP) ที่ครอบคลุมภัยคุกคามทางไซเบอร์ และระบบงานสำคัญ ระบบที่เชื่อมต่อกับบุคคลภายนอกที่เกี่ยวข้องโดยเฉพาะระบบงานหรือข้อมูลที่มีผลกระทบต่อการให้บริการหรือต่อระบบของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ นอกจากนี้ มีการทดสอบระบบสำรองในลักษณะเสมือนจริง (DR live test) เพื่อให้มั่นใจว่าระบบสำรองสามารถรองรับธุรกิจให้สามารถดำเนินได้อย่างต่อเนื่อง
- ควรทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีโอกาสเกิดขึ้นโดยให้ครอบคลุมตามสถานการณ์จำลอง (Scenario) ที่สะท้อนภัยคุกคามทางไซเบอร์รูปแบบใหม่ ๆ ที่มีโอกาสเกิดขึ้น โดยมีการทดสอบในรูปแบบต่าง ๆ เช่น ลักษณะ Table Top หรือการจำลองการโจมตีทางไซเบอร์ (Cyber War Game/Cyber Simulation) เป็นต้น
- ควรรายงานผลการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT DRP) และ แผนในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan) มาทบทวนและปรับปรุงกระบวนการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ที่เกี่ยวข้องทั้งหมดให้มีประสิทธิภาพยิ่งขึ้น
- ควรทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ ครอบคลุม ธุรกรรมสำคัญและเชื่อมโยงไปยังธุรกิจหรือองค์กรที่เกี่ยวข้อง
- ควรทดสอบการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response) ที่ซับซ้อนซึ่งเคยเกิดขึ้นกับองค์กรอื่น เพื่อให้มั่นใจในความพร้อมในการรองรับสถานการณ์ในลักษณะเดียวกัน
- ควรจัดให้มีกระบวนการหาสาเหตุที่แท้จริง (Root Cause) ของปัญหาที่พบในระหว่างการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) การทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT DRP) ที่ครอบคลุมเหตุการณ์ภัยคุกคามทางไซเบอร์ เพื่อใช้ประโยชน์ในการแก้ไขปัญหาในภายหลัง

- ควรมีการทดสอบศักยภาพ (Stress Test) ในการบริหารจัดการความเสี่ยงด้านไซเบอร์ โดยใช้สถานการณ์จำลองเหตุการณ์ผิดปกติทางไซเบอร์ที่ส่งผลกระทบต่อการให้บริการของระบบหรือก่อให้เกิดความเสียหายอย่างมีนัยสำคัญ

- ควรมีการทดสอบแผนฉุกเฉินให้ครอบคลุมการย้ายศูนย์หลัก การเปลี่ยนแปลงกระบวนการทำงาน การเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ อันเนื่องมาจากเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยไม่ก่อให้เกิดการหยุดชะงักหรือกระทบต่อความสามารถในการให้บริการ และไม่ก่อให้เกิดความเสียหายต่อข้อมูล

3) บทบาทหน้าที่การรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Incident Response Function)

11.2 การบริหารจัดการเหตุการณ์ผิดปกติ

1) กระบวนการบริหารจัดการเหตุการณ์ผิดปกติ ควรมีการดำเนินการ ดังนี้

- จัดให้มีรายชื่อหน่วยงานภายนอกพร้อมช่องทางการติดต่อที่เป็นปัจจุบัน เพื่อใช้ติดต่อกรณีเกิดเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์หรือเมื่อมีความจำเป็น เพื่อทำให้สามารถแก้ไขสถานการณ์ได้อย่างทันการณ์

- จัดให้มีกระบวนการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ได้รับผลกระทบจากเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์ซึ่งครอบคลุมการจำกัดการเข้าถึง การยกเลิกใช้งาน การทำลาย หรือทดแทน รวมถึงการตั้งค่าใหม่และการทดสอบ ก่อนนำกลับมาใช้งาน

- มีกระบวนการในการตัดสินใจใช้แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดกับหน่วยงานภายนอกที่เกี่ยวข้อง

- มีการวิเคราะห์เหตุการณ์ผิดปกติทางด้านความมั่นคงปลอดภัยตั้งแต่ช่วงแรกเมื่อตรวจพบเหตุการณ์บุกรุก เพื่อตอบสนองและลดผลกระทบต่อเหตุการณ์ดังกล่าวที่อาจเกิดขึ้นได้อย่างทันการณ์

11.3 การส่งต่อและการรายงานข้อมูลเหตุการณ์ (Escalation and Reporting)

1) การส่งต่อและการสื่อสารข้อมูลเหตุการณ์ ควรมีการดำเนินการ ดังนี้

- มีการกำหนดช่องทางและวิธีการการสื่อสารและการส่งต่อข้อมูลเหตุการณ์ทางไซเบอร์ไปยังผู้ที่เกี่ยวข้อง เพื่อให้พนักงานสามารถรายงานข้อมูลเหตุการณ์ทางไซเบอร์ได้อย่างทันการณ์

- มีระเบียบวิธีปฏิบัติในการแจ้งหน่วยงานที่เกี่ยวข้องทราบ เมื่อเกิดเหตุการณ์ผิดปกติทางไซเบอร์ เช่น มีการเข้าถึงหรือใช้ข้อมูลระหว่างหน่วยงานจากผู้ไม่ประสงค์ดี เป็นต้น

- มีการกำหนดเงื่อนไขการรายงานเหตุการณ์ผิดปกติทางไซเบอร์หรือช่องโหว่ของระบบที่ตรวจพบตามระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

- มีแผนสื่อสารเหตุการณ์ผิดปกติทางไซเบอร์ไปยังองค์กรหรือหน่วยงานภายนอกที่เกี่ยวข้องหรือที่ได้รับผลกระทบ

- มีแผนสื่อสารเหตุการณ์ผิดปกติทางไซเบอร์ไปยังสื่อมวลชนตามความจำเป็นและเหมาะสม

2) การรายงานเหตุการณ์ผิดปกติ ควรมีการดำเนินการ ดังนี้

- มีการจัดประเภทของเหตุการณ์ บันทึก ติดตามและรายงานเหตุการณ์ผิดปกติทางไซเบอร์ที่เกิดขึ้น

- มีกระบวนการส่งข้อมูลเหตุการณ์ต่อผู้รับผิดชอบในการวิเคราะห์ รับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Escalation Process)

- มีการจัดทำรายงานสรุปเหตุการณ์ผิดปกติ ภัยคุกคาม หรือเหตุละเมิด (Violations) ทางไซเบอร์ที่เกิดขึ้น

12. การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from Information Security Incidents)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรนำความรู้ที่ได้รับจากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ เพื่อใช้ในการเสริมสร้างความแข็งแกร่งและปรับปรุงข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

1) ผู้ดูแลระบบต้องบันทึกเหตุละเมิดด้านความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไขจากเหตุการณ์ที่เกิดขึ้น เพื่อเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

2) ต้องมีการทบทวนเหตุละเมิดความมั่นคงปลอดภัย เพื่อป้องกันการเกิดปัญหาเดิมซ้ำ

3) ต้องมีการจัดทำรายการเฝ้าระวังล่วงหน้าจากเหตุละเมิดความมั่นคง เพื่อป้องกันการเกิดปัญหาเดิมซ้ำ

4) ต้องมีการวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก หรือ ละเมิด หรือระบาดที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

13. การเก็บรวบรวมหลักฐานและบันทึกเหตุการณ์
(Collection of Evidence and Logging)

13.1 ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรกำหนดขั้นตอนและดำเนินการตามขั้นตอนในการระบุ การรวบรวม การได้มา และการเก็บรักษาหลักฐานที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ โดยมีการดำเนินการ อย่างน้อย ดังนี้

1) ผู้ดูแลระบบต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่า ได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูลผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ และกฎหมายที่เกี่ยวข้อง

2) ส่วนกฎหมายและผู้ดูแลระบบสารสนเทศที่สำคัญ ต้องศึกษากฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง

13.2 ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรกำหนดขั้นตอนการเฝ้าติดตามและการบันทึกเหตุการณ์ของการเชื่อมต่อระบบอิเล็กทรอนิกส์ เพื่อให้สามารถตรวจสอบปัญหาหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น

1) มีการบันทึกเหตุการณ์ที่เกี่ยวข้องกับข้อมูลผู้เชื่อมต่อ ตัวอย่างเช่น รหัสผู้ใช้งาน กิจกรรมของผู้ใช้วันที่และเวลาของเหตุการณ์ การเข้าถึงระบบสารสนเทศที่สำเร็จและไม่สำเร็จ การเข้าถึงไฟล์และชนิดของการเข้าถึง การเปลี่ยนแปลงการกำหนดค่าของระบบสารสนเทศ การบุกรุก ที่อยู่เครือข่ายและโพรโทคอล เป็นต้น

2) มีรายงานการบันทึกเหตุการณ์และรายงานการเฝ้าติดตามข้อมูลที่เกี่ยวข้องให้กับผู้ใช้บริการเมื่อมีเหตุจำเป็นหรือเหตุสงสัย

3) มีการป้องกันการเปลี่ยนแปลงข้อมูลบันทึกเหตุการณ์ทั้งหมดและบันทึกการดำเนินงานที่ไม่ได้รับอนุญาต เช่น การปรับเปลี่ยนประเภทของข้อความที่บันทึกไว้ ข้อมูลการบันทึกเหตุการณ์ถูกแก้ไขหรือลบ เป็นต้น

14. ความพร้อมใช้งานของระบบสารสนเทศเพื่อความต่อเนื่องทางธุรกิจ
(ICT Readiness for Business Continuity)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรมีการวางแผน ดำเนินการ บำรุงรักษา และทดสอบความพร้อมใช้งานของระบบสารเทศที่เป็นไปตามวัตถุประสงค์และข้อกำหนดของความพร้อมใช้งานระบบสารสนเทศเพื่อความต่อเนื่องทางธุรกิจ สำหรับรองรับการหยุดชะงักของกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือภัยพิบัติที่เกิดขึ้นเพื่อให้การบริการดำเนินงานได้อย่างต่อเนื่อง

14.1 ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรวางแผนการรักษาความมั่นคงปลอดภัยสารสนเทศให้มีระดับที่เหมาะสมในระหว่างการหยุดชะงัก

14.2 การจัดทำแผนความต่อเนื่องทางธุรกิจสำหรับระบบสารสนเทศที่ให้บริการเพื่อรองรับภัยคุกคามต่าง ๆ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว การชุมนุมทางการเมือง การโจมตีทางไซเบอร์ เป็นต้น ประกอบด้วยประเด็นสำคัญ ดังนี้

1) บทบาทหน้าที่ความรับผิดชอบ

2) กระบวนการประกาศใช้แผน

3) รายละเอียดการจัดการจากเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น

4) ขั้นตอนการกู้คืนกิจกรรมที่มีการจัดลำดับความสำคัญตามระยะเวลาที่กำหนดไว้

5) รายละเอียดเกี่ยวกับการตอบสนองต่อเหตุกรณ์ เช่น วิธีการสื่อสารวิธีการแจ้งผู้ใช้บริการ ผู้แจ้ง เป็นต้น

6) กระบวนการกลับสู่ภาวะปกติหลังจากเหตุการณ์สิ้นสุด

14.3 แผนความต่อเนื่องทางธุรกิจ ต้องได้รับการอนุมัติจากผู้บริหารหรือผู้มีอำนาจที่เกี่ยวข้อง

14.4 ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรตรวจสอบว่า

1) มีการบริหารจัดการที่เพียงพอ เพื่อเตรียมพร้อมสำหรับการบรรเทาและตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยโดยใช้บุคลากรที่มีประสบการณ์ และความสามารถที่เกี่ยวข้อง

2) มีบุคลากรตอบสนองต่อเหตุการณ์ที่มีหน้าที่รับผิดชอบและความสามารถในการจัดการเหตุการณ์ที่เกิดขึ้น

3) มีการทบทวน และประเมินแผนความต่อเนื่องทางธุรกิจที่ได้เตรียมไว้ตามระยะเวลาที่กำหนด เพื่อให้มั่นใจว่าแผนนั้นยังถูกต้องและได้ผลเมื่อมีเหตุฉุกเฉินเกิดขึ้น

4) มีการจัดทำแผนการทดสอบเพื่อทดสอบ หรือซักซ้อมความพร้อมในการกู้คืนกระบวนการทางธุรกิจที่สำคัญแผนการทดสอบควรระบุถึงวัตถุประสงค์และเป้าหมายในการทดสอบกำหนดการในการทดสอบสถานการณ์ที่จะใช้ในการทดสอบ เป็นต้น

5) มีการกำหนดรูปแบบในการทดสอบหรือซักซ้อมให้สอดคล้องกับสถานการณ์ รวมถึงพิจารณาความเพียงพอของทรัพยากรที่มีอยู่ เช่น การฝึกซ้อมแผนบนโต๊ะ (table top exercise) การทดสอบแบบจำลองสถานการณ์หรือการทดสอบแบบเต็มรูปแบบ ซึ่งจะดำเนินการใกล้เคียงกับสถานการณ์จริงกับองค์ประกอบทั้งหมดของแผนความต่อเนื่องทางธุรกิจ เป็นต้น

6) มีการบันทึกผลการทดสอบเพื่อใช้ในการประเมินและปรับปรุงแผนความต่อเนื่องทางธุรกิจให้ดียิ่งขึ้น

14.5 ผู้ให้บริการต้องติดตามผลเมื่อประกาศใช้แผนและดำเนินการตามแผนความต่อเนื่องทางธุรกิจรวมถึงการบันทึกระยะเวลาการกู้คืนที่ดำเนินการสำเร็จและไม่สำเร็จ

1) มีกระบวนการตัดสินใจสำหรับการประกาศใช้แผนความต่อเนื่องทางธุรกิจ

2) มีการบันทึกการประกาศใช้แผนและการดำเนินการตามแผนความต่อเนื่องทางธุรกิจ รวมทั้งการดำเนินการตามขั้นตอนการกู้คืนและเวลาสิ้นสุดของการกู้คืนการให้บริการ

15. การป้องกันข้อมูล (Protection of Records)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรป้องกันบันทึกจากการสูญหาย การถูกทำลาย การปลอมแปลง และการเข้าถึงหรือเผยแพร่โดยไม่ได้รับอนุญาต โดยอาจมีการป้องกันบันทึกจากการสูญหาย การถูกทำลาย การปลอมแปลง และการเข้าถึงหรือเผยแพร่โดยไม่ได้รับอนุญาต โดยการรักษาความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of PII) ควรระบุและปฏิบัติตามข้อกำหนดเกี่ยวกับการรักษาความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคลที่เป็นไปตามกฎหมาย ระเบียบข้อบังคับ และข้อกำหนดในสัญญา ซึ่งควรมีการตรวจสอบอย่างอิสระในด้านความมั่นคงปลอดภัยสารสนเทศ เช่น ตรวจสอบการจัดการและการดำเนินงานที่เกี่ยวข้องกับบุคลากร กระบวนการทำงาน และเทคโนโลยี เป็นต้น โดยการตรวจสอบนี้ควรได้รับการทบทวนตามช่วงเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงสำคัญเกิดขึ้น

16. การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with Policies, Rules and Standards for Information Security)

เพื่อกำหนดให้มีการติดตามและตรวจสอบการปฏิบัติงานที่สอดคล้องกับนโยบายหรือแนวปฏิบัติภายในรวมถึงข้อกำหนดทางกฎหมายและมาตรฐานสากล เพื่อเป็นการหลีกเลี่ยงการละเมิดกฎหมาย ระเบียบข้อบังคับ หรือข้อผูกพันตามสัญญาที่เกี่ยวกับความมั่นคงปลอดภัย ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรมีการทบทวนการปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ เพื่อเป็นแนวทางในการปฏิบัติงานของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

17. เอกสารขั้นตอนการปฏิบัติงาน (Documented Operating Procedures)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรจัดทำเอกสารขั้นตอนการปฏิบัติงานของอุปกรณ์ประมวลผลสารสนเทศ และเอกสารขั้นตอนการปฏิบัติงานนี้ควรเข้าถึงได้โดยบุคลากรที่เกี่ยวข้อง เพื่อให้การปฏิบัติงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัยจึงสมควรให้มีการกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติงาน ดังนั้น จำเป็นต้องมีการจัดทำคู่มือปฏิบัติงาน (Documented Operating Procedures) มีความพร้อมใช้สำหรับผู้ที่ต้องการนำไปใช้ต่อ และการแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties) ให้ชัดเจนและเหมาะสม เพื่อลดความเสียหายที่อาจเกิดกับทรัพย์สินสารสนเทศของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ต้องจัดให้มีคู่มือปฏิบัติงาน (Documented Operating Procedures) โดยมีการดำเนินการอย่างน้อยดังต่อไปนี้

1) จัดทำและปรับปรุงคู่มือการปฏิบัติงาน เพื่อใช้เป็นแนวทางในการปฏิบัติงาน ทั้งนี้ คู่มือดังกล่าวสามารถจัดทำในรูปแบบสิ่งพิมพ์หรืออิเล็กทรอนิกส์

2) ฝึกอบรมแก่เจ้าหน้าที่ฝ่ายบริหารเทคโนโลยีดิจิทัล เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง

3) ทดสอบการปฏิบัติงานตามคู่มือที่จัดทำขึ้น

4) คู่มือการปฏิบัติงานต้องได้รับอนุมัติจากผู้จัดการฝ่ายบริหารเทคโนโลยีดิจิทัลเป็นอย่างน้อย

5) ต้องมีการกำหนดให้มีการควบคุมการเข้าถึงคู่มือการปฏิบัติงาน เพื่อป้องกันการเข้าถึงและเปิดเผยคู่มือการปฏิบัติงานโดยมิได้รับอนุญาต

6) ต้องมีการจัดทำทะเบียนคู่มือการปฏิบัติงาน และต้องมีการทบทวนทะเบียนคู่มืออย่างน้อยปีละ 1 ครั้ง เพื่อให้เกิดความมั่นใจและง่ายต่อการค้นหาคู่มือและเจ้าของคู่มือปฏิบัติงานผู้เป็นเจ้าของทรัพย์สินสารสนเทศ ต้องควบคุมให้มีการแบ่งหน้าที่ความรับผิดชอบ (Segregation of Duties) อย่างเหมาะสมเพื่อลดความเสี่ยงในการใช้ทรัพย์สินสารสนเทศของผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ในทางที่ไม่เหมาะสมทั้งโดยเจตนาและไม่เจตนา โดยต้องกำหนดให้มีการแบ่งแยกหน้าที่รับผิดชอบในแต่ละกระบวนการและมีการตรวจสอบการทำงานซึ่งกันและกัน ตัวอย่างเช่น ผู้พัฒนาระบบสารสนเทศ ต้องไม่มีสิทธิในการเข้าถึงระบบที่ให้บริการจริง และต้องไม่มีสิทธิในการติดตั้งซอฟต์แวร์และแอปพลิเคชันในระบบที่ให้บริการจริงเป็นต้น ในกรณีที่ไม่สามารถดำเนินการได้ ต้องมีการพิจารณาการควบคุมในด้านอื่น ๆ เช่น การเฝ้าระวังการปฏิบัติงานและการสอบทานหลักฐานการตรวจสอบ (Audit Trail) โดยหัวหน้างานหรือพนักงานและลูกจ้างอื่น ซึ่งไม่มีความเกี่ยวข้องโดยตรงกับการปฏิบัติงานนั้น ๆ เป็นต้น

18. การรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บ (Security of Data at Rest)

เพื่อกำหนดวิธีการรักษาความมั่นคงปลอดภัยของข้อมูลที่ถูกจัดเก็บอย่างมีประสิทธิผลและเหมาะสม เพื่อป้องกันความลับ การพิสูจน์ตัวตนและความถูกต้องครบถ้วนของข้อมูล เช่น ข้อมูลองค์กรฐานข้อมูล และข้อมูลที่จัดเก็บอยู่ในสื่อบันทึกข้อมูลประเภทต่าง ๆ มีการดำเนินการ อย่างน้อย ดังนี้

18.1 ระบุข้อมูลที่สำคัญที่อยู่ในความรับผิดชอบขององค์กร โดยต้องคำนึงถึงความต้องการทางธุรกิจที่เกี่ยวข้องและภาระผูกพันทางกฎหมาย และวิธีการควบคุมการเข้าถึงข้อมูล การใช้งานร่วมกัน การคัดลอกการส่งและการแจกจ่าย สำหรับข้อมูลที่สำคัญและข้อมูลลับ

18.2 ต้องเก็บรักษาข้อมูลที่สำคัญไว้ตามระยะเวลาที่กำหนด โดยขึ้นอยู่กับชนิดของข้อมูลและความสำคัญของข้อมูล โดยให้เก็บรักษาข้อมูลที่สำคัญไว้ช่วงระยะเวลาหนึ่งให้สอดคล้องกับกฎหมายหรือข้อตกลงที่กำหนด เพื่อเป็นหลักฐานทางกฎหมาย และการดำเนินการให้บริการ และมีกระบวนการเก็บรักษาข้อมูลที่มีความมั่นคงปลอดภัย เพื่อให้มั่นใจว่าสามารถเข้าถึงข้อมูลได้ตลอดระยะเวลาเก็บรักษา

18.3 มีกลไกการเข้ารหัสลับ (Cryptographic) เพื่อปกป้องข้อมูลลับ และความถูกต้องครบถ้วนของข้อมูลที่จัดเก็บอยู่ในสื่อบันทึกข้อมูลระหว่างการส่งออกนอกพื้นที่ที่มีการควบคุมและในการรับหรือส่งข้อมูลภายใน และระหว่างองค์กร ดังนี้

1) มีบันทึกเหตุการณ์และตรวจสอบกิจกรรมที่เกี่ยวกับการรับหรือส่งข้อมูลทั้งภายในและภายนอกองค์กร

2) กำหนดให้มีการใช้เทคนิคการเข้ารหัสลับ ที่สอดคล้องกับกฎหมายและข้อกำหนดตามข้อตกลงต่าง ๆ ขององค์กร เพื่อป้องกันข้อมูลที่สำคัญและข้อมูลลับ

3) ควรมีแนวทางการบริหารจัดการกุญแจเข้ารหัสลับ (Cryptographic key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับขององค์กร เช่น การกำหนดบทบาทและหน้าที่ กระบวนการจัดเก็บ กระบวนการเปลี่ยนแปลงข้อมูลที่สำคัญ กระบวนการยกเลิกการใช้งาน กระบวนการบันทึกและตรวจสอบกิจกรรม หรือกระบวนการจัดการที่สำคัญ เป็นต้น

18.4 มีกลไกการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลสำคัญที่ถูกจัดเก็บ โดยไม่ได้รับอนุญาต เช่น การป้องกันการแก้ไขเปลี่ยนแปลงลายมือชื่ออิเล็กทรอนิกส์ โดยการใช้ฟังก์ชันแฮช (Hash Function) เป็นต้น เพื่อใช้ตรวจสอบความถูกต้องครบถ้วนของข้อมูล

19. การรักษาความมั่นคงปลอดภัยของส่วนเชื่อมต่อบริการ (Interface Security)

มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศสำหรับส่วนเชื่อมต่อบริการระหว่างองค์กรที่ใช้ข้อมูลอิเล็กทรอนิกส์ ประกอบด้วยหัวข้อ ดังนี้

1) ขอบข่ายของบริการวัตถุประสงค์ด้านความมั่นคงปลอดภัย

2) ทรัพย์สินสารสนเทศสำคัญที่สนับสนุนการบริการและการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์เพื่อควบคุมการใช้ข้อมูลร่วมกัน และการรักษาความมั่นคงปลอดภัยในส่วนเชื่อมต่อระบบสารสนเทศหรือระบบเครือข่ายของผู้ใช้บริการ

3) มีวิธีการปกป้องข้อมูลด้วยการส่งข้อมูลผ่านช่องทางที่เข้ารหัสลับ เช่น การใช้ Transport Layer Security (TLS) 1.2 หรือเวอร์ชันที่สูงกว่า

4) มีวิธีการควบคุมทางเครือข่ายเพื่อรักษาความลับและความถูกต้องครบถ้วนของข้อมูลสำคัญที่มีการรับส่งผ่านทางเครือข่ายสาธารณะ หรือผ่านเครือข่ายไร้สาย หรือระบบสารสนเทศที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ

5) มีการระบุข้อมูลที่แตกต่างกัน (Unique Identifier) เพื่อใช้ในการระบุตัวตนผู้ใช้งานได้ เช่น กำหนดเลขที่หรือรหัสประจำตัว หรือชื่อผู้ใช้บริการ (ภาษาอังกฤษ) หรือชื่ออื่น ๆ ที่ระบบรองรับได้และสามารถสื่อความหมายถึงข้อมูลผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ได้อย่างชัดเจน

20. การรักษาความมั่นคงปลอดภัยของซอฟต์แวร์ (Software Security)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรกำหนดแนวทางที่ทำให้มั่นใจว่าซอฟต์แวร์ที่ให้บริการมีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม โดยแนวทางการรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์ที่จัดหาหรือพัฒนาขึ้นมาใช้งาน ประกอบด้วยหัวข้อต่อไปนี้

1) การรักษาความมั่นคงปลอดภัยของสภาพแวดล้อมการพัฒนา

2) มีคำแนะนำเกี่ยวกับความมั่นคงปลอดภัยในวงจรการพัฒนาซอฟต์แวร์ เช่น การรักษาความมั่นคงปลอดภัยในวิธีการพัฒนาซอฟต์แวร์ และแนวทางการเขียนโปรแกรมอย่างปลอดภัย เป็นต้น

3) มีข้อกำหนดด้านความมั่นคงปลอดภัยในขั้นตอนการออกแบบ

4) มีการเก็บรักษาที่มีความมั่นคงปลอดภัย

5) การควบคุมเวอร์ชัน

6) ความมั่นคงปลอดภัยของซอฟต์แวร์ที่ต้องการ

7) ความสามารถของบุคลากรในการตรวจพบและแก้ปัญหาช่องโหว่ด้านความมั่นคงปลอดภัย

8) สร้างความตระหนักเกี่ยวกับแนวทางการรักษาความมั่นคงปลอดภัยของซอฟต์แวร์ให้กับบุคลากรหลัก

21. ข้อกำหนดในการทำงานร่วมกัน (Interoperability)

ผู้เชื่อมต่อระบบอิเล็กทรอนิกส์ ควรกำหนดกระบวนการหรือขั้นตอนการทำงานร่วมกันระหว่างผู้เชื่อมต่อระบบอิเล็กทรอนิกส์กับหน่วยงานต่าง ๆ เพื่อให้มั่นใจได้ว่าได้ออกแบบระบบที่สามารถทำงานร่วมกันระหว่างหน่วยงานได้ โดยมีมามาตรฐานที่เป็นที่ยอมรับมาใช้ในการทำงานร่วมกัน ตัวอย่างเช่น

1) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ระหว่างหน่วยงานที่เป็นแนวทางการจัดทำเอกสารและข้อความให้อยู่ในรูปของ XML File การสร้างและการตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ และใช้เป็นแนวทางการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์

2) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยข้อความอิเล็กทรอนิกส์ สำหรับการซื้อขายสินค้าและบริการ เป็นมาตรฐานที่กำหนดรูปแบบโครงสร้างข้อมูล XML สำหรับการซื้อขายสินค้าและบริการ เพื่อสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์

3) การใช้งาน OpenID ที่เป็นโพรโทคอลที่ใช้ยืนยันตัวตนและการตรวจสอบผู้ใช้งานระหว่างผู้ใช้งานและผู้ให้บริการ เป็นต้น

4) รองรับการจัดทำข้อมูลในรูปแบบที่มีโครงสร้างและไม่มีโครงสร้างให้แก่ผู้ใช้บริการหากมีการโอนย้ายบริการหรือมีการร้องขอ เช่น ไฟล์ชนิด .doc, .xls, .pdf, log และ flat file เป็นต้น

บรรณานุกรม

[1] กฎกระทรวง ฉบับที่ 384 ออกตามความในประมวลรัษฎากร ว่าด้วยการดำเนินการเกี่ยวกับเอกสารหลักฐานหรือหนังสือด้วยกระบวนการทางอิเล็กทรอนิกส์. (2565).

[2] ประกาศอธิบดีกรมสรรพากร (ฉบับที่ 48) เรื่อง กำหนดมาตรฐานเกี่ยวกับรูปแบบ วิธีการส่ง การเก็บรักษาเอกสารหลักฐานหรือหนังสือ และความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับการดำเนินการที่เกี่ยวข้องกับกระบวนการทางอิเล็กทรอนิกส์. (2566).

[3] ประกาศกรมสรรพากร เรื่อง นโยบายธรรมาภิบาลข้อมูลของกรมสรรพากร พ.ศ. 2563 และประกาศกรมสรรพากร เรื่อง แนวปฏิบัติธรรมาภิบาลข้อมูลของกรมสรรพากร พ.ศ. 2563.

[4] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560.

[5] พระราชบัญญัติประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564.

[6] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570).

[7] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2562). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์. ว่าด้วยการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการจัดทำ ส่งมอบ และเก็บรักษาข้อมูลอิเล็กทรอนิกส์. ขมธอ. 21-2562

[8] ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27002:2022 (Annex A: Information Security Controls Reference).

[9] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2561). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์. ขมธอ. 18-2561

[10] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2561). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน. ขมธอ. 19-2561

[11] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2561). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน. ขมธอ. 20-2561

[12] Department of Finance and Deregulation, Australian Government Information Management Office. (2009). The National e-Authentication Framework.

[13] ประมวลกฎหมายอาญา.

[14] Department of Economic and Social Affairs, United Nations, New York. (2012). United Nations E-Government Survey 2012.

[15] ประกาศธนาคารแห่งประเทศไทยที่ สนส. 19/2562. (2562). เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน ประกาศ ณ วันที่ 2 กันยายน พ.ศ. 2562 คัดจากราชกิจจานุเบกษา เล่มที่ 136 ตอนพิเศษ 219 ง วันที่ 2 กันยายน 2562.

[16] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2561). ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร. ขมธอ. 17-2561