บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)
Airports of Thailand Public Company Limited

ประกาศบริษัท ท่าอากาศยานไทย จำกัด (มหาชน)

เรื่อง นโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

(AOT ICT Security Policy)

(ฉบับทบทวนประจำปีงบประมาณ 2567)

บริษัท ท่าอากาศยานไทย จำกัด (มหาชน) (ทอท.) เป็นองค์กรที่ดำเนินธุรกิจท่าอากาศยานในการให้บริการด้านการขนส่งทางอากาศตามมาตรฐานการดำเนินงานสนามบินเป็นไปตามกฎหมายที่รัฐกำหนด ซึ่งสอดคล้องกับมาตรฐานขององค์การการบินพลเรือนระหว่างประเทศ (International Civil Aviation Organization : ICAO) โดย ทอท. ได้นำเทคโนโลยีสารสนเทศและการสื่อสารมาสนับสนุนด้านการบริหารองค์กร ด้านปฏิบัติการท่าอากาศยาน ด้านการพาณิชย์ และการแลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานทั้งภาครัฐและเอกชนเพื่อรองรับการให้บริการท่าอากาศยานในความรับผิดชอบของ ทอท. ได้อย่างต่อเนื่อง

เพื่อให้ระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. มีความมั่นคงปลอดภัยในการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) รวมทั้งสร้างความเชื่อมั่นแก่พนักงาน ทอท. สายการบิน ผู้โดยสาร ผู้ใช้บริการท่าอากาศยาน และหน่วยงานทั้งภาครัฐและเอกชน ตลอดจนประชาชนทั่วไป จึงเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. โดยให้ดำเนินการ ดังนี้

1. ยกเลิกประกาศ ทอท. เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Policy) ลงวันที่ 1 ตุลาคม 2561

2. สายงานเทคโนโลยีดิจิทัลและการสื่อสาร เป็นผู้กำหนดให้มีนโยบาย นโยบายสนับสนุน แนวทางการปฏิบัติงาน มาตรฐานการปฏิบัติงานและขั้นตอนการปฏิบัติงาน รวมถึงเอกสารอื่นใดที่ต้องดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปตามพระราชบัญญัติฯ พระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์ดังต่อไปนี้

2.1 จัดทำนโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. และแนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. โดยต้องประกอบด้วยเนื้อหาอย่างน้อย ดังนี้

2.1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ โดยมีเนื้อหาครอบคลุมอย่างน้อย 4 ด้าน ดังนี้

(1) การเข้าถึงระบบสารสนเทศ

(2) การเข้าถึงระบบเครือข่าย

(3) การเข้าถึงระบบปฏิบัติการ

(4) การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

2.1.2 การจัดให้...

2.1.2 การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

2.1.3 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

2.2 กำหนดนโยบาย นโยบายสนับสนุน แนวทางการปฏิบัติงาน มาตรฐานการปฏิบัติงาน ขั้นตอนการปฏิบัติงาน และวิธีการปฏิบัติงาน รวมถึงเอกสารอื่นใดที่เกี่ยวข้องเพื่อให้พนักงาน ทอท. ทุกระดับและบุคคลภายนอกที่ปฏิบัติงานให้กับ ทอท. ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2.3 เผยแพร่นโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ให้กับพนักงาน ทอท. ทุกระดับและบุคคลภายนอกที่ปฏิบัติงานให้กับ ทอท. ได้รับทราบและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. และถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2.4 ตรวจสอบและประเมินผลการดำเนินการให้เป็นไปตามนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ที่กำหนด

2.5 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

2.6 ทบทวนนโยบาย นโยบายสนับสนุน แนวทางการปฏิบัติงาน มาตรฐานการปฏิบัติงาน ขั้นตอนการปฏิบัติงาน และวิธีการปฏิบัติงาน รวมถึงเอกสารอื่นใดด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร เป็นประจำทุก 2 ปี หรือปรับปรุงทันทีเมื่อมีความจำเป็น

2.7 กรรมการผู้อำนวยการใหญ่/ผู้อำนวยการใหญ่ ทอท. หรือผู้บริหารระดับสูงที่ได้รับมอบหมายมีอำนาจออกคำสั่งหรือกำหนดนโยบายสนับสนุน แนวทางการปฏิบัติงาน มาตรฐานการปฏิบัติงาน ขั้นตอนการปฏิบัติงานและวิธีการปฏิบัติงาน รวมถึงเอกสารอื่นใดให้เป็นไปตามนโยบายฉบับนี้ และในกรณีที่เป็นปัญหาเกี่ยวกับการปฏิบัติตามนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ให้กรรมการผู้อำนวยการใหญ่/ผู้อำนวยการใหญ่ ทอท. หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย เป็นผู้วินิจฉัยและให้ถือเป็นที่สุด

2.8 กรรมการผู้อำนวยการใหญ่/ผู้อำนวยการใหญ่ ทอท. เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น กรณีระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร หรือสินทรัพย์สารสนเทศของ ทอท. เกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืน การปฏิบัติตามนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

2.9 ให้รองกรรมการผู้อำนวยการใหญ่สายงานเทคโนโลยีดิจิทัลและการสื่อสาร เป็นผู้รับผิดชอบต่อการกำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้คำปรึกษาและข้อเสนอแนะการปฏิบัติตามนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

2.10 ให้พนักงาน...

2.10 ให้พนักงาน ทอท. ทุกระดับและบุคคลภายนอกที่ปฏิบัติงานร่วมกับ ทอท. รับทราบและปฏิบัติตามนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. รวมทั้งนโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร และแนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร ตามเอกสารแนบท้ายนี้อย่างเคร่งครัด ทั้งนี้การละเมิดหรือฝ่าฝืนถือเป็นความผิดทางวินัยตามระเบียบข้อบังคับของ ทอท. และกรณีการกระทำผิดตามกฎหมายถือเป็นความผิดเฉพาะส่วนบุคคล

ประกาศ ณ วันที่ 17 ตุลาคม พ.ศ. 2566

(นายกีรติ กิจมานะวัฒน์)
ผู้อำนวยการใหญ่

AIRPORTS OF THAILAND PLC.
บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)

เอกสารแนบท้ายประกาศ

- นโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.
  (AOT ICT Security Supporting Policy)

- แนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.
  (AOT ICT Security Guideline)

บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)

ปีงบประมาณ 2567

สายงานเทคโนโลยีดิจิทัลและการสื่อสาร

Supporting Policy

นโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

AOT ICT Security Supporting Policy

รหัสเอกสาร : Document No.: SP-1608010-001

Version: 2

ผู้จัดทำเอกสาร

ส่วนมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสาร (สมส.)

ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสาร (ฝกท.)

โทรศัพท์ 55300

เจ้าของเอกสาร

สายงานเทคโนโลยีดิจิทัลและการสื่อสาร

รายละเอียดเอกสาร	
ประเภทเอกสาร :	นโยบายสนับสนุน (SP)
เจ้าของเอกสาร :	ส่วนมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสาร (สมส.) ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสาร (ฝกท.)

ผู้ทบทวน	ผู้อนุมัติ
(นายธวัชชัย รัตนทองคง)	(นายกิตติพจน์ เวณุนันท์)
ตำแหน่ง ผอก.ฝกท.	ตำแหน่ง รฝบท.
วันที่ 17 ต.ค. 66	วันที่ 17 ต.ค. 66

Version	วันที่บังคับใช้	ชื่อผู้จัดทำเอกสาร	สาระสำคัญของการแก้ไข/ปรับปรุง	หมายเหตุ
1	1 ตุลาคม 2561	น.ส.ฉัตรวดี ศิริโภค	เอกสารประกาศใช้ครั้งแรก	
2	ตุลาคม 2566	น.ส.ฉัตรวดี ศิริโภค	• แก้ไข Header • ทบทวนปรับปรุงสอดคล้องตามข้อกำหนดวิธีการแบบปลอดภัยในระดับเคร่งครัด พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 • ยกเลิกลำดับการแก้ไข • ปรับชื่อและรหัสตามโครงสร้างใหม่	

Version	วันที่บังคับใช้	ชื่อผู้จัดทำเอกสาร	สาระสำคัญของการแก้ไข/ปรับปรุง	หมายเหตุ
			• เพิ่มนิยาม เทคโนโลยีดิจิทัลและการสื่อสาร • แก้ไข ชื่อหมวดให้สอดคล้องตามมาตรฐาน ISO/IEC 27001:2013 • เพิ่มหลักเกณฑ์ที่อ้างอิงข้อ 1.8 - 1.11 • ปรับปรุงข้อมูล หมวด 1 ข้อ 1.3 • ปรับปรุงข้อมูล หมวด 2 ข้อ 2.4 - 2.5 • ปรับปรุงข้อมูล หมวด 3 ข้อ 3.2 • ปรับปรุงข้อมูล หมวด 4 ข้อ 4.1 • ปรับปรุงข้อมูล หมวด 5 ข้อ 5.8 – 5.11 • ปรับปรุงข้อมูล หมวด 7 ข้อ 7.5 – 7.6 • ปรับปรุงข้อมูล หมวด 10 ข้อ 10.1, 10.3, 10.5 และ 10.6 • ปรับปรุงข้อมูล หมวด 11 ข้อ 11.2 • ปรับปรุงข้อมูล หมวด 13 ข้อ 13.2 • ปรับปรุงข้อมูล หมวด 14 ข้อ 14.5	

สารบัญ

หน้า

1. หลักเกณฑ์ที่อ้างอิง 5

2. หลักการและเหตุผล 6

3. ขอบเขต 6

4. คำนิยาม 8

หมวด 1 การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ 11

หมวด 2 การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบทางเทคโนโลยีสารสนเทศ และการสื่อสาร 11

หมวด 3 การสร้างความมั่นคงปลอดภัยด้านบุคลากร 12

หมวด 4 การบริหารจัดการสินทรัพย์สารสนเทศ 13

หมวด 5 การควบคุมการเข้าถึงระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร 14

หมวด 6 การเข้ารหัสข้อมูล 15

หมวด 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม 15

หมวด 8 ความปลอดภัยด้านการดำเนินงาน 16

หมวด 9 ความปลอดภัยด้านการสื่อสาร 16

หมวด 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร 17

หมวด 11 ความปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก 17

หมวด 12 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ... 18

หมวด 13 การบริหารจัดการความต่อเนื่องด้านการดำเนินงาน 18

หมวด 14 การปฏิบัติตามกฎหมาย และข้อกำหนด 19

ภาคผนวก ก. มาตรฐานและข้อกำหนดอ้างอิง 20

1. หลักเกณฑ์ที่อ้างอิง

1.1 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

1.2 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551

1.3 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

1.3.1 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวทางการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

1.3.2 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวทางการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556

1.4 พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 (วิธีการแบบปลอดภัยในระดับเคร่งครัด)

1.5 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1.6 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

1.7 ประกาศบริษัท ท่าอากาศยานไทย จำกัด (มหาชน) เรื่อง นโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Policy) ณ วันที่ 1 ตุลาคม พ.ศ. 2561

1.8 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.8.1 ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1.8.2 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคาม ทางไซเบอร์แต่ละระดับ พ.ศ. 2564

1.9 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.10 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

2. หลักการและเหตุผล

เพื่อให้ระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ท่าอากาศยานไทย จำกัด (มหาชน) (ทอท.) มีความมั่นคงปลอดภัยในการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) สำหรับสินทรัพย์สารสนเทศ และข้อมูลสารสนเทศสำคัญของ ทอท. ในการดำเนินธุรกิจให้พ้นจากภัยคุกคามและปัจจัยเสี่ยงทั้งจากภายในและภายนอกองค์กร ไม่ว่าจะเกิดขึ้นโดยเจตนาหรือไม่ก็ตาม พร้อมทั้งลดความเสียหายต่างๆ ที่อาจเกิดขึ้นจากเหตุอันล่วงละเมิดด้านความมั่นคงปลอดภัย และเพื่อรักษาไว้ ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง และเป็นการปฏิบัติให้สอดคล้องตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง ซึ่งมีผลบังคับใช้กับ ทอท. รวมทั้งเป็นการสร้างความเชื่อมั่นแก่พนักงาน ทอท. สายการบิน ผู้โดยสาร ผู้ใช้บริการท่าอากาศยาน และหน่วยงานทั้งภาครัฐและเอกชน ตลอดจนประชาชนทั่วไป ในการใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

3. ขอบเขต

นโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Supporting Policy) มีขอบเขตครอบคลุม ดังนี้

3.1 ระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งสินทรัพย์สารสนเทศของ ทอท. เช่น ระบบคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ ข้อมูลสารสนเทศ และระบบสารสนเทศ

3.2 ข้อมูลสารสนเทศสำคัญทั้งหมดในการดำเนินกิจการของ ทอท. ทั้งในส่วนที่เป็นอิเล็กทรอนิกส์และกระดาษ ตั้งแต่การสร้าง การจัดเก็บ การใช้งาน และการทำลาย

3.3 บุคคลที่มีส่วนเกี่ยวข้องในการดำเนินงานระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร ตลอดจนสินทรัพย์สารสนเทศและข้อมูลสารสนเทศของ ทอท. ได้แก่ ผู้บริหาร พนักงาน ลูกจ้าง ลูกจ้างทดลองปฏิบัติงาน บุคคลหรือหน่วยงานภายนอกที่มาใช้บริการหรือให้บริการที่เกี่ยวข้องกับระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. บุคคลหรือหน่วยงานภายนอกที่เป็นคู่สัญญากับ ทอท.

3.4 นโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.(AOT ICT Security Supporting Policy) มีเนื้อหาครอบคลุม 14 หมวด ดังนี้

หมวด 1 การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ
หมวด 2 การจัดโครงสร้างความมั่นคงปลอดภัยทางระบบเทคโนโลยีสารสนเทศและการสื่อสาร
หมวด 3 การสร้างความมั่นคงปลอดภัยด้านบุคลากร
หมวด 4 การบริหารจัดการสินทรัพย์สารสนเทศ
หมวด 5 การควบคุมการเข้าถึงระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร
หมวด 6 การเข้ารหัสข้อมูล

หมวด 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม
หมวด 8 ความปลอดภัยด้านการดำเนินงาน
หมวด 9 ความปลอดภัยด้านการสื่อสาร
หมวด 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร
หมวด 11 ความปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก
หมวด 12 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด
หมวด 13 การบริหารจัดการความต่อเนื่องด้านการดำเนินงาน
หมวด 14 การปฏิบัติตามกฎหมาย และข้อกำหนด

4. คำนิยาม

4.1 “พนักงาน” หมายความว่า พนักงาน ทอท. และลูกจ้าง ของ ทอท.

4.2 “หัวหน้าส่วนงาน” หมายความว่า ผู้อำนวยการฝ่าย/ศูนย์/สำนัก หรือผู้บริหารหน่วยงานในระดับเทียบเท่าของ ทอท.

4.3 “ผู้ใช้งานภายนอก” หมายความว่า บุคคลภายนอกที่มีสิทธิใช้ระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

4.4 “ผู้ใช้งาน” หมายความว่า พนักงาน ทอท. และผู้ใช้งานภายนอก ที่เกี่ยวข้อง เข้าถึง หรือเข้าใช้งานสินทรัพย์สารสนเทศ และระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

4.5 “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิการใช้งาน สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับการใช้งานสินทรัพย์สารสนเทศ และระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

4.6 “สินทรัพย์” หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

4.7 “สินทรัพย์สารสนเทศ” หมายความว่า ทรัพย์สินสารสนเทศ* ระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีความหมายครอบคลุม ดังนี้

(1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(2) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

4.8 “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” (Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึง หรือใช้งานสินทรัพย์สารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

4.9 “ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Security) หมายความว่า ความมั่นคงปลอดภัยของสินทรัพย์สารสนเทศ ประกอบด้วย การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (non-Repudiation) และความน่าเชื่อถือ (Reliability)

---

*ตามพระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2553 ทรัพย์สินสารสนเทศ หมายความว่า

(1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(2) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

4.10 “เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

4.11 “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information Security Incident) หมายความว่า เหตุขัดข้อง อุบัติการณ์ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

4.12 “การรักษาความลับ” (Confidentiality) หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันสินทรัพย์สารสนเทศ จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

4.13 “การรักษาความถูกต้องครบถ้วน” (Integrity) หมายความว่า การดำเนินการเพื่อให้สินทรัพย์สารสนเทศอยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอนหรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

4.14 “การรักษาสภาพพร้อมใช้งาน” (Availability) หมายความว่า การจัดทำให้สินทรัพย์สารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

4.15 “การประเมินความเสี่ยงด้านสารสนเทศ” (Information Security Risk Assessment) หมายความว่า การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารสำหรับสินทรัพย์สารสนเทศของ ทอท.

4.16 “ระบบสารสนเทศ” หมายความว่า กลุ่มของระบบงานหรือโปรแกรมประยุกต์ที่ประกอบด้วยฮาร์ดแวร์หรือตัวอุปกรณ์ และซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บ และแจกจ่ายข้อมูลข่าวสาร เพื่อสนับสนุนการปฏิบัติงานของส่วนงานต่างๆ

4.17 “ระบบสารสนเทศที่มีความสำคัญ” หมายความว่า ระบบสารสนเทศหรือระบบงานหรือโปรแกรมประยุกต์ของ ทอท. ที่มีการประเมินว่ามีความสำคัญ และมีผลกระทบต่อการดำเนินธุรกิจของ ทอท. หากระบบดังกล่าวหยุดชะงักหรือไม่สามารถให้บริการได้

4.18 “ส่วนงานที่ดูแลระบบการให้บริการ” หมายความว่า ส่วนงานที่รับผิดชอบดูแลระบบทางเทคโนโลยีสารสนเทศและการสื่อสารที่มีการให้บริการ (Production) ทั้งที่อยู่ในความรับผิดชอบของสายงานเทคโนโลยีดิจิทัลและการสื่อสาร และส่วนงานอื่นของ ทอท.

4.19 “เจ้าของระบบสารสนเทศ” หมายความว่า ส่วนงาน ทอท. ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการบริหารจัดการ กำกับดูแล และควบคุมการใช้งานระบบสารสนเทศของ ทอท. ให้สามารถดำเนินงานตามภารกิจของ ทอท. ได้อย่างครบถ้วนสมบูรณ์

4.20 “ข้อมูลสารสนเทศ” หมายความว่า ข่าวสาร ข้อเท็จจริง ข้อมูลในรูปแบบใดๆ หรือข้อมูลที่มีการประมวลผลใดๆ ทั้งในเหตุการณ์หรือกิจกรรมต่างๆ

4.21 “เจ้าของข้อมูลสารสนเทศ” หมายความว่า ส่วนงานที่มีหน้าที่รับผิดชอบในการกำหนดกระบวนการนำเข้า ปรับปรุง ประมวลผล และตรวจสอบความถูกต้องของข้อมูลสารสนเทศของ ทอท. ให้มีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ โดยเป็นผู้รับผิดชอบข้อมูลสารสนเทศ ซึ่งได้รับผลกระทบโดยตรงหากข้อมูลสารสนเทศเหล่านั้นเกิดเสียหายหรือสูญหาย

4.22 “อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่” หมายความว่า อุปกรณ์คอมพิวเตอร์และสื่อสารใดๆ ที่มีระบบปฏิบัติการสามารถประมวลผลได้ด้วยตัวเอง เพื่อการเข้าถึง การใช้งานและจัดเก็บสารสนเทศ เช่น เครื่องคอมพิวเตอร์โน๊ตบุ๊ค สมาร์ทโฟน แท็บเล็ต เป็นต้น

4.23 “สื่อบันทึกข้อมูลที่เคลื่อนย้ายได้” หมายความว่า สื่อหรืออุปกรณ์ที่ใช้ในการบันทึกข้อมูลที่เคลื่อนย้ายได้ เช่น เทป ฮาร์ดดิสก์ แฟลชไดร์ฟ แผ่นบันทึกข้อมูลซีดี/ดีวีดี เป็นต้น

4.24 “การใช้บริการหน่วยงานภายนอก” หมายความว่า การที่ ทอท.ได้มีการทำสัญญากับผู้ให้บริการภายนอกเพื่อดำเนินการแทนในบางกลุ่มงานที่โดยปกติ ทอท. ต้องดำเนินการเองทั้งหมด หรือบางส่วน รวมทั้งการติดต่อประสานกับผู้ให้บริการภายนอก เพื่อการนำเสนอหรือประชุมหารือ เพื่อให้ข้อมูลสารสนเทศต่างๆ กับ ทอท.

4.25 “ระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร” หมายความว่า ระบบที่ประกอบด้วยอุปกรณ์คอมพิวเตอร์ทั้งฮาร์ดแวร์ โปรแกรมคอมพิวเตอร์ อุปกรณ์เครือข่ายและสื่อสารข้อมูล ข้อมูลสารสนเทศและสื่อบันทึกข้อมูล ระบบสารสนเทศ สายสัญญาณและจุดเชื่อมต่อและอุปกรณ์ต่อพ่วงที่เกี่ยวข้อง

4.26 “เทคโนโลยีดิจิทัลและการสื่อสาร” หมายความว่า การนำเครื่องมือ อุปกรณ์คอมพิวเตอร์ ทั้งฮาร์ดแวร์ โปรแกรมคอมพิวเตอร์ อุปกรณ์เครือข่ายและสื่อสารข้อมูล ข้อมูลสารสนเทศ และสื่อบันทึกข้อมูล ระบบสารสนเทศ สายสัญญาณและจุดเชื่อมต่อและอุปกรณ์ต่อพ่วงที่เกี่ยวข้อง รวมทั้งอุปกรณ์ดิจิทัล อาทิ คอมพิวเตอร์ โทรศัพท์ แท็บเลต โปรแกรมคอมพิวเตอร์ และสื่อออนไลน์ มาใช้ให้เกิดประโยชน์สูงสุดในการสื่อสาร การปฏิบัติงาน และการทำงานร่วมกัน หรือใช้เพื่อพัฒนากระบวนการทำงาน หรือระบบงานในองค์กรให้มีความทันสมัยและมีประสิทธิภาพ

4.27 “ผู้ให้บริการภายนอก” หมายความว่า กลุ่มของบุคคลหรือบุคคลธรรมดาที่เป็นผู้ให้บริการภายนอก ที่มีความเชี่ยวชาญเฉพาะด้านในงานหนึ่งงานใดเพื่อรับบทบาทการทำงานนั้นๆ

หมวด 1 การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

วัตถุประสงค์

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. โดยผู้ใช้งานได้รับทราบถึงความสำคัญ หน้าที่ ความรับผิดชอบ และแนวทางการปฏิบัติงานในการควบคุมความเสี่ยงด้านต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร เพื่อใช้งานได้ตรงตามวัตถุประสงค์ของ ทอท.

เนื้อหานโยบาย

1.1 ให้มีการจัดทำ ปรับปรุง ประกาศใช้ และเผยแพร่ นโยบาย นโยบายสนับสนุน แนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. โดยมีการทบทวนเป็นประจำทุก 2 ปี หรือปรับปรุงทันทีเมื่อมีความจำเป็น

1.2 ให้มีการจัดทำกรอบบริหารความเสี่ยงด้านสารสนเทศ โดยมีการทบทวนการประเมินความเสี่ยงด้านสารสนเทศเป็นประจำทุกปี เพื่อพิจารณาทบทวนนโยบาย นโยบายสนับสนุน แนวทางการปฏิบัติงานมาตรฐานการปฏิบัติงาน ขั้นตอนการปฏิบัติงาน และวิธีการปฏิบัติงาน รวมถึงเอกสารอื่นใดที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมตามสภาพความเสี่ยงของ ทอท.

1.3 นโยบายฉบับนี้ถือเป็นนโยบายสำคัญอย่างยิ่งยวดที่ต้องปฏิบัติตาม ในกรณีที่มีข้อจำกัดในการปฏิบัติตามนโยบาย หน่วยงาน/ส่วนงานสามารถขอยกเว้นการปฏิบัติได้ โดยต้องได้รับการอนุมัติจากคณะกรรมการบริหารเทคโนโลยีดิจิทัลและการสื่อสารของ ทอท. ซึ่งต้องมีการวิเคราะห์ความเสี่ยงพร้อมมาตรการควบคุมภายใน

หมวด 2 การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์

เพื่อบริหารและจัดการความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.ในการกำหนดโครงสร้างด้านการบริหารจัดการทั้งสำหรับภายในและภายนอกองค์กร

เนื้อหานโยบาย

2.1 ให้มีการกำหนดหน้าที่ความรับผิดชอบสำหรับการพิจารณาอนุมัติแผนงานโครงการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

2.2 ให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารก่อนเริ่มการพัฒนาหรือดำเนินงานแผนงาน/โครงการด้านเทคโนโลยีสารสนเทศและการสื่อสาร

2.3 ให้มีการควบคุมการนำอุปกรณ์คอมพิวเตอร์และสื่อสาร และอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่มาใช้งานภายใน ทอท.

2.4 ให้มีการควบคุมการนำอุปกรณ์คอมพิวเตอร์และสื่อสารทุกประเภททั้งที่ ทอท. จัดหาให้ใช้งาน และที่เป็นอุปกรณ์ส่วนตัว มาใช้ในการปฏิบัติงานเพื่อเข้าถึงระบบทางเทคโนโลยีสารสนเทศและการสื่อสารจากภายนอกองค์กร

2.5 การนำอุปกรณ์คอมพิวเตอร์และสื่อสารทุกประเภทและที่เป็นอุปกรณ์ส่วนตัว เพื่อเชื่อมต่อกับระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร ของ ทอท. ต้องดำเนินการผ่านช่องทางที่ ทอท. กำหนด หรือต้องได้รับอนุญาตจากส่วนงานดูแลระบบการให้บริการหรือตามแนวทางปฏิบัติที่ ทอท. กำหนดไว้

หมวด 3 การสร้างความมั่นคงปลอดภัยด้านบุคลากร

วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร โดยเป็นการลดความเสี่ยงที่อาจเกิดขึ้นจากบุคลากร

เนื้อหานโยบาย

3.1 ให้มีกระบวนการคัดเลือกบุคลากรอย่างเหมาะสมตามตำแหน่งหน้าที่และระดับข้อมูลสารสนเทศที่สำคัญ

3.2 ให้มีการระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของพนักงาน และคู่สัญญากับผู้ให้บริการภายนอก ให้สอดคล้องกับนโยบายในการปฏิบัติงานหรือให้บริการระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ควรจัดให้มีการลงนามในเงื่อนไขการจ้างงาน ซึ่งระบุหน้าที่ความรับผิดชอบด้านการรักษาความปลอดภัยสารสนเทศและการไม่เปิดเผยความลับ ก่อนเริ่มงาน

3.3 ให้มีการฝึกอบรม ให้ความรู้ และสร้างความตระหนักด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. สำหรับผู้ใช้งาน

3.4 ให้มีกระบวนการในกรณียุติการว่าจ้างหรือเปลี่ยนแปลงหน้าที่งาน รวมทั้งการยกเลิกสิทธิ และการส่งคืนสินทรัพย์ เมื่อหมดภาระหน้าที่

หมวด 4 การบริหารจัดการสินทรัพย์สารสนเทศ

วัตถุประสงค์

เพื่อป้องกันสินทรัพย์สารสนเทศจากความเสียหาย และ/หรือ การนำไปใช้อย่างผิดวัตถุประสงค์ ทั้งจากการปฏิบัติหน้าที่ของพนักงาน ทอท. และบุคคลภายนอก

เนื้อหานโยบาย

4.1 ให้มีการจัดทำและทบทวนรายการสินทรัพย์สารสนเทศที่สำคัญให้ข้อมูลเป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง โดยระบุเจ้าของข้อมูลและเจ้าของระบบสารสนเทศ เพื่อควบคุมและกำหนดการเข้าใช้ข้อมูลสารสนเทศและสินทรัพย์สารสนเทศของ ทอท.

4.2 ให้มีการจัดชั้นข้อมูลสารสนเทศตามความสำคัญของข้อมูลสารสนเทศ กำหนดไว้ 5 ระดับ ได้แก่ ลับที่สุด ลับมาก ลับ ข้อมูลสารสนเทศที่ใช้เฉพาะภายใน และข้อมูลสารสนเทศเผยแพร่ โดยมีการป้องกันอย่างเหมาะสม รวมทั้งให้มีการกำหนดความรับผิดชอบให้แก่ผู้มีอำนาจกำหนดชั้นความลับ เป็นผู้พิจารณากำหนดระดับชั้นความลับของข้อมูลสารสนเทศ และการยกเลิกหรือปรับระดับชั้นความลับตามความจำเป็น

4.3 ให้มีการควบคุมข้อมูลสารสนเทศ เช่น การจัดทำเอกสาร การจัดทำทะเบียน การตรวจสอบ การสำเนา การแปล การโอน การส่ง การรับ การเก็บรักษา การยืม การทำลาย การสูญหาย การเปิดเผยข้อมูลสารสนเทศ และการปฏิบัติในเวลาฉุกเฉินตามการจัดชั้นข้อมูลสารสนเทศ

4.4 ให้มีการควบคุมการใช้สื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ เพื่อไม่ให้เกิดการรั่วไหลของข้อมูลสารสนเทศ หรือเสี่ยงต่อการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

4.5 สินทรัพย์สารสนเทศ ของ ทอท. จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อใช้ในภารกิจของ ทอท. เท่านั้น ห้ามผู้ใช้งานนำไปใช้ในกิจกรรมที่ ทอท. ไม่ได้กำหนด หรือเพื่อการประกอบธุระส่วนบุคคล ซึ่งอาจทำให้เกิดความเสียหายต่อ ทอท. หากพบความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อนี้ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นแต่เพียงผู้เดียว

4.6 ข้อมูลสารสนเทศของ ทอท. ถือเป็นสินทรัพย์สารสนเทศของ ทอท. ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าส่วนงานเจ้าของข้อมูลสารสนเทศและ/หรือ เจ้าของระบบสารสนเทศนั้นๆ

4.7 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบ ดูแล และรักษาสินทรัพย์สารสนเทศที่ ทอท. มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง การยืมหรือคืนสินทรัพย์จะต้องถูกบันทึกและตรวจสอบทุกครั้ง โดยเจ้าหน้าที่ผู้รับผิดชอบซึ่ง ทอท. ได้มอบหมายให้ดูแล

หมวด 5 การควบคุมการเข้าถึงระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์

เพื่อกำหนดการควบคุมการเข้าถึงและใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.ครอบคลุมการเข้าถึงระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ รวมถึงระบบงานหรือโปรแกรมประยุกต์และสารสนเทศ โดยมีการควบคุมและจัดการสิทธิการเข้าถึงและใช้งานอย่างเหมาะสม

เนื้อหานโยบาย

5.1 ให้มีการควบคุมการเข้าถึงและควบคุมการใช้งานสารสนเทศ ครอบคลุมข้อกำหนดการใช้งานตามภารกิจ

5.2 ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบทางเทคโนโลยีสารสนเทศและการสื่อสารเฉพาะผู้ที่ได้รับอนุญาตแล้ว

5.3 ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตการเปิดเผย การล่วงรู้ หรือ การลักลอบทำสำเนาข้อมูลสารสนเทศ

5.4 ให้มีการควบคุมการเข้าถึงระบบสารสนเทศ เฉพาะผู้ที่ได้รับอนุญาตแล้ว

5.5 ให้มีการควบคุมการเข้าถึงระบบเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

5.6 ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต และมีการกำหนดเวลาตัดการเชื่อมต่อหรือการจำกัดระยะเวลาการเชื่อมต่อ

5.7 ให้มีการควบคุมการเข้าถึงระบบงานหรือโปรแกรมประยุกต์ และข้อมูลสารสนเทศ โดยมีการจำกัดการเข้าถึง

5.8 ให้มีการควบคุมการเข้าถึงซอร์สโค้ด (รหัสต้นฉบับ) ของโปรแกรม ให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาต และให้มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging Record) แสดงการเข้าถึงโปรแกรมต้นฉบับให้เพียงพอในการตรวจสอบ การเข้าถึง เปลี่ยนแปลง และแก้ไขโปรแกรมต้นฉบับ

5.9 ให้มีการบริหารจัดการสิทธิการใช้งานหรือสิทธิพิเศษตามระดับสิทธิ โดยต้องมีการจำกัดและควบคุมในการให้สิทธิตามกลุ่มผู้ใช้งาน

5.10 ให้มีการจัดการสิทธิของผู้ใช้งานสำหรับการพัฒนาระบบ รวมทั้งต้องพัฒนาและทดสอบระบบสารสนเทศให้เป็นไปตามมาตรฐานฯ ที่กำหนด

5.11 ให้มีการทบทวนสิทธิการใช้งานบนระบบสารสนเทศตามมาตรฐานฯ ที่กำหนดโดยทบทวนสิทธิตามรอบระยะเวลา และเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมทั้งการถอดถอนและปรับปรุงสิทธิให้เป็นปัจจุบันเพื่อให้มั่นใจว่าไม่มีการกำหนดสิทธิเกินกว่าความจำเป็น

หมวด 6 การเข้ารหัสข้อมูล

วัตถุประสงค์

เพื่อให้ข้อมูลสารสนเทศมีความมั่นคงปลอดภัย รักษาไว้ซึ่งความลับ ความถูกต้อง และป้องกันการรั่วไหลของข้อมูลสารสนเทศ

เนื้อหานโยบาย

6.1 ให้มีการควบคุมการใช้งานการเข้ารหัสข้อมูลอิเล็กทรอนิกส์ และการใช้กุญแจสำหรับการเข้ารหัสเพื่อป้องกันข้อมูลที่มีความสำคัญ โดยมีการเข้ารหัสข้อมูลอิเล็กทรอนิกส์ให้สอดคล้องกับระดับชั้นความลับของข้อมูล

หมวด 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดให้มีการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงการปกป้องและป้องกันเกี่ยวกับการดูแลอุปกรณ์และระบบสนับสนุนสำหรับระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร

เนื้อหานโยบาย

7.1 ให้มีการกำหนดประเภทพื้นที่ควบคุมที่ต้องมีการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

7.2 ให้มีการป้องกันการเข้าถึงอุปกรณ์คอมพิวเตอร์และสื่อสารทางเทคโนโลยีสารสนเทศและการสื่อสาร

7.3 ให้มีการดูแลบำรุงรักษาระบบสนับสนุนและอำนวยความสะดวก (Facilities) สำหรับระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร

7.4 ให้มีการควบคุมการนำอุปกรณ์คอมพิวเตอร์และสื่อสารเข้า-ออกพื้นที่ควบคุม และบริหารจัดการอุปกรณ์คอมพิวเตอร์และสื่อสารที่ไม่มีการใช้งาน หรือการนำอุปกรณ์คอมพิวเตอร์และสื่อสารกลับมาใช้งานใหม่

7.5 ให้มีการรักษาความปลอดภัยทางกายภาพที่อาจเกิดขึ้นทั้งจากมนุษย์และ/หรือภัยธรรมชาติ

7.6 ให้มีการแยกพื้นที่สำหรับการติดต่อ หรือการรับ-ส่งของจากบุคคลภายนอกออกจากบริเวณที่มีทรัพย์สินสารสนเทศ

หมวด 8 ความปลอดภัยด้านการดำเนินงาน

วัตถุประสงค์

เพื่อกำหนดให้การปฏิบัติงานและดำเนินการระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. เป็นไปอย่างถูกต้อง ปลอดภัย และพร้อมใช้งานอยู่เสมอ โดยลดความเสี่ยงที่อาจเกิดขึ้นเป็นภัยคุกคามที่มีผลต่อการปฏิบัติงาน

เนื้อหานโยบาย

8.1 ให้มีการจัดทำขั้นตอนการปฏิบัติงาน โดยระบุผู้รับผิดชอบและหน้าที่ความรับผิดชอบอย่างชัดเจน

8.2 ให้มีการบริหารจัดการและควบคุมการเปลี่ยนแปลงของอุปกรณ์และซอฟต์แวร์ทั้งหมด (ซอฟต์แวร์ระบบสารสนเทศ ซอฟต์แวร์สำหรับอุปกรณ์คอมพิวเตอร์และสื่อสาร และซอฟต์แวร์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร)

8.3 ให้มีการตรวจสถานะการทำงานของระบบทางเทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ

8.4 ให้มีระบบป้องกันไวรัสคอมพิวเตอร์และโปรแกรมชุดคำสั่งที่ไม่พึงประสงค์

8.5 ให้มีการสำรองข้อมูลสารสนเทศและทดสอบสภาพพร้อมใช้งาน

8.6 ให้มีการบันทึกข้อมูลการใช้งาน (Log) ระบบที่มีความสำคัญ และสามารถตรวจสอบได้

8.7 ให้มีการตรวจประเมินระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร โดยเฉพาะดำเนินการตรวจสอบช่องโหว่ทางเทคนิค (Vulnerabilities Assessment) และการทดสอบเจาะระบบ (Penetration testing) สำหรับระบบสารสนเทศที่มีความสำคัญ

8.8 ให้มีการวางแผนก่อนดำเนินการตรวจประเมินระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อป้องกันเหตุขัดข้องในการทำงาน

หมวด 9 ความปลอดภัยด้านการสื่อสาร

วัตถุประสงค์

เพื่อบริหารจัดการระบบเครือข่ายและการส่งผ่านข้อมูลสารสนเทศไปยังหน่วยงานภายนอก อย่างมั่นคงปลอดภัย เพื่อป้องกันไม่ให้ข้อมูลสารสนเทศถูกเปิดเผยหรือแก้ไข

เนื้อหานโยบาย

9.1 ให้มีการบริหารจัดการและบำรุงรักษาระบบเครือข่าย เพื่อให้ระบบทางเทคโนโลยีสารสนเทศและการสื่อสารมีความมั่นคงปลอดภัย

9.2 ให้มีการควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศระหว่าง ทอท. กับหน่วยงานภายนอก อย่างปลอดภัย

หมวด 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร

วัตถุประสงค์

เพื่อให้การจัดหา การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร ได้พิจารณาถึงประเด็นด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

เนื้อหานโยบาย

10.1 ให้มีการพิจารณาถึงประเด็นด้านความมั่นคงปลอดภัย เพื่อเป็นองค์ประกอบพื้นฐานที่สำคัญในการจัดหา พัฒนา ติดตั้ง และบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสาร เมื่อมีการจัดหาระบบใหม่หรือพัฒนาต่อจากระบบเดิม

10.2 ให้มีการทดสอบระบบก่อนนำมาใช้งานจริง

10.3 ให้มีการควบคุมซอฟต์แวร์/เวอร์ชันซอฟต์แวร์ และโปรแกรมที่มีการติดตั้งสำหรับการใช้งานจริง

10.4 ให้มีการควบคุม กำกับดูแล ตรวจสอบ และเฝ้าระวังการพัฒนาระบบสารสนเทศที่ดำเนินการโดยหน่วยงานภายนอก

10.5 ให้มีการควบคุมข้อมูลสำคัญและเป็นความลับที่นำมาใช้ในการทดสอบ ซึ่งเมื่อนำข้อมูลดังกล่าวมาทดสอบควรทำการปกป้องข้อมูลด้วยการปิดบังข้อมูลสำคัญ (Data Masking) เพื่อไม่ให้ล่วงรู้ข้อมูลจริงได้

10.6 ให้มีการแบ่งแยกสภาวะแวดล้อมสำหรับการพัฒนาระบบสารสนเทศ ออกจากระบบสารสนเทศที่ใช้งานจริง

หมวด 11 ความปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก

วัตถุประสงค์

เพื่อบริหารจัดการผู้ให้บริการภายนอกให้มีการดำเนินการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นไปตามที่ ทอท. กำหนด

เนื้อหานโยบาย

11.1 ให้มีการบริหารจัดการผู้ให้บริการภายนอก โดยกำหนดเงื่อนไขที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร และมีการประเมินผลการให้บริการของผู้ให้บริการภายนอก

11.2 ให้มีการลงชื่อรับทราบข้อตกลงการรักษาความปลอดภัยสารสนเทศที่สอดคล้องกับนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ซึ่งรวมถึงความรับผิดชอบของบุคคลหรือหน่วยงานภายนอก หากเกิดความเสียหาย

หมวด 12 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

วัตถุประสงค์

เพื่อให้มีการจัดการเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของ ทอท. รวมทั้งสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ในช่วงระยะเวลาที่เหมาะสม

เนื้อหานโยบาย

12.1 ให้มีการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ที่เกี่ยวข้องในการใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. อย่างเหมาะสม

12.2 ให้มีช่องทางการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ที่เกี่ยวข้องในการใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

หมวด 13 การบริหารจัดการความต่อเนื่องด้านการดำเนินงาน

วัตถุประสงค์

เพื่อป้องกันการหยุดชะงักของการดำเนินงานทางธุรกิจ อันเป็นผลมาจากความล้มเหลวของระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร ของ ทอท. และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะที่กำหนด

เนื้อหานโยบาย

13.1 ให้มีแผนรองรับความต่อเนื่องในการดำเนินธุรกิจ และแผนเตรียมความพร้อมกรณีฉุกเฉิน สำหรับระบบสารสนเทศที่มีความสำคัญ ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้

13.2 ให้มีการทดสอบสภาพความพร้อมใช้และทบทวนปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง เพื่อนำผลการทดสอบมาปรับปรุงและพัฒนาแผนการบริหารการดำเนินธุรกิจอย่างต่อเนื่อง

13.3 ให้มีระบบสำรองสำหรับระบบสารสนเทศที่มีความสำคัญ

หมวด 14 การปฏิบัติตามกฎหมาย และข้อกำหนด

วัตถุประสงค์

เพื่อให้การดำเนินการทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. เป็นไปตามนโยบาย นโยบายสนับสนุน แนวทางการปฏิบัติงาน มาตรฐานการปฏิบัติงาน ขั้นตอนการปฏิบัติงาน ด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

เนื้อหานโยบาย

14.1 ให้ใช้งานซอฟต์แวร์ที่ได้รับลิขสิทธิ์หรือได้รับสิทธิให้ใช้งานได้ถูกต้องตามกฎหมายเท่านั้น หากมีการละเมิดอันเกิดจากผู้ใช้งาน โดย ทอท. จะไม่รับผิดชอบต่อความผิดที่เกิดขึ้นจากผู้ใช้งาน

14.2 ให้มีการป้องกันข้อมูลส่วนบุคคลไม่ให้ถูกเปิดเผย โดยเป็นไปตามระดับชั้นความลับของข้อมูล

14.3 ให้มีการตรวจทานการปฏิบัติงานให้สอดคล้องตามกฎหมาย ระเบียบ ข้อบังคับ นโยบาย นโยบายสนับสนุน แนวทางการปฏิบัติงาน มาตรฐานการปฏิบัติงาน ขั้นตอนการปฏิบัติงาน และวิธีการปฏิบัติงาน รวมถึงเอกสารอื่นใดที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. และกฎเกณฑ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยของระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. อย่างน้อยปีละ 1 ครั้ง

14.4 ให้มีการตรวจสอบระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. โดยส่วนงานที่รับผิดชอบการตรวจสอบภายในของ ทอท. หรือจากผู้ตรวจสอบภายนอก อย่างน้อยปีละ 1 ครั้ง

14.5 ให้มีการตรวจสอบเพื่อหาช่องโหว่หรือจุดอ่อนด้านเทคนิค เพื่อให้เกิดความเชื่อมั่นว่าระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ให้บริการมีความมั่นคงปลอดภัย

ภาคผนวก ก. มาตรฐานและข้อกำหนดอ้างอิง

มาตรฐาน	ISO/IEC 27001:2013 - Information Security Management System (ISMS) Requirements
ข้อกำหนด	Clause 5.2 Policy Annex 5.1.1 Policies for information Security

Guideline

แนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

AOT ICT Security Guideline

รหัสเอกสาร : Document No. GU-1608010-001

Version: 2

ผู้จัดทำเอกสาร

ส่วนมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสาร (สมส.)

ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสาร (ฝกท.)

โทรศัพท์ (800) 55300

เจ้าของเอกสาร

สายงานเทคโนโลยีดิจิทัลและการสื่อสาร (สงทส.)

รายละเอียดเอกสาร	
ประเภทเอกสาร :	แนวทางการปฏิบัติงาน (GU)
ผู้จัดทำเอกสาร :	ส่วนมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสาร (สมส.) ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสาร (ฝกท.)

ผู้ทบทวน	ผู้อนุมัติ
(นายธวัชชัย รัตนทองคง)	(นายกิตติพจน์ เวณุนันทน์)
ตำแหน่ง ผอก.ฝกท.	ตำแหน่ง รฝบท.
วันที่ 17 ต.ค. 66	วันที่ 17 ต.ค. 66

Version	วันที่บังคับใช้	ชื่อผู้จัดทำเอกสาร	สาระสำคัญของการแก้ไข/ปรับปรุง	หมายเหตุ
1	1 ตุลาคม 2561	น.ส.ฉัตรวดี ศิริโภค	เอกสารประกาศใช้ครั้งแรก	
2	ตุลาคม 2566	น.ส.ฉัตรวดี ศิริโภค	• แก้ไข Header • ทบทวนปรับปรุงสอดคล้องตามข้อกำหนดวิธีการแบบปลอดภัยในระดับเคร่งครัด พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 • ยกเลิกลำดับการแก้ไข • ปรับชื่อและรหัสตามโครงสร้างใหม่ • เพิ่มนิยาม เทคโนโลยีดิจิทัลและการสื่อสาร	

Version	วันที่บังคับใช้	ชื่อผู้จัดทำเอกสาร	สาระสำคัญของการแก้ไข/ปรับปรุง	หมายเหตุ
			• เพิ่มหลักเกณฑ์ที่อ้างอิงข้อ 1.8 - 1.11 • ปรับปรุงข้อมูล หมวด 3 ข้อ 3.3 (3) และ 3.5 (3) • ปรับปรุงข้อมูล หมวด 4 ข้อ 4.6, 4.7 และ 4.10 (2) • ปรับปรุงข้อมูล หมวด 5 ข้อ 5.6 (4.3) และ 5.7 (3) • ปรับปรุงข้อมูล หมวด 10 ข้อ 10.5 • ปรับปรุงข้อมูล หมวด 12 ข้อ 12.1 (6) • ปรับปรุงข้อมูล หมวด 13 ข้อ 13.5	

สารบัญ

หน้า

1. หลักเกณฑ์ที่อ้างอิง 5

2. หลักการและเหตุผล 6

3. ขอบเขต 6

4. คำนิยาม 7

หมวด 1 การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ 10

หมวด 2 การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร 11

หมวด 3 การสร้างความมั่นคงปลอดภัยด้านบุคลากร 12

หมวด 4 การบริหารจัดการสินทรัพย์สารสนเทศ 13

หมวด 5 การควบคุมการเข้าถึงระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร 16

หมวด 6 การเข้ารหัสข้อมูล 25

หมวด 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม 26

หมวด 8 ความปลอดภัยด้านการดำเนินงาน 29

หมวด 9 ความปลอดภัยด้านการสื่อสาร 32

หมวด 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร 33

หมวด 11 ความปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก 36

หมวด 12 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด 37

หมวด 13 การบริหารจัดการความต่อเนื่องด้านการดำเนินงาน 38

หมวด 14 การปฏิบัติตามกฎหมาย และข้อกำหนด 39

ภาคผนวก ก. มาตรฐานและข้อกำหนดอ้างอิง 40

1. หลักเกณฑ์ที่อ้างอิง

1.1 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

1.2 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551

1.3 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

1.3.1 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวทางการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

1.3.2 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวทางการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556

1.4 พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 (วิธีการแบบปลอดภัยในระดับเคร่งครัด)

1.5 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1.6 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

1.7 ประกาศบริษัท ท่าอากาศยานไทย จำกัด (มหาชน) เรื่อง นโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Policy) ณ วันที่ 1 ตุลาคม พ.ศ. 2561

1.8 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.8.1 ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1.8.2 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคาม ทางไซเบอร์แต่ละระดับ พ.ศ. 2564

1.9 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.10 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

2. หลักการและเหตุผล

เพื่อให้ระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ บริษัท ท่าอากาศยานไทย จำกัด (มหาชน) (ทอท.) มีความมั่นคงปลอดภัยในการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) สำหรับสินทรัพย์สารสนเทศและข้อมูลสารสนเทศสำคัญของ ทอท. ในการดำเนินธุรกิจให้พ้นจากภัยคุกคามและปัจจัยเสี่ยงทั้งจากภายในและภายนอกองค์กร ไม่ว่าจะเกิดขึ้นโดยเจตนาหรือไม่ก็ตาม พร้อมทั้งเพื่อลดความเสียหายต่างๆ ที่อาจเกิดขึ้นจากเหตุอันล่วงละเมิดด้านความมั่นคงปลอดภัย และเพื่อรักษาไว้ ซึ่งความสามารถในการดำเนินธุรกิจได้อย่างต่อเนื่อง และเป็นการปฏิบัติให้สอดคล้องตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องซึ่งมีผลบังคับใช้กับ ทอท. รวมทั้งเป็นการสร้างความเชื่อมั่นแก่พนักงาน ทอท. สายการบิน ผู้โดยสาร ผู้ใช้บริการท่าอากาศยาน และหน่วยงานทั้งภาครัฐและเอกชน ตลอดจนประชาชนทั่วไป ในการใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

3. ขอบเขต

แนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Guidelines) มีขอบเขตครอบคลุม ดังนี้

3.1 ระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งสินทรัพย์สารสนเทศของ ทอท. เช่น ระบบคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ ข้อมูลสารสนเทศ และระบบสารสนเทศ

3.2 ข้อมูลสารสนเทศสำคัญทั้งหมดในการดำเนินกิจการของ ทอท. ทั้งในส่วนที่เป็นอิเล็กทรอนิกส์และกระดาษ ตั้งแต่การสร้าง การจัดเก็บ การใช้งาน และการทำลาย

3.3 บุคคลที่มีส่วนเกี่ยวข้องในการดำเนินงานทางเทคโนโลยีสารสนเทศและการสื่อสาร ตลอดจนสินทรัพย์สารสนเทศและข้อมูลสารสนเทศของ ทอท. ได้แก่ ผู้บริหาร พนักงาน ลูกจ้าง ลูกจ้างทดลองปฏิบัติงาน บุคคลหรือหน่วยงานภายนอกที่มาใช้บริการหรือให้บริการที่เกี่ยวข้องกับระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. บุคคลหรือหน่วยงานภายนอกที่เป็นคู่สัญญากับ ทอท.

3.4 แนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Guidelines) มีเนื้อหาครอบคลุม 14 หมวด ดังนี้

หมวด 1 การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ
หมวด 2 การจัดโครงสร้างความมั่นคงปลอดภัยทางระบบเทคโนโลยีสารสนเทศและการสื่อสาร
หมวด 3 การสร้างความมั่นคงปลอดภัยด้านบุคลากร
หมวด 4 การบริหารจัดการสินทรัพย์สารสนเทศ
หมวด 5 การควบคุมการเข้าถึงระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร
หมวด 6 การเข้ารหัสข้อมูล
หมวด 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

หมวด 8 ความปลอดภัยด้านการดำเนินงาน

หมวด 9 การบริหารจัดการด้านการสื่อสาร

หมวด 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร

หมวด 11 ความปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก

หมวด 12 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

หมวด 13 การบริหารจัดการความต่อเนื่องด้านการดำเนินงาน

หมวด 14 การปฏิบัติตามกฎหมาย และข้อกำหนด

ทั้งนี้ หากบุคคลที่มีส่วนเกี่ยวข้องในการดำเนินงานทางเทคโนโลยีสารสนเทศและการสื่อสารตามข้อ 3.3 ดำเนินการต่างจากแนวทางการปฏิบัติงานนี้ บุคคลที่มีส่วนเกี่ยวข้องดังกล่าวต้องพิสูจน์ให้เห็นได้ว่าการดำเนินการนั้นยังคงอยู่ภายใต้หลักการและข้อกำหนดของแนวทางการปฏิบัติงานฉบับนี้

4. คำนิยาม

4.1 “พนักงาน” หมายความว่า พนักงาน ทอท. และลูกจ้าง ของ ทอท.

4.2 “หัวหน้าส่วนงาน” หมายความว่า ผู้อำนวยการฝ่าย/ศูนย์/สำนัก หรือผู้บริหารหน่วยงานในระดับเทียบเท่าของ ทอท.

4.3 “ผู้ใช้งานภายนอก” หมายความว่า บุคคลภายนอกที่มีสิทธิใช้ระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

4.4 “ผู้ใช้งาน” หมายความว่า พนักงาน ทอท. และผู้ใช้งานภายนอกที่เกี่ยวข้อง เข้าถึง หรือเข้าใช้งานสินทรัพย์สารสนเทศ และระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

4.5 “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิการใช้งาน สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดเกี่ยวข้องกับการใช้งานสินทรัพย์สารสนเทศ และระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

4.6 “สินทรัพย์” หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

4.7 “สินทรัพย์สารสนเทศ” หมายความว่า ทรัพย์สินสารสนเทศ* ระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีความหมายครอบคลุม ดังนี้

(1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(2) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

4.8 “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” (Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึง หรือใช้งานสินทรัพย์สารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

4.9 “ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Security) หมายความว่า ความมั่นคงปลอดภัยของสินทรัพย์สารสนเทศ ประกอบด้วย การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (non-Repudiation) และความน่าเชื่อถือ (Reliability)

4.10 “เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

4.11 “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information Security Incident) หมายความว่า เหตุขัดข้อง อุบัติการณ์ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

4.12 “การรักษาความลับ” (Confidentiality) หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันสินทรัพย์สารสนเทศ จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

4.13 “การรักษาความถูกต้องครบถ้วน” (Integrity) หมายความว่า การดำเนินการเพื่อให้สินทรัพย์สารสนเทศอยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งาน ประมวลผล โอนหรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

---

*ตามพระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2553 ทรัพย์สินสารสนเทศ หมายความว่า

(1) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(2) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(3) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

4.14 “การรักษาสภาพพร้อมใช้งาน” (Availability) หมายความว่า การจัดทำให้สินทรัพย์สารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

4.15 “การประเมินความเสี่ยงด้านสารสนเทศ” (Information Security Risk Assessment) หมายความว่า การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศสำหรับสินทรัพย์สารสนเทศของ ทอท.

4.16 “ระบบสารสนเทศ” หมายความว่า กลุ่มของระบบงานหรือโปรแกรมประยุกต์ที่ประกอบด้วยฮาร์ดแวร์หรือตัวอุปกรณ์ และซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บ และแจกจ่ายข้อมูลข่าวสาร เพื่อสนับสนุนการปฏิบัติงานของส่วนงานต่างๆ

4.17 “ระบบสารสนเทศที่มีความสำคัญ” หมายความว่า ระบบสารสนเทศหรือระบบงานหรือโปรแกรมประยุกต์ของ ทอท. ที่มีการประเมินว่ามีความสำคัญและมีผลกระทบต่อการดำเนินธุรกิจของ ทอท. หากระบบดังกล่าวหยุดชะงักหรือไม่สามารถให้บริการได้

4.18 “ส่วนงานที่ดูแลระบบการให้บริการ” หมายความว่า ส่วนงานที่รับผิดชอบดูแลระบบทางเทคโนโลยีสารสนเทศและการสื่อสารที่มีการให้บริการ (Production) ทั้งที่อยู่ในความรับผิดชอบของสายงานเทคโนโลยีดิจิทัลและการสื่อสาร และส่วนงานอื่นของ ทอท.

4.19 “เจ้าของระบบสารสนเทศ” หมายความว่า ส่วนงาน ทอท. ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการบริหารจัดการ กำกับดูแล และควบคุมการใช้งานระบบสารสนเทศของ ทอท. ให้สามารถดำเนินงานตามภารกิจของ ทอท. ได้อย่างครบถ้วนสมบูรณ์

4.20 “ข้อมูลสารสนเทศ” หมายความว่า ข่าวสาร ข้อเท็จจริง ข้อมูลในรูปแบบใดๆ หรือข้อมูลที่มีการประมวลผลใดๆ ทั้งในเหตุการณ์หรือกิจกรรมต่างๆ

4.21 “เจ้าของข้อมูลสารสนเทศ” หมายความว่า ส่วนงานที่มีหน้าที่รับผิดชอบในการกำหนดกระบวนการนำเข้า ปรับปรุง ประมวลผล และตรวจสอบความถูกต้องของข้อมูลสารสนเทศของ ทอท. ให้มีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ โดยเป็นผู้รับผิดชอบข้อมูลสารสนเทศ ซึ่งได้รับผลกระทบโดยตรงหากข้อมูลสารสนเทศเหล่านั้นเกิดเสียหายหรือสูญหาย

4.22 “อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่” หมายความว่า อุปกรณ์คอมพิวเตอร์และสื่อสารใดๆ ที่มีระบบปฏิบัติการสามารถประมวลผลได้ด้วยตัวเองเพื่อการเข้าถึง การใช้งานและจัดเก็บสารสนเทศ เช่น เครื่องคอมพิวเตอร์โน้ตบุ๊ค สมาร์ทโฟน แท็บเล็ต เป็นต้น

4.23 “สื่อบันทึกข้อมูลที่เคลื่อนย้ายได้” หมายความว่า สื่อหรืออุปกรณ์ที่ใช้ในการบันทึกข้อมูลที่เคลื่อนย้ายได้ เช่น เทป ฮาร์ดดิสก์ แฟลชไดร์ฟ แผ่นบันทึกข้อมูลซีดี/ดีวีดี เป็นต้น

4.24 “การใช้บริการหน่วยงานภายนอก” หมายความว่า การที่ ทอท. ได้มีการทำสัญญากับผู้ให้บริการภายนอกเพื่อดำเนินการแทนในบางกลุ่มงานที่โดยปกติ ทอท. ต้องดำเนินการเองทั้งหมดหรือบางส่วน รวมทั้งการติดต่อประสานกับผู้ให้บริการภายนอกเพื่อการนำเสนอหรือประชุมหารือเพื่อให้ข้อมูลสารสนเทศต่างๆ กับ ทอท.

4.25 “ระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร” หมายความว่า ระบบที่ประกอบด้วย อุปกรณ์คอมพิวเตอร์ ทั้งฮาร์ดแวร์ โปรแกรมคอมพิวเตอร์ อุปกรณ์เครือข่ายและสื่อสารข้อมูล ข้อมูลสารสนเทศและสื่อบันทึกข้อมูล ระบบสารสนเทศ สายสัญญาณและจุดเชื่อมต่อและอุปกรณ์ต่อพ่วงที่เกี่ยวข้อง

4.26 “เทคโนโลยีดิจิทัลและการสื่อสาร” หมายความว่า การนำเครื่องมือ อุปกรณ์คอมพิวเตอร์ ทั้งฮาร์ดแวร์ โปรแกรมคอมพิวเตอร์ อุปกรณ์เครือข่ายและสื่อสารข้อมูล ข้อมูลสารสนเทศ และสื่อบันทึกข้อมูล ระบบสารสนเทศ สายสัญญาณและจุดเชื่อมต่อและอุปกรณ์ต่อพ่วงที่เกี่ยวข้อง รวมทั้งอุปกรณ์ดิจิทัล อาทิ คอมพิวเตอร์ โทรศัพท์ แท็บเลต โปรแกรมคอมพิวเตอร์ และสื่อออนไลน์ มาใช้ให้เกิดประโยชน์สูงสุดในการสื่อสาร การปฏิบัติงาน และการทำงานร่วมกัน หรือใช้เพื่อพัฒนากระบวนการทำงาน หรือระบบงานในองค์กรให้มีความทันสมัยและมีประสิทธิภาพ

4.27 “ผู้ให้บริการภายนอก” หมายความว่า กลุ่มของบุคคลหรือบุคคลธรรมดาที่เป็นผู้ให้บริการภายนอกที่มีความเชี่ยวชาญเฉพาะด้านในงานหนึ่งงานใดเพื่อรับบทบาทการทำงานนั้นๆ

หมวด 1 การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

แนวทางการปฏิบัติงาน

1.1 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสารรับผิดชอบการจัดทำ ทบทวน ปรับปรุง ประกาศใช้และเผยแพร่ นโยบาย นโยบายสนับสนุน และแนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. โดยการนำเสนอกรรมการผู้อำนวยการใหญ่ ทอท. พิจารณาลงนามอนุมัติ เป็นประกาศและเผยแพร่ผ่านช่องทางประชาสัมพันธ์ภายในองค์กร เพื่อให้ผู้ใช้งานรับทราบและถือปฏิบัติโดยทั่วกัน

1.2 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสารรับผิดชอบการทบทวนปรับปรุงนโยบายและแนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. เป็นประจำทุก 2 ปี หรือปรับปรุงทันทีเมื่อมีความจำเป็น/หรือเมื่อมีการเปลี่ยนแปลงซึ่งมีนัยสำคัญที่ส่งผลต่อการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

1.3 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสาร ร่วมกับส่วนงานที่เกี่ยวข้อง กำหนดกรอบบริหารความเสี่ยงและขั้นตอนการปฏิบัติงานการประเมินความเสี่ยงด้านสารสนเทศ มีการกำหนดเกณฑ์ความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้ พร้อมทั้งการกำหนดแนวทางการปฏิบัติงานในการควบคุมความเสี่ยงอย่างเหมาะสม โดยกำหนดให้มีการประเมินความเสี่ยงด้านสารสนเทศเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลง พร้อมทั้งทบทวนปรับปรุงนโยบาย นโยบายสนับสนุน แนวทางการปฏิบัติงาน มาตรฐานการปฏิบัติงาน และขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยอย่างเหมาะสมตามสภาพความเสี่ยงของ ทอท. เพื่อนำเสนอผู้บริหารพิจารณาอนุมัติ

หมวด 2 การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร

แนวทางการปฏิบัติงาน

2.1 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสาร และส่วนงาน ทอท. ที่เกี่ยวข้อง นำเสนอแผนงานโครงการด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ต่อคณะกรรมการบริหารเทคโนโลยีดิจิทัลและการสื่อสารของ ทอท. เพื่อพิจารณาอนุมัติ

2.2 ให้คณะทำงานบริหารความเสี่ยงและควบคุมภายในของสายงานเทคโนโลยีดิจิทัลและการสื่อสาร มีหน้าที่รับผิดชอบในการพิจารณาและให้ความเห็นแนวทางการบริหารความเสี่ยงด้านสารสนเทศ ของ ทอท.

2.3 หัวหน้าส่วนงานมีหน้าที่สนับสนุนเจ้าหน้าที่ในสังกัดในการปฏิบัติตามนโยบาย นโยบายสนับสนุน และแนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

2.4 ให้ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสารรวบรวมจัดทำรายชื่อและข้อมูลสำหรับการประสานงานระหว่างส่วนงานภายใน ทอท. หรือติดต่อกับหน่วยงานภายนอก ทอท. หรือผู้เชี่ยวชาญที่เกี่ยวข้องเพื่อดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ เช่น แผนรองรับความต่อเนื่องทางธุรกิจหรือแผนฉุกเฉินกรณีที่ระบบทางเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถใช้งานได้ ข่าวสารที่เกี่ยวกับไวรัสคอมพิวเตอร์และการป้องกันไวรัสคอมพิวเตอร์

2.5 ส่วนงานที่ดูแลระบบการให้บริการ มีหน้าที่ควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสาร และอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ มาใช้งานตามภารกิจหน้าที่และการดำเนินธุรกิจของ ทอท. ดังนี้

(1) ให้ใช้งานได้เฉพาะอุปกรณ์คอมพิวเตอร์และสื่อสาร และอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ ทอท. ติดตั้งและจัดหาให้ใช้งาน

(2) ให้ใช้งานได้เฉพาะอุปกรณ์คอมพิวเตอร์และสื่อสาร และอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ของส่วนตัว ที่ได้รับอนุญาตให้ใช้งาน โดยต้องลงทะเบียนการใช้งานกับสายงานเทคโนโลยีดิจิทัลและการสื่อสาร รวมทั้งต้องควบคุมไม่ให้มีการนำอุปกรณ์คอมพิวเตอร์และสื่อสารทุกชนิดเชื่อมต่อกับระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร ของ ทอท. โดยไม่ได้รับอนุญาตจากส่วนงานดูแลระบบการให้บริการ โดยมีการดำเนินการอย่างน้อย ดังนี้

(2.1) เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์โน้ตบุ๊ค เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์อื่นใดที่ส่วนงานดูแลระบบการให้บริการพิจารณาแล้วเข้าข่ายอุปกรณ์ข้างต้น ที่เป็นของส่วนตัวหรือ ที่ ทอท. ไม่ได้จัดหาให้ใช้งาน ต้องลงทะเบียนการใช้งานเครื่องกับส่วนงานดูแลระบบการให้บริการ

(2.2) สมาร์ทโฟน แท็ปเล็ต และอุปกรณ์อื่นใดที่ส่วนงานดูแลระบบการให้บริการพิจารณาแล้วเข้าข่ายอุปกรณ์ข้างต้น ที่เป็นของส่วนตัวหรือที่ ทอท. ไม่ได้จัดหาให้ใช้งาน ต้องลงทะเบียนผู้ใช้งานผ่านระบบที่ ทอท. จัดหาให้ใช้งาน

2.6 ส่วนงานที่ดูแลระบบการให้บริการ มีหน้าที่ควบคุมการนำอุปกรณ์คอมพิวเตอร์และสื่อสารทุกประเภท ทั้งที่ ทอท. จัดหาให้ใช้งาน และที่เป็นของส่วนตัว มาใช้ในการเข้าถึงระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร จากภายนอกองค์กรเพื่อพัฒนา ปรับปรุง และบำรุงรักษาระบบ ดังนี้

(1) ผู้มีความประสงค์จะขอใช้งานต้องร้องขอการใช้งานเป็นลายลักษณ์อักษร โดยได้รับอนุญาตจากส่วนงานดูแลระบบการให้บริการหรือส่วนงานสายงานเทคโนโลยีดิจิทัลและการสื่อสารที่รับผิดชอบเพื่อดำเนินการ

(2) ต้องมีรายละเอียดอย่างน้อย ดังนี้ รายละเอียดของผู้ร้องขอ (ชื่อ/นามสกุล รหัสพนักงาน สังกัด สถานที่ปฏิบัติงาน) แผนงาน (ถ้ามี) เหตุผลความจำเป็น วัตถุประสงค์ ระบบสารสนเทศ/ระบบทางเทคโนโลยีสารสนเทศ วิธีการเข้าถึง ระยะเวลา (จำนวนวันหรือเดือน) ช่วงเวลาที่ขอเข้าใช้

(3) ตรวจทานการเข้าดำเนินการดังกล่าวตามที่ได้ร้องขอ

หมวด 3 การสร้างความมั่นคงปลอดภัยด้านบุคลากร

แนวทางการปฏิบัติงาน

3.1 หัวหน้าส่วนงานร่วมกับส่วนงานด้านทรัพยากรบุคคล จัดทำคำอธิบายแบบบรรยายลักษณะงาน (Job Description) ซึ่งระบุหน้าที่ตามภารกิจและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของพนักงานที่เกี่ยวข้องอย่างชัดเจน โดยมีข้อพิจารณาเพื่อดำเนินการ ดังนี้

(1) มีขั้นตอนปฏิบัติในการตรวจสอบคุณสมบัติและการคัดเลือกเจ้าหน้าที่เพื่อปฏิบัติงานหรือเข้าใช้ระบบสารสนเทศอย่างรัดกุมโดยเฉพาะในตำแหน่งงานที่เกี่ยวข้องกับระดับข้อมูลสารสนเทศที่สำคัญ

(2) มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีผู้ปฏิบัติงานหลักไม่สามารถดำเนินการได้

(3) ระบุความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ ในเงื่อนไขการจ้างงาน

3.2 ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสารร่วมกับส่วนงานด้านทรัพยากรบุคคลจัดทำข้อตกลงการไม่เปิดเผยข้อมูลสำหรับผู้ใช้งาน เพื่อให้ตระหนักถึงการไม่เปิดเผยข้อมูลสารสนเทศสำคัญหรือข้อมูลความลับของ ทอท. เพื่อป้องกันการรั่วไหลของข้อมูลสารสนเทศ

3.3 สายงานเทคโนโลยีดิจิทัลและการสื่อสารร่วมกับส่วนงานด้านพัฒนาทรัพยากรบุคคลจัดให้มีการฝึกอบรมหลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศให้กับผู้ใช้งานเป็นประจำทุกปี เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยมีเนื้อหาอย่างน้อย ดังนี้

(1) หัวข้อเกี่ยวกับการสร้างความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงแนวทางการป้องกัน

(2) หัวข้อเกี่ยวกับการบริหารจัดการการเข้าถึงของผู้ใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน ครอบคลุมเรื่องการใช้งานสินทรัพย์สารสนเทศ การลงทะเบียนผู้ใช้งาน การบริหารจัดการสิทธิของผู้ใช้งาน การบริหารจัดการรหัสผ่าน และการทบทวนสิทธิของผู้ใช้งาน

(3) หัวข้อเกี่ยวกับกฎหมาย กฎระเบียบ นโยบาย นโยบายสนับสนุนและแนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงกระบวนการทางวินัยเมื่อพบความผิดฐานละเมิดการรักษาความปลอดภัยสารสนเทศ เพื่อให้ปฏิบัติตามได้อย่างถูกต้องเหมาะสม

3.4 หัวหน้าส่วนงาน มีหน้าที่สนับสนุนให้พนักงานหรือบุคลากรในสังกัด เข้ารับการอบรม หรือเข้าร่วมรับการให้ความรู้ ดังนี้

(1) การปฏิบัติงานตามภารกิจและหน้าที่ความรับผิดชอบ

(2) การสร้างความตระหนักความมั่นคงปลอดภัยสารสนเทศตามข้อ 3.3

3.5 ในกรณีที่ยุติการว่าจ้างหรือเปลี่ยนแปลงหน้าที่งาน หัวหน้าส่วนงานมีหน้าที่ดำเนินการให้บุคลากรในสังกัดดำเนินการ ดังนี้

(1) ดำเนินการตามขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับส่วนงานด้านทรัพยากรบุคคล สำหรับผู้ที่สิ้นสุดการว่าจ้าง เลิกจ้าง หรือ เปลี่ยนแปลงหน้าที่งานจากเดิม

(2) ดำเนินการร่วมกับส่วนงานเจ้าของระบบสารสนเทศหรือเจ้าของข้อมูลสารสนเทศ หรือ ส่วนงานที่เกี่ยวข้อง เพื่อยกเลิกสิทธิหรือเปลี่ยนแปลงสิทธิในการเข้าใช้สินทรัพย์สารสนเทศ ของ ทอท. สำหรับผู้ที่สิ้นสุดการว่าจ้าง เลิกจ้าง หรือ เปลี่ยนแปลงหน้าที่งานจากเดิม เมื่อสิ้นสุดการปฏิบัติงาน และให้มีการตรวจสอบการดำเนินการยกเลิกสิทธิดังกล่าวโดยหัวหน้าส่วนงานต้นสังกัด

(3) ดำเนินการแจ้งพนักงาน และผู้ใช้งานจากหน่วยงานภายนอกให้ส่งคืนทรัพย์สินทั้งหมดขององค์กรที่อยู่ในครอบครอง เมื่อสิ้นสุดการจ้างงาน สัญญาจ้างหรือข้อตกลง

หมวด 4 การบริหารจัดการสินทรัพย์สารสนเทศ

แนวทางการปฏิบัติงาน

4.1 การจัดชั้นข้อมูลสารสนเทศ เป็นการกำหนดลำดับชั้นความลับของข้อมูลสารสนเทศ ดังนี้

(1) ลับที่สุด (Top Secret) หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ของ ทอท. อย่างร้ายแรงที่สุด

(2) ลับมาก (Secret) หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์ของ ทอท. อย่างร้ายแรง

(3) ลับ (Confidential) หมายถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ของ ทอท.

(4) ข้อมูลสารสนเทศที่ใช้เฉพาะภายใน (Internal Use) หมายถึง ข้อมูลข่าวสารที่กำหนดให้ใช้เฉพาะส่วนงานหรือภายใน ทอท. ซึ่งมีการจำกัดการเข้าถึงหรือใช้งานได้เฉพาะกลุ่ม โดยมิให้เปิดเผยต่อผู้ที่ไม่เกี่ยวข้องโดยไม่ได้รับอนุญาต

(5) ข้อมูลสารสนเทศเผยแพร่ (Public) หมายถึง ข้อมูลข่าวสารที่สามารถเผยแพร่ได้ โดยมีการควบคุมที่เหมาะสม

4.2 เวลาการเข้าถึงหรือการเข้าใช้งานสินทรัพย์สารสนเทศ กำหนดดังนี้

(1) การเข้าถึงสินทรัพย์สารสนเทศในเวลาราชการ (8.00-17.00 น.)

(2) การเข้าถึงสินทรัพย์สารสนเทศนอกเวลาราชการ (17.00-08.00 น.)

(3) การเข้าถึงสินทรัพย์สารสนเทศในช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

(4) การเข้าถึงสินทรัพย์สารสนเทศ 24 ชั่วโมง (ทุกช่วงเวลา)

(5) การเข้าถึงสินทรัพย์สารสนเทศในช่วงเวลาพิเศษเป็นรายครั้ง โดยระบุช่วงเวลาและจำนวนระยะเวลา ได้แก่ จำนวนวัน จำนวนสัปดาห์ จำนวนเดือน ตามเวลาที่ร้องขอ

4.3 ช่องทางการเข้าถึงหรือการเข้าใช้งานสินทรัพย์สารสนเทศ กำหนดดังนี้

(1) ติดต่อด้วยตนเอง

(2) เคาน์เตอร์บริการ

(3) หนังสือหรือบันทึกข้อความ

(4) โทรศัพท์หรือโทรสาร

(5) ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)

(6) ระบบสารสนเทศ

(7) ระบบอินทราเน็ตหรือช่องทางสื่อสารภายใน ทอท.

(8) ระบบอินเทอร์เน็ตหรือช่องทางสื่อสารภายนอก ทอท.

(9) วงจรการเชื่อมต่อโดยตรง

(10) ระบบการประชุมและการทำงานร่วมกันทางอิเล็กทรอนิกส์

4.4 ให้ส่วนงานที่ดูแลระบบการให้บริการ จัดทำรายการทะเบียนสินทรัพย์สารสนเทศที่อยู่ในความรับผิดชอบเพื่อให้ทราบถึงสินทรัพย์สารสนเทศสำคัญในการรักษาความมั่นคงปลอดภัยสารสนเทศ และมีการทบทวนรายการสินทรัพย์สารสนเทศให้เป็นปัจจุบันอย่างสม่ำเสมอ

4.5 ให้ส่วนงานที่ดูแลระบบการให้บริการร่วมกับส่วนงาน ทอท. ที่เกี่ยวข้องระบุส่วนงานผู้เป็นเจ้าของหรือผู้ดูแลสินทรัพย์สารสนเทศในระดับฝ่าย โดยเฉพาะการระบุเจ้าของข้อมูลสารสนเทศหรือเจ้าของระบบสารสนเทศเพื่อควบคุมการเข้าถึงและการเข้าใช้งานสินทรัพย์สารสนเทศ

4.6 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสารร่วมกับส่วนงานที่เกี่ยวข้อง จัดทำข้อตกลงการใช้งานสินทรัพย์สารสนเทศของ ทอท. (Acceptable Use Agreement) เพื่อให้ผู้ใช้งานได้รับทราบและปฏิบัติโดยตระหนักและระมัดระวังต่อการใช้งานสินทรัพย์สารสนเทศให้สอดคล้องตามนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Policy) รวมทั้งนโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Supporting Policy) และแนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Guideline)

4.7 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสารร่วมกับส่วนงานที่เกี่ยวข้อง หรือส่วนงานเจ้าของข้อมูลสารสนเทศจัดทำข้อปฏิบัติการจัดชั้นข้อมูลสารสนเทศให้สอดคล้องตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 โดยการจำแนกตามชั้นความลับ ข้อมูลที่ใช้เฉพาะภายใน ทอท. และข้อมูลเผยแพร่/ข้อมูลข่าวสารทั่วไป พร้อมทั้งกำหนดข้อปฏิบัติในการจัดการ ปกป้อง รักษา จัดเก็บ และทำลายอย่างเหมาะสม รวมทั้งการจัดทำป้ายสัญลักษณ์ (Labeling) สำหรับข้อมูลสารสนเทศที่มีความสำคัญ ตามลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลสารสนเทศ

4.8 ในกรณีที่ยุติการว่าจ้างหรือเปลี่ยนแปลงหน้าที่งาน หัวหน้าส่วนงานมีหน้าที่ดำเนินการให้บุคลากรในสังกัดดำเนินการเรื่องการส่งคืนสินทรัพย์สารสนเทศ ทอท. ของผู้ที่สิ้นสุดการว่าจ้าง เลิกจ้าง หรือเปลี่ยนแปลงหน้าที่งานจากเดิม ที่มีสินทรัพย์สารสนเทศอยู่ในความครอบครอง เมื่อสิ้นสุดการปฏิบัติงาน

4.9 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสาร ร่วมกับส่วนงานที่เกี่ยวข้อง ควบคุมสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ ดังนี้

(1) สื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ที่สามารถนำมาใช้งานภายใน ทอท. ประกอบด้วย เทป แฟลชไดร์ฟ แผ่นบันทึกข้อมูลซีดี/ดีวีดี และกระดาษ

ยกเว้นการใช้งานสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้กับอุปกรณ์คอมพิวเตอร์และสื่อสารใดๆ ที่ส่วนงานดูแลระบบการให้บริการประเมินแล้วว่า อาจทำให้เกิดความเสียหายกับระบบสารสนเทศที่สำคัญของ ทอท. หรือส่งผลต่อการให้บริการท่าอากาศยานในความรับผิดชอบของ ทอท.

(2) สื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ที่ได้รับอนุญาตให้ใช้งานที่มีการบันทึกข้อมูลอิเล็กทรอนิกส์ที่สามารถสแกนไวรัสได้ ต้องได้รับการสแกนไวรัสคอมพิวเตอร์ ก่อนการเปิดใช้งานข้อมูลสารสนเทศทุกครั้ง

(3) ต้องทำลายข้อมูลสารสนเทศของ ทอท. ที่บันทึกอยู่ในสื่อบันทึกข้อมูลก่อนทำการเปลี่ยน ทดแทน ทำลายหรือจำหน่ายสื่อบันทึกข้อมูล ด้วยวิธีการที่ได้มาตรฐาน ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
แฟลชไดร์ฟ	ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่นบันทึกข้อมูลซีดี/ดีวีดี	หัก หรือใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการตัดทำลายเนื้อเทป ทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการ Zero fill ซึ่งอ้างอิงตามมาตรฐาน NIST 800-88 การทำลายข้อมูลบนฮาร์ดดิสก์
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร หรือเผาทำลาย

4.10 ส่วนงานที่ดูแลระบบการให้บริการ ต้องจัดให้มีขั้นตอนการปฏิบัติงานการขนย้ายสื่อบันทึกข้อมูลที่มีการสำรองข้อมูลของ ทอท. (backup) โดย

(1) ต้องได้รับการป้องกันการเข้าถึงโดยบุคคลภายนอก เช่น ใส่กระเป๋าที่มีรหัสเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(2) ต้องขนย้ายด้วยวิธีที่ไม่ทำให้สื่อบันทึกข้อมูลเสียหาย เพื่อเป็นการป้องกันการรั่วไหลของข้อมูลสารสนเทศที่อาจจะเกิดขึ้นได้ และให้สื่อบันทึกข้อมูลและอุปกรณ์สารสนเทศมีความพร้อมใช้

(3) มีการบันทึกข้อมูลการรับ-ส่งสื่อบันทึกข้อมูล

หมวด 5 การควบคุมการเข้าถึงระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร

<u>แนวทางการปฏิบัติงานการควบคุมการเข้าถึงระบบสารสนเทศ</u>

5.1 เจ้าของระบบสารสนเทศหรือเจ้าของข้อมูลสารสนเทศ มีหน้าที่กำหนดกลุ่มผู้ใช้งาน และกำหนดระดับชั้นการเข้าถึง โดยกำหนดสิทธิของผู้ใช้งาน รวมถึงการยกเลิกสิทธิหรือเปลี่ยนแปลงสิทธิ และการทบทวนสิทธิของผู้ใช้งานสำหรับการใช้ข้อมูลสารสนเทศหรือระบบที่อยู่ในความรับผิดชอบ โดยมีแนวทางดำเนินการ ดังนี้

(1) กำหนดกลุ่มผู้ใช้งานและสิทธิของผู้ใช้งาน โดยอนุญาตให้สิทธิการใช้งานเมื่อได้รับการร้องขอจากผู้ใช้งาน ซึ่งผ่านความเห็นชอบจากหัวหน้าส่วนงานต้นสังกัดของผู้ใช้งาน

(2) พิจารณากำหนดกลุ่มผู้ใช้งานและสิทธิของผู้ใช้งาน โดยพิจารณาประเด็นสำหรับการใช้งาน ดังนี้

(2.1) ตามภารกิจและหน้าที่ที่ได้รับมอบหมายของผู้ใช้งาน

(2.2) หลักการตามความจำเป็นต่อการใช้งาน

(3) กำหนดกลุ่มผู้ใช้งาน ดังนี้

(3.1) ผู้ใช้งาน (User)

(3.2) ผู้ดูแลระบบ (System Administrator)

(3.3) ผู้ดูแลข้อมูลหรือฐานข้อมูล (Database Administrator)

(3.4) ผู้พัฒนาหรือสนับสนุนการใช้งานระบบสารสนเทศ (Programmer, Developer, Application Support)

(3.5) อื่นๆ (ตามฟังก์ชั่นของระบบสารสนเทศ)

(4) กำหนดสิทธิของผู้ใช้งาน ดังนี้

(4.1) สิทธิของผู้ใช้งานทั่วไป

(4.2) สิทธิพิเศษ คือสิทธิของผู้ใช้งานที่ต้องเข้าถึงระบบสารสนเทศที่ไม่ใช่หน้าที่ความรับผิดชอบโดยปกติ แต่มีความจำเป็นต้องเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนด

(4.3) สิทธิระดับสูง ได้แก่ สิทธิของผู้ดูแลระบบ/ผู้ดูแลข้อมูล หรือผู้ดูแลฐานข้อมูล/ผู้ที่ได้รับมอบหมายดูแลจัดการสารสนเทศหรือดำเนินการด้านระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร ที่เกี่ยวข้องในการให้บริการระบบ

(4.4) สิทธิสูงสุดของผู้ดูแลระบบที่กำหนดมากับระบบตั้งแต่เริ่มต้น (Default)

(4.5) สิทธิอื่นๆ ในการสนับสนุนการใช้งานระบบ

(5) กำหนดสิทธิการเข้าถึงหรือสิทธิการใช้งาน ดังนี้

(5.1) อ่านอย่างเดียว (Read Only)

(5.2) นำเข้าข้อมูล (Insert/Create)

(5.3) แก้ไข (Update)

(5.4) ลบข้อมูล (Delete)

(5.5) อนุมัติ (Approve)

(5.6) ไม่มีสิทธิ (Not Allow)

(6) ยกเลิกสิทธิหรือเปลี่ยนแปลงสิทธิของผู้ใช้งาน ตามที่ได้รับแจ้งจากส่วนงานด้านทรัพยากรบุคคลหรือส่วนงานต้นสังกัด ในข้อใดข้อหนึ่ง ดังนี้

(6.1) เมื่อผู้ใช้งานสิ้นสุดการว่าจ้างจาก ทอท.

(6.2) เมื่อมีการเปลี่ยนแปลงตำแหน่งหน้าที่งาน

(7) ทบทวนสิทธิของผู้ใช้งาน เมื่อครบกำหนดรอบระยะเวลาตามที่กำหนดในกระบวนการทบทวนสิทธิของผู้ใช้งานสำหรับระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

(8) พิจารณาการควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย (รายละเอียดตามข้อปฏิบัติในหัวข้อ หมวด 4 การบริหารจัดการสินทรัพย์สารสนเทศ) ดังนี้

(8.1) การจัดชั้นข้อมูลสารสนเทศ

(8.2) เวลาการเข้าถึงหรือการเข้าใช้งาน

(8.3) ช่องทางการเข้าถึงหรือการเข้าใช้งาน

(8.4) สิทธิของผู้ใช้งานตามกลุ่มผู้ใช้งาน

(9) เจ้าของระบบสารสนเทศหรือเจ้าของข้อมูลสารสนเทศต้องจัดให้มีผู้ปฏิบัติงานในระดับการอนุมัติการเข้าถึงข้อมูลสารสนเทศและระบบสารสนเทศให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง

(10) กรณีเป็นระบบสารสนเทศหลักหรือระบบที่มีการใช้งานร่วมกันจากหลายส่วนงานซึ่งไม่ได้กำหนดเจ้าของระบบสารสนเทศ ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสารเป็นผู้ดำเนินการระบุส่วนงานเจ้าของระบบและเจ้าของข้อมูลสารสนเทศ เพื่อกำหนดความรับผิดชอบให้กับผู้ดูแลระบบ (System Administrator) ในการอนุมัติสิทธิในการใช้งาน (Authorized Owner)

5.2 ส่วนงานที่ดูแลระบบการให้บริการร่วมกับส่วนงานสายงานเทคโนโลยีดิจิทัลและการสื่อสารและเจ้าของระบบสารสนเทศ มีหน้าที่จำแนกกลุ่มทรัพยากรของระบบและการทำงานด้านระบบทางเทคโนโลยีสารสนเทศและการสื่อสารในส่วนที่รับผิดชอบ สำหรับสนับสนุนการปฏิบัติงานในการควบคุมการเข้าถึงข้อมูลสารสนเทศและระบบสารสนเทศ โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยตามที่กำหนดของระบบสารสนเทศแต่ละระบบ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

<u>แนวทางการปฏิบัติงานการบริหารจัดการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน</u>

5.3 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่จัดให้มีขั้นตอนการปฏิบัติงานและดำเนินการตามขั้นตอนการปฏิบัติงานสำหรับการลงทะเบียนผู้ใช้งานและการยกเลิกสิทธิผู้ใช้งาน โดยมีข้อปฏิบัติ ดังนี้

(1) กำหนดให้มีขั้นตอนการลงทะเบียนผู้ใช้งานและการยกเลิกสิทธิผู้ใช้งาน สำหรับผู้ใช้งานทั้งที่เป็นพนักงาน ทอท. และผู้ใช้งานภายนอก โดยมีใบร้องขอจากผู้ใช้งานที่ได้รับความเห็นชอบจากหัวหน้าส่วนงานต้นสังกัดหรือผู้มีอำนาจลงชื่ออนุมัติของหน่วยงานนั้นๆ

(2) จัดทำทะเบียนคุมโดยมีรายละเอียดของส่วนงาน ชื่อ-สกุล และตำแหน่ง สิทธิที่ได้รับ จัดทำไว้เป็นหลักฐาน

(3) กำหนดชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน โดยผู้ใช้งานทุกคนต้องมีชื่อบัญชีผู้ใช้งานของตนเอง

(4) กรณีเป็นข้อจำกัดของระบบ หรือมีความจำเป็นต้องมีการใช้งานชื่อบัญชีผู้ใช้งานร่วมกัน ต้องได้รับอนุญาตจากหัวหน้าส่วนงานเจ้าของระบบสารสนเทศหรือส่วนงานเจ้าของข้อมูลสารสนเทศ โดยระบุชื่อผู้ใช้งานและจำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน

5.4 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่จัดการ ยกเลิก หรือเปลี่ยนแปลงสิทธิของผู้ใช้งานตามที่ได้รับอนุมัติโดยเจ้าของระบบสารสนเทศหรือส่วนงานเจ้าของข้อมูลสารสนเทศ

5.5 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่สนับสนุนและจัดให้มีการทบทวนสิทธิของผู้ใช้งานอย่างสม่ำเสมอ โดยจัดส่งรายชื่อผู้ใช้งานปัจจุบันในระบบสารสนเทศและทะเบียนควบคุมให้กับส่วนงาน ทอท. หรือหน่วยงานภายนอกที่ได้รับสิทธิ เจ้าของระบบสารสนเทศและเจ้าของข้อมูลสารสนเทศ พิจารณาทบทวนอย่างน้อยปีละ 1 ครั้ง

5.6 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่บริหารจัดการรหัสผ่านของผู้ใช้งาน ครอบคลุมการออกรหัสผ่านและการเปลี่ยนรหัสผ่านตามกระบวนการที่กำหนด และสอดคล้องตามมาตรฐาน ISO/IEC 27001, ISO/IEC 27002 โดยมีข้อปฏิบัติ ดังนี้

(1) รหัสผ่านถือเป็นข้อมูลระดับชั้นความลับ จึงต้องรักษารหัสผ่านไม่ให้มีผู้อื่นใดที่ไม่ใช่ผู้ใช้งานสามารถเข้าถึงหรือล่วงรู้ได้

(2) ทุกครั้งที่มีการตั้งค่ารหัสผ่านใหม่ (Reset) ต้องมีการเก็บบันทึก หรือมีใบร้องขอจากผู้ใช้งาน

(3) ปฏิบัติตามข้อกำหนดในเรื่องการกำหนดค่ารหัสผ่าน โดยมีแนวทางดำเนินการตั้งรหัสผ่านที่ยากต่อการคาดเดา เช่น ไม่ใช้ข้อมูลส่วนตัวมาเป็นรหัสผ่าน ไม่ใช้คำที่มีในพจนานุกรม และมีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยให้มีอักขระพิเศษและตัวเลข เป็นต้น ทั้งนี้ กรณีที่เป็นข้อจำกัดของระบบให้จัดทำบันทึกแจ้งให้หัวหน้าส่วนงานหรือผู้บังคับบัญชารับทราบ

(4) กรณีผู้ใช้งานเป็นผู้ที่ได้รับสิทธิพิเศษ หรือสิทธิระดับสูง ต้องมีการควบคุมรหัสผ่านในการเข้าใช้งานอย่างรัดกุม โดยมีแนวทางดำเนินการอย่างน้อย ดังนี้

(4.1) ได้รับความเห็นชอบเป็นลายลักษณ์อักษร จากหัวหน้าส่วนงานต้นสังกัดหรือผู้มีอำนาจหน้าที่

(4.2) กำหนดระยะเวลาในการใช้งาน และให้ระงับทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4.3) กำหนดให้มีการเปลี่ยนรหัสผ่านใหม่ภายหลังจากการขออนุมัติใช้งาน หรืออย่างน้อยทุก 6 เดือน

(4.4) กำหนดรหัสผ่านให้มีระดับความปลอดภัยที่เหมาะสมและรัดกุม โดยกำหนดให้มีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยให้มีอักขระพิเศษและตัวเลข

(4.5) กำหนดให้ไม่ใช้ข้อมูลส่วนตัวหรือคำที่มีในพจนานุกรมมาเป็นรหัสผ่าน

(4.6) กำหนดให้ผู้ใช้งานป้อนรหัสผ่านผิดต่อเนื่องกันได้ไม่เกิน 3 ครั้ง

(4.7) กำหนดให้เปลี่ยนรหัสผ่านไม่ซ้ำรหัสผ่านเดิมที่ผ่านมาอย่างน้อย 3 ครั้งสุดท้าย

(4.8) กำหนดการทบทวนสิทธิสำหรับผู้มีสิทธิพิเศษหรือผู้มีสิทธิในระดับสูง เป็นประจำทุก 6 เดือน

(4.9) กรณีที่เป็นข้อจำกัดของระบบสารสนเทศ ให้จัดทำบันทึกแจ้งให้หัวหน้าส่วนงานหรือผู้บังคับบัญชารับทราบ

(5) มีวิธีการที่รัดกุมในการจัดส่งข้อมูลสำหรับยืนยันตัวตน (Secret Authentication Information) เช่น ชื่อผู้ใช้งาน/รหัสผ่านเข้าระบบ โดย

(5.1) หากเป็นการส่งข้อมูลสำหรับยืนยันตัวตนในรูปแบบเอกสาร ให้ทำการส่งโดยการใส่ซองปิดผนึกและส่งถึงผู้ใช้งาน

(5.2) หากเป็นการส่งข้อมูลสำหรับยืนยันตัวตนในรูปแบบอีเมล หรือสื่ออิเล็กทรอนิกส์ ให้ทำการเข้ารหัสไฟล์/สื่อบันทึกข้อมูล และ/หรือ ทำการควบคุมการเข้าถึงไฟล์/สื่อโดยใช้รหัสผ่าน

(6) กรณีที่มีเครื่องมือเพื่อใช้ตรวจสอบความเหมาะสมของรหัสผ่าน ให้มีการจัดทำระบบบริหารจัดการรหัสผ่านที่มีการทำงานเชิงโต้ตอบ (Interactive)

<u>แนวทางการปฏิบัติงานการควบคุมการเข้าถึงระบบเครือข่าย</u>

5.7 ส่วนงานที่รับผิดชอบระบบเครือข่ายหรือส่วนงานที่ดูแลระบบเครือข่ายในการปฏิบัติงานของส่วนงานมีหน้าที่ดังนี้

(1) บริหารจัดการผู้มีสิทธิในการเข้าถึงอุปกรณ์เครือข่าย และจัดทำตารางกำหนดสิทธิสำหรับผู้มีสิทธิในการเข้าถึงอุปกรณ์เครือข่ายคอมพิวเตอร์เพื่อบริหารจัดการ ดังนี้

(1.1) ผู้บริหารส่วนงานในระดับส่วนงานหรือที่มีหน้าที่รับผิดชอบในการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์

(1.2) พนักงานที่มีภารกิจหรือหน้าที่รับผิดชอบด้านงานจัดการและบริหารอุปกรณ์เครือข่ายคอมพิวเตอร์

(1.3) พนักงานที่มีภารกิจหรือหน้าที่รับผิดชอบด้านงานเฝ้าดูแลและรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์

(1.4) พนักงานที่มีภารกิจหรือหน้าที่รับผิดชอบด้านงานระบบเครือข่ายสายสัญญาณ

(1.5) พนักงานที่มีภารกิจหรือหน้าที่รับผิดชอบด้านดูแลจัดการและบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์

(1.6) บริษัทผู้ให้บริการภายนอกที่ ทอท. ว่าจ้างในการให้บริการหรือบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์

(2) จัดการสิทธิในการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์ในการบริหารจัดการค่าติดตั้งระบบ (Configuration) แบ่งเป็น 2 ระดับ ดังนี้

(2.1) Read Only

(2.2) Read/Write

(3) กำหนดรอบระยะเวลาในการเปลี่ยนแปลงรหัสผ่านที่ใช้ในการเข้าถึงอุปกรณ์เครือข่ายคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง

(4) จัดการสิทธิและยืนยันตัวบุคคลผู้ใช้งานที่อยู่ภายนอกองค์กรในการเข้าถึงอุปกรณ์เครือข่ายคอมพิวเตอร์โดยผ่านระบบ Virtual Private Network (VPN) และบัญชีผู้ใช้งานและรหัสผ่านเพื่อให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบ

(5) บริหารจัดการเพื่อตรวจสอบและพิสูจน์อุปกรณ์ที่ได้รับอนุญาตในการใช้งานบริการเครือข่ายสำหรับระบบสารสนเทศที่มีความสำคัญโดยใช้ MAC Address หรือ IP Address

(6) บริหารจัดการการให้บริการเครือข่ายและการใช้งานพอร์ตเครือข่าย โดยมีข้อปฏิบัติเพื่อดำเนินการดังนี้

(6.1) เปิดเฉพาะบริการ (Service) เท่าที่จำเป็น และจำกัดการเข้าถึงให้ใช้งานได้เฉพาะผู้ที่มีความจำเป็นและได้รับอนุญาตเท่านั้น

(6.2) มีการควบคุมและตรวจสอบไม่ให้มีการเปิดให้บริการบนเครือข่ายโดยไม่ได้รับอนุญาต

(6.3) จัดทำทะเบียนพอร์ตเครือข่ายที่อนุญาตให้ใช้งานหรือไม่อนุญาตให้ใช้งาน รวมถึงกรณีปิดใช้งานเป็นค่าเริ่มต้น

(6.4) ดำเนินการจัดการสำหรับการให้บริการใช้งาน Social Media ให้เป็นไปตามข้อตกลงการใช้งานสินทรัพย์สารสนเทศของ ทอท.

(7) จัดทำกฎเกณฑ์หรือข้อกำหนดนโยบายในการบริหารจัดการอุปกรณ์รักษาความปลอดภัยเครือข่าย (Firewall Policy) โดยมีการทบทวนปรับปรุงเป็นประจำอย่างน้อยปีละ 1 ครั้ง

(8) มีการบันทึกข้อมูลกิจกรรมการใช้งาน (Log) สำหรับการทำงานของระบบคอมพิวเตอร์แม่ข่ายของระบบที่ใช้ตรวจสอบสภาพการทำงานของอุปกรณ์ระบบเครือข่าย (Network Monitoring Equipment) การใช้งานของโปรแกรมระบบงาน และระบบป้องกันการบุกรุกของระบบเครือข่าย

(9) มีแนวทางการปฏิบัติงานการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกกิจกรรมการใช้งาน (Log) ต่างๆ และกำหนดสิทธิการเข้าถึงเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(10) มีการตั้งเวลาของอุปกรณ์เครือข่ายตามมาตรฐานที่ ทอท. ใช้อ้างอิงโดยสอดคล้องกับข้อกำหนดของกฎหมาย

(11) การแก้ไขหรือเพิ่มเติมสิทธิในการบริหารจัดการระบบเครือข่ายที่นอกเหนือไปจากที่กำหนด หรือการบริหารจัดการระบบเครือข่ายในสภาวะฉุกเฉิน ให้อยู่ในอำนาจของผู้มีหน้าที่ในการพิจารณาอนุมัติให้ดำเนินการ

แนวทางการปฏิบัติงานการควบคุมการเข้าถึงระบบปฏิบัติการ

5.8 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่จัดทำและดำเนินการตามขั้นตอนการปฏิบัติงานเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยและการยืนยันตัวตนของผู้ใช้งาน โดยมีแนวทางการปฏิบัติอย่างน้อย ดังนี้

(1) ตรวจสอบยืนยันตัวตนและสิทธิการเข้าใช้งานของผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบปฏิบัติการตามชื่อบัญชีผู้ใช้งานและรหัสผ่าน สำหรับการเข้าสู่ระบบปฏิบัติการตามที่ได้รับสิทธิหรือได้รับอนุญาต

(2) กรณีที่เป็นชื่อบัญชีที่มีผู้ใช้งานร่วมกัน จะต้องสามารถตรวจสอบเพื่อระบุตัวตนของผู้ใช้งานได้ หรือตรวจสอบจากอุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เพื่อตรวจสอบยืนยันคุณลักษณะเฉพาะตัวของบุคคลได้

(3) สามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทางที่อาจเข้าข่ายมีการเจาะระบบหรือการเข้าระบบไม่ถูกต้อง

(4) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(5) มีการบันทึกข้อมูลกิจกรรมการใช้งาน (Log) สำหรับการป้อนข้อมูลเพื่อการเข้าใช้งานระบบปฏิบัติการ

(6) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการ โดยการใช้คำสั่งด้วย Command Line และจำกัดสิทธิเฉพาะผู้ที่ได้รับสิทธิหรือได้รับมอบหมายในการบริหารจัดการเท่านั้น

(7) มีการแจ้งเตือนกรณีข้อมูลยืนยันตัวตนของชื่อบัญชีผู้ใช้งานและรหัสผ่านที่ป้อนไม่ถูกต้องทั้งนี้จะต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์ ซึ่งอาจเป็นช่องทางหนึ่งของการเจาะระบบโดยผู้ไม่ประสงค์ดี

(8) กรณีที่เป็นข้อจำกัดของระบบสารสนเทศ ให้จัดทำบันทึกแจ้งให้หัวหน้าส่วนงานหรือผู้บังคับบัญชารับทราบ

(9) กรณีที่มีเครื่องมือเพื่อใช้ตรวจสอบความเหมาะสมของรหัสผ่าน มีแนวทางการปฏิบัติงานเพื่อดำเนินการให้มีการจัดทำระบบบริหารจัดการรหัสผ่านที่มีการทำงานเชิงโต้ตอบ (Interactive)

5.9 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่บริหารจัดการและควบคุมการให้บริการและใช้งานระบบ ดังนี้

(1) ควบคุมการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ประมวลผลของระบบสารสนเทศที่มีความสำคัญ ที่มีการติดตั้งใช้งานระบบปฏิบัติการ ระบบฐานข้อมูล หรือ ระบบงานที่มีระบบปฏิบัติการเฉพาะ ไม่ให้มีการติดตั้งโปรแกรมอรรถประโยชน์อื่นที่ไม่ได้รับอนุญาต กรณีมีความจำเป็นจะต้องได้รับอนุญาตจากหัวหน้าส่วนงานที่ดูแลระบบการให้บริการ และให้มีการบันทึกทะเบียนโปรแกรมอรรถประโยชน์ที่ติดตั้งดังกล่าว พร้อมทั้งการตรวจสอบด้านความมั่นคงปลอดภัยอย่างเหมาะสม โดยโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานต้องมีลิขสิทธิ์ให้ใช้งานได้ตามกฎหมาย

(2) บริหารจัดการและตั้งค่าระบบให้ยุติการใช้งานระบบ หากไม่มีการใช้งานอย่างต่อเนื่อง เมื่อไม่มีการใช้งานภายในระยะเวลา 15 นาที หรือตามข้อจำกัดของระบบ หากผู้ใช้งานต้องการใช้งานต่อ ต้องลงชื่อและรหัสผ่านอีกครั้ง

(3) จำกัดระยะเวลาในการเชื่อมต่อการใช้งานระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง อย่างน้อย 2 ชั่วโมง ต่อการเชื่อมต่อระบบหนึ่งครั้ง หรือตามความเหมาะสม หรือตามข้อจำกัดของระบบ เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนด

แนวทางการปฏิบัติงานการควบคุมการเข้าถึงระบบงาน/โปรแกรมประยุกต์ สารสนเทศและซอร์สโค้ด

5.10 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่ดำเนินการเพื่อจำกัดการเข้าถึงสารสนเทศ ซอร์สโค้ด และการใช้งานระบบงาน/โปรแกรมประยุกต์ ดังนี้

(1) ดำเนินการตามแนวทางการปฏิบัติงานการบริหารจัดการการเข้าถึงระบบสารสนเทศของผู้ใช้งานและการควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อจำกัดและควบคุมการเข้าถึง/การเข้าใช้งานของผู้ใช้งานและบุคลากรส่วนงานที่เกี่ยวข้องในการสนับสนุนการเข้าใช้งาน/การเข้าถึงสารสนเทศและฟังก์ชั่นต่างๆ ของโปรแกรมประยุกต์

(2) ให้มีขั้นตอนการปฏิบัติงานการควบคุมการเข้าถึงซอร์สโค้ด เพื่อจำกัดและควบคุมการเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(3) ดำเนินการร่วมกับส่วนงานสายงานเทคโนโลยีดิจิทัลและการสื่อสารในการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ประมวลผลในการให้บริการระบบสารสนเทศที่มีความสำคัญสูงในพื้นที่หวงห้ามเด็ดขาด และพื้นที่หวงห้ามเฉพาะ

(4) ระบบงาน/โปรแกรมประยุกต์ และสารสนเทศ รวมทั้งโปรแกรมอรรถประโยชน์ต่างๆ ที่อนุญาตให้ใช้งานต้องมีลิขสิทธิ์ให้ใช้งานได้ตามกฎหมาย

แนวทางการปฏิบัติงานสำหรับผู้ใช้งาน

5.11 ผู้ใช้งานมีหน้าที่ความรับผิดชอบในการเข้าใช้งานข้อมูลสารสนเทศและสินทรัพย์สารสนเทศ ดังนี้

(1) แจ้งขอมีสิทธิในการเข้า-ออกพื้นที่ต่างๆ ภายใน ทอท. ตามสิทธิที่ได้รับตามภารกิจและหน้าที่ที่ได้รับมอบหมายของผู้ใช้งานภายใต้หลักการตามความจำเป็นต่อการใช้งาน

(2) มีชื่อบัญชีผู้ใช้งานและรหัสผ่านในการใช้งานระบบสารสนเทศ โดยลงทะเบียนขอเป็นผู้มีสิทธิในการใช้งานระบบสารสนเทศตามภารกิจและหน้าที่ที่ได้รับมอบหมายของผู้ใช้งาน ภายใต้หลักการตามความจำเป็นต่อการใช้งาน

(3) ใช้งานรหัสผ่านเพื่อเข้าถึงหรือใช้งานระบบสารสนเทศตามที่ได้รับสิทธิหรือได้รับอนุญาต โดยมีแนวทางการปฏิบัติงาน ดังนี้

(3.1) ตั้งรหัสที่ยากต่อการเดา

(3.2) ไม่เปิดเผยรหัสผ่าน

(3.3) จัดเก็บรหัสผ่านไว้ในสถานที่ปลอดภัย

(3.4) เปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(3.5) มีความยาวขั้นต่ำไม่น้อยกว่า 8 ตัวอักษร โดยรวมถึงอักขระพิเศษและตัวเลข

(3.6) ไม่ใช้ข้อมูลส่วนตัวในการตั้งรหัสผ่าน เช่น วันเดือนปีเกิด คำในพจนานุกรม เป็นต้น

(3.7) ไม่ตั้งจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(3.8) เปลี่ยนรหัสตามรอบระยะเวลาที่กำหนดไว้

(3.9) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(3.10)ไม่กำหนดให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่าน

5.12 ผู้ใช้งานมีหน้าที่ความรับผิดชอบในการดูแลรักษาสินทรัพย์สารสนเทศในความครอบครองของตน ดังนี้

(1) ผู้ใช้งานมีหน้าที่รับผิดชอบป้องกันอุปกรณ์ในความครอบครองของตน หรือขณะที่ไม่มีผู้ใช้งานอุปกรณ์ เพื่อป้องกันการสูญหายหรือเสียหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

(2) ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จการใช้งาน

(3) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอ เมื่อไม่มีการใช้งานภายในระยะเวลาที่กำหนด และใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถเปิดหน้าจอได้ หากต้องการใช้งานต่อ

(4) ต้องจัดเก็บหรือล็อคอุปกรณ์ เมื่อไม่มีการใช้งานหรือโดยไม่มีผู้ดูแลชั่วคราว

(5) ต้องดำเนินการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ รวมถึงการเปิดเผย การล่วงรู้ตามแนวทางการปฏิบัติงานสำหรับการจัดชั้นข้อมูลสารสนเทศในการปกป้องข้อมูลสารสนเทศที่อยู่ในรูปแบบเอกสารและข้อมูลอิเล็กทรอนิกส์ที่มีการจัดเก็บและการดำเนินการใดๆ ที่เกี่ยวข้อง

(6) กรณีที่เป็นข้อมูลสารสนเทศชั้นความลับตามประเภทการจัดชั้นข้อมูลสารสนเทศ จะต้องมีการเข้ารหัสข้อมูลตามวิธีการและแนวทางการปฏิบัติงานที่กำหนด รวมทั้งการจัดการข้อมูลสารสนเทศที่เป็นความลับตามพระราชบัญญัติข้อมูลข่าวสารของราชการ และระเบียบการรักษาความลับทางราชการ พ.ศ. 2544

(7) ต้องจัดเก็บรักษาสินทรัพย์สารสนเทศที่มีความสำคัญในสถานที่ที่มีการรักษาความปลอดภัย โดยไม่จัดวางสินทรัพย์สารสนเทศหรือเอกสารที่มีความสำคัญบนโต๊ะทำงานหรือโดยเปิดเผย โดยปราศจากการควบคุมหรือป้องกันเรื่องการเปิดเผย การล่วงรู้ การแก้ไขข้อมูลสารสนเทศ การลักลอบทำสำเนา การทำให้เสียหายหรือสูญหาย

(8) ห้ามโยกย้ายอุปกรณ์คอมพิวเตอร์และสื่อสารที่ ทอท. จัดหาและติดตั้งให้ใช้งานตามภารกิจหน้าที่โดยไม่ได้รับอนุญาตจากสายงานเทคโนโลยีดิจิทัลและการสื่อสาร หากต้องการโยกย้ายตำแหน่งติดตั้งต้องได้รับอนุญาตจากผู้บังคับบัญชาของส่วนงานตามลำดับชั้น และแจ้งส่วนงานที่ดูแลระบบการให้บริการที่รับผิดชอบเพื่อพิจารณาดำเนินการต่อไป

(9) ห้ามดัดแปลง ถอดถอน ทำลาย หรือกระทำการอื่นใดที่ก่อให้เกิดความเสี่ยงที่อาจทำให้อุปกรณ์คอมพิวเตอร์และสื่อสารที่ ทอท. จัดหาและติดตั้งให้ใช้งานเกิดความเสียหาย

(10) ห้ามนำอุปกรณ์คอมพิวเตอร์และสื่อสารที่ ทอท. จัดหาและติดตั้งให้ใช้งานเชื่อมต่อกับเครือข่ายของผู้ให้บริการภายนอกโดยไม่ได้รับอนุญาตจากสายงานเทคโนโลยีดิจิทัลและการสื่อสาร

หมวด 6 การเข้ารหัสข้อมูล

แนวทางการปฏิบัติงาน

6.1 ต้องกำหนดให้มีวิธีการเข้ารหัสข้อมูลอิเล็กทรอนิกส์ที่เป็นไปตามมาตรฐานสากล และเหมาะสมกับลำดับชั้นความลับของข้อมูล

6.2 การรับและส่งข้อมูลที่มีความสำคัญระหว่าง ทอท. กับหน่วยงานภายนอก ต้องผ่านช่องทางที่มีการเข้ารหัสตามที่กำหนดไว้ เช่น SSL, VPN, SFTP เป็นต้น

6.3 กรณีที่มีการใช้กุญแจการเข้ารหัสต้องมีมาตรฐานการปฏิบัติงานในการบริหารจัดการกุญแจการเข้ารหัสโดยครอบคลุมการสร้าง การจัดเก็บ การจัดส่ง และการเปลี่ยนแปลง

หมวด 7 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

แนวทางการปฏิบัติงาน

7.1 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสารร่วมกับส่วนงาน ทอท. ที่เกี่ยวข้อง กำหนดประเภทพื้นที่ควบคุมที่ต้องมีการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงศูนย์คอมพิวเตอร์ โดยมีการจัดทำแผนผังแสดงตำแหน่งเพื่อการควบคุม และไม่ให้เผยแพร่โดยไม่ได้รับอนุญาตจากส่วนงานเจ้าของพื้นที่ โดยจำแนกพื้นที่ควบคุมดังนี้

(1) พื้นที่หวงห้ามเด็ดขาด หมายความว่า พื้นที่ที่มีการติดตั้งระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร หรือ สินทรัพย์สารสนเทศที่มีความสำคัญสูง ซึ่งต้องมีการควบคุมรักษาความมั่นคงปลอดภัยในระดับสูงสุด โดยกำหนดให้เฉพาะพนักงานที่รับผิดชอบเท่านั้น ที่ได้รับอนุญาตและมีสิทธิเข้า-ออก ห้ามบุคคลภายนอกหรือผู้ที่ไม่มีสิทธิเข้า-ออก ยกเว้นได้รับการอนุญาตเป็นลายลักษณ์อักษรจากส่วนงานเจ้าของพื้นที่เพื่อขอเข้าพื้นที่ พื้นที่หวงห้ามเด็ดขาด ได้แก่ ศูนย์คอมพิวเตอร์ ห้องความมั่นคง (Strong Room) ห้องเครื่องคอมพิวเตอร์แม่ข่าย ห้องระบบเครือข่ายหลัก

(2) พื้นที่หวงห้ามเฉพาะ หมายความว่า พื้นที่ที่มีการติดตั้งระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร หรือ สินทรัพย์สารสนเทศสำคัญ รวมถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีการควบคุมรักษาความมั่นคงปลอดภัยอย่างเข้มงวด โดยกำหนดให้เฉพาะพนักงานที่รับผิดชอบเท่านั้นที่ได้รับอนุญาตและมีสิทธิเข้า-ออก ห้ามบุคคลภายนอกหรือผู้ที่ไม่มีสิทธิเข้า-ออก ผู้ที่ไม่มีสิทธิจะต้องดำเนินการขออนุญาตส่วนงานเจ้าของพื้นที่ เพื่อขอเข้าพื้นที่ พื้นที่หวงห้ามเฉพาะ ได้แก่ พื้นที่บริเวณหรือห้องควบคุมระบบ (Control Room) ห้องติดตั้งระบบสนับสนุนและอำนวยความสะดวกสำหรับระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร (Facilities Room) ห้องปฏิบัติงานด้านความปลอดภัยระบบเครือข่าย (Network Monitoring Room) พื้นที่ที่ตั้งเครื่องคอมพิวเตอร์แม่ข่ายตามเขตพื้นที่ที่ไม่ใช่ส่วนกลาง ห้องอุปกรณ์ระบบเครือข่ายและสื่อสารโทรคมนาคม (Tele data Room)

(3) พื้นที่ควบคุมเฉพาะ หมายความว่า พื้นที่ที่เป็นสถานที่ปฏิบัติงานของพนักงานระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร ผู้บริหาร และพนักงาน ทอท. ที่รับผิดชอบดูแลและควบคุมระบบ รวมถึงพื้นที่ภายในอาคารซึ่งมีการติดตั้งใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารในความรับผิดชอบของสายงานเทคโนโลยีดิจิทัลและการสื่อสาร พื้นที่ควบคุมเฉพาะ ได้แก่ ห้องประชุม ห้องทำงานของผู้บริหาร สถานที่ปฏิบัติงานของพนักงานระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร พื้นที่ส่งมอบผลิตภัณฑ์ระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร (Delivery / Unpacking Area)

(4) พื้นที่ควบคุมทั่วไป หมายความว่า พื้นที่ที่เป็นพื้นที่ส่วนกลาง สถานที่ปฏิบัติงานของพนักงาน ทอท. ที่ไม่เกี่ยวข้องในการดูแลหรือใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร พื้นที่ควบคุมทั่วไป ได้แก่ สถานที่ปฏิบัติงาน (ในส่วนที่ไม่เกี่ยวข้องกับระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร) พื้นที่อาคารผู้โดยสาร พื้นที่ภายในอาคาร พื้นที่ทางเดินภายในอาคาร พื้นที่หน้าลิฟต์โดยสาร

7.2 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสารร่วมกับส่วนงาน ทอท. ที่เกี่ยวข้องจัดทำขั้นตอนการปฏิบัติงานการควบคุมการเข้า-ออกพื้นที่ควบคุมที่ต้องมีการรักษาความมั่นคงปลอดภัยสารสนเทศ และพื้นที่ติดตั้งหรือใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีการควบคุมอย่างเหมาะสมอย่างน้อย ดังนี้

(1) สถานที่ตั้งของระบบทางเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้า-ออกที่รัดกุม และอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

(2) มีเจ้าหน้าที่รักษาความปลอดภัยหน้าบริเวณพื้นที่หวงห้ามเด็ดขาดและพื้นที่หวงห้ามเฉพาะ

(3) พนักงาน ทอท. ต้องติดบัตรพนักงานตลอดเวลาที่อยู่ในพื้นที่

(4) บุคคลภายนอก หรือผู้ที่ไม่มีสิทธิเข้าพื้นที่ เมื่อได้รับอนุญาตจะต้องแลกบัตรและติดบัตรแสดงตนตลอดเวลาที่อยู่ในพื้นที่

(5) บุคคลภายนอก หรือผู้ที่ไม่มีสิทธิเข้าพื้นที่ เมื่อได้รับอนุญาตเข้าศูนย์คอมพิวเตอร์ หรือพื้นที่ที่หวงห้ามเด็ดขาดจะต้องลงบันทึกวันที่และเวลาเข้า-ออก พร้อมทั้งวัตถุประสงค์ โดยต้องมีพนักงาน ทอท. หรือผู้รับจ้าง/ผู้รับดำเนินการภายใต้สัญญางานจ้างดูแลและบำรุงรักษาสิ่งอำนวยความสะดวกในศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองของ ทอท. หรือผู้ที่ได้รับมอบหมายพาเข้าพื้นที่และควบคุมดูแลการเข้าพื้นที่

7.3 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสารร่วมกับส่วนงาน ทอท. ที่เกี่ยวข้องจัดทำขั้นตอนการปฏิบัติงานการควบคุมการนำอุปกรณ์เข้า-ออกพื้นที่ควบคุมและจัดการอุปกรณ์ที่ไม่มีการใช้งาน โดยมีการควบคุมอย่างเหมาะสมอย่างน้อย ดังนี้

(1) การนำอุปกรณ์ใดๆ เข้าหรือออกศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้ามเด็ดขาด ต้องปฏิบัติตามระเบียบและกระบวนการที่กำหนด โดยได้รับอนุญาตเป็นลายลักษณ์อักษรจากส่วนงานเจ้าของพื้นที่หรือส่วนงานดูแลระบบการให้บริการ

(2) ห้ามนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารใดๆ เชื่อมต่อเข้ากับระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ในขณะเข้าปฏิบัติงานในพื้นที่ควบคุม โดยที่ไม่ใช่ภาระหน้าที่ หรือไม่ได้รับอนุญาตจากส่วนงานเจ้าของพื้นที่หรือส่วนงานดูแลระบบการให้บริการ

(3) อุปกรณ์ที่ไม่มีการใช้งานแล้วต้องได้รับการตรวจสอบและอนุมัติให้กำจัด ทำลาย หรือนำอุปกรณ์กลับมาใช้งานใหม่

(4) ข้อมูลในอุปกรณ์ที่ไม่มีการใช้งานแล้วต้องได้รับอนุมัติในการทำลายข้อมูล และทำลายข้อมูลตามขั้นตอนการปฏิบัติงานการทำลายข้อมูลที่กำหนด หรือมีการควบคุมด้วยข้อตกลงการไม่เปิดเผยข้อมูล

7.4 ให้สายงานเทคโนโลยีดิจิทัลและการสื่อสารร่วมกับส่วนงาน ทอท. ที่เกี่ยวข้อง จัดทำแนวทางการปฏิบัติงานสำหรับการรักษาความปลอดภัยและการบำรุงรักษาในการให้บริการระบบสนับสนุนของศูนย์คอมพิวเตอร์ โดยมีการควบคุมที่เหมาะสมในการให้บริการได้อย่างต่อเนื่อง ดังนี้

(1) มีระบบสำรองไฟฟ้า (UPS) และระบบไฟฟ้าสำรองโดยเครื่องกำเนิดไฟฟ้า (Generator) อย่างเพียงพอ โดยมีการกำหนดรอบในการตรวจสอบและบำรุงรักษาระบบอย่างเหมาะสม

(2) มีระบบปรับอากาศ ระบบควบคุมอุณหภูมิและความชื้น ระบบเตือนภัยน้ำรั่ว โดยมีการกำหนดรอบในการตรวจสอบและบำรุงรักษาระบบอย่างเหมาะสม

(3) มีระบบป้องกันอัคคีภัย อุปกรณ์แจ้งเหตุ ควบคุม และป้องกันอัคคีภัย โดยมีการกำหนดรอบในการตรวจสอบและบำรุงรักษาระบบอย่างเหมาะสม

(4) มีระบบกล้องโทรทัศน์วงจรปิดภายในศูนย์คอมพิวเตอร์ พื้นที่หวงห้ามเด็ดขาดและพื้นที่หวงห้ามเฉพาะ โดยมีการกำหนดรอบในการตรวจสอบและบำรุงรักษาระบบอย่างเหมาะสม

(5) จัดทำผังรายการอุปกรณ์และสายสัญญาณในศูนย์คอมพิวเตอร์ รวมถึงการตรวจสอบและบำรุงรักษาอุปกรณ์อย่างเหมาะสม

(6) มีแผนอพยพ หรือ แผนป้องกันอุบัติภัย หรือแผนรองรับกรณีฉุกเฉิน เมื่อเกิดภัยพิบัติหรือภัยคุกคามที่มีผลต่อการดำเนินงาน

(7) ให้มีการล็อคตู้หรือป้องกันการเข้าถึงอุปกรณ์อย่างรัดกุม

(8) ให้มีการควบคุมการเข้าถึงสายไฟฟ้า และสายสัญญาณ โดยไม่ได้รับอนุญาต เพื่อป้องกันการเกิดอุปสรรคต่อสายไฟฟ้า และสายสัญญาณ ที่ทำให้เกิดความเสียหาย และป้องกันการดักรับสัญญาณ เช่น สายไฟฟ้าหรือสายสัญญาณต้องอยู่ในท่อร้อยสาย เดินท่อบนราง เป็นต้น

(9) ห้ามเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์และสื่อสารของ ทอท. โดยไม่ได้รับอนุญาตหรือไม่ใช่ภารกิจหน้าที่ตามที่ได้รับมอบหมาย

7.5 ส่วนงานที่รับผิดชอบด้านงานรักษาความมั่นคงปลอดภัยสำหรับศูนย์บริการเครื่องคอมพิวเตอร์แม่ข่าย หรือศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ซึ่งประกอบด้วยเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์จัดเก็บข้อมูลกลาง (Storage) ชุดควบคุม ตรวจสอบและเฝ้าระวัง (System Monitor and Control) และอุปกรณ์ต่อพ่วงอื่นๆ จะต้องดำเนินการ ดังนี้

(1) รักษาความมั่นคงและดำรงไว้ซึ่งการให้บริการเครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งตามศูนย์คอมพิวเตอร์แต่ละแห่งของ ทอท. ให้อยู่ในสภาวะพร้อมใช้งานได้อย่างต่อเนื่อง

(2) อำนาจหน้าที่สำหรับการเปิด-ปิดเครื่องคอมพิวเตอร์แม่ข่ายสำหรับศูนย์คอมพิวเตอร์ของ ทอท. ไม่ว่าจะเป็นบางส่วนหรือทั้งหมดให้ขออนุมัติต่อผู้บังคับบัญชาตามลำดับชั้นโดยให้พิจารณาความสำคัญของชุดโปรแกรมที่มีผลกระทบต่อผู้ใช้งานนั้นเป็นสำคัญ

(3) จัดสรรวางเครื่องคอมพิวเตอร์แม่ข่ายหลักและเครื่องคอมพิวเตอร์แม่ข่ายสำรองในพื้นที่ชั้นใน (Trust Zone) ให้ถูกต้องตามหลักวิชาการสายวิชาชีพที่ดี โดยต้องไม่เปิดโอกาสให้บุคคลภายนอกหรือบริษัทเอกชนใดๆ ต่อเชื่อมในพื้นที่ชั้นในได้ หากมีความจำเป็นให้หัวหน้าส่วนงานจัดทำเรื่องขออนุมัติการเชื่อมต่อดังกล่าวเสนอผู้บังคับบัญชาตามลำดับชั้นก่อนการดำเนินการ

7.6 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่บำรุงรักษาระบบทางเทคโนโลยีสารสนเทศและการสื่อสารที่อยู่ในความรับผิดชอบให้อยู่ในสภาพพร้อมใช้งานอย่างต่อเนื่อง รวมทั้งการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) การบำรุงรักษาเชิงแก้ไข (Corrective Maintenance) การซ่อมบำรุงระบบอุปกรณ์คอมพิวเตอร์ และระบบสนับสนุนศูนย์คอมพิวเตอร์

หมวด 8 ความปลอดภัยด้านการดำเนินงาน

แนวทางการปฏิบัติงาน

8.1 ส่วนงานที่ดูแลระบบการให้บริการมีเอกสารขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติงาน สำหรับการปฏิบัติงานระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร หรือระบบสารสนเทศที่มีความสำคัญ ระบุผู้รับผิดชอบและหน้าที่ความรับผิดชอบอย่างชัดเจน โดยมีการทบทวนอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

8.2 กำหนดให้มีขั้นตอนการปฏิบัติงานการควบคุมการเปลี่ยนแปลงที่เป็นลายลักษณ์อักษร ทั้งในกรณีการติดตั้ง เปลี่ยนแปลง หรือแก้ไข อุปกรณ์และซอฟต์แวร์สำหรับอุปกรณ์คอมพิวเตอร์และสื่อสาร รวมถึงการตรวจสอบภายหลังการเปลี่ยนแปลงแก้ไข

8.3 ส่วนงานที่ดูแลระบบการให้บริการมีกระบวนการในการติดตาม ตรวจสอบสถานะและประสิทธิภาพการทำงานของระบบสารสนเทศที่สำคัญเป็นประจำอย่างต่อเนื่องสม่ำเสมอ เช่น การรับส่งข้อมูลสารสนเทศ การใช้ฮาร์ดดิสก์ การใช้งานหน่วยประมวลผล (CPU) การใช้งานหน่วยความจำ เป็นต้น

8.4 ส่วนงานที่ดูแลระบบการให้บริการร่วมกับส่วนงานเจ้าของระบบสารสนเทศพิจารณาจำแนกระบบที่ให้บริการสำหรับการใช้งานจริง (Production) ออกจากสภาพแวดล้อมสำหรับการพัฒนาระบบและการทดสอบระบบ สำหรับระบบสารสนเทศที่มีความสำคัญ

8.5 ส่วนงานที่ดูแลระบบการให้บริการรับผิดชอบดูแลการติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์หรือโปรแกรมที่ไม่พึงประสงค์ ดังนี้

(1) ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์หรือโปรแกรมที่ไม่พึงประสงค์ที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการและระบบสารสนเทศที่มีความสำคัญ กรณีที่มีข้อจำกัดให้จัดทำเป็นรายงานบันทึกแจ้งหัวหน้าส่วนงาน

(2) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการและระบบสารสนเทศที่มีความสำคัญไม่ให้มีการเชื่อมต่อระบบอินเทอร์เน็ต ยกเว้นกรณีที่มีข้อจำกัดเพื่อใช้งานตามวัตถุประสงค์การใช้งานต้องได้รับอนุญาตจากหัวหน้าส่วนงาน

(3) เครื่องคอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์หรือโปรแกรมที่ไม่พึงประสงค์ตามที่ ทอท. จัดไว้ให้ โดยเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องมีการปรับปรุงเวอร์ชั่นของระบบ และชุดข้อมูลไวรัสคอมพิวเตอร์ (Virus Definition/Pattern) จากส่วนกลางให้เป็นปัจจุบันอยู่เสมอ ในกรณีที่มีความจำเป็นต้องขอยกเว้นการติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์หรือโปรแกรมที่ไม่พึงประสงค์ เช่น เครื่องคอมพิวเตอร์เพื่อการพัฒนาหรือเพื่อวัตถุประสงค์อื่น ต้องได้รับอนุญาตจากหัวหน้าส่วนงาน

(4) เครื่องคอมพิวเตอร์ส่วนตัวหรืออุปกรณ์คอมพิวเตอร์หรืออุปกรณ์สื่อสารใดๆ ที่ผู้ใช้งานนำมาใช้และได้รับอนุญาตให้เชื่อมต่อกับระบบเครือข่าย จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์หรือดำเนินการตามแนวทางการปฏิบัติงานของส่วนงานที่ดูแลระบบการให้บริการ

(5) ห้ามผู้ใช้งานติดตั้งโปรแกรมใดๆ โดยไม่ได้รับอนุญาตจากหัวหน้าส่วนงานที่ดูแลระบบให้บริการหรือไม่ทราบแหล่งที่มา หรือไม่ได้มาจากแหล่งที่ฝ่ายปฏิบัติการและบำรุงรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารรับรอง

(6) เผยแพร่ข่าวสารรวมทั้งคู่มือในการป้องกันไวรัสคอมพิวเตอร์หรือโปรแกรมที่ไม่พึงประสงค์ หรือภัยคุกคามระบบทางเทคโนโลยีสารสนเทศและการสื่อสารผ่านช่องทางประชาสัมพันธ์ภายในองค์กรอย่างสม่ำเสมอ

8.6 ส่วนงานที่ดูแลระบบการให้บริการมีการจัดทำระบบสำรองข้อมูลสำหรับระบบสารสนเทศที่มีความสำคัญให้อยู่ในสภาพพร้อมใช้งาน ดังนี้

(1) จัดทำระบบสำรองข้อมูลที่เหมาะสม โดยมีการจัดทำแผนสำรองข้อมูล

(2) สำรองข้อมูลสารสนเทศสำคัญที่สอดคล้องตามแผนสำรองข้อมูลรวมถึงระบบปฏิบัติการ (Operating System) ระบบงาน/โปรแกรมประยุกต์ (Application) และชุดคำสั่งหรือค่าติดตั้งระบบที่ใช้งานให้ครบถ้วน พร้อมทั้งให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

(3) ขั้นตอนหรือวิธีการปฏิบัติงานในการสำรองข้อมูลสารสนเทศเพื่อเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยมีการกำหนดรายละเอียดอย่างน้อย ดังนี้

(3.1) ผู้รับผิดชอบในการสำรองข้อมูลสารสนเทศ

(3.2) ประเภทข้อมูลสารสนเทศและข้อมูลสารสนเทศที่สำรอง

(3.3) ความถี่ในการสำรอง (รายวัน/รายสัปดาห์/รายเดือน/รายไตรมาส/ราย 6 เดือน/รายปี/อื่นๆ ตามที่กำหนด)

(3.4) ประเภทสื่อที่บันทึก (Media)

(3.5) จำนวนที่ใช้ในการสำเนา (Copy)

(3.6) สถานที่และวิธีการเก็บรักษาสื่อบันทึก รวมถึงวิธีการนำข้อมูลสารสนเทศกลับมาใช้งาน

(3.7) ขั้นตอนและวิธีการสำรอง

(3.8) วิธีการทำลายสื่อบันทึก

(3.9) การบันทึกการปฏิบัติงาน (Log) เกี่ยวกับการสำรองข้อมูลสารสนเทศของพนักงานเพื่อตรวจสอบความถูกต้องครบถ้วน และมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

8.7 ส่วนงานที่ดูแลระบบการให้บริการต้องดำเนินการทดสอบสภาพพร้อมใช้ของระบบสำรองสำหรับระบบงานที่มีความสำคัญ พร้อมบันทึกผลการทดสอบ รวมทั้งทบทวนและปรับปรุงระบบสำรองข้อมูลและแผนการสำรองข้อมูลอย่างน้อยปีละ 1 ครั้ง

8.8 ส่วนงานที่ดูแลระบบการให้บริการต้องดำเนินการ ตรวจสอบ เฝ้าระวัง และรายงานผลพฤติกรรมการให้บริการของเครื่องคอมพิวเตอร์แม่ข่าย ทอท. โดยให้มีการจัดเก็บ Log ของระบบปฏิบัติการ ระบบโปรแกรม และระบบฐานข้อมูล เพื่อเก็บเป็นหลักฐานสามารถนำกลับมาตรวจสอบได้ในภายหลังตามที่กฎหมายกำหนด และเก็บไว้ในที่ปลอดภัย พร้อมทั้งรายงานผลต่อผู้บังคับบัญชาตามลำดับชั้นทันทีที่พบเหตุการณ์ผิดปกติ

8.9 ส่วนงานที่ดูแลระบบการให้บริการมีกระบวนการบันทึกข้อมูลการใช้งานระบบสารสนเทศที่สามารถตรวจสอบถึงผู้ใช้งานได้ ดังนี้

(1) มีการบันทึกข้อมูลกิจกรรมการใช้งาน (Log) ของระบบอินเทอร์เน็ต และระบบสารสนเทศที่สำคัญ โดยมีการจัดเก็บบันทึกข้อมูลเป็นระยะเวลาอย่างน้อย 90 วัน หรือตามที่กฎหมายกำหนด

(2) มีระบบตรวจสอบการเข้าใช้งาน และบันทึกการพยายามเข้าใช้งานที่ไม่ปกติ รวมทั้งการบันทึกและวิเคราะห์ข้อผิดพลาดที่เกิดขึ้นจากการลงชื่อเข้าใช้งาน

(3) มีการบันทึกข้อมูลการเข้าใช้งานหรือกิจกรรมของผู้ดูแลระบบ

(4) มีการจัดเก็บข้อมูลบันทึกกิจกรรมการใช้งานให้มีความปลอดภัยโดยมีการป้องกันการเข้าถึงข้อมูลบันทึกกิจกรรมการใช้งาน เพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต

(5) มีการตั้งเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ตามมาตรเวลาจากเครื่องให้บริการเทียบเวลาหลักของศูนย์คอมพิวเตอร์ ทอท.

8.10 ส่วนงานที่ดูแลระบบการให้บริการ ดำเนินการวางแผนก่อนการตรวจประเมินระบบทางเทคโนโลยีสารสนเทศและการสื่อสารเพื่อป้องกันเหตุขัดข้องในการทำงาน โดยเฉพาะการตรวจสอบทางเทคนิคสำหรับระบบสารสนเทศที่มีความสำคัญ โดยมีการกำหนดช่วงเวลาที่เหมาะสม

หมวด 9 ความปลอดภัยด้านการสื่อสาร

แนวทางการปฏิบัติงาน

9.1 ส่วนงานที่รับผิดชอบระบบเครือข่ายหรือส่วนงานที่ดูแลระบบเครือข่ายในการปฏิบัติงานของส่วนงานมีหน้าที่ ดังนี้

(1) บริหารจัดการและบำรุงรักษาระบบเครือข่าย ทอท. ให้อยู่ในสภาพความพร้อมใช้งานอย่างต่อเนื่อง สำหรับการใช้งานระบบสารสนเทศ ซึ่ง ทอท. จัดหาให้สำหรับผู้ใช้งานตามภารกิจและหน้าที่ที่รับผิดชอบในการดำเนินธุรกิจของ ทอท. โดยสามารถเข้าถึงหรือใช้งานเฉพาะระบบสารสนเทศหรือบริการทางเครือข่ายที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(2) บริหารจัดการและบำรุงรักษาระบบเครือข่าย ทอท. ตามการจัดกลุ่มบริการทางเครือข่ายที่มีไว้ให้บริการ และมีการปรับปรุงแผนผังระบบเครือข่ายให้เป็นปัจจุบัน โดยจำแนก ดังนี้

(2.1) อินเทอร์เน็ตโซน (Internet Zone) เครือข่ายภายนอก ทอท. สำหรับระบบอินเทอร์เน็ตในการเข้าใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของกลุ่มผู้ใช้งานจากเครือข่ายภายนอก ทอท.

(2.2) อินทราเน็ตโซน (Intranet Zone) เครือข่ายภายใน ทอท. สำหรับระบบอินทราเน็ตในการเข้าใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. จากเครือข่ายภายใน ทอท. สำหรับกลุ่มของระบบสารสนเทศที่ใช้ภายใน ทอท.

(2.3) เอ็กซ์ทราเน็ตโซน (Extranet Zone) สำหรับระบบเครือข่ายเฉพาะ ที่มีการเชื่อมต่อจากหน่วยงานภายนอกกับระบบเครือข่าย ทอท. สำหรับกลุ่มของบริการสารสนเทศที่มีข้อตกลงกับหน่วยงานภายนอก

(2.4) DMZ (Demilitarized Zone) ส่วนเครือข่ายกลางระหว่างเครือข่ายภายในและเครือข่ายภายนอกของ ทอท. ที่มีการเชื่อมต่อกับเครือข่ายสื่อสารต่างๆ สำหรับกลุ่มผู้ใช้งาน

(2.5) ศูนย์บริการเครื่องคอมพิวเตอร์แม่ข่าย (Server Farm Zone) สำหรับการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายกลุ่มระบบสารสนเทศและระบบการให้บริการของระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

(3) บริหารจัดการอุปกรณ์ระบบเครือข่ายของ ทอท. โดยจัดการสิทธิการเข้าถึงอุปกรณ์ระบบเครือข่ายตามประเภทอุปกรณ์ ดังนี้

(3.1) อุปกรณ์ที่ใช้เชื่อมต่อระบบเครือข่ายหลัก (Core Switch)

(3.2) อุปกรณ์ที่ใช้เชื่อมต่อระบบเครือข่ายทั่วไป (Network Switch) เช่น Distribution Switch, Access Switch หรือ Router เป็นต้น

(3.3) อุปกรณ์ที่ใช้ตรวจสอบสภาพการทำงานของอุปกรณ์ระบบเครือข่าย (Network Monitoring Equipment)

(3.4) อุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (Security Network Equipment)

9.2 ส่วนงานสายงานเทคโนโลยีดิจิทัลและการสื่อสาร และส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่ควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของเครื่องคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลสารสนเทศสอดคล้องกับแนวทางการปฏิบัติงานการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ โดยมีแนวทางการปฏิบัติงานเพื่อดำเนินการ ดังนี้

(1) จัดทำตารางควบคุมเส้นทาง (Routing Table) หรือกำหนดการบังคับใช้เส้นทางเครือข่ายเพื่อเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้

(2) ควบคุมไม่ให้มีการเปิดเผยหมายเลขเครือข่าย (IP Address)

(3) กำหนดให้มีการแยกเครือข่ายย่อย (Subnet) เพื่อใช้ภายใน ทอท.

(4) กำหนดให้มีการจำกัดระยะเวลาสำหรับการเชื่อมต่อระยะไกลไปยังอุปกรณ์ โดยตั้งค่าอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายเพื่อยกเลิกการเชื่อมต่อโดยอัตโนมัติ

(5) ปิดการให้บริการ Telnet ในการเชื่อมต่อแบบระยะไกลไปยังอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น Firewall หากมีความจำเป็นให้ใช้โปรโตคอล HTTPS หรือ SSH (Secure Shell) สำหรับการเชื่อมต่อ

(6) การเข้าถึงระบบเครือข่ายในลักษณะการเข้าถึงจากทางไกล (Remote access) ต้องได้รับอนุมัติจากหัวหน้าส่วนงานที่ดูแลระบบการให้บริการหรือส่วนงานสายงานเทคโนโลยีดิจิทัลและการสื่อสารเป็นลายลักษณ์อักษร

9.3 ส่วนงานที่ดูแลระบบการให้บริการ มีหน้าที่ควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศ ดังนี้

(1) ให้มีการกำหนดขั้นตอนการปฏิบัติงานการแลกเปลี่ยนข้อมูลสารสนเทศอย่างปลอดภัย ในกรณีที่มีการแลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานภายนอก

(2) ให้จัดทำข้อตกลงการแลกเปลี่ยนข้อมูลสารสนเทศระหว่าง ทอท. กับหน่วยงานภายนอก

(3) ให้จัดเตรียมระบบสารสนเทศสำหรับการแลกเปลี่ยนสารสนเทศระหว่าง ทอท. กับหน่วยงานภายนอก

(4) ไม่อนุญาตให้ใช้อีเมลสาธารณะในเครือข่ายของ ทอท. เช่น Hotmail, Yahoo หรือ Gmail เป็นต้น เพื่อป้องกันข้อมูลสารสนเทศของ ทอท. รั่วไหล

หมวด 10 การจัดหา การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร

แนวทางการปฏิบัติงาน

10.1 ส่วนงานที่ดูแลระบบการให้บริการร่วมกับสายงานเทคโนโลยีดิจิทัลและการสื่อสาร และเจ้าของระบบสารสนเทศ มีหน้าที่ดำเนินการเพื่อการจัดหาและการพัฒนาระบบสารสนเทศในการใช้งานภายใน ทอท. ดังนี้

(1) กำหนดให้มีขั้นตอนการปฏิบัติงานการควบคุมการเปลี่ยนแปลงระบบทางเทคโนโลยีสารสนเทศและการสื่อสารที่เป็นลายลักษณ์อักษร ทั้งในกรณีการพัฒนาขึ้นใหม่ หรือเปลี่ยนแปลงแก้ไขระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงการตรวจสอบภายหลังการเปลี่ยนแปลงแก้ไข เพื่อให้ระบบทางเทคโนโลยีสารสนเทศและการสื่อสารสามารถทำงานได้อย่างเป็นปกติ

(2) ให้มีการทดสอบระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งประเภทที่พัฒนาขึ้นใหม่ การเปลี่ยนแปลงแก้ไข หรือระหว่างการพัฒนาระบบ ซึ่งให้มีข้อกำหนดการทดสอบในการตรวจรับ โดยพิจารณา ดังนี้

(2.1) ทดสอบระบบ (System Test)

(2.2) ทดสอบเฉพาะส่วน (Unit Test)

(2.3) ทดสอบการทำงานร่วมกัน (Integration Test)

(2.4) ทดสอบประสิทธิภาพ (Performance/Stress Test)

(2.5) ทดสอบการใช้งานโดยผู้ใช้งาน (User Acceptance Test)

(2.6) ทดสอบด้านความมั่นคงปลอดภัย (Security Test)

(3) การพัฒนาระบบต้องเป็นไปตามข้อกำหนดตามหลักการวิศวกรรมด้านความมั่นคงปลอดภัย ดังต่อไปนี้

(3.1) การรักษาความลับของข้อมูลสารสนเทศ (Confidentiality)

(3.2) การรักษาความถูกต้องสมบูรณ์ของข้อมูลสารสนเทศ (Integrity)

(3.3) ความพร้อมใช้ของข้อมูลสารสนเทศ (Availability)

(3.4) การระบุตัวตนผู้ใช้งาน (Identification)

(3.5) การพิสูจน์ตัวตนผู้ใช้งาน (Authentication)

(3.6) การกำหนดสิทธิ (Authorization)

(3.7) การเก็บบันทึกปูมเหตุการณ์ของการพัฒนาระบบ (Audit Logging) ที่เกี่ยวข้องกับการเปลี่ยนแปลง เพื่อใช้ประกอบในกรณีที่มีการตรวจสอบ

(3.8) มาตรฐานรักษาความมั่นคงปลอดภัยที่ต้องปฏิบัติตาม เช่น OWASP, SANS Top 20 เป็นต้น

(3.9) ความต่อเนื่องของการให้บริการระบบสารสนเทศ (Continuity)

10.2 ผู้พัฒนาระบบต้องพัฒนาระบบสารสนเทศให้มีการปกป้องข้อมูลสารสนเทศและการใช้งานระบบสารสนเทศผ่านเครือข่ายสาธารณะ (Public networks) อย่างปลอดภัย ดังนี้

(1) ไม่พัฒนาระบบสารสนเทศที่จะทำลายกลไกรักษาความปลอดภัยของระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(2) ไม่พัฒนาระบบสารสนเทศซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญ (Priority) ในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(3) ไม่พัฒนาระบบสารสนเทศที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือมัลแวร์

(4) ไม่พัฒนาระบบสารสนเทศที่จะทำลายสิทธิการใช้งานซอฟต์แวร์

(5) ไม่นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพ ที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย ไม่ว่าจากช่องทางการสื่อสารใดๆ ก็ตาม

10.3 ผู้พัฒนาระบบต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบ ดังต่อไปนี้

(1) การให้สิทธิต่ำที่สุด (Least Privileges)

(2) การให้สิทธิเฉพาะที่จำเป็นในการปฏิบัติงาน (Need to know)

(3) การออกแบบระบบให้สามารถป้องกันได้หลายๆ ชั้น (Defense in-Depth)

(4) การออกแบบในลักษณะเปิด (Open Design)

(5) พัฒนาระบบสารสนเทศตามหลักการวิศวกรรมด้านความมั่นคงปลอดภัย (Security Engineering Principles) ตามข้อ 10.1(3)

10.4 กำหนดให้มีการทดสอบระบบสารสนเทศที่มีการพัฒนา การปรับปรุงหรือจัดหาใหม่ และลงชื่อยอมรับผลการทดสอบโดยผู้ใช้งานระบบ และ/หรือเจ้าของระบบ และ/หรือผู้ดูแลระบบที่เกี่ยวข้องแล้วแต่กรณี ก่อนการดำเนินการติดตั้งเพื่อใช้งานจริง (Production)

10.5 ให้มีการจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูปเฉพาะที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกควบคุมอย่างเข้มงวด ดังนี้

(1) จัดทำรายการ Standard Software List ที่อนุญาตให้ติดตั้งบนระบบปฏิบัติการ (Operating System)

(2) จัดให้มีเครื่องมือ (Tools) หรือการสุ่มตรวจสอบ Software ที่เครื่องคอมพิวเตอร์ของพนักงานว่าตรงตาม Standard Software List ที่กำหนดไว้

10.6 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่ควบคุมการติดตั้งซอฟต์แวร์โปรแกรมของระบบสารสนเทศสำหรับการใช้งานจริง โดยมีการควบคุมอย่างน้อย ดังนี้

(1) มีการอนุมัติตามขั้นตอน

(2) มีการควบคุมเวอร์ชั่นหรือการเปลี่ยนแปลงรุ่นของซอฟต์แวร์หรือโปรแกรมที่ใช้งานจริง (Version Change Control)

(3) มีการจัดเก็บรักษาและควบคุมการเข้าถึงชุดคำสั่งต้นฉบับของซอฟต์แวร์โปรแกรม (Source Code)

หมวด 11 ความปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก

แนวทางการปฏิบัติงาน

11.1 ให้ส่วนงาน ทอท. ที่มีการใช้บริการหน่วยงานภายนอก พิจารณาดำเนินการ ดังนี้

(1) พิจารณากำหนดเกณฑ์ในการคัดเลือกและประเมินผู้ให้บริการโดยพิจารณาจากฐานข้อมูลการคัดกรองของกรมบัญชีกลาง และเงื่อนไขการจัดซื้อจัดจ้างตามระเบียบพัสดุของ ทอท. โดยมีการประเมินทั้งก่อนการว่าจ้าง ระหว่างการว่าจ้างตามงวดงาน และเมื่อสิ้นสุดสัญญาการว่าจ้าง

(2) ประเมินความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงหรือการใช้งานสินทรัพย์สารสนเทศของ ทอท. โดยบุคคลภายนอก หน่วยงานภายนอก คู่สัญญา และผู้ใช้บริการ

(3) แจ้งบุคคลภายนอก หน่วยงานภายนอก คู่สัญญา และผู้ให้บริการทราบและปฏิบัติตามนโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Supporting Policy) และแนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Guideline) ก่อนเข้าใช้งานสินทรัพย์สารสนเทศของ ทอท.

(4) ให้บุคคลภายนอก หน่วยงานภายนอก และ/หรือ บุคลากรของหน่วยงานภายนอก ลงชื่อในข้อตกลงการไม่เปิดเผยข้อมูล (Non-disclosure Agreement) ก่อนเข้าดำเนินการ

(5) กรณีที่บุคคลภายนอก หน่วยงานภายนอก คู่สัญญา และผู้ให้บริการต้องมีการเข้าใช้สินทรัพย์สารสนเทศของ ทอท. จะต้องทำเรื่องนำเสนอหัวหน้าส่วนงานต้นสังกัด/คณะกรรมการตรวจรับพัสดุ เพื่อเสนอรองกรรมการผู้อำนวยการใหญ่ สายงานเทคโนโลยีดิจิทัลและการสื่อสาร เพื่อพิจารณาอนุมัติเป็นลายลักษณ์อักษรสำหรับการขอสิทธิในการเข้าถึงและเข้าใช้งานสินทรัพย์สารสนเทศของ ทอท.

11.2 ให้ส่วนงานต้นสังกัดที่มีการใช้บริการหน่วยงานภายนอก หรือส่วนงานที่ดูแลระบบการให้บริการหรือส่วนงานที่ได้รับมอบหมาย ดำเนินการควบคุมกำกับดูแลการให้บริการของหน่วยงานภายนอก เป็นไปอย่างเหมาะสมตามการประเมินความเสี่ยงและนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. รวมทั้งให้สอดคล้องกับระเบียบ นโยบาย และเงื่อนไขตามสัญญา โดยมีการตรวจสอบการให้บริการศึกษาจากรายงาน หรือข้อมูลสารสนเทศที่กำหนดให้บันทึกไว้ตามสัญญา

11.3 กำหนดให้มีกระบวนการและขั้นตอนสำหรับการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก กรณีที่ต้องมีการเปลี่ยนแปลงในสาระสำคัญ ทั้งที่เกิดขึ้นจากหน่วยงานภายนอกหรือจากส่วนงานต้นสังกัดที่มีการใช้บริการหน่วยงานภายนอก

11.4 การเปลี่ยนแปลงเงื่อนไขการให้บริการ การเปลี่ยนแปลงรูปแบบ หรือเทคโนโลยีของผู้ให้บริการภายนอกที่มีสาระสำคัญ ส่วนงานต้นสังกัดหรือส่วนงาน/หน่วยงานที่เกี่ยวข้องที่ใช้บริการต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยที่อาจจะเกิดขึ้นก่อนการเปลี่ยนแปลง

11.5 ให้มีการติดตาม ทบทวน และตรวจสอบการดำเนินงานของผู้ให้บริการภายนอกอย่างสม่ำเสมอ เพื่อให้เป็นไปตามสัญญา หรือข้อตกลงระดับการให้บริการ

หมวด 12 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

แนวทางการปฏิบัติงาน

12.1 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่รับแจ้งเหตุและดำเนินการแก้ไขข้อบกพร่องหรือเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) ด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อการจัดการหรือแก้ไขปัญหาได้อย่างเหมาะสม โดยมีแนวทาง ดังนี้

(1) จัดหาช่องทางการสื่อสารภายใน ทอท. สำหรับให้ผู้ใช้งานสามารถแจ้งข้อบกพร่องหรือเหตุการณ์ด้านความมั่นคงปลอดภัย และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

(2) จัดการแก้ไขปัญหาภายในระยะเวลาที่ตกลงสำหรับการแก้ไขปัญหา พร้อมรายงานให้ผู้บังคับบัญชาทราบอย่างสม่ำเสมอ โดยต้องรวบรวมปัญหา และวิเคราะห์ถึงสาเหตุที่เกิดขึ้น เพื่อศึกษาแนวทางแก้ไขและป้องกันปัญหาที่อาจเกิดขึ้นอีกในอนาคต

(3) ให้มีการจัดทำขั้นตอนการปฏิบัติงานการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยตามผลการประเมินความเสี่ยง

(4) กรณีที่เป็นเหตุการณ์หรือสถานการณ์ที่ไม่อาจดำเนินการแก้ไขได้หรืออาจไม่สามารถแก้ไขภายในระยะเวลาที่กำหนด ซึ่งมีผลกระทบต่อการใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ให้ผู้รับผิดชอบแจ้งผู้บังคับบัญชาและผู้ที่เกี่ยวข้อง เพื่อพิจารณาประกาศใช้แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และ/หรือแผนรองรับความต่อเนื่องในการดำเนินธุรกิจ

(5) กรณีที่เป็นเหตุการณ์หรือสถานการณ์อันเนื่องมาจากการละเมิดกฎหมายที่เกี่ยวข้องในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือธุรกรรมทางอิเล็กทรอนิกส์ ให้ผู้ที่ได้รับมอบหมายของ ทอท. เป็นผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ ซึ่งได้รับการแต่งตั้งตามกฎหมาย

(6) ส่วนงานที่ดูแลระบบการให้บริการต้องจัดเก็บรวบรวมหลักฐานเบื้องต้น สำหรับเหตุการณ์ผิดปกติที่มีผลต่อความปลอดภัยสารสนเทศ ให้อยู่ในสถานะที่เชื่อถือได้ เพียงพอต่อการสืบค้นหาสาเหตุของการเกิดเหตุการณ์ผิดปกติ

หมวด 13 การบริหารจัดการความต่อเนื่องด้านการดำเนินงาน

แนวทางการปฏิบัติงาน

13.1 ส่วนงานที่ดูแลระบบการให้บริการต้องจัดทำระบบสำรองสำหรับระบบสารสนเทศที่มีความสำคัญ และแผนเตรียมความพร้อมกรณีฉุกเฉินให้สอดคล้องกับการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) และการประเมินความเสี่ยง (Risk Assessment)

13.2 ส่วนงานที่ดูแลระบบการให้บริการต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินให้สามารถกู้ระบบทางเทคโนโลยีสารสนเทศและการสื่อสาร หรือจัดหาระบบสำรองหรือทดแทนได้โดยเร็ว เพื่อให้เกิดความเสียหายน้อยที่สุด โดยพิจารณาแนวทาง ดังนี้

(1) จัดลำดับความสำคัญของระบบสารสนเทศ ความสัมพันธ์ของระบบสารสนเทศ และระยะเวลาในการกู้คืนในแต่ละระบบสารสนเทศ

(2) กำหนดสถานการณ์ หรือลำดับความรุนแรงของปัญหา

(3) มีขั้นตอนการแก้ไขปัญหาในแต่ละสถานการณ์

(4) กำหนดผู้รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ

(5) จัดทำรายชื่อ และเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

(6) จัดทำรายละเอียดของอุปกรณ์ และซอฟต์แวร์ที่จำเป็นในกรณีฉุกเฉินของแต่ละระบบงาน เช่น รุ่นเครื่องคอมพิวเตอร์ คุณลักษณะของเครื่องคอมพิวเตอร์ (Specification) ค่าติดตั้งระบบ (Configuration) และอุปกรณ์ระบบเครือข่าย เป็นต้น

(7) ในกรณีที่มีศูนย์คอมพิวเตอร์สำรอง ให้ระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง และแผนที่ เป็นต้น

(8) ปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ และต้องมีสำเนาอย่างน้อย 1 ชุด เก็บไว้แยกจากกัน

(9) ในกรณีที่เกิดเหตุการณ์ฉุกเฉินต้องมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหา

13.3 ส่วนงานที่ดูแลระบบการให้บริการร่วมกับส่วนงานที่เกี่ยวข้องดำเนินการทดสอบแผนเตรียมความพร้อมกรณีฉุกเฉิน และระบบสำรอง หมุนเวียนเป็นประจำทุกปี โดยทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้งานได้จริงในทางปฏิบัติ และให้ผู้ที่เกี่ยวข้องมีความเข้าใจในการดำเนินงาน พร้อมบันทึกผลการทดสอบ

13.4 ส่วนงานที่ดูแลระบบการให้บริการมีหน้าที่ทบทวนและปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง โดยพิจารณาจากผลการทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉิน และมีความเหมาะสมสอดคล้องกับการใช้งานตามภารกิจ

13.5 ส่วนงานที่ดูแลระบบการให้บริการ ต้องจัดหา และติดตั้งอุปกรณ์ประมวลผลสำรองสำหรับระบบสารสนเทศที่มีความสำคัญ เพื่อให้ระบบสามารถใช้งานได้อย่างต่อเนื่อง

หมวด 14 การปฏิบัติตามกฎหมาย และข้อกำหนด

แนวทางการปฏิบัติงาน

14.1 ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศและการสื่อสารมีหน้าที่ตรวจทานการปฏิบัติงานของส่วนงานต่างๆ ของ ทอท. ตามนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Policy) รวมถึงนโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Supporting Policy) มาตรฐานการปฏิบัติงาน แนวทางการปฏิบัติงาน ขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัย รวมทั้งการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และกฎเกณฑ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและ การสื่อสาร อย่างน้อยปีละ 1 ครั้ง

14.2 ให้ส่วนงานที่รับผิดชอบการตรวจสอบระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. หรือผู้ตรวจสอบภายนอกร่วมกับสายงานเทคโนโลยีดิจิทัลและการสื่อสาร ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศหรือระบบงานที่มีความสำคัญ อย่างน้อยปีละ 1 ครั้ง เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศที่เป็นปัจจุบันของ ทอท. โดยรายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบ และกรรมการผู้อำนวยการใหญ่ ทอท.

กรณีเป็นการตรวจสอบด้านเทคนิคหรือการตรวจสอบเฉพาะด้าน ให้ดำเนินการร่วมกับสายงานเทคโนโลยีดิจิทัลและการสื่อสาร โดยมีการควบคุมและจัดเก็บเครื่องมือตรวจสอบ เพื่อป้องกันการเข้าถึงหรือนำมาใช้โดยไม่เหมาะสมและมิให้ส่งผลกระทบต่อการใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

กรณีเป็นการตรวจสอบด้านเทคนิคหรือการตรวจสอบเฉพาะด้าน ซึ่ง ทอท. ไม่สามารถดำเนินการเองได้ ให้ดำเนินการร่วมกับสายงานเทคโนโลยีดิจิทัลและการสื่อสาร เพื่อจัดจ้างผู้เชี่ยวชาญภายนอกในการดำเนินการตรวจสอบ โดยมีการควบคุมการใช้งานเครื่องมือตรวจสอบ มิให้ส่งผลกระทบต่อการใช้งานระบบทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.

ภาคผนวก ก. มาตรฐานและข้อกำหนดอ้างอิง

มาตรฐาน	ISO/IEC 27001:2013 - Information Security Management System (ISMS) Requirements
ข้อกำหนด	Clause 5.2 Policy Annex 5.1.1 Policies for information Security