นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
และ
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

ฝ่ายจัดการเทคโนโลยีและระบบสารสนเทศกลาง

สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)

ตุลาคม พ.ศ. 2565

สารบัญ

ส่วนที่ 1 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นิยาม

“สทอภ.”	หมายถึง	สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)
“ฝ่ายจัดการเทคโนโลยีและระบบสารสนเทศกลาง”	หมายถึง	หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้ คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ และ เครือข่ายสารสนเทศภายใน สทอภ.
“ผู้บังคับบัญชา”	หมายถึง	ผู้มีอำนาจสั่งการตามโครงสร้างของสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)
“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief of Information Officer: CIO)”	หมายถึง	เจ้าหน้าที่ที่ผู้อำนวยการมอบหมายให้ดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง
“การรักษาความมั่นคงปลอดภัย (IT Security)”	หมายถึง	การรักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
“มาตรฐาน (Standard)”	หมายถึง	บรรทัดฐานที่บังคับใช้ในการปฏิบัติจริง เพื่อให้ได้ตามวัตถุประสงค์ หรือเป้าหมาย ได้แก่ การกำหนดรหัสผ่านต้องมีความยาวไม่ต่ำกว่า 8 ตัวอักษร เป็นต้น
“วิธีการปฏิบัติ (Procedure)”	หมายถึง	รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มา ซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
“แนวทางปฏิบัติ (Guideline)”	หมายถึง	แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
“ผู้ใช้งานระบบ (System User)”	หมายถึง	บุคคลที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้งาน บริหารจัดการข้อมูลส่วนบุคคล ได้แก่ รหัสผ่าน (Password) หรือ ไฟล์งานที่ถูกสร้างขึ้น โดยมีสิทธิและหน้าที่ที่ขึ้นกับบทบาท (Role) ซึ่ง สทอภ. กำหนดไว้
“ผู้ดูแลระบบ (System Administrator)”	หมายถึง	เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบ ในการดูแลรักษาระบบ และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึง โปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของ เครือข่ายคอมพิวเตอร์
“เจ้าหน้าที่ (Officer)”	หมายถึง	เจ้าหน้าที่ ลูกจ้าง ลูกจ้างโครงการ จ้างเหมาเอกชน เจ้าหน้าที่ประจำ โครงการ และที่ปรึกษาผู้เชี่ยวชาญ ของ สทอภ.
“หน่วยงานภายนอก (Third party)”	หมายถึง	องค์กรซึ่ง สทอภ. อนุญาตให้มีสิทธิในการเข้าถึงและใช้ข้อมูลหรือสินทรัพย์ต่างๆ ของ สทอภ. โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจ
“บุคคลภายนอก (Third Person)”	หมายถึง	บุคคลที่ไม่ใช่เจ้าหน้าที่ของ สทอภ.
“ผู้บริหารระดับสูงสุด”	หมายถึง	ผู้อำนวยการ สทอภ.
“ผู้บริหารระดับสูง (Top Management Level)”	หมายถึง	รองผู้อำนวยการสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ
“ผู้บริหารระดับกลาง (Middle Management Level)”	หมายถึง	ผู้อำนวยการสำนัก
“ผู้บริหารระดับต้น (Management Level)”	หมายถึง	หัวหน้าฝ่าย

“สิทธิของผู้ใช้งาน”	หมายถึง	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข่องกับระบบสารสนเทศของหนวยงาน โดยหนวยงานจะเปนผู่พิจารณาสิทธิในการใชสินทรัพย
“เจ้าของข้อมูลและสารสนเทศ (Data and Information Owner)”	หมายถึง	ผู้ที่เป็นผู้สร้างข้อมูลและสารสนเทศซึ่งมีหน้าที่ • กำหนดการจัดระดับชั้นความลับ และจัดทำ label ให้แก่ข้อมูลนั้นๆ • อนุญาตให้ผู้ใช้งานเข้าใช้ข้อมูลนั้นๆ • ทำการควบคุมตามที่กำหนดไว้ในแนวทางการจัดระดับชั้นความลับ
“เจ้าของระบบสารสนเทศ (System Owner)”	หมายถึง	ผู้ที่มีหน้าที่ดูแลและบริหารจัดการระบบสารสนเทศของตนเอง
“ผู้ส่งข้อมูลและสารสนเทศ (Data and Information Sender)”	หมายถึง	เจ้าของข้อมูลและสารสนเทศ และ/หรือ ผู้ที่ได้รับอนุญาตจากเจ้าของ ข้อมูลและสารสนเทศให้ใช้ข้อมูลได้ ที่ต้องการส่งข้อมูลและ สารสนเทศไปยังบุคคลภายใน/บุคคลภายนอก สทอภ.
“ความมั่นคงปลอดภัยด้านสารสนเทศ (Information security)”	หมายถึง	การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)
“ข้อมูลคอมพิวเตอร์ (Computer Data)”	หมายถึง	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์ อาจประมวลผลได้ และ ให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตาม พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551
“สารสนเทศ (Information)”	หมายถึง	ข้อเท็จจริงที่ได้จากข้อมูลคอมพิวเตอร์นำมาผ่านการประมวลผล การ จัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ”	หมายถึง	การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตหน่วยงานภายนอก ตลอดจนอาจ กำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
“ระบบคอมพิวเตอร์ (Computer System)”	หมายถึง	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
“ระบบเครือข่าย (Network System)”	หมายถึง	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ สทอภ. ได้แก่ ระบบ LAN ระบบ Intranet ระบบ Internet เป็นต้น

“ระบบ LAN (Local Area Network) และ “ระบบอินทราเน็ต (Intranet)”	หมายถึง	ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานของ สทอภ. เข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
“ระบบอินเทอร์เน็ต (Internet)”	หมายถึง	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ ต่างๆ ของ สทอภ. เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
“ระบบเทคโนโลยีสารสนเทศ (Information Technology System)”	หมายถึง	ระบบงานของ สทอภ. ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์ และ ระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่ สทอภ. สามารถ นำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการ ให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) โปรแกรม (Software) ข้อมูล (Data) สารสนเทศ (Information) เป็นต้น
“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspaces)”	หมายถึง	พื้นที่ที่ สทอภ. อนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น • พื้นที่ทำงานทั่วไป • พื้นที่ทำงานของผู้ดูแลระบบ • พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย • พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์
“เจ้าของข้อมูล (Data Owner)”	หมายถึง	ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้นๆ หรือได้รับ ผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหายหรือเสียหาย
“เจ้าของระบบงาน (System Owner)”	หมายถึง	ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลและ พัฒนาระบบ ของ สทอภ.
“สินทรัพย์ (Asset)”	หมายถึง	สินทรัพย์ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สทอภ. ได้แก่ อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
“จดหมายอิเล็กทรอนิกส์ (e-mail)”	หมายถึง	ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง
“ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address)”	หมายถึง	ชุดอักขระที่ระบุเฉพาะเจาะจงถึงตำแหน่งที่อยู่ของตู้ไปรษณีย์ของผู้ที่ ใช้จดหมายอิเล็กทรอนิกส์ ซึ่งจะประกอบด้วยชื่อของบุคคล ได้แก่ First name และตามด้วยสัญลักษณ์ @ และชื่อของโดเมน (Domain name) ได้แก่ username@gistda.or.th
“รหัสผ่าน (Password)”	หมายถึง	เครื่องมือรักษาความปลอดภัยที่ประกอบด้วยชุดของตัวอักษร ซึ่งใช้ตรวจสอบสิทธิในการเข้าถึงระบบแก่ผู้ใช้แต่ละคน เพื่อแสดงรับรองความถูกต้องแท้จริง (Authentication) ของผู้ใช้
“ชุดคำสั่งไม่พึงประสงค์ (Malicious Code)”	หมายถึง	ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

“ช่องโหว่ (Vulnerability)” “ความเสี่ยง (Risk)”	หมายถึง	ช่องทางของระบบซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ที่ทำให้ระบบสารสนเทศไม่ สามารถทำงานได้ตามวัตถุประสงค์
“มัลแวร์ (Malware)”	หมายถึง	โปรแกรมคอมพิวเตอร์สร้างขึ้นมาเพื่อให้เกิดความเสียหายหรือรบกวนการทำงานของระบบทำให้ข้อมูลรั่วไหลเปิดช่องให้มีผู้บุกรุกเข้ามาหรือสร้างความเดือดร้อนรำคาญ ได้แก่ ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนคอมพิวเตอร์ (Computer Worm) ม้าโทรจัน (Trojan Horse) โปรแกรมเข้ารหัสไฟล์คอมพิวเตอร์เพื่อเรียกค่าไถ่ (Ransomware) เป็นต้น
“แชร์แวร์ (Shareware)”	หมายถึง	โปรแกรมที่ผู้ผลิตหรือผู้ที่ได้ลิขสิทธิ์โปรแกรมนั้น ๆ ยินยอมให้สามารถ ทดลองใช้โปรแกรม ซึ่งอาจจะใช้งานได้ครบตามความสามารถ ทั้งหมดของโปรแกรมหรือเพียงบางส่วน แต่มีกำหนดระยะเวลาหรือจำนวนการใช้งานเมื่อครบตามที่ได้ตกลงกันไว้ก็ไม่สามารถใช้โปรแกรมได้ต้องสั่งซื้อโปรแกรมจากผู้ผลิตเพื่อใช้งานต่อไป
“ฟรีแวร์ (Freeware)”	หมายถึง	โปรแกรมที่ผู้ผลิตหรือผู้ที่ได้ลิขสิทธิ์โปรแกรมนั้น ๆ ยินยอมให้มีการคัดลอก และนำไปใช้ได้โดยไม่คิดค่าใช้จ่าย
“ชุดคำสั่งต้นฉบับ (Source Code)”	หมายถึง	เป็นชุดคำสั่งที่ใช้สั่งงานคอมพิวเตอร์หรือภาษาในโปรแกรมคอมพิวเตอร์โดยปกติจะเป็นข้อความ (Text) ที่มนุษย์สามารถอ่านเข้าใจได้ เมื่อคอมพิวเตอร์ได้รับคำสั่งจาก Source Code คอมพิวเตอร์ก็จะทำการแปลงเป็นภาษาที่คอมพิวเตอร์เข้าใจ โดยใช้ Interpreter หรือ Compiler ในการแปลง
“โอเพนซอร์ส (Open Source)”	หมายถึง	ซอฟต์แวร์ที่สามารถนำไปใช้งาน ศึกษา แก้ไข และเผยแพร่ได้อย่างเสรี ปราศจากเงื่อนไขเพิ่มเติม การพัฒนาที่เปิดเผย Source Code ให้สาธารณะนำไปพัฒนาต่อยอดได้ ทำให้เกิดการร่วมมือกันทำงานอย่างไร้พรมแดนผ่านเครือข่ายอินเทอร์เน็ต
“หน่วยงานดูแลรับผิดชอบด้านตรวจสอบภายใน”	หมายถึง	หน่วยงานของ สทอภ. ที่มีหน้าที่รับผิดชอบในการสอบทานให้ดำเนิน ไปภายใต้มาตรฐานและแนวทางการปฏิบัติที่ได้กำหนดไว้ในนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ สทอภ. โดยหน่วยงานที่รับผิดชอบคือ สำนักตรวจสอบภายใน ของ สทอภ.
“หน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง”	หมายถึง	หน่วยงานของ สทอภ. ที่มีหน้าที่รับผิดชอบในการวิเคราะห์และประเมินความเสี่ยงระบบสารสนเทศของ สทอภ. ที่เกี่ยวกับการบริหารงาน เพื่อให้ สทอภ. มีคุณภาพ ประสิทธิภาพในการปฏิบัติงานมากยิ่งขึ้น และลดโอกาสความเสียหายที่อาจจะเกิดขึ้นได้ โดยหน่วยงานที่รับผิดชอบคือ ฝ่ายจัดการเทคโนโลยีและระบบสารสนเทศกลาง ของ สทอภ.

“หน่วยงานดูแลรับผิดชอบด้านกฎหมาย”	หมายถึง	หน่วยงานของ สทอภ. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการดำเนินการยกร่างกฎหมาย พิจารณา และให้คำปรึกษาตอบข้อหารือที่เกี่ยวกับ กฎหมาย ระเบียบ คำสั่ง บันทึกสั่งการดำเนินการเกี่ยวกับนิติกรรม ของ สทอภ. ดำเนินการบอกกล่าวทวงถาม รวบรวมพยานหลักฐาน เพื่อดำเนินคดี ดำเนินการสอบสวนข้อเท็จจริงและหาผู้รับผิดทางแพ่ง ให้คำปรึกษาทางกฎหมายแก่ “เจ้าหน้าที่” ของ สทอภ. ตลอดจน ประสานงานกับหน่วยงานต่าง ๆ ในเรื่องที่เกี่ยวข้อง โดยหน่วยงานที่รับผิดชอบคือ ฝ่ายกฎหมายและสัญญา ของ สทอภ.
“หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ”	หมายถึง	หน่วยงานของ สทอภ. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการกำหนดนโยบายและแนวทางปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ติดต่อประสานงานความร่วมมือทางด้านความมั่นคงปลอดภัยระหว่างองค์กร วางแผนควบคุมระบบความมั่นคงปลอดภัยด้านสารสนเทศและการเตือนภัย รวมถึงวิเคราะห์หาวิธีการแก้ไขช่องโหว่ของระบบสารสนเทศ และรายงานเกี่ยวกับการฝ่าฝืนนโยบายดังกล่าวไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) โดยหน่วยงานที่รับผิดชอบคือ ฝ่ายจัดการเทคโนโลยีและระบบสารสนเทศกลาง ของ สทอภ.
“หน่วยงานดูแลรับผิดชอบการบริหารงานบุคคล”	หมายถึง	หน่วยงานของ สทอภ. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการสรรหา “เจ้าหน้าที่” ใหม่ การตรวจสอบคุณสมบัติของผู้สมัคร การกำหนด เงื่อนไขการจ้างงาน การลงนามมิให้เปิดเผยความลับของ สทอภ. รวมทั้งการรายงานเกี่ยวกับการจ้างงาน การเปลี่ยนแปลงสภาพการจ้างงาน การลาออกจากงาน การถึงแก่กรรม การโยกย้าย และการพักงานหรือการลงโทษทางวินัยให้แก่หน่วยงานที่รับผิดชอบระบบสารสนเทศทราบ โดยหน่วยงานที่รับผิดชอบคือ ฝ่ายทรัพยากรบุคคล ของ สทอภ.
“หน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร”	หมายถึง	หน่วยงานของ สทอภ. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการจัดการประชุม สัมมนา หรืออบรมให้ความรู้แก่บุคลากรและผู้ใช้งานเกี่ยวกับวิธีปฏิบัติงาน เพื่อสร้างความมั่นคงปลอดภัยให้กับสารสนเทศของ สทอภ. โดยหน่วยงานที่รับผิดชอบคือ ฝ่ายพัฒนาศักยภาพองค์กร ของ สทอภ.
“หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่”	หมายถึง	หน่วยงานของ สทอภ. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ควบคุมการเข้า-ออก อาคารและสำนักงาน จัดเตรียมการป้องกันต่อภัยคุกคามต่าง ๆ ทั้ง จากมนุษย์และธรรมชาติ ได้แก่ ไฟไหม้ น้ำท่วม เป็นต้น โดย หน่วยงานที่รับผิดชอบคือ ฝ่ายพัสดุ ของ สทอภ.
“หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและสินทรัพย์ที่เป็นซอฟต์แวร์”	หมายถึง	หน่วยงานของ สทอภ. ที่มีหน้าที่รับผิดชอบเกี่ยวกับการจัดการข้อมูล และสินทรัพย์ที่เป็นซอฟต์แวร์ โดยหน่วยงานที่รับผิดชอบคือ ฝ่ายจัดการเทคโนโลยีและระบบสารสนเทศกลาง ของ สทอภ.

“หน่วยงานที่รับผิดชอบอุปกรณ์สำคัญของระบบสารสนเทศ”	หมายถึง	หน่วยงานของ สทอภ. ที่มีอุปกรณ์สำคัญของระบบสารสนเทศและมี ห้อง Server/Data Center ในความดูแล หน้าที่รับผิดชอบดูแลอุปกรณ์สำคัญของระบบสารสนเทศที่ครอบครองอยู่ คือ ฝ่ายจัดการเทคโนโลยีและระบบสารสนเทศกลาง ของ สทอภ.
“การบริหารจัดการเปลี่ยนแปลง (Change Management)”	หมายถึง	การเปลี่ยนแปลงระบบสารสนเทศ ซึ่งการเปลี่ยนแปลงดังกล่าวจะมีผลกระทบต่อฮาร์ดแวร์ ซอฟต์แวร์ระบบ (System Software) โปรแกรมประยุกต์ (Application Software) ระบบเครือข่าย เป็นต้น
“เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event)”	หมายถึง	สภาพของการให้บริการหรือการแจ้งเตือนของระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident)”	หมายถึง	สถานการณ์ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม
“ข้อมูลและสารสนเทศที่กำหนดชั้นความลับ (Confidential Data and Information)”	หมายถึง	ข้อมูลและสารสนเทศที่มีความสำคัญ และเป็นความลับทางราชการ ซึ่งถ้าหากถูกเปิดเผยออกไปแล้ว จะเกิดความเสียหายหรือเกิดผลเสียอื่น ๆ ต่อหน่วยงานภาครัฐ ซึ่ง สทอภ. ได้กำหนดชั้นความลับตาม ความสำคัญของเนื้อหา การจำกัดการเข้าถึงและจำกัดให้ทราบเท่าที่จำเป็นสอดคล้องกับ “ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544” โดยได้กำหนดชั้นความลับของข้อมูลและสารสนเทศไว้ 3 ระดับ คือ ชั้นลับที่สุด ชั้นลับมาก และชั้นลับ
“ชั้นลับที่สุด (Top Secret)”	หมายถึง	ข้อมูลและสารสนเทศซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐและ สทอภ. อย่างร้ายแรงที่สุด “ผู้บริหาร” และ “เจ้าของข้อมูลและสารสนเทศ” เท่านั้นที่จะสามารถเข้าใช้งานข้อมูลและสารสนเทศประเภทนี้ได้ “ผู้ใช้” ที่ ต้องการใช้ข้อมูลและสารสนเทศดังกล่าวจะต้องได้รับอนุญาตจาก “ผู้บริหารระดับกลาง” ของเจ้าของข้อมูลและสารสนเทศขึ้นไปเท่านั้น ตัวอย่างข้อมูลและสารสนเทศชั้นลับที่สุด ได้แก่ • รายงานเสนอการแต่งตั้ง ถอดถอนหรือโยกย้ายเจ้าหน้าที่ในตำแหน่งที่สำคัญมาก • การเจรจาข้อตกลงที่สำคัญกับหน่วยงานที่เกี่ยวข้อง • สัญญาที่ทำขึ้นระหว่างองค์กร • เทคนิคที่ต้องอาศัยความชำนาญพิเศษ • อื่นๆ ตามที่เจ้าของข้อมูลและสารสนเทศกำหนด

“ชั้นลับมาก (Secret)”	หมายถึง	ข้อมูลบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐและ สทอภ. อย่างร้ายแรง หากถูกเปิดเผยออกไปหรือสูญหายจะก่อให้เกิดผลกระทบต่อประสิทธิภาพในการปฏิบัติงานของหน่วยงานอาจจะก่อให้เกิดความสูญเสียความเชื่อมั่นโดย “ผู้บริหาร” และ “เจ้าของข้อมูลและสารสนเทศ” เท่านั้นที่จะสามารถเข้าใช้งานข้อมูลและสารสนเทศประเภทนี้ได้ “ผู้ใช้” ที่ต้องการใช้ข้อมูลและสารสนเทศดังกล่าว จะต้องได้รับอนุญาตจาก “ผู้บริหารระดับต้น” ของเจ้าของข้อมูลและสารสนเทศขึ้นไปเท่านั้น ตัวอย่างข้อมูลและสารสนเทศชั้นลับมาก ได้แก่ • การดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงตำแหน่งที่สำคัญใน สทอภ. • ระเบียบวาระและรายงานการประชุมลับ • ประกาศหรือคำสั่งที่สำคัญที่อยู่ระหว่างการดำเนินการ • อื่น ๆ ตามที่เจ้าของข้อมูลและสารสนเทศกำหนด
“ชั้นลับ (Confidential)”	หมายถึง	ข้อมูลและสารสนเทศลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์ของ สทอภ. ซึ่งไม่พึงเปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบ ในกรณี “ผู้ใช้” ที่ต้องการใช้ข้อมูลและสารสนเทศ ดังกล่าวจะต้องได้รับอนุญาตจาก “เจ้าของข้อมูลและสารสนเทศ” เป็นอย่างน้อย ตัวอย่างข้อมูลและสารสนเทศชั้นลับ ได้แก่ • ขั้นตอนปฏิบัติงานภายใน สทอภ. • อื่นๆ ตามที่เจ้าของข้อมูลและสารสนเทศกำหนด
ชั้นความลับของระบบสารสนเทศ	หมายถึง	ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศ ที่ต้องเก็บเป็นความลับ ได้แก่ รายชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ที่ใช้สำหรับเข้าสู่ระบบงานคอมพิวเตอร์ต่าง ๆ การตั้งค่าระบบ (Configuration) สิทธิ์ในการใช้งานระบบสารสนเทศ (Access Control list) เป็นต้น
สื่อสังคมออนไลน์ (Social Media)	หมายถึง	ช่องทางหรือสื่อใด ๆ ที่ใช้เผยแพร่ข้อมูลและแสดงความคิดเห็นบนโลก ออนไลน์ ที่เปิดโอกาสให้ผู้ใช้สามารถสร้างสรรค์เนื้อหาได้ด้วยตนเองได้แก่ บล็อกเสรี (Blog) วิกิพีเดีย (Wikipedia) พันทิป (Pantip) เว็บเครือข่ายสังคม (Social Network) ต่างๆ ได้แก่ Facebook Twitter LinkedIn Line Instagram Flickr Myspace Multiply และ YouTube เป็นต้น
ผู้มีส่วนได้ส่วนเสีย	หมายถึง	บุคลากรภายนอก ได้แก่ ผู้รับบริการ ประชาชน ผู้ประกอบการ บุคคลทั่วไป หน่วยงานราชการ รัฐวิสาหกิจ ภาคเอกชน สทอภ. ระหว่างประเทศที่เกี่ยวข้อง สถานศึกษา นิสิต นักศึกษา
โพสต์ (Post)	หมายถึง	การส่งข้อความตัวอักษร ภาพ หรือคลิปวีดิโอ คลิปเสียง การถ่ายทอดสดผ่านสื่อสังคมออนไลน์ การเข้าสู่สื่อออนไลน์ ได้แก่ เว็บไซต์ เพื่อแสดงความคิดเห็นหรือเผยแพร่ข้อมูลข่าวสาร
ข้อมูลส่วนบุคคล	หมายถึง	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ไซเบอร์	หมายถึง	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป
การรักษาความมั่นคงปลอดภัยไซเบอร์	หมายถึง	มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ
ภัยคุกคามทางไซเบอร์	หมายถึง	การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ	หมายถึง	คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความ มั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทาง เศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์ สาธารณะ

หมวด 1
นโยบายความมั่นคงปลอดภัย
(Security Policy)

1. คำแถลงนโยบาย

สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (สทอภ.) จัดทำนโยบายนี้เพื่อเป็นส่วนหนึ่งของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ในการป้องกันภัยคุกคาม ลดความเสี่ยงจากช่องโหว่และผู้บุกรุก เพื่อให้สารสนเทศมีความปลอดภัย สามารถรักษาความลับและความถูกต้องของข้อมูล และมีความพร้อมในการให้บริการอยู่ในระดับที่ยอมรับได้ สทอภ. จึงได้กำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศเพื่อเป็นแนวทางเสริมสร้างความมั่นคงปลอดภัยด้านสารสนเทศให้กับ สทอภ. หรือหน่วยงานที่มีความเกี่ยวข้องในการปฏิบัติงานกับ สทอภ. โดยนโยบายนี้มีจุดประสงค์เพื่อการสนับสนุนการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของ สทอภ. ดังนี้

- เพื่อให้เกิดความเชื่อมั่นและมีความปลอดภัยในการใช้งานระบบสารสนเทศของ สทอภ. ทำให้การปฏิบัติงานมีประสิทธิภาพและประสิทธิผล
- เพื่อการใช้งานเป็นไปตามภารกิจของ สทอภ. ในการควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยให้มีการควบคุมการเข้าถึงสารสนเทศ และปรับปรุงให้สอดคล้องกับ ข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย
- เพื่อเผยแพร่ให้ **“เจ้าหน้าที่ (Officer)”** ทุกระดับใน สทอภ. ได้รับทราบ และทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- เพื่อให้มีการดำเนินการที่เหมาะสมและสัมฤทธิ์ผล มีการตรวจสอบและประเมินนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
- เพื่อสร้างความตื่นตัวให้**“เจ้าหน้าที่ (Officer)”** และ **“หน่วยงานภายนอก”** ที่ปฏิบัติงานให้กับ สทอภ. ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ
- เพื่อดำเนินการหรือประสานงานกับหน่วยงานอื่น ๆ ทั้งภายในประเทศและต่างประเทศในการสนับสนุนความรู้หรือข้อมูลด้านความมั่นคงปลอดภัย ที่เป็นประโยชน์ต่อการทำงานหรือการพัฒนาบุคลากรที่ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

2. องค์ประกอบของนโยบาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สทอภ. ใช้แนวทางและกระบวนการโดยอ้างอิงจากพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2.5) ประจำปี 2550 รายละเอียดบางส่วนจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรฐาน ISO/IEC 27001 ซึ่งประกอบด้วย 11 หมวด ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังต่อไปนี้

หมวด 1 นโยบายความมั่นคงปลอดภัย (Security Policy) มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับการใช้งานระบบสารสนเทศของ สทอภ. เพื่อให้สอดคล้องกับข้อกำหนดทางราชการ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งจัดทำเป็นลายลักษณ์อักษร

โดยที่ฝ่ายบริหารเห็นชอบและอนุมัติ และเผยแพร่ให้ “เจ้าหน้าที่” ทุกระดับได้รับรู้ มีการทบทวนนโยบายฯ ตามระยะเวลาที่กำหนดพร้อมทั้งปรับเปลี่ยนนโยบายตามความเหมาะสม

หมวด 2 โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information security) มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สทอภ. ที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก โดยจัดให้มีคณะทำงานและบุคลากรเฉพาะด้านความมั่นคงปลอดภัย มีการประสานงานความรับผิดชอบ ประเมินความเสี่ยง และตรวจสอบการทำงานด้านความมั่นคงปลอดภัย รวมทั้งประสานงานกับหน่วยงานภายนอกและผู้ใช้งานสารสนเทศจากภายนอก โดยมีการระบุและจัดทำข้อกำหนดที่ชัดเจนในการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สทอภ.

หมวด 3 การบริหารจัดการทรัพย์สิน (Asset Management) มีจุดประสงค์เพื่อป้องกันทรัพย์สินของ สทอภ. จากความเสียหายที่อาจเกิดขึ้นได้ และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสม โดยมีการจัดทำบัญชีทรัพย์สิน ระบุผู้เป็นเจ้าของทรัพย์สิน และกำหนดหลักเกณฑ์การใช้งานทรัพย์สินที่เหมาะสม มีการจัดหมวดหมู่ทรัพย์สินตามระดับชั้นความลับและจัดทำป้ายชื่อเพื่อการบริหารจัดการทรัพย์สินตามที่ได้จัดหมวดหมู่ไว้

หมวด 4 ความมั่นคงปลอดภัยทางด้านทรัพยากรบุคคล (Human Resource Security) มีจุดประสงค์เพื่อให้ “เจ้าหน้าที่ (Officer)” ผู้ที่ สทอภ. ทำสัญญาจ้างและหน่วยงานภายนอก เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตน ทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และการสิ้นสุดหรือการเปลี่ยนการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

หมวด 5 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) มีจุดประสงค์เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ป้องกันสินทรัพย์ไม่ให้เกิดการสูญหาย ถูกขโมย เกิดความเสียหาย เกิดการก่อกวนหรือแทรกแซง ป้องกันการถูกเปิดเผยโดยไม่ได้รับอนุญาต และป้องกันไม่ให้กิจกรรมการดำเนินงานต่างๆ ของ สทอภ. เกิดการติดขัดหรือหยุดชะงัก ได้แก่ การมีระบบกระแสไฟฟ้าสำรอง ระบบสื่อสารสำรอง เป็นต้น

หมวด 6 การบริหารจัดการด้านการสื่อสารและการดำเนินงาน (Communications and Operations Management) มีจุดประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย รักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลง ลดความเสี่ยงจากความล้มเหลวของระบบป้องกันซอฟท์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟท์แวร์ที่ไม่ประสงค์ดี ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายสินทรัพย์โดยไม่ได้รับอนุญาต รักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกัน สร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ และตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

หมวด 7 การควบคุมการเข้าถึง (Access Control) มีจุดประสงค์เพื่อควบคุมการเข้าถึงหรือควบคุมการใช้งานสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

หมวด 8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition, Development and Maintenance) มีจุดประสงค์เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ ป้องกันความผิดพลาด การสูญหายและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาตหรือการใช้งานสารสนเทศผิดวัตถุประสงค์ รักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยวิธีการเข้ารหัสข้อมูล สร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์ สารสนเทศ และไฟล์ต่างๆ ของระบบที่ให้บริการ ลดความความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

หมวด 9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information Security Incident Management) มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ สทอภ. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศของ สทอภ. รวมถึงการรับมือภัยคุกคามทางไซเบอร์

หมวด 10 การบริหารความต่อเนื่องในการดำเนินงาน (Continuity Management) มีจุดประสงค์เพื่อป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมต่าง ๆ ป้องกันกระบวนการทำงานที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

หมวด 11 การปฏิบัติตามข้อกำหนด (Compliance) มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อการปฏิบัติงานน้อยที่สุด

หมวด 2
โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร
(Organization of Information Security)

จุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สทอภ. ที่ถูกเข้าถึงถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก โดยจัดให้มีคณะทำงานและบุคลากรเฉพาะด้านความมั่นคงปลอดภัย มีการประสานงานความรับผิดชอบประเมินความเสี่ยง และตรวจสอบการทำงานด้านความมั่นคงปลอดภัย รวมทั้งประสานงานกับหน่วยงานภายนอกและผู้ใช้งานสารสนเทศจากภายนอก โดยมีการระบุและจัดทำข้อกำหนดที่ชัดเจนในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สทอภ. โดยประกอบด้วย

- นโยบายสิทธิ หน้าที่และความรับผิดชอบ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ
- นโยบายการควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศต่อหน่วยงานภายนอก
- นโยบายสำหรับผู้ปฏิบัติงานชั่วคราว

นโยบายสิทธิ หน้าที่และความรับผิดชอบ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

1. วัตถุประสงค์

นโยบายนี้ระบุถึงสิทธิของผู้ใช้งาน หน้าที่ และความรับผิดชอบของบุคคล หน่วยงานที่มีส่วนเกี่ยวข้องในการใช้งาน การดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ สทอภ. เพื่อเป็นการปกป้องสินทรัพย์ของ สทอภ. ให้มีความมั่นคงปลอดภัยนโยบายนี้มีผลกับผู้ใช้งานที่มีส่วนเกี่ยวข้องกับ สทอภ. ทั้งหมด

2. สิทธิหน้าที่และความรับผิดชอบ

2.1. “ผู้บริหารระดับสูงสุด” “ผู้บริหารระดับสูง” และ “CIO”

หน้าที่ และความรับผิดชอบ

2.1.1. ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่ สทอภ. หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศของ สทอภ. ต้องเป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้น โดยมีอำนาจจัดตั้งคณะกรรมการเพื่อสอบสวนข้อเท็จจริงที่เกิดขึ้น

สิทธิ

2.1.2. สามารถกำหนดชั้นความลับทุกชั้นความลับ สำหรับข้อมูลและสารสนเทศที่กำหนดชั้นความลับของ สทอภ. ที่อยู่ภายใต้สายงานการบังคับบัญชา

2.1.3. สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

2.1.4. สามารถสั่งการอนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

2.1.5. สามารถมอบอำนาจอย่างเป็นลายลักษณ์อักษรให้ผู้ใต้บังคับบัญชามีสิทธิในการสั่งการอนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งาน

สารสนเทศที่กำหนด ชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

2.1.6. สามารถแต่งตั้งให้ “เจ้าหน้าที่” ของ สทอภ. ทำหน้าที่เป็นผู้ดูแลระบบสำหรับงานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา

2.1.7. สามารถอนุญาตให้หน่วยงานภายนอกเข้ามาปฏิบัติงานกับระบบสารสนเทศของ สทอภ.

2.1.8. สามารถกำหนดและจำแนกพื้นที่ใช้งานระบบสารสนเทศของ สทอภ. ที่อยู่ภายใต้สายงานการบังคับบัญชา

2.1.9. สามารถกำหนดสิทธิของผู้ใช้งานในการผ่านเข้าออกพื้นที่ใช้งานระบบสารสนเทศของ สทอภ. ที่อยู่ภายใต้สายงานการบังคับบัญชา และต้องกำกับดูแลให้ผู้ที่มีสิทธิผ่านเข้าออกดังกล่าว ปฏิบัติตามนโยบาย กฎระเบียบ ข้อบังคับ อันเกี่ยวข้องกับระบบสารสนเทศของ สทอภ. อย่างเคร่งครัด

2.2. “ผู้บริหารระดับสูงสุด” “ผู้บริหารระดับสูง” และ “CIO”

หน้าที่ และความรับผิดชอบ

2.2.1. ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่ สทอภ. หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศของ สทอภ. ต้องเป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหายหรืออันตรายที่เกิดขึ้น โดยมีอำนาจจัดตั้งคณะกรรมการเพื่อสอบสวนข้อเท็จจริงที่เกิดขึ้น

2.2.2. มีหน้าที่แจ้งต่อหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เพื่อให้รับทราบและรวบรวมข้อมูลอันเกี่ยวกับ

- การกำหนดหรือเปลี่ยนแปลงสิทธิของผู้ใช้งานที่อยู่ภายใต้สายงานการบังคับบัญชา
- การกำหนดหรือเปลี่ยนแปลงพื้นที่ใช้งานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา
- การกำหนดหรือเปลี่ยนแปลงชั้นความลับของข้อมูลที่อยู่ภายใต้สายงานการบังคับบัญชา

สิทธิ

2.2.3. สามารถกำหนดชั้นความลับทุกชั้นความลับ สำหรับข้อมูลและสารสนเทศที่กำหนดชั้นความลับของ สทอภ. ที่อยู่ภายใต้สายงานการบังคับบัญชา

2.2.4. สามารถเสนอต่อผู้บริหารระดับสูง เพื่อพิจารณาสั่งการให้ข้อมูลหรือสารสนเทศอันเป็นผลลัพธ์ ซึ่งเกิดจากการประมวลผลข้อมูลหรือสารสนเทศที่มาจากสายงานการบังคับบัญชา (ได้แก่ ผลลัพธ์จากการประมวลผลข้อมูลหรือสารสนเทศที่มาจากหลายหน่วยงาน หรือมีการกำหนดชั้นความลับไว้ต่างกัน) ได้รับการกำหนดชั้นความลับตามความเหมาะสม

2.2.5. สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับทุกชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

2.2.6. สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับอื่นๆ ของ สทอภ. เท่าที่ ได้รับอนุญาตจากผู้บริหารระดับสูง

2.2.7. สามารถสั่งการ อนุญาต เพิกถอน และระงับสิทธิของผู้ใช้งานในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับที่อยู่ภายใต้สายงานการบังคับบัญชา

2.2.8. สามารถเสนอเพื่อแต่งตั้งให้ “เจ้าหน้าที่ (Officer)” ของ สทอภ. ทำหน้าที่เป็นผู้ดูแลระบบสำหรับงานระบบสารสนเทศที่อยู่ภายใต้สายงานการบังคับบัญชา ทั้งนี้ขึ้นอยู่กับหน้าที่ความผิดชอบของหน่วยงานนั้นๆ

2.2.9. สามารถเสนอต่อผู้บริหารระดับสูงเพื่อขออนุญาตให้หน่วยงานภายนอกเข้าปฏิบัติงานกับระบบสารสนเทศของ สทอภ. ที่อยู่ภายใต้สายงานการบังคับบัญชา

2.2.10. สามารถกำหนดและจำแนกพื้นที่ใช้งานระบบสารสนเทศของ สทอภ. ที่อยู่ภายใต้สายงานการบังคับบัญชา

2.2.11. สามารถกำหนดสิทธิของผู้ใช้งานในการผ่านเข้าออกพื้นที่ใช้งานระบบสารสนเทศของ สทอภ. ที่อยู่ภายใต้สายงานการบังคับบัญชา และมีหน้าที่ต้องกำกับดูแลให้ผู้ที่มีสิทธิผ่านเข้าออกดังกล่าว ปฏิบัติตามนโยบาย กฎระเบียบ ข้อบังคับ อันเกี่ยวข้องกับระบบสารสนเทศของ สทอภ. อย่างเคร่งครัด

2.3. “ผู้บริหารระดับต้น”

หน้าที่ และความรับผิดชอบ

2.3.1. ควบคุมดูแลให้ผู้ใต้บังคับบัญชาปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

2.3.2. ควบคุม ดูแล รับผิดชอบอุปกรณ์ด้านเทคโนโลยีสารสนเทศของหน่วยงาน

สิทธิ

2.3.3. สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับเฉพาะ “ชั้นลับ” ที่อยู่ภายใต้สายงานการบังคับบัญชา

2.3.4. สามารถเข้าถึงและใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับเฉพาะ “ชั้นลับมาก” เท่าที่ได้รับอนุญาตจาก “ผู้บริหารระดับสูง” โดยต้องผ่านความเห็นชอบของ “ผู้บริหารระดับกลาง” ที่เป็นเจ้าของงานระบบสารสนเทศ

2.3.5. สามารถอนุญาตให้บุคคลหรือผู้ใช้งานยืมอุปกรณ์ด้านเทคโนโลยีสารสนเทศในความรับผิดชอบ ได้แก่ Projector, PC เป็นต้น

2.4. “ผู้ดูแลระบบ (System Administrator)”

หน้าที่ และความรับผิดชอบ

2.4.1. ไม่มีสิทธิเปิดอ่านจดหมายอิเล็กทรอนิกส์หรือการสื่อสารระหว่างกันที่เป็นส่วนตัว (ได้แก่ Gmail, Outlook, line) ของ “ผู้ใช้งาน” ยกเว้นในกรณีที่ใช้ในการสืบสวนเกี่ยวกับการใช้งาน ระบบอย่างไม่ถูกต้อง หรือละเมิดสิทธิผู้อื่น หรือมีการร้องขอจากหน่วยงานภายนอกตามคำสั่ง ศาลหรือตามกฎหมาย

2.4.2. ไม่มีสิทธิเปิดอ่าน หรือใช้งานข้อมูลและสารสนเทศที่กำหนดชั้นความลับ ยกเว้นในกรณีที่ได้รับอนุญาตสิทธิเป็นลายลักษณ์อักษรจากผู้บริหาร สทอภ. ที่สามารถอนุญาตสิทธิในการเข้าถึง หรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับนั้น

2.4.3. แจ้งให้ผู้ใช้งานทราบล่วงหน้าถึงวันเวลาที่ต้องปิดระบบเพื่อบำรุงรักษาปรับปรุงหรือเปลี่ยนแปลงระบบ ซึ่งส่งผลให้ต้องหยุดบริการในช่วงเวลาหนึ่ง ยกเว้นในกรณีฉุกเฉินผู้ดูแล ระบบมีสิทธิปิดระบบทันที และจะต้องพยายามให้ผู้ใช้งานสามารถเก็บบันทึกข้อมูลได้อย่างสมบูรณ์ก่อนที่จะดำเนินการปิดระบบ และทำรายงานให้ผู้บังคับบัญชาทราบ

2.4.4. ต้องดูแลรักษา ตรวจสอบแก้ไข และเสนอ สทอภ. ให้ปรับปรุงระบบสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อให้ระบบสามารถใช้งานได้ดี มีเสถียรภาพ มีความมั่นคงปลอดภัย และมีประสิทธิภาพอยู่เสมอ

2.4.5. ติดตาม กำชับผู้ใช้งาน และปรับปรุงฐานข้อมูลของผู้ใช้งาน ให้มีความถูกต้องเป็นปัจจุบันอยู่เสมอ รวมทั้งต้องลบบัญชีผู้ใช้งานของผู้ที่หมดสิทธิในการใช้งานระบบออกจากฐานข้อมูล

2.4.6. ต้องติดตามข่าวสาร ภาวะภัยคุกคาม ช่องโหว่ของระบบสารสนเทศ และต้องปรับปรุงดูแลระบบเพื่อลดความเสี่ยงของการถูกบุกรุกอย่างสม่ำเสมอ

2.4.7. ต้องขออนุญาตผู้บังคับบัญชาในกรณีที่มีการร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ในการประเมิน ตรวจสอบ ทดสอบ หาจุดอ่อนช่อง โหว่ อันเกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศ และทำการแก้ไขอย่างรวดเร็ว

2.4.8. ต้องแจ้งต่อหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ทันทีและทำรายงานแจ้งผู้บังคับบัญชาตามลำดับชั้น ในกรณีที่ตรวจพบหรือได้รับรายงานจาก ผู้ใช้งานหรือสงสัยว่าระบบสารสนเทศที่รับผิดชอบโดยตรงหรือระบบที่เกี่ยวข้องอื่นใดของ สทอภ. ถูกละเมิดทางด้านความมั่นคงปลอดภัย

สิทธิ

2.4.9. สามารถยุติการทำงานของระบบสารสนเทศ ซึ่งพบว่าเป็นภัยต่อความมั่นคงปลอดภัย หรือ สร้างภาระให้ระบบสารสนเทศของ สทอภ. โดยไม่จำเป็นต้องมีการแจ้งล่วงหน้าในกรณีฉุกเฉิน เท่านั้น และติดตามสอบสวนหาสาเหตุที่มาของภัยหรือภาระนั้น และทำรายงานให้ผู้บังคับบัญชาที่รับผิดชอบระบบทราบ

2.4.10. สามารถยุติการทำงานของระบบสารสนเทศที่เปิดใช้โดยไม่ได้รับอนุญาตจาก สทอภ. โดยไม่ต้องมีการแจ้งล่วงหน้า และติดตามสอบสวนหาสาเหตุที่มาของระบบงานนั้น และทำรายงาน ให้ผู้บังคับบัญชาทราบ

2.4.11. สามารถจำกัดหรือระงับสิทธิของผู้ใช้งานระบบอย่างไม่เหมาะสม และแจ้งให้ผู้บริหาร สทอภ. ตั้งคณะกรรมการพิจารณาสอบสวนหรือลงโทษตามความเหมาะสม

2.5. “เจ้าของข้อมูล (Information Owner)”

หน้าที่ และความรับผิดชอบ

2.5.1. ตรวจทานระดับชั้นความปลอดภัยของข้อมูลเพื่อให้มั่นใจว่ายังเป็นไปตามความต้องการของการปฏิบัติงานและมีความเหมาะสมและสอดคล้องกับระดับความปลอดภัยนั้น ๆ

2.5.2. ตรวจสอบให้แน่ใจว่าข้อมูลที่ได้มีการระบุหรือแสดงระดับความปลอดภัยตามที่ได้จัดระดับไว้อย่างถูกต้องและเหมาะสม ไม่ว่าจะอยู่ในรูปแบบหรือสื่อประเภทใดก็ตาม

2.5.3. จัดทำข้อกำหนดในการสำรองข้อมูล และดำเนินการให้มีการจัดการในเรื่องของการละเมิดความปลอดภัยอย่างเหมาะสม

สิทธิ

2.5.4. อนุมัติและตรวจทานเพื่อให้แน่ใจว่าสิทธิของผู้ใช้งานถูกต้องเหมาะสม

2.5.5. กำหนดระดับชั้นความปลอดภัยให้กับข้อมูล

2.5.6. กำหนดพื้นฐานการรักษาความปลอดภัยในการเข้าถึงข้อมูลของหน่วยงาน

2.6. “เจ้าของระบบงาน (Application Owner)”

หน้าที่ และความรับผิดชอบ

2.6.1. ตรวจสอบให้แน่ใจว่าระบบงานสามารถทำงานได้ถูกต้องตามความต้องการได้อย่างสม่ำเสมอ

2.6.2. ควบคุมดูแลความปลอดภัยในการเข้าใช้งานระบบงาน และความปลอดภัยของข้อมูล

2.6.3. อนุมัติ ตรวจทาน และรับรองสิทธิการเข้าใช้ระบบที่เหมาะกับระดับความสำคัญของข้อมูล

2.6.4. จัดทำข้อกำหนดในการสำรองข้อมูลและ Source Code ของระบบงาน

2.6.5. ดำเนินการหรือมีการจัดการในเรื่องของการละเมิดความปลอดภัยอย่างเหมาะสม

สิทธิ

2.6.6. สามารถมอบหมายหน้าที่และความรับผิดชอบดังกล่าวข้างต้นให้แก่บุคคลอื่นที่เหมาะสม แต่เจ้าของระบบงานยังคงมีหน้าที่และความรับผิดชอบต่อระบบงานดังกล่าวโดยสมบูรณ์

2.7. “ผู้ใช้ (Users)”

หน้าที่ และความรับผิดชอบ

2.7.1. อุปกรณ์ระบบคอมพิวเตอร์และระบบเครือข่าย สทอภ. มีไว้เพื่อใช้ในกิจการของ สทอภ. เท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บริหาร สทอภ.

2.7.2. ต้องช่วยกันรักษาอุปกรณ์ต่าง ๆ ไม่ให้เกิดความเสียหาย หากมีความเสียหายจากอุบัติเหตุ หรือ ภัยต่าง ๆ ผู้ใช้งานต้องรายงานผู้ดูแลระบบ และผู้บังคับบัญชาให้รับทราบทันที

2.7.3. การขอใช้งานอุปกรณ์และระบบต่าง ๆ ผู้ใช้งานต้องสามารถแสดงบัตรประจำตัวที่ถูกต้องได้หากผู้ดูแลระบบร้องขอ

2.7.4. พึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ ได้แก่ ไม่ Download ไฟล์ขนาดใหญ่โดยไม่จำเป็น ไม่ส่งหรือกระจายส่งต่อจดหมายอิเล็กทรอนิกส์ในลักษณะจดหมายลูกโซ่ ฯลฯ

2.7.5. เพื่อให้การบริหารระบบเป็นไปอย่างถูกต้อง ผู้ใช้งานต้องให้ข้อมูลประจำตัวที่ถูกต้องสำหรับการเปิดบัญชีผู้ใช้งาน (User ID หรือ Login Account)

2.7.6. ต้องรับผิดชอบในการกำหนดรหัสผ่าน (Password) ที่ปลอดภัยตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

2.7.7. ต้องไม่อนุญาตให้ผู้อื่นใช้งานระบบคอมพิวเตอร์ผ่านบัญชีผู้ใช้งานของตนโดยเด็ดขาด มิฉะนั้น ผู้ใช้งานอาจมีความผิดทางวินัยและต้องรับผิดชอบต่อปัญหาที่เกิดขึ้น ได้แก่ การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย ฯลฯ

2.7.8. ต้องรายงานต่อผู้ดูแลระบบและผู้บังคับบัญชาโดยทันที ในกรณีตรวจพบหรือสงสัยว่ามีการนำบัญชีผู้ใช้งานของตนหรือของผู้อื่นไปใช้งานโดยไม่ได้รับอนุญาต หรือใช้งานในทางมิชอบ และพบเห็นพฤติกรรมการล่วงละเมิดความมั่นคงปลอดภัยทุกอย่างในระบบ

2.7.9. ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

2.7.10. ไม่ล่วงล้ำเข้าในบริเวณพื้นที่ใช้งานระบบสารสนเทศที่ไม่ได้รับอนุญาต

2.7.11. ต้องใช้ระบบในลักษณะที่ถูกต้องตามกฎหมาย ไม่ละเมิดสิทธิ์และไม่ก่อความเดือดร้อนหรือความเสียหายแก่บุคคลหรือองค์กรอื่น

2.7.12. ไม่ติดตั้งหรือเปิดให้บริการระบบเครือข่ายบนเครื่องของ สทอภ. เพื่อทำภารกิจส่วนตัว

2.7.13. ต้องคืนสินทรัพย์ สทอภ. อันเกี่ยวกับการปฏิบัติหน้าที่ในทันทีที่พ้นหน้าที่ ได้แก่ อุปกรณ์ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ

2.7.14. ต้องทำรายงานแจ้งให้ผู้ดูแลระบบและผู้บังคับบัญชาทราบทันที ในกรณีที่มีการเคลื่อนย้ายถอดถอนอุปกรณ์ระบบสารสนเทศ

2.7.15. ต้องปฏิบัติตามมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และวิธีการปฏิบัติ (Procedure) อันเกี่ยวเนื่องกับความมั่นคงปลอดภัยด้านสารสนเทศของ สทอภ.

2.7.16. ห้ามผู้ใช้งานติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องของ สทอภ. ก่อนได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ เพื่อป้องกันปัญหาด้านลิขสิทธิ์ และ ปัญหาอื่นๆ ที่จะเกิดขึ้นภายหลังการติดตั้ง ได้แก่การติดตั้ง Access Point ด้วยตนเองแล้วเกิดการเจาะระบบเข้ามาในระบบเครือข่ายของ สทอภ.หรือทำให้เกิดการแพร่กระจายของ ไวรัสและภัยคุกคามอื่นๆ เป็นต้นควบคุมดูแลความปลอดภัยในการเข้าใช้งานระบบงานและความปลอดภัยของข้อมูล

2.7.17. หากพบว่าระบบรักษาความปลอดภัยมีข้อบกพร่อง หรือสงสัยว่า มีผู้ใดกระทำการที่น่าสงสัยให้แจ้งต่อผู้ดูแลระบบโดยทันที

2.7.18. ต้องให้ความร่วมมือกับเจ้าหน้าที่ที่ได้รับมอบหมายให้ทำการสืบสวนสอบสวนเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยของ สทอภ.

สิทธิ

2.7.19. สามารถเข้าถึงข้อมูลข่าวสาร ที่มิใช่ข้อมูลและสารสนเทศที่กำหนดชั้นความลับของ สทอภ. ยกเว้นในกรณีที่ได้รับอนุญาตสิทธิเป็นลายลักษณ์อักษรจากผู้บริหาร สทอภ. ที่สามารถอนุญาตสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศที่กำหนดชั้นความลับนั้น

2.8. “หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ”

หน้าที่ และความรับผิดชอบ

2.8.1. พิจารณารายละเอียดการฝ่าฝืนหรือการละเมิดข้อบังคับและนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของ สทอภ. ถ้าเป็นการฝ่าฝืนระเบียบขั้นรุนแรงหรือกรณีที่ฝ่าฝืนแล้วก่อให้เกิดความเสียหายแก่ สทอภ. หรือต่อบุคคลก็จะจัดทำบันทึกรายงานเกี่ยวกับการฝ่าฝืนนโยบายดังกล่าวไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

2.8.2. ในกรณีการละเมิดหรือฝ่าฝืนมีเจตนาไม่ชัดเจน ผู้ละเมิดหรือฝ่าฝืนจะถูกตักเตือนและชี้แจงให้เข้าใจถึงข้อปฏิบัติที่ถูกต้องหากมีการกระทำการฝ่าฝืนนั้นอีก ให้แต่งตั้งคณะกรรมการพิจารณา และต้องรายงานการกระทำดังกล่าว ไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) และผู้บังคับบัญชาที่เกี่ยวข้องทันที โดยให้มีการสอบสวน และดำเนินการทางวินัยตามความรุนแรงของผลกระทบจากการละเมิดหรือฝ่าฝืนข้อบังคับนั้น ๆ

2.8.3. ป้องกันและแก้ไขปัญหาที่เกิดขึ้นทันที เพื่อให้แน่ใจว่าการละเมิดหรือฝ่าฝืนเหล่านั้นจะไม่ลุกลามเป็นปัญหาใหญ่

2.8.4. จัดอบรมส่งเสริมให้ผู้ใช้งานตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศ

2.8.5. ให้คำแนะนำด้านเทคนิคที่เกี่ยวกับการรักษาความปลอดภัยของระบบสารสนเทศ

2.8.6. วางแผนควบคุมระบบความมั่นคงปลอดภัยด้านสารสนเทศและการเตือนภัยรวมถึงวิเคราะห์หาวิธีการแก้ไขจุดอ่อนของระบบสารสนเทศ

2.8.7. สืบสวนเหตุการณ์ต่าง ๆ ที่ไม่เป็นไปตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

2.8.8. ติดต่อและประสานงานเพื่อสร้างความร่วมมือทางด้านความมั่นคงปลอดภัยระหว่างองค์กร

2.8.9. รวบรวมรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น ๆ ได้แก่ สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ ศูนย์ประสานงานความมั่นคงปลอดภัยด้านสารสนเทศคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

สิทธิ

2.8.10. กำหนดกระบวนการในการอนุมัติการใช้งานระบบสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

2.8.11. การดำเนินการทางกฎหมายใด ๆ ต้องได้รับความช่วยเหลือจากหน่วยงานดูแลรับผิดชอบด้านกฎหมายและตัวแทนของ สทอภ. และในการดำเนินคดีใด ๆ ที่เกี่ยวข้องกับ สทอภ. ต้องเป็นหน้าที่ของเจ้าหน้าที่ระดับผู้บริหารที่ได้รับมอบหมายเท่านั้น

2.9. "หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ"

หน้าที่ และความรับผิดชอบ

2.9.1. พัฒนา ติดตั้ง ตรวจสอบ ปรับปรุง ซ่อมแซมและบำรุงรักษาอุปกรณ์ บริหารจัดการระบบเกี่ยวกับอุปกรณ์ IT Infrastructure ให้แก่หน่วยงานของ สทอภ. ทั้งหมด

2.9.2. บริหารจัดการระบบเครือข่ายเชื่อมโยงคอมพิวเตอร์ (Network Administration) ที่ใช้งานภายใน สทอภ. ทุกระบบ และควบคุมการเชื่อมต่อเครือข่ายอินเทอร์เน็ตโดยตรงผ่านช่องทางอื่น ได้แก่ Dial up Modem รวมทั้งควบคุมการเชื่อมต่อเครือข่ายจากภายนอก ได้แก่ การ Remote เครื่องคอมพิวเตอร์ การใช้งาน VPN เป็นต้น

2.9.3. รับผิดชอบในการจัดหาและควบคุมการใช้งาน Corporate Antivirus จัดเตรียมคู่มือและข้อมูลต่างๆ ที่เกี่ยวกับ Corporate Antivirus จัดทำสถิติ กราฟ และผลการใช้งาน รวมไปถึงการอนุญาตหรือจำกัดการใช้งานของผู้ใช้งาน

2.9.4. รับผิดชอบในการบำรุงรักษา ปิดช่องโหว่ในระบบ Corporate Antivirus ปรับปรุง Virus Signature ระบบ Corporate Antivirus ให้ทันสมัย เสนองบประมาณผ่านหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ปรับเพิ่มลดจำนวนลิขสิทธิ์ของ Corporate Antivirus อนุญาตหรือจำกัดการใช้งานของผู้ใช้งาน และดำเนินการในส่วนที่เกี่ยวข้อง

2.9.5. รับผิดชอบการจัดทำและปรับปรุงเนื้อหาของเว็บไซต์ของ สทอภ. (www.gistda.or.th)

2.9.6. ควบคุมการติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องคอมพิวเตอร์ของ สทอภ.

2.9.7. รับผิดชอบร่วมกับผู้ดูแลระบบในการตรวจสอบซอฟต์แวร์ เพื่อป้องกันการละเมิดข้อตกลงและหาทางป้องกันซอฟต์แวร์ที่ใช้ในการตรวจประเมินระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิดหรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้นๆ

2.9.8. จัดทำข้อมูลสินทรัพย์ระบบสารสนเทศของ สทอภ. รวมถึงค่า Configuration ของอุปกรณ์เครือข่าย เพื่อประสิทธิภาพในบริหารจัดการระบบสารสนเทศของ สทอภ.

2.9.9. ให้คำแนะนำและเป็นที่ปรึกษาในการพิจารณารายละเอียดการฝ่าฝืนหรือการละเมิดข้อบังคับและนโยบายความมั่นคงปลอดภัยระบบสารสนเทศของ สทอภ. และแก้ไขปัญหาที่เกิดขึ้นดังกล่าว

2.9.10. ควบคุมระบบความมั่นคงปลอดภัยด้านสารสนเทศและการเตือนภัย รวมถึงวิเคราะห์หาวิธีการแก้ไขจุดอ่อนของระบบสารสนเทศ

2.9.11. กำหนดและควบคุมการสำรองและกู้คืน (Backup & Recovery) ระบบสารสนเทศของ สทอภ.

2.9.12. ควบคุมการพิสูจน์ตัวตน (Authentication) ก่อนเข้าถึงระบบสารสนเทศของ สทอภ.

2.10. “หน่วยงานดูแลรับผิดชอบด้านตรวจสอบภายใน”

หน้าที่ และความรับผิดชอบ

2.10.1. ตรวจสอบการปฏิบัติงานของผู้ใช้งานให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ สทอภ. ที่ดำเนินไปภายใต้มาตรฐานและแนวทางการปฏิบัติที่ได้กำหนดไว้ในนโยบาย และร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เพื่อป้องกันสินทรัพย์และข้อมูลต่าง ๆ ของ สทอภ.

2.10.2. ให้ความช่วยเหลือแก่หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ในการชี้ถึงความเสี่ยงต่าง ๆ รวมถึงภัยคุกคามอันอาจก่อให้เกิดอันตรายต่อความมั่นคงปลอดภัยของ สทอภ.

2.11. “หน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง” มีหน้าที่และความรับผิดชอบในการวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ เพื่อปรับปรุงให้องค์กรมีคุณภาพ ประสิทธิภาพ และลดโอกาสความเสียหายที่อาจจะเกิดขึ้นได้

2.12. “หน่วยงานดูแลรับผิดชอบด้านกฎหมาย” มีหน้าที่และความรับผิดชอบในการให้ความเห็นหรือให้คำปรึกษาเกี่ยวกับระเบียบ ข้อกำหนด กฎเกณฑ์ ข้อบังคับ กฎหมาย พระราชบัญญัติ พระราชกฤษฎีกา การฟ้องร้องดำเนินคดี รวมถึงข้อละเมิดสินทรัพย์ทางปัญญา ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของ สทอภ.

2.13. “หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคล”

หน้าที่ และความรับผิดชอบ

2.13.1. ตรวจสอบคุณสมบัติของผู้สมัครเกี่ยวกับการละเมิดด้านความมั่นคงปลอดภัยระบบสารสนเทศ

2.13.2. การให้ “เจ้าหน้าที่” ลงนามมิให้เปิดเผยความลับของ สทอภ.

2.13.3. รายงานข้อมูลการว่าจ้างงาน การเปลี่ยนแปลงสภาพการว่าจ้างงาน การลาออกจากงาน การถึงแก่กรรม การโยกย้าย และการพักงานหรือการลงโทษทางวินัย ให้แก่ หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เพื่อบริหารจัดการทรัพยากรระบบสารสนเทศ และ สิทธิ์ในการเข้าถึงระบบงานต่าง ๆ

2.14. “หน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร” มีหน้าที่และความรับผิดชอบในการให้ความเห็นหรือให้คำปรึกษาเกี่ยวกับระเบียบ ข้อกำหนด กฎเกณฑ์ ข้อบังคับ กฎหมาย พระราชบัญญัติ พระราชกฤษฎีกา การฟ้องร้องดำเนินคดี รวมถึงข้อละเมิดสินทรัพย์ทางปัญญา ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศของ สทอภ.

2.15. “หน่วยงานดูแลรับผิดชอบด้านอาคารและสถานที่” มีหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม ควบคุมการเข้า-ออกอาคารและสำนักงานจัดเตรียมการป้องกันต่อภัยคุกคามต่าง ๆ ทั้งจากมนุษย์และธรรมชาติ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว ความไม่สงบของบ้านเมือง เป็นต้น

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก
(IT Security of Third-Party Policy)

1. วัตถุประสงค์

เพื่อควบคุมหน่วยงานภายนอกที่มีการใช้งานระบบสารสนเทศและทรัพยากรสารสนเทศอื่น ๆ ของ สทอภ. ให้เป็นไปอย่างมั่นคงปลอดภัย นโยบายนี้ใช้กำกับการดำเนินงานซึ่งไม่สามารถทำขึ้นภายใน สทอภ. ได้แก่ การพัฒนาระบบสารสนเทศ การใช้บริการของที่ปรึกษา การใช้บริการด้านระบบสารสนเทศจากภายนอก

2. การระบุสัญญาเพื่อควบคุมการเข้าใช้งานของหน่วยงานภายนอก

2.1. หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าถึงแหล่งข้อมูลของ สทอภ. จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้บังคับบัญชาเจ้าของข้อมูล ซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าว

2.2. ต้องทำการแจ้งเป็นลายลักษณ์อักษรให้หน่วยงานภายนอกทราบถึงความสำคัญที่มีต่อความมั่นคงปลอดภัยด้านสารสนเทศของข้อมูลสารสนเทศ ซึ่งหน่วยงานภายนอกจะต้องลงนามในเอกสารสัญญาเรื่องการไม่เปิดเผยข้อมูลของ สทอภ. โดยเอกสารดังกล่าวจะถูกจัดเก็บไว้เป็นหลักฐานในส่วนของผู้ร่วมสัญญาต้องทำการลงนามในสัญญาเรื่องการปกปิดเป็นความลับ และจัดเก็บเอกสารไว้ในแฟ้มสัญญา

2.3. เจ้าของโครงการหรือผู้จัดการโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดย หน่วยงานภายนอก ต้องกำหนดการเข้าใช้เฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

2.4. คู่สัญญาหรือหน่วยงานภายนอก มีหน้าที่ที่ต้องแจ้งให้กับผู้เป็นเจ้าของหรือผู้รับผิดชอบโครงการทราบทันทีที่พบว่ามีการคุกคามที่มีผลต่อความมั่นคงปลอดภัยในลักษณะใด ๆ ก็ตาม รวมถึงการเข้าถึงข้อมูลโดยผู้ไม่มีสิทธิ หรือการผ่อนปรน หรือละเว้นไม่ปฏิบัติตามวินัยความมั่นคงปลอดภัย ด้านสารสนเทศของ สทอภ. นอกจากนั้น “เจ้าหน้าที่ (Officer)” ของ สทอภ. ผู้ซึ่งรับทราบถึงเหตุการณ์คุกคามด้านความปลอดภัยซึ่งเกิดจากคู่สัญญาหรือบุคคลที่สาม ต้องแจ้งให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ทราบทันทีตามกระบวนการ ในนโยบายการรายงานเหตุการณ์ด้านความปลอดภัย

2.5. สัญญาการใช้งานระบบสารสนเทศทั้งหมดที่มีการจัดทำขึ้นต้องระบุถึง “สิทธิในการตรวจสอบ” เพื่อให้มั่นใจได้ว่า สทอภ. สามารถเข้าไปประเมินสภาพแวดล้อมของการควบคุมภายในทั้งทางกายภาพ (Physical) และทาง Logical ของคู่สัญญาหรือหน่วยงานภายนอกได้

3. การให้ความสนับสนุนจาก สทอภ.

หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าถึงแหล่งข้อมูลของ สทอภ. จะต้องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้บังคับบัญชาเจ้าของข้อมูลซึ่งเป็นผู้รับผิดชอบต่อการกระทำทั้งหมดของบุคคลดังกล่าว

4. มาตรฐานการเลือกหน่วยงานภายนอกโดยทั่วไป

4.1. ผู้บังคับบัญชาที่รับผิดชอบโครงการ ต้องขอข้อมูลเบื้องต้นของหน่วยงานภายนอกในรายที่ยังไม่ทราบรายละเอียด ซึ่งอาจจะรวมถึงข้อมูลด้านการเงินที่ใช้อ้างอิงได้

4.2. สทอภ. ต้องพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบที่เข้าไปปฏิบัติงานและข้อมูลที่ให้ไป

4.3. สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของ สทอภ. ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานในการประมวลผลข้อมูลนั้น

5. มาตรฐานการเลือกหน่วยงานภายนอกโดยทั่วไป

5.1. กรณีที่มีความจำเป็น สทอภ. จะให้สิทธิหน่วยงานภายนอกในการเข้าถึงข้อมูลเดียวกับผู้ใช้งานภายในโดยจะจำกัดเพียงการเข้าถึงข้อมูลเท่าที่จำเป็นเพื่อให้งานเสร็จสมบูรณ์
ข้อพิจารณา ให้อยู่ในดุลพินิจของผู้บังคับบัญชาเจ้าของข้อมูลนั้น ๆ หรือหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ

5.2. หน่วยงานภายนอก ที่ปรึกษา หรือคู่สัญญาที่ทำงานโดยตรงให้กับ สทอภ. ทุกคน ไม่ว่าจะทำงานอยู่ภายใน สทอภ. หรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของ สทอภ. โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเครือข่ายและข้อมูลต่างๆ ของ สทอภ.

6. มาตรฐานทั่วไปของหนังสือสัญญาว่าจ้าง ที่ต้องมีการใช้งานระบบสารสนเทศจากหน่วยงานภายนอก
ต้องประกอบไปด้วยข้อความดังต่อไปนี้

6.1. สัญญาในการยอมรับนโยบายและการควบคุมด้านความมั่นคงปลอดภัยของ สทอภ.

6.2. สิทธิสำหรับ สทอภ. ที่จะตรวจสอบสภาพแวดล้อมการทำงานรวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก

6.3. เอกสารต่างๆ เกี่ยวกับมาตรการการควบคุมที่ใช้ทั้งด้าน Physical และด้าน Logical เพื่อให้มั่นใจได้ว่าระบบงานของผู้ให้บริการจากภายนอกสามารถรักษาความมั่นคงปลอดภัยได้ทั้ง 3 ด้าน คือการรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

6.4. ข้อกำหนดทางด้านกฎหมาย ได้แก่ความลับส่วนบุคคล (Privacy) และการป้องกันข้อมูล

นโยบายสำหรับผู้ปฏิบัติงานชั่วคราว
(Temporary Worker Policy)

1. วัตถุประสงค์

เพื่อให้ทุกหน่วยงาน กำกับ ดูแล ผู้ปฏิบัติงานชั่วคราว (Temporary Worker) ที่ไม่ใช่ “เจ้าหน้าที่ (Officer)” ของ สทอภ. และอยู่ในความรับผิดชอบ ให้ใช้ระบบสารสนเทศอย่างเหมาะสม เกิดประโยชน์สูงสุด และปลอดภัย จึงกำหนดข้อปฏิบัติเพื่อความปลอดภัยของระบบสารสนเทศ ดังนี้

2. การขอรับสิทธิของผู้ใช้งาน

2.1. หน่วยงานที่มีความประสงค์ขออนุญาตให้ผู้ปฏิบัติงานชั่วคราวเข้าสู่ระบบสารสนเทศของ สทอภ. ให้ขออนุมัติจากผู้บังคับบัญชาระดับสำนักขึ้นไปที่มีอำนาจครอบคลุมระบบสารสนเทศที่ ผู้ปฏิบัติงานชั่วคราวต้องการจะเข้าถึงทั้งหมด ทั้งนี้ให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่ สทอภ. กำหนด

2.2. ผู้ดูแลระบบจะกำหนด Username และ Password ให้กับผู้ปฏิบัติงานชั่วคราวทุกท่านที่ได้รับอนุมัติจากผู้บริหารตามข้อ 2.1.

3. การดูแลระหว่างการปฏิบัติงานชั่วคราว

3.1. ผู้บังคับบัญชาตามข้อ 2.1. ต้องกำหนดให้มีหัวหน้าหน่วยงานที่เกี่ยวข้อง เป็นผู้ดูแลผู้ปฏิบัติงานชั่วคราวตลอดระยะเวลาการปฏิบัติงาน

3.2. หัวหน้าหน่วยงานที่ได้รับมอบหมายจากผู้บังคับบัญชาตามข้อ 3.1. ต้องชี้แจงให้ผู้ปฏิบัติงานชั่วคราวปฏิบัติตามข้อกำหนดว่าด้วยความมั่นคงปลอดภัยของระบบสารสนเทศและคำสั่งที่ เกี่ยวข้องอย่างเคร่งครัด

3.3. หัวหน้าหน่วยงานที่ได้รับมอบหมายจากผู้บังคับบัญชาตามข้อ 3.1. มีหน้าที่กำกับ ดูแลพฤติกรรมการใช้ระบบสารสนเทศของ สทอภ. ให้เป็นไปตามความต้องการของหน่วยงาน

3.4. หัวหน้าหน่วยงานสามารถยกเลิกสิทธิการใช้ระบบของผู้ปฏิบัติงานชั่วคราวที่มีพฤติกรรมการใช้ระบบสารสนเทศของ สทอภ. ในทางที่ไม่เหมาะสม

4. การดูแลระหว่างการปฏิบัติงานชั่วคราว

4.1. ผู้ปฏิบัติงานชั่วคราวที่ได้ทำการสร้างข้อมูลอิเล็กทรอนิกส์ที่ไม่ก่อให้เกิดประโยชน์กับ สทอภ. ไว้บนระบบสารสนเทศของ สทอภ. จะต้องทำการลบข้อมูลทิ้งทั้งหมดโดยผู้ดูแล ผู้ปฏิบัติงานชั่วคราวต้องกำกับดูแลการลบข้อมูลอิเล็กทรอนิกส์ดังกล่าว

4.2. ผู้ดูแลระบบต้องลบ Username และ Password ของผู้ปฏิบัติงานชั่วคราวทันที หลังจากสิ้นสุดการปฏิบัติงาน

4.3. ผู้ดูแลผู้ปฏิบัติงานชั่วคราวต้องแจ้งผู้บังคับบัญชาทันทีที่ผู้ปฏิบัติงานชั่วคราวหมดความจำเป็นหรือเลิกการปฏิบัติงานก่อนกำหนด หรือครบกำหนดการปฏิบัติงานชั่วคราว

5. การดูแลเรื่องข้อมูลด้านเทคโนโลยีสารสนเทศที่เป็นความลับ

5.1. ผู้ปฏิบัติงานชั่วคราวต้องไม่เปิดเผยข้อมูลในระบบสารสนเทศของ สทอภ. ต่อบุคคลอื่นที่ไม่เกี่ยวข้องกับการปฏิบัติงานนั้น ทั้งระหว่างการปฏิบัติงานและภายหลังการปฏิบัติงานเสร็จสิ้นไปแล้ว ยกเว้นกรณีที่จำเป็นตามคำสั่งศาลหรือตามกฎหมาย

5.2. สทอภ. สงวนสิทธิ์ที่จะเรียกร้องค่าเสียหาย หากพบว่าผู้ปฏิบัติงานชั่วคราวนำข้อมูลที่เป็นความลับในระบบสารสนเทศของ สทอภ. ไปใช้เพื่อประโยชน์ส่วนตนหรือเพื่อประโยชน์ของบุคคล/นิติบุคคลอื่น ๆ

6. สิทธิในการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว

การใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว หมายถึง การที่ผู้ปฏิบัติงานชั่วคราวเข้ามาปฏิบัติงานในระบบสารสนเทศของ สทอภ. โดยผ่าน Dial-up Modem, เครือข่าย Internet, เครือข่าย Wireless หรือเครือข่ายคอมพิวเตอร์อื่นๆ ที่อยู่นอกเหนือการควบคุมของ สทอภ.

สิทธิในการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราวเป็นสิทธิที่ สทอภ. จะอนุญาตให้เฉพาะกับตัวบุคคลในระหว่างที่บุคคลนั้นสังกัดอยู่กับบริษัท/องค์กรใดเท่านั้น โดยไม่สามารถถ่ายโอนกันได้ระหว่างบุคคล บริษัท หรือองค์กร หากบุคคลผู้เคยได้รับสิทธิดังกล่าวไม่ได้สังกัดอยู่กับบริษัท/องค์กรที่เคยได้รับสิทธิแล้วให้ถือว่าบุคคลดังกล่าวหมดสิทธิไป

6.1. สทอภ. อาจจะให้สิทธิใช้งาน Remote Access ในการปฏิบัติงานชั่วคราวคือ ผู้ปฏิบัติงานชั่วคราวที่เป็นที่ปรึกษา (Consultant) หรือผู้ปฏิบัติงานตามสัญญาจ้าง (Contractor) เท่านั้น ผู้ปฏิบัติงานชั่วคราวที่เป็นนิสิตนักศึกษาฝึกงานอาจจะไม่ได้รับสิทธิดังกล่าว

6.2. ผู้ปฏิบัติงานชั่วคราวจะต้องขออนุญาตผู้บังคับบัญชาหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศล่วงหน้าก่อนเข้ามาใช้งาน Remote Access สู่ระบบสารสนเทศของผู้ปฏิบัติงานชั่วคราวจะต้องระบุวัตถุประสงค์ วิธีการ Access และขอบข่ายของการ Access ที่แน่ชัด และ สทอภ. อาจจะอนุญาตให้เป็นรายครั้ง หรือเป็นช่วงระยะเวลาจำกัดแล้วแต่กรณีและความจำเป็น

6.3. สทอภ. สงวนลิขสิทธิ์ที่จะดำเนินคดีตามกฎหมายกับการโยกย้ายเปลี่ยนแปลงโปรแกรมหรือข้อมูลของ สทอภ. อื่นใดนอกเหนือไปจากที่ผู้ปฏิบัติงานชั่วคราวได้รับอนุญาต

6.4. สทอภ. สงวนสิทธิ์เรียกร้องค่าเสียหาย หากระบบคอมพิวเตอร์ของ สทอภ. ได้รับความเสียหาย ได้แก่ การติดไวรัสคอมพิวเตอร์ จากการใช้งาน Remote Access ในการปฏิบัติงานชั่วคราว

หมวด 3
การบริหารจัดการสินทรัพย์
(Asset Management)

จุดประสงค์ เพื่อป้องกันสินทรัพย์ของ สทอภ. จากความเสียหายที่อาจเกิดขึ้นได้ และกำหนดระดับของการป้องกันสารสนเทศอย่างเหมาะสม โดยมีการจัดทำบัญชีสินทรัพย์ ระบุผู้เป็นเจ้าของสินทรัพย์ และ กำหนดหลักเกณฑ์การใช้งานสินทรัพย์ที่เหมาะสม มีการจัดหมวดหมู่สินทรัพย์ตามระดับชั้นความลับ และจัดทำป้ายชื่อเพื่อการบริหารจัดการสินทรัพย์ตามที่ได้จัดหมวดหมู่ไว้ โดยมีนโยบายดังนี้

นโยบายการจัดหมวดหมู่และการควบคุมทรัพย์สิน
(Asset Classification and Control Policy)

1. วัตถุประสงค์

เพื่อเป็นการกำหนดมาตรฐานในการจัดหมวดหมู่และการควบคุมทรัพย์สินของ สทอภ. เพื่อป้องกันทรัพย์สินจากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกขโมย และสิ่งที่สร้างความเสียหายที่อาจเกิดขึ้นได้

2. การจัดหมวดหมู่และการควบคุมทรัพย์สิน

2.1. การจัดทำบัญชีทรัพย์สิน (Inventory of Assets)

ผู้บังคับบัญชาแต่ละหน่วยงานต้องทำบัญชีทรัพย์สินของหน่วยงานและแบ่งประเภทให้ชัดเจน ซึ่งรวมถึงบัญชีครุภัณฑ์คอมพิวเตอร์และบัญชีข้อมูลที่เก็บไว้ในสื่อต่าง ๆ ทั้งหมด เพื่อใช้ในการกำหนดมูลค่าทรัพย์สิน ระดับความสำคัญและวิธีการป้องกันที่เหมาะสม รวมทั้งต้องระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) ตามที่กำหนดไว้ในบัญชีทรัพย์สิน ซึ่งมีแนวทางปฏิบัติ ดังนี้

2.1.1. ทรัพย์สินของ สทอภ. ที่เป็นครุภัณฑ์อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย และซอฟต์แวร์ที่มีค่าลิขสิทธิ์ ต้องมีการขึ้นบัญชีไว้ในสมุดทะเบียน หรือระบบของ สทอภ. ตามหลักเกณฑ์หรือสัญญาที่ได้มีการกำหนดไว้สำหรับระบบดังกล่าว

2.1.2. ทรัพย์สินของ สทอภ. ที่เป็นซอฟต์แวร์ที่ใช้เพื่อการให้บริการของ สทอภ. ซึ่งไม่มีค่าลิขสิทธิ์ หากหน่วยงานใดมีการใช้งานให้หน่วยงานนั้นทำทะเบียนการใช้งานไว้ที่หน่วยงาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและทรัพย์สินที่เป็นซอฟต์แวร์ของ สทอภ. เพื่อประโยชน์ในการค้นหาติดตามและสำรวจช่องโหว่ที่อาจมีผลกระทบต่อความมั่นคงปลอดภัยในระบบสารสนเทศ

2.1.3. อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ซอฟต์แวร์ที่หน่วยงานจัดเช่าต้องกำหนดให้มีเจ้าหน้าที่ของหน่วยงานเป็นผู้รับผิดชอบ และจะต้องจัดทำบัญชีรายการของอุปกรณ์ ซอฟต์แวร์ หรือระบบงานคอมพิวเตอร์ที่เช่ามาใช้งาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและทรัพย์สินของ สทอภ.

2.1.4. สื่อบันทึกหรือบรรจุข้อมูล ทั้งกรณีที่เป็นทรัพย์สินของ สทอภ. หากหน่วยงานใดมีการใช้สื่อเพื่อบันทึกข้อมูลที่มีการกำหนดชั้นความลับ “ชั้นลับที่สุด” หรือ “ชั้นลับมาก” หรือ “ชั้นลับ” หน่วยงานนั้นจะต้องมีการทำบัญชีควบคุมการใช้งานเพื่อระบุผู้รับผิดชอบและป้องกันไม่ให้รั่วไหล

2.2. การตรวจสอบบัญชีสินทรัพย์ (Inventory Check)

ผู้บังคับบัญชาแต่ละหน่วยงาน ต้องจัดให้มีการตรวจสอบบัญชีทรัพย์สินตามระยะเวลาที่กำหนดไว้ ได้แก่ เดือนละครั้ง (สำหรับระบบสำคัญ) หรือปีละครั้ง (สำหรับระบบการใช้งานทั่วไป)

2.3. การจัดหมวดหมู่ข้อมูลและสารสนเทศ (Data and Information Classification)

2.3.1. ข้อมูลดิจิทัล (Digital Data) หรือสารสนเทศดิจิทัล (Digital Information) ให้หน่วยงานระบุชนิดลักษณะของข้อมูลให้ชัดเจนว่าเกี่ยวกับเรื่องใด (Topic) มีความสำคัญอย่างไร (Importance) และ ต้องมีการจัดลำดับชั้นความลับเป็นอย่างใดอย่างหนึ่งต่อไปนี้

- “ชั้นลับที่สุด”
- “ชั้นลับมาก”
- “ชั้นลับ”

โดยยึดถือจากคำนิยามในหมวดที่ 1 ทั้งนี้หากไม่ได้มีการกำหนดชั้นความลับที่ชัดเจนไว้ให้ถือว่าข้อมูลหรือสารสนเทศนั้นเป็น “ชั้นเปิดเผย” โดยปริยาย

2.3.2. เอกสารหรือสิ่งตีพิมพ์ที่พิมพ์หรือทำซ้ำขึ้นมาจากข้อมูลดิจิทัลหรือสารสนเทศดิจิทัล ซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับข้อมูลดิจิทัลหรือสารสนเทศดิจิทัลนั้น ยกเว้นว่ามีการจัดลำดับชั้นความลับใหม่โดยหน่วยงานผู้ผลิตเอกสารหรือสิ่งพิมพ์นั้น

2.3.3. ผู้บังคับบัญชาแต่ละหน่วยงานต้องทำการจัดหมวดหมู่ กำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันสารสนเทศของ สทอภ. ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดย สทอภ. จัดให้มีกระบวนการในการจัดหมวดหมู่ของข้อมูลและทรัพย์สิน ได้แก่ ชั้นลับที่สุด ชั้นลับมากและชั้นลับ การกำหนดแนวทางการแบ่งชั้นความลับของข้อมูล ต้องอยู่ในการควบคุมดูแลและรักษาความปลอดภัยที่เหมาะสมไม่ว่าจะอยู่ในรูปแบบใดก็ตาม

2.3.4. ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การเก็บรักษา จนถึงการทำลายและกำหนดเป็นระเบียบปฏิบัติ ให้ “เจ้าหน้าที่” ของ สทอภ. ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

2.4. การจัดทำป้ายชื่อ ข้อมูล และ สารสนเทศ (Data and Information Labeling and Handling)

2.4.1. ผู้บังคับบัญชาแต่ละหน่วยงาน ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับข้อมูลและสารสนเทศ โดยแยกตามหมวดหมู่ที่กำหนดไว้ มีการส่งมอบและจัดเก็บตามขั้นตอนกระบวนการต่าง ๆ ซึ่งประกอบไปด้วย การถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสาร และการทำลาย มีแนวทางปฏิบัติดังนี้

2.4.1.1. ข้อมูลที่อยู่ “ชั้นลับที่สุด” ทั้งฉบับจริงและสำเนาต้องมีการระบุถึงระดับความปลอดภัยของข้อมูลในเอกสารตรงบริเวณส่วนหัวและ/หรือส่วนท้ายของเอกสารทุกหน้า

2.4.1.2. การนำส่งเอกสารข้อมูล “ชั้นลับที่สุด” ต้องใส่ซองเอกสารลับเฉพาะ ที่ไม่สามารถเห็นถึงเนื้อหาของเอกสารที่บรรจุภายในและปิดผนึกลงชื่อของผู้รับอย่างชัดเจน

2.4.1.3. ข้อมูลที่อยู่ “ชั้นลับที่สุด” ต้องมีการจัดเก็บในลิ้นชักหรือตู้ที่มีการล็อคหรือ ห้องที่มีการออกแบบพิเศษสำหรับการเก็บรักษาเอกสารเหล่านี้โดยเฉพาะและจำกัดเฉพาะผู้ที่มีสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลดังกล่าวได้

2.4.1.4. การทำสำเนาเอกสารข้อมูลที่อยู่ “ชั้นลับที่สุด” ต้องได้รับการอนุมัติจากผู้บริหารระดับสูงเท่านั้น

2.4.1.5. ข้อมูลที่อยู่ “ชั้นลับที่สุด” ต้องมีการควบคุมดูแลอย่างใกล้ชิดในขณะที่ใช้งานเครื่องพิมพ์และเครื่องถ่ายเอกสาร เพื่อพิมพ์หรือทำสำเนาของข้อมูล

2.4.1.6. ข้อมูลที่อยู่ “ชั้นลับที่สุด” ผู้ที่ควบคุมการใช้งานเท่านั้นที่ได้รับอนุญาตให้ตรวจสอบข้อมูลที่พิมพ์หรือสำเนา

2.4.1.7. ข้อมูลที่ถูกจัดอยู่ใน “ชั้นลับมาก” ต้องใช้ระบบการนำส่งแบบใส่ 2 ซองซ้อนกัน โดยซองด้านในระบุถึงชื่อและประเภทของข้อมูลอย่างชัดเจน ส่วนซองด้านนอกจะระบุถึงชื่อและที่อยู่ของผู้รับเท่านั้น

2.4.1.8. ข้อมูล “ชั้นลับมาก” ต้องส่งให้ถึงมือผู้รับที่ระบุเท่านั้นและต้องมีลายเซ็นของผู้รับระบุว่าได้รับเอกสารแล้ว

2.4.1.9. การทำสำเนาเอกสารข้อมูลที่อยู่ “ชั้นลับมาก” ต้องได้รับการอนุมัติจากผู้บริหารระดับกลางเท่านั้น

2.4.1.10. ข้อมูลที่อยู่ “ชั้นลับมาก” ต้องถูกจัดพิมพ์จากเครื่องพิมพ์ที่เชื่อมโยงกับระบบเครือข่ายที่สามารถควบคุมการใช้ได้เพื่อป้องกันการอ่าน เปลี่ยนแปลง หรือลบข้อมูลได้จากผู้ที่ไม่ได้รับอนุญาต

2.4.1.11. เอกสารข้อมูล “ชั้นลับที่สุด” “ชั้นลับมาก” และ “ชั้นลับ” ที่ไม่ได้นำมาใช้แล้วต้องถูก รวบรวม ขีดฆ่า และทำเครื่องหมาย “ทำลายได้” และนำเอกสารไปทำลายเพื่อไม่ให้สามารถอ่านหรือนำมาใช้ได้อีก โดยการฉีกหรือเผาทำลาย

หมวด 4
ความมั่นคงปลอดภัยทางด้านทรัพยากรบุคคล
(Human Resource Security)

จุดประสงค์ เพื่อให้ “เจ้าหน้าที่ (Officer)” เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบของตนทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และการสิ้นสุดหรือการเปลี่ยนการจ้างงาน ซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์ รวมทั้งลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่ โดยมีนโยบายดังนี้

นโยบายความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล
(Human Resource Security Policy)

1. วัตถุประสงค์

เพื่อเป็นมาตรฐานในการควบคุมความปลอดภัยส่วนบุคคล โดยกำหนดเป็นมาตรฐานเกี่ยวกับผู้บริหาร “เจ้าหน้าที่ (Officer)”ของ สทอภ. เริ่มตั้งแต่กระบวนการสรรหา “เจ้าหน้าที่ (Officer)” ใหม่ เพื่อให้มั่นใจว่ามีการพิจารณาคุณสมบัติอย่างเพียงพอก่อนที่จะมีการว่าจ้างตลอดจนเมื่อเริ่มปฏิบัติงานต้องมีการกำหนดสิทธิในการเข้าสู่อาคารสถานที่และระบบงานที่สำคัญ เพื่อปฏิบัติงานตามหน้าที่และสิทธินั้น และจะต้องมีการยกเลิก เมื่อสิ้นสุดการว่าจ้างหรือมีการโยกย้ายการปฏิบัติงานของ “เจ้าหน้าที่” ดังกล่าว

2. มาตรฐานการสร้างความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากร

2.1. การกำหนดหน้าที่ความรับผิดชอบพื้นฐานด้านความมั่นคงปลอดภัย (Including Basic Security in Job Responsibilities)

ผู้บังคับบัญชาแต่ละหน่วยงานต้องกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในคุณสมบัติของบุคลากร IT ตามที่กำหนดเอาไว้ในนโยบาย หมวด 6 การบริหารจัดการด้านการ สื่อสารและการดำเนินงาน (Communications and Operations Management)

2.2. การตรวจสอบคุณสมบัติของผู้สมัคร (Personnel Screening)

2.2.1. หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคล ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็น “เจ้าหน้าที่ (Officer)” โดยจะต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบสารสนเทศของหน่วยงานใดมาก่อน

2.2.2. หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคล จะต้องจัดเตรียมข้อมูลที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ สทอภ. เพื่อให้ “เจ้าหน้าที่ (Officer)” ที่เข้ามาใหม่ได้ศึกษาและรับทราบ

2.2.3. “เจ้าหน้าที่ (Officer)” ใหม่ทุกคนจะต้องลงนามรับทราบและยอมรับสัญญาในนโยบายความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ความรับผิดชอบตามนโยบายเหล่านั้น

2.3. การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

2.3.1. หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคล ต้องกำหนดเงื่อนไขการจ้างงานที่รวมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของ สทอภ.

2.3.2. หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคล ต้องแจ้งรายละเอียดของ “เจ้าหน้าที่ (Officer)” ที่ บรรจุใหม่ สิ้นสุดการว่าจ้าง หรือมีการโยกย้ายการปฏิบัติงาน ให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ทราบทันที เพื่อให้การบริหารจัดการบัญชีผู้ใช้งาน (User ID) เป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด

2.3.3. ผู้บังคับบัญชาของทุกหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ ต้องกำหนดเปลี่ยนแปลง หรือ ยกเลิกสิทธิของผู้ใช้งานที่เกี่ยวกับ Login หรือ User ID เพื่อให้สอดคล้องกับการเปลี่ยนแปลง สถานะของการว่าจ้างนั้นทันที โดยต้องเก็บข้อมูลให้สามารถตรวจสอบประวัติการเปลี่ยนแปลง สิทธิในระบบสารสนเทศที่เกิดขึ้นเหล่านั้นได้

2.3.4. เมื่อสิ้นสุดการเป็นเจ้าหน้าที่หรือเปลี่ยนลักษณะการปฏิบัติงาน ผู้ใช้งานจะต้องคืนสินทรัพย์อันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นของ สทอภ. ได้แก่ อุปกรณ์ระบบสารสนเทศ ข้อมูล และสำเนาของข้อมูล บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ให้แก่ สทอภ. ในทันทีที่พ้นหน้าที่

2.4. การลงนามมิให้เปิดเผยความลับของ สทอภ. (Confidentiality Agreements)

หน่วยงานดูแลรับผิดชอบด้านบริหารงานบุคคล ต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่ (Officer)” และ สทอภ. ว่าจะไม่เปิดเผยความลับของ สทอภ. โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้าง “เจ้าหน้าที่ (Officer)” นั้น ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

3. การอบรมเจ้าหน้าที่

หน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร ร่วมกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ดำเนินการอบรม “เจ้าหน้าที่ (Officer)” ได้รับทราบและตระหนักถึงภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้สามารถป้องกันภัยที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศได้อย่างมีประสิทธิภาพ

3.1. การให้ความรู้และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information Security Education and Training)

3.1.1. หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ร่วมกับหน่วยงานดูแลรับผิดชอบด้านพัฒนาบุคลากรและวัฒนธรรมองค์กร ต้องจัดการประชุมสัมมนา หรืออบรมให้ความรู้แก่ “เจ้าหน้าที่ (Officer)” เกี่ยวกับวิธีปฏิบัติงานเพื่อสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศและเครือข่ายของ สทอภ. โดยหลักสูตรการอบรมขึ้นอยู่กับหน้าที่ความรับผิดชอบของ “เจ้าหน้าที่ (Officer)”

3.1.2. หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ มีหน้าที่ในการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบสารสนเทศของ สทอภ. ด้วย

3.1.3. “เจ้าหน้าที่ (Officer)” ใหม่ของ สทอภ. ต้องได้รับการอบรมเกี่ยวกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้องกับ สทอภ. โดยต้องเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของ “เจ้าหน้าที่ (Officer)” ด้วย

3.2. กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary Process)

สทอภ. จัดให้มี “มาตรการดำเนินการกับผู้ฝ่าฝืนละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ สทอภ.” โดยมีข้อปฏิบัติ ดังนี้

3.2.1. การฝ่าฝืนระเบียบโดยเล็กน้อยจากความไม่ตั้งใจหรือบังเอิญ โดยก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ส่วนบุคคล ผู้ดูแลระบบจะแจ้งเตือนโดยวาจา หรือจดหมายอิเล็กทรอนิกส์ หรือเป็นลายลักษณ์อักษร แต่หากเป็นการกระทำผิดซ้ำซ้อน สทอภ. จะพิจารณาลงโทษตามข้อ 3.2.6.

3.2.2. การฝ่าฝืนระเบียบขั้นรุนแรง โดยก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลบนระบบสารสนเทศเป็นวงกว้าง ที่เกิดจากการละเมิดกฎโดยเจตนาซึ่งสร้างความเสียหายให้แก่ระบบ ยกเว้นการกระทำดังกล่าวได้รับสิทธิ์และได้รับอนุญาต ได้แก่ กรณีการสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) การทดลอง Crack Password การทดลองถอดรหัส การตรวจสอบ Network Traffic โดยไม่ได้รับอนุญาตหรือมีเหตุอันสมควร เป็นต้น สทอภ. จะพิจารณาลงโทษตามข้อ 3.2.6.

3.2.3. การเข้าถึงระบบโดยมิชอบหรือโดยไม่มีอำนาจ (Unauthorized access) แบ่งเป็นการเข้าถึงทั้งในระดับกายภาพ การเข้าถึงระบบสารสนเทศหรือข้อมูล และการเข้าถึงโดยผ่านเครือข่ายสาธารณะได้แก่ การลักลอบดักฟังหรือดักเก็บข้อมูลที่มีชั้นความลับ ทั้งในส่วนของการติดตั้งซอฟท์แวร์และ ฮาร์ดแวร์ที่สามารถดักจับข้อมูล การสแกนหาช่องโหว่ในระบบ (Vulnerability Scan) การทดสอบการเจาะระบบ (Penetration Test) การทดลอง Crack Password การทดลองถอดรหัส การตรวจสอบ Network Traffic โดยไม่ได้รับอนุญาตหรือมีเหตุอันสมควร เป็นต้น สทอภ. จะพิจารณาลงโทษตามข้อ 3.2.6.

3.2.4. การสร้างโฮมเพจส่วนตัว หรือการส่งต่อข้อมูลที่แสดงออกในลักษณะที่ขัดต่อกฎหมาย กฎระเบียบ และศีลธรรม สทอภ. จะพิจารณาลงโทษตามข้อ 3.2.6.

3.2.5. การก่อความวุ่นวายที่ขัดต่อกฎระเบียบของ สทอภ. หรือสร้างความเดือดร้อน รบกวนการทำงานของผู้ใช้งานอื่น ๆ ในระบบเครือข่าย สทอภ. จะพิจารณาลงโทษตามข้อ 3.2.6.

3.2.6. กรณีที่ฝ่าฝืนหรือละเมิดข้อกำหนดในระเบียบนี้ และก่อให้เกิดความเสียหายแก่ สทอภ. หรือบุคคลหนึ่งบุคคลใด สทอภ. จะพิจารณาดำเนินการทางวินัยและกฎหมายแก่ผู้ใช้งานหรือหน่วยงานภายนอกนั้นตามความเหมาะสม ดังต่อไปนี้

- ผู้ดูแลระบบจะพิจารณาระงับการใช้งาน และจะแจ้งชื่อผู้ใช้งานที่ทำผิดระเบียบไปยังหน่วยงานต้นสังกัดให้รับทราบ หรือแจ้งผู้บริหาร สทอภ. รับทราบและพิจารณาตั้งกรรมการสอบสวนข้อเท็จจริง เพื่อพิจารณาจากความรุนแรงหรือความเสียหายที่เกิดขึ้นเป็นรายกรณีไป และ สทอภ. อาจพิจารณาดำเนินการทางวินัยหรือทางกฎหมายแก่ผู้นั้นตามความเหมาะสม
- ลงโทษทางวินัยต่อผู้ละเมิดตามความเหมาะสม เพื่อมิให้เกิดการละเมิดซ้ำ และในกรณีที่ ผู้ละเมิดเป็นหน่วยงานภายนอก ให้ดำเนินการตามกฎหมายต่อไป
- หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อ สทอภ. อย่างร้ายแรง หรือเข้าข่ายความผิดตามกฎหมาย ให้ส่งตัวไปดำเนินการตามกฎหมายต่อไป
- หากการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อระบบสารสนเทศและต้องเสียค่าใช้จ่ายในการกู้คืน สทอภ. สามารถเรียกร้องค่าเสียหายในส่วนนี้ เพื่อเป็นค่าใช้จ่ายในการกู้คืน

ข้อยกเว้น : กิจกรรมที่เกี่ยวกับการทดสอบระบบสารสนเทศ เพื่อตรวจสอบหรือส่งเสริมความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่าย หากปฏิบัติโดยหน่วยงานหรือบุคคลที่ได้รับอนุญาตหรือโดยหน่วยงาน หรือบุคคลได้รับมอบหมายจาก สทอภ. แล้ว จะไม่ถือว่าเป็นการฝ่าฝืนระเบียบนี้

หมวด 5
ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security)

จุดประสงค์ เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาตของสินทรัพย์สารสนเทศของ สทอภ. ไม่ให้เกิดการสูญหาย ถูกขโมย เกิดความเสียหาย เกิดการก่อกวนหรือแทรกแซงป้องกันการถูกเปิดเผยโดยไม่ได้รับอนุญาตของสินทรัพย์ของ สทอภ. และป้องกันไม่ให้กิจกรรมการดำเนินงานต่าง ๆ ของ สทอภ. เกิดการติดขัดหรือหยุดชะงัก โดยมีนโยบายดังนี้

นโยบายความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security Policy)

1. วัตถุประสงค์

เพื่อเป็นมาตรฐานในความมั่นคงปลอดภัยด้านสารสนเทศทางกายภาพที่เกี่ยวกับสถานที่ ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นสินทรัพย์ของ สทอภ. โดยนโยบายนี้มีผลบังคับใช้กับผู้ใช้งานและหน่วยงาน สทอภ. ซึ่งมีส่วนเกี่ยวข้องกับการใช้ระบบสารสนเทศของ สทอภ.

2. มาตรฐานการสร้างความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากร

2.1. ทุกหน่วยงานตั้งแต่ระดับสำนักขึ้นไป จะต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวัง ควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ และประกาศให้รับทราบทั่วกัน (ต้องระบุให้ชัดเจนว่ามีพื้นที่ใช้งานระบบสารสนเทศกี่ประเภทและประเภทใดบ้าง)

2.2. ทุกหน่วยงานต้องกำหนดการติดตั้งอุปกรณ์ในพื้นที่ใช้งานระบบสารสนเทศให้สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

3. การควบคุมการเข้าออก (Physical Entry Controls)

สำนัก/ฝ่ายต่าง ๆ ต้องดูแลสถานที่พื้นที่ใช้งานระบบสารสนเทศที่อยู่ในความรับผิดชอบ โดยต้องกำหนดมาตรการในการควบคุมการเข้าออกของเจ้าหน้าที่ (Officer) โดยจะได้รับสิทธิ์ในการเข้าออกสถานที่ทำงานได้เฉพาะบริเวณที่กำหนดเท่านั้น ส่วนบุคคลภายนอก การขอเข้าพื้นที่นั้นจะต้องได้รับอนุญาตจากเจ้าของพื้นที่เป็นกรณีไป ซึ่งมีแนวทางปฏิบัติเบื้องต้น ดังนี้

3.1. เจ้าหน้าที่ (Officer) จะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนดเท่านั้น

3.2. หากมีบุคคลภายนอก ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตหรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้จะต้องแสดงบัตรประจำตัวที่ สทอภ. ออกให้ หรือบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่)

4. ความมั่นคงปลอดภัยด้านสารสนเทศสำหรับสำนักงาน ห้องทำงาน และเครื่องมือต่างๆ (Securing Offices, Rooms and Facilities)

4.1. ผู้บังคับบัญชาแต่ละหน่วยงาน ต้องจัดให้มีมาตรการความมั่นคงปลอดภัยด้านสารสนเทศให้กับสำนักงาน ห้องทำงานและเครื่องมือต่าง ๆ ได้แก่ เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก ประตูหน้าต่างของสำนักงานต้องล็อคเมื่อไม่มีคนอยู่ เป็นต้น โดยมีแนวทางปฏิบัติ ได้แก่ กั้นพื้นที่อย่างรอบด้าน (ได้แก่ ติดตั้งผนัง ติดตั้งเหล็กดัด ล็อคประตูที่ใช้ดอกกุญแจ หรือมีระบบ Access Control) และปรับปรุงให้มีความเหมาะสมทางสภาวะแวดล้อม (ได้แก่ ติดตั้งระบบปรับอากาศ การควบคุมความชื้น เป็นต้น)

4.2. การปฏิบัติงานในพื้นที่ควบคุม (Working in Control Areas)

4.2.1. ผู้บังคับบัญชาแต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณ พื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวิดีโอในบริเวณนั้น เป็นต้น

4.2.2. ต้องมีป้ายประกาศข้อความ **“ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวิดีโอ”** และ **“ห้ามสูบบุหรี่”** บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

4.3. การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access, Delivery, and Loading Areas)

หน่วยงานต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยหน่วยงานภายนอก เพื่อป้องกันการเข้าถึงสินทรัพย์ของ สทอภ. โดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ต้องจัดเป็นบริเวณแยกออกมาต่างหาก

4.4. ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

4.4.1. ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

4.4.2. ผู้บังคับบัญชาที่เป็นเจ้าของระบบงาน ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ ได้แก่ จัดให้มีการซ่อมบำรุงปีละ 1 ครั้ง หรือระบบที่สำคัญมากอาจจะกำหนดให้มีการบำรุงรักษาทุกสิ้นเดือน เป็นต้น

4.4.3. ผู้บังคับบัญชาแต่ละหน่วยงาน ต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของ สทอภ. ได้แก่ Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน โดยต้องปฏิบัติตามระเบียบในการใช้งานการยืม-คืน

4.4.4. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

- กำหนดเลขไอพีแอดเดรสที่เจาะจง (Fix IP address) ให้อุปกรณ์ที่ขึ้นทะเบียนไว้และ บันทึกเป็นบัญชีเก็บไว้
- ใช้ซอฟต์แวร์บริหารจัดการอุปกรณ์เครือข่าย (Monitoring) โดยระบุอุปกรณ์จากเลขไอพีแอดเดรสเพื่อดูพฤติกรรมการใช้งานรวมถึงควบคุมการเข้าถึงบริการ

4.4.5. ผู้บังคับบัญชาแต่ละหน่วยงาน ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ (Secure Disposal of Reuse of Equipment) ซึ่งมีข้อมูลสำคัญเก็บไว้ ได้แก่ ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น ทั้งนี้ เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว ซึ่งมีแนวทางปฏิบัติ ดังนี้

ระดับความปลอดภัย	สื่อที่อ่านเขียนด้วยแสง (Optical Media)	สื่ออิเล็กทรอนิคส์ (Electronic Media)
1 (ลับ)	ทำลายสื่อโดย อุปกรณ์ทำลายสื่อเฉพาะ	ลบล้างข้อมูล และสามารถทิ้งได้
2 (ลับมาก)	ทำลายสื่อโดย อุปกรณ์ทำลายสื่อเฉพาะ	ลบล้างข้อมูล หรือทำลายสื่อ โดยอุปกรณ์ทำลายสื่อเฉพาะ
3 (ลับที่สุด)	ทำลายสื่อ โดยอุปกรณ์ทำลายสื่อเฉพาะ	ลบล้างข้อมูล และทำลายสื่อ โดยอุปกรณ์ทำลายสื่อเฉพาะ
4 (ข้อมูลส่วนบุคคล)	ดำเนินการตาม พรบ. คุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 และ 37	ดำเนินการตาม พรบ. คุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 และ 37

4.5. ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security) หน่วยงานต้องกำหนดให้มีระบบป้องกันภัย โดยมีแนวทางปฏิบัติ ดังนี้

4.5.1. ต้องมีระบบเตือนภัย/ป้องกันภัย ได้แก่ ระบบดับเพลิง หรือระบบเตือนอัคคีภัย

4.5.2. ต้องมีการวางแผน และซักซ้อมการปฏิบัติรับมือกับภัย

4.5.3. ห้ามกระทำการใดๆ ให้เกิดมีประกายไฟหรือเปลวไฟ

4.5.4. ระบบที่สำคัญของ สทอภ. จะต้องมีการปฏิบัติตามนโยบายแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ เพื่อป้องกันผลกระทบที่จะเกิดขึ้นกับการปฏิบัติงานของ สทอภ.

4.6. การจัดการระบบไฟฟ้า (Power System) และระบบสายสัญญาณ (Data Cable) ผู้บังคับบัญชาแต่ละหน่วยงานต้องทราบถึงการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในพื้นที่ใช้งานระบบสารสนเทศที่อยู่ในความรับผิดชอบและจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่หรือบุคคลที่มีสิทธิเท่านั้น

4.7. การควบคุมทั่วไป (General Controls)

4.7.1. “เจ้าหน้าที่ (Officer)” ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศที่เป็น “ชั้นลับที่สุด” หรือ “ชั้นลับมาก” หรือ “ชั้นลับ” ไว้ในที่สามารถพบเห็นได้ง่าย (Clear Desk) โดยจัดเก็บไว้ในที่ที่ปลอดภัย นอกจากนี้ ตู้จ่ายเอกสารหรือจดหมายและเครื่องโทรสารจะต้องได้รับการดูแลให้ปลอดภัยด้วย

4.7.2. การเคลื่อนย้ายสินทรัพย์ของ สทอภ. ผู้ดูแลระบบแต่ละหน่วยงาน ต้องทำเป็นบันทึกและขออนุญาตจากผู้บังคับบัญชาอย่างถูกต้องในการเคลื่อนย้าย ซึ่งมีแนวทางปฏิบัติ ดังนี้

4.7.2.1. ผู้ที่รับผิดชอบในการย้ายสถานที่ทำงาน ต้องตรวจสอบความเรียบร้อยครั้งสุดท้ายทันทีหลังจากที่ทำการย้ายของเสร็จสิ้น รวมทั้งตรวจสอบพื้นที่และสินทรัพย์ด้วย การย้ายสถานที่ทำงานเป็นช่วงเวลาที่ต้องระวังเรื่องการรักษาความปลอดภัยที่อาจมีการมองข้ามได้ โดยเฉพาะช่วงเวลาที่ต้องเร่งจัดการย้ายให้เสร็จสิ้น จึงต้องให้ความระมัดระวัง เพราะอาจมีการผ่อนปรนมาตรการรักษาความปลอดภัยต่อข้อมูลที่มีความสำคัญหรือต่อระบบเครือข่ายของ สทอภ. ได้

4.7.2.2. ข้อมูลที่มีความสำคัญมาก รวมถึงข้อมูลในคอมพิวเตอร์แบบพกพา (Notebook) ต้องมีการเคลื่อนย้ายโดยผู้เป็นเจ้าของข้อมูลเท่านั้น ห้ามเคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล

4.7.2.3. ผู้ใช้งานจะต้องแน่ใจว่าข้อมูลสำคัญใด ๆ ต้องมีการป้องกันการเข้าถึงข้อมูลจากผู้ที่ไม่ใช่เจ้าของข้อมูล ได้แก่ การเข้ารหัสไฟล์ เป็นต้น

4.7.2.4. ผู้ที่มีส่วนร่วมในการเคลื่อนย้ายสถานที่ทำงาน จะต้องมีการตรวจตราสถานที่ย้ายสินทรัพย์ออก เพื่อให้มั่นใจได้ว่าไม่มีข้อมูลใดหลงเหลืออยู่ มีการกำหนดความรับผิดชอบในการดูแลให้ครอบคลุมส่วนที่เก็บเอกสาร (ได้แก่ ตู้เก็บแฟ้มเอกสาร, ห้องเก็บรักษาแฟ้มข้อมูล, ห้องนิรภัย เป็นต้น)

4.7.2.5. ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลงหรือเคลื่อนย้าย เพื่อใช้เป็นข้อมูลในการควบคุมสินทรัพย์ของ สทอภ.

หมวด 6
การบริหารจัดการด้านการสื่อสารและการดำเนินงาน
(Communications and Operations Management)

จุดประสงค์ เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย ให้เป็นไปตามข้อตกลง ลดความเสี่ยงจากการล้มเหลวของระบบป้องกันซอฟท์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟท์แวร์ที่ไม่ประสงค์ดี ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายสินทรัพย์สารสนเทศโดยไม่ได้รับอนุญาต รักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกัน สร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ และตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่เหมาะสม และไม่ได้รับอนุญาต โดยประกอบด้วย

- นโยบายความมั่นคงปลอดภัยด้านเครือข่ายคอมพิวเตอร์
- นโยบายการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์
- นโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์
- นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
- นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา
- นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล
- นโยบายการแลกเปลี่ยนสารสนเทศ
- นโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์

นโยบายความมั่นคงปลอดภัยด้านเครือข่ายคอมพิวเตอร์
(Computer Network Security Policy)

1. วัตถุประสงค์

นโยบายนี้กำหนดขึ้นเพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างถูกต้องและปลอดภัย จึงจำเป็นต้องมีการบริหารจัดการเครือข่ายของ สทอภ. ให้มีความมั่นคงปลอดภัยด้านความถูกต้อง การเก็บรักษาเป็นความลับ และความพร้อมในการใช้งาน นโยบายดังกล่าวนี้มีผลบังคับใช้กับ “เจ้าหน้าที่” ของ สทอภ. และ หน่วยงานภายนอกที่ขออนุญาตใช้งานระบบสารสนเทศของ สทอภ.

2. มาตรฐานทั่วไป

2.1. การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน (Operational Procedures and Responsibilities)

2.1.1. ผู้บังคับบัญชาที่เป็นเจ้าของระบบงาน ต้องจัดทำคู่มือและขั้นตอนการปฏิบัติงานของระบบงานนั้น ๆ โดยมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่าย

2.1.2. ในกรณีที่มีการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ หน่วยงานที่ดูแลระบบสารสนเทศนั้นต้องทำการบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ

2.1.3. ผู้บังคับบัญชาที่เป็นเจ้าของระบบงาน ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบสารสนเทศและเครือข่ายที่หน่วยงานนั้น ๆ รับผิดชอบ

2.1.4. ผู้บังคับบัญชาที่เป็นเจ้าของระบบงาน ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้ละเมิด

2.1.5. ผู้บังคับบัญชาที่เป็นเจ้าของระบบงาน ต้องแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบสารสนเทศออกจากเครื่องที่ทำงานจริงหรือเครื่องให้บริการ

2.1.6. ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอก สทอภ. หน่วยงานที่รับผิดชอบต้อง ปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิของผู้ใช้งานที่ได้รับ และตรวจสอบการใช้งานอย่างสม่ำเสมอ

2.2. การบริหารจัดการการเปลี่ยนแปลงในการให้บริการต่อหน่วยงานภายนอก (Managing Changes to Third Party Services)

ผู้บังคับบัญชาที่เป็นเจ้าของระบบงานต้องปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก ได้แก่ การปรับปรุงหรือพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก โดยต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ก่อนจึงจะสามารถดำเนินการได้ รวมทั้งปรับปรุงเอกสารที่เกี่ยวข้องให้ทันสมัยเมื่อมีการเปลี่ยนแปลงสารสนเทศ

2.3. การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance)

2.3.1. หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ต้องมีการวางแผนกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต โดยสำรวจความต้องการทรัพยากรสารสนเทศให้ครบถ้วน เพื่อไม่ให้โครงการเกิดความล่าช้าในการจัดซื้อจัดหา และต้องคำนึงถึงความมั่นคงปลอดภัยของสารสนเทศด้วย ซึ่งจะทำให้ระบบมีความมั่นคงปลอดภัยและไม่เกิดค่าใช้จ่ายในภายหลัง

2.3.2. ผู้บังคับบัญชาที่เป็นเจ้าของระบบงานต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน ได้แก่ การตรวจรับระบบตาม TOR ที่ได้กำหนดไว้ เป็นต้น

2.4. การป้องกันซอฟต์แวร์และสารสนเทศของ สทอภ. ให้ปลอดภัยจากการถูกทำลายจากซอฟต์แวร์ที่ไม่ประสงค์ดี (Protection Against Malicious Software)

หน่วยงานต่าง ๆ ต้องจัดให้มีการติดตั้งและใช้งานซอฟต์แวร์ป้องกันไวรัส เพื่อป้องกันความเสียหายและการรั่วไหลของข้อมูล โดยมีแนวทางปฏิบัติดังนี้

2.4.1. ห้ามนำเครื่องคอมพิวเตอร์ ซอฟต์แวร์หรือข้อมูลที่มีความเสี่ยงต่อการติดมัลแวร์มาติดตั้งใช้งาน

2.4.2. ต้องสำรองข้อมูลสำคัญเก็บไว้ในที่ที่ปลอดภัย ได้แก่ สื่อจัดเก็บข้อมูลแบบพกพา หรือเนื้อที่บนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ สทอภ. จัดสรรไว้ให้ เพื่อลดปัญหาการกู้คืนสภาพข้อมูลที่ถูกทำลายโดยไวรัส

2.4.3. ห้ามผู้ใช้งานปรับแต่ง หรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันไวรัสที่ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ตามที่ สทอภ. จัดหาให้

2.4.4. ผู้ใช้งานต้องมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบการ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบหากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

2.4.5. ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อสงสัยว่ามีการติดไวรัส

2.5. การสำรองข้อมูล

2.5.1. ผู้ดูแลระบบสารสนเทศที่สำคัญนั้น ๆ ต้องสำรองข้อมูลที่สำคัญเก็บไว้ตามระยะเวลาที่เหมาะสม

2.5.2. ผู้ดูแลระบบต้องบันทึกรายละเอียดการสำรองข้อมูลโดยมีรายละเอียด เวลาเริ่มต้นและสิ้นสุด ชื่อผู้ทำการสำรองข้อมูล และชนิดของข้อมูลที่บันทึก

2.5.3. กรณีที่เกิดการผิดพลาดในการสำรองข้อมูล สำรองข้อมูลต้องบันทึก รายละเอียดของข้อผิดพลาดที่เกิดขึ้นพร้อมแนวทางแก้ไข

2.5.4. ผู้ดูแลระบบต้องมีการสำรองข้อมูลภายนอกสำนักงาน ตามความเหมาะสมเมื่อระบบงานถูกโจมตีหรือเกิดความเสียหายเพื่อให้สามารถกู้ข้อมูลกลับคืนได้

2.5.5. ผู้ดูแลระบบต้องเข้ารหัสข้อมูลที่สำรองตามชั้นความลับ โดยใช้เทคโนโลยีที่เหมาะสมเพื่อป้องกันข้อมูลสำรองถูกเปิดเผย

2.6. การบริหารจัดการเครือข่าย (Network Management)

2.6.1. ผู้ดูแลระบบต้องบริหารจัดการความมั่นคงปลอดภัยในเครือข่าย ซึ่งมีแนวทางปฏิบัติดังนี้

2.6.1.1. **ระบบเครือข่ายภายใน** อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่าย เพื่อการทำงานภายใน สทอภ. ได้แก่ Router หรือ Switch มีข้อปฏิบัติดังนี้

- อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมโยงเครือข่าย ต้องปิด Service Port ที่ไม่จำเป็น และในการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่าเริ่มต้น ได้แก่ Default Community, Default Username และ Default Password
- การเชื่อมโยงเครือข่ายเพื่อใช้งานระบบต่าง ๆ จะสามารถกระทำได้ก็ต่อเมื่อได้รับอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ การเชื่อมโยงเครือข่ายเองโดยพลการ หากทำให้เกิดความเสียหายกับระบบเครือข่ายจะต้องถูกลงโทษตามที่กำหนดไว้
- ผู้ดูแลระบบจะต้องมีแผนดำเนินการบำรุงรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์ เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ
- ผู้ดูแลระบบมีหน้าที่ในการติดตั้งอุปกรณ์ซอฟต์แวร์ระบบการเข้ารหัสข้อมูลอัตโนมัติ หรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ
- ผู้ดูแลระบบมีหน้าที่ในการติดตั้งอุปกรณ์ซอฟต์แวร์ระบบการเข้ารหัสข้อมูลอัตโนมัติ หรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ
- ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

2.6.1.2. **ระบบ Remote Access** อุปกรณ์ Remote Access Server (RAS) ที่ติดตั้งใช้งานใน Remote Area หรือเพื่อการทำงานกับหน่วยงานภายนอก ได้แก่ Remote Access Server (RAS), Remote VPN, Remote Router มีข้อปฏิบัติดังนี้

- อุปกรณ์ RAS จะต้องทำ Hardening และบันทึกการทำ Configuration Set Up ของอุปกรณ์ RAS ทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง
- เมื่อเสร็จสิ้นการทดสอบการใช้งานอุปกรณ์ RAS แล้วให้ลบ User/Password ที่ใช้ในงานทดสอบทันที
- อุปกรณ์ RAS ที่สามารถ Management ทาง Remote Terminal ได้ จะต้องไม่ใช้ค่าเริ่มต้น ได้แก่ Default Community, Default Username และ Default Password

2.6.1.3. **อุปกรณ์ Server** อุปกรณ์ Server ที่ติดตั้งเพื่อการทำงานภายใน สทอภ. มีข้อปฏิบัติดังนี้

- ผู้ดูแลระบบต้องเปลี่ยนค่าบัญชีผู้ใช้งานและรหัสผ่านที่ถูกกำหนดมาตั้งแต่เริ่มต้น (Default Username/Default Password)
- ต้องทำ Hardening และบันทึกการทำ Configuration Set up ของอุปกรณ์ Server และจัดทำเป็นเอกสารทุกครั้งที่ติดตั้งหรือเปลี่ยนแปลง
- ต้องเปิด Port ที่จำเป็นเท่านั้น ส่วน Port ที่ไม่ใช้งานต้องปิดทั้งหมด
- ต้องบันทึกการติดตั้ง Service Patch ทุกครั้ง
- ต้องไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ
- เมื่อ Log on เพื่อใช้งาน Server ผ่าน Console แล้วเมื่อเลิกใช้งานจะต้อง Logoff User นั้นโดยทันที
- ผู้ดูแลระบบจะต้องสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยเดือนละครั้ง และทดสอบการสำรองข้อมูลอย่างน้อยปีละ 2 ครั้ง โดยต้องสอดคล้องกับความสำคัญของระบบ

2.6.1.4. **อุปกรณ์ PC Terminal** มีข้อปฏิบัติดังนี้

- ต้องเปิด Port ที่จำเป็นเท่านั้น ส่วน Port ที่ไม่ใช้งานต้องปิดทั้งหมด
- ต้องติดตั้ง Protocol เฉพาะที่ทำงานร่วมกับ Server เท่านั้น
- ต้องบันทึกการติดตั้ง Service Patch ทุกครั้ง
- เมื่อ Log on เพื่อใช้งาน Server ผ่าน Terminal Console แล้วเมื่อเลิกใช้งานจะต้อง Logoff User นั้นโดยทันที

2.6.2. **การป้องกันการใช้งานเครือข่าย**

2.6.2.1. ห้ามนำอุปกรณ์เครือข่ายมาติดตั้งกับระบบเครือข่ายของ สทอภ. โดยไม่รับอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ

2.6.2.2. ห้ามผู้ใช้งานเครือข่ายกระทำการใด ๆ ที่รบกวนระบบเครือข่าย ได้แก่ การเปิดใช้งาน Service DHCP เพื่อเชื่อมต่อเข้ากับระบบเครือข่ายของ สทอภ. เอง

2.6.2.3. ตรวจสอบการเชื่อมต่อเครือข่ายและจำกัดสิทธิ์ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

2.6.2.4. ตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่ายด้วยอุปกรณ์ไฟล์วอล และระบบตรวจจับการบุกรุก (IPS/IDS)

2.6.2.5. ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต โดยมีการควบคุมการเข้าถึงพอร์ตที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และเปิดใช้บริการ (Service) ที่จำเป็นเท่านั้น เช่น SSH SFTP และ ping เป็นต้น

2.6.2.6. มีการดูแลตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

2.6.2.7. มีการควบคุมการเข้าถึงระบบสารสนเทศด้วยการพิสูจน์ตัวตน (Authentication) โดยเครื่องคอมพิวเตอร์ของผู้ใช้งานจะต้องมีการกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศและมีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร ก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก สทอภ. สามารถเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศของ สทอภ. ได้

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของ สทอภ. โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สายของ สทอภ.

2. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย มีแนวทางปฏิบัติ ดังนี้

2.1. **“ผู้ใช้”** ต้องไม่นำอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless Access Point) มาติดตั้งใช้งานเองโดยไม่ได้รับความเห็นชอบ

2.2. **“ผู้ใช้”** ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ สทอภ. จะต้องทำการลงทะเบียนกับ “ผู้ดูแลระบบ” ของ ฝทส.

2.3. **“ผู้ใช้”** จะต้องปฏิบัติตามคำแนะนำการใช้งานของ ฝทส. เพื่อการรักษาความมั่นคงปลอดภัยโดยเคร่งครัด

2.4. **“ผู้ดูแลระบบ”** ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้ในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบ ตามความจำเป็นในการใช้งาน

2.5. **“ผู้ดูแลระบบ”** ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับ/ส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

2.6. **“ผู้ดูแลระบบ”** ต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและต้องสำรวจว่าสัญญาณรั่วไหลออกไปภายนอก

2.7. **“ผู้ดูแลระบบ”** ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณไร้สายมาใช้งาน

2.8. **“ผู้ดูแลระบบ”** ต้องเปลี่ยนค่า Login ID และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ Login ID และรหัสผ่านที่มีความปลอดภัยเพื่อป้องกันผู้โจมตี ไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

2.9. **“ผู้ดูแลระบบ”** ต้องมีการติดตั้งอุปกรณ์ป้องกันการเข้าถึงเครือข่าย (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายใน

2.10. **“ผู้ดูแลระบบ”** ต้องกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สาย ติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

2.11. **“ผู้ดูแลระบบ”** ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอเพื่อตรวจสอบ และบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

นโยบายการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์
(Internet and E-mail Policy)

1. วัตถุประสงค์

นโยบายนี้ ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานรับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์(E-mail) ให้มีการป้องกันการเข้าถึงหรือการเปลี่ยนแปลงแก้ไขข้อความใน E-mail โดยไม่ได้รับอนุญาต และการรักษาข้อมูลและทรัพยากรต่างๆ ของ สทอภ. ให้มีความมั่นคงปลอดภัย

2. การใช้งานอินเทอร์เน็ต

2.1. **"ผู้ดูแลระบบ"** ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ สทอภ. จัดสรรไว้เท่านั้น ได้แก่ Proxy, Firewall, IPS-IDS เป็นต้น **"ผู้ใช้"** ต้องไม่ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ได้แก่ ADSL **ยกเว้น**มีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการ สทอภ. เป็นลายลักษณ์อักษร

2.2. เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์พกพา และอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ก่อนทำการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการและโปรแกรม Web Browser

2.3. ในการรับ/ส่งข้อมูลคอมพิวเตอร์ผ่านทางระบบเครือข่ายอินเทอร์เน็ตจะต้องมีการตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับ/ส่งข้อมูลทุกครั้ง

2.4. **"ผู้ใช้"** ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ สทอภ. เพื่อหาประโยชน์ส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ผิดกฎหมาย เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือ เว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

2.5. **"ผู้ใช้"** จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ สทอภ.

2.6. **"ผู้ใช้"** ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ผิดกฎหมาย ข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ สทอภ.

2.7. **"ผู้ใช้"** ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ สทอภ. ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบเครือข่ายอินเทอร์เน็ต

2.8. **"ผู้ใช้"** ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านระบบเครือข่ายอินเทอร์เน็ต

2.9. **"ผู้ใช้"** ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพบุคคลอื่น ที่เกิดจากการสร้างขึ้น ตัดต่อ แต่ง เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้บุคคลอื่นนั้นเสีย ชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

2.10. **"ผู้ใช้"** มีหน้าที่ที่จะตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนระบบเครือข่ายอินเทอร์เน็ตก่อนนำข้อมูลไปใช้

2.11. **"ผู้ใช้"** ต้องระมัดระวังการดาวน์โหลดโปรแกรม ซึ่งรวมถึง Patch หรือ Fixes ต่างๆ และรูปภาพหรือเนื้อหา (Content) ที่มาจากระบบเครือข่ายอินเทอร์เน็ต โดยต้องไม่ละเมิดกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

2.12. **“ผู้ใช้”** ต้องไม่บอกสถานที่หรือข้อมูลส่วนตัว ได้แก่ ชื่อ ที่อยู่ เบอร์โทรศัพท์ ประกาศผ่านระบบเครือข่ายอินเทอร์เน็ต

2.13. การใช้งานเว็บบอร์ด (Web board) ของ สทอภ. “ผู้ใช้” ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ สทอภ.

2.14. ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ สทอภ. การทำลายความสัมพันธ์กับเจ้าหน้าที่และหน่วยงานอื่นๆ

2.15. หลังจากใช้งานระบบเครือข่ายอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

2.16. ไม่ใช้งานโปรแกรมประเภทติดต่อสื่อสารข้อความ ได้แก่ Facebook, Twitter ในเรื่องส่วนตัว ระหว่างเวลาทำงานหรือเวลา 8.30 - 12.00 น. และ 13.00 - 16.30 น.

2.17. ไม่ติดตั้งและใช้งานโปรแกรมประเภทตรวจสอบ หรือ รบกวนการทำงานของระบบเครือข่ายคอมพิวเตอร์ ได้แก่ โปรแกรม Bit torrent หรือ โปรแกรมตรวจสอบหรือตรวจจับข้อมูลในระบบเครือข่ายก่อนได้รับอนุญาตจากผู้มีอำนาจ และ ฝทส. เป็นลายลักษณ์อักษร

2.18. ไม่ควรเข้าใช้งาน Website ที่มีการส่งข้อมูลแบบ Streaming ที่ใช้ Bandwidth สูง ได้แก่ Online Radio, Online TV, Online Video เป็นต้น หรือดาวน์โหลด/อัปโหลด ไฟล์ที่มีขนาดใหญ่ ในระหว่างเวลาทำงานหรือเวลา 8.30 - 12.00 น. และ 13.00 - 16.30 น. เนื่องจากจะทำให้การรับ-ส่งข้อมูลในระบบเครือข่ายล่าช้าและกระทบต่อการปฏิบัติงานของเจ้าหน้าที่คนอื่น ๆ ทั้งนี้หากหน่วยงานมีความจำเป็นต้องใช้เข้าถึง Website ที่ มีการส่งข้อมูลแบบ Streaming ที่ใช้ Bandwidth สูงในช่วงเวลาทำงาน ให้แจ้ง ฝทส. เพื่อ พิจารณาดำเนินการต่อไป

3. การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

3.1. ผู้ใช้งานต้องระมัดระวังการใช้งานระบบจดหมายอิเล็กทรอนิกส์ ของ สทอภ. เพื่อไม่ให้เกิดความเสียหายต่อ สทอภ. จะต้องไม่กระทำผิดกฎหมาย ละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้ระบบจดหมายอิเล็กทรอนิกส์ ของ สทอภ. โดยมีหลักกฎหมายที่เกี่ยวข้อง อย่างน้อยดังนี้

3.1.1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

3.1.2. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

3.1.3. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562

3.1.4. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น

3.2. **“ผู้ดูแลระบบ”** ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ สทอภ. ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ ได้แก่ ในกรณีที่ผู้ใช้งานลาออก ผู้ดูแลระบบจะต้องพิจารณาเพื่อแก้ไขสิทธิ์ในการใช้งานจดหมายอิเล็กทรอนิกส์ของผู้ใช้งานที่ลาออกทันที

3.3. **“ผู้ดูแลระบบ”** ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของ สทอภ.

3.4. **“ผู้ใช้”** ที่ต้องการใช้งานจดหมายอิเล็กทรอนิกส์ต้องติดต่อ ฝทส. เพื่อกรอกรายละเอียดในแบบฟอร์มขอใช้บริการระบบ IT และส่งระบบสารบรรณอิเล็กทรอนิกส์ มายัง ฝทส./สจก.

3.5. สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะมีการบังคับเปลี่ยนรหัสผ่านโดยทันที

3.6. การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติ ดังนี้ รหัสผ่านจะต้องมีทั้งตัวอักษร ตัวเลข และสัญลักษณ์พิเศษ ประสมกัน และกำหนดความยาวของรหัสผ่านอย่างน้อย 8 ตัวอักษรเพื่อความปลอดภัย

3.7. **“ผู้ใช้”** ต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

3.8. **“ผู้ใช้”** ต้องมีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอและเคร่งครัด ได้แก่ เปลี่ยนรหัสผ่านทุก 6 เดือน

3.9. **“ผู้ใช้”** ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อ สทอภ. หรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาผลประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของ สทอภ.

3.10. **“ผู้ใช้”** ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่อ อ่าน รับ/ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

3.11. **“ผู้ใช้”** ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ สทอภ. เพื่อการทำงานของ สทอภ. เท่านั้น

3.12. **“ผู้ใช้”** ต้องไม่ประกาศ รหัสผ่าน (Password) E-mail Account ของตนเองผ่านเครือข่ายอินเทอร์เน็ต

3.13. **“ผู้ใช้”** ต้องทำการออกจากระบบจดหมายอิเล็กทรอนิกส์ (Log out) ทุกครั้ง เพื่อป้องกันบุคคลอื่นลักลอบเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์ของ สทอภ.

3.14. **“ผู้ใช้”** ต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File ได้แก่ .exe, .com เป็นต้น

3.15. **“ผู้ใช้”** ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

3.16. **“ผู้ใช้”** ต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับ/ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของ สทอภ. ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

3.17. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อของจดหมายอิเล็กทรอนิกส์

3.18. **“ผู้ใช้”** ต้องตรวจสอบกล่องเก็บจดหมายอิเล็กทรอนิกส์ (Mail Box) และจดหมายขยะ (Junk Mail) ของตนเอง เพื่อจัดเก็บจดหมายอิเล็กทรอนิกส์ในกล่องเก็บจดหมายอิเล็กทรอนิกส์เท่าที่จำเป็น และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการหรือไม่เกี่ยวข้องกับงานของ สทอภ. ออกจากกล่องเก็บจดหมายอิเล็กทรอนิกส์ เพื่อลดปริมาณการใช้พื้นที่ในการจัดเก็บของผู้ใช้งาน

นโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์
(Corporate Antivirus for PC and Notebook Computer Policy)

1. วัตถุประสงค์

นโยบายนี้ได้ถูกจัดทำขึ้นเพื่อต้องการให้เกิดความมั่นคงปลอดภัยของระบบสารสนเทศ สทอภ. ช่วยลดภาวะเสี่ยงของปัญหาที่จะเกิดขึ้นกับระบบสารสนเทศทั้งในส่วนของอุปกรณ์และระบบฐานข้อมูลของ สทอภ. ทำให้การทำงานมีความต่อเนื่องไม่เกิดการหยุดชะงัก

2. แนวทางปฏิบัติการใช้งานระบบป้องกันไวรัส (Corporate Antivirus)

เพื่อลดความเสี่ยงและปัญหาการติดไวรัสในเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์แม่ข่ายของ สทอภ. รวมทั้งให้มีหลักการปฏิบัติที่สอดคล้องกัน ต้องปฏิบัติดังต่อไปนี้

2.1. ให้ระบบ Corporate Antivirus ซึ่งหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ เป็นผู้จัดหาเป็นระบบ Antivirus หลักสำหรับเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) ที่เป็นทรัพย์สินของ สทอภ. โดยมีหลักพิจารณาให้ความสำคัญ (High Priority) กับกลุ่มต่อไปนี้เป็นอย่างน้อย

- 2.1.1. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา (Notebook) ที่ต้องติดต่อใช้งานกับระบบงานสำคัญ และหรือระบบสารสนเทศที่มีข้อมูลความลับของ สทอภ. ได้แก่ ERP, HR, Ebudget เป็นต้น
- 2.1.2. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา (Notebook) ที่ใช้ทำงานกับข้อมูลสำคัญ หรือข้อมูลอันเป็นความลับของ สทอภ. ได้แก่ การจัดทำข้อกำหนด การทำร่างสัญญาทางกฎหมาย การทำงานด้านบัญชี/การเงิน เป็นต้น
- 2.1.3. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา (Notebook) ที่ใช้ควบคุมระบบงานสำคัญ (System Management) ของ สทอภ.
- 2.1.4. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา (Notebook) ของผู้บริหารระดับต้นขึ้นไป
- 2.1.5. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา (Notebook) ที่ใช้พัฒนาซอฟท์แวร์ หรือ ใช้ทำงาน System Administration หรือ Network Administration
- 2.1.6. เครื่องคอมพิวเตอร์ (PC) หรือเครื่องคอมพิวเตอร์พกพา (Notebook) ของผู้ใช้งานที่ต้องทำหน้าที่ติดต่อกับหน่วยงานภายนอก หรือที่ต้องเชื่อมต่อกับทั้ง Intranet และ Internet เพื่อประโยชน์ทางราชการหรือภาพลักษณ์ของ สทอภ.

2.2. กำหนดให้หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศร่วมกับหน่วยงานที่เกี่ยวข้องเป็นผู้ประสานงานและดำเนินการที่เกี่ยวข้อง ได้แก่

- 2.2.1. แจ้งให้หน่วยงานภายใน สทอภ. รับทราบโดยหนังสือเวียน หรือสื่ออื่นตามความเหมาะสม
- 2.2.2. หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศเป็นผู้รับผิดชอบดูแลบำรุงรักษากำกับความทันสมัย Patch ปิดช่องโหว่ในระบบ Corporate Antivirus เสนองบประมาณปรับเพิ่มลด จำนวน Licenses อนุญาตหรือจำกัดการใช้งานของผู้ใช้งาน และดำเนินการในส่วนที่เกี่ยวข้อง

2.2.3. หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศดำเนินการให้การ Update Virus Signature เป็นไปอย่างอัตโนมัติ และจัดทำ Configuration ของระบบ Antivirus ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

2.2.4. หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ จะต้องปฏิบัติตามนโยบายเกี่ยวกับการ ใช้งานระบบ Antivirus ที่ใช้งานภายใน Intranet ดังนี้

2.2.4.1. หากเป็น Antivirus ที่ไม่มีลิขสิทธิ์ถูกต้อง สทอภ. จะไม่อนุญาตให้ใช้งาน ทั้งนี้หน่วยงานต้องหันมาใช้ระบบ Corporate Antivirus ของหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศเป็นหลัก

2.3. กรณี Antivirus ที่ใช้กับระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย หรือสำหรับอุปกรณ์อื่นที่ไม่ใช่เครื่องคอมพิวเตอร์ (PC) และเครื่องคอมพิวเตอร์พกพา (Notebook) หน่วยงานใดมีความจำเป็นต้องใช้งาน ให้ส่งเรื่องให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ พิจารณาเป็นรายกรณีไป

2.4. ในกรณีตรวจพบว่าผู้ใช้งาน หรือ หน่วยงานไม่ปฏิบัติตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ สามารถเข้าตรวจสอบสาเหตุได้ และ จะดำเนินการแจ้งผลการตรวจสอบให้แก่ผู้บังคับบัญชา และผู้บริหารระดับสูงด้านสารสนเทศทราบต่อไป

นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
(Personal Computer)

1. วัตถุประสงค์

กำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้น เพื่อช่วยให้ผู้ใช้ (User) ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้ต้องทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของ สทอภ. ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

2. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล มีแนวทางปฏิบัติ ดังนี้

2.1. เครื่องคอมพิวเตอร์ที่ สทอภ. อนุญาตให้ **“ผู้ใช้”** ใช้งาน เป็นสินทรัพย์ของ สทอภ. ดังนั้นผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ เพื่องานของ สทอภ.

2.2. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของ สทอภ. ต้องเป็นโปรแกรมที่ สทอภ. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.3. ไม่อนุญาตให้ **“ผู้ใช้”** ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ส่วนบุคคลของ สทอภ.

2.4. **“ผู้ใช้”** ต้องไม่ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ ที่มีการทำงานกระทบต่อระบบส่วนกลาง

2.5. การตั้งชื่อเครื่องคอมพิวเตอร์ส่วนบุคคลจะต้องตั้งชื่อและกำหนดโดย ฝทส. เท่านั้น

2.6. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อม จะต้องดำเนินการโดย ฝทส. หรือ หน่วยงานที่เกี่ยวข้องเท่านั้น

2.7. ก่อนใช้งานสื่อบันทึกพกพาต่างๆ ได้แก่ แผ่น CD Flash Drive หรือ External Hard Disk เป็นต้น ต้องมีการตรวจสอบเพื่อตรวจหาไวรัสโดยโปรแกรมป้องกันไวรัส

2.8. ต้องไม่เก็บข้อมูลสำคัญของ สทอภ. ไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

2.9. **“ผู้ใช้”** มีหน้าที่และรับผิดชอบต่อการดูแลและรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยต้องปฏิบัติดังนี้

2.9.1. ต้องไม่รับประทานอาหารหรือนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณพื้นที่ติดตั้งเครื่องคอมพิวเตอร์

2.9.2. ต้องไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอคอมพิวเตอร์ หรือ Disk Drive

3. การควบคุมการเข้าถึงระบบปฏิบัติการ มีแนวทางปฏิบัติ ดังนี้

3.1. **“ผู้ใช้”** ต้องกำหนดชื่อผู้ใช้งาน (Login) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

3.2. **“ผู้ใช้”** ต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 15 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

3.3. **“ผู้ใช้”** ต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน และรหัสผ่านเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3.4. ในระหว่างเวลาพักกลางวัน และหลังเลิกงาน **“ผู้ใช้”** ต้อง Log out ออกจากเครื่องคอมพิวเตอร์ หรือ ล็อคหน้าจอด้วยโปรแกรม Screen Saver

4. **การใช้รหัสผ่าน (Password)** มีแนวทางปฏิบัติ ดังนี้
   4.1. **"ผู้ใช้"** ต้องกำหนดรหัสผ่าน ให้มีความยาว 8 ตัวอักษรและมีส่วนประกอบของอักษร อักขระพิเศษและหรือตัวเลขประสมกัน โดยไม่ใช้ข้อความที่ง่ายแก่การคาดเดา
   4.2. **"ผู้ใช้"** ต้องเก็บรหัสผ่านเป็นความลับ และต้องไม่เปิดเผยรหัสผ่านให้ผู้อื่นทราบ
   4.3. **"ผู้ใช้"** ต้องเก็บรหัสผ่านไว้ในสถานที่ที่ปลอดภัยที่ผู้อื่นไม่สามารถค้นพบได้
   4.4. **"ผู้ใช้"** ไม่พิมพ์รหัสผ่าน ในขณะที่มีผู้อื่นเห็นการพิมพ์ดังกล่าว
   4.5. **"ผู้ใช้"** ต้องเปลี่ยนรหัสผ่านของตนเองทุก ๆ 6 เดือน
5. **การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์** มีแนวทางปฏิบัติ ดังนี้
   5.1. **"ผู้ใช้"** ต้องทำการปรับปรุง (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
   5.2. **"ผู้ใช้"** ต้องตรวจสอบไวรัสจากสื่อต่าง ๆ ได้แก่ แผ่น CD Flash Drive หรือ External HardDisk เป็นต้น ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์
   5.3. **"ผู้ใช้"** ต้องตรวจสอบก่อนใช้งานไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากระบบเครือข่ายอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส
   5.4. **"ผู้ใช้"** ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดๆที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
6. **การสำรองข้อมูลและการกู้คืนข้อมูล** มีแนวทางปฏิบัติ ดังนี้
   6.1. "ผู้ใช้" ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ส่วนบุคคลไว้บนสื่อบันทึกอื่นๆ ได้แก่ แผ่น CD Flash Drive หรือ External HardDisk เป็นต้น
   6.2. "ผู้ใช้" มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
   6.3. "ผู้ใช้" ที่ต้องการเคลื่อนย้ายสื่อสำรองข้อมูลออกนอกสถานที่จะต้องมีการป้องกันการเข้าถึงข้อมูลอย่างมั่นคงปลอดภัย
   6.4. แผ่นสื่อสำรองข้อมูล ได้แก่ แผ่น CD ที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก
7. **การนำออกครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง** มีแนวทางปฏิบัติ ดังนี้
   7.1. "ผู้ใช้" ที่จะนำครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง จะต้องกรอกรายละเอียดตามแบบฟอร์มการนำสินทรัพย์ออกนอกอาคารสถานที่ ให้ถูกต้องและครบถ้วนเท่านั้น จึงจะอนุญาตให้นำออกครุภัณฑ์คอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงได้
   7.2. "ผู้ใช้" ต้องเก็บสำเนาแบบฟอร์มการนำสินทรัพย์ออกนอกอาคารสถานที่ไว้เพื่อเป็นหลักฐาน
8. **การบำรุงรักษาครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง** มีแนวทางปฏิบัติ ดังนี้
   8.1. ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงจะต้องขึ้นทะเบียนครุภัณฑ์เพื่อความสะดวกในการตรวจสอบและการบำรุงรักษา
   8.2. ฝทส. จะให้บริการเฉพาะครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่ขึ้นทะเบียนครุภัณฑ์แล้วหรืออยู่ระหว่างการส่งมอบแล้วเท่านั้น
   8.3. หากครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงเกิดการชำรุดเสียหาย ไม่สามารถใช้งานได้ทั้งด้านซอฟต์แวร์หรือฮาร์ดแวร์ "ผู้ใช้" มีหน้าที่จะต้องแจ้งให้ ฝทส. รับทราบเพื่อดำเนินการแก้ไขต่อไป

8.4. หากครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอยู่ในสัญญาหรือระยะเวลาการรับประกันเกิดการชำรุดเสียหาย ฝทส. หรือหน่วยงานเจ้าของครุภัณฑ์คอมพิวเตอร์ มีหน้าที่ติดต่อคู่สัญญาหรือผู้แทนจำหน่ายเพื่อดำเนินการตรวจซ่อมตามที่ระบุในสัญญา

8.5. หากครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงอยู่นอกเหนือหรือพ้นระยะเวลาการรับประกัน ฝทส. มีหน้าที่ซ่อมแซมในเบื้องต้นหรือประสานกับหน่วยงานเจ้าของครุภัณฑ์คอมพิวเตอร์ในการดำเนินการซ่อมแซมต่อไป

นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา
(Notebook Computer)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพา และการนำไปปฏิบัติงานภายนอก สทอภ. เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ของ สทอภ. ให้เกิดความปลอดภัย ผู้ใช้จึงต้องรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งานการบำรุงรักษา และสิ่งที่ต้องหลีกเลี่ยง ในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล มีแนวทางปฏิบัติ ดังนี้

2.1. เครื่องคอมพิวเตอร์ที่ สทอภ. อนุญาตให้ **“ผู้ใช้”** ใช้งานเป็นสินทรัพย์ของ สทอภ. ดังนั้นผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของ สทอภ.

2.2. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของ สทอภ. ต้องเป็นโปรแกรมที่ สทอภ. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพา หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.3. การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) แบบพกพาจะต้องกำหนดและตั้งชื่อโดย ฝทส.

2.4. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดย ฝทส. หรือ หน่วยงานที่เกี่ยวข้อง

2.5. “ผู้ใช้” ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

2.6. ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

2.7. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันจากการกระทบกระเทือน ได้แก่ การตกจากโต๊ะทำงาน หรือ หลุดมือ

2.8. ไม่ใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยน

2.9. การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องเพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

2.10. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง ได้แก่ ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD เครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

2.11. ไม่วางของทับบนหน้าจอและแป้นพิมพ์

2.12. การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

2.13. ไม่วางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ ได้แก่ แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

2.14. การเช็ดทำความสะอาดหน้าจอภาพ ต้องเช็ดอย่างเบามือที่สุดและต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วน

3. ความปลอดภัยทางด้านกายภาพ มีแนวทางปฏิบัติ ดังนี้

3.1. “ผู้ใช้” มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ได้แก่ ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในสถานที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

3.2. “ผู้ใช้” ต้องไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระแทก

3.3. “ผู้ใช้” ต้องไม่ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Components) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่

4. การควบคุมการเข้าถึงระบบปฏิบัติการ และการใช้รหัสผ่าน (Password) มีแนวทางปฏิบัติ ดังนี้

4.1. “ผู้ใช้” ต้องกำหนดชื่อผู้ใช้งาน (Login) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

4.2. “ผู้ใช้” ต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 15 นาที ให้ทำการปิดล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

4.3. “ผู้ใช้” ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ มีแนวทางปฏิบัติ ดังนี้

5.1. “ผู้ใช้” ต้องทำการปรับปรุง (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

5.2. “ผู้ใช้” ต้องไม่ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

5.3. หาก “ผู้ใช้” พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) “ผู้ใช้” ต้องไม่เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งไม่พึงประสงค์ (Malware) ไปยังเครื่องคอมพิวเตอร์อื่น ๆ ได้

6. การสำรองข้อมูลและการกู้คืนข้อมูล มีแนวทางปฏิบัติ ดังนี้

6.1. “ผู้ใช้” ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา

6.2. “ผู้ใช้” ต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการเกิดการรั่วไหลข้อมูล

6.3. “ผู้ใช้” ที่ต้องการเคลื่อนย้ายสื่อสำรองข้อมูลออกนอกสถานที่จะต้องมีการป้องกันการเข้าถึงข้อมูลอย่างมั่นคงปลอดภัย

6.4. สื่อสำรองข้อมูลต่าง ๆ เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนข้อมูลสม่ำเสมอ

6.5. แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

7. การบำรุงรักษาครุภัณฑ์คอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพา มีแนวทางปฏิบัติ ดังนี้

7.1. เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาจะต้องขึ้นทะเบียนครุภัณฑ์เพื่อความสะดวกในการตรวจสอบและการบำรุงรักษา

7.2. ฝทส. จะให้บริการเฉพาะเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาที่ขึ้นทะเบียนครุภัณฑ์แล้ว หรืออยู่ระหว่างการส่งมอบแล้วเท่านั้น

7.3. หากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาเกิดการชำรุดเสียหาย ไม่สามารถใช้งานได้ทั้งด้านซอฟต์แวร์หรือฮาร์ดแวร์ “ผู้ใช้” มีหน้าที่จะต้องแจ้งให้ ฝทส. รับทราบ เพื่อดำเนินการแก้ไขต่อไป

7.4. หากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาอยู่ในสัญญาหรือระยะเวลาการรับประกันเกิดการชำรุดเสียหาย ฝทส. หรือหน่วยงานเจ้าของเครื่องคอมพิวเตอร์พกพา มีหน้าที่ติดต่อคู่สัญญาหรือผู้แทนจำหน่าย เพื่อดำเนินการตรวจซ่อมตามที่ระบุในสัญญา

7.5. หากเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์ต่อพ่วงแบบพกพาอยู่นอกเหนือหรือพ้นระยะเวลาการรับประกัน ฝทส. หรือหน่วยงานเจ้าของเครื่องคอมพิวเตอร์พกพามีหน้าที่ซ่อมแซมในเบื้องต้นหรือประสานกับฝ่ายพัสดุ ในการจัดหาอะไหล่ หรือบริษัทในการดำเนินการซ่อมแซมต่อไป

นโยบายการใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ (Portable Device)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ ได้แก่ คอมพิวเตอร์แท็บเล็ต เป็นต้น และการควบคุมดูแลการนำอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ไปปฏิบัติงานภายนอก สทอภ. เพื่อเป็นการป้องกันข้อมูล และอุปกรณ์ของ สทอภ. ให้มีความมั่นคงปลอดภัย “ผู้ใช้” จึงต้องรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งานการบำรุงรักษา และสิ่งที่ต้องหลีกเลี่ยงในการใช้อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

2. การใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ มีแนวทางปฏิบัติ ดังนี้

2.1. อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ที่ สทอภ. อนุญาตให้ “ผู้ใช้” ใช้งานเป็นสินทรัพย์ของ สทอภ. ดังนั้นผู้ใช้จึงต้องใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่อย่างระมัดระวัง และเพื่องานของ สทอภ.

2.2. โปรแกรมที่ได้ถูกติดตั้งลงบนอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ของ สทอภ. ต้องเป็นโปรแกรมที่ สทอภ. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.3. การเคลื่อนย้ายหรือส่งอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ตรวจซ่อมจะต้องดำเนินการโดย ฝทส. หรือหน่วยงานเจ้าของอุปกรณ์

2.4. “ผู้ใช้” ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

2.5. “ผู้ใช้” ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่และรักษาสภาพของอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ให้มีสภาพเดิม

2.6. “ผู้ใช้” ต้องไม่ใส่อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยน

2.7. การใช้อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่เป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด “ผู้ใช้” ต้องปิดเครื่องเพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

2.8. ไม่วางอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ ได้แก่ แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

2.9. การเช็ดทำความสะอาดหน้าจอภาพ ต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วน

3. ความปลอดภัยทางด้านกายภาพ มีแนวทางปฏิบัติ ดังนี้

3.1. “**ผู้ใช้**” มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย และไม่วางเครื่องทิ้งไว้ในสถานที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

3.2. “**ผู้ใช้**” ต้องไม่เก็บหรือใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระแทก

3.3. “**ผู้ใช้**” ต้องไม่ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Components) ที่ติดตั้งอยู่ภายใน รวมถึงอุปกรณ์สำรองไฟฟ้า

4. การควบคุมการเข้าถึงระบบปฏิบัติการ และการใช้รหัสผ่าน (Password) มีแนวทางปฏิบัติ ดังนี้

4.1. **“ผู้ใช้”** ต้องกำหนดชื่อผู้ใช้งาน (Login) และรหัสผ่าน (Password) ในการใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่

4.2. **“ผู้ใช้”** ต้องกำหนดรหัสผ่านตามรูปแบบเฉพาะของอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ชนิดนั้น ๆ

4.3. **“ผู้ใช้”** ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่เชื่อมต่อกับระบบเครือข่ายของ สทอภ.

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ มีแนวทางปฏิบัติ ดังนี้

5.1. “**ผู้ใช้**” ต้องทำการปรับปรุง (Update) ระบบปฏิบัติการ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

5.2. หาก “**ผู้ใช้**” พบหรือสงสัยว่าอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ “**ผู้ใช้**” ต้องไม่เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งไม่พึงประสงค์ (Malware) ไปยังเครื่องคอมพิวเตอร์อื่น ๆ ได้

6. การสำรองข้อมูลและการกู้คืนข้อมูล มีแนวทางปฏิบัติ ดังนี้

6.1. **“ผู้ใช้”** ต้องทำการสำรองข้อมูลจากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ โดยวิธีการและสื่อ (Media) ต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

6.2. **“ผู้ใช้”** ต้องเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อเกิดการรั่วไหลข้อมูล

6.3. **“ผู้ใช้”** ที่ต้องการเคลื่อนย้ายสื่อสำรองข้อมูลออกนอกสถานที่จะต้องมีการป้องกันการเข้าถึงข้อมูลอย่างมั่นคงปลอดภัย

7. การบำรุงรักษาอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ มีแนวทางปฏิบัติ ดังนี้

7.1. อุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่จะต้องขึ้นทะเบียนครุภัณฑ์เพื่อความสะดวกในการตรวจสอบและการบำรุงรักษา

7.2. ฝทส. จะให้บริการเฉพาะอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่ ที่ขึ้นทะเบียนครุภัณฑ์แล้วหรืออยู่ระหว่างการส่งมอบแล้วเท่านั้น

7.3. หากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่เกิดการชำรุดเสียหาย ไม่สามารถใช้งานได้ทั้งด้านซอฟต์แวร์หรือฮาร์ดแวร์ **“ผู้ใช้”** มีหน้าที่จะต้องแจ้งให้ ฝทส. รับทราบเพื่อดำเนินการแก้ไขต่อไป

7.4. หากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่อยู่ในสัญญาหรือระยะเวลาการรับประกันเกิดการชำรุดเสียหาย ฝทส. หรือหน่วยงานเจ้าของครุภัณฑ์มีหน้าที่ติดต่อคู่สัญญาหรือผู้แทนจำหน่าย เพื่อดำเนินการตรวจซ่อมตามที่ระบุในสัญญา

7.5. หากอุปกรณ์เชื่อมต่อเครือข่ายแบบเคลื่อนที่อยู่นอกเหนือหรือพ้นระยะเวลาการรับประกัน ฝทส. มีหน้าที่ซ่อมแซมในเบื้องต้นหรือประสานกับหน่วยงานเจ้าของครุภัณฑ์ ในการดำเนินการซ่อมแซมต่อไป

นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล
(Media Handling Policy)

1. วัตถุประสงค์

นโยบายนี้จัดทำขึ้นเพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายสินทรัพย์สารสนเทศโดยไม่ได้รับอนุญาต

2. การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนที่ย้ายได้ (Management of Removable Media) มีแนวทางปฏิบัติ ดังนี้

2.1. ข้อมูลที่มีชั้นความลับ ต้องกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว

2.2. ในกรณีที่สื่อบันทึกข้อมูลนั้นไม่ได้ถูกนำมาใช้งานแล้ว ก่อนที่จะนำออกไปจาก สทอภ. ต้องมั่นใจข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก

2.3. ในกรณีที่จำเป็นต้องนำสื่อบันทึกข้อมูลออกไป จะต้องได้รับการอนุมัติจากหน่วยงานที่รับผิดชอบสื่อบันทึกข้อมูลดังกล่าว และต้องบันทึกการโยกย้ายเพื่อใช้ในการตรวจสอบ

2.4. สื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต ได้แก่ อุณหภูมิสูงหรือต่ำเกินไป

2.5. ในการจัดเก็บสื่อบันทึกข้อมูลที่สำคัญ ต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล ได้แก่ มีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน กำหนดบุคลากรที่มีสิทธิในการใช้งาน เป็นต้น

2.6. ถ้าข้อมูลที่ต้องการจัดเก็บมีอายุการจัดเก็บยาวนานกว่าอายุการใช้งานของสื่อบันทึกข้อมูล ต้องจัดเก็บไว้ที่แหล่งอื่น เพื่อป้องกันการสูญหายของข้อมูล

2.7. ต้องจัดทำทะเบียนบันทึกข้อมูลของสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เพื่อลดโอกาสการสูญหายของข้อมูล

2.8. ตัวอ่านสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ จะต้องใช้เพื่อเหตุผลทางราชการเท่านั้น การมอบอำนาจในระดับต่าง ๆ ต้องทำเป็นเอกสารอย่างชัดเจน

3. การกำจัดสื่อบันทึกข้อมูล (Disposal of Media)

การทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีก ต้องเป็นไปอย่างมั่นคงและปลอดภัย เพื่อลดความเสี่ยงของการรั่วไหลข้อมูลของ สทอภ. ไปยังผู้อื่นที่ไม่ได้รับอนุญาต ซึ่งมีแนวทางปฏิบัติดังนี้

3.1. สื่อที่บันทึกข้อมูลที่มีความสำคัญมาก จะต้องมีการทำลายด้วยวิธีการที่ปลอดภัย ได้แก่ การเผา หรือแยกชิ้นส่วนเป็นชิ้นเล็ก ๆ หรือลบข้อมูลด้วยโปรแกรมอื่น ๆ ที่มีใช้ใน สทอภ.

3.2. กระบวนการต่าง ๆ ต้องระบุวิธีการกำจัดสื่อบันทึกข้อมูลอย่างชัดเจน เพื่อความปลอดภัยของข้อมูล ได้แก่ ปฏิบัติตามแนวทางความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

3.3. เพื่อความสะดวก ต้องรวบรวมสื่อทั้งหมดที่ไม่ต้องการแล้วกำจัดพร้อมกันด้วยวิธีการที่ปลอดภัย

3.4. ในกรณีที่เลือกใช้บริการกำจัดสื่อและเอกสาร รวมทั้งอุปกรณ์ต่าง ๆ จากหน่วยงานภายนอก ต้องระวังในการเลือกใช้บริการ ต้องเลือกหน่วยงานภายนอกที่มีการควบคุมที่ดีและมีประสบการณ์

3.5. ในการกำจัดสื่อบันทึกข้อมูล จะต้องมีการบันทึกเพื่อใช้ในการตรวจสอบ

3.6. หากเป็นสื่อบันทึกข้อมูลส่วนบุคคล กระบวนการในการทำลายให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 และ 37

หมายเหตุ : ข้อมูลที่ไม่มีความสำคัญเมื่อมีการรวบรวมเป็นจำนวนมาก ๆ อาจจะกลายเป็นข้อมูลที่มีความสำคัญได้ ดังนั้นในการกำจัด ต้องคำนึงถึงข้อมูลที่มีการรวบรวมไว้ด้วย

4. **ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information Handling Procedures)** เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์ มีแนวทางปฏิบัติดังนี้

4.1. ติดป้ายชื่อของสื่อบันทึกข้อมูลทั้งหมด เพื่อระบุประเภท

4.2. จำกัดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศของผู้ที่ไม่ได้รับอนุญาต

4.3. ทำบันทึกข้อมูลเกี่ยวกับผู้ที่มีสิทธิได้รับข้อมูล

4.4. ข้อมูลที่ป้อนเข้าสู่ระบบและในระหว่างการประมวลผลต้องมีความครบถ้วน และต้องตรวจสอบผลลัพธ์ที่ออกมาด้วย

4.5. ต้องมีการปกป้องข้อมูลที่อยู่ในระหว่างการแสดงผลลัพธ์ออกมาตามระดับความสำคัญ

4.6. เก็บรักษาสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต

4.7. กระจายข้อมูลให้ผู้ที่มีสิทธิได้รับข้อมูลเท่านั้น

4.8. ทบทวนการกระจายข้อมูลและรายชื่อของผู้ที่มีสิทธิได้รับข้อมูลอย่างต่อเนื่อง

หมายเหตุ : กระบวนการเหล่านี้ครอบคลุมทั้งสื่อที่เป็นเอกสาร ระบบคอมพิวเตอร์ ระบบเครือข่าย โทรศัพท์เคลื่อนที่ จดหมายอิเล็กทรอนิกส์ การสื่อสารด้วยเสียง มัลติมีเดีย การบริการของไปรษณีย์ เครื่องถ่ายเอกสาร

5. **การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of System Documentation)**

มาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต ให้ดำเนินการจัดทำชั้นความลับของเอกสารระบบ และดำเนินการตามนโยบายการจัดหมวดหมู่และการควบคุมสินทรัพย์

นโยบายการแลกเปลี่ยนสารสนเทศ
(Information Exchange Policies)

1. **วัตถุประสงค์**

นโยบายนี้จัดทำขึ้นเพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

2. **ข้อระวังสำหรับการแลกเปลี่ยนสารสนเทศ (Information Exchange Policies and Procedures)** เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร และหน่วยงานภายนอก โดยผ่านทางช่องทางการสื่อสารทุกชนิด ต้องพิจารณาดังต่อไปนี้

2.1. ในกรณีข้อมูลที่แลกเปลี่ยนเป็นข้อมูลส่วนบุคคล ให้ดำเนินการตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมวดที่ 2

2.2. การป้องกันจากการถูกดักจับ คัดลอก แก้ไข ส่งผิดเส้นทาง และการทำลายข้อมูล

2.3. การตรวจจับและป้องกัน Source Code ที่ไม่พึงประสงค์ ซึ่งอาจถูกส่งผ่านการสื่อสารทางอิเล็กทรอนิกส์

2.4. การป้องกันการส่งข้อมูลที่สำคัญด้วยวิธีการแนบเอกสาร (Attachment File)

2.5. แนวทางปฏิบัติต้องสอดคล้องกับแนวทางความมั่นคงปลอดภัยของอุปกรณ์ (Equipment Security)

2.6. การสื่อสารไร้สาย ต้องคำนึงถึงความเสี่ยงจะที่เกิดขึ้นด้วย

2.7. ผู้ใช้งานต้องรับผิดชอบในบทบาทหน้าที่ ไม่ฝ่าฝืนนโยบายหรือกฎระเบียบของ สทอภ. ได้แก่ การหมิ่นประมาท การข่มขู่หรือก่อกวนความสงบ การปลอมตัว การส่งต่อจดหมายลูกโซ่ การจัดซื้อจัดจ้างนอกเหนือการอนุมัติ เป็นต้น

2.8. เทคนิคการเข้ารหัส เพื่อปกป้องความลับความสมบูรณ์และความถูกต้องของสารสนเทศ

2.9. แนวทางในการเก็บรักษาและทำลายจดหมายทางราชการต้องเป็นไปตามที่กฎหมายกำหนด

2.10. ไม่ทิ้งเอกสารสำคัญไว้ที่เครื่องถ่ายเอกสาร เครื่องพิมพ์หรือเครื่องโทรสาร ซึ่งผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้

2.11. ควบคุมและยับยั้งการส่งต่อข้อมูลของอุปกรณ์สื่อสาร เช่นการส่งต่อจดหมายอิเล็กทรอนิกส์อัตโนมัติไปนอก สทอภ.

2.12. เตือนผู้ใช้งานให้มีความระมัดระวังไม่ให้ข้อมูลสำคัญรั่วไหลโดยการดักฟังหรือได้ยินแบบไม่ตั้งใจในขณะใช้โทรศัพท์ ได้แก่

- 2.12.1. คนที่อยู่บริเวณใกล้ ๆ ในขณะที่ใช้โทรศัพท์เคลื่อนที่
- 2.12.2. การดักฟังหรือการแอบฟังทางสายโทรศัพท์

2.13. เตือนผู้ใช้งานเกี่ยวกับปัญหาในการใช้เครื่องโทรสาร ได้แก่

- 2.13.1. การเข้าถึงของผู้ที่ไม่ได้รับอนุญาต เพื่อดึงข้อมูลภายในเครื่องที่จัดเก็บไว้
- 2.13.2. การตั้งโปรแกรมในการส่งไปยังเลขหมายปลายทางโดยตั้งใจและไม่ตั้งใจ
- 2.13.3. การส่งเอกสารหรือข้อความผิดเลขหมายโดยการโทรที่ผิดพลาดหรือบันทึกเลขหมายผิด
- 2.13.4. เครื่องโทรสารและเครื่องถ่ายเอกสารรุ่นใหม่จะมีหน่วยความจำในการเก็บเอกสารบางหน้าหรือการส่งที่ผิดพลาด ซึ่งจะถูกพิมพ์ออกมาเมื่อเครื่องทำงานได้ตามปกติ

3. ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange Agreements) ในการแลกเปลี่ยนสารสนเทศ ต้องคำนึงถึงข้อตกลงในการแลกเปลี่ยนสารสนเทศดังต่อไปนี้

3.1. ในกรณีข้อมูลที่แลกเปลี่ยนเป็นข้อมูลส่วนบุคคล ให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมวดที่ 2

3.2. การบริหารจัดการในการควบคุมและแจ้งให้ทราบเกี่ยวกับการสื่อสาร การส่งและการรับ

3.3. การแจ้งให้ผู้ส่งรับทราบเกี่ยวกับการสื่อสาร การส่งและการรับ

3.4. กระบวนการที่สามารถติดตามและปฏิเสธความรับผิดชอบไม่ได้

3.5. มาตรฐานทางเทคนิคขั้นต่ำในการบรรจุและส่งออก

3.6. สัญญาข้อตกลง

3.7. มาตรฐานในการระบุตัวผู้ส่งเอกสาร

3.8. ความรับผิดชอบและภาระหน้าที่เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของสารสนเทศ เช่น การสูญหายของข้อมูล เป็นต้น

3.9. ใช้ระบบป้ายชื่อตามข้อตกลงสำหรับข้อมูลที่มีความสำคัญ เพื่อเข้าใจได้ทันทีในความหมายของป้ายชื่อและเป็นการปกป้องสารสนเทศอย่างเหมาะสม

3.10. ความเป็นเจ้าของและความรับผิดชอบสำหรับการปกป้องข้อมูล ลิขสิทธิ์ การปฏิบัติตามใบอนุญาตการใช้งานซอฟท์แวร์ และค่าตอบแทนต่าง ๆ

3.11. มาตรฐานทางเทคนิคในการบันทึกและอ่านข้อมูลสารสนเทศและซอฟท์แวร์

3.12. การควบคุมพิเศษที่จำเป็นในการปกป้องข้อมูลสำคัญ เช่น การใช้กุญแจเข้ารหัสข้อมูล เป็นต้น

4. การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical Media in Transit)

เพื่อป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร ต้องพิจารณาดังต่อไปนี้

4.1. การส่งสื่อบันทึกข้อมูลที่มีข้อมูลส่วนบุคคลอยู่ ให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมวดที่ 2

4.2. ใช้วิธีการขนส่งหรือพนักงานส่งของที่เชื่อถือได้

4.3. รายชื่อของพนักงานส่งหรือบริษัทส่งของต้องได้รับการอนุมัติจากผู้บริหาร

4.4. การบรรจุภัณฑ์ต้องป้องกันความเสียหายในระหว่างการส่ง โดยเป็นไปตามข้อกำหนดของผู้ผลิต ตัวอย่างการป้องกันปัจจัยทางกายภาพที่จะมีผลต่อการกู้คืนข้อมูล ได้แก่ ความร้อน ความชื้น และสนามแม่เหล็ก

4.5. การควบคุมที่จำเป็นในการปกป้องข้อมูลสำคัญจากการเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต

4.5.1. ใช้ตู้ที่มีกุญแจล็อค

4.5.2. ส่งด้วยมือตนเองและลงบันทึกการรับ-ส่ง เพื่อสามารถตรวจสอบได้

4.5.3. บางกรณีอาจจะต้องใช้วิธีการแยกส่งออกหลาย ๆ ส่วนและหลาย ๆ เส้นทาง เพื่อกระจายความเสี่ยง

5. การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) ต้องพิจารณาถึงความมั่นคงปลอดภัย ดังต่อไปนี้

5.1. การส่งข้อความทางอิเล็กทรอนิกส์ หากเป็นข้อมูลส่วนบุคคลให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมวดที่ 2

5.2. ตรวจสอบที่อยู่ปลายทางของผู้รับ และการส่งข้อความว่ามีความถูกต้องหรือไม่ ก่อนที่จะส่งข้อความ

5.3. ผู้ให้บริการส่งข้อความทางอิเล็กทรอนิกส์ ต้องมีความน่าเชื่อถือและสามารถใช้บริการได้

5.4. ข้อกำหนดทางกฎหมาย เช่นการใช้ลายมือชื่ออิเล็กทรอนิกส์

5.5. การใช้บริการแบบสาธารณะ ต้องระวังในการรับ-ส่งข้อมูลที่เป็นความลับของ สทอภ. ได้แก่ การ Chat การแชร์ไฟล์ เป็นต้น

5.6. ในการส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) ต้องจัดส่งโดยใช้ช่องทางที่ สทอภ. กำหนด

นโยบายสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly Available Information)

การยืนยันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ ครอบคลุมถึงซอฟท์แวร์ ข้อมูลและสารสนเทศอื่น ๆ ที่ต้องการความถูกต้องในระดับสูงที่จะถูกเผยแพร่ออกสู่สาธารณะ จะต้องมีวิธีการในการตรวจสอบ ได้แก่ ลายมือชื่ออิเล็กทรอนิกส์ รวมถึงการตรวจสอบการเข้าถึงข้อมูลจาก เครือข่ายสาธารณะ ข้อมูลที่เผยแพร่ต้องจะมีการตรวจสอบความผิดพลาดต่าง ๆ และได้รับการอนุมัติก่อน ซึ่งผู้เผยแพร่ข้อมูลต้องพิจารณาดังต่อไปนี้

- สารสนเทศนั้นต้องเป็นไปตามกฎหมายที่เกี่ยวข้องกับการปกป้องข้อมูล
- สารสนเทศที่นำเข้าและประมวลผลโดยระบบจะต้องสมบูรณ์และถูกต้องตามสภาวะกาล
- สารสนเทศสำคัญจะต้องถูกปกป้องในระหว่างที่มีการรวบรวม ประมวลผลและจัดเก็บ
- ต้องไม่มีเส้นทางเชื่อมโยง (Link) จากหน้าเว็บไซต์เข้าสู่ระบบงานคอมพิวเตอร์ภายในของ สทอภ.

นโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์
(Social Media Policy)

1. วัตถุประสงค์

เพื่อเป็นแนวทางในการกำกับดูแลการเผยแพร่ข้อมูลและการเข้าถึงสื่อเครือข่ายสังคมออนไลน์ของ สทอภ. รวมถึงบริการอิเล็กทรอนิกส์ตลอดจนการแสดงความคิดเห็นของบุคลากรใน สทอภ. ผ่านสื่อเครือข่ายสังคมออนไลน์ให้เป็นไปอย่างถูกต้องเหมาะสม มีความเป็นระเบียบเรียบร้อยและเกิดประโยชน์สูงสุด ดังนั้น สทอภ. จึงเห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ ให้เป็นไปในทางสร้างสรรค์ โดยมีวัตถุประสงค์ ดังนี้

1.1. เพื่อให้ สทอภ.มีการกำหนดขอบเขตของการใช้สื่อสังคมออนไลน์ทั้งในระดับตัวบุคคลและระดับองค์กร
1.2. เพื่อสร้างและรักษาภาพลักษณ์ของบุคลากรและการดำเนินงานของ สทอภ.
1.3. เพื่อลดความเสี่ยงหรือหลีกเลี่ยงปัญหาอันอาจจะเกิดขึ้นจากการใช้สื่อสังคมออนไลน์
1.4. เพื่อป้องกันการเปิดเผยข้อมูลความลับในทุกระดับทั้ง สทอภ. บริการอิเล็กทรอนิกส์ ผู้มีส่วนได้ส่วนเสีย รวมถึงบุคลากรใน สทอภ.

2. ขอบเขตของนโยบาย

ภายใต้นโยบายนี้ การเข้าถึงสื่อเครือข่ายสังคมออนไลน์ และการเผยแพร่ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง ข้อมูลใด ๆ หรือแสดงความคิดเห็นส่วนตัวผ่านสื่อสังคมออนไลน์ มีผลบังคับเหมือนกับการเผยแพร่ข้อมูลหรือแสดงความคิดเห็นผ่านทางช่องทางอื่น ๆ โดยการใช้งานสื่อสังคมออนไลน์ทุกประเภท จะต้องปฏิบัติและสอดคล้องตามแนวนโยบายของ สทอภ. ได้แก่ พรบ.ข้อมูลข่าวสารของทางราชการ พ.ศ.2540 พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฉบับ พ.ศ. 2560 พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551 อย่างเคร่งครัด

3. องค์ประกอบของนโยบาย

3.1. แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ทั่วไป
3.2. แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ในระดับบุคคล
3.3. แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ในระดับองค์กร

แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ทั่วไป

1. หลักการและแนวปฏิบัติทั่วไป

1.1. สทอภ. อนุญาตให้ใช้ระบบเครือข่ายสำหรับเข้าถึงสื่อสังคมออนไลน์ประเภทเว็บไซต์ที่ไม่มีเนื้อหาขัดต่อกฎหมายศีลธรรม
1.2. บุคลากรของ สทอภ. สามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์ เพื่อประโยชน์ในการเผยแพร่ประชาสัมพันธ์ที่เกี่ยวข้องกับ สทอภ. ติดต่อสื่อสารระหว่างกัน แต่ต้องแยกแยะให้ชัดเจนว่าข้อความใดเป็น “ข่าวประชาสัมพันธ์” ข้อความใดเป็น “ความคิดเห็น” “ความคิดเห็นส่วนบุคคล” “การแลกเปลี่ยนข่าวสารส่วนตัว” “การเผยแพร่ข่าวสารเรื่องงาน” หรืออื่น ๆ และความคิดเห็นดังกล่าวต้องคำนึงถึงประโยชน์สาธารณะด้วย
1.3. การเผยแพร่ประชาสัมพันธ์ที่ประชาสัมพันธ์ในนามของ สทอภ. ผู้เผยแพร่ต้องแสดงตำแหน่งหน้าที่ สังกัด ให้ชัดเจน เพื่อความน่าเชื่อถือ และเพื่อให้ผู้ที่ติดตามสามารถใช้ดุลพินิจในการติดตามได้

1.4. พึงระมัดระวังการใช้ถ้อยคำและภาษา ที่อาจเป็นการดูหมิ่น ทั้งการหมิ่นประมาทบุคคลอื่น หรือหมิ่นประมาทองค์กรและต้องใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์ ไม่ขัดต่อกฎหมาย

1.5. พึงงดเว้นการนำรูปบุคคลอื่น รูปบุคคลสาธารณะ หรือรูปที่สร้างความเสียหายให้แก่บุคคลอื่น องค์กร และสังคม มาแสดงว่าเป็นรูปของตนเอง

1.6. พึงงดเว้นการโพสข้อมูลลามกอนาจาร และอื่น ๆ ที่ไม่เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วยุหรือขัดต่อจริยธรรม ได้แก่ การเมือง ศาสนา ชนชาติ เป็นต้น

1.7. พึงงดเว้นการอ้างอิงหรือเปิดเผยถึงข้อมูลผู้มีส่วนได้ส่วนเสีย ตลอดจนผู้มีส่วนเกี่ยวข้องอย่างเปิดเผยก่อนได้รับอนุญาต

1.8. การใช้สื่อเครือข่ายสังคมออนไลน์จะต้องไม่รบกวนการปฏิบัติงานหรือหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

2. หลักการส่งต่อข้อมูล

2.1. ต้องส่งข้อมูลเฉพาะบุคคลที่รู้จัก แสดงตัวตน ตำแหน่ง หน้าที่การงาน สถานะที่ชัดเจนเท่านั้น

2.2. ต้องตรวจสอบที่มาและความถูกต้องของข้อมูล ก่อนทำการส่งต่อข้อมูลลงในสื่อสังคมออนไลน์

2.3. งดเว้นการส่งต่อข้อมูลของ สทอภ. ที่มีชั้นความลับทุกกรณี

2.4. งดเว้นการส่งต่อข้อมูลหรือข้อความที่เป็นเท็จ

2.5. การเผยแพร่และส่งต่อข้อมูลส่วนบุคคลต้องคำนึงถึงสิทธิของเจ้าของข้อมูลส่วนบุคคล และบทกำหนดโทษตามที่ พรบ.คุ้มครองข้อมูลส่วนบุคคลกำหนดไว้

3. หลักความรับผิดชอบ

หากพบข้อมูลใดๆ ที่ไม่เหมาะสม หรือไม่ถูกต้อง (ได้แก่ สิ่งที่เป็นลิขสิทธิ์ของผู้อื่น หรือการแสดงความคิดเห็นที่เป็นการหมิ่นประมาท) ต้องดำเนินการลบข้อมูลดังกล่าวออกทันที เพื่อลดโอกาสที่จะเกิดข้อขัดแย้งทางกฎหมาย และผลกระทบด้านลบต่อ สทอภ.

4. ข้อสงวนสิทธิ์

4.1. สทอภ. ไม่รับผิดชอบต่อผลของการกระทำที่เกิดจากผู้ใช้งาน และ/หรือบัญชีผู้ใช้งานที่ฝ่าฝืนต่อนโยบายนี้

4.2. หาก สทอภ. ตรวจสอบพบว่าบัญชีผู้ใช้งานใดละเมิดต่อนโยบายนี้ สทอภ. ขอสงวนสิทธิ์ในการระงับและ/หรือยกเลิกบัญชีผู้ใช้งานอินเตอร์เน็ต และ/หรือหยุดให้บริการแก่ผู้ใช้งานนั้น

4.3. หากการกระทำอันฝ่าฝืนต่อนโยบายนี้เป็นความผิดตามกฎหมาย ให้สทอภ. ดำเนินคดีตามกฎหมายโดยลำดับต่อไป

แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ในระดับบุคคล

การนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรใน สทอภ. มีแนวนโยบายและแนวปฏิบัติดังนี้

1. กรณีใช้ชื่อบัญชีผู้ใช้งาน (user account) ที่ระบุถึงต้นสังกัด ผู้ใช้งานพึงใช้ความระมัดระวังในการปฏิบัติตามข้อบังคับจริยธรรม หลักเกณฑ์ และแนวปฏิบัติของ สทอภ. ที่กำกับดูแลตามที่ระบุไว้ในขอบเขตของนโยบาย โดยเฉพาะความถูกต้องและการใช้ภาษาที่เหมาะสม
2. กรณีใช้ชื่อบัญชีผู้ใช้งานที่ระบุถึงตัวตนอันอาจทำให้ผู้ติดตาม (followers) หรือเพื่อนในเครือข่าย (friends) เข้าใจได้ว่าเป็นบุคลากรใน สทอภ. ผู้ใช้งานพึงระมัดระวังการนำเสนอข้อมูลข่าวและการแสดงความคิดเห็นที่อาจนำไปสู่ความเสียหายขององค์กร สังคม และบุคคลอื่น

3. หากการโพสข้อมูลข่าวสารหรือความคิดเห็นผ่านสื่อสังคมออนไลน์ของบุคลากรใน สทอภ. เกิดความผิดพลาดจนก่อให้เกิดความเสียหายต่อองค์กร สังคม และบุคคลอื่น ผู้ใช้งานต้องแสดงความรับผิดชอบต่อองค์กร สังคม และบุคคลอื่นที่ได้รับความเสียหาย ทั้งนี้ ต้องให้ผู้ที่ได้รับความเสียหายได้ มีโอกาสชี้แจงข้อมูลข่าวสารในด้านของตนด้วย

แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์เพื่อประชาสัมพันธ์ในระดับองค์กร

การใช้สื่อสังคมออนไลน์เพื่อประชาสัมพันธ์ในระดับองค์กร ต้องที่จะคำนึงถึงรายละเอียดดังนี้

1. การตั้งค่าบนสื่อสังคมออนไลน์ขององค์กร การใช้ชื่อหรือตราสัญลักษณ์ขององค์กร เพื่อเปิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ โดยมีวัตถุประสงค์เพื่อการประชาสัมพันธ์ เผยแพร่ข้อมูลข่าวสาร หรือการสื่อสารภายในองค์กร จะต้องผ่านการรับทราบและเห็นชอบจากผู้มีอำนาจขององค์กรก่อน
2. การปกป้องข้อมูลที่เป็นความลับขององค์กร ในกรณีที่มีบัญชีผู้ใช้งานขององค์กร ต้องมีการตั้งค่าความเป็นส่วนตัว (Privacy) เพื่อป้องกันไม่ให้บุคคลอื่นโพสต์ข้อความหรือเข้าถึงข้อมูลที่มีชั้นความลับ โดยมีการกำหนดให้อยู่ในวงจำกัดเท่านั้น และต้องให้ความระมัดระวังในการโพสต์ข้อความเฉพาะกลุ่มหรือส่วนบุคคลที่ไม่ต้องการเผยแพร่ให้สาธารณะชนรับรู้
3. การนำเสนอข้อมูลข่าวสารขององค์กรผ่านสื่อสังคมออนไลน์ ต้องเป็นไปตามข้อบังคับจริยธรรม หลักเกณฑ์ และแนวปฏิบัติขององค์กรที่กำกับดูแลตามที่ระบุไว้ในขอบเขตของนโยบาย
4. การนำเสนอข้อมูลข่าวสารขององค์กร ผ่านสื่อสังคมออนไลน์ ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อมูล ต้องให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน
5. ต้องแยกบัญชีผู้ใช้สื่อสังคมออนไลน์แบบส่วนตัวกับแบบองค์กรที่ทำหน้าที่ประชาสัมพันธ์องค์กรออกจากกัน
6. หลีกเลี่ยงการสื่อสารข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง และข้อมูลใด ๆ ขององค์กรหรือที่เกี่ยวข้องกับองค์กรที่ก่อให้เกิดความขัดแย้ง หรือโต้แย้งในสังคม ขัดต่อหลักกฎหมายทั้งในประเทศและในระดับสากล

หมวด 7
การควบคุมการเข้าถึง
(Access Control)

จุดประสงค์ เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผยหรือ การขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสาร ประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร โดยประกอบด้วย

- นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
- นโยบายการบริหารจัดการรหัสผ่าน
- นโยบายการควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
(IT Access Control Policy)

1. วัตถุประสงค์

นโยบายนี้ระบุถึงข้อกำหนดเพื่อควบคุมสำหรับการเข้าถึงระบบสารสนเทศของ สทอภ. เพื่อให้มีความมั่นคงปลอดภัย และป้องกันไม่ให้ผู้ไม่มีสิทธิใช้งานสามารถเข้าถึงระบบได้

2. กระบวนการความมั่นคงปลอดภัยด้านสารสนเทศของการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

2.1. สถานที่ตั้งของระบบสารสนเทศที่สำคัญ ต้องมีการควบคุมการเข้าออกที่รัดกุมและให้เฉพาะบุคคลที่ได้รับอนุญาตและมีความจำเป็นเท่านั้นสามารถเข้าใช้งานได้

2.2. ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบและข้อมูลให้เหมาะสมกับการบริการและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิอย่างสม่ำเสมอ

2.3. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงบริการได้

2.4. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของ สทอภ. และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลที่สำคัญ ทั้งนี้ผู้ที่สามารถใช้ซอฟต์แวร์ หรือฮาร์ดแวร์ในการตรวจตราและเฝ้าระวังในระบบเครือข่ายหรือระบบงานใด ๆ ต้องเป็นผู้ที่ได้รับอนุญาตจากหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ อย่างถูกต้องเท่านั้น

2.5. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

2.6. ในการขออนุญาตเข้าสู่ระบบงานต่าง ๆ จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบกำหนดให้มีการลงนามอนุมัติและเก็บเอกสารดังกล่าวไว้เป็นหลักฐาน

2.7. เจ้าของข้อมูลและเจ้าของระบบงานนั้น ๆ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

2.8. ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชา เจ้าของข้อมูลและเจ้าของระบบงานก่อนตามความจำเป็นในการเข้าใช้ระบบงานคอมพิวเตอร์ของ สทอภ.

3. การบริหารจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

3.1. การลงทะเบียนผู้ใช้งาน (User Registration)

3.1.1. ผู้ใช้งานต้องกรอกข้อมูลในแบบฟอร์มขอใช้งานระบบสารสนเทศ เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

3.1.2. ผู้บังคับบัญชาทำการพิจารณาอนุมัติโดยต้องเป็นไปตามหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย และนำส่งให้เจ้าของระบบดำเนินการต่อไป

3.1.3. เจ้าของระบบต้องทำการพิจารณาอนุมัติโดยคำนึงถึงเหตุผลความจำเป็นและหน้าที่ความรับผิดชอบของผู้ใช้งานว่ามีความจำเป็นต้องเข้าถึงระบบที่ตัวเองดูแลรับผิดชอบและเหมาะสมตามความรับผิดชอบหรือไม่

3.1.4. เจ้าของระบบตั้งค่าต่าง ๆ ในระบบตามรายละเอียดในแบบฟอร์ม พร้อมทำการทดสอบระบบต่าง ๆ เพื่อให้แน่ใจว่าสิทธิที่ทำการกำหนดเป็นไปตามคำร้องขอจากผู้ใช้งาน

3.2. การบริหารจัดการสิทธิการใช้งานระบบ (Privilege Management)

3.2.1. ผู้ดูแลระบบต้องกำหนดสิทธิของผู้ใช้งานตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน ได้แก่ กำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศระบบงานตามความจำเป็นขั้นต่ำเท่านั้น

3.2.2. ผู้ใช้งานต้องได้รับการอนุมัติสิทธิให้เสร็จสมบูรณ์ก่อน จึงจะสามารถเข้าใช้งานระบบได้

3.2.3. ผู้ดูแลระบบต้องจัดทำบัญชีผู้ใช้งาน

3.2.4. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่งและกำนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

3.2.5. ยกเลิก เพิกถอน สิทธิการเข้าถึงระบบสารสนเทศและการตัดออกจากบัญชีผู้ใช้งานเมื่อมีการเปลี่ยนตำแหน่งหรือสิ้นสุดการจ้าง

3.3. การบริหารจัดการรหัสผ่านของผู้ใช้งาน (User Password Management)

เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ ผู้ใช้งานต้องปฏิบัติตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

3.4. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

ผู้ดูแลระบบ เจ้าของข้อมูลและเจ้าของระบบงาน ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่เหมาะสม โดยต้องมีการสอบทานความเหมาะสมของสิทธิของ ผู้ใช้งานในการเข้าใช้ข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงหรือควบคุมการใช้งานสารสนเทศจากผู้ที่ไม่ได้รับอนุญาต ต้องพิจารณาดังต่อไปนี้

4.1. ในกรณีที่อนุญาตให้ Protocol บางประเภทสามารถเข้าถึงระบบเครือข่ายของ สทอภ. จะต้องมีมาตรการการป้องกันล่วงหน้าและขั้นตอนการปฏิบัติงานโดยเฉพาะ

4.2. แม้ว่าจะมีการติดตั้ง Router และ Firewall เพื่อรักษาความปลอดภัยของระบบคอมพิวเตอร์แล้วก็ตาม การแก้ไขหรือเปลี่ยนแปลง Router และ Firewall ในภายหลังอาจก่อให้เกิดความเสี่ยงต่อระบบงานได้ เพื่อลดความเสี่ยงต่าง ๆ ทุกครั้งที่มีการเปลี่ยนแปลง Router และ Firewall จะต้องปฏิบัติตามนโยบายการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ

4.3. ห้ามทำ Packet Forwarding หรือ Re-routing สำหรับ Server ที่มีการติดตั้ง Protocol ที่สามารถทำได้ได้แก่ กำหนดให้ FTP ไม่สามารถทำ IP Forwarding หรือ Passive mode ได้

4.4. หมายเลขเครือข่ายภายใน (Internal Network Address) ของ สทอภ. จำเป็นต้องมีการป้องกันมิให้ส่วนงานที่เชื่อมต่อจากภายนอกสามารถมองเห็นได้ เพื่อป้องกันไม่ให้ Hackers หรือผู้ที่ไม่เกี่ยวข้องสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบงานเครือข่ายและส่วนประกอบของคอมพิวเตอร์ของ สทอภ. ได้โดยง่าย

4.5. ต้องกำหนด Access Control List ของอุปกรณ์ Firewall และ Router ให้ป้องกันการส่งข้อมูลที่มาจากการปลอมแปลงหมายเลข IP Address และ หมายเลขของอุปกรณ์ (MAC Address)

4.6. สำหรับข้อมูลที่ผ่านเข้าและส่งออกจากระบบเครือข่าย สทอภ. ต้องส่งข้อมูลผ่าน Firewall เพื่อป้องกันการเชื่อมต่อจากผู้ที่ไม่ได้รับอนุญาต โดยกำหนดให้ผู้ดูแลระบบเครือข่ายเป็นผู้อนุมัติการเชื่อมต่อระบบเครือข่ายจากภายนอกของ สทอภ.

4.7. การเข้าสู่ระบบเครือข่ายของ สทอภ. ผ่านอินเทอร์เน็ตจะต้องมีการพิสูจน์ตัวตน และได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านระบบสารสนเทศก่อน

4.8. ระบบเครือข่ายทั้งหมดของ สทอภ. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก สทอภ. ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering ได้แก่ การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

4.9. ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายัง สทอภ. โดยต้องกำหนดให้การเชื่อมต่อนี้เข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะกับระบบงานที่กำหนดไว้เท่านั้น และไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่าย สทอภ. ได้โดยอิสระ

4.10. ผู้ดูแลระบบต้องจัดแบ่งระหว่างเครือข่ายภายในและเครือข่ายภายนอก (Segregation in Networks) โดยพิจารณาจากบริการเครือข่ายของกลุ่มผู้ใช้งานทั้งสองฝ่าย โดยใช้ระบบหรืออุปกรณ์ป้องกันการบุกรุกด้วยการใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่น ๆ

5. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก สทอภ. (User Authentication for External Connections)

ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก สทอภ. สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของ สทอภ. ได้

5.1. ผู้ใช้งานทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบเสียก่อน

5.2. การเข้าสู่ระบบของ สทอภ. ต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี เช่นการใช้บัญชีผู้ใช้ร่วมกับรหัสผ่าน เป็นต้น

5.3. ต้องแจ้งเป็นลายลักษณ์อักษรให้กับบุคคลที่ใช้บริการด้านสารสนเทศตามสัญญา ถึงความสำคัญที่มีต่อการรักษาความปลอดภัยของข้อมูลสารสนเทศ ซึ่งแต่ละบุคคลต้องลงนามในเอกสารสัญญาเรื่องการไม่เปิดเผยข้อมูลของ สทอภ. และจัดเก็บเอกสารไว้ในแฟ้มสัญญา

5.4. การเข้าสู่ระบบของ สทอภ. จากอินเทอร์เน็ต หรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องมีบัญชีรายชื่ออยู่ในทะเบียนผู้ใช้งาน และเพื่อเพิ่มความปลอดภัยในการเข้าสู่ระบบต้องมีการใช้วิธีการเข้ารหัส (Cryptographic) ร่วมกับการควบคุม

6. การควบคุมอุปกรณ์ที่ผู้ดูแลระบบได้ติดตั้งไว้สำหรับการเข้าถึงจากภายนอก (Remote Diagnostic Port Protection)

ผู้บังคับบัญชาแต่ละหน่วยงาน ต้องกำหนดให้มีการควบคุมการใช้งานอุปกรณ์ที่ผู้ดูแลระบบได้ติดตั้งไว้ภายใน สทอภ. เพื่อใช้ในการดูแลรักษาระบบจากภายนอก โดยมีแนวทางปฏิบัติดังนี้

6.1. การเข้าสู่ระบบเครือข่ายของ สทอภ. จากระยะไกลนั้น ก่อให้เกิดช่องโหว่ที่มีความเสี่ยงสูงต่อความมั่นคงปลอดภัยของข้อมูลและทรัพยากร การควบคุมผู้ใช้งานที่เข้าสู่ระบบจากระยะไกล จึงต้องมีมาตรการความมั่นคงปลอดภัยด้านสารสนเทศที่เพิ่มขึ้นจากมาตรการเข้าสู่ระบบภายใน สทอภ. ดังนี้

6.1.1.ปิดการใช้งานพอร์ตสายแลนที่ไม่ใช้งาน

6.1.2.ปิดการใช้งานปลั๊กไฟที่ไม่ใช้งาน

6.1.3.เปิดให้ใช้งานพอร์ตหรือบริการที่ได้รับอนุญาตเป็นลายลักษณ์อักษรเท่านั้น โดยมีการกำหนดระยะเวลาเปิดใช้งานอย่างจำกัด

6.1.4.ปิดกั้นการใช้งานพอร์ต USB ในอุปกรณ์ที่มีข้อมูลสำคัญ

6.2. วิธีใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลของ สทอภ. จากระยะไกลได้นั้น ต้องได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามนโยบายฯ ทุกเรื่องที่เกี่ยวข้องกับการเข้าสู่ระบบและข้อมูลของ สทอภ. เมื่อติดต่อจากระยะไกล นอกจากนี้เจ้าของข้อมูลมีหน้าที่ดูแลรักษาและเปลี่ยนแปลงรายชื่อของผู้ใช้งานที่สามารถเข้าสู่ระบบจากระยะไกลให้ถูกต้องและเหมาะสม สามารถให้หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศตรวจสอบความถูกต้องได้

6.3. ต้องมีการกำหนดวิธีการพิสูจน์ตัวตน (Authentication Requirements)

6.4. ก่อนจะกำหนดสิทธิของผู้ใช้งานในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงรายละเอียดที่เกี่ยวข้อง ได้แก่ ระยะเวลาที่จะทำการ Remote หมายเลข IP ของเครื่องคอมพิวเตอร์ต้นทาง (Source IP Address) หมายเลข IP ของเครื่องคอมพิวเตอร์ปลายทาง (Destination IP Address) ที่จะ Remote เหตุผลหรือความจำเป็นรวมทั้งหลักฐานอย่างพอเพียงและต้องได้รับอนุมัติจากฝ่ายที่เป็นเจ้าของข้อมูลอย่างเป็นทางการเท่านั้น

6.5. ต้องควบคุม Port ที่ใช้ในการ Remote เข้าสู่ระบบงานของ สทอภ. อย่างรัดกุม ผู้ใช้งานที่มีความจำเป็นที่จะใช้งาน Remote ต้องได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ

6.6. ไม่ควรนำซอฟต์แวร์การควบคุมจากระยะไกลได้แก่ Team Viewer PC-Anywhere หรือ Carbon copy มาใช้กับคอมพิวเตอร์ของ สทอภ. เพราะซอฟต์แวร์ดังกล่าวสามารถเป็นช่องทางให้ผู้ที่ไม่ประสงค์ดีเข้ามายังเครือข่ายของ สทอภ. และได้สิทธิพิเศษในการเข้าสู่ระบบทั้งนี้หากมีความจำเป็นต้องใช้ซอฟต์แวร์การควบคุมระยะไกลดังกล่าว ต้องได้รับอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามนโยบายฯ ทุกเรื่องที่เกี่ยวข้องกับการเข้าสู่ระบบและข้อมูลของ สทอภ.

6.7. การอนุญาตให้ผู้ดูแลระบบต่าง ๆ เข้าสู่ระบบข้อมูลของ สทอภ. จากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และต้องไม่เปิด Port เพื่อการซ่อมบำรุงระบบจากระยะไกลทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องถูกปิดไม่ให้สามารถใช้การได้และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น เมื่อผู้จัดจำหน่ายระบบทำการซ่อมบำรุงเสร็จเรียบร้อยแล้ว Port ดังกล่าวจะต้องทำการปิดไม่ให้ใช้การได้อีกครั้ง

7. ความมั่นคงปลอดภัยสำหรับการให้บริการเครือข่าย (Security of Network Services)

ผู้บังคับบัญชาแต่ละหน่วยงานและผู้ดูแลระบบ ต้องจัดทำข้อกำหนดหรือสัญญาด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่าง สทอภ. กับเจ้าหน้าที่ผู้ปฏิบัติงานภายใน สทอภ. ซึ่งมีแนวทางปฏิบัติดังนี้

7.1. ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิของผู้ใช้งาน เพื่อควบคุม “เจ้าหน้าที่” ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

7.2. ผู้ดูแลระบบต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

7.3. ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ “เจ้าหน้าที่” สามารถใช้เส้นทางอื่น ๆ ได้ ดังนี้

7.3.1. ห้ามให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) และแผนผังเครือข่าย (Network diagram)

7.3.2. อนุญาตใช้เส้นทางเครือข่าย เพื่อเชื่อมเครือข่ายปลายทางเฉพาะผ่านช่องทางที่กำหนดไว้

7.4. ระบบเครือข่ายทั้งหมดของ สทอภ. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก สทอภ. ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering ได้แก่ การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

7.5. ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายัง สทอภ. โดยต้องกำหนดให้การเชื่อมต่อนี้เข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะกับระบบงานที่กำหนดไว้เท่านั้น และไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิเข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่าย สทอภ. ได้โดยอิสระ

8. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

8.1. ผู้ดูแลระบบต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย โดยมีแนวทางปฏิบัติดังนี้

8.1.1. ต้องไม่แสดงรุ่น (Version)ของโปรแกรมจนกว่าจะ Log On เสร็จสิ้นสมบูรณ์

8.1.2. ต้องไม่แสดง Help ระหว่าง Log On ซึ่งอาจช่วยให้ Hacker ค้นหาช่องทางเข้าได้

8.1.3. ตรวจสอบความถูกต้องของข้อมูลนำเข้าเฉพาะเมื่อการนำเข้าเสร็จสิ้นสมบูรณ์แล้ว ถ้ามีความผิดพลาด ระบบต้องไม่แสดงว่าข้อมูลนำเข้าส่วนใดไม่ถูกต้อง

8.1.4. จำกัดจำนวนครั้งของการพยายามเข้าใช้ระบบ ได้แก่ ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง เป็นต้น และต้องพิจารณาเพิ่มเติมประเด็นต่อไปนี้

- บันทึกการพยายามทั้งที่สำเร็จและไม่สำเร็จ
- หลังจาก Log On ผิดพลาด บังคับระยะเวลาทิ้งช่วงก่อนที่จะยอมให้ทำต่อไป
- ตัดการเชื่อมโยงเครือข่าย
- ส่งข้อความเตือนไปยังหน้าจอของระบบ ถ้าความพยายามในการ Log On หลายครั้งเกินจำนวนครั้งมากที่สุดที่ยอมรับได้

8.1.5. จำกัดจำนวนครั้งสูงสุดในการ Log On ผิดพลาด ถ้าเกินกว่านั้นระบบต้องหยุดการให้ Log On

8.1.6. ต้องแสดงข้อมูลต่อไปนี้หลังจากที่ Log On สำเร็จ

- วันที่และเวลาของการ Log On สำเร็จ
- รายละเอียดของการพยายาม Log On ที่ไม่สำเร็จ ตั้งแต่การ Log On ครั้งที่แล้ว หรือสามารถค้นหาข้อมูลการ Log On ที่ผ่านมาได้

8.2. ผู้ดูแลระบบต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ มีแนวทางปฏิบัติดังนี้

8.2.1.ต้องบังคับใช้สำหรับผู้ใช้งานทุกประเภท

8.2.2. User ID ของผู้ใช้งานต้องสามารถตรวจสอบร่องรอยกิจกรรมของผู้ใช้งานแต่ละคนได้ในภายหลัง

8.2.3.กิจกรรมงานประจำต้องไม่ดำเนินการโดยผู้ใช้งานที่ได้สิทธิพิเศษ

8.2.4.กรณีที่จำเป็นต้องตรวจยืนยันตัวตนอย่างเข้มงวด อาจใช้วิธีอื่นแทนการใช้รหัสผ่านในการตรวจยืนยันตัวตนได้ ได้แก่ วิธีการใช้การเข้ารหัสเพื่อรักษาความลับโดยใช้สมาร์ทการ์ด หรือ วิธีการทางไบโอเมตริก เป็นต้น

8.3. ผู้ดูแลระบบต้องมีการบริหารจัดการรหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

8.4. ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว มีแนวทางปฏิบัติดังนี้

8.4.1.การใช้ยูทิลิตี้ต้องมีการระบุตัวตน ตรวจสอบยืนยัน และการควบคุมสิทธิของผู้ใช้งาน

8.4.2.แยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมประยุกต์

8.4.3.จำกัดการใช้งานของระบบยูทิลิตี้ให้เฉพาะสำหรับผู้ใช้งานที่จำเป็น

8.4.4.การให้สิทธิการใช้ยูทิลิตี้แบบเฉพาะกิจ

8.4.5.ต้องจำกัดสิทธิการใช้งานระบบยูทิลิตี้

8.4.6.การยกเลิกระบบยูทิลิตี้ที่ไม่ได้ใช้งานหรือไม่จำเป็น

8.4.7.ต้องไม่ให้สิทธิการใช้ยูทิลิตี้กับผู้ใช้งานที่มีสิทธิเข้าถึงระบบโปรแกรมประยุกต์

8.4.8.ห้ามติดตั้งและใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์

8.5. ผู้ดูแลระบบต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้งานเมื่อไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้ มีแนวทางปฏิบัติดังนี้

8.5.1.มีกลไกในการเคลียร์ Session เมื่อไม่ได้ใช้งานมาเป็นระยะเวลาที่กำหนด (Time-out)

8.5.2.Time-out ต้องกำหนดให้เหมาะสมกับความเสี่ยงนั้น ประเภทข้อมูลที่เกี่ยวข้อง และระบบซอฟต์แวร์นั้น ๆ ซึ่งกำหนดการใช้งานเป็นระยะเวลา 1 ชั่วโมงต่อการใช้งาน 1 ครั้ง

8.6. ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง มีแนวทางปฏิบัติดังนี้

8.6.1.ตัดการเชื่อมต่อเมื่อใช้งานได้ระยะหนึ่ง ซึ่งได้กำหนดไว้ล่วงหน้า

8.6.2.จำกัดการเชื่อมต่อเครือข่ายให้เฉพาะภายในระยะเวลาทำการ โดยกำหนดให้ใช้งานได้ 3 ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง

8.6.3.ให้ตรวจสอบยืนยันตัวตนใหม่ทุกช่วงเวลาที่กำหนด

9. การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

9.1. ผู้ดูแลระบบต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของแอปพลิเคชันตามนโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ โดยต้องแยกตามประเภทของผู้ใช้งาน การจำกัดสิทธิของผู้ใช้งานต้องพิจารณาอยู่บนพื้นฐานความจำเป็นของระบบซอฟต์แวร์แต่ละระบบ โดยมีแนวทางปฏิบัติดังนี้

9.1.1.เตรียมหน้าจอหรือเมนูสำหรับควบคุมการเข้าถึงระบบของผู้ใช้งานแต่ละกลุ่ม โดยต้องแสดงข้อมูลที่ถูกต้องและเหมาะสมกับผู้ใช้งานแต่ละกลุ่ม

9.1.2.ควบคุมสิทธิการเข้าถึงข้อมูลของผู้ใช้งานแต่ละกลุ่ม

9.1.3.ควบคุมสิทธิการเข้าถึงข้อมูลของระบบซอฟต์แวร์อื่น

9.2. เจ้าของระบบงานต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ โดยมีแนวทางปฏิบัติดังนี้

9.2.1. ต้องระบุให้ชัดเจนว่าระบบโปรแกรมประยุกต์ดังกล่าวมีความสำคัญ (Important) มีความเสี่ยงที่จะเกิดผลกระทบสูง (Sensibility) ต่อหน่วยงานอย่างไรและเจ้าของระบบต้องจัดทำรายละเอียดดังกล่าวเป็นเอกสาร

9.2.2. เมื่อจำเป็นต้องใช้ระบบร่วมกันกับระบบอื่นหรือผู้ใช้งานอื่น จะต้องมีการระบุความเสี่ยงและมีการยอมรับโดยเจ้าของระบบนั้น

10. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

10.1. สร้างความตระหนักรู้ให้เกิดความเข้าใจในมาตรการป้องกัน

10.2. ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

10.3. ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา 30 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

10.4. ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
(IT Access Control Policy)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการใช้รหัสผ่าน

2. การบริหารจัดการรหัสผ่าน

2.1. รหัสผ่านเป็นวิธีพื้นฐานในการระบุตัวตน ดังนั้นจึงต้องมีการควบคุมที่เข้มงวดเพื่อให้มั่นใจว่า ผู้ที่เข้ามาใช้ระบบนั้นคือบุคคลที่มีสิทธิเข้าสู่ระบบข้อมูลของ สทอภ. จริง

2.2. ผู้ใช้งานระบบต้องลงนามยินยอมในสัญญาเรื่องการเก็บรักษารหัสผ่านไว้เป็นความลับ ซึ่งข้อความดังกล่าวรวมอยู่ในเงื่อนไขการจ้างงาน

2.3. สำหรับผู้ใช้งานรายใหม่จะได้รับรหัสผ่านเริ่มแรกในการผ่านเข้าระบบและเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที และต้องเปลี่ยนรหัสผ่านตามระยะเวลาอย่างน้อยปีละ 2 ครั้ง

2.4. รหัสผ่านชั่วคราวจะมีการนำมาใช้สำหรับผู้ใช้งานที่ลืมรหัสผ่านและมีหลักฐานพิสูจน์ตนได้ว่าเป็นผู้ใช้งานที่มีสิทธิใช้งานระบบจริง ได้แก่ ตรวจสอบบัตร “เจ้าหน้าที่” เป็นต้น รหัสผ่านดังกล่าวต้องใช้อย่างระมัดระวังและจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

2.5. ต้องกำหนดให้ผู้ใช้งานป้อน User ID และรหัสผ่านในการใช้งาน เพื่อป้องกันการปฏิเสธความรับผิดชอบ

2.6. กำหนดให้ผู้ใช้งานสามารถกำหนดรหัสผ่านของตนเองได้และมีกระบวนการตรวจสอบอีกครั้งก่อนยืนยันการเปลี่ยนรหัสผ่านเพื่อป้องกันความผิดพลาด

2.7. แนะนำให้ผู้ใช้งานกำหนดรหัสผ่านที่มีคุณภาพ ต้องมีการแนะนำว่ารหัสผ่านที่ผู้ใช้งานกำหนดนั้นอยู่ในระดับอ่อน ปานกลาง หรือแข็งแกร่ง เป็นต้น

2.8. ต้องไม่แสดงรหัสผ่านที่พิมพ์ลงไปหรือซ่อนไม่ให้มองเห็นหรือเข้าใจได้

3. การใช้งานรหัสผ่าน

3.1. เก็บรหัสผ่านไว้เป็นความลับ

3.2. ไม่เก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ในรูปแบบที่สามารถอ่านได้ หรือไม่เก็บรักษารหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถเห็นหรือเข้าถึงได้ง่าย ได้แก่ บนเครื่องคอมพิวเตอร์ บนโต๊ะทำงาน เป็นต้น และต้องเก็บข้อมูลรหัสผ่านไว้ต่างหากจากข้อมูลอื่น

3.3. ไม่พิมพ์รหัสผ่านในขณะที่มีผู้อื่นเห็นการพิมพ์ดังกล่าว

3.4. ไม่ทำการใด ๆ เพื่อให้ตนเองทราบถึงบัญชีผู้ใช้งานหรือรหัสผ่านของผู้อื่น

3.5. เปลี่ยนรหัสผ่านส่วนของตนเองในครั้งแรกของการใช้งาน ไม่ว่าระบบจะบังคับให้มีการเปลี่ยนรหัสผ่านหรือไม่ก็ตาม และไม่ตั้งรหัสผ่านซ้ำกับรหัสผ่านเดิม

3.6. เมื่อผู้ใช้งานตรวจพบ หรือสงสัยว่ารหัสผ่านของผู้ใช้งานถูกนำไปใช้โดยผู้อื่น ผู้ใช้งานต้องรายงานเหตุการณ์ให้ผู้ดูแลระบบทราบ และให้ดำเนินการเปลี่ยนรหัสผ่านทันที

3.7. ถ้าพบว่ารหัสผ่านของตนถูกล็อคโดยไม่ทราบสาเหตุ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบ

3.8. ในกรณีที่ได้รับความช่วยเหลือในการแก้ไขปัญหาและต้องการให้ใส่รหัสผ่าน ผู้ใช้งานต้องไม่ให้รหัสผ่านแก่ผู้ช่วยเหลือ แต่ต้องใส่รหัสผ่านด้วยตนเอง

4. การกำหนดรหัสผ่าน

4.1. การกำหนดรหัสผ่านต้องไม่ใช้คำศัพท์ที่มาจากพจนานุกรม, ชื่อหนัง, ชื่อสถานที่หรือชื่อสิ่งลึกลับ และต้องไม่ใช้ข้อมูลที่เกี่ยวข้องกับ สทอภ. หรือเป็นข้อมูลส่วนตัวของผู้ใช้งานซึ่งอาจง่ายแก่การคาดเดา (ได้แก่ ว/ด/ป เกิด, เลขบัตรประชาชน, รหัส“เจ้าหน้าที่”, ที่อยู่, ชื่อบุคคลในครอบครัว, เบอร์โทรศัพท์เป็นต้น)

4.2. ต้องไม่กำหนดรหัสผ่านที่ประกอบด้วยตัวอักษรหรือตัวเลขที่เรียงซ้ำกันเกินกว่า 3 ตัว หรือเรียงกันตามลำดับ ได้แก่ aaaabbbb, 11111111, abcdefg

4.3. รหัสผ่านที่แนะนำต้องมีลักษณะดังนี้

4.3.1.ต้องมีความยาวอย่างน้อย 8 ตัวอักษรหรือตามที่ผู้ดูแลระบบกำหนด

4.3.2..ต้องมีส่วนประกอบของอักษรอักขระพิเศษหรือตัวเลขประสมกันตามลักษณะดังนี้

- ตัวอักษรใหญ่ ได้แก่ A, B, C, ...
- ตัวอักษรเล็ก ได้แก่ a, b, c, ...
- ตัวเลข ได้แก่ 0, 1, 2, ...
- สัญลักษณ์พิเศษ ได้แก่ !, @, # , $, ...

5. การเปลี่ยนรหัสผ่าน

5.1. รหัสผ่านเข้าสู่ระบบ (ได้แก่ root, admin ฯลฯ) ต้องเปลี่ยนอย่างน้อยทุก 6 เดือน

5.2. รหัสผ่านของผู้ใช้งานต้องเปลี่ยนอย่างน้อยทุก 6 เดือน

6. การยกเลิกรหัสผ่าน

รหัสผ่านของผู้ใช้งานที่ลาออก สิ้นสุดการจ้างงานหรือย้าย ต้องดำเนินการยกเลิกสิทธิ (Disable) ของผู้ใช้งานในระบบ หลังจาก 15 วัน ส่วนการลบข้อมูลผู้ใช้จะพิจารณาเป็นแต่ละกรณี

นโยบายการควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร
(Mobile Computing and Teleworking Policy)

1. วัตถุประสงค์

นโยบายนี้จัดทำขึ้นเพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

2. อุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communications)

เพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (ได้แก่ Notebook , Tablet และ Smart Phone เป็นต้น) ต้องพิจารณาดังต่อไปนี้

2.1. ในกรณีที่มีการใช้งานเครื่องคอมพิวเตอร์แบบพกพาที่เป็นสินทรัพย์ของ สทอภ. จะต้องปฏิบัติตามนโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook Computer Policy) อย่างเคร่งครัด

2.2. อุปกรณ์สื่อสารประเภทพกพาที่ได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศแล้วเท่านั้นที่จะสามารถเข้าถึงข้อมูลสารสนเทศของ สทอภ. ได้

2.3. อุปกรณ์สื่อสารประเภทพกพาจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

2.4. ไม่เก็บข้อมูลสำคัญของ สทอภ. ไว้บนอุปกรณ์สื่อสารประเภทพกพา แต่ถ้าไม่สามารถจัดเก็บ บนเครื่องคอมพิวเตอร์ส่วนบุคคลของ สทอภ. ที่ใช้งานอยู่ได้ ข้อมูลที่จัดเก็บบนอุปกรณ์สื่อสารประเภทพกพาจะต้องมีวิธีการป้องกันบุคคลอื่น ๆ เข้าถึงข้อมูลสำคัญดังกล่าว ได้แก่ การใช้ รหัสผ่าน (Password) ในการป้องกันเป็นต้น

2.5. ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

2.6. ผู้ใช้งานอุปกรณ์สื่อสารประเภทพกพา ต้องระวังการแอบดูข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต

2.7. คอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายอื่น ๆ ได้แก่ อุปกรณ์ทวนสัญญาณเครือข่ายไร้สาย (Wireless Repeater) ที่ต้องการเชื่อมต่อกับระบบของ สทอภ. จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ

2.8. กรณีที่อุปกรณ์สื่อสารประเภทพกพาเป็นสมบัติของ สทอภ. การคืนเครื่องหรือส่งซ่อม ให้ผู้ใช้งานทำสำเนาข้อมูลจากอุปกรณ์สื่อสารประเภทพกพาเก็บไว้ทั้งหมด และลบข้อมูลทั้งหมดที่มีอยู่บนอุปกรณ์สื่อสารประเภทพกพา ก่อนส่งให้หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศ

2.9. อุปกรณ์สื่อสารประเภทพกพา ได้แก่ เครื่องคอมพิวเตอร์แบบพกพา (Notebook, Tablet หรือ Smart Phone) ต้องมีกระบวนการเพื่ออัพเดทระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ ตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ของ สทอภ.

2.10. หากผู้ใช้งานหมดสภาพการเป็น “เจ้าหน้าที่” ของ สทอภ. สิทธิในการใช้งานอุปกรณ์สื่อสารประเภทพกพาที่เป็นสมบัติของ สทอภ. เป็นอันสิ้นสุดลงทันที

2.11. สทอภ. อาจดำเนินการทางวินัย แพ่ง หรืออาญา กับผู้ที่ล่วงละเมิดโดยการใช้อุปกรณ์สื่อสารประเภทพกพาของ สทอภ. เพื่อเข้าถึงล่วงละเมิดใช้งาน หรือล่วงละเมิดเผยแพร่ข้อมูลสารสนเทศที่เป็นความลับโดยที่ผู้นั้นไม่มีสิทธิอันชอบ

หมวด 8
การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
(Information System Acquisition, Development and Maintenance)

จุดประสงค์ เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ ป้องกันความผิดพลาด การสูญหายและการเปลี่ยนแปลงสารสนเทศ หรือการใช้งานสารสนเทศผิดวัตถุประสงค์ รักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยวิธีการเข้ารหัสข้อมูล สร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สารสนเทศ และไฟล์ต่าง ๆ ของระบบที่ให้บริการลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ โดยประกอบด้วย

- นโยบายการพัฒนาระบบสารสนเทศ
- นโยบายการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ

นโยบายการพัฒนาระบบสารสนเทศ
(IT Systems Development Policy)

1. วัตถุประสงค์

เพื่อลดความเสี่ยงต่อการเสียหายหรือการเปลี่ยนแปลงแก้ไขข้อมูลและระบบสารสนเทศ ที่มีความสำคัญต่อการปฏิบัติงานของ สทอภ.

2. ความมั่นคงปลอดภัยด้านสารสนเทศในการพัฒนาระบบสารสนเทศ

2.1. หน่วยงานที่ดูแลระบบสารสนเทศ จะต้องทำการวิเคราะห์ระบบสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้

2.1.1.มาตรการปฏิบัติก่อนเกิดความเสียหาย ได้แก่ การสำรองข้อมูล ระบบเครือข่ายสำรอง เป็นต้น

2.1.2.มาตรการปฏิบัติหลังเกิดความเสียหาย ได้แก่ แผนการกู้คืน ระยะเวลาในการกู้คืน เป็นต้น

2.2. การพัฒนาระบบสารสนเทศต้องมีการควบคุม เพื่อให้เกิดความถูกต้องและเหมาะสมของข้อมูลที่นำเข้าและผลลัพธ์ที่ได้จากระบบ จึงจำเป็นที่จะต้องมีระบบการตรวจทานความถูกต้องของข้อมูลที่ดี เพื่อลดความเสี่ยงของการนำข้อมูลเข้าและการประมวลผลข้อมูล

2.3. หากระบบสารสนเทศที่พัฒนาขึ้น มีความเกี่ยวข้องกับการดำเนินงานขององค์กร การเงิน สุขภาพ ชีวิต ทรัพย์สิน ภาพลักษณ์ขององค์กร หน่วยงานเจ้าของระบบ ต้องทำการประเมินความเสี่ยง (Risk Evaluation) เพื่อให้ทราบถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินงานขององค์กร รวมทั้งและต้องจัดทำข้อตกลงในการให้บริการ (Service Level Agreement) ของระบบสารสนเทศที่พัฒนาด้วย

2.4. หน่วยงานภายใน สทอภ. ที่มีการพัฒนาระบบสารสนเทศ และอยู่ภายใต้โดเมนเนม gistda.or.th (sub domain) ต้องแจ้งข้อมูลเกี่ยวกับระบบสารสนเทศนั้นให้ ฝทส. ดังนี้

2.4.1.รายชื่อผู้ดูแลรับผิดชอบระบบสารสนเทศ พร้อมเบอร์โทรศัพท์ และ อีเมล์

2.4.2.ชื่อหน่วยงาน

2.4.3.หมายเลข IP Address และสถานที่ติดตั้งระบบสารสนเทศ

2.4.4.รายละเอียดทางเทคนิค ได้แก่ ระบบปฏิบัติการที่ใช้ ระบบฐานข้อมูล เทคโนโลยีหรือภาษาคอมพิวเตอร์ที่ใช้พัฒนาระบบสารสนเทศ เป็นอย่างน้อย

2.5. หน่วยงานภายใน สทอภ. ที่มีการพัฒนาระบบสารสนเทศที่ให้บริการในลักษณะ Web Application และอยู่ภายใต้โดเมนเนม gistda.or.th (sub domain) จะต้องให้บริการผ่าน Protocal HTTPS โดยหน่วยงานสามารถขอใบรับรองอิเล็กทรอนิกส์ จาก ฝทส.

2.6. หน่วยงานภายใน สทอภ. ที่มีการพัฒนาระบบสารสนเทศในลักษณะ Web Application หรือ Mobile Application จะต้องควบคุมการพัฒนาระบบสารสนเทศให้เป็นไปตามมาตรฐานการเขียน code ที่ดี (security coding) ได้แก่ OWAPS เป็นต้น

2.7. การพัฒนาระบบฐานข้อมูลของระบบสารสนเทศนั้น หากฐานข้อมูลดังกล่าวมีการจัดเก็บข้อมูลส่วนบุคคล ต้องพิจารณาถึงการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล การลบหรือทำลายข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยของข้อมูล ให้เป็นไปตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.8. การตรวจสอบข้อมูลนำเข้า (Input Data Validate) ในกรณีที่เจ้าของข้อมูลต้องการนำข้อมูลเข้าไปยังระบบสารสนเทศ ก่อนที่จะนำเข้าต้องตรวจสอบข้อมูลว่าเป็นข้อมูลที่ถูกต้อง ครบถ้วนและไม่ก่อให้เกิดความเสียหายต่อระบบ และ ในกรณีที่เป็นข้อมูลส่วนบุคคล ผู้เก็บรวบรวมต้องแจ้งให้เจ้าของข้อมูลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลข้อมูลส่วนบุคคล โดยให้เป็นไปตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.9. การควบคุมข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of Internal Processing) ในกรณีที่เจ้าของข้อมูลมีการนำข้อมูลเข้าไปยังระบบสารสนเทศ ในระหว่างการประมวลผลจะต้องกำหนดกลไกสำหรับการตรวจสอบว่า ข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ ได้แก่ อาจมีสาเหตุจากความผิดพลาดในการประมวลผล การกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น

2.10. การตรวจสอบความถูกต้องของข้อความ (Message Integrity) เจ้าของข้อมูลต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอปพลิเคชัน (เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง) รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต

2.11. การตรวจสอบข้อมูลผลลัพธ์ (Output Data Validation) ก่อนนำข้อมูลออกจากระบบต้องปฏิบัติดังนี้

2.11.1. มีการอนุญาตจากเจ้าของข้อมูลให้นำข้อมูลออกจากระบบได้

2.11.2. มีการตรวจสอบความถูกต้องของข้อมูล

2.11.3. มีกระบวนการบันทึกโดยเข้ารหัสข้อมูล สามารถพิสูจน์และรับรองข้อมูล ในกรณีที่เป็นข้อมูลในชั้นความลับ

3. มาตรการการเข้ารหัสข้อมูล (Cryptographic Controls)

3.1. ต้องมีการกำหนดชั้นความลับของข้อมูลและสารสนเทศ เพื่อให้ทราบถึงสถานะและการดำเนินการในการเข้ารหัสข้อมูลสารสนเทศที่ใช้

3.2. เจ้าของข้อมูลต้องกำหนดให้มีการเข้ารหัสข้อมูลตามมาตรฐานสากล ได้แก่อัลกอริทึม RSA, DES, 3DES เป็นต้น และต้องมีการกำหนดชั้นความลับของข้อมูลและสารสนเทศ เพื่อให้ทราบถึงสถานะและการดำเนินการในการเข้ารหัสข้อมูลสารสนเทศที่ใช้

3.3. อัลกอริทึมที่เรียกใช้ต้องรองรับโปรแกรมประยุกต์ที่นำไปใช้งานได้ ได้แก่ PGP (Pretty Good Privacy), SSL (Secure Socket Layer), TLS (Transport Layer Security) เป็นต้น

3.4. ความยาวของคีย์ในการเข้ารหัสต้องไม่น้อยกว่า 56 บิตสำหรับการเข้ารหัสแบบสมมาตร (Symmetric) และแบบอสมมาตร (Asymmetric) ต้องมีความยาวไม่น้อยกว่าตามที่ตกลงกันไว้

3.5. เจ้าของข้อมูลต้องมีการทบทวนมาตรฐานของคีย์ที่เข้ารหัสในทุก ๆ ปี เพื่อให้สอดคล้องกับความปลอดภัยและประสิทธิภาพของเครื่องที่ดำเนินงาน

3.6. กรณีที่ไม่ทราบหรือต้องการข้อมูลเกี่ยวกับการเข้ารหัสเพิ่มเติม ให้ติดต่อมาที่หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ

3.7. ข้อมูลที่มีการเข้ารหัสต้องจัดให้มีกระบวนการในการบริหารจัดการกุญแจ (Key Management) ที่มีประสิทธิภาพ โดยการดำเนินการเกี่ยวกับกุญแจทุกประเภท ได้แก่ การสร้าง การจัดเก็บ การจัดส่ง และการเปลี่ยน ต้องกระทำอย่างปลอดภัยและมีการควบคุมที่เหมาะสม

4. ความมั่นคงปลอดภัยด้านสารสนเทศของแฟ้มข้อมูลระบบ (Security of System Files)

4.1. หลักการควบคุมการติดตั้งซอฟต์แวร์ (Control of Operational Software) ผู้บังคับบัญชาต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ให้สอดคล้องกับหลักเกณฑ์การติดตั้งระบบสารสนเทศใหม่

4.2. หลักการป้องกันข้อมูลจริงที่ใช้ในการทดสอบระบบ (Protect of System Test Data) ข้อมูลจริงที่จะนำใช้ทดสอบระบบ ต้องได้รับอนุญาตจากผู้บังคับบัญชาที่รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องลบข้อมูลจริงออกจากระบบทดสอบทันที และบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ทดสอบอะไรบ้าง รวมถึงวันเวลาและหน่วยงานที่ทดสอบแจ้งไปยังผู้บังคับบัญชาที่รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

4.3. หลักการควบคุมการใช้งานซอฟต์แวร์ไลบารี่ (Access Control to Program Source Library) ผู้บังคับบัญชาและหน่วยงานเจ้าของระบบต้องมีการควบคุมการใช้งานไลบารี ซึ่งประกอบด้วย Source Code ของระบบที่ใช้งานจริงหรือระบบที่ให้บริการ โดยมีแนวทางปฏิบัติดังนี้

4.3.1. ห้ามเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริง และต้องเก็บไว้ในที่ปลอดภัย

4.3.2. ผู้บังคับบัญชาที่รับผิดชอบต้องแต่งตั้งผู้มีอำนาจในการดูแลและปรับปรุงไลบารี่

4.3.3. ระหว่างทดสอบต้องไม่เก็บ Source Code ที่ใช้ทดสอบรวมกับไลบารี่ที่ใช้งานได้จริง

4.4. การเผยแพร่ไฟล์เอกสารดิจิทัลที่มีชั้นความลับ ได้แก่เอกสารราชการ ที่มีการประทับลับ และลับมาก ผ่านสื่อออนไลน์ ได้แก่ เว็บไซต์ หรือโมบายแอปพลิเคชั่น จะต้องได้รับอนุญาตจากผู้อำนวยการหน่วยงานเป็นอย่างน้อย จึงสามารถเผยแพร่เอกสารผ่านสื่อออนไลน์ได้

5. ขั้นตอนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการพัฒนาระบบ (Security in Development and Support Processes)

5.1. การตรวจสอบซอฟต์แวร์ที่จัดหามาใช้งานผู้บังคับบัญชาหรือหน่วยงานที่เกี่ยวข้องต้องมีการตรวจสอบหรือทดสอบซอฟต์แวร์ที่จัดหามาใช้งานก่อนติดตั้ง เพื่อป้องกันตัว Source Code ที่ไม่พึงประสงค์แฝงตัวมากับตัวซอฟต์แวร์นั้น (Covert Channel and Trojan Code)

5.2. การควบคุมการว่าจ้างพัฒนาระบบ (Outsourced Software Development) ผู้บังคับบัญชาหรือหน่วยงานที่ว่าจ้างการพัฒนาระบบต้องมีการทำสัญญาว่าจ้างการพัฒนา ระบบ ซึ่งต้องครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบ ระบบโดยละเอียดก่อนติดตั้งใช้งานจริง การรับรองคุณภาพของระบบ รวมถึงการกำหนดขอบเขตในการจ้างพัฒนาระบบ

5.3. การตรวจสอบระบบสารสนเทศทั้งหมดที่เกี่ยวข้อง (Technical Review of Operating System Changes) ผู้บังคับบัญชาหรือหน่วยงานที่ว่าจ้างการพัฒนาระบบ ต้องตรวจสอบ ระบบสารสนเทศที่เกี่ยวข้องภายหลังที่ได้ติดตั้งระบบใหม่ เพื่อให้ทราบถึงผลกระทบจากการพัฒนาระบบและเป็นไปตามเงื่อนไขในการว่าจ้าง พร้อมทั้งมีการตรวจสอบจากหน่วยงาน ที่เกี่ยวข้องหลังจากการติดตั้งระบบใหม่หรือการปรับปรุง โดยแจ้งไปยังผู้บังคับบัญชาที่รับผิดชอบ และเก็บรายละเอียดตัวเอกสารไว้เป็นหลักฐาน

6. การติดตั้งระบบสารสนเทศใหม่

6.1. รายการอุปกรณ์ที่จะนำมาติดตั้งพร้อมกับรายละเอียดคุณลักษณะเฉพาะของอุปกรณ์ ชื่อรุ่น ยี่ห้อ และหมายเลขครุภัณฑ์

6.2. รายการซอฟต์แวร์แพคเกจที่จะนำมาติดตั้ง พร้อมกับรายละเอียด ยี่ห้อ เวอร์ชั่น ประเภท ซอฟต์แวร์และหมายเลขครุภัณฑ์

6.3. รายการของระบบงานที่พัฒนาใหม่ ประกอบด้วย ชื่อระบบงาน หรือชื่อโครงการ ภาษาที่ใช้ในการพัฒนา เครื่องมือในการพัฒนา ชื่อซอฟต์แวร์และเวอร์ชั่นของระบบฐานข้อมูลที่ใช้

6.4. ชื่อโครงการ เลขที่สัญญา และหน่วยงานที่รับผิดชอบ พร้อมรายชื่อ เบอร์โทรศัพท์ อีเมล์ของผู้ประสานงานด้านนโยบายและด้านเทคนิค

6.5. วันที่ เวลา ที่ติดตั้งระบบงาน และวันที่ เวลาเปิดใช้งาน

6.6. กรณีการติดตั้งระบบงานที่มีการเชื่อมต่อออนไลน์จะต้องผ่านการทดสอบความมั่นคงปลอดภัยของซอสโค้ด และมีหลักฐานการตรวจสอบความมั่นคงปลอดภัยและจะต้องไม่มีช่องโหว่ระดับความเสี่ยงสูง (Critical Risk) หรือมีหลักฐานแสดงว่าได้ดำเนินการแก้ไขแล้วจึงสามารถเปิดใช้งานได้

นโยบายการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศ
(IT change management policy)

1. วัตถุประสงค์

การเปลี่ยนแปลงระบบงานใด ๆ จะต้องมีการควบคุม เพื่อไม่ให้มีผลกระทบต่อโปรแกรมประยุกต์ (Application Software) โปรแกรมระบบ (System Software) ระบบเครือข่าย (Network System) หรือการเปลี่ยนแปลงอื่น ๆ ที่เกิดจากการเปลี่ยนแปลงระบบงาน ได้แก่ การพัฒนาระบบ การทดสอบระบบ จะต้องอยู่ภายใต้การควบคุมที่เหมาะสมและเพียงพอ โดยวิธีการดังกล่าวจะช่วยให้ระบบสารสนเทศนั้น ๆ สามารถทำงานเข้ากันได้ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์

การเปลี่ยนแปลงแก้ไข ต้องมีคำขอการเปลี่ยนแปลงอย่างเป็นทางการ ซึ่งมีการอนุมัติโดยผู้บริหารที่มีอำนาจอนุมัติการเปลี่ยนแปลงระบบงานนั้น ๆ

2. ความต้องการในการขอให้มีการเปลี่ยนแปลง

2.1. ผู้ร้องขอต้องดำเนินการตามกระบวนการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้งานจริงหรือใช้งานอยู่แล้วโดยทำหนังสือแจ้งไปยังหน่วยงานเจ้าของข้อมูล หน่วยงานเจ้าของระบบงาน และหรือหน่วยงานที่เกี่ยวข้องทุกส่วนให้รับทราบก่อนทำการแก้ไขซอฟต์แวร์นั้น และต้องมีการอนุมัติโดยผู้มีอำนาจในการลงนามในแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form by User) แบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ จะต้องมีข้อมูลที่จำเป็นดังนี้

2.1.1. คำขอให้แก้ไขต้องมาจากผู้มีสิทธิ

2.1.2. เหตุผลการปฏิบัติงานที่ต้องมีการเปลี่ยนแปลง

2.1.3. ลักษณะของข้อบกพร่องที่ทำให้ต้องมีการเปลี่ยนแปลง (ถ้ามี)

2.1.4. ทรัพยากรที่จำเป็นต้องใช้ในการเปลี่ยนแปลงระบบงาน

2.1.5. รายละเอียดการทดสอบ (Test Script)

2.1.6. กระบวนการนำระบบเดิมที่ใช้งานได้กลับมาใช้ใหม่ ในกรณีที่ระบบใหม่มีปัญหา

2.1.7. เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ

2.1.8. ต้องเก็บรายละเอียดของคำขอไว้เป็นหลักฐาน

2.2. ผู้บังคับบัญชาเจ้าของข้อมูล (Information Owner) และผู้บังคับบัญชาเจ้าของระบบงาน (Application Owner) ที่เกี่ยวข้องกับการเปลี่ยนแปลงนั้น ๆ จะต้องพิจารณาเหตุผลของคำขอ เปลี่ยนแปลง และทำการลงนามอนุมัติในคำขอเปลี่ยนแปลง

2.3. ทุกครั้งที่มีการเปลี่ยนแปลงระบบงาน จะต้องมีการจัดเตรียมและปรับปรุงคู่มือในการใช้งานระบบงานและคู่มือในการอบรมให้กับผู้ใช้งาน ต้องมีการจัดทำและปรับปรุงให้สอดคล้องกับการเปลี่ยนแปลงระบบงานอยู่เสมอ

3. การกำหนดบทบาทและหน้าที่การเปลี่ยนแปลง

3.1. ต้องมีการกำหนดบทบาทและความรับผิดชอบของแต่ละบุคคลที่เกี่ยวข้องกับกระบวนการควบคุมการเปลี่ยนแปลงอย่างชัดเจน เพื่อการควบคุมที่ดีต้องไม่ทำโดยบุคคลเดียวกัน

3.2. ต้องมีการกำหนดผู้รับผิดชอบระบบอย่างชัดเจน และเมื่อมีการเปลี่ยนแปลงผู้รับผิดชอบหรือบทบาทความรับผิดชอบจะต้องแจ้งให้ ฝทส. ทราบอย่างชัดเจน

3.3. โปรแกรมที่ใช้งานจริงสำหรับระบบงานนั้น ๆ ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิในการโอนย้ายโปรแกรมที่พร้อมใช้งานไปยังส่วนที่ใช้งานจริง

3.4. ต้องแบ่งแยกส่วนที่ใช้สำหรับงานต่อไปนี้ออกจากกัน ได้แก่ ส่วนการพัฒนาระบบงาน ส่วนที่ใช้สำหรับโอนย้ายโปรแกรมก่อนการย้ายเข้าส่วนที่ใช้งานจริง ส่วนที่ใช้ทดสอบระบบสำหรับผู้ใช้งาน และส่วนที่ใช้งานจริงในแต่ละส่วนต้องมีการควบคุมการเข้าใช้งานที่ดี

4. การเปลี่ยนแปลงระบบคอมพิวเตอร์ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูล

4.1. การเปลี่ยนแปลงต่อระบบคอมพิวเตอร์ ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูล จะต้องได้รับอนุมัติจากผู้บังคับบัญชาที่ดูแลระบบงานนั้น ๆ เป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการหยุดชะงักของการปฏิบัติงาน หรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

4.2. การเปลี่ยนแปลงระบบงานใด ๆ ต้องไม่รบกวนหรือขัดขวางการปฏิบัติงานของระบบงานปัจจุบัน และการเปลี่ยนแปลงดังกล่าวนั้น จะต้องสามารถใช้งานร่วมกับข้อมูลและระบบงานที่มีการใช้อยู่ในปัจจุบันได้ด้วย

4.3. การเปลี่ยนแปลงอุปกรณ์หรือสื่อที่ใช้ในการจัดเก็บข้อมูล ต้องทำการลบข้อมูลที่ไม่ใช้งานแล้วทั้งหมดของ สทอภ. อย่างถาวรออกจากอุปกรณ์หรือสื่อที่ใช้สำหรับเก็บข้อมูลที่มีการเปลี่ยนแปลง

4.4. มีกระบวนการทำลาย หรือจำหน่ายอุปกรณ์เสื่อมสภาพหรือหมดอายุ

4.5. ผู้รับผิดชอบระบบต้องแจ้ง ฝทส. เมื่อมีอุปกรณ์เครือข่ายหรือเครื่องแม่ข่ายของระบบงานใหม่มาติดตั้ง

5. การเปลี่ยนแปลง Source Code

5.1. สำหรับ Source Code ที่ใช้งานจริงต้องมั่นใจว่า Source Code ทั้งหมดมีการจัดเก็บไว้ในที่เดียวกัน ซึ่งการเปลี่ยนแปลงจะต้องได้รับอนุมัติให้ทำการแก้ไขแล้วเท่านั้น เมื่อมีการแก้ไขโปรแกรมจะมีการนำเอา Source Code จากที่จัดเก็บไปทำการแก้ไข การเปลี่ยนแปลงแก้ไข Source Code ที่ใช้งานจริงต้องมีการควบคุม Version ของ Source Code อย่างเคร่งครัด

5.2. ผู้ทำหน้าที่ในการเปลี่ยนแปลงแก้ไขต้องถูกจำกัดสิทธิในการเข้าถึงส่วนระบบงานที่ใช้จริงผู้ทำการแก้ไขจะได้รับอนุญาตให้ทำการคัดสำเนา Source Code เพื่อใช้ในการแก้ไขพัฒนาโปรแกรมในส่วนที่ใช้สำหรับการพัฒนาระบบงาน และทำการย้ายโปรแกรมที่แก้ไขเสร็จเข้าสู่ส่วนที่ใช้สำหรับโอนย้ายโปรแกรมก่อนการย้ายเข้าส่วนที่ใช้งานจริงเท่านั้น

5.3. กรณีการแก้ไขซอสโค้ดของระบบงานที่มีการเชื่อมต่อออนไลน์จะต้องผ่านการทดสอบความมั่นคงปลอดภัยของซอสโค้ด และมีหลักฐานการตรวจสอบความมั่นคงปลอดภัยและจะต้องไม่มีช่องโหว่ระดับความเสี่ยงสูง (Critical Risk) หรือมีหลักฐานแสดงว่าได้ดำเนินการแก้ไขแล้วจึงสามารถเปิดใช้งานได้

6. การควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ (Restrictions on Changes to Software Packages)

ผู้ดูแลระบบหรือหน่วยงานที่ดูแลระบบต้องจัดให้มีการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจที่จัดซื้อ โดยมีแนวทางปฏิบัติดังนี้

6.1. หลีกเลี่ยงการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจ

6.2. ในกรณีที่หลีกเลี่ยงไม่ได้ในการเปลี่ยนแปลงแก้ไข ให้ขออนุญาตเจ้าของลิขสิทธิ์เพื่อเปลี่ยนแปลงแก้ไขหรือมอบให้ผู้ขายดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์แพ็กเกจให้

6.3. ในการเปลี่ยนแปลงซอฟต์แวร์แพ็กเกจ ให้ฝ่ายที่รับผิดชอบเก็บตัวซอฟต์แวร์ต้นฉบับไว้อีกชุดหนึ่ง

6.4. ตัวซอฟต์แวร์แพ็กเกจที่แก้ไขจะต้องได้รับการตรวจสอบเป็นอย่างดีว่าจะไม่มีผลกระทบต่อระบบ

6.5. กรณีมีการ Update Patch หรือมีการแก้ไขช่องโหว่ของซอฟต์แวร์แพ็กเกจ จะต้องทำการทดสอบผลกระทบจากการ Update Patch ดังกล่าวก่อนจะนำไปใช้งานกับระบบงานจริง

7. การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

หน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยงและหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ร่วมกันกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว ซึ่งมีแนวทางปฏิบัติดังต่อไปนี้

7.1. ต้องกำหนดหน้าที่ความรับผิดชอบที่ชัดเจน ได้แก่ การเฝ้าระวังภัยคุกคาม การประเมินความเสี่ยงของภัยคุกคาม การ Patch ปิดช่องโหว่ในระบบ การตรวจสอบสินทรัพย์ที่ได้จัดหมวดหมู่ไว้ เป็นต้น

7.2. เจ้าของระบบงานต้องวิเคราะห์ความเสี่ยง และประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาดที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศทุก 12 เดือน

7.3. ในกรณีที่จะทำการ Update Patch ของระบบสำคัญ ๆ จะต้องดำเนินการสำรองข้อมูล Source Code และจัดเก็บค่าคอนฟิค (Config) ของระบบ รวมทั้งต้องมีการทดสอบและประเมินก่อนว่าจะไม่ก่อให้เกิดความเสียหายต่อระบบ แต่ถ้าไม่สามารถ Update Patch ได้ ก็ให้พิจารณาดังต่อไปนี้

7.3.1.ปิด Service หรือการทำงานที่เกี่ยวข้องกับช่องโหว่ ในกรณีที่ Service ดังกล่าวส่งผลกระทบร้ายแรงต่อระบบเครือข่ายคอมพิวเตอร์หรือระบบงานคอมพิวเตอร์อื่น ๆ

7.3.2.ปรับปรุงหรือเพิ่มระดับ Security ในการเข้าถึงที่บริเวณรอบนอกเครือข่าย ได้แก่ เพิ่ม Firewall หรือ IPS (Intrusion Prevention System) เป็นต้น

7.3.3.เพิ่มการเฝ้าระวัง เพื่อตรวจจับหรือป้องกันการโจมตีเครือข่าย

7.3.4.สร้างความตระหนักเกี่ยวกับช่องโหว่ที่เกิดขึ้น

7.3.5.เก็บ Log ของเหตุการณ์ที่เกิดขึ้นทั้งหมดเพื่อใช้ในการตรวจสอบ

7.3.6.กระบวนการบริหารจัดการช่องโหว่ที่มีดำเนินการ ได้แก่ การเฝ้าระวัง ต้องมั่นใจว่ามีประสิทธิภาพและประสิทธิผล

7.3.7.ระบบที่มีความเสี่ยงสูงจะต้องมีการเตรียมการเป็นอันดับแรกตามลำดับความสำคัญ

8. แนวทางปฏิบัติของการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (โดยผู้ใช้งาน)

8.1. ผู้ร้องขอจะต้องกรอกรายละเอียดลงในแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form by User) โดยผ่านการอนุมัติจากผู้บังคับบัญชา และ/หรือ Process Owner ส่งแบบคำขอฯ ไปยังหน่วยงานผู้ดูแลระบบ

8.2. ในกรณีเร่งด่วน อนุโลมให้ผู้ร้องขอส่งแบบคำขอการเพิ่มความต้องการ/การเปลี่ยนแปลงระบบ (Change Request Form by User) ทางอีเมล์ก่อนการส่งต้นฉบับ

8.3. หน่วยงานผู้ดูแลระบบ พิจารณาตามคำขอโดยศึกษา วิเคราะห์ ผลกระทบจากการแก้ไขแนวทางในการกลับคืนสู่สภาพเดิม (Recovery) กำหนดแนวทางการดำเนินงาน ระยะเวลาและผู้ดำเนินการแก้ไข ได้แก่ ผู้วิเคราะห์ ผู้จัดทำหรือปรับปรุงโปรแกรม ผู้ทดสอบระบบ เป็นต้น

8.4. หน่วยงานผู้ดูแลระบบ แจ้งผลการวิเคราะห์กลับไปยังผู้อนุมัติแบบคำขอฯ เพื่อรับทราบ และ/หรือยืนยัน พร้อมให้แจ้งรายชื่อผู้ดำเนินการทำ User Acceptance Test (UAT) ในกรณีที่หน่วยงานผู้ดูแลระบบเป็นผู้ร้องขอ ที่มีผลกระทบต่อระบบโดยรวม ได้แก่ การเปลี่ยนแปลงเวอร์ชั่นโปรแกรม การแก้ไขระบบเครื่อง Server อุปกรณ์เครือข่าย ฯลฯ จะต้องมีการทดสอบยอมรับระบบ (UAT) ก่อนนำไปในระบบใช้งานจริงเสมอ โดยหน่วยงานผู้ดูแลระบบแจ้งหน่วยงานที่เกี่ยวข้องทราบ เพื่อร่วมดำเนินการทำ UAT ต่อไป

8.5. หน่วยงานผู้ดูแลระบบต้องดำเนินการให้ผู้ร้องขอ และ/หรือผู้ใช้งานที่เกี่ยวข้องทำการทดสอบยอมรับระบบ (UAT) พร้อมลงนาม

8.6. หน่วยงานผู้ดูแลระบบต้องดำเนินการ ให้ผู้ร้องขอ และ/หรือ ผู้รับผิดชอบดูแลข้อมูล (Data Owner) ดำเนินการแปลงข้อมูล (Data Conversion) (ถ้ามี) โดยผู้รับผิดชอบดูแลข้อมูล (Data Owner) ต้องจัดเตรียม ตรวจสอบ รับรองความถูกต้องของข้อมูลทั้งก่อนและหลังนำเข้าระบบ

8.7. หลังจากผ่านการทดสอบการยอมรับระบบ หน่วยงานผู้ดูแลระบบ จะต้องจัดทำคู่มือระบบงาน (Systems Manual) และ/หรือ จัดการอบรมการใช้งาน/จัดทำคู่มือการใช้งาน (User/Operation Manual) ให้กับผู้ใช้งาน

8.8. หน่วยงานผู้ดูแลระบบ แจ้งผู้เกี่ยวข้องนำส่วนที่เปลี่ยนแปลงแก้ไขเข้าสู่ระบบใช้งานจริง (Production)

8.9. Process Owner และหน่วยงานผู้ดูแลระบบติดตามตรวจสอบ (Monitor and Track Error) ว่าระบบสามารถทำงานได้ถูกต้องตามวัตถุประสงค์ภายในระยะเวลาที่เหมาะสม

8.10. เมื่อได้ดำเนินงานแล้ว หน่วยงานผู้ดูแลระบบต้องจัดเก็บเอกสารที่เกี่ยวข้อง ได้แก่ แบบคำขอฯ แนวทางการดำเนินงาน รายละเอียดการดำเนินงาน เอกสารการทดสอบ คู่มือ ฯลฯ ให้สามารถใช้อ้างอิงได้

9. แนวทางปฏิบัติของการเปลี่ยนแปลง/แก้ไขระบบ (โดยผู้ดูแลระบบ)

9.1. ผู้ดูแลระบบ กรอกรายละเอียดลงในแบบฟอร์มการเปลี่ยนแปลง/แก้ไขระบบเครือข่าย (Change Request Form by Admin) โดยผ่านการอนุมัติจากผู้บังคับบัญชา

9.2. ผู้ดูแลระบบ ต้องระบุรายละเอียดในการเปลี่ยนแปลง/แก้ไขระบบเครือข่ายอย่างชัดเจน ได้แก่ วันเวลาที่แจ้ง รายละเอียดของผู้ดูแลระบบ สถานที่ปฏิบัติงานแก้ปัญหา วิธีการแจ้ง ปัญหา/สาเหตุการแก้ไข รายละเอียดของการปฏิบัติงาน ระยะเวลาในการแก้ไข ระบบที่ได้รับผลกระทบ

9.3. ผู้ดำเนินการแก้ไขต้องมีการเตรียมแผนสำรองฉุกเฉิน ในกรณีที่การเปลี่ยนแปลง/แก้ไขระบบเครือข่ายนั้นเกิดปัญหา เมื่อเกิดการล้มเหลวในการเปลี่ยนแปลง/แก้ไขระบบเครือข่าย ผู้ดำเนินการแก้ไขจะต้องสามารถเปลี่ยนกลับมาใช้ระบบเดิมได้ตามปกติ

9.4. เมื่อได้ดำเนินงานแล้ว ผู้ดำเนินการแก้ไขต้องลงนามและจัดเก็บเอกสารที่เกี่ยวข้อง ได้แก่ แบบฟอร์มฯ ที่ผู้แจ้งปัญหาหรือผู้ดูแลระบบแจ้งมา เอกสารหรือรายละเอียดของระบบทั้งก่อนและหลังการแก้ไข เป็นต้น เพื่อให้สามารถใช้อ้างอิงได้

หมวด 9
การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด
(Information Security Incident Management)

จุดประสงค์ เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ สทอภ. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของ สทอภ. โดยมีนโยบายดังนี้

นโยบายการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด
(Information Security Incident Management Policy)

1. วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของ สทอภ. ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และให้มีวิธีการที่สอดคล้องและได้ผล ในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของ สทอภ.

2. การตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่นอกเหนือจากการควบคุมและการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟท์แวร์ (Responding to Security Incidents and Malfunctions)

เพื่อลดความเสียหายจากเหตุการณ์ละเมิดความมั่นคงปลอดภัยและการทำงานของระบบที่บกพร่อง ได้แก่ ไวรัสคอมพิวเตอร์แพร่กระจาย ระบบถูกบุกรุกภัยคุกคามทางไซเบอร์ เป็นต้น โดยให้ดำเนินการดังนี้

2.1. “ผู้ใช้งาน” ต้องรายงานเหตุการณ์ต่าง ๆ ที่เกิดขึ้นให้แก่ผู้รับผิดชอบหรือผู้ดูแลระบบทราบ โดยเร่งด่วน ดังนี้

2.1.1. รายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events)

2.1.2. รายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

2.1.3. รายงานการทำงานที่บกพร่องหรือทำงานผิดปกติของซอฟต์แวร์ (Reporting Software Malfunctions)

2.2. ในกรณีที่ไม่สามารถติดต่อ “ผู้ดูแลระบบ” ได้ในขณะนั้นให้รายงานกับผู้บังคับบัญชา ตามลำดับขั้น และรายงานให้หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ทราบด้วย

2.3. “ผู้ดูแลระบบ” ร่วมกับ “หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ” ต้องประเมินขอบเขต (Scope) และความรุนแรง (Severity) ของปัญหา โดยหากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้าง รุนแรง หรือมีผลต่อชื่อเสียงของ สทอภ. จะต้องรายงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบโดยด่วน เพื่อหาแนวทางแก้ไขและป้องกันไม่ให้เกิดเหตุการณ์ดังกล่าวในครั้งต่อไป

2.4. ในกรณีที่ความเสียหายจากเหตุการณ์ละเมิดความมั่นคงปลอดภัย เกิดขึ้นกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของ สทอภ. และมีเหตุสงสัยว่าเป็นภัยคุกคามทางไซเบอร์ ให้ดำเนินการตามขั้นตอนการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือแผนรับมือภัยคุกคามทางไซเบอร์ ของ สทอภ.

3. การบริหารจัดการและการปรับปรุงแก้ไขต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่นอกเหนือจากการควบคุม (Management of Information Security Incidents and Improvements)

เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่นอกเหนือจากการควบคุม ต้องยึดหลักปฏิบัติดังต่อไปนี้

3.1. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures) ผู้บังคับบัญชาที่มีระบบงานสารสนเทศอยู่ในความดูแล ต้องมีการกำหนดหน้าที่ความรับผิดชอบและกำหนดขั้นตอนปฏิบัติ เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่นอกเหนือจากการควบคุม และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

3.2. การเรียนรู้จากสถานการณ์ด้านความมั่นคงปลอดภัยที่นอกเหนือจากการควบคุม (Learning from Security Incidents)

3.2.1.“ผู้ดูแลระบบ” ต้องบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย จุดอ่อน ช่องโหว่ ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

3.2.2.“ผู้ดูแลระบบ” มีหน้าที่จัดทำสรุปรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัยให้ผู้บังคับบัญชาและหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ อย่างน้อยเดือนละ 1 ครั้ง

3.2.3.หน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ และหน่วยงานดูแลรับผิดชอบด้านบริหารความเสี่ยง ต้องร่วมกันวิเคราะห์ความเสี่ยงและประเมินสถานการณ์การบุกรุก/ละเมิด/ระบาด ที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศทุก 12 เดือน

3.3. การเก็บรวบรวมหลักฐาน (Collection of Evidence)

3.3.1.หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบองค์กร และกฎหมาย (ระยะเวลา 90 วัน หรือ 1 ปี เป็นต้น)

3.3.2.หน่วยงานที่มีระบบงานสารสนเทศที่สำคัญต้องศึกษาถึงลักษณะของหลักฐานที่มีความสมบูรณ์และมีคุณภาพ เพื่อสามารถนำไปใช้ในกระบวนการของศาลได้

4. การรายงานเหตุการณ์น่าสงสัย

4.1. “ผู้ใช้งาน” มีหน้าที่รับผิดชอบในการรายงานเหตุการณ์ทันทีที่สงสัยว่าเป็นเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล

4.2. ถ้าหากพบเหตุการณ์ที่น่าสงสัยให้ทำการรายงานต่อผู้ดูแลระบบ หรือผู้บังคับบัญชาทันที ได้แก่เหตุการณ์ต่อไปนี้

4.2.1.พบว่ารหัสผ่านส่วนบุคคลของตนถูกล็อค โดยไม่ทราบสาเหตุ

4.2.2.เวลาการเข้าใช้งานระบบครั้งล่าสุด (Last Logon Time) ที่ผิดปกติ

4.2.3.พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน ได้แก่ มีไฟล์ที่ไม่รู้จัก การเปลี่ยนแปลงของค่าต่าง ๆ

4.2.4.มีการไม่ปฏิบัติตามขั้นตอนความมั่นคงปลอดภัย

4.2.5.พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล

4.2.6.พบหรือคาดว่าข้อมูลในระบบจะถูกทำลาย แก้ไข หรือลบทิ้ง

4.2.7.มีความพยายามที่จะเข้าใช้อย่างระบบอย่างผิดวิธี ไม่ว่าจะสำเร็จหรือไม่

4.2.8.การให้บริการของระบบเกิดการชะงัก หรือไม่สามารถให้บริการ

4.2.9.เกิดการละเมิดสิทธิเข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล

4.2.10. การแก้ไขค่าความปลอดภัยในระบบได้แก่ Hardware, Software หรือ Firmware โดยผู้ใช้งานไม่ทราบ

หมวด 10
การบริหารความต่อเนื่องในการดำเนินงาน
(Government Continuity Management)

จุดประสงค์ เพื่อป้องกันการติดขัดหรือหยุดชะงักของกิจกรรมต่าง ๆ ป้องกันกระบวนการปฏิบัติงานที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม โดยมีนโยบายดังนี้

นโยบายแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ
(IT Contingency Plan Policy)

1. วัตถุประสงค์

ข้อมูลเป็นสินทรัพย์ที่สำคัญที่สุด ต้องจะทำการสำรองข้อมูลและเก็บรักษาข้อมูลของระบบสารสนเทศที่สำคัญต่อการปฏิบัติงานของ สทอภ. ไว้ พร้อมทั้งทำการกู้คืนข้อมูลเพื่อให้การปฏิบัติงานของ สทอภ. เป็นไปอย่างต่อเนื่อง นโยบายนี้เป็นส่วนหนึ่งของการสนับสนุนแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ และหน่วยงานที่รับผิดชอบระบบและข้อมูลจะต้องปฏิบัติอย่างเคร่งครัด เพื่อทำให้การปฏิบัติงานของ สทอภ. เป็นไปอย่างมีประสิทธิภาพ ประสิทธิผล และอย่างต่อเนื่อง

2. คำแถลงนโยบาย

2.1. ขั้นตอนเตรียมการของแผนรองรับเหตุการณ์ฉุกเฉิน

2.1.1.สทอภ. ต้องจัดตั้งคณะทำงานแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงานเจ้าของข้อมูล เจ้าของระบบงาน หน่วยงานที่ดูแลระบบเครือข่าย เป็นต้น

2.1.2.คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ที่เป็นลายลักษณ์อักษร และปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละหนึ่งครั้ง

2.1.3.กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ต้องประกอบด้วยหัวข้อหลัก ดังนี้

- การวิเคราะห์ผลกระทบของปฏิบัติงาน (Impact Analysis)
- ประเมินความเสี่ยงและการควบคุม (Risk Analysis &Control)
- การวางกลยุทธ์สำหรับแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ (IT Contingency Plan Strategy Development)
- การพัฒนาแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ (IT Contingency Plan Development)
- การประชาสัมพันธ์แผนรองรับเหตุการณ์ฉุกเฉินและการฝึกอบรม
- การทดสอบ ปรับปรุงแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

2.1.4.แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ต้องพิจารณา ดังนี้

- การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการปฏิบัติงานและการให้บริการของ สทอภ.

- การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย ได้แก่กำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
- การดำเนินการเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง ได้แก่ การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
- การกลับคืนสู่การทำงานปกติเพื่อให้งานของ สทอภ. กลับสู่สภาวะปกติ ได้แก่ การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

2.2. แนวทางปฏิบัติของการสำรองข้อมูลและการกู้คืนข้อมูล

2.2.1. เจ้าของข้อมูลต้องตรวจสอบว่าข้อมูลสำคัญทั้งหมดที่เกี่ยวข้องกับปฏิบัติงานของ สทอภ. ได้มีการสำรองข้อมูลอย่างสม่ำเสมอและต่อเนื่องตามแนวทางปฏิบัติของ สทอภ. เจ้าของข้อมูลแต่ละระบบจึงมีหน้าที่ที่จะต้องประสานงานกับหน่วยงานดูแลข้อมูลที่เกี่ยวข้องเพื่อให้แน่ใจได้ว่าข้อมูลและฐานข้อมูลได้มีการสำรองข้อมูลเอาไว้อย่างครบถ้วนและเตรียมพร้อมเพื่อนำกลับมาใช้เมื่อเกิดเหตุการณ์ฉุกเฉิน

2.2.2. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของสำนักงาน ซึ่งได้จากการวิเคราะห์ผลกระทบเชิงธุรกิจ (Business Impact Analysis: BIA)

2.2.3. หน่วยงานที่รับผิดชอบการสำรองข้อมูล ต้องทำการทดลองนำเอาสื่อที่สำรองข้อมูลไว้มาทดสอบอย่างน้อยปีละครั้ง เพื่อให้มั่นใจได้ว่าสามารถนำข้อมูลกลับมาใช้ได้อีกเมื่อเกิดเหตุการณ์ฉุกเฉิน

2.2.4. การทดสอบการนำข้อมูลกลับมาใช้นั้นให้ใช้ข้อมูลสำรองที่ได้จากของระบบงานจริงและกระทำบนระบบสำหรับการทดสอบเท่านั้น

2.3. แนวทางปฏิบัติของการเก็บรักษาข้อมูลและสารสนเทศ

2.3.1. เจ้าของข้อมูลเป็นผู้จัดเก็บรักษาข้อมูลเกี่ยวกับระบบ ซึ่งได้แก่ ข้อมูลเกี่ยวกับระบบปฏิบัติการ (OS) ระบบเครือข่าย และซอฟต์แวร์ระบบงาน (ทั้ง Source Code และ Executable Files) โดยให้เป็นไปตามความต้องการที่เจ้าของข้อมูลในระบบนั้นกำหนด จำนวนครั้งและระยะเวลาในการเก็บรักษาข้อมูลดังกล่าวต้องสอดคล้องกับการประเมินความเสี่ยงของข้อมูลนั้น ๆ ด้วย

2.3.2. ก่อนที่จะมีการปรับปรุงหรือเปลี่ยนแปลงระบบ หน่วยงานที่รับผิดชอบต้องทำการ สำรองข้อมูลของระบบทุกครั้ง

2.3.3. ถ้าการสำรองข้อมูลถูกดำเนินการที่เซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์หลัก (Host) และเป็นข้อมูลของระบบงานที่สำคัญจะต้องเพิ่มจำนวนครั้งในการสำรองข้อมูลของเซิร์ฟเวอร์นั้นด้วย

2.3.4. ข้อมูลและสารสนเทศที่มีความสำคัญมากต่อการปฏิบัติงานของ สทอภ. จะต้องทำการสำรองข้อมูลไว้ทุกวัน และข้อมูลสำรองดังกล่าวต้องมีการจัดเก็บไว้นอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลักอย่างเหมาะสม โดยตรวจสอบให้แน่ใจว่าสถานที่นั้นมีความปลอดภัย

2.3.5. ระบบข้อมูลที่สำคัญทั้งหมดของ สทอภ. ต้องมีระบบการประมวลผลสำรองระบบเครือข่ายสำรอง เพื่อป้องกันการพึ่งพาระบบหลักเพียงระบบเดียว ในกรณีที่ระบบหนึ่งไม่สามารถทำงานได้สามารถใช้งานอีกระบบหนึ่งได้ทันทีเพื่อให้งานหลักของ สทอภ. ดำเนินต่อไปได้

2.3.6. ข้อมูลและสารสนเทศที่ถูกจัดประเภทเป็นข้อมูลธรรมดา ซึ่งไม่ส่งผลกระทบต่อการดำเนินกิจการของ สทอภ. จำนวนครั้งในการสำรองข้อมูลนั้นขึ้นอยู่กับการพิจารณาของเจ้าของข้อมูล และข้อมูลดังกล่าวจะถูกนำไปจัดเก็บในสถานที่ ๆ มีความปลอดภัย

ตัวอย่างโครงสร้างของแผนกู้คืนระบบสารสนเทศ

โครงสร้างของแผนกู้คืนระบบสารสนเทศนี้จัดทำขึ้นเพื่อให้หน่วยงานใน สทอภ. ใช้เป็นแนวทางในการจัดทำแผนกู้คืนระบบสารสนเทศที่มีประสิทธิภาพ เพื่อเตรียมรองรับเหตุการณ์และลดผลกระทบต่าง ๆ ที่อาจเกิดขึ้น รวมทั้งการฟื้นฟูระบบสารสนเทศของ สทอภ. ให้กลับคืนสู่สภาพปกติได้ภายในเวลาที่เหมาะสม ซึ่งทำให้ สทอภ. ดำเนินงานได้อย่างต่อเนื่องหรือได้รับผลกระทบน้อยที่สุดหลังจากเกิดเหตุการณ์หยุดชะงักหน่วยงานของ สทอภ. ต้องพิจารณาปรับใช้ให้เหมาะสมกับสถานการณ์ในปัจจุบันด้วย

โดยทั่วไป ตัวอย่างโครงสร้างของแผนกู้คืนระบบสารสนเทศต้องมีเนื้อหาครอบคลุมเรื่องต่าง ๆ ดังนี้

1. **ชื่อแผนกู้คืนระบบ.....** (ระบุชื่อแผน)
2. **วัตถุประสงค์ในการจัดทำแผนกู้คืน** ระบุวัตถุประสงค์ของแผน ความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นต่อ สทอภ. และหน่วยงานภายนอกที่เกี่ยวข้อง รวมทั้งผลลัพธ์ที่คาดหวังจากการนำแผนดังกล่าวมาใช้
3. **ขอบเขตของแผนกู้คืน** ระบุขอบเขตของระบบงาน รายละเอียดของกระบวนการทำงานและส่วนงานที่แผนดังกล่าวมีผลบังคับใช้ รวมทั้งรายละเอียดกระบวนการทำงาน (Work flow)
4. **รายละเอียดของระบบสารสนเทศ** ระบุชื่อ และโครงสร้างของระบบสารสนเทศ โครงสร้างระบบรักษาความปลอดภัย และการติดต่อสื่อสาร
5. **การกำหนดผู้รับผิดชอบสั่งการ** ระบุผู้มีอำนาจตัดสินใจ และสั่งการในการนำแผนมาปฏิบัติ โครงสร้างการบังคับบัญชา (ผู้สั่งการ และผู้รับผิดชอบ) บทบาทหน้าที่ และขอบเขตอำนาจความรับผิดชอบ รวมทั้งการกำหนดผู้รับผิดชอบแทนในกรณีที่ผู้สั่งการในลำดับแรกไม่สามารถปฏิบัติงานได้
6. **สถานที่ปฏิบัติงานทดแทน** ระบุสถานที่ที่ใช้ปฏิบัติงานแทนในกรณีเกิดภัยพิบัติจนเป็นเหตุให้ไม่สามารถใช้สถานที่ทำงานเดิมได้
7. **การบันทึกการเปลี่ยนแปลงของแผน** ระบุวันที่ ชื่อผู้จัดทำ หรือแก้ไขชื่อผู้ตรวจทาน และ รายละเอียดโดยย่อเมื่อมีการแก้ไขแผน
8. **กำหนดแผนการปฏิบัติงาน** ระบุสถานการณ์และเงื่อนไขในการปฏิบัติงานตามแผน รายละเอียด ขั้นตอน ทรัพยากรที่ใช้ และข้อจำกัดในการปฏิบัติโดยละเอียด ซึ่งต้องมีแนวปฏิบัติที่ครอบคลุมการ วางแผนที่สำคัญ 4 ด้าน ดังนี้

   8.1. การเตรียมความพร้อมก่อนเกิดเหตุการณ์ความเสียหาย การกำหนดกระบวนการป้องกันและควบคุมความเสี่ยง เพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย

   8.2. การตอบสนองต่อเหตุการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย รวมทั้งผลกระทบอื่น ในขณะที่มีเหตุการณ์ความเสียหายเกิดขึ้น โดยมีกระบวนการดังนี้

   8.2.1. *เงื่อนไขการเริ่มปฏิบัติตามแผน* กำหนดหรือระบุเงื่อนไขสถานการณ์

   8.2.2. *ระบุขั้นตอนการดำเนินการพื้นฐาน* ประเมินสถานการณ์เบื้องต้น สถานที่ สาเหตุ และขอบเขตความเสียหาย ระบุวิธีการปฏิบัติงานเพื่อระงับเหตุการณ์ความเสียหาย วิธีการดำเนินงานต่าง ๆ ที่เกี่ยวข้อง แนวทางการเก็บรักษาข้อมูลเอกสารความปลอดภัยของผู้ปฏิบัติงาน การเคลื่อนย้ายอพยพ “เจ้าหน้าที่” และทรัพยากรทางเทคโนโลยีสารสนเทศที่จำเป็น

   8.2.3. *ระบุแผนปฏิบัติการด้านการติดต่อสื่อสาร* กำหนดวิธีการติดต่อสื่อสารและประสานงานกับหน่วยงาน หรือบุคคลอื่นที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อแจ้งสถานการณ์ และแนวทางการดำเนินงาน หรือสถานที่ติดต่องานฉุกเฉิน รวมทั้ง จัดทำรายชื่อของหน่วยงาน หรือผู้ที่มีหน้าที่รับผิดชอบในการดำเนินการช่วยเหลือยุติเหตุการณ์ความเสียหายทั้งภายในและภายนอก สทอภ.

   8.2.4. *ระบุความต้องการใช้ทรัพยากรต่าง ๆ* ระบุความต้องการทรัพยากรที่มีความจำเป็น จำนวนแรงงาน สถานที่ ระบบการสื่อสารโทรคมนาคม สาธารณูปโภค อุปกรณ์ และเครื่องมือต่าง ๆ ให้ชัดเจน

8.3. การดำเนินการเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง เป็นแผนปฏิบัติการต่อเนื่อง จากแผนในข้อ 8.2 เพื่อให้ระบบเทคโนโลยีที่สนับสนุนการดำเนินงานของ สทอภ. มีความต่อเนื่องไม่หยุดชะงัก หรือสามารถกลับคืนมาในระยะเวลาการกู้คืนที่กำหนด และไม่ก่อให้เกิดผลกระทบต่อเนื่องอื่น ๆ โดยมีรายละเอียดดังนี้

8.3.1. *เงื่อนไขการเริ่มปฏิบัติตามแผน* กำหนด หรือระบุเงื่อนไข เหตุการณ์

8.3.2. *ระบุขั้นตอนการดำเนินการพื้นฐาน* กำหนดลำดับขั้นตอน ลำดับความสำคัญและระยะเวลาในการกู้ระบบ ระบุวิธีการปฏิบัติงาน วิธีการนำระบบข้อมูลสำรองมาใช้งานเพื่อให้เกิดการปฏิบัติงานต่อเนื่องได้โดยทันที

8.3.3. *ระบุแผนปฏิบัติการด้านการติดต่อสื่อสาร* กำหนดวิธีการติดต่อสื่อสารและ ประสานงานกับหน่วยงาน หรือบุคคลอื่นที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อแจ้งข้อเท็จจริง และแนวทางการดำเนินงาน หรือสถานที่ติดต่องานชั่วคราว

8.3.4. *ระบุความต้องการใช้ทรัพยากรต่าง ๆ* ระบุความต้องการทรัพยากรที่มีความจำเป็น หากมีการกู้ระบบที่ต้องใช้ระยะเวลานาน จำนวนแรงงาน สถานที่ปฏิบัติงานสำรอง ระบบการสื่อสารโทรคมนาคม สาธารณูปโภค อุปกรณ์และเครื่องมือต่าง ๆ

8.4. การกลับคืนสู่การทำงานปกติ เพื่อฟื้นฟูและจัดระบบงานให้กลับเข้าสู่การดำเนินงานตามปกติ รวมทั้งการสรุปประเมินความเสียหายที่เกิดขึ้น และแนวทางการป้องกันในอนาคตด้วย โดยมีรายละเอียดดังนี้

8.4.1. *ระบุขั้นตอนการดำเนินการ* ระบุวิธีการปฏิบัติงานเพื่อฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ กระบวนการควบคุมการติดตั้ง การตั้งค่าและทดสอบระบบที่ถูกกู้คืนมา หรือทดแทนใหม่ การรายงานสรุปความเสียหายต่อผู้บังคับบัญชา

8.4.2. *ระบุรายชื่อผู้ที่เกี่ยวข้อง* จัดทำรายชื่อของหน่วยงาน หรือผู้ที่มีหน้าที่รับผิดชอบทั้งจากภายในและภายนอก สทอภ. ในการดำเนินการช่วยเหลือเพื่อฟื้นฟูให้เหตุการณ์กลับสู่ภาวะปกติ

9. การประชาสัมพันธ์แผนรองรับเหตุการณ์ฉุกเฉินและการฝึกอบรม ระบุขั้นตอนและวิธีการประชาสัมพันธ์ให้แก่ “เจ้าหน้าที่” ของ สทอภ. และจัดฝึกอบรมให้แก่หน่วยงานและ “เจ้าหน้าที่” ผู้มีส่วนเกี่ยวข้องให้รับทราบถึงวัตถุประสงค์ ขั้นตอนการปฏิบัติงาน การประสานงาน การติดต่อสื่อสารระหว่างกลุ่ม ขั้นตอนการรายงาน ระบบรักษาความปลอดภัย และหน้าที่ความรับผิดชอบของตนเองตามแผนอย่างชัดเจน

10. การทดสอบ ปรับปรุงและสอบทานแผนฉุกเฉิน

10.1. การทดสอบ

10.1.1. กำหนดเวลาการทดสอบแผน กำหนดการทดสอบแผนกู้คืนที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้น จนสิ้นสุดกระบวนการทดสอบ

10.1.2. กำหนดเหตุการณ์จำลองที่จะใช้ทดสอบ และรายละเอียดในการกำหนดรายละเอียดของเหตุการณ์จำลอง ต้องระบุวัตถุประสงค์ ขอบเขตของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผน

10.1.3. กำหนดทรัพยากรต่าง ๆ ที่ใช้ในการทดสอบแผน กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุมประสานงาน และรับผิดชอบในการจัดการทดสอบแผนกู้คืน รวมถึงสถานที่และอุปกรณ์เครื่องมือต่าง ๆ และงบประมาณที่ต้องใช้ด้วย

10.1.4. กำหนดเกณฑ์การประเมินผล กำหนดผู้รับผิดชอบในการประเมินผล เกณฑ์การประเมินผลซึ่งอาจมีความแตกต่างกันไปตามลักษณะของระบบงาน กระบวนการทำงาน และวัตถุประสงค์ของการทดสอบในแต่ละครั้ง

10.2. การปรับปรุงและสอบทานแผน

10.2.1. กำหนดเวลาการทบทวนแผน กำหนดแผนงาน แนวทาง และระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

10.2.2. กำหนดผู้รับผิดชอบในการสอบทาน ต้องกำหนดผู้สอบทานแผน เพื่อยืนยันถึงความเหมาะสมของขั้นตอนต่าง ๆ ในการจัดทำแผน

10.2.3. มีการทบทวนแผนการปฏิบัติงานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ 1 ครั้ง

11. รายละเอียดเพิ่มเติม รายละเอียดอื่น ๆ ที่ต้องมีในแผนกู้คืนระบบสารสนเทศ มีดังนี้

11.1. รายชื่อ ที่อยู่ และหมายเลขโทรศัพท์ของ “เจ้าหน้าที่” ที่มีหน้าที่รับผิดชอบในการปฏิบัติตามแผน

11.2. รายชื่อหน่วยงาน สถานที่ตั้ง และหมายเลขโทรศัพท์ขององค์กรภายนอกที่เกี่ยวข้อง

11.3. รายละเอียดการปฏิบัติตามแผน (Checklist)

11.4. รูปแบบรายงานต่าง ๆ ที่จำเป็น

หมวด 11
การปฏิบัติตามข้อกำหนด
(Compliance)

จุดประสงค์ เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ และให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุด และมีการแทรกแซงหรือทำให้หยุดชะงักต่อปฏิบัติงานน้อยที่สุด โดยมีนโยบายดังนี้

นโยบายการปฏิบัติตามข้อกำหนดทางกฎหมาย
(Compliance with Legal Requirements Policy)

1. วัตถุประสงค์

เพื่อเป็นแนวทางในการปฏิบัติสำหรับการใช้งานซอฟต์แวร์ของ สทอภ. และของบุคคลที่สามซึ่งมีการนำมาใช้ภายใน สทอภ. รวมถึงเรื่องของการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมายและข้อกำหนดในการใช้ซอฟต์แวร์ของผู้ใช้งานและผู้ที่เกี่ยวข้องกับ สทอภ.

2. การระบุข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)

หน่วยงานดูแลรับผิดชอบด้านกฎหมาย ต้องระบุข้อกำหนดทางด้านกฎหมาย ระเบียบปฏิบัติ และสัญญาว่าจ้างรวมทั้งสัญญาที่ทำกับหน่วยงานภายนอก ที่เกี่ยวข้องกับการดำเนินงานหรือการปฏิบัติงานของ สทอภ. ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

3. การปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ในการใช้งานทรัพย์สินทางปัญญา (Compliance with Intellectual property rights (IPR))

3.1. การจัดซื้อและการนำซอฟต์แวร์ของบุคคลที่สามมาใช้ใน สทอภ. ต้องเป็นไปตามข้อตกลงเรื่องการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมาย (Licensing Agreement) ที่ได้ทำไว้กับเจ้าของลิขสิทธิ์

3.2. ผู้ที่ใช้ซอฟต์แวร์บนระบบสารสนเทศของ สทอภ. ต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

3.3. มีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับ ได้แก่ การลงทะเบียนเพื่อใช้งาน ซอฟต์แวร์และต้องเก็บหลักฐานแสดงความเป็นเจ้าของลิขสิทธิ์ มีการตรวจสอบอย่างสม่ำเสมอว่าซอฟต์แวร์ที่ติดตั้งมีลิขสิทธิ์ถูกต้อง

3.4. ซอฟต์แวร์ที่พัฒนาขึ้นโดย/หรือเพื่อ สทอภ. ถือเป็นสินทรัพย์ของ สทอภ. ซึ่งครอบคลุมถึง ซอฟต์แวร์หรือระบบงานที่พัฒนาโดยบุคคลภายนอกเพื่อให้กับ สทอภ. ทั้งนี้เพื่อเป็นการป้องกันข้อพิพาทในเรื่องกรรมสิทธิ์ของซอฟต์แวร์ที่อาจเกิดขึ้นหลังจากเสร็จสิ้นโครงการ

3.5. ซอฟต์แวร์ที่ถูกพัฒนาโดย “เจ้าหน้าที่ (Officer)” ของ สทอภ. ในระหว่างเวลาทำงานถือเป็นทรัพย์สินของ สทอภ.

3.6. เครื่องคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์แบบพกพา และเครื่องเซิร์ฟเวอร์ โดยผู้ใช้งานหรือเจ้าของระบบสารสนเทศ จะต้องตรวจสอบการใช้งานซอฟต์แวร์เป็นประจำว่าได้มีการปฏิบัติตามข้อตกลงเรื่องการอนุญาตให้ใช้ซอฟต์แวร์ตามกฎหมายซอฟต์แวร์ทั้งหมด

3.7. หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศและผู้ดูแลระบบ ต้องคอยตรวจสอบซอฟต์แวร์ถ้าหากพบว่ามีการละเมิดข้อตกลงจะต้องประสานงานกับเจ้าของระบบสารสนเทศเพื่อทำการยกเลิกการติดตั้งหรือลบทิ้ง

3.8. การ Download โปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆจาก Vendor ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

3.9. การติดตั้งซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์ระบบงาน (Operating System and Application Software) ต้องกระทำโดยเจ้าหน้าที่ของหน่วยงานที่ได้รับอนุญาตเท่านั้น ถ้ามีการติดตั้งซอฟต์แวร์ใด ๆ ในเครื่องคอมพิวเตอร์ของ สทอภ. โดยไม่ได้รับอนุญาต แล้วเกิดข้อพิพาทเกี่ยวกับกฎหมายลิขสิทธิ์และรายละเอียดข้อบังคับต่าง ๆ ของผู้ผลิตซอฟต์แวร์นั้น ๆ ทาง “สทอภ. จะไม่ขอรับผิดชอบไม่ว่ากรณีใด ๆ”

3.10. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของ สทอภ. เป็นโปรแกรมที่ สทอภ. ได้ซื้อลิขสิทธิ์มาถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

4. การป้องกันข้อมูลสำคัญของ สทอภ. (Protection of Organizational Records)

เพื่อเป็นการป้องกันข้อมูลสำคัญของ สทอภ. หน่วยงานต่าง ๆ ต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของ สทอภ. ได้แก่

- นโยบายความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
- นโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์
- นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
- นโยบายการแลกเปลี่ยนสารสนเทศ
- นโยบายการควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กรเป็นต้น

5. การป้องกันข้อมูลส่วนตัวและการเข้ารหัส มีแนวทางการปฏิบัติดังนี้

5.1. ผู้ดูแลระบบ ต้องจัดให้มีวิธีการป้องกันข้อมูลส่วนตัวของ “เจ้าหน้าที่” ได้แก่ ข้อมูลในจดหมายอิเล็กทรอนิกส์ข้อมูลในระบบบริหารงานบุคคล เป็นต้น เพื่อใช้เป็นหลักฐานอ้างอิงในทางกฎหมายในกรณีที่มีข้อพิพาทกัน

5.2. ผู้ดูแลระบบ ต้องศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายของประเทศ เกี่ยวกับการเข้ารหัสข้อมูล รวมทั้งเมื่อจำเป็นต้องโยกย้ายข้อมูลที่เข้ารหัสไว้ หรืออุปกรณ์หรือเครื่องมือ หรือระบบที่ใช้ในการเข้ารหัสข้อมูลไปยังอีกประเทศหนึ่งให้ศึกษาและปฏิบัติตามข้อกำหนดหรือกฎหมายของประเทศนั้นด้วย

6. การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of Misuse of Information Processing Facilities) มีแนวทางปฏิบัติดังนี้

6.1. อุปกรณ์ประมวลผลสารสนเทศของ สทอภ. มีไว้เพื่อใช้ในกิจการของ สทอภ. เท่านั้น ยกเว้นในกรณีที่ผู้ใช้งานได้รับอนุญาตเป็นกรณีเฉพาะจากผู้บริหาร สทอภ.

6.2. อุปกรณ์ประมวลผลสารสนเทศที่ สทอภ. เช่ามาใช้งานหน่วยงานที่เช่าจะต้องจัดทำบัญชีรายการของอุปกรณ์ประมวลผลสารสนเทศที่เช่ามาใช้งาน และให้ส่งสำเนาดังกล่าวให้หน่วยงานที่รับผิดชอบในการจัดการข้อมูลและสินทรัพย์ของ สทอภ.

6.3. ผู้บังคับบัญชาแต่ละหน่วยงาน ต้องกำหนดให้มีการป้องกันสินทรัพย์และอุปกรณ์ของ สทอภ. ได้แก่ Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน โดยต้องปฏิบัติตามระเบียบในการใช้งานการยืม-คืน

6.4. ต้องมีการปรับปรุงเอกสารหรือทะเบียนควบคุมอุปกรณ์ต่าง ๆ เมื่อมีการเปลี่ยนแปลง เพื่อใช้เป็นข้อมูลในการควบคุมทรัพย์สินของ สทอภ.

6.5. ผู้ใช้งานต้องไม่ทำการแก้ไขเปลี่ยนแปลง หรืออนุญาตให้ผู้ที่ไม่ได้รับอนุญาตทำการแก้ไข เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์ประมวลผลสารสนเทศในเครื่องที่ตนรับผิดชอบ

6.6. ไม่อนุญาตให้ผู้ใช้งานติดตั้งโปรแกรมหรืออุปกรณ์ในเครื่องของ สทอภ. การเปลี่ยนแปลงต่อระบบคอมพิวเตอร์ ฮาร์ดแวร์ อุปกรณ์ และสื่อที่ใช้ในการจัดเก็บข้อมูล จะต้องได้รับอนุมัติจากผู้บังคับบัญชาที่ดูแลระบบงานนั้น ๆ เป็นลายลักษณ์อักษร เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและการแก้ไขโดยไม่ได้ตั้งใจ ซึ่งอาจมีผลต่อการหยุดชะงัก หรือการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต

6.7. อุปกรณ์ประมวลผลสารสนเทศจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตามนโยบายการบริหารจัดการรหัสผ่าน (Password Management Policy)

6.8. อุปกรณ์ประมวลผลสารสนเทศที่ สทอภ. จัดซื้อ/จัดหา ต้องมีกระบวนการเพื่ออัพเดทระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ของ สทอภ.

7. การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of Cryptographic Controls)

หน่วยงานต่าง ๆ ซึ่งเป็นเจ้าของข้อมูล ต้องใช้มาตรการการเข้ารหัสข้อมูล (Cryptographic controls) ตามที่ได้กำหนดในนโยบายการพัฒนาระบบสารสนเทศ

8. การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)

ผู้บังคับบัญชาแต่ละหน่วยงาน ต้องกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยของ สทอภ.

9. การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical compliance checking)

เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคของ สทอภ. จึงต้องปฏิบัติตามแนวทางดังต่อไปนี้

9.1. ผู้ดูแลระบบต้องดูแลรักษา ตรวจสอบแก้ไข และเสนอ สทอภ. ให้ปรับปรุงระบบสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อให้ระบบสามารถใช้งานได้ดี มีเสถียรภาพ มีความมั่นคงปลอดภัย และมีประสิทธิภาพอยู่เสมอ

9.2. ผู้ดูแลระบบต้องขออนุญาตผู้บังคับบัญชาในกรณีที่มีการร่วมมือกับหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ในการประเมิน ตรวจสอบ ทดสอบ หาจุดอ่อน ช่องโหว่อันเกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศ และทำการแก้ไขอย่างรวดเร็ว

9.3. ผู้บังคับบัญชาแต่ละหน่วยงาน ต้องจัดให้มีการตรวจสอบบัญชีทรัพย์สินตามระยะเวลาที่กำหนดไว้ เพื่อตรวจสอบและแก้ไขปัญหาช่องโหว่ที่เกิดขึ้น

9.4. ในกรณีที่มีการเคลื่อนย้าย ผู้ที่รับผิดชอบในการย้ายสถานที่ทำงาน ต้องตรวจสอบความเรียบร้อยครั้งสุดท้ายทันทีหลังจากที่ทำการย้ายของเสร็จสิ้น รวมทั้งตรวจสอบพื้นที่และทรัพย์สินด้วยการย้ายสถานที่ทำงาน เป็นช่วงเวลาที่ต้องระวังเรื่องการรักษาความปลอดภัยที่อาจมีการมองข้ามได้โดยเฉพาะช่วงเวลาที่ต้องเร่งจัดการย้ายให้เสร็จสิ้น จึงต้องให้ความระมัดระวัง เพราะอาจมีการผ่อนปรนมาตรการรักษาความปลอดภัยต่อข้อมูลที่มีความสำคัญหรือต่อระบบเครือข่ายของ สทอภ. ได้

9.5. ผู้ใช้งานต้องมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบการ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอย่างสม่ำเสมอ และแจ้งให้ผู้ดูแลระบบทราบ หากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

9.6. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด ได้แก่ การตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส หลีกเลี่ยงในการเปิดไฟล์ที่เป็น Executable file ได้แก่ .EXE, .COM

9.7. ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่าง ๆ ได้แก่ Thump Drive หรือ SD Card ก่อน นำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ที่รับผิดชอบ

9.8. ต้องมีการตรวจสอบการใช้งานระบบ (Monitoring System Use) อย่างสม่ำเสมอ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศ โดยต้องมีการประเมินความเสี่ยงและปฏิบัติตามที่กฎหมายกำหนด

9.9. การเข้าสู่ระบบของ สทอภ. จากอินเทอร์เน็ต หรือการเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องตรวจสอบผู้ใช้งานจากสิ่งที่รู้อยู่ ได้แก่ รหัสผ่าน และเพื่อเพิ่มความปลอดภัยการพิสูจน์ตนต้องมีการใช้วิธีการเข้ารหัส (Cryptographic) ร่วมกับการควบคุม

9.10. ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอก สทอภ. หน่วยงานที่รับผิดชอบต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิที่ได้รับ และตรวจสอบการใช้งานอย่างสม่ำเสมอ

10. มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls) ผู้บังคับบัญชาที่ดูแลระบบงานสำคัญหรือระบบสารสนเทศที่มีข้อมูลความลับของ สทอภ. ได้แก่ ระบบบริหารทรัพยากรบุคคล ระบบบริหารงบประมาณ ฯลฯ เป็นต้น ต้องวางแผนการตรวจประเมินระบบทั้งหมด โดยการตรวจประเมินที่จะดำเนินการจะต้องมีผลกระทบต่อระบบและกระบวนการดำเนินงานของ สทอภ. น้อยที่สุด ดังนี้

<u>การประเมินความเสี่ยงด้านสารสนเทศ</u>

(1). ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Risk Assessment) อย่างน้อยปีละ 1 ครั้ง

(2). ตรวจสอบ ประเมิน และส่งผลการตรวจประเมินความเสี่ยงที่ดำเนินการโดย ผู้ตรวจสอบภายใน (internal Auditor)

<u>แนวทางในการบริหารจัดการความเสี่ยงที่ต้องพิจารณา</u>

(1) ต้องจัดทำรายงานในการบริหารจัดการความเสี่ยงพร้อมข้อเสนอแนะ

(2) ต้องทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ 1 ครั้ง

(3) ต้องทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

11. การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit tools)

หน่วยงานดูแลรับผิดชอบด้านตรวจสอบภายใน หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศและหน่วยงานดูแลรับผิดชอบความมั่นคงปลอดภัยระบบสารสนเทศและนโยบายฯ ต้องร่วมกันหาทางป้องกันซอฟต์แวร์ที่ใช้ในการตรวจประเมินระบบ มิให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิดหรือป้องกันข้อมูลสำคัญที่เป็นผลลัพธ์จากการตรวจสอบโดยซอฟต์แวร์นั้น ๆ

แนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

กรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework)

สทอภ. ดำเนินการตามกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่องประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ซึ่งสามารถสรุปกิจกรรมการดำเนินการต่าง ๆ ดังต่อไปนี้

รายละเอียดของแต่ละกิจกรรมมีดังนี้

- การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)
- มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)
- มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)
- มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
- มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

<u>กิจกรรมการระบุความเสี่ยง (Identify)</u>

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 4 ขั้นตอน ดังนี้

1. การจัดการทรัพย์สิน (Asset Management)
2. การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)
3. การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and PenetrationTesting)
4. การจัดการผู้ให้บริการภายนอก (Third Party Management)

1. การจัดการทรัพย์สิน (Asset Management)

1.1. สทอภ. ต้องจัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญและต้องทบทวนทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

1.1.1. ชื่อ/คำอธิบายของทรัพย์สินของบริการที่สำคัญ

1.1.2. ฟังก์ชันที่สำคัญของทรัพย์สินของบริการที่สำคัญ

1.1.3. การระบุและการจัดลำดับความสำคัญของทรัพย์สินของบริการที่สำคัญ

1.1.4. ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญ

1.2. สทอภ. ต้องมีการตรวจสอบและปรับปรุงทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ

1.3. สทอภ. ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ อย่างน้อยปีละ 1 ครั้ง

2. การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

2.1. สทอภ. ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด

2.2. สทอภ. ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

2.2.1.วันที่ระบุความเสี่ยง (Date the Risk is Identified)

2.2.2.คำอธิบายของความเสี่ยง (Description of the Risk)

2.2.3.โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

2.2.4.ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

2.2.5.การจัดการความเสี่ยง (Risk Treatment)

2.2.6.สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)

2.2.7.ความเสี่ยงที่เหลือ (Residual Risk)

3. การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

3.1. สทอภ. ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ อ้างอิงตามหลักการบริหารความเสี่ยง เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญเช่น ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)

3.2. สทอภ. ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย

3.2.1.การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

3.2.2.การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

3.2.3.การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture SecurityReview)

3.3. สทอภ. ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อหรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญการเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบและการปรับเปลี่ยนเทคโนโลยี เป็นต้น

3.4. สทอภ. ควรพิจารณาดำเนินการทดสอบเจาะระบบ (PenetrationTesting) บริการที่สำคัญโดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

3.5. สทอภ. ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ โดยเฉพาะอย่างยิ่งทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

3.6. สทอภ. ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้งตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

3.7. สทอภ. ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด

3.8. ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน

3.9. ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

3.10. หากได้รับการร้องขอจาก กกม.หรือสำนักงานต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานดังกล่าว ไปยังสำนักงานภายในกำหนด 30 วันนับแต่วันที่ได้รับหนังสือ

4. การจัดการผู้ใช้บริการภายนอก (Third Party Management)

4.1. ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของ สทอภ. แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญ

4.2. ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

4.2.1. ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญตามความต้องการทางธุรกิจขององค์กรและโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

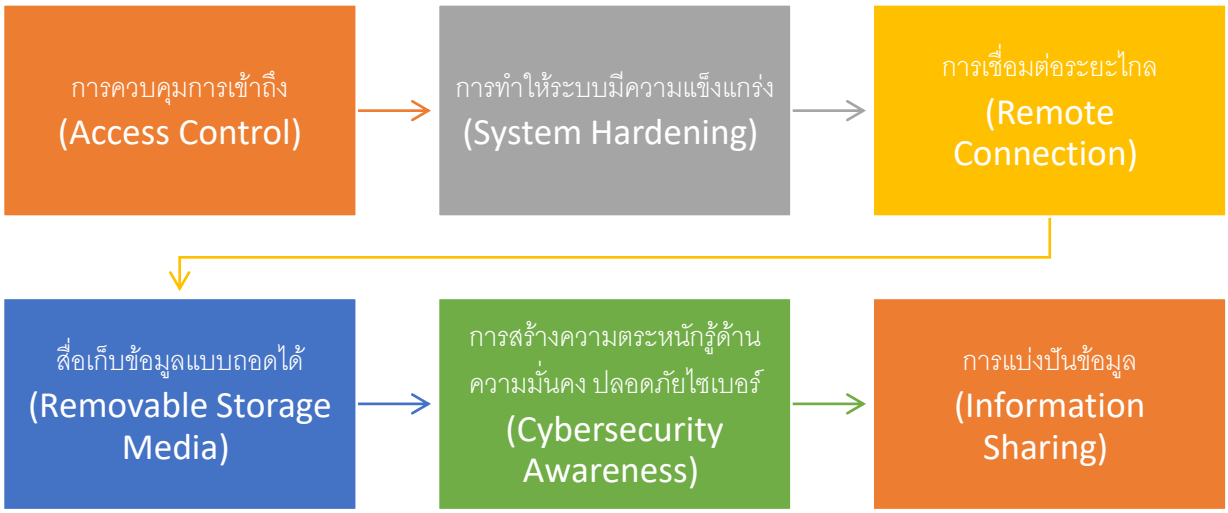
4.2.2. ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจากภัยคุกคามทางไซเบอร์

4.2.3. ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

4.2.4. สิทธิ์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

กิจกรรมการกำหนดมาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 6 ขั้นตอน ดังนี้



1. การควบคุมการเข้าถึง (Access Control)

1.1. ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของ สทอภ. จำกัดไว้ที่

1.1.1.บุคลากร และกิจกรรมที่ได้รับอนุญาต

1.1.2.อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

1.2. ในส่วนที่เกี่ยวกับภาระหน้าที่การตรวจสอบการเข้าถึงบริการที่สำคัญของ สทอภ. ต้องกำหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาต มีการใช้เทคนิคการตรวจสอบสิทธิ์ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ

1.3. ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของ สทอภ. และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

1.4. ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่นUSB พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดย

1.4.1.ทำภายใต้การดูแลของหน่วยงานเท่านั้น

1.4.2.ดำเนินการในสถานที่หากเป็นไปได้

2. การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

2.1. ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)

2.2. มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

2.2.1.สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

2.2.2.การแบ่งแยกหน้าที่ (Separation of Duties)

2.2.3.การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

2.2.4.การลบบัญชีที่ไม่ได้ใช้

2.2.5.การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

2.2.6.การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

2.2.7.การป้องกันมัลแวร์ (Malware)

2.2.8.การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

2.3. ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของ สทอภ.

2.3.1.ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของ สทอภ. อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

2.4. ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

3. การเชื่อมต่อระยะไกล (Remote Connection)

3.1. ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ สทอภ. มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

3.2. สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ สทอภ. ปฏิบัติตามแนวทางปฏิบัติ ดังต่อไปนี้

3.2.1.ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น

3.2.2.ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง

3.2.3.ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

3.2.4.ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ สทอภ. เว้นแต่จะได้รับ อนุญาตอย่างชัดเจนเนื่องจากความต้องการของ สทอภ.

3.2.5.จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

4. สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

4.1. ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญ สทอภ. โดยใช้มาตรการอย่างน้อย ดังนี้

4.1.1.ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับ สื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็น เท่านั้น

4.1.2.ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตจาก สทอภ. เท่านั้น

4.1.3.ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของ สทอภ.

4.2. ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของ สทอภ. บนสื่อบันทึกข้อมูลแบบถอดได้

5. การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

5.1. ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับเจ้าหน้าที่ ลูกจ้าง สทอภ ลูกจ้างโครงการ บริษัทคู่สัญญา Outsource และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

5.1.1.กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่

- พนักงานใหม่ (New Employees)
- ผู้ใช้และระดับบริหาร (Users and Management)
- เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT
- ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

5.1.2.การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของ สทอภ.

5.1.3.การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

5.1.4.การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ

5.1.5.ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

<u>กิจกรรมกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)</u>

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 1 ขั้นตอน ดังนี้

1. การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

1.1 ต้องสร้างกลไกและกระบวนการเพื่อ

1.1.1 ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของ สทอภ.

1.1.2 การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

1.1.3 การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ เกี่ยวข้องกับบริการที่สำคัญของ สทอภ. หรือไม่

1.2 ต้องดำเนินการทบทวนกลไกและกระบวนการอย่างน้อยปีละ 1 ครั้งเพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

<u>กิจกรรมการกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)</u>

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 3 ขั้นตอน ดังนี้

1. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

สทอภ. ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

2. แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

2.1. ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์

2.2. ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

2.2.1.จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

2.2.2.ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

2.2.3.ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

2.2.4.ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

2.2.5.ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดียสำหรับการเผยแพร่ข้อมูล)

2.3. ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

2.4. ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้งเพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

3. การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

3.1. สทอภ. ต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์หากได้รับคำสั่งเป็นลายลักษณ์อักษร การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าว อาจดำเนินการได้ทั้งในระดับชาติหรือระดับภาคส่วน สทอภ. ต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

3.2. ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ สทอภ. เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคาม ทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤต และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้อง กับการดำเนินงานของบริการที่สำคัญของ สทอภ.

<u>กิจกรรมการกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)</u>

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 1 ขั้นตอน ดังนี้

1. การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

1.1. ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (BusinessContinuityPlan:BCP) เพื่อให้แน่ใจว่า บริการที่สำคัญของ สทอภ. สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการ หยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอกเพื่อพิจารณาความสอดคล้อง กับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

1.2. ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

2. ขั้นตอนการปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Risk Assessment Procedure)

2.1. ขั้นตอนและหลักเกณฑ์การประเมินความเสี่ยง (Risk Assessment and Risk Criteria)

2.1.1.กำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite) เป็นระดับความเสี่ยงที่หน่วยงานยอมรับได้ เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจหรือภารกิจและช่วยประกอบการตัดสินใจในการบริหารความเสี่ยงของผู้บริหาร

Risk Level	Risk Tolerance Description
Very High	ระดับของความเสี่ยงที่ไม่สามารถยอมรับได้มีผลกระทบรุนแรง ส่งผลให้บริการที่สำคัญหยุดชะงัก จำเป็นต้องดำเนินการลดความเสี่ยง หรือถ่ายโอนความเสี่ยงในทันที
High	ระดับของความเสี่ยงที่ไม่สามารถยอมรับได้ จำเป็นต้องดำเนินการลดความเสี่ยงภายใน 1 เดือน
Medium High	ระดับของความเสี่ยงที่ไม่สามารถยอมรับได้ จำเป็นต้องดำเนินการลดความเสี่ยงภายใน 3-6 เดือน
Medium	ระดับของความเสี่ยงที่สามารถยอมรับได้ โดยมีมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย มีการตรวจสอบและเฝ้าระวังอย่างสม่ำเสมอ
Low	ระดับของความเสี่ยงที่สามารถยอมรับได้ โดยมีมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย มีการตรวจสอบและเฝ้าระวังเป็นระยะ

2.2. การประเมินความเสี่ยง (Risk Assessments)

เป็นกระบวนการที่ใช้สำหรับการประเมินความเสี่ยงที่สนใจหรือที่มีผลกระทบต่อกาบรรลุวัตถุประสงค์ ขององค์กร จนได้ระดับของความเสี่ยงในที่สุด โดยมี 3 ขั้นตอนหลัก ดังนี้

2.2.1.การระบุความเสี่ยง (Risk Identification) คือการระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงภัยคุกคามทางไซเบอร์ และช่องโหว่ที่สำคัญโดยเหตุการณ์ความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัย ภายนอก ตลอดจนการระบุการควบคุมที่มีอยู่ในปัจจุบันและผู้รับผิดชอบต่อความเสี่ยงหรือเจ้าของความเสี่ยง (Risk Owners) โดยสามารถระบุความเสี่ยงด้านไซเบอร์นั้นสามารถแบ่งได้เป็น 3 ขั้นตอน ดังนี้

2.2.1.1. ระบุทรัพย์สิน (Identify Asset) ระบุทรัพย์สินและบันทึกลงทะเบียนทรัพย์สิน (Inventory) โดยครอบคลุมถึงขอบเขต เครือข่ายของบริการที่สำคัญของ (Inventory) หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ

2.2.1.2. การระบุและการจัดลำดับความสำคัญของทรัพย์สินบริการที่สำคัญของหน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยการพิจารณาผลกระทบของการสูญเสียคุณลักษณะ C-I-A ของแต่ละด้าน เช่น การให้บริการ การเงิน ชื่อเสียง กฎหมาย เป็นต้น

2.2.2.การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)

2.2.2.1. การระบุขอบเขตของทรัพย์สินและบริการ (Scope Identification) ในทะเบียนทรัพย์สิน (Inventory)

2.2.2.2. การระบุภัยคุกคาม (Threat Identification) ระบุเหตุการณ์ภัยคุกคามที่มีความเป็นไปได้ที่ผู้ไม่หวังดีสามารถโจมตีหรือยึดครองบริการที่สำคัญได้

2.2.2.3. การสร้างแบบจำลองการโจมตี (Attack Modelling) หลังจากระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้วองค์กรต้องกำหนดลำดับการโจมตีที่มีความเป็นไปได้ว่าจะเกิดขึ้น โดยจำลองและอธิบายรูปแบบการโจมตีเพื่อหาแนวทางการป้องกัน

2.2.3.สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios) การสร้างสถานะการณ์ความเสี่ยงเป็นขั้นตอนสุดท้ายในการระบุความเสี่ยง โดยมีเป้าหมายเพื่อสร้างสถานการณ์ความเสี่ยงที่อาจทำให้เกิดความผิดพลาดในมุมมองที่สมจริงตามสภาพแวดล้อมของระบบและภัยคุกคามที่เกี่ยวข้องโดยสถานการณ์ความเสี่ยงประกอบด้วย

2.2.3.1. ทรัพย์สิน (Asset) รายการทรัพย์สินที่มีการกำหนดระดับความสำคัญ

2.2.3.2. เหตุการณ์ภัยคุกคาม (Threat event) การระบุเหตุการณ์ภัยคุกคามที่มีการโจมตีทรัพย์สินหรือบริการที่สำคัญ

2.2.3.3. จุดอ่อน (Vulnerability) จุดอ่อนของทรัพย์สินหรือจุดอ่อนของกระบวนการสนับสนุน ที่ภัยคุกคามสามารถใช้ประโยชน์ได้ โดยจุดอ่อนดังกล่าว อาจได้มาจากการทดสอบเจาะระบบ การตรวจสอบภายใน หรือจากสภาพแวดล้อมจากการเปลี่ยนแปลงเทคโนโลยี บางอย่าง

2.2.3.4. ผลที่ตามมา (Consequence) ผลจากเหตุการณ์ภัยคุกคาม

Threat Event | Vulnerability | Asset | Consequence

2.2.4.การวิเคราะห์ความเสี่ยง (Risk Analysis) เป็นการวิเคราะห์องค์ประกอบในแต่ละสถานการณ์ความเสี่ยง (Risk Scenarios) โดยพิจารณา

Likelihood: ความน่าจะเป็น (โอกาส) ที่เหตุการภัยคุกคามที่กำหนด จะใช้ประโยชน์จากจุดอ่อน หรือช่องโหว่

Impact: ระดับความรุนแรงของผลกระทบที่เกิดจากเหตุการณ์ภัยคุกคามใช้ประโยชน์จากจุดอ่อนหรือช่องโหว่ ซึ่งระดับความรุนแรงขึ้นอยู่กับว่าส่งผลกระทบกับบุคคล องค์กร หรือชาติ

2.2.4.1. การกำหนดโอกาส (Determine Likelihood)

โอกาสที่จะเกิดสถานการณ์ความเสี่ยงด้านไซเบอร์ ควรได้รับการประเมินจากภัยคุกคามและจุดอ่อน (threats and vulnerabilities) โดยพิจารณาจากปัจจัย ดังนี้

- Discoverability ผู้ไม่หวังดีสามารถค้นพบจุดอ่อนของทรัพย์สินได้ง่ายแค่ไหน
- Exploitability ผู้ไม่หวังดีสามารถใช้ประโยชน์จากจุดอ่อนของทรัพย์สินได้ง่ายแค่ไหน
- Reproducibility ผู้ไม่หวังดีสามารถโจมตีซ้ำทรัพย์สินได้ง่ายแค่ไหน

Likelihood Rating	Discoverability	Exploitability	Reproducibility
Highly Likely (5)	จุดอ่อนของทรัพย์สิน สามารถค้นพบได้จากการสแกน Public Domain สามารถค้นพบได้จากการสแกน Public Domain	การโจมตี สามารถทำได้โดยไม่มีสิทธิการเข้าถึงของเป้าหมาย สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยไม่มีต้องมีความรู้ด้านเทคนิคการโจมตี	การโจมตี สามารถทำซ้ำได้ตามต้องการโดยไม่มีการกำหนดค่าหรือเงื่อนไขเหตุการณ์ใด ๆ
Likely (4)	จุดอ่อนของทรัพย์สิน สามารถค้นพบได้จากการสแกน Port สามารถค้นพบและโจมตีจากเครือข่ายที่อยู่	การโจมตี สามารถทำได้โดยการจำกัดสิทธิการเข้าถึงของเป้าหมาย สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยมีความรู้ขั้นพื้นฐาน	การโจมตี สามารถทำซ้ำได้ตามต้องการโดยไม่มีการกำหนดค่าบางอย่างที่เป้าหมาย

Likelihood Rating	Discoverability	Exploitability	Reproducibility
	ใกล้เคียงหรือติดกัน (adjacent subnets or network segments)		สามารถทำซ้ำได้ด้วยการปรับแต่งช่องโหว่ที่เผยเล็กน้อย เช่น การเปลี่ยนพารามิเตอร์
Possible (3)	จุดอ่อนของทรัพย์สิน สามารถค้นพบได้จากโดยตรวจสอบกาตอบสนองพฤติกรรม และการสื่อสารของเป้าหมาย (network sniffing) สามารถค้นพบและโจมตีได้จากภายในเครือข่ายย่อยหรือเครือข่ายเดียวกัน	การโจมตี สามารถทำได้ด้วยการเข้าถึงโดยใช้สิทธิพิเศษของเป้าหมาย (admin/SYSTEM/root) สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยมีความรู้เทคนิคระดับปานกลาง	การโจมตี สามารถทำซ้ำได้โดยมีเงื่อนไขเหตุการณ์ที่คาดการณ์ได้ สามารถทำซ้ำได้ด้วยการปรับแต่งช่องโหว่เฉพาะสำหรับเป้าหมาย
Unlikely (2)	จุดอ่อนของทรัพย์สิน สามารถค้นพบได้โดยการใช้งาน สามารถค้นพบและโจมตีได้จากการเข้าถึงระบบแบบ Local	การโจมตี สามารถทำได้ด้วยการเข้าถึงโดยใช้สิทธิพิเศษของเป้าหมาย (admin/SYSTEM/root) สามารถทำได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ / เครื่องมือเฉพาะโดยมีความรู้เทคนิคระดับสูง สามารถเชื่อมโยงไปยังช่องโหว่ของระบบที่อยู่ใกล้เคียง	การโจมตี สามารถทำซ้ำได้โดยมีเงื่อนไขเหตุการณ์จากการสุ่ม สามารถทำซ้ำได้จากทฤษฎีหรือช่องโหว่ที่มีการพิสูจน์และเผยแพร่สู่สาธารณะ
Rare (1)	จุดอ่อนของทรัพย์สิน สามารถค้นพบได้โดยการอ่าน Source Code สามารถค้นพบและโจมตีได้จากการเข้าถึงด้านกายภาพ	การโจมตี สามารถทำได้ด้วยการเข้าถึง โดยใช้สิทธิพิเศษของเป้าหมาย (admin/SYSTEM/root) รวมถึง multi factor authentication สามารถทำได้ด้วยเครื่องมือเฉพาะ ที่ต้องใช้ความรู้ด้านเทคนิคจากผู้เชี่ยวชาญ สามารถเชื่อมโยงไปยังช่องโหว่ของระบบที่อยู่ใกล้เคียง	การโจมตี ไม่สามารถทำซ้ำได้

จากตาราง สามารถคำนวณคะแนนได้ตามขั้นตอน ดังนี้

- ให้ค่าคะแนนของแต่ละปัจจัย (Discoverability, Exploitability, Reproducibility)
- เฉลี่ยคะแนน โดยปัดเศษเป็นจำนวนเต็มคะแนนที่ปัดเศษแล้วจะเป็นโอกาสของสถานการณ์ความเสี่ยง

2.2.4.2. การกำหนดโอกาส (Determine Likelihood)

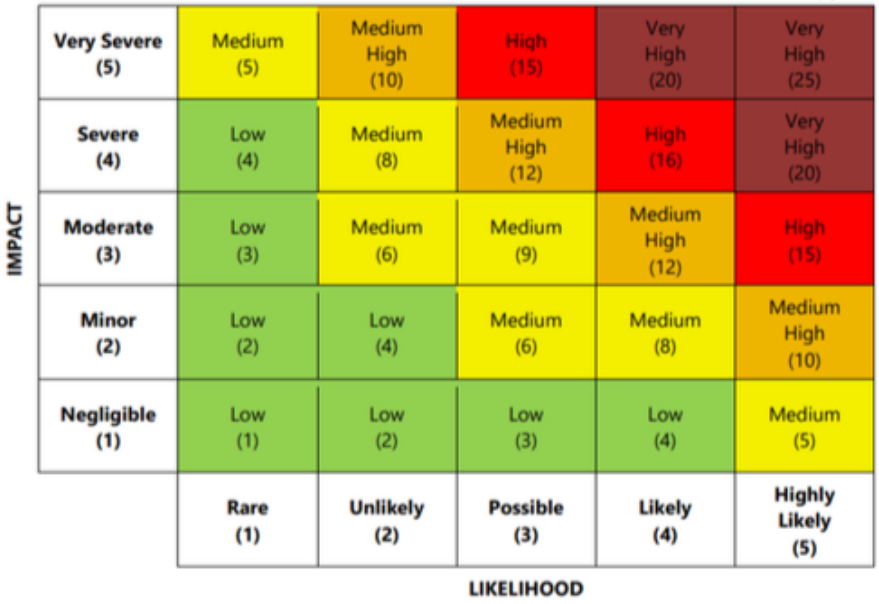
สถานการณ์ความเสี่ยงถูกพิจารณาจากการสูญเสีย C-I-A ของทรัพย์สิน โดยส่งผลกระทบ 3 ระดับ ดังนี้

- ชาติ (National) เป็นอันตรายต่อความมั่นคงของชาติและเศรษฐกิจ
- องค์กร (Organizational) การหยุดชะงักของการดำเนินธุรกิจ ความเสียหายต่อชื่อเสียงและความสูญเสียด้านการเงิน
- บุคคล (Individual) การสูญเสียชีวิตหรือได้รับบาดเจ็บ

Impact Rating	Confidentiality	Integrity	Availability
Very Severe (5)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจจะส่งผลกระทบอย่างร้ายแรงมากต่อองค์กร บุคคล หรือประเทศชาติ	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจจะส่งผลกระทบอย่างร้ายแรงมากต่อองค์กร บุคคล หรือประเทศชาติ	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์อาจส่งผลกระทบอย่างร้ายแรงมากต่อองค์กร บุคคล หรือประเทศชาติ
Severe (4)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจจะส่งผลกระทบอย่างร้ายแรงต่อองค์กร บุคคล หรือประเทศชาติ	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจจะส่งผลกระทบอย่างร้ายแรง ต่อองค์กร บุคคล หรือประเทศชาติ	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์อาจส่งผลกระทบอย่างร้ายแรงต่อองค์กร บุคคล หรือประเทศชาติ
Moderate (3)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจจะส่งผลกระทบปานกลางต่อองค์กร บุคคล หรือประเทศชาติ	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจจะส่งผลกระทบปานกลางต่อองค์กร บุคคล หรือประเทศชาติ	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์อาจส่งผลกระทบปานกลางต่อองค์กร บุคคล หรือประเทศชาติ
Minor (2)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจจะส่งผลกระทบอย่างจำกัดต่อองค์กรหรือบุคคล	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจจะส่งผลกระทบอย่างจำกัดต่อองค์กรหรือบุคคล	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์อาจส่งผลกระทบอย่างจำกัดต่อองค์กรหรือบุคคล
Negligible (1)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจจะส่งผลกระทบเล็กน้อยต่อองค์กรหรือบุคคล	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจจะส่งผลกระทบเล็กน้อยต่อองค์กรหรือบุคคล	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลหรือระบบคอมพิวเตอร์อาจส่งผลกระทบเล็กน้อยต่อองค์กรหรือบุคคล

2.2.5.การประเมินค่าความเสี่ยง (Risk Evaluation)

เป็นการพิจารณาค่าระดับของสถานการความเสี่ยงดังตารางต่อไปนี้



2.3. การจัดการความเสี่ยง (Risk Treatment)

เมื่อทราบผลการประเมินความเสี่ยง และพบว่าค่าความเสี่ยงกว่าระดับความเสี่ยงหน่วยงานยอมรับได้ ให้เจ้าของทรัพย์สินดังกล่าว หน่วยงานต้องดำเนินการดังนี้

2.3.1.การเลือกแนวทางการจัดการความเสี่ยง (Selection of risk treatment option) พิจารณาแนวทางในการจัดการความเสี่ยงมี 4 แนวทาง ได้แก่

2.3.1.1. การยอมรับความเสี่ยง (Accept Risk) การรับความเสี่ยงโดยไม่ต้องดำเนินการใด ๆ เพื่อเพิ่มเติมเพื่อลดความเสี่ยง ซึ่งอยู่ในระดับที่องค์กรยอมรับได้

2.3.1.2. การหลีกเลี่ยงความเสี่ยง (Avoid Risk) การยุติการดำเนินการ/กิจกรรมที่ทำให้องค์กรมีความเสี่ยง ในกรณีที่ความเสี่ยงนั้นส่งผลเสียมากกว่าผลประโยชน์

2.3.1.3. การโอนความเสี่ยง (Transfer Risk) การแบ่งปันความเสี่ยงส่วนหนึ่งให้กับบุคคลหรือหน่วยงานอื่น ตัวเลือกนี้ช่วยลดผลกระทบ (Impact) ซึ่งเป็นองค์ประกอบของความเสี่ยง

2.3.1.4. การลดความเสี่ยง (Reduce Risk) การกำหนดมาตรการหรือแนวทางเพื่อลดระดับของความเสี่ยง เช่น การใช้ Firewall เพื่อจำกัดการรับส่งข้อมูลผ่านระบบเครือข่ายภายในและภายนอก

2.3.2.การเตรียมและดำเนินการตามแผนจัดการความเสี่ยง (Preparing and implementing risk treatment plans) ในการจัดเตรียมและดำเนินการตามแผนจัดการความเสี่ยงหน่วยงาน ต้องพิจารณาเลือกแนวทางการจัดการความเสี่ยงที่เหมาะสม โดยพิจารณาหลักการ

2.3.2.1. การลดโอกาสเกิด (Reduces likelihood)

- การอบรมความตระหนักรู้ด้านความมั่นคงปลอดภัยด้านไซเบอร์ให้กับผู้ที่เกี่ยวข้อง (Cyber Security Awareness Training)
- การควบคุมทางเทคนิค (Technical controls)
- การตรวจสอบและติดตามการปฏิบัติงาน (Audit and compliance programs)
- การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)
- การจัดการผู้ให้บริการภายนอก (Third Party Management)

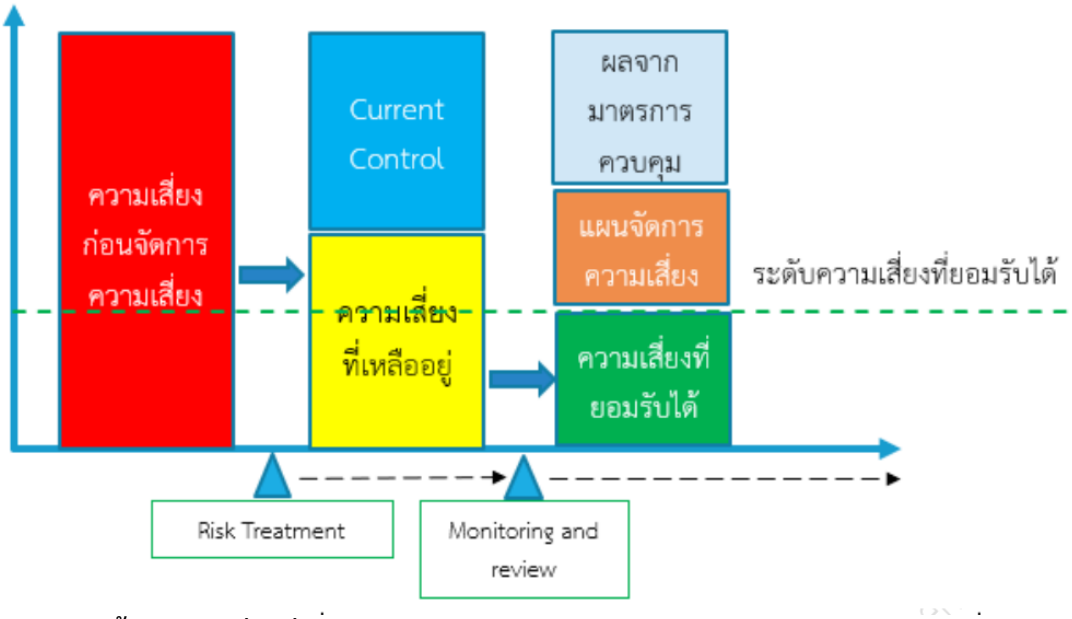
2.3.2.2. การลดผลกระทบ (Reduces impact)

- การกำหนดแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP)

2.3.2.3. การกำหนดแผนฟื้นฟูภัยพิบัติ (Disaster recovery plans)

- การกำหนดเงื่อนไขในสัญญา (Contract conditions)
- การสำรองอุปกรณ์ (Redundancy)

2.4. แท่งผลกระทบต่อกระบวนการ หรือภารกิจหลักขององค์กร รวมถึงยังเป็นกระบวนการที่ใช้ติดตามผลของการวางมาตรการควบคุม (Security Control) ว่ามาตรการดังกล่าวช่วยลดผลกระทบ โอกาสเกิด และระดับความเสี่ยงได้หรือไม่



กำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI)

คือปัจจัย หรือข้อมูลที่สะท้อนให้เห็นแนวโน้มของระดับความเสี่ยง สามารถใช้เป็นเครื่องมือในการแจ้งเตือนล่วงหน้าเพื่อใช้ในการติดตามและเฝ้าระวังความเสี่ยง

ลักษณะของตัวชี้วัดความเสี่ยงที่ดี

- ควรมีลักษณะมองไปในอนาคต ชี้วัดความเสี่ยงนำ (Forward Looking/Leading Indicator) ซึ่งสามารถสะท้อนแนวโน้มของความเสี่ยงได้ เช่น ช่องโหว่ของระบบที่อยู่ในระดับสูงขึ้นไปที่ยังไม่ได้รับการปิดภายใน 3 เดือน เป็นต้น
- ควรเป็นข้อมูลเชิงสถิติหรือข้อมูลที่วัดค่าได้จริง เช่น ระยะเวลาการหยุดชะงักของระบบงาน เป็นต้น
- สัมพันธ์กับเหตุการณ์ความเสี่ยง อาจเชื่อมโยงมาจากสาเหตุความเสี่ยง
- สามารถกำหนดตัวชี้วัดได้มากกว่า 1 ตัวชี้วัดใน 1 เหตุการณ์

2.5. การบันทึกและรายงานผลการประเมินความเสี่ยง (Recording and reporting) การบันทึกผลการประเมินความเสี่ยง ต้องบันทึกทะเบียนความเสี่ยงและจัดทำเป็นเอกสารโดยมีรายละเอียด ดังนี้

- วันที่ระบุความเสี่ยง (Date the Risk is Identified)
- คำอธิบายของความเสี่ยง (Description of the Risk)
- โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
- ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- การจัดการความเสี่ยง (Risk Treatment)
- เจ้าของความเสี่ยง (Risk Owner)
- สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)
- ความเสี่ยงที่เหลือ (Residual Risk)

การรายงานผลการประเมินความเสี่ยง

เป็นกระบวนการที่ใช้สำหรับการสื่อสารและอธิบายความเสี่ยงปัจจุบัน โดยมีวัตถุประสงค์เพื่อให้ผู้ที่มีส่วนเกี่ยวข้อง และผู้บริหารใช้เป็นข้อมูลประกอบการตัดสินใจในการดำเนินการบริหารความเสี่ยงได้อย่างเหมาะสม โดยจัดทำเอกสาร ดังต่อไปนี้

- รายงานผลการประเมินความเสี่ยง (Risk Assessment Report)
- รายงานผลการจัดการความเสี่ยง (Risk Treatment Plan)

3. ขั้นตอนปฏิบัติการบริหารจัดการบัญชีทรัพย์สินสารสนเทศ (Asset Management Procedure)

3.1. การจัดทำบัญชีทรัพย์สินสารสนเทศ โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

3.1.1.ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญหน่วยงาน

3.1.2.ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญหน่วยงาน

3.1.3.การระบุและการจัดลำดับความสำคัญของทรัพย์สิน

3.1.4.เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญหน่วยงาน

3.1.5.ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญหน่วยงาน

3.1.6.การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญหน่วยงาน

3.1.7.ระดับชั้นความลับของทรัพย์สิน

3.1.8.ประเภทของทรัพย์สิน แบ่งออกเป็น 5 ประเภท

3.1.8.1. ฮาร์ดแวร์ เช่น เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย อุปกรณ์เครือข่าย และอุปกรณ์ที่เกี่ยวข้อง เป็นต้น

3.1.8.2. ซอฟต์แวร์ เช่น ระบบปฏิบัติการ ระบบงาน ระบบฐานข้อมูล เป็นต้น

3.1.8.3. ข้อมูล เช่น ค่า Configuration ข้อมูลในฐานข้อมูลระบบ ข้อมูล Log ของระบบงาน ข้อมูลส่วนบุคคล เป็นต้น

3.1.8.4. บุคลากร เช่น ข้าราชการ พนักงานราชการ พนักงาน ลูกจ้างเหมาจ่าย และผู้ที่เกี่ยวข้อง เป็นต้น

3.1.8.5. ระบบงานบริการ เช่น บริการจากหน่วยงานภายนอก เป็นต้น

3.2. ในการขึ้นทะเบียนให้ใช้แบบฟอร์มรายการบัญชีทรัพย์สิน (Asset Inventory) และแบบฟอร์ม อื่นที่เกี่ยวข้อง

3.3. ระบุชื่อทรัพย์สินฟังก์ชันที่สำคัญของทรัพย์สินผู้เป็นเจ้าของทรัพย์สินหรือได้รับมอบหมายให้ดูแลทรัพย์สินนั้น กำหนดระดับความสำคัญของทรัพย์สิน วันที่ที่ลงทะเบียนทรัพย์สิน ประเภทของทรัพย์สิน และตำแหน่งทางกายภาพของทรัพย์สิน ในรายการบัญชีทรัพย์สิน

3.4. กำหนดระดับชั้นความลับของข้อมูลนั้นไว้ในรายการบัญชีทรัพย์สินตามขั้นตอนการกำหนดระดับชั้นความลับของหน่วยงาน

3.5. กำหนดวิธีการเรียกทรัพย์สินสารสนเทศโดยใช้รูปแบบอย่างหนึ่งอย่างใดเช่นหมายเลขครุภัณฑ์หรือ จากการกำหนด Asset ID เป็นต้น

3.6. การเพิ่มเติมการปรับปรุงและการทบทวนบัญชีทรัพย์สินสารสนเทศ

3.6.1.กรณีมีทรัพย์สินใหม่เกิดขึ้น เช่น เกิดจากแผนงานหรือโครงการในปีงบประมาณนั้น ให้เพิ่มเติมทรัพย์สินที่เกี่ยวข้องลงไปในรายการบัญชีทรัพย์สิน

3.6.2.ทรัพย์สินใหม่ต้องผ่านมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ

3.6.3.ดำเนินการประเมินความเสี่ยง และกำหนดแผนการจัดการความเสี่ยง

3.6.4.กรณีมีการเปลี่ยนแปลงต่อทรัพย์สินในรายการบัญชีทรัพย์สิน เช่น เปลี่ยนแปลงผู้เป็นเจ้าของทรัพย์สิน เปลี่ยนระดับความสำคัญ ให้ปรับปรุงข้อมูลในรายการบัญชีทรัพย์สินให้มีความถูกต้อง

3.6.5.กรณีมีการหมดอายุ หรือการเปลี่ยนใหม่ตามอายุการใช้งานของทรัพย์สินนั้น ให้ลบข้อมูลเดิมทิ้งไป หรือทำเครื่องหมายเพื่อให้ทราบว่าปัจจุบันไม่ได้เป็นทรัพย์สินที่ต้องบริหารจัดการอีกแล้ว

3.6.6.ดำเนินการทบทวนข้อมูลและปรับปรุงรายการในบัญชีทรัพย์สินสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงใดๆ กับทรัพย์สินสารสนเทศ เพื่อให้ข้อมูลมีความถูกต้องเป็นปัจจุบันและเชื่อถือได้

3.7. การประเมินระดับความสำคัญของทรัพย์สิน

3.7.1.การรักษาความลับ (Confidentiality) ทรัพย์สินหรือข้อมูลจะเป็นความลับ อนุญาตให้ผู้ที่มีสิทธิเท่านั้นที่จะสามารถเข้าถึงได้

3.7.2.การรักษาความถูกต้อง ครบถ้วนสมบูรณ์ (Integrity) ทรัพย์สินหรือข้อมูลที่จัดเก็บหรือที่ผ่านการประมวลผลจะต้องมีความถูกต้อง ครบถ้วนสมบูรณ์ ไม่ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

3.7.3.ความพร้อมใช้งาน (Availability) ทรัพย์สินหรือข้อมูลจะต้องพร้อมใช้งานในเวลาที่ต้องการ

พิจารณาระดับความสำคัญ โดยใช้สมการ

$$Asset\ Value = \sum_{i=1}^{n} (loss\ value\ of\ security\ components \times weight)$$

i คือ security component ที่ถูกนำมาพิจารณา (ค่า C-I-A)

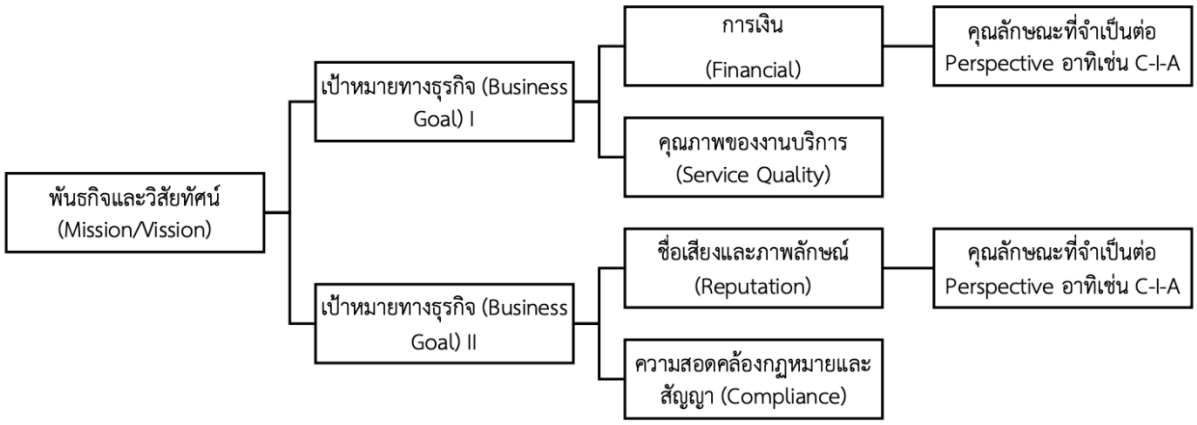
n คือ จำนวนมุมมอง (Perspective) ตามวัตถุประสงค์และเป้าหมายขององค์กร

weight คือ การให้ค่าน้ำหนักตามมุมมอง (Perspective)

loss Value of security componence คือ ระดับของผลกระทบจากการสูญเสีย C-I-A ของทรัพย์สิน

การกำหนดน้ำหนักของคุณลักษณะของความมั่นคงปลอดภัยสารสนเทศ (Security Component)

ทั้งนี้ การเลือกใช้มุมมอง (Perspective) และการกำหนดน้ำหนักของคุณลักษณะของความมั่นคงปลอดภัยสารสนเทศ (Security Component) ให้พิจารณาตามวัตถุประสงค์และเป้าหมายขององค์กร (Mission) เพื่อสร้างความสอดคล้องกับความต้องการทางธุรกิจ



กำหนดให้มีการพิจารณาผลกระทบของการสูญเสียคุณลักษณะ C-I-A ในแต่ละด้านมุมของการ ให้บริการที่สำคัญ โดยอย่างน้อยครอบคลุม ดังนี้

- กระทบด้านการเงิน (Financial Perspective)
- ผลกระทบด้านชื่อเสียงองค์กรและภาพลักษณ์ (Reputation Perspective)

กำหนดระดับความสำคัญทรัพย์สิน (Asset Value)

จะถูกแบ่งระดับชั้นความสำคัญ โดยการแบ่งช่วงสัดส่วนของค่าเต็มของมูลค่าทรัพย์สิน (100%) กำหนดเกณฑ์พิจารณา ดังนี้

ระดับ	ค่า Total Asset Value (weight = 1)
High	มากกว่าหรือเท่ากับ 4
Medium	มากกว่า 2 และน้อยกว่า 4
Low	น้อยกว่าหรือเท่ากับ 2

ตัวอย่างการกำหนดระดับความสำคัญของทรัพย์สินของอุปกรณ์ระบบ SCADA

ชื่อทรัพย์สิน	Financial Perspective (50%)			รวม	Reputation Perspective (50%)			รวม
	C	I	A		C	I	A	
SCADA Genessis32	3	5	5	4.33	5	5	5	5.00

หมายเหตุ : ค่าคะแนนการสูญเสียคุณลักษณะ *C-I-A* ของทรัพย์สิน พิจารณาจาก ภาคผนวก ก
ระดับความสำคัญ = ค่าเฉลี่ยของผลรวมของมุมมอง (Perspective) ด้านการเงิน ชื่อเสียงและภาพลักษณ์ องค์กร
total Asset Value = Financial (0.5 * 4.33) + Reputation (0.5 * 5.0) total Asset Value =2.16 + 2.50 = 4.66 (High)

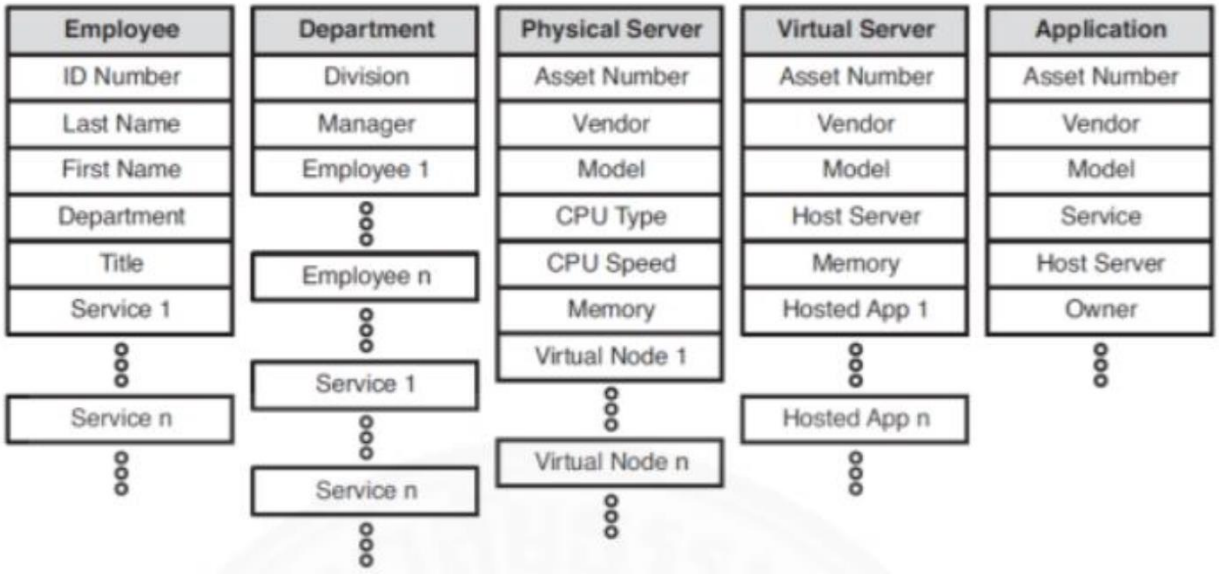
4. การกำหนดการขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญหน่วยงาน

การประยุกต์ใช้ Configuration Management Database (CMDB) ซึ่งเป็นฐานข้อมูลของโครงสร้าง พื้นฐานด้านเทคโนโลยีสารสนเทศ ที่ใช้ในการบันทึกข้อมูลของ Configuration Item (CI) และความสัมพันธ์ ระหว่าง Configuration Item ซึ่งสามารถแบ่งองค์ประกอบได้ ดังนี้

4.1. เชิงกายภาพ (Physical) ตัวอย่างเช่น อุปกรณ์ Hardware, อาคารสถานที่แผนกและบุคลากรในองค์กร เป็นต้น

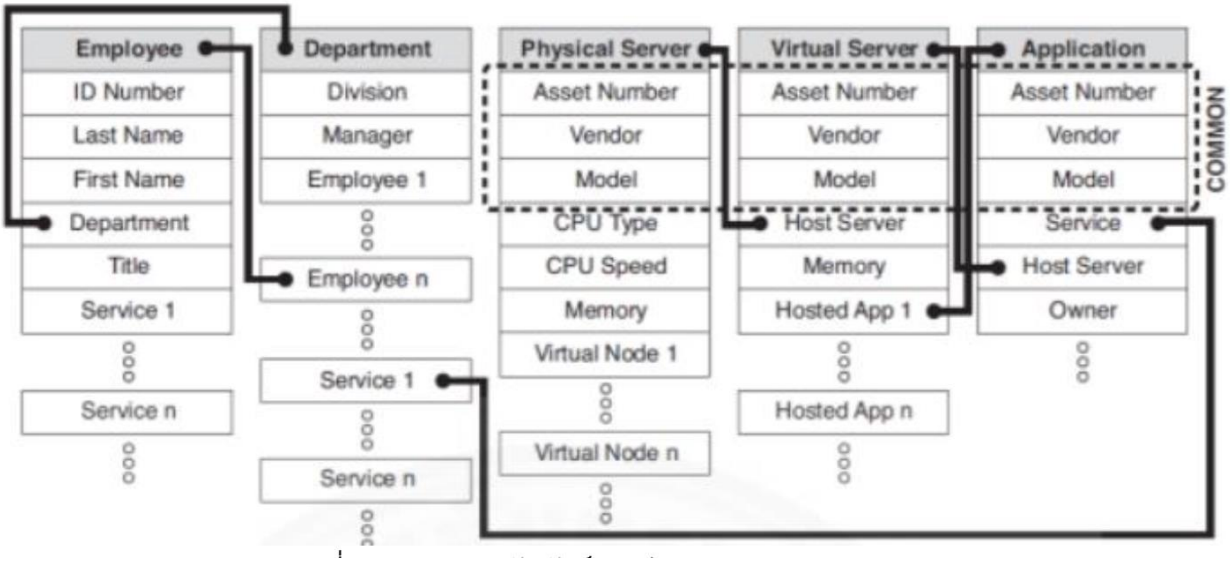
4.2. เชิงตรรกะ (Logical) ตัวอย่างเช่น โปรแกรมประยุกต์ (Application Software) เป็นต้น

4.3. เชิงแนวคิด (Conceptual) เช่น บริการของธุรกิจ (Business Service) เป็นต้น



จากรูปแสดงให้เห็นว่า CI จะมีคุณลักษณะ (Attribute) ของตัวเอง เช่น Physical Server จะมีลักษณะเฉพาะคือ หมายเลขทรัพย์สิน (Asset Number), ความเร็วหน่วยประมวลผล (CPU Speed), หน่วยความจำ (Memory), โมเดล (Model) และผู้จำหน่าย (Vendor) เป็นต้น

ทั้งนี้หากมองแต่ละ CI แยกออกจากกัน จะยากต่อการพิจารณาว่าแต่ละ CI มีการทำงานร่วมกันอย่างไร หากต้องการนำข้อมูลของแต่ละ CI ไปประยุกต์ใช้ให้เกิดประโยชน์มากขึ้น จำเป็นต้องสร้าง ความสัมพันธ์ (Relationship) ระหว่าง CI



จากรูปแสดงให้เห็นว่าแต่ละ CI สามารถเป็นสมาชิก หรือถูกติดตั้งบน CI อื่นได้ ซึ่งจะมีความซับซ้อน เกินกว่าการใช้เพียงตาราง (Table) ในการเก็บข้อมูลและความสัมพันธ์ทั้งหมด ฉะนั้นการใช้ฐานข้อมูล (Database) จะช่วยให้สามารถจัดระเบียบความสัมพันธ์ที่ซับซ้อนของ CI ได้ดีขึ้น ซึ่งความสัมพันธ์ระหว่าง CI นี้ สามารถบันทึกและบริหารจัดการภายใต้ CMDB

การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ

1. สทอภ. ต้องมีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (information security incident management) โดยอย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้
   1.1. กำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Incident response plan) อย่างเป็นลายลักษณ์อักษร และประเมินเหตุการณ์หรือจุดอ่อนของการรักษาความปลอดภัยระบบสารสนเทศ เพื่อพิจารณาระดับความรุนแรงของเหตุการณ์และผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ และต้องจัดให้มีการทดสอบกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

   ทั้งนี้ สทอภ. ต้องจัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ที่เกิดขึ้น และทำหน้าที่ในการรายงานเหตุการณ์ต่อผู้บริหารระดับสูงหรือผู้เกี่ยวข้องให้ทราบและดำเนินการต่อไป

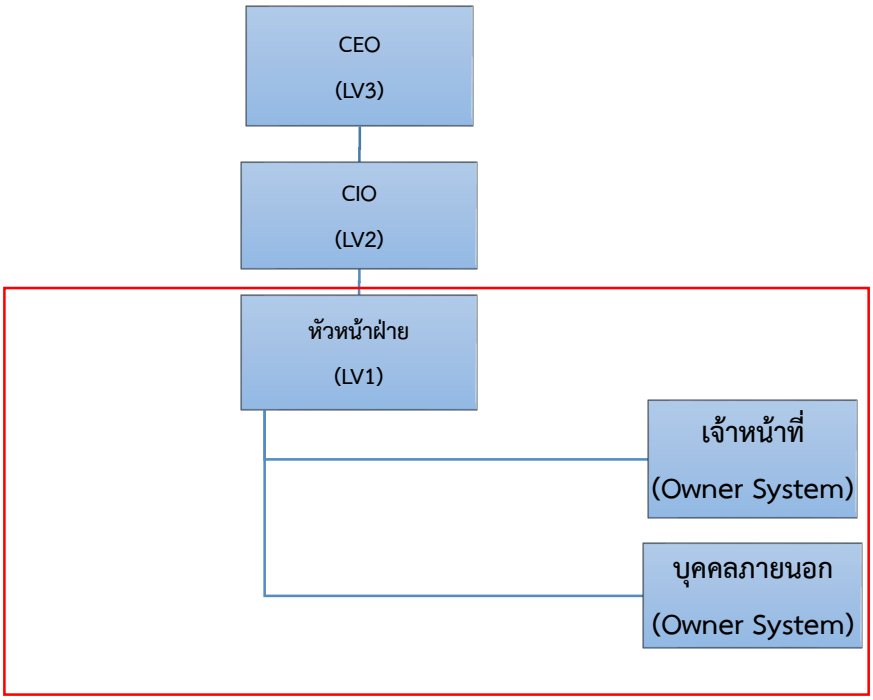
   1.2. จัดให้มีบุคคลหรือหน่วยงาน (point of contact) เพื่อทำหน้าที่รายงานเหตุการณ์ที่เกิดขึ้นต่อ CIO โดยกำหนดกระบวนการรายงานดังต่อไปนี้

   1.2.1. Systems Organization Chart

   แผนภูมิ ผู้มีส่วนเกี่ยวข้องและผู้รับผิดชอบระบบ โดยรายละเอียดมีดังนี้เป็นอย่างน้อย

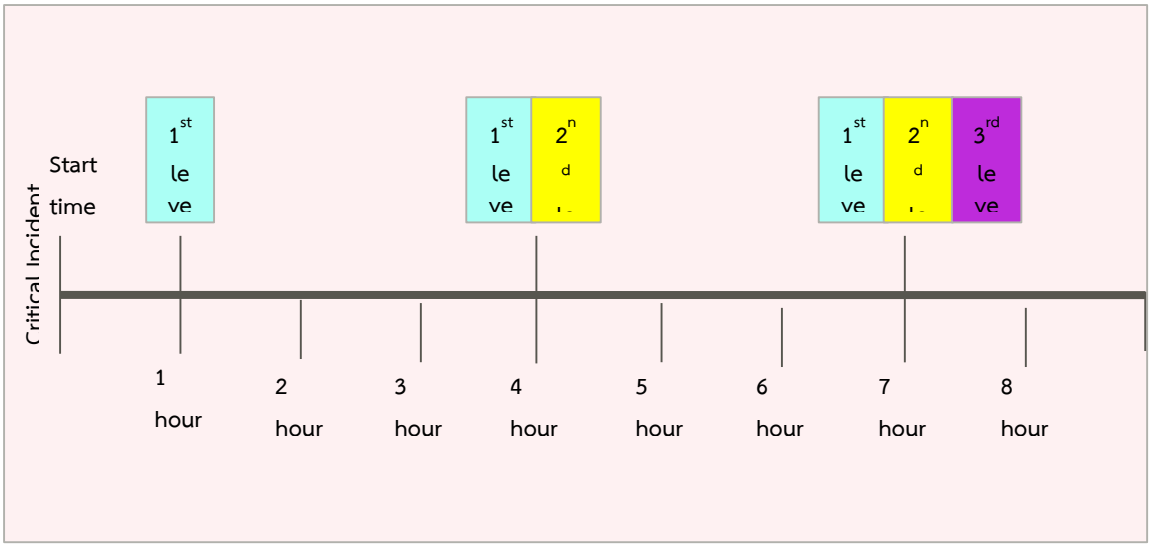
   * กรณีที่เป็น เจ้าหน้าที่ ลูกจ้าง ของ สทอภ.
   - ชื่อ-นามสกุล
   - สำนัก/ฝ่าย
   - ตำแหน่ง
   - เบอร์โทรศัพท์ ที่สามารถติดต่อได้อย่างเร่งด่วน
   - บทบาทหน้าที่ ที่รับผิดชอบในระบบ

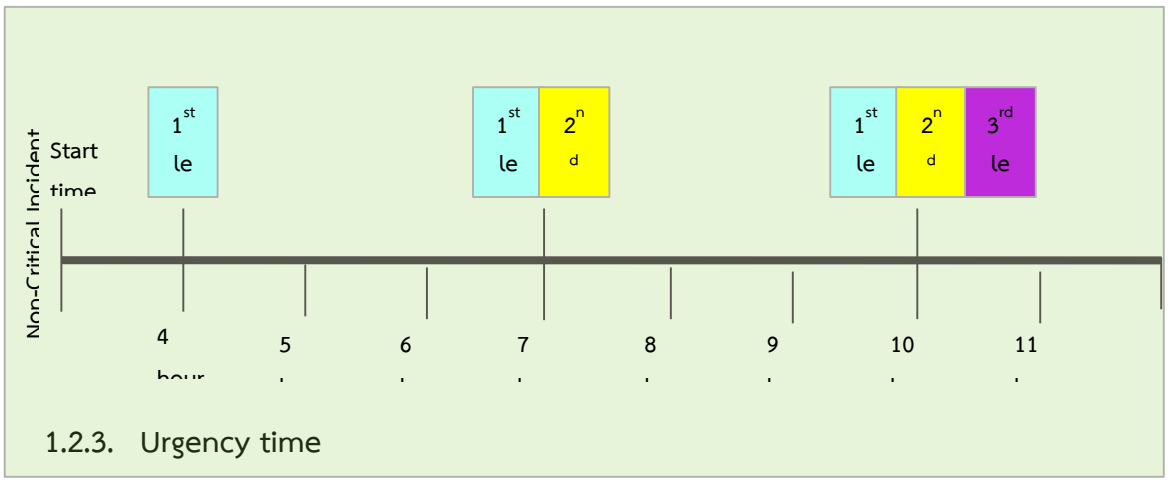
   * กรณีที่เป็น บุคคลภายนอก บริษัทคู่สัญญา
   - ชื่อบริษัท
   - ที่อยู่ บริษัท
   - ชื่อ-นามสกุล
   - วันที่สิ้นสุดสัญญา
   - เบอร์โทรศัพท์ ที่สามารถติดต่อได้อย่างเร่งด่วน
   - บทบาทหน้าที่ ที่รับผิดชอบในระบบ



1.2.2. Escalation process

ระยะเวลาในการดำเนินงานและประสานงานไปยังผู้เกี่ยวข้องเมื่อมีการแก้ไขปัญหาในระบบ





1.2.3. Urgency time

1.2.3.1. Response time: ระยะเวลาการตอบสนองต่อสถานการณ์ incident โดยบันทึกสาเหตุและแนวทางการแก้ไขปัญหาในระบบ ticket (ticket status เปลี่ยนจาก "assigned" เป็น "In-progress")

1.2.3.2. Process: วิธีการดำเนินการแก้ไขปัญหาและความคืบหน้าในการแก้ไขปัญหา

1.2.3.3. Resolution time: ระยะเวลาที่สามารถดำเนินการแก้ไข incident แล้วเสร็จ (ticket status เปลี่ยนสถานะเป็น "resolved")

Response time	Process	Resolution
1. วันเวลาที่เกิดเหตุการณ์ 2. หน่วยงาน / ระบบที่เกิดเหตุ รายละเอียดของเหตุการณ์ ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น 4. ชื่อผู้ติดต่อ / ประสานงานของระบบเพื่อให้ข้อมูล	1. วันเวลาที่เกิดเหตุการณ์ 2. หน่วยงาน / ระบบที่เกิดเหตุ รายละเอียดและสาเหตุของเหตุการณ์ ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้นโดยประเมินมูลค่าความเสียหายที่อาจเกิดขึ้นกับ สทอภ. 4. การดำเนินการแก้ไขปัญหา และระยะเวลาในการแก้ไข 5. ความคืบหน้าในการแก้ไขปัญหา	1. วันเวลาที่เกิดเหตุการณ์ 2. หน่วยงาน / ระบบที่เกิดเหตุ รายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้นโดยประเมินมูลค่า ความเสียหายที่อาจเกิดขึ้นกับ สทอภ. 4. การดำเนินการแก้ไขปัญหา 5. ผลการแก้ไขปัญหา และระยะเวลาในการแก้ไข 6. แนวทางป้องกันในอนาคต และการเก็บรวบรวม หลักฐานเพื่อระบุสาเหตุและแนวทางแก้ไขต่อไป
รายงานโดยทันทีเมื่อทราบเหตุการณ์และตรวจสอบยืนยันในเบื้องต้นแล้ว	รายงานภายใน 4 ชั่วโมงหลังทราบเหตุการณ์และตรวจสอบยืนยันแล้ว	รายงานเมื่อเหตุการณ์ยุติแล้วเสร็จภายใน 2 ชั่วโมง

2. สทอภ. ต้องกำหนดให้มีการบริหารความต่อเนื่องทางธุรกิจในด้านระบบสารสนเทศ (information security of business continuity management)
3. สทอภ. ต้องกำหนดแผนการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (IT continuity plan) เพื่อให้ สทอภ.สามารถกู้ระบบสารสนเทศหรือจัดหาระบบปฏิบัติการมาดำเนินการทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหายน้อยที่สุด และยังคงดำเนินธุรกิจได้อย่างต่อเนื่อง โดยมีรายละเอียดอย่างน้อยดังนี้
   3.1. จัดลำดับความสำคัญในการกู้คืนระบบงานให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น รวมถึงความสัมพันธ์ของแต่ละระบบงาน และการกำหนดระยะเวลาในการกลับคืนสภาพการดำเนินงานตามปกติของระบบงาน
   3.2. ขั้นตอนการแก้ไขปัญหาหรือตอบสนองต่อเหตุการณ์ในแต่ละสถานการณ์ที่เกิดขึ้น
   3.3. บุคคลที่ทำหน้าที่รับผิดชอบและมีอำนาจตัดสินใจ รวมถึงกำหนดเจ้าหน้าที่ผู้รับผิดชอบที่สามารถปฏิบัติงานได้ในแต่ละสถานการณ์รวมทั้งมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

ลักษณะของภัยคุกคามทางไซเบอร์ และปัจจัยที่ใช้ในการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับ

ในการพิจารณาระบุระดับของภัยคุกคามทางไซเบอร์ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรพิจารณาจากเหตุการณ์ต่าง ๆ ที่เป็นพฤติการณ์แวดล้อม ผลกระทบที่เกิดขึ้น ความเสี่ยงหรือแนวโน้มที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ในกรณีต่าง ๆ เพื่อพิจารณาว่าลักษณะของภัยคุกคามทางไซเบอร์นั้นอยู่ในระดับใด โดยให้พิจารณาจากปัจจัยที่ใช้ในการประเมินทั้ง 4 ปัจจัย ดังนี้

(1) ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน

(2) ลักษณะผลกระทบต่อข้อมูลในระบบ

(3) แนวโน้มในการกู้คืนระบบ

(4) ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ

ตาราง ลักษณะภัยคุกคามทางไซเบอร์

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี A	กรณี B
ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน	การประทุษร้ายต่อคอมพิวเตอร์หรือ ระบบคอมพิวเตอร์ ดังนี้ 1) ระบบคอมพิวเตอร์ของหน่วยงาน โครงสร้างพื้นฐานสำคัญของประเทศ 2) อุปกรณ์หรือระบบงานอื่นใดที่ใช้สำหรับการให้บริการของ สทอภ. ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือ ระบบงานดังกล่าว ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของ สทอภ. ด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบ หรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ถูกใช้สำหรับให้บริการหลัก ดังนี้ 1) ระบบคอมพิวเตอร์ 2) โครงสร้างสำคัญทางสารสนเทศ ทั้งนี้ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว แสดงให้เห็นได้ว่า ผู้โจมตีมีความมุ่งหมายที่จะทำให้โครงสร้างพื้นฐานสำคัญของประเทศเสียหายจนไม่สามารถทำงานหรือให้บริการได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตี มีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลอันมีลักษณะดังนี้ 1) การทำงานของ สทอภ. หรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจน สทอภ. ไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของ สทอภ. ได้ 2) เป็นข้อมูลที่เกี่ยวข้องกับชีวิตของบุคคลจำนวนมาก หรือเป็นข้อมูลคอมพิวเตอร์จำนวนมากในระดับประเทศ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตี มีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลใด ๆ อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของ สทอภ. หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญาการรบ หรือการสงคราม

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี A	กรณี B
ลักษณะผลกระทบต่อข้อมูลในระบบ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตี มีความมุ่งหมายให้เกิดการประทุษร้าย ต่อข้อมูล ซึ่งส่งผลกระทบทำให้ระบบคอมพิวเตอร์ของ สทอภ. หรือการให้บริการของ สทอภ. ด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตี มีความมุ่งหมายให้เกิดการประทุษร้าย ต่อข้อมูลที่ใช้สำหรับระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศ ซึ่งส่งผลให้บริการหลักไม่สามารถทำงาน หรือให้บริการได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตี มีความมุ่งหมายให้เกิดการประทุษร้าย ต่อข้อมูลอันมีลักษณะดังนี้ 1) เป็นข้อมูลที่เกี่ยวข้องกับการทำงานของหน่วยงาน สทอภ. หรือการให้บริการ ของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชน 2) เป็นข้อมูลที่เกี่ยวข้องกับชีวิตของบุคคลจำนวนมาก หรือเป็นข้อมูลคอมพิวเตอร์จำนวนมาก ใน ระดับประเทศ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตี มีความมุ่งหมายให้เกิดการประทุษร้าย ต่อข้อมูลใด ๆ อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของ สทอภ. หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้าย ตามประมวลกฎหมายอาญาการรบ หรือการสงคราม

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี A	กรณี B
แนวโน้มในการกู้คืนระบบ	สามารถกู้คืนระบบคอมพิวเตอร์ หรือ ทำให้บริการของ สทอภ. กลับมาได้บางส่วน โดยสามารถดำเนินการได้ตามแผนการกู้คืน	ไม่สามารถกู้คืนระบบ หรือโครงสร้างสำคัญทางสารสนเทศ ที่ใช้สำหรับให้บริการหลักได้ตามแผนการกู้คืน	ไม่สามารถกู้คืนการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของประเทศได้ตามแผนการกู้คืน ทำให้ 1) สทอภ. ไม่สามารถควบคุมการทำงาน ส่วนกลางของระบบคอมพิวเตอร์ของ สทอภ.ได้ 2) มีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคล จำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	ไม่สามารถกู้คืนอุปกรณ์หรือระบบงานที่ได้รับผลกระทบได้ และจำเป็นต้องมีมาตรการเร่งด่วนในการกู้คืนอุปกรณ์ หรือระบบงานที่เกี่ยวข้อง

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี A	กรณี B
ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ	ส่งผลหรืออาจส่งผลกระทบต่อผู้ใช้บริการในวงจำกัด	อาจส่งผลกระทบต่อผู้ใช้บริการทั้งหมด	ส่งผลกระทบต่อผู้ใช้บริการทั้งหมด หรืออาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต	ส่งผลหรืออาจส่งผลกระทบต่อ ความสงบเรียบร้อยของประชาชน หรือ เป็นภัยต่อความมั่นคงของ สทอภ. หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่ง ของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญาการรบหรือการสงคราม

การระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตาราง ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับ และการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคาม ทางไซเบอร์สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับ ไม่ร้ายแรง	1) ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้แนวทางดังกล่าวรวมถึง 1.1 การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่าย ภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดีแล้ว เป็นต้น 1.2 การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของ ฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและภายนอกหน่วยงาน เป็นต้น 1.3 การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด 2) ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และเพื่อใช้ในกระบวนการ ทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี ทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดเนินคดี 3) ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุ หมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้การค้นหาและ วิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น 4) ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้องตลอดจน ผู้ที่อาจได้รับผลกระทบอย่างทันท่วงที โดยอาจขอความช่วยเหลือไปยังบุคคลหรือหน่วยงานต่าง ๆ

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	5) ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่น การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ firewall) การติดตั้งลายเซ็นของ Anti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพในโครงสร้างพื้นฐานและดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ 6) ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติ ภายในกรอบระยะเวลาที่กำหนด (restore within time period) เช่น การกู้คืนระบบ ให้กลับมาดำเนินการได้ตามปกติ(integrity restoration) การสร้างระบบงานขึ้นใหม่ (rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์ (install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) 7) สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการเฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	ดำเนินการตามข้อ 1 และดำเนินมาตรการเพิ่มเติม ดังนี้ 1) หากมีความจำเป็น ให้หน่วยงานดำเนินการใช้ระบบงานสำรองสำหรับการประมวลผล (alternate processing) การจัดเก็บข้อมูล (storage site) และกู้คืนข้อมูลที่เกี่ยวข้องกับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (transaction recovery) 2) ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือ ไปยังหน่วยงานที่เกี่ยวข้อง (supply chain coordination) รวมถึงแจ้งไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ 3) ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในหน่วยงานซึ่งครอบคลุมถึงรูปแบบ ระดับความลับ และเนื้อหาที่ต้องรายงาน ลำดับชั้น การรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือ ที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ (ถ้าระบบมีความพร้อม)) 4) ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานควบคุมหรือกำกับดูแล พนักงาน เจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติหน้าที่ตามกฎหมาย 5) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติในการรับมือหรือสนับสนุนการรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (Automated incident handling processes) (ถ้าระบบมีความพร้อม)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤต	ดำเนินการตามข้อ 1 ถึงข้อ 2 และดำเนินมาตรการเพิ่มเติม ดังนี้ ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถ ให้บริการได้ภายในกรอบระยะเวลาที่กำหนด (restore within time period) โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและเครือข่ายของหน่วยงานทำได้อย่างรวดเร็ว

การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) นั้น หน่วยงานควรกำหนดขั้นตอน วิธีปฏิบัติหรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน โดยพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุในตาราง ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง (โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็น ต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไป ในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี)

เมื่อมีการเก็บรวบรวมข้อมูลและหลักฐานที่จำเป็นตามวรรคหนึ่งแล้ว หน่วยงานควรนำข้อมูล และหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	ภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ให้ดำเนินการดังนี้ 1) นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้างพื้นฐานของบริการ นโยบายและกระบวนการการฝึกบุคลากร การระบุผู้มีอำนาจดำเนินงาน และเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤต	2) รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และวัตถุประสงค์ของการโจมตี เป็นต้น เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบ 3) ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสม และเป็นปัจจุบัน 4) เก็บรักษาข้อมูลและหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือใช้ในกรณีที่ต้องการร้องทุกข์ หรือดำเนินคดีตามแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์

แนวปฏิบัติพื้นฐาน (Security Control Baselines) ตามรายละเอียดที่กำหนดไว้ในตารางนี้เป็นเพียงแนวทางที่ฝ่ายจัดการเทคโนโลยีและระบบสารสนเทศกลาง เห็นว่ามีความเหมาะสมที่จะช่วยให้ สทอภ. สามารถดำเนินมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับได้อย่างมีประสิทธิภาพ และสามารถบรรลุวัตถุประสงค์ตามหลักการของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 อย่างไรก็ดี ผู้ดูแลระบบสามารถหารือร่วมกับฝ่ายจัดการเทคโนโลยีและระบบสารสนเทศกลาง เพื่อให้มีแนวทางการดำเนินมาตรการที่เหมาะสมและสอดคล้องกับลักษณะการดำเนินภารกิจการให้บริการ หรือทรัพยากรที่มีอยู่ภายใต้ความรับผิดชอบของหน่วยงานได้

การกำกับดูแลที่ดีและการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity Governance & Risk Management)

ในปัจจุบัน สทอภ. จำเป็นต้องตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยของภัยคุกคามทางไซเบอร์ ซึ่งการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk) เพียงอย่างเดียวอาจจะยังไม่เพียงพอในการรับมือกับภัยคุกคามที่ไม่อาจคาดคิด ไม่แน่นอน ไม่สามารถคาดการณ์ได้ และที่ไม่รู้ (unknown, unpredictable, uncertain, unexpected) ดังนั้น เพื่อให้ สทอภ.ตระหนักและ ให้ความสำคัญต่อ cyber risk ที่จะเกิดขึ้น จึงได้กำหนดแนวทางปฏิบัติในเบื้องต้นที่ สทอภ.สามารถนำไปปรับใช้เพื่อให้การบริหารจัดการความเสี่ยงมีความครอบคลุมถึงความเสี่ยงด้านภัยคุกคามทางไซเบอร์มากขึ้น โดยมีรายละเอียดดังนี้

1. การกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity Governance)
   1.1. สทอภ. ต้องกำหนดบทบาทหน้าที่ความรับผิดชอบของคณะกรรมการและผู้บริหารระดับสูงในการกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์เพื่อให้สทอภ.มีมาตรฐานในการรักษาความปลอดภัยที่สามารถระบุ (identify) ป้องกัน (protect) ตรวจพบ (detect) รับมือ (response) และสามารถกู้คืน (recovery) เพื่อกลับสู่สภาวะปกติได้ และสนับสนุนให้ สทอภ. มีขีดความสามารถที่เพียงพอเหมาะสมกับปริมาณและความซับซ้อนของระบบ IT ของ สทอภ. โดยกำหนดนโยบายการบริหารจัดการความเสี่ยงครอบคลุมความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber Risk) รวมถึงกำหนดให้มีการรายงานข้อมูลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ ให้คณะกรรมการและผู้บริหารระดับสูงที่ได้รับมอบหมายรับทราบเป็นประจำ
   1.2. กำหนดให้มีหน่วยงานหรือทีมงานที่ทำหน้าที่รับผิดชอบในการประเมิน ติดตามดูแล ป้องกัน และ รับมือกับภัยคุกคามทางไซเบอร์ และรายงานข้อมูลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ ให้คณะกรรมการและผู้บริหารระดับสูงที่ได้รับมอบหมายรับทราบอย่างสม่ำเสมอ ทั้งนี้ สทอภ. อาจพิจารณากำหนดให้มีเจ้าหน้าที่ หรือ ทีมงานเฉพาะที่ทำหน้าที่รับผิดชอบในการรับมือและจัดการกับเหตุการณ์ผิดปกติทางไซเบอร์ได้ทันเวลาเพื่อลดผลกระทบที่จะเกิดขึ้น
   1.3. สทอภ. ต้องจัดอบรมให้ความรู้เรื่องภัยคุกคามทางไซเบอร์ (Cybersecurity Awareness) ที่อาจเกิดขึ้นอย่างน้อยปีละ 1 ครั้ง เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและตระหนักถึงความจำเป็นในการรักษาความปลอดภัยและเข้าใจถึงผลกระทบที่จะเกิดขึ้นตามมาหากเกิดเหตุการณ์ขึ้น รวมทั้งสื่อสารแนวทางการป้องกันและการรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์
   1.4. กำหนดให้มีช่องทางในการประสานงานระหว่างหน่วยงานภายในและภายนอกองค์กร อย่างชัดเจน รวมถึงผู้ให้บริการจากภายนอก เพื่อกำหนดแนวทางในการรับมือและแก้ไขเหตุการณ์ทางด้านความปลอดภัยได้อย่างมีประสิทธิภาพและทันเวลา
2. การบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์

   สทอภ. ต้องกำหนดนโยบายในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ที่ครอบคลุมการระบุความเสี่ยงด้านภัยคุกคามทางไซเบอร์ การป้องกัน การตรวจพบ การรับมือและการกู้คืน รวมทั้งทบทวนและ อัพเดทข้อมูลภัยคุกคามทางไซเบอร์ใหม่ ๆ ตลอดเวลา เพื่อให้เท่าทันต่อการเปลี่ยนแปลงที่เกิดขึ้น โดยมีรายละเอียดดังนี้

   2.1. การระบุ (Identify) สทอภ. ต้องทำการระบุว่า กระบวนการดำเนินงานและทรัพย์สินสารสนเทศใดบ้างที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ และต้องได้รับการรักษาความมั่นคงปลอดภัย เพื่อบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีต่อ ระบบ ทรัพย์สิน ข้อมูล ของ สทอภ. ได้อย่างเหมาะสมการ
   2.2. ป้องกัน (Protect) สทอภ. ต้องมีมาตรการป้องกันที่เหมาะสมเพื่อจำกัดผลกระทบของเหตุการณ์ภัยคุกคามไซเบอร์ ซึ่งครอบคลุมถึงเรื่องการควบคุมการเข้าถึงการฝึกอบรมและการสร้างความตระหนักให้แก่เจ้าหน้าที่และผู้ที่เกี่ยวข้อง ความปลอดภัยของข้อมูล และมาตรการด้านความมั่นคงปลอดภัยต่างๆ ทั้งกระบวนการและวิธีปฏิบัติตลอดจนเทคโนโลยี นอกจากนี้ สทอภ. ต้องทำการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบอิเล็กทรอนิกส์อย่างสม่ำเสมอ เพื่อให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง รวมทั้งการเปลี่ยนแปลงแก้ไข Patch หรือ update software

2.3. การตรวจจับ (Detect) สทอภ. ต้องมีกระบวนการติดตามเฝ้าระวัง และตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง และแจ้งเตือนถึงสิ่งที่ผิดปกติต่าง ๆ รวมถึงการติดตามเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากทั้งภายในและภายนอก วิเคราะห์จุดอ่อนหรือช่องโหว่ของภัยคุกคามที่เกิดขึ้น เพื่อเป็นข้อมูลประกอบในการพิจารณาทบทวนแนวทางการป้องกันความเสี่ยงและผลกระทบที่จะเกิดขึ้นกับ สทอภ. ในอนาคต

2.4. การตอบสนอง / การรับมือ (Respond) สทอภ. ต้องกำหนดแผนการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์และแนวทางแก้ไขปัญหา รวมถึงจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่องให้ครอบคลุมกรณีที่ผลกระทบหรือความเสียหายจากภัยคุกคามทางไซเบอร์ทำให้การดำเนินงานหยุดชะงัก เพื่อให้สามารถรักษาระดับความปลอดภัยและการให้บริการอย่างต่อเนื่อง และ สทอภ. ต้องทำการวิเคราะห์หาสาเหตุและตรวจหาหลักฐานของภัยคุกคามที่เกิดขึ้น รวมถึงมีกระบวนการสื่อสารกับลูกค้า ประชาชน และผู้มีส่วนได้เสียที่ชัดเจน เพื่อความเข้าใจที่ถูกต้องตรงกันต่อสถานการณ์ที่เกิดขึ้นของสทอภ.

2.5. การกู้คืน (Recovery) สทอภ. ต้องกำหนดแผนและกระบวนการในการกู้คืนระบบให้สามารถกลับมาดำเนินการได้ตามปกติภายในระยะเวลาที่กำหนด รวมถึงทำการทบทวนปรับปรุงแผนให้เป็นปัจจุบันเพื่อให้ทันต่อสถานการณ์และนำบทเรียนที่ได้รับจากเหตุการณ์ภัยคุกคามที่เกิดขึ้น (Lesson Learned) มาเป็นส่วนหนึ่งในการทบทวนแผนและกระบวนการกู้คืนระบบให้มีประสิทธิภาพยิ่งขึ้น เพื่อป้องกันปัญหาและผลกระทบที่จะเกิดขึ้นซ้ำในอนาคต

ภาคผนวก ก

เกณฑ์การพิจารณามูลค่าทรัพย์สินทาง C-I-A (Asset Loss Value Criteria)

ภาคผนวก ก : เกณฑ์การพิจารณามูลค่าทรัพย์สินทาง C-I-A (Asset Loss Value Criteria)						
คุณลักษณะของความมั่นคงปลอดภัย	ระดับผลกระทบ	ประเภททรัพย์สิน				
		Hardware	Software	Information	People	Service
การเป็นความลับ (Confidentiality)	ระดับ 1	ไม่มีผลกระทบหรือผลกระทบต่ำมาก ทรัพย์สินสามารถถูกเปิดเผยและเข้าถึงได้จากสาธารณะ	ไม่มีผลกระทบหรือผลกระทบต่ำมาก ทรัพย์สินสามารถถูกใช้งานได้โดยบุคคลทั่วไป เนื่องจากไม่มีการประมวลผลสารสนเทศที่มีชั้นความลับใด ๆ	ทรัพย์สินสามารถถูกเปิดเผยได้ เป็นสาธารณะ ไม่มีผลกระทบใดๆ	ไม่มีผลกระทบใด ๆ เมื่อบุคคลดังกล่าวถูกเปิดเผยในที่สาธารณะ	ไม่มีผลกระทบใด ๆ เป็นงานบริการที่เป็นสาธารณะ ไม่มีการประมวลผลข้อมูลที่มีชั้นความลับ หรือเข้าถึงพื้นที่ที่เป็นเขตควบคุมใด ๆ
	ระดับ 3	หากสามารถเข้าถึงหรือใช้งานโดยไม่ได้รับอนุญาต จะส่งผลให้เกิดความเสียหายปานกลาง เนื่องจากเป็นอุปกรณ์ที่ใช้ในการดำเนินงานสำหรับงานบริการสนับสนุนต่าง ๆ แต่ไม่ใช่	หากสามารถเข้าถึงหรือใช้งานโดยไม่ได้รับอนุญาต จส่งผลให้เกิดควาเสียหายปานกลางเนื่องจากเป็นซอฟต์แวร์ที่ใช้ในการดำเนินงานสำหรับงาน	ทรัพย์สินถูกเปิดเผยไม่ได้ต่อบุคคลที่ไม่เกี่ยวข้องหรือไม่มีสิทธิเข้าถึง เพราะเป็นข้อมูลลับมาก	เมื่อบุคคลดังกล่าวถูกเปิดเผยหน้าที่ความรับผิดชอบต่อสาธารณะหรือผู้ที่ไม่เกี่ยวข้องอาจส่งผลกระทบปานกลางต่อการทำงาน เช่น การ	หากการเปิดเผยข้อมูลของระบบบริการ จะส่งผลกระทบต่อการดำเนินงานหรือให้บริการปานกลาง เนื่องจากระบบบริการดังกล่าว ถูกนำมาใช้ในการดำเนินงานสนับสนุนระบบงานหลักของหน่วยงาน

ภาคผนวก ก : เกณฑ์การพิจารณามูลค่าทรัพย์สินทาง C-I-A (Asset Loss Value Criteria)						
คุณลักษณะของความมั่นคงปลอดภัย	ระดับผลกระทบ	ประเภททรัพย์สิน				
		Hardware	Software	Information	People	Service
		งานบริการหลักของหน่วยงาน	บริการสนับสนุนต่าง ๆ แต่ไม่ใช่งานบริการหลักของหน่วยงาน		ขัดแย้งระหว่างองค์กร ความไม่เสมอภาค	
	ระดับ 5	หากสามารถเข้าถึงหรือใช้งานโดยไม่ได้รับอนุญาต จะส่งผลให้เกิดความเสียหายสูงมาก เนื่องจากเป็นอุปกรณ์ที่ใช้ในงานบริการหลักและบริการสนับสนุนอื่น ๆ ของของหน่วยงานหรือส่งผลกระทบถึงหน่วยงานภายนอกอื่น ๆ หรือระบบงานอื่น ๆ	หากสามารถเข้าถึงหรือใช้งานโดยไม่ได้รับอนุญาต จะส่งผลให้เกิดความเสียหายสูงมาก เนื่องจากเป็นซอฟต์แวร์ที่ใช้ในงานบริการหลักและบริการสนับสนุนอื่น ๆ ของหน่วยงาน หรือส่งผลกระทบถึงหน่วยงานภายนอกอื่น ๆ หรือระบบงานอื่น	ทรัพย์สินถูกเปิดเผยไม่ได้ต่อบุคคลที่ไม่เกี่ยวข้องหรือไม่มีสิทธิเข้าถึง เพราะเป็นข้อมูลลับมากที่สุดและสามารถถูกใช้เพื่อเข้าถึงข้อมูลในทุกระดับชั้น หรือระดับชั้นลับลับมาก ลับที่สุดได้	บุคคลดังกล่าวไม่สามารถถูกเปิดเผยได้เนื่องจากถูกกำหนดโดยบทบาทหน้าที่จากผู้มีอำนาจให้ปกปิดตัวตน เพื่อการดำเนินการสิ่งใดสิ่งหนึ่งที่มีความสำคัญมาก	หากการเปิดเผยข้อมูลของระบบบริการ จะส่งผลกระทบต่อการดำเนินงานหรือให้บริการสูง เนื่องจากระบบบริการดังกล่าว ถูกนำมาใช้ในการดำเนินงานของระบบงานหลักของหน่วยงาน และในระบบสารสนเทศอื่น ๆ ที่สำคัญ ทั้งภายในและภายนอกหน่วยงาน

ภาคผนวก ก : เกณฑ์การพิจารณามูลค่าทรัพย์สินทาง C-I-A (Asset Loss Value Criteria)						
คุณลักษณะของความมั่นคงปลอดภัย	ระดับผลกระทบ	ประเภททรัพย์สิน				
		Hardware	Software	Information	People	Service
ความถูกต้องและเสถียรภาพ (Integrity)	ระดับ 1	การเปลี่ยนแปลงองค์ประกอบหรือการทำงานที่ไม่มีความถูกต้องเสถียรภาพของอุปกรณ์ไม่ส่งผลกระทบใด ๆ หรือส่งผลกระทบน้อยมาก	การเปลี่ยนแปลงองค์ประกอบหรือการทำงานที่ไม่มีความถูกต้องเสถียรภาพของซอฟต์แวร์ไม่ส่งผลกระทบใดๆ หรือส่งผลกระทบน้อยมาก	การผิดพลาดหรือเปลี่ยนแปลงไปของทรัพย์สินไม่ส่งผลกระทบใด ๆ หรือส่งผลกระทบน้อยมากเนื่องจากไม่ได้ใช้งานในระบบงานใด ๆ ที่เกี่ยวข้อง	ความผิดพลาดในการทำงานของบุคคลดังกล่าว ไม่ส่งผลกระทบใด ๆ หรือส่งผลกระทบน้อยมากเนื่องจากบุคคลดังกล่าวมีหน้าที่ความรับผิดชอบที่ไม่สำคัญใด ๆ หรือไม่เกี่ยวข้องกับระบบงานใด ๆ ในขอบเขต	ความผิดพลาดในการทำงานของงานบริการดังกล่าว ไม่ส่งผลกระทบใด ๆ หรือส่งผลกระทบน้อยมาก เนื่องจากงานบริการดังกล่าวมีหน้าที่ความรับผิดชอบที่ไม่สำคัญใด ๆ หรือไม่เกี่ยวข้องกับระบบงานใด ๆ ในขอบเขต
	ระดับ3	การเปลี่ยนแปลงองค์ประกอบหรือการทำงานที่ไม่มีความถูกต้องเสถียรภาพของอุปกรณ์ส่งผลกระทบและสร้างความเสียหายปานกลางเนื่องจากเป็นอุปกรณ์ที่ใช้ในการดำเนินงานระบบสนับสนุน	ความผิดพลาดของข้อมูลส่งผลกระทบและสร้างความเสียหายปานกลางเนื่องจากเป็นซอฟต์แวร์ที่ใช้ในการดำเนินงานระบบสนับสนุน	ความผิดพลาดของข้อมูลส่งผลกระทบและสร้างความเสียหายปานกลางเนื่องจากเป็นข้อมูลที่ใช้ในการดำเนินงานระบบสนับสนุน	ความผิดพลาดในการทำงานของบุคคลดังกล่าว ส่งผลกระทบปานกลาง เนื่องจากบุคคลดังกล่าวมีหน้าที่ความรับผิดชอบที่ต่อระบบงานสนับสนุน	ความผิดพลาดในการทำงานของงานบริการดังกล่าว ส่งผลกระทบปานกลาง เนื่องจากงานบริการดังกล่าวมีหน้าที่ความรับผิดชอบที่ต่อระบบงานสนับสนุน

ภาคผนวก ก : เกณฑ์การพิจารณามูลค่าทรัพย์สินทาง C-I-A (Asset Loss Value Criteria)						
คุณลักษณะของความมั่นคงปลอดภัย	ระดับผลกระทบ	ประเภททรัพย์สิน				
		Hardware	Software	Information	People	Service
	ระดับ5	การเปลี่ยนแปลงองค์ประกอบหรือการทำงานที่ไม่มีความถูกต้อง เสถียรภาพของอุปกรณ์ส่งผลกระทบและสร้างความเสียหายสูง เนื่องจากเป็นอุปกรณ์ที่ใช้ในการดำเนินงานระบบหลักและระบบอื่นๆ ทั้งในหน่วยงานภายในและภายนอก รวมถึงการใช้ระยะเวลาการแก้ไขที่นาน หรือต้องมีการประกาศใช้แผนฉุกเฉิน	ความผิดพลาดของข้อมูลส่งผลกระทบและสร้างความเสียหายสูง เนื่องจากเป็นซอฟต์แวร์ที่ใช้ในการดำเนินงานระบบหลักและระบบอื่นๆ ทั้งในหน่วยงานภายในและภายนอก รวมถึงการใช้ระยะเวลาการแก้ไขที่นานหรือต้องมีการประกาศใช้แผนฉุกเฉิน	ความผิดพลาดของข้อมูลส่งผลกระทบและสร้างความเสียหายสูง เนื่องจากเป็นข้อมูลที่ใช้ในการดำเนินงานระบบหลักและระบบอื่น ๆ ทั้งในหน่วยงานภายในและภายนอก รวมถึงการใช้ระยะเวลาการแก้ไขที่นานหรือต้องมีการประกาศใช้แผนฉุกเฉิน	ความผิดพลาดในการทำงานของบุคคลดังกล่าว ส่งผลกระทบสูงมาก เนื่องจากบุคคลดังกล่าวมีหน้าที่ความรับผิดชอบที่ต่อระบบงานหลักและระบบงานสนับสนุนอื่น ๆ ความผิดพลาดจากการทำงานของบุคคลดังกล่าวสามารถนำมาซึ่งการหยุดชะงักของงานบริการและการใช้แผนฉุกเฉิน	ความผิดพลาดในการทำงานของงานบริการดังกล่าว ส่งผลกระทบสูงมาก เนื่องจากงานบริการดังกล่าวมีหน้าที่ความรับผิดชอบที่ต่อระบบงานหลักและระบบงานสนับสนุนอื่น ๆ ความผิดพลาดจากการทำงานของงานบริการดังกล่าวสามารถนำมาซึ่งการหยุดชะงักของงานบริการและการใช้แผนฉุกเฉิน

ภาคผนวก ก : เกณฑ์การพิจารณามูลค่าทรัพย์สินทาง C-I-A (Asset Loss Value Criteria)						
คุณลักษณะของความมั่นคงปลอดภัย	ระดับผลกระทบ	ประเภททรัพย์สิน				
		Hardware	Software	Information	People	Service
ความพร้อมใช้ (Availability)	ระดับ 1	หากไม่มีอุปกรณ์ดังกล่าวเพื่อใช้งานได้ตามที่ต้องการ จะไม่ส่งผลกระทบใด ๆ หรือส่งผลกระทบน้อยมาก เนื่องจากไม่มีความเกี่ยวข้องใด ๆ กับระบบงานในขอบเขต	หากไม่มีซอฟต์แวร์ดังกล่าวเพื่อใช้งานได้ตามที่ต้องการ จะไม่ส่งผลกระทบใด ๆ หรือส่งผลกระทบน้อยมาก เนื่องจากไม่มีความเกี่ยวข้องใด ๆ กับระบบงานในขอบเขต	หากไม่มีข้อมูลดังกล่าวเพื่อใช้งานได้ตามที่ต้องการ จะไม่ส่งผลกระทบใดๆ หรือส่งผลกระทบน้อยมาก เนื่องจากไม่มีความเกี่ยวข้องใดๆ กับระบบงานในขอบเขต	หากไม่มีเจ้าหน้าที่หรือบุคลดังกล่าวในตำแหน่งหน้าที่นั้นๆ จะส่งผลกระทบน้อยมาก	หากไม่มีงานบริการดังกล่าว จะไม่ส่งผลกระทบใดๆ หรือส่งผลกระทบน้อยมาก เนื่องจากเป็นงานบริการทั่วๆ ไป สามารถทดแทนได้โดยหน่วยงานอื่นๆ
	ระดับ 3	หากไม่มีอุปกรณ์ดังกล่าวเพื่อใช้งานได้ตามที่ต้องการ จะส่งผลให้เกิดความเสียหายปานกลาง เนื่องจากเป็นอุปกรณ์ที่ใช้ในระบบงานสนับสนุนเป็นอุปกรณ์สามารถจัดหาทดแทนได้	หากไม่มีซอฟต์แวร์ดังกล่าวเพื่อใช้งานได้ตามที่ต้องการจะส่งผลให้เกิดความเสียหายปานกลางเนื่องจากเป็นซอฟต์แวร์ที่ใช้ในระบบงานสนับสนุนสามารถจัดหาทดแทนได้	หากไม่มีข้อมูลดังกล่าวเพื่อใช้งานได้ตามที่ต้องการ จะส่งผลให้เกิดความเสียหายปานกลาง เนื่องจากเป็นข้อมูลที่ใช้ในระบบงานสนับสนุนเป็นข้อมูลที่มีการสำรองไว้บางส่วน	หากไม่มีเจ้าหน้าที่หรือบุคคลดังกล่าวในตำแหน่งหน้าที่นั้น ๆ จะส่งผลกระทบปานกลาง เพราะมีหน้าที่ดูแลระบบสนับสนุนของระบบหลัก ต้องการความชำนาญพิเศษ สามารถหาทดแทนได้	หากไม่มีงานบริการดังกล่าว จะส่งผลกระทบปานกลาง เนื่องจากเป็นงานบริการที่เกี่ยวข้องกับระบบสนับสนุน สามารถทดแทนได้ยากโดยหน่วยงานอื่นๆ

ภาคผนวก ก : เกณฑ์การพิจารณามูลค่าทรัพย์สินทาง C-I-A (Asset Loss Value Criteria)						
คุณลักษณะของความมั่นคงปลอดภัย	ระดับผลกระทบ	ประเภททรัพย์สิน				
		Hardware	Software	Information	People	Service
	ระดับ 5	หากไม่มีอุปกรณ์ดังกล่าวเพื่อใช้งานได้ตามที่ต้องการ จะส่งผลให้เกิดความเสียหายสูงมาก เนื่องจากเป็นอุปกรณ์ที่ใช้ในระบบงานหลักและระบบงานอื่นๆทั้งภายในภายนอกองค์กรเป็นอุปกรณ์ที่ไม่สามารถจัดหาทดแทนได้ หรือมีมูลค่าสูงมากหรือใช้เวลานานมากในการจัดหา	หากไม่มีซอฟต์แวร์ดังกล่าวเพื่อใช้งานได้ตามที่ต้องการ จะส่งผลให้เกิดความเสียหายสูงมาก เนื่องจากเป็นซอฟต์แวร์ที่ใช้ในระบบงานหลักและระบบงานอื่นๆ ทั้งภายในภายนอกองค์กรเป็นซอฟต์แวร์ที่ไม่สามารถจัดหาทดแทนได้ หรือมีมูลค่าสูงมากหรือใช้เวลานานมากในการจัดหา	หากไม่มีข้อมูลดังกล่าวเพื่อใช้งานได้ตามที่ต้องการ จะส่งผลให้เกิดความเสียหายสูงมาก เนื่องจากเป็นข้อมูลที่ใช้ในระบบงานหลักและระบบงานอื่น ๆ ทั้งภายในภายนอกองค์กรเป็นข้อมูลขนาดใหญ่มากที่ไม่สามารถสำรองไว้ได้ หรือได้เพียงบางส่วนเท่านั้น และอาจใช้ระยะเวลาในการกู้คืนนานมาก (รวมถึงข้อมูลเป็นความลับมาก จึงถูกกู้คืนได้เพียงบุคคลที่ได้รับอนุญาตเท่านั้น ทำให้เกิดความยากลำบากในการกู้คืน)	หากไม่มีเจ้าหน้าที่หรือบุคคลดังกล่าวในตำแหน่งหน้าที่นั้น ๆ จะส่งผลกระทบสูงมาก เพราะมีหน้าที่ดูแลระบบหลักและระบบสารสนเทศอื่น ๆ ทั้งภายในและภายนอกองค์กร ต้องการความชำนาญพิเศษ ประสบการณ์ที่สูงและความคุ้นเคยกับสภาพแวดล้อมองค์กร หรืออยู่ในระดับผู้บริหาร	หากไม่มีงานบริการดังกล่าวจะส่งผลกระทบสูงมาก เนื่องจากเป็นงานบริการที่เกี่ยวข้องกับระบบหลักและระบบสารสนเทศอื่น ๆ ทั้งภายในและภายนอกองค์กร หรือเป็นเจ้าของผลิตภัณฑ์ที่ไม่สามรถหาทดแทนได้จากหน่วยงานอื่น ๆ การทำงานของงานบริการนั้นถือว่าสำคัญมาก จนเสมือนเป็นการผูกขาดทางธุรกิจ