สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

นโยบายและแนวทางปฏิบัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Policy)

จัดทำโดย บริษัท เอเชี่ยน อินเทลลีเจนท์ อินฟอร์เมชั่น เทคโนโลยี จำกัด

รหัสเอกสาร:	Pol-01
ชื่อเอกสาร:	นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
หมายเลขปรับปรุงเอกสาร:	2565-V1
วันที่เอกสารมีผลบังคับใช้:	16 มีนาคม 2565
เจ้าของเอกสาร:	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ประวัติการปรับปรุงเอกสาร

หมายเลขปรับปรุงเอกสาร (version):	**คำอธิบายและเหตุผลในการแก้ไข**
2565-V1.0	เอกสารเผยแพร่ฉบับแรก

รายการบันทึก

ลำดับ	**รายการบันทึก**	**ผู้รับผิดชอบ**	**อายุการจัดเก็บหลักฐาน**	**วิธีการจัดเก็บหลักฐาน**

สารบัญ

เรื่อง **หน้า**

สารบัญ (ต่อ)

เรื่อง **หน้า**

1. หลักการและเหตุผล

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม (สมอ.) ได้จัดทำ “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565” ขึ้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานเป็นไปอย่างมีประสิทธิภาพและเสถียรภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่อง ทั้งยังช่วยให้หน่วยงานสามารถลดผลกระทบจากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดทำให้ระบบความมั่นคงปลอดภัยของหน่วยงานถูกบุกรุกหรือถูกโจมตี ตลอดจนช่วยให้หน่วยงานสามารถฟื้นฟูระบบอย่างรวดเร็วภายหลังจากภัยคุกคามได้สิ้นสุดลง

2. วัตถุประสงค์

สมอ. ได้จัดทำ “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565” โดยมีวัตถุประสงค์ดังนี้

2.1 เพื่อกำหนดนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

2.2 เพื่อสร้างความเชื่อมั่นด้านความมั่นคงปลอดภัยไซเบอร์ และการดำเนินงานต่างๆ ภายในหน่วยงานเป็นไปอย่างมีประสิทธิภาพ ประสิทธิผลและเสถียรภาพ

2.3 เพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ ผู้บริหาร ผู้ดูแลระบบ และผู้ใช้งานภายในหน่วยงาน รวมทั้งบุคคลภายนอกที่ปฏิบัติงานภายในหน่วยงานมีความรู้ ความเข้าใจและมีความตระหนักถึงความสำคัญในนโยบายและแนวทางปฏิบัติพร้อมทั้งปฏิบัติตามนโยบายแนวทางปฏิบัตินี้อย่างเคร่งครัด

3. องค์ประกอบและขอบเขตของนโยบาย

นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สมอ. จัดทำขึ้นเพื่อกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยขอบเขตมีผลบังคับใช้นโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ครอบคลุมหน่วยงานและการให้บริการภายในทั้งหมดของ สมอ. โดยมีรายละเอียดนโยบายและแนวทางปฏิบัติดังนี้

4. คำนิยาม

ลำดับ	คำศัพท์	ความหมาย
1	หน่วยงาน หรือ องค์กร หรือ บริษัท	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม (สมอ.)
2	ศส.	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สมอ.

ลำดับ	คำศัพท์	ความหมาย
3	ผู้ใช้งาน (User)	ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างตามสัญญาจ้างในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของ สมอ.
4	สิทธิของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
5	ผู้ดูแลระบบ (System Administrator)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบงาน
6	สินทรัพย์	ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตน อันมีมูลค่า หรือคุณค่าสำหรับหน่วยงาน
7	การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)	การอนุญาต การกำหนดสิทธิ หรือมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบสารสนเทศและระบบเครือข่าย
8	ความมั่นคงปลอดภัยด้านสารสนเทศ	การธำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ
9	เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)	กรณีระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์ อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
10	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
11	ระบบอินเทอร์เน็ต (Internet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล
12	ระบบอินทราเน็ต (Intranet)	ระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
13	ระบบสารสนเทศ	ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหารการสนับสนุนให้การบริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

ลำดับ	คำศัพท์	ความหมาย
14	หน่วยงานภายนอก	องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและการใช้งานข้อมูล หรือทรัพย์สินต่างๆ ของหน่วยงานโดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล
15	จดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-mail)	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงกันข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น
16	สื่อบันทึกพกพา	สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Disk หรือ Floppy Disk เป็นต้น
17	ชื่อผู้ใช้ (Username)	ชุดของตัวอักษร หรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์ และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้
18	รหัสผ่าน (Password)	ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
19	อุปกรณ์จัดเส้นทาง (Router)	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น
20	การเข้ารหัส (Encryption)	การนาข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัส เพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
21	การพิสูจน์ยืนยันตัวตน (Authentication)	ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการ พิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
22	SSID (Service Set Identifier)	บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน
23	WEP (Wired Equivalent Privacy)	ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้
24	WPA (Wi-Fi Protected Access)	ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP
25	MAC Address (Media Access Control Address)	หมายเลขเฉพาะที่ใช้อ้างอิงถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน 16 เลข 6 คู่

ลำดับ	คำศัพท์	ความหมาย
26	VPN (Virtual Private Network)	เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับ-ส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ตทาให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
27	แผนผังระบบเครือข่าย (Network Diagram)	แผนผังซึ่งแสดงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน
28	เครื่องแม่ข่าย (Server)	เครื่องหรือโปรแกรมคอมพิวเตอร์ซึ่งทำงานให้บริการในระบบเครือข่ายแก่ลูกข่าย
29	อุปกรณ์กระจายสัญญาณข้อมูล (Switch)	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ - ส่งข้อมูล
30	ไฟร์วอลล์ (Firewall)	เทคโนโลยีป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์จากบุคคลภายนอกเพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย
31	อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)	อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย
32	อัปเดต (Update)	ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ
33	ไฟล์ที่สามารถประมวลผลได้ (Executable File)	ไฟล์โปรแกรมหรือชุดคำสั่งที่สามารถเรียกใช้งานได้ทันที เช่น ไฟล์ที่มีชื่อสกุลเหล่านี้ .exe .com .bat .vbs .scr .pif .hta
34	ช่องโหว่ (Vulnerability)	ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าว เพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
35	ข้อมูลจราจรทางคอมพิวเตอร์ (Log)	ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำหนด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลาและชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์
36	IDS (Intrusion Detection System)	ระบบตรวจจับการบุกรุกเป็นเครื่องมือรักษาความปลอดภัยรองจากไฟร์วอลล์ใช้ในการตรวจจับความพยายามในการบุกรุก เครือข่าย และเตือนภัยให้กับผู้ดูแลระบบได้รับทราบ
37	IPS (Intrusion Prevention System)	ระบบตรวจจับการบุกรุกโดยจะทำงานคล้าย ๆ กับ IDS แต่จะมีคุณสมบัติพิเศษในการจู่โจมกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ไม่จำเป็นต้องอาศัยโปรแกรมหรือ Hardware ตัวอื่น ๆ

ลำดับ	คำศัพท์	ความหมาย
38	Configuration	การกำหนดคุณสมบัติของคอมพิวเตอร์ อุปกรณ์หรือโปรแกรมใด ๆ ที่จะนำมาใช้กับคอมพิวเตอร์เพื่อให้การทำงานมีประสิทธิภาพเหมาะสมกับงานที่ต้องการ
39	Wireless LAN Client	เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลนใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ ซึ่งเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ

5. นโยบายอุปกรณ์แบบพกพา (Mobile device policy)

นโยบายและมาตรการสนับสนุนสำหรับการใช้งานอุปกรณ์แบบพกพาจะต้องมีการนำมาใช้งานเพื่อบริหารจัดการความเสี่ยงจากการใช้อุปกรณ์แบบพกพาโดยจะต้องดำเนินการ ดังนี้

5.1 อุปกรณ์สื่อสารประเภทพกพาต้องได้รับการอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศแล้วเท่านั้น จึงจะสามารถเข้าถึงข้อมูลสารสนเทศของ สมอ. ได้

5.2 อุปกรณ์สื่อสารประเภทพกพาจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตามแนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

5.3 ไม่ควรเก็บข้อมูลสำคัญของ สมอ. ไว้บนอุปกรณ์สื่อสารประเภทพกพาแต่ถ้ามีความจำเป็นที่ต้องจัดเก็บบนอุปกรณ์สื่อสารประเภทพกพาจะต้องมีการเข้ารหัสข้อมูลตามแนวทางการเข้ารหัสของ สมอ.

5.4 ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

5.5 ข้อมูลที่มีชั้นความลับซึ่งถูกจัดเก็บไว้บนอุปกรณ์สื่อสารประเภทพกพาหรือถูกส่งผ่านเครือข่ายไร้สายที่ต้องส่งออกไปนอก สมอ. ต้องได้รับการอนุมัติจากเจ้าของข้อมูลและเข้ารหัสข้อมูลก่อนเท่านั้น ไม่ควรเคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและจะต้องกำหนดให้มีการทำลายเมื่อไม่มีการใช้งานแล้ว

5.6 ระบบคอมพิวเตอร์อื่นที่ต้องการเชื่อมต่อกับระบบของ สมอ. จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศ

5.7 ต้องมีการรักษาความปลอดภัยทางกายภาพร่วมด้วย เช่น จะต้องปิดห้องทำงานเมื่อไม่มีบุคคลที่ได้รับอนุญาตอยู่ประจำโต๊ะทำงานและชั้นเก็บเอกสารต่าง ๆ จะต้องล็อคอย่างดี

5.8 กรณีที่อุปกรณ์สื่อสารประเภทพกพาเป็นสมบัติของ สมอ. การคืนเครื่องหรือส่งซ่อมให้ผู้ใช้งานทำสำเนาข้อมูลจากอุปกรณ์สื่อสารประเภทพกพาเก็บไว้ทั้งหมด และลบข้อมูลทั้งหมดที่มีอยู่บนอุปกรณ์สื่อสารประเภทพกพาก่อนส่งซ่อม

5.9 อุปกรณ์สื่อสารประเภทพกพา เช่น เครื่องคอมพิวเตอร์แบบพกพา (Notebook) หรือ Smart Device ควรมีกระบวนการเพื่ออัปเดตระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ตามแนวปฏิบัติการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ของ สมอ.

5.10 การเข้าถึงและใช้ข้อมูลสารสนเทศ ซึ่งรวมถึงชั้นความลับของผู้ใช้งานเป็นอันสิ้นสุดลงทันทีเมื่อผู้ใช้งานพ้นสภาพตามสิทธิ์ของผู้ใช้งาน

5.11 สมอ. อาจดำเนินการทางวินัย แพ่ง หรืออาญา กับผู้ที่ล่วงละเมิดการเข้าถึง ล่วงละเมิดใช้งานหรือล่วงละเมิดเผยแพร่ข้อมูลสารสนเทศที่เป็นความลับโดยที่ผู้นั้นไม่มีสิทธิ์อันชอบ

6. นโยบายการปฏิบัติงานจากระยะไกล (Teleworking Policy)

นโยบายและมาตรการสนับสนุนสำหรับการปฏิบัติงานจากภายนอกต้องมีการนำมาใช้งานเพื่อป้องกันข้อมูลที่มีการเข้าถึงการประมวลผลหรือการจัดเก็บจาก สมอ. โดยจะต้องดำเนินการดังนี้

6.1 ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอก สมอ. หน่วยงานที่รับผิดชอบต้องปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิ์ที่ได้รับและมีการตรวจสอบการใช้งานอย่างสม่ำเสมอ

6.2 ไม่อนุญาตให้ใช้งาน Remote Access สำหรับการปฏิบัติงานภายใต้ขอบเขตการดำเนินงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เว้นแต่กรณีเกิดเหตุฉุกเฉินหรือเกิดเหตุการณ์ภัยพิบัติที่มีความจำเป็นต้องให้มีการปฏิบัติงานจากภายนอกเท่านั้น กรณีที่ต้องมีการเชื่อมต่อ Remote Access เพื่อปฏิบัติงานจากภายนอก ต้องได้รับการอนุมัติการเชื่อมต่อผ่านระบบ Virtual Private Network (VPN) ของ สมอ. เท่านั้น

6.3 การเข้าสู่ข้อมูลของ สมอ. จากระยะไกลได้นั้นต้องได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศก่อนและผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติฯ ที่เกี่ยวข้องกับการเข้าสู่ระบบและข้อมูลของ สมอ. จากระยะไกลนอกจากนี้เจ้าของข้อมูลมีหน้าที่ดูแลรักษาและเปลี่ยนแปลงรายชื่อของผู้ใช้งานที่สามารถเข้าสู่ระบบจากระยะไกลให้ถูกต้องและเหมาะสมเพื่อให้หน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศตรวจสอบความถูกต้องได้

6.4 ต้องมีการกำหนดวิธีการพิสูจน์ตัวตน

6.5 ก่อนจะกำหนดสิทธิ์ของผู้ใช้งานในการเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นอย่างเพียงพอ และต้องได้รับอนุมัติจากหน่วยงานที่เป็นเจ้าของข้อมูลอย่างเป็นทางการเท่านั้น

6.6 ต้องควบคุม Port ที่ใช้ในการเข้าสู่ระบบโดยการโทรเข้า / โทรออก (Dial-in / Dial-out) อย่างรัดกุม (ถ้ามี) ผู้ใช้งานที่มีความจำเป็นที่จะต้องใช้สาย Analog ในการเข้าสู่ระบบโดยวิธีการโทรเข้า / โทรออก ต้องได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่าย

ระบบสารสนเทศ นอกจากนี้สายที่ใช้ในการโทรออกต้องถูกตั้งค่าให้สามารถโทรออกได้เท่านั้น (ถ้าทำได้) การเข้าสู่ระบบโดยการโทรเข้านั้นต้องมีการดูแล และการจัดการโดยผู้ดูแลระบบ และวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

6.7 ห้ามนำซอฟต์แวร์การควบคุมจากระยะไกล เช่น PC-Anywhere หรือ Carbon copy มาใช้กับคอมพิวเตอร์ของ สมอ. การใช้ซอฟต์แวร์ที่ไม่เหมาะสมดังกล่าวสามารถเป็นช่องทางให้ผู้ที่ไม่ประสงค์ดีเข้ามายังเครือข่ายของ สมอ.

7. นโยบายการควบคุมการเข้าถึง (Access control policy)

7.1 ความต้องการการให้บริการสำหรับการควบคุมการเข้าถึง

7.1.1 นโยบายควบคุมการเข้าถึง (Access control policy) นโยบายควบคุมการเข้าถึงต้องมีการดำเนินการดังนี้

7.1.1.1 กำหนดให้มีการควบคุมการเผยแพร่ข้อมูลและการให้สิทธิ์ เช่น หลักการความจำเป็นที่ต้องรู้ (Need to know), ระดับของความปลอดภัยและการจัดระดับชั้นการเข้าถึงข้อมูล

7.1.1.2 ควบคุมการจัดการสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญทุกระบบ

7.1.1.3 การแบ่งแยกการควบคุมการเข้าถึง เช่น การร้องขอเข้าถึงการให้สิทธิ์การเข้าถึง การบริหารการเข้าถึง

7.1.1.4 ต้องมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้งทุกระบบสารสนเทศที่มีความสำคัญ

7.1.1.5 ต้องถอดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศเมื่อบุคลากรพ้นสภาพ โยกย้าย เปลี่ยนผู้รับผิดชอบ หรือมีการปรับเปลี่ยนอย่างมีนัยสำคัญ

7.1.1.6 ควบคุมการกำหนดหน้าที่ของผู้มีสิทธิ์เข้าถึงด้วยสิทธิพิเศษ และมีการตรวจสอบหรือทบทวนการใช้งานสิทธิ์พิเศษอย่างสม่ำเสมอหรืออย่างน้อยปีละ 1 ครั้ง

7.1.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services) ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ได้รับอนุมัติการเข้าถึงเท่านั้น โดยจะต้องดำเนินการดังนี้

7.1.2.1 การกำหนดเครือข่าย และบริการเครือข่ายที่อนุญาตให้เข้าถึง

7.1.2.2 ขั้นตอนให้สิทธิ์ที่อนุญาตให้เข้าถึงเครือข่าย และบริการเครือข่าย

7.1.2.3 การควบคุมการจัดการ และขั้นตอนเพื่อป้องกันการเชื่อมต่อเครือข่าย และบริการเครือข่าย

7.1.2.4 วิธีที่ใช้ในการเข้าถึงเครือข่าย และบริการเครือข่าย เช่น การใช้ Virtual Private Network (VPN) หรือ เครือข่ายไร้สาย

7.1.2.5 ระบบเครือข่ายที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอก ต้องมีการใช้อุปกรณ์หรือซอฟต์แวร์ในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

7.2 การบริหารจัดการการเข้าถึงด้านระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

7.2.1 การลงทะเบียนและถอดถอนผู้ใช้งาน (User registration and deregistration) ขั้นตอนการจัดการรหัสผู้ใช้งานจะต้องดำเนินการดังนี้

7.2.1.1 ใช้รหัสผู้ใช้งานที่ไม่ซ้ำกันเพื่อให้ผู้ใช้งานรับผิดชอบสำหรับการดำเนินการของตน

7.2.1.2 ยกเลิกการใช้งาน หรือถอดถอนรหัสผู้ใช้งานของคนที่ลาออก โยกย้าย หรือเปลี่ยนแปลงความรับผิดชอบอย่างทันท่วงที ณ วันที่มีผล หรือก่อนวันที่มีผลหากไม่มีความจำเป็นต้องใช้งานแล้ว

7.2.1.3 กำหนดรอบในการยกเลิกการใช้งาน หรือถอดถอนรหัสผู้ใช้งาน

7.2.1.4 กำหนดให้มีการทบทวนรหัสผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง

7.2.1.5 กำหนดให้มีการตรวจสอบกรณีรหัสผู้ใช้งานไม่ได้ใช้งานมากกว่า 90 วัน ให้ดำเนินการระงับรหัสผู้ใช้งานชั่วคราว หากไม่มีการร้องขอการใช้งานรหัสผู้ใช้งานหรือไม่มีผลกระทบใด ๆ หลังจากนั้นอีก 30 วันให้ดำเนินการลบรหัสอย่างทันท่วงที

7.2.1.6 กรณีพบรหัสผู้ใช้งานที่เป็นระบบ (System user) ที่ไม่ได้ใช้งานมากกว่า 90 วัน และมีความจำเป็นต้องใช้งานเพื่อให้ระบบด้านเทคโนโลยีสารสนเทศให้บริการได้ ให้บันทึกไว้การตรวจสอบไว้ในผลการทบทวนและไม่ต้องดำเนินการใดๆ

7.2.2 การจัดเตรียมการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน (User access provisioning) ขั้นตอนการจัดเตรียมการเข้าถึงของผู้ใช้งานจะต้องดำเนินการดังนี้

7.2.2.1 ได้รับสิทธิ์จากเจ้าของระบบเทคโนโลยีสารสนเทศ

7.2.2.2 ตรวจสอบว่าระดับของการเข้าถึงที่ได้รับเหมาะสมกับนโยบายการเข้าถึงและสอดคล้องกับข้อกำหนดอื่น เช่น การแบ่งแยกหน้าที่ (Segregation of duties)

7.2.2.3 ต้องมั่นใจว่าสิทธิ์การเข้าถึงไม่ได้ถูกเปิดใช้งานก่อนที่ขั้นตอนการให้สิทธิ์จะเสร็จสมบูรณ์

7.2.2.4 การบันทึกที่ส่วนกลางของการให้สิทธิ์การเข้าถึงสำหรับรหัสผู้ใช้งานที่เข้าถึงระบบสารสนเทศและบริการ

7.2.2.5 ปรับเปลี่ยนสิทธิ์การเข้าถึงของผู้ใช้งานที่เปลี่ยนหน้าที่ หรืองานที่รับผิดชอบและถอดถอนสิทธิ์การเข้าถึงของผู้ใช้งานทันทีที่ลาออกหรือโยกย้าย

7.2.2.6 มีการทบทวนสิทธิ์การเข้าถึงตามรอบกับเจ้าของระบบสารสนเทศหรือบริการหรืออย่างน้อยปีละ 1 ครั้ง

7.2.3 การบริหารจัดการสิทธิ์การเข้าถึงตามระดับพิเศษ (Management of privileged access rights) ขั้นตอนการบริหารจัดการสิทธิ์การเข้าถึงตามระดับพิเศษ จะต้องดำเนินการดังนี้

7.2.3.1 การกำหนดสิทธิ์การเข้าถึงระดับพิเศษของระบบปฏิบัติการ ระบบการจัดการฐานข้อมูล และแอปพลิเคชัน ต้องได้รับการควบคุมเป็นพิเศษ และระบุตัวตนของผู้ที่ใช้งานด้วย

7.2.3.2 สิทธิ์การเข้าถึงระดับพิเศษควรจัดสรรให้กับผู้ใช้งานตามความจำเป็นในการใช้งาน

7.2.3.3 การให้สิทธิ์และบันทึกของการแจกจ่ายสิทธิ์การเข้าถึงระดับพิเศษทั้งหมดต้องได้รับการควบคุมการใช้งาน

7.2.3.4 กำหนดระยะเวลาในการใช้งานสิทธิ์การเข้าถึงระดับพิเศษ

7.2.3.5 สิทธิ์การเข้าถึงระดับพิเศษควรถูกกำหนดให้กับผู้ใช้งานสำหรับงานที่เกี่ยวข้องกับระบบเท่านั้น และการทำงานทั่วไปควรดำเนินการด้วยรหัสผู้ใช้งานที่มีสิทธิ์ในระดับปกติ

7.2.3.6 การใช้งานด้วยสิทธิ์การเข้าถึงระดับพิเศษควรทบทวนอย่างสม่ำเสมอเพื่อตรวจสอบว่าได้มีการใช้งานที่เหมาะสมตรงตามวัตถุประสงค์ของการใช้งาน

7.2.3.7 กำหนดให้มีการทบทวนสิทธิ์พิเศษอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง

7.2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users) ขั้นตอนการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งานต้องดำเนินการดังนี้

7.2.4.1 ผู้ใช้งานควรลงนามในรายงานเพื่อเก็บข้อมูลความลับสำหรับการพิสูจน์ โดยการลงนามให้รวมข้อกำหนด และเงื่อนไขของของการจ้างงานด้วย

7.2.4.2 เมื่อผู้ใช้งานต้องการจัดเก็บข้อมูลความลับสำหรับการพิสูจน์ตัวตนของตนเอง ผู้ใช้งานควรได้รับข้อมูลความลับสำหรับการพิสูจน์ตัวตนชั่วคราวที่ปลอดภัยในขั้นต้นซึ่งผู้ใช้งานจะถูกบังคับให้เปลี่ยนเมื่อใช้งานในครั้งแรก

7.2.4.3 ควรมีการกำหนดขั้นตอนเพื่อตรวจสอบตัวตนของผู้ใช้งานก่อนที่จะให้ข้อมูลความลับสำหรับการพิสูจน์ตัวตนที่ขอใหม่ ทดแทน หรือชั่วคราว

7.2.4.4 ข้อมูลความลับสำหรับการพิสูจน์ตัวตนชั่วคราวควรมอบให้แก่ผู้ใช้งานในลักษณะที่ปลอดภัย ไม่อนุญาตให้ใช้บุคคลภายนอกหรือข้อความอีเมลที่ไม่มีการป้องกัน

7.2.4.5 ข้อมูลความลับสำหรับการพิสูจน์ตัวตนชั่วคราวต้องเป็นข้อมูลเฉพาะบุคคล และต้องไม่คาดเดาได้ง่าย

7.2.4.6 ข้อมูลความลับสำหรับการพิสูจน์ตัวตนของเจ้าของผลิตภัณฑ์ที่เป็นค่าเริ่มต้นต้องถูกเปลี่ยนหลังจากการติดตั้งระบบหรือซอฟต์แวร์อย่างทันท่วงที

7.2.5 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights) ขั้นตอนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานจะต้องดำเนินการ ดังนี้

7.2.5.1 สิทธิ์การเข้าถึงของผู้ใช้งานต้องได้รับการทบทวนตามรอบที่ได้กำหนดไว้อย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง และหลังจากการเปลี่ยนแปลง เช่น การเลื่อนตำแหน่ง การลดตำแหน่ง การลาออก การโยกย้าย การเปลี่ยนความรับผิดชอบ

7.2.5.2 สิทธิ์การเข้าถึงของผู้ใช้งานควรได้รับการทบทวนและปรับเปลี่ยนเมื่อมีการย้ายตำแหน่งภายใน สมอ.

7.2.5.3 สิทธิ์การเข้าถึงระดับพิเศษควรได้รับการทบทวนตามรอบที่ได้กำหนดไว้อย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง และหลังจากการเปลี่ยนแปลง เช่น การเลื่อนตำแหน่ง การลดตำแหน่ง การลาออก การโยกย้าย การเปลี่ยนความรับผิดชอบ

7.2.5.4 การได้รับสิทธิ์ระดับพิเศษควรมีการตรวจสอบเป็นประจำเพื่อให้มั่นใจว่าไม่มีผู้ใช้งานที่ไม่ได้รับอนุญาตได้รับสิทธิ์ระดับพิเศษ

7.2.5.5 การเปลี่ยนแปลงบัญชีผู้ในงานระดับพิเศษต้องได้รับการบันทึกและมีการทบทวนตามรอบการเปลี่ยนแปลง

7.2.6 การถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงของผู้ใช้งาน (Removal or adjustment of access right) ขั้นตอนการถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงของผู้ใช้งานจะต้องดำเนินการดังนี้

7.2.6.1 เมื่อสิ้นสุดการจ้างงานต้องมีการถอน หรือระงับสิทธิ์การเข้าถึงของผู้ใช้งานที่เกี่ยวข้องกับข้อมูลและทรัพย์สิน

7.2.6.2 สิทธิ์การเข้าถึงต้องถูกถอนออก หรือ ปรับเปลี่ยนทั้งทางกายภาพ และลอจิคัล

7.2.6.3 เอกสารใด ๆ ที่ระบุสิทธิ์การเข้าถึงของเจ้าหน้าที่และบุคคลภายนอกจะต้องถูกถอนออก หรือปรับเปลี่ยน ทันทีที่ลาออก หรือ หมดสัญญาจ้าง ในกรณีที่ผู้ใช้งานเป็นบุคคลภายนอกและทราบรหัสผ่านสำหรับบัญชีผู้ใช้งานที่ยังใช้งานอยู่ต้องเปลี่ยนรหัสผ่านทันทีที่สิ้นสุดการจ้างงาน หรือหมดสัญญา

7.3 ความรับผิดชอบของผู้ใช้งาน

7.3.1 การใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตน (Use of secret authentication information) ขั้นตอนการใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตนจะต้องดำเนินการดังนี้

7.3.1.1 ผู้ใช้งานต้องจัดเก็บข้อมูลความลับสำหรับการพิสูจน์ตัวตนไว้เป็นความลับ ต้องมั่นใจว่าไม่ได้เปิดเผยข้อมูลดังกล่าวต่อคนอื่น

7.3.1.2 หลีกเลี่ยงการการเก็บบันทึกข้อมูลความลับสำหรับการพิสูจน์ตัวตน (เช่น กระดาษ ซอฟต์แวร์ หรือ อุปกรณ์มือถือ ยกเว้นจะสามารถจัดเก็บได้อย่างปลอดภัยและวิธีการจัดเก็บได้รับการอนุมัติแล้ว (เช่น ตู้ล็อคอย่างแน่นหนา ห้องนิรภัย)

7.3.1.3 เปลี่ยนข้อมูลความลับสำหรับการพิสูจน์ตัวตนเมื่อมีข้อบ่งชี้ว่ามีภัยคุกคาม

7.3.1.4 เมื่อรหัสผ่านถูกใช้เป็นข้อมูลความลับสำหรับการพิสูจน์ตัวตน ให้เลือกรหัสผ่านที่มีคุณภาพตามข้อ 7.4.3

7.3.1.5 ต้องมั่นใจว่ามีการป้องกันรหัสผ่านอย่างเหมาะสมเมื่อใช้รหัสผ่านเป็นข้อมูลความลับสำหรับการพิสูจน์ตัวตนในขั้นตอนการเข้าสู่ระบบแบบอัตโนมัติ และในขั้นตอนการจัดเก็บ

7.4 การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน

7.4.1 ข้อกำหนดการเข้าถึงสารสนเทศ (Information Access Restriction)
ขั้นตอนสำหรับข้อกำหนดการเข้าถึงสารสนเทศจะต้องดำเนินการดังนี้

7.4.1.1 ต้องมีการจัดเตรียมหน้าจอหรือเมนูสำหรับควบคุมการเข้าถึงระบบ

7.4.1.2 ควบคุมสิทธิ์การเข้าถึงของผู้ใช้งาน เช่น อ่าน, เขียน และลบ

7.4.1.3 ควบคุมสิทธิ์การเข้าถึงของแอปพลิเคชัน

7.4.1.4 จัดเตรียมสิทธิ์การเข้าถึงทางกายภาพ และลอจิคัลสำหรับระบบและแอปพลิเคชันที่สำคัญ

7.4.2 ขั้นตอนในการเข้าสู่ระบบอย่างปลอดภัย (Secure log-on procedure) ขั้นตอนในการเข้าสู่ระบบอย่างปลอดภัยจะต้องดำเนินการ ดังนี้

7.4.2.1 ไม่แสดงข้อมูล เช่น ชื่อ, รุ่น, ไอพีแอดเดรสของระบบ หรือแอปพลิเคชันจนกว่าจะมีการเข้าสู่ระบบจะเสร็จสิ้นสมบูรณ์

7.4.2.2 ไม่ควรแสดงข้อความเพิ่มเติมระหว่างเข้าสู่ระบบซึ่งอาจช่วยให้ผู้ที่ไม่ได้รับอนุญาตเข้าสู่ระบบได้

7.4.2.3 ตรวจสอบความถูกต้องของข้อมูลนำเข้าเฉพาะเมื่อการเข้าสู่ระบบเสร็จสิ้นสมบูรณ์แล้ว ถ้ามีความผิดพลาดระบบไม่ควรแสดงว่าข้อมูลนำเข้าส่วนไหนไม่ถูกต้อง

7.4.2.4 จำกัดจำนวนครั้งของการพยายามเข้าสู่ระบบ เช่น ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง และหลังการเข้าสู่ระบบผิดพลาดให้บังคับระยะเวลาทิ้งช่วง เช่น 15 นาที ก่อนที่จะยอมให้เข้าสู่ระบบอีกครั้ง ขึ้นอยู่กับระบบสารสนเทศที่มีความสำคัญต่อการให้บริการ

7.4.2.5 ตัดการใช้งานของผู้ใช้งานที่ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่ง เช่น 30 นาที โดยเฉพาะในพื้นที่ที่ความเสี่ยงสูง เช่น เครือข่ายสาธารณะ หรือ เครือข่ายภายนอกของ สมอ. หรือ บนอุปกรณ์เคลื่อนที่

7.4.3 ระบบบริหารจัดการรหัสผ่าน (Password Management System) ขั้นตอนในการเข้าสู่ระบบอย่างปลอดภัยจะต้องดำเนินการดังนี้

7.4.3.1 บังคับการใช้รหัสผู้ใช้งาน และรหัสผ่านให้ใช้งานสำหรับแต่ละบุคคลเท่านั้น

7.4.3.2 บังคับใช้รหัสผ่านที่มีคุณภาพ รายละเอียดดังนี้

1) ต้องมีความยาวมากกว่าหรือเท่ากับ 8 ตัวอักษร เป็นอย่างน้อย

2) ต้องมีส่วนประกอบของอักษรตัวเล็ก ตัวใหญ่ อักขระพิเศษ และตัวเลขประกอบกัน

3) บังคับผู้ใช้งานให้เปลี่ยนรหัสผ่านในการเข้าสู่ระบบครั้งแรก
4) บังคับให้เปลี่ยนรหัสผ่านตามรอบ เช่น ทุก 60 วัน, ทุก 90 วัน
5) ไม่แสดงรหัสผ่านบนหน้าจอที่ผู้ใช้งานกำลังป้อนข้อมูล
7) จัดเก็บไฟล์รหัสผ่านแยกจากข้อมูลทั่วไปของแอปพลิเคชัน
8) รหัสผ่านต้องไม่ง่ายต่อการคาดเดา เช่น ไม่ตั้งรหัสผ่าน 1234 abcd
9) ต้องไม่บันทึกรหัสผ่านในระบบความจำของโปรแกรม

7.4.4 การใช้งานโปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs) ขั้นตอนในการใช้งานโปรแกรมอรรถประโยชน์จะต้องดำเนินการ ดังนี้

7.4.4.1 ใช้โปรแกรมอรรถประโยชน์ต้องมีการระบุตัวตน พิสูจน์ตัวตน และการควบคุมสิทธิ์ของผู้ใช้งาน

7.4.4.2 จำกัดการใช้งานของโปรแกรมอรรถประโยชน์ตามขั้นต่ำที่ต้องใช้งานสำหรับผู้ใช้งานที่ได้รับอนุญาตให้ใช้งาน

7.4.4.3 การขอใช้งานโปรแกรมอรรถประโยชน์ แบบเฉพาะกิจ (ad hoc) ต้องได้รับการอนุมัติจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศส.) ก่อนทุกครั้ง

7.4.4.4 ต้องมีการจำกัดสิทธิ์ในการใช้งานโปรแกรมอรรถประโยชน์ตามความจำเป็นและเหมาะสม

7.4.4.5 ต้องมีการบันทึกประวัติการใช้งานของโปรแกรมอรรถประโยชน์

7.4.4.6 ต้องจัดทำเอกสารระดับการให้สิทธิ์ในการเข้าถึงโปรแกรมอรรถประโยชน์

7.4.4.7 ต้องดำเนินการยกเลิกโปรแกรมอรรถประโยชน์ที่ไม่ได้ใช้งานหรือไม่จำเป็น

7.4.5 การควบคุมการเข้าถึงโปรแกรมซอร์สโค้ด (Access Control to Program Source Code) ขั้นตอนในการควบคุมการเข้าถึงโปรแกรมซอร์สโค้ดจะต้องดำเนินการ ดังนี้

7.4.5.1 ต้องไม่เก็บ Source Code Library ไว้บนระบบที่ใช้งานจริง (Production System)

7.4.5.2 การเข้าถึง Source code ต้องจำกัดสิทธิ์ให้เฉพาะผู้ใช้งานที่จำเป็น เช่น โปรแกรมเมอร์ หรือผู้มีสิทธิ์เฉพาะหน้าที่ที่ได้รับมอบหมายเท่านั้น

7.4.5.3 ระหว่างการทดสอบต้องไม่เก็บ Source code ที่ใช้ทดสอบร่วมกับที่ใช้งานจริง

7.4.5.4 ต้องจัดเก็บ Source code ในสภาพแวดล้อมที่ปลอดภัย

7.4.5.5 ต้องมีการบันทึกประวัติการเข้าถึง Source code

7.4.5.6 การเปลี่ยนแปลงหรือแก้ไข Source code ต้องได้รับการอนุมัติจาก ศส. ก่อนเสมอ

8. นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

8.1 การใช้มาตรการเข้ารหัสข้อมูลจะต้องดำเนินการ ดังนี้

8.1.1 กำหนดวิธีการเข้ารหัสข้อมูลตามมาตรฐานสากล

8.1.2 อัลกอริทึมที่ใช้ในการเข้ารหัสต้องมีความปลอดภัย

8.1.2.1 การเข้ารหัสแบบสมมาตรควรกำหนดให้ใช้อัลกอริทึมที่มีความปลอดภัย เช่น AES-128, AES-256

8.1.2.2 การเข้ารหัสแบบอสมมาตรควรกำหนดให้ใช้อัลกอริทึมที่มีความปลอดภัย เช่น RSA2048

8.1.2.3 ฟังก์ชันแฮชควรกำหนดให้ใช้อัลกอริทึมที่มีความปลอดภัย เช่น ECDSA-256, SHA-256, SHA-384, SHA-512

8.1.3 โปรโตคอลที่ใช้สื่อสารต้องมีความปลอดภัย

8.1.3.1 การใช้งานผ่านเว็บ HTTPS ควรใช้งานโปรโตคอล SSL/TLS ที่เป็น TLS 1.2, 1.3 ขึ้นไป หรือตามมาตรฐานสากล ณ ช่วงเวลานั้น

8.1.3.2 การรับส่งข้อมูลควรใช้งานโปรโตคอลที่ปลอดภัย เช่น SSH File Transfer Protocol (SFTP), File Transfer Protocol SSL/TLS (FTPS), Secure Shell (SSH), Remote Desktop Connection (RDP)

8.1.3.3 การใช้งานทางไกลควรใช้งานโปรโตคอลที่ปลอดภัย เช่น Internet Protocol Security (IPSEC), Virtual Private Network (VPN)

8.1.3.4 การใช้งานข้อความ หรือ จดหมายอิเล็กทรอนิกส์ ควรใช้งานโปรโตคอลที่ปลอดภัย เช่น Secure/Multipurpose Internet Mail Extensions (S/MIME), Pretty Good Privacy (PGP)

8.1.4 ต้องมีการทบทวนมาตรฐานของการเข้ารหัสในทุก ๆ ปี เพื่อให้สอดคล้องกับความปลอดภัยตามมาตรฐานสากล ณ ช่วงเวลานั้น

9. นโยบายการบริหารจัดการกุญแจ (Key Management Policy)

9.1 การบริหารจัดการกุญแจจะต้องดำเนินการดังนี้

9.1.1 ข้อมูลที่ถูกเข้ารหัสต้องมีกระบวนการในการบริหารจัดการกุญแจอย่างมีประสิทธิภาพ โดยดำเนินการในขั้นตอนที่เกี่ยวข้องกับกุญแจทุกประเภท เช่น การสร้าง การจัดเก็บ การจัดส่ง การสำรอง การแจกจ่าย และการทำลาย ซึ่งต้องมีการควบคุมอย่างเหมาะสมและปลอดภัย

9.1.2 กุญแจลับ หรือ กุญแจส่วนตัวที่ใช้สำหรับการเข้ารหัสจะต้องถูกจัดเก็บไว้เป็นความลับและมีความปลอดภัยเสมอ

10. นโยบายการควบคุมการเข้าถึงทางกายภาพ (Physical Control Policy)

10.1 การกำหนดความปลอดภัยของพื้นที่

10.1.1 พื้นที่ใช้งานระบบสารสนเทศ (Physical Security Perimeter)

10.1.1.1 ต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ

เพื่อการเฝ้าระวังควบคุมและรักษา ความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

10.1.1.2 ต้องกำหนดการติดตั้งอุปกรณ์ในพื้นที่ใช้งานระบบสารสนเทศให้สอดคล้องกับความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

10.1.1.3 หน่วยงานที่รับผิดชอบอุปกรณ์ที่สำคัญของระบบสารสนเทศ ต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย เช่น กล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถ ป้องกันภัยคุกคามจากผู้บุกรุก ในพื้นที่ใช้งานระบบสารสนเทศ ได้แก่ ศูนย์ปฏิบัติการ SOC ห้อง Server/Data Center ห้อง Network Control หรือห้อง Network Center ห้องเก็บข้อมูลสำรองเพื่อให้เป็นไปตามมาตรฐานสากลที่กำหนดไว้

10.1.1.4 ไม่อนุญาตให้ถ่ายภาพ บันทึกวิดีโอหรือเสียง ภายในบริเวณที่ต้องมีความมั่นคงปลอดภัย ด้านสารสนเทศ (Secure Areas) เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

10.1.2 การควบคุมการ เข้า - ออก (Physical entry controls)

10.1.2.1 ระบุตัวตนผู้ใช้งานและช่วงเวลาที่มีสิทธิ์ผ่าน เข้า - ออก ในแต่ละพื้นที่อย่างชัดเจน

10.1.2.2 ผู้ใช้งานจะได้รับสิทธิ์ให้ เข้า - ออก สถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนดเท่านั้น

10.1.2.3 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งานขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า ศส. ต้องตรวจสอบ เหตุผลและความจำเป็นก่อนที่จะอนุญาตหรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราวทั้งนี้จะต้องแสดงบัตรประจำตัวที่หรือบัตรประจำตัวประชาชนหรือบัตรประจำตัวอื่นที่ราชการออกให้โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคล และการขอ เข้า - ออก ไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่)

10.1.2.4 ต้องขออนุญาตเข้ามาปฏิบัติงานในพื้นที่ให้ปฏิบัติตามขั้นตอนปฏิบัติการขอเข้าพื้นที่

10.1.3 ความปลอดภัยของสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

10.1.3.1 พื้นที่สำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่าน เข้า - ออก ของบุคคลทั่วไป

10.1.3.2 พื้นที่สำนักงานจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณดังกล่าว

10.1.3.3 พื้นที่สำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ ควรมีความปลอดภัย เช่น กั้นพื้นที่ อย่างรอบด้าน ติดตั้งผนังติดตั้งเหล็กดัดล็อคประตูที่ใช้ดอกกุญแจหรือมีระบบ Access Control

10.1.4 การป้องกันภัยคุกคามภายนอก และสิ่งแวดล้อม (Protecting against external and environmental threats)

10.1.4.1 พื้นที่สำนักงานที่มีระบบสำคัญจะต้องมีการควบคุมการ เข้า - ออก อย่างเข้มงวด และตั้งอยู่ในพื้นที่ที่ปลอดภัยจากภัยทางธรรมชาติ เช่น แผ่นดินไหว หรือน้ำท่วม

10.1.4.2 ต้องจะมีอุปกรณ์ดับเพลิงอย่างเพียงพอและเหมาะสม ทั้งนี้ในพื้นที่ที่ต้องมีการรักษาความปลอดภัยควรพิจารณาติดตั้งระบบดับเพลิงอัตโนมัติ

10.1.4.3 ต้องดูแลเรื่องความสะอาดของพื้นที่โดยทั่วไปอย่างสม่ำเสมอ เพื่อไม่ให้มีวัสดุที่เป็นเชื้อเพลิงอยู่ในพื้นที่ดังกล่าว

10.1.5 การปฏิบัติงานในพื้นที่ควบคุม (Working in Control Areas)

10.1.5.1 ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวิดีโอในบริเวณควบคุม เป็นต้น

10.1.5.2 ต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวิดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

10.1.6 การจัดเตรียมพื้นที่สำหรับส่งมอบ (Delivery and loading areas)

10.1.6.1 ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ควรจัดเป็นบริเวณแยกออกมา

10.1.6.2 ต้องจัดให้มีขั้นตอนการลงทะเบียนเพื่อบริหารจัดการทรัพย์สินที่ถูกส่งมอบ

10.2 การกำหนดความปลอดภัยของอุปกรณ์

10.2.1 การจัดวางและป้องกันอุปกรณ์ (Equipment siting and protection)

10.2.1.1 ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจจะเกิดขึ้นกับอุปกรณ์เหล่านั้น

10.2.1.2 มีการจัดเตรียมพื้นที่จัดเก็บอุปกรณ์ที่ปลอดภัย และไม่สามารถเข้าถึงได้โดยง่าย เช่น ตู้หรือลิ้นชักที่มีกุญแจล็อค

10.2.1.3 ห้ามมิให้มีการสูบบุหรี่ รับประทานอาหารและน้ำดื่ม ในพื้นที่จัดวางอุปกรณ์ของศูนย์เทคโนโลยีสารสนเทศ

10.2.1.4 ห้ามนำสารเคมี และเครื่องมือที่อาจก่อให้เกิดอันตรายกับอุปกรณ์เข้ามาในบริเวณพื้นที่ปฏิบัติงาน นอกจากได้รับการพิจารณาอนุญาตและตรวจสอบความเหมาะสมแล้วเท่านั้น

10.2.1.5 ทำการติดตั้งระบบป้องกันฟ้าผ่ากับอาคารอย่างเหมาะสม

10.2.2 ระบบสาธารณูปโภคพื้นฐาน (Supporting utilities)

10.2.2.1 ต้องมีระบบไฟฟ้าสำรองอัตโนมัติเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่องและต้องมีการตรวจสอบระบบไฟฟ้าสำรองและบำรุงรักษาตามความเหมาะสม

10.2.2.2 ต้องจัดให้มีระบบเตือนภัย / ป้องกันภัย เช่น ระบบดับเพลิง ระบบเตือนอัคคีภัย

10.2.2.3 ต้องมีการวางแผน และซักซ้อมการปฏิบัติรับมือกับภัยพิบัติ เช่น อัคคีภัย อย่างน้อยปีละ 1 ครั้ง

10.2.2.4 ระบบที่สำคัญจะต้องมีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ เพื่อลดความสูญเสียที่อาจเกิดขึ้นจากผลกระทบจากเหตุการณ์ภัยพิบัติหรือเหตุการณ์ไม่คาดคิด

10.2.3 ความปลอดภัยของสายเคเบิล (Cabling security)

10.2.3.1 ต้องคำนึงถึงการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน เช่น ผ่านเข้ามาทางใต้ดินผ่านช่องพิเศษที่จัดไว้ หรือเป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย

10.2.3.2 ต้องจัดเก็บสายเคเบิลทั้งหมดที่ใช้ในการรับ ส่งข้อมูลไว้ในรางหรืออุปกรณ์ป้องกันเพื่อป้องกันการดักจับข้อมูลหรืออุบัติเหตุที่อาจทำให้สายขาดหรือชำรุดได้

10.2.3.3 ต้องแยกสายไฟทั้งหมดออกจากสายเคเบิลในการรับ - ส่งข้อมูล เพื่อป้องกันสัญญาณรบกวน

10.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

10.2.4.1 ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงปีละ 1 ครั้งหรือระบบที่สำคัญมากอาจจะกำหนดให้มีการบำรุงรักษาทุก 3 เดือน

10.2.4.2 ทุกครั้งที่ต้องมีการซ่อมแซมอุปกรณ์ใด ๆ จะต้องทำการบันทึกรายการซ่อมบำรุงรักษา อุปกรณ์ดังกล่าวทุกครั้ง

10.2.4.3 ต้องบำรุงรักษาระบบควบคุมสภาพแวดล้อมและอุปกรณ์ต่าง ๆ ตามคำแนะนำที่ผู้ผลิตระบุไว้

10.2.4.4 กำหนดให้บุคลากรที่ผ่านการฝึกอบรมและได้รับอนุญาตเท่านั้น ที่จะสามารถทำการซ่อมบำรุงระบบและอุปกรณ์ต่าง ๆ

10.2.5 การนำทรัพย์สินออกนอกสถานที่ (Removal of assets)

10.2.5.1 การเคลื่อนย้ายสินทรัพย์ต้องทำเป็นบันทึกและขออนุญาตอย่างถูกต้องในการเคลื่อนย้าย

10.2.5.2 เมื่อมีการนำอุปกรณ์และสื่อที่เคลื่อนย้ายได้ออกไปใช้นอกสถานที่ ผู้ที่รับผิดชอบต้องมีมาตรการการป้องกันการสูญหาย

10.2.5.3 การเคลื่อนย้ายทรัพย์สินใด ๆ จะต้องได้รับการอนุญาตลายลักษณ์อักษรและต้องมีการเก็บบันทึกการอนุญาตดังกล่าว

10.2.5.4 ต้องกำหนดระยะเวลาที่ต้องการยืมทรัพย์สิน หรือเวลาที่จะทำการเคลื่อนย้ายทรัพย์สิน และต้องบันทึกการเคลื่อนย้ายทรัพย์สินทุกครั้ง

10.2.6 ความปลอดภัยของอุปกรณ์และทรัพย์สินภายนอกสถานที่ (Security of equipment and assets off-premises)

10.2.6.1 ปฏิบัติตามคำแนะนำในการใช้งานจากเจ้าของผลิตภัณฑ์ของอุปกรณ์และทรัพย์สินอย่างเคร่งครัด

10.2.6.2 ไม่วางอุปกรณ์และทรัพย์สินไว้ในที่สาธารณะ โดยขาดการดูแลหรือเฝ้าระวัง

10.2.6.3 ต้องกำหนดให้มีการป้องกันทรัพย์สินและอุปกรณ์ เช่น Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน

10.2.7 การทำลายอย่างปลอดภัยหรือนำกลับมาใช้งานของอุปกรณ์ (Secure disposal or re-use of equipment)

10.2.7.1 ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ทั้งนี้เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว

10.2.7.2 การทำลายหรือการนำอุปกรณ์กลับมาใช้ใหม่จะต้องถูกกำหนดขั้นตอนการดำเนินงาน ในการทำลายหรือการนำอุปกรณ์อิเล็กทรอนิกส์กลับมาใช้ใหม่เพื่อให้แน่ใจได้ว่าข้อมูลใด ๆ ที่อยู่ในอุปกรณ์ ดังกล่าวได้ถูกลบทิ้งโดยที่ไม่สามารถกู้คืนกลับมาใช้ได้อีก

10.2.8 อุปกรณ์ที่ไม่อยู่ระหว่างการใช้งาน (Unattended user equipment)

10.2.8.1 ต้องใช้งานซอฟต์แวร์พักหน้าจอ โดยตั้งเวลาให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่าน

10.2.8.2 ต้องทำการออกจากโปรแกรม หรือบริการระบบเครือข่ายเมื่อไม่ใช้งาน

10.2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and Clear screen policy)

10.2.9.1 ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศที่เป็นข้อมูลความลับ หรือลับมาก ไว้ในที่สามารถพบเห็นได้ง่าย โดยจัดเก็บไว้ในที่ที่ปลอดภัย นอกจากนี้ตู้จ่ายเอกสารหรือจดหมายและเครื่องโทรสารจะต้องได้รับการดูแลให้ปลอดภัยด้วย

10.2.9.2 เมื่อสั่งพิมพ์งานเอกสารที่มีข้อมูลสำคัญ ผู้สั่งพิมพ์ต้องทำการจัดเก็บเอกสารโดยทันที

10.2.9.3 อุปกรณ์คอมพิวเตอร์ต้องล็อค หรือ ป้องกันหน้าจอและคีย์บอร์ดที่มีกลไกป้องกันด้วยรหัสผ่านโทเคน หรือกลไกลการพิสูจน์ตัวตนผู้ใช้งานเมื่อไม่ได้ใช้งาน

10.2.9.4 สื่อที่มีข้อมูลอ่อนไหว หรือมีการระบุชั้นความลับไว้ต้องนำออกจากเครื่องถ่ายเอกสารอย่างทันที

11. นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

ต้องปฏิบัติตามนโยบายข้อ 10.2.9

12. นโยบายการสำรองข้อมูล (Backup Policy)

12.1 ต้องสำรองข้อมูลที่สำคัญเก็บไว้ตามระยะเวลาที่เหมาะสม

12.2 ต้องบันทึกรายละเอียดการสำรองข้อมูล โดยมีรายละเอียดเวลาเริ่มต้นและสิ้นสุด ชื่อผู้ทำการสำรองข้อมูลและชนิดของข้อมูลที่บันทึก

12.3 กรณีที่เกิดการผิดพลาดในการสำรองข้อมูล ผู้สำรองข้อมูลต้องบันทึกรายละเอียดของข้อผิดพลาดที่เกิดขึ้นพร้อมแนวทางแก้ไข

12.4 ต้องมีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสม เพื่อให้สามารถกู้ข้อมูลกลับคืนได้ป้องกันระบบจากการถูกโจมตีหรือความเสียหายที่อาจเกิดขึ้น

12.5 ต้องควบคุมความปลอดภัยของข้อมูลที่สำรองตามชั้นความลับ โดยใช้เทคโนโลยีที่เหมาะสมเพื่อป้องกันข้อมูลสำรองถูกเปิดเผย

12.6 ต้องจัดให้มีการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ และการทดสอบควรดำเนินการบนสื่อที่จัดเตรียมไว้แยกจากสื่อที่ใช้สำหรับสำรองข้อมูลตามปกติ เพื่อป้องกันกรณีการทดสอบการกู้คืนข้อมูลไม่สำเร็จซึ่งอาจจะทำให้ข้อมูลที่สำรองไว้เสียหายและไม่สามารถนำกลับมาใช้งานได้

13. นโยบายการถ่ายโอนสารสนเทศ (Information transfer policy)

13.1 ขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ

13.1.1 ต้องออกแบบขั้นตอนเพื่อป้องกันการถ่ายโอนข้อมูลจากการถูกดักจับ คัดลอก แก้ไข ส่งผิดเส้นทาง

13.1.2 ต้องมีขั้นตอนสำหรับการตรวจจับและป้องกันมัลแวร์ซึ่งอาจถูกส่งผ่านการสื่อสารทางอิเล็กทรอนิกส์

13.1.3 ต้องมีการป้องกันการส่งข้อมูลที่สำคัญด้วยวิธีการแนบเอกสาร

13.1.4 ผู้ใช้งานต้องรับผิดชอบในบทบาทหน้าที่ ไม่ฝ่าฝืนนโยบายและแนวปฏิบัติ เช่น การหมิ่นประมาท การข่มขู่หรือก่อกวนความสงบ การปลอมตัว การส่งต่อจดหมายลูกโซ่ การจัดซื้อจัดจ้างนอกเหนือการอนุมัติ

13.1.5 ต้องมีเทคนิคการเข้ารหัสเพื่อปกป้องความลับ ความสมบูรณ์ และความถูกต้องของข้อมูล

13.1.6 ต้องมีแนวทางในการเก็บรักษาและทำลายสำหรับจดหมายธุรกิจต้องเป็นไปตามที่กฎหมายกำหนด

13.1.7 ต้องไม่ทิ้งเอกสารสำคัญไว้ที่เครื่องถ่ายเอกสาร เครื่องพิมพ์หรือเครื่องโทรสาร ซึ่งผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้

13.1.8 ต้องควบคุมและยับยั้งการส่งต่อข้อมูลของอุปกรณ์สื่อสาร เช่น การส่งต่อเมลอัตโนมัติไปที่อยู่อีเมลนอกสำนักงาน

13.1.9 ต้องแนะนำและอบรมให้ความรู้ต่อผู้ใช้งานให้ใช้มาตรการที่เหมาะสมเพื่อป้องกันข้อมูลรั่วไหล

13.1.10 ต้องมีการควบคุมและตรวจสอบเครื่องโทรสารและเครื่องถ่ายเอกสารรุ่นใหม่ที่มีหน่วยความจำในการเก็บเอกสารบางหน้า หรือการส่งข้อมูลที่พิมพ์ผิดพลาด ซึ่งอาจจะถูกพิมพ์ออกมาเมื่อเครื่องทำงานได้ตามปกติ

13.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ

13.2.1 ต้องมีการบริหารจัดการในการควบคุมและแจ้งให้ทราบเกี่ยวกับการสื่อสารการส่งและการรับข้อมูล

13.2.2 ต้องมีการแจ้งให้ผู้ส่งรับทราบเกี่ยวกับการสื่อสารการส่งและการรับข้อมูล

13.2.3 ต้องมีกระบวนการที่สามารถติดตามและปฏิเสธความรับผิดชอบไม่ได้

13.2.4 ต้องมีมาตรฐานทางเทคนิคขั้นต่ำในการสื่อสาร เช่น เอกสารมาตรฐานการเข้ารหัสแบบสมมาตรด้วย AES-128, AES-256 และการเข้ารหัสแบบอสมมาตรด้วย RSA2048

13.2.5 ต้องมีสัญญาข้อตกลง เช่น สัญญาระหว่าง สมอ. และผู้ให้บริการภายนอกที่จะมีการสื่อสารผ่านเครือข่ายที่ปลอดภัยและมีการเข้ารหัส

13.2.6 ต้องมีมาตรฐานในการระบุตัวผู้ส่งเอกสาร

13.2.7 ต้องใช้ระบบป้ายชื่อตามข้อตกลงสำหรับข้อมูลที่มีความสำคัญ เพื่อเข้าใจได้ทันทีในความหมายของป้ายชื่อและข้อมูลได้รับการปกป้องข้อมูลอย่างเหมาะสม

13.2.8 ต้องมีการควบคุมพิเศษที่จำเป็นในการปกป้องข้อมูลสำคัญ เช่น การเข้ารหัสแบบสมมาตรด้วย AES-128, AES-256 และการเข้ารหัสแบบอสมมาตรด้วย RSA2048

13.2.9 ต้องมีการควบคุมการเข้าถึงในระดับที่ยอมรับได้และปลอดภัย

13.3 การส่งข้อความทางอิเล็กทรอนิกส์

13.3.1 ต้องปกป้องข้อความจากผู้ที่ไม่ได้รับอนุญาตไม่ให้มีการแก้ไขข้อความหรือทำให้ระบบใช้งานไม่ได้

13.3.2 ต้องมั่นใจว่าที่อยู่ปลายทาง และการส่งข้อความถูกต้อง

13.3.3 ต้องมีความน่าเชื่อถือและความสามารถในการให้บริการ

13.3.4 ต้องปฏิบัติตามข้อกำหนดทางกฎหมาย เช่น การใช้ลายมืออิเล็กทรอนิกส์

13.3.5 การใช้บริการแบบสาธารณะ ต้องระวังในการรับ – ส่งข้อมูลที่เป็นความลับ เช่น โปรแกรมแชท เครือข่ายสังคม ออนไลน์ การแชร์ไฟล์

13.3.6 ต้องมีการระบุตัวตนในการควบคุมการเข้าถึงจากระบบเครือข่ายสาธารณะต้องปฏิบัติตามมาตรการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างเข้มงวด

13.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ

13.4.1 ต้องจัดให้มีการลงนามในสัญญาการรักษาความลับหรือการไม่เปิดเผยความลับระหว่างผู้ใช้งานและ สมอ. ว่าจะไม่เปิดเผยความลับของ สมอ. ทั้งนี้ต้องมีผลผูกพันทั้งในขณะทำงาน และผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 2 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

13.4.2 บุคลากรที่ต้องลงนามในสัญญาการรักษาความลับหรือการไม่เปิดเผยความลับ ประกอบไปด้วย ข้าราชการ พนักงาน ลูกจ้าง และบุคลากรจากหน่วยงานภายนอก รวมถึงนักศึกษา

ฝึกงานทุกคน ซึ่งเป็นส่วนหนึ่งของเงื่อนไขและข้อกำหนดในการจ้างงาน หรือการฝึกงาน และจะต้องจัดเก็บหลักฐานการลงนามไว้ด้วย

14. นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

14.1 ระบบสารสนเทศต้องได้รับการพัฒนาในสภาพแวดล้อมที่มีความมั่นคงปลอดภัยทั้งทางกายภาพและลอจิคัล เช่น สถานที่ที่ใช้ในการพัฒนาระบบต้องไม่สามารถเข้าถึงโดยผู้ไม่เกี่ยวข้องได้โดยง่าย

14.2 การพัฒนาระบบสารสนเทศต้องคำนึงถึงความมั่นคงปลอดภัยตลอดวงจรชีวิตของการพัฒนาซอฟต์แวร์ โดยครอบคลุมตั้งแต่ขั้นตอนการรวบรวมความต้องการ การออกแบบ การพัฒนา การทดสอบ การใช้งาน ตลอดไปจนถึงการยกเลิกการใช้งานระบบ

14.3 ขั้นตอนการพัฒนาระบบสารสนเทศต้องมีการกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ ดังต่อไปนี้

14.3.1 การป้องกันข้อมูลจากการถูกเปิดเผยโดยไม่ได้รับอนุญาต

14.3.2 การป้องกันข้อมูลจากการถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

14.3.3 ความต้องการด้านความพร้อมใช้งานของข้อมูลและระบบสารสนเทศ

14.3.4 การพิสูจน์ตัวตนของผู้ใช้งานและผู้ดูแลระบบ

14.3.5 การจัดการสิทธิ์ในการใช้งานระบบ

14.3.6 ความต้องการในการตรวจสอบและจัดเก็บประวัติการใช้งาน ประวัติการเข้าถึง

14.3.7 การป้องกันการปฏิเสธการทำรายการ

14.3.8 การบริหารจัดการค่าการปรับแต่ง, เซสชั่น และการจัดการกับข้อผิดพลาดที่เกิดขึ้น

14.3.9 ความต้องการด้านสมรรถนะของระบบสารสนเทศ เช่น ความเร็วในการประมวลผลข้อมูล ความสามารถในการเก็บข้อมูล การประมวลผลในด้านภาพกราฟฟิก ขนาดหน่วยความจำ

14.3.10 ความต้องการด้านความมั่นคงปลอดภัยอื่น ๆ ที่สอดคล้องกับข้อกำหนดกฎหมายหรือกฎระเบียบที่องค์กรต้องปฏิบัติตาม

14.4 ต้องกำหนดจุดทบทวนด้านความมั่นคงปลอดภัยในแต่ละระยะการดำเนินงานของโครงการ เช่น มีการกำหนดให้มีการสอบทานด้านความมั่นคงปลอดภัยในขั้นตอน การออกแบบ การพัฒนา การทดสอบ และก่อนการใช้งานจริง

14.5 ต้องรักษาความปลอดภัยของพื้นที่ที่ใช้ในการจัดเก็บข้อมูลอย่างเหมาะสม เช่น มีการกำหนดและจำกัดสิทธิ์ในการเข้าถึงฐานข้อมูล

14.6 ผู้พัฒนาระบบสารสนเทศต้องได้รับการอบรมความรู้ด้านการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย เช่น Secure Coding ตามมาตรฐาน OWASP (Open Web Application Security Project) รวมถึงความรู้เกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศเป็นประจำทุกปี

15. ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)

15.1 ต้องมีการกำหนดมาตรการควบคุมการเข้าถึงสารสนเทศของ สมอ. โดยผู้ให้บริการภายนอกอย่างเหมาะสมและปลอดภัย

15.2 ต้องมีการกำหนดประเภทของสารสนเทศที่ผู้ให้บริการภายนอกสามารถเข้าถึงได้ และกำหนดมาตรการเฝ้าระวังและสอบทานอย่างเหมาะสม

15.3 ต้องมีการให้ความรู้แก่ผู้ที่มีส่วนเกี่ยวข้องกับผู้ให้บริการภายนอก เพื่อช่วยในการเฝ้าระวังด้านความมั่นคงปลอดภัยสารสนเทศ

16. นโยบายการจัดชั้นความลับ (Information classification policy)

16.1 การจัดชั้นความลับของสารสนเทศ

16.1.1 เจ้าของสารสนเทศมีหน้าที่ในการกำหนดชั้นความลับของสารสนเทศตามกระบวนการจัดชั้นความลับของสารสนเทศภายใต้รับความผิดชอบของตน

16.1.2 การป้องกันสารสนเทศต้องพิจารณาทั้ง 3 ด้าน คือ การรักษาความลับ การรักษาความสมบูรณ์และความพร้อมใช้งาน

15.1.1 ข้อมูลหรือสารสนเทศให้หน่วยงานระบุชนิดลักษณะของข้อมูลให้ชัดเจนว่าเกี่ยวกับเรื่องใด มีความสำคัญอย่างไร และต้องมีการจัดลำดับชั้นความลับเป็นอย่างใดอย่างหนึ่งต่อไปนี้ เช่น ชั้นเปิดเผย ชั้นใช้ภายใน ชั้นลับ ชั้นลับมาก ชั้นลับที่สุด

16.1.3 ข้อมูลหรือสารสนเทศซึ่งมีการกำหนดชั้นความลับไว้ทั้งในกรณีทั้งหมดหรือบางส่วนให้ถือว่ามีชั้นความลับเดียวกันกับข้อมูลหรือสารสนเทศนั้นยกเว้นว่ามีการจัดลำดับชั้นความลับใหม่โดยหน่วยงานเจ้าของข้อมูลหรือสารสนเทศนั้น

16.1.4 ต้องทำการจัดหมวดหมู่กำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสารเพื่อป้องกันสารสนเทศให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดยให้ปฏิบัติตามกระบวนการการจัดระดับชั้นความลับข้อมูลและสารสนเทศ

16.1.5 ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การเก็บรักษาจนถึงการทำลายตามกระบวนการการจัดระดับชั้นความลับข้อมูลและสารสนเทศ

16.2 การบ่งชี้สารสนเทศ

16.2.1 เจ้าหน้าที่ และผู้ปฏิบัติงานตามสัญญาจ้างทุกคนต้องปฏิบัติตามขั้นตอนในการจัดทำป้ายชื่อสารสนเทศ

16.2.2 การจัดทำป้ายชื่อต้องสอดคล้องกับระดับชั้นความลับที่กำหนดไว้ในการจัดชั้นความลับสารสนเทศ

16.2.3 การจัดทำป้ายชื่อสารสนเทศต้องครอบคลุมสารสนเทศทั้งในรูปแบบที่เป็นกายภาพและอิเล็กทรอนิกส์

16.2.4 ต้องจัดให้มีวิธีการจัดทำ และจัดการป้ายชื่อสำหรับสารสนเทศ โดยแยกตามหมวดหมู่ที่กำหนดไว้ มีการส่งมอบและจัดเก็บตามขั้นตอนกระบวนการต่าง ๆ ซึ่งประกอบไปด้วยการถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสารและการทำลาย ให้ปฏิบัติตามแนวทางปฏิบัติของระเบียบปฏิบัติของทางราชการตามกฎหมายที่เกี่ยวข้อง

16.2.5 หากมีความจำเป็นจะต้องกำหนดระดับชั้นความลับของข้อมูลในสื่อบันทึกดังกล่าวเป็นระดับอื่น จะต้องติดป้ายชื่อให้กับสื่อบันทึกดังกล่าว ให้สอดคล้องกับข้อมูลดังกล่าว

16.2.6 ข้อมูลทุกระดับชั้น จะต้องถูกส่งผ่านระบบอีเมลของ สมอ. เท่านั้น กรณีมีช่องทางอื่น ๆ ที่มีความจำเป็นต้องใช้ส่งข้อมูลจะต้องได้รับอนุญาตจาก ศส. เพื่อพิจารณาถึงความปลอดภัยอย่างเหมาะสม

16.3 การจัดการทรัพย์สิน

16.3.1 กระบวนการปฏิบัติงานในการจัดการสินทรัพย์ต้องสอดคล้องและเป็นไปในทิศทางเดียวกับการจัดชั้นความลับสารสนเทศ

16.3.2 ต้องมีการจัดเก็บสินทรัพย์ตามรายละเอียดการจัดเก็บจากผู้ผลิต หากสินทรัพย์นั้นต้องการการจัดเก็บเป็นพิเศษ

17. นโยบายการจัดการสื่อบันทึกข้อมูล (Media Handling policy)

17.1 การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้

17.1.1 ข้อมูลที่มีชั้นความลับ ชั้นความลับมาก ชั้นความลับที่สุด ต้องกำหนดให้มีการทำลายสื่อบันทึกข้อมูลเมื่อไม่มีการใช้งานแล้ว

17.1.2 ในกรณีที่สื่อบันทึกข้อมูลนั้นไม่ได้ถูกนำมาใช้งานแล้ว ก่อนที่จะนำออกไปจาก สมอ. ต้องมั่นใจว่าข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก

17.1.3 ในกรณีที่จำเป็นต้องนำสื่อบันทึกข้อมูลออกไป จะต้องได้รับการอนุมัติจากผู้ที่รับผิดชอบสื่อบันทึกข้อมูลดังกล่าว และต้องบันทึกการโยกย้ายเพื่อใช้ในการตรวจสอบภายหลัง

17.1.4 สื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต เช่น อุณหภูมิสูงหรือต่ำเกินไป

17.1.5 ในการจัดเก็บสื่อบันทึกข้อมูลที่สำคัญ ต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล เช่น มีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน กำหนดบุคลากรที่มีสิทธิ์ในการใช้งาน

17.1.6 ถ้าข้อมูลที่ต้องการจัดเก็บมีอายุการจัดเก็บยาวนานกว่าอายุการใช้งานของสื่อบันทึกข้อมูล ควรจัดเก็บไว้ที่แหล่งอื่นเพื่อป้องกันการสูญหายของข้อมูล

17.1.7 ต้องจัดทำทะเบียนบันทึกข้อมูลของสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้เพื่อลดโอกาสการสูญหายของข้อมูล

17.2 การทำลายสื่อบันทึกข้อมูล

17.2.1 สื่อที่บันทึกข้อมูลที่มีความสำคัญมาก จะต้องมีการทำลายด้วยวิธีการที่ปลอดภัย เช่น การเผาหรือแยกชิ้นส่วนเป็นชิ้นเล็ก ๆ หรือลบข้อมูลด้วยซอฟต์แวร์อื่น ๆ ที่มีใช้ใน สมอ.

17.2.2 กระบวนการต่าง ๆ ต้องระบุวิธีการกำจัดสื่อบันทึกข้อมูลอย่างชัดเจนเพื่อความปลอดภัยของข้อมูล

17.2.3 เพื่อความสะดวกควรรวบรวมสื่อทั้งหมดที่ไม่ต้องการแล้วกำจัดพร้อมกันด้วยวิธีการที่ปลอดภัย

17.2.4 ในกรณีที่เลือกใช้บริการกำจัดสื่อและเอกสารรวมทั้งอุปกรณ์ต่าง ๆ จากหน่วยงานภายนอก ควรระมัดระวังในการเลือกใช้บริการต้องเลือกหน่วยงานภายนอกที่มีการควบคุมที่ดี มีมาตรฐานและมีประสบการณ์

17.2.5 ในการกำจัดสื่อบันทึกข้อมูลจะต้องมีการบันทึกเพื่อใช้ในการตรวจสอบ

17.3 การเคลื่อนย้ายสื่อบันทึกข้อมูล

17.3.1 ใช้วิธีการขนส่งหรือพนักงานส่งของที่เชื่อถือได้

17.3.2 รายชื่อของพนักงานส่งของหรือบริษัทส่งของควรได้รับการอนุมัติจากผู้มีอำนาจ

17.3.3 กระบวนการตรวจสอบพนักงานส่งของต้องมีการปรับปรุงอย่างสม่ำเสมอ

17.3.4 การบรรจุภัณฑ์ต้องป้องกันความเสียหายในระหว่างการขนส่งโดยเป็นไปตามข้อกำหนดของผู้ผลิต ตัวอย่างการป้องกันปัจจัยทางกายภาพที่จะมีผลต่อการกู้คืนข้อมูล เช่น ความร้อน, ความชื้น และสนามแม่เหล็ก

17.3.5 การควบคุมที่จำเป็นในการปกป้องข้อมูลสำคัญจากการเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต

17.3.5.1 ใช้ตู้ที่มีกุญแจล็อค

17.3.5.2 ส่งด้วยมือตนเองและลงบันทึกการรับเพื่อสามารถตรวจสอบได้

17.3.5.3 บางกรณีอาจจะต้องใช้วิธีการแยกส่งออกหลาย ๆ ส่วนและหลาย ๆ เส้นทางเพื่อกระจายความเสี่ยง

18. การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software)

18.1 การควบคุมการติดตั้งซอฟต์แวร์

18.1.1 ต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ซอฟต์แวร์อุดช่องโหว่ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดี ว่าไม่ก่อให้เกิดปัญหาหรือผลกระทบต่อเครื่องที่ให้บริการอยู่

18.1.2 มีการบริหารจัดการเวอร์ชันของซอฟต์แวร์ และมีการจัดเก็บซอฟต์แวร์เวอร์ชันก่อนหน้าไว้ในกรณีที่มีความจำเป็นต้องทำการถอยกลับไปใช้เวอร์ชันก่อนหน้านี้

19. การบริหารจัดการช่องโหว่ (Technical Vulnerability Management)

19.1 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

19.1.1 ต้องกำหนดหน้าที่ความรับผิดชอบที่ชัดเจน เช่น การเฝ้าระวังภัยคุกคามการประเมินความเสี่ยงของภัยคุกคาม การแพตช์ปิดช่องโหว่ในระบบ การตรวจสอบสินทรัพย์ที่ได้จัดส่วนหมวดหมู่ไว้

19.1.2 ต้องร่วมกันวิเคราะห์ความเสี่ยงและประเมินสถานการณ์การบุกรุก ละเมิด ระบาดที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง

19.1.3 ในกรณีที่จะทำการอัพเดทแพตช์ของระบบสำคัญ ๆ ต้องมีการทดสอบและประเมิน ก่อนว่าจะไม่ก่อให้เกิดความเสียหายหรือมีผลกระทบต่อระบบ แต่ถ้าไม่สามารถอัปเดตแพตช์ได้ก็ให้พิจารณาดังต่อไปนี้

19.1.3.1 ปิด Service หรือ การทำงานที่เกี่ยวข้องกับช่องโหว่

19.1.3.2 ปรับปรุงหรือเพิ่มระดับความปลอดภัยในการเข้าถึงที่บริเวณรอบนอกเครือข่าย เช่น เพิ่มอุปกรณ์ไฟร์วอลล์ หรือ IPS (Intrusion Prevention System)

19.1.3.3 เพิ่มการเฝ้าระวังเพื่อตรวจจับหรือป้องกันการโจมตีเครือข่ายอย่างเข้มงวด

19.1.3.4 ต้องมีการสร้างความตระหนักเกี่ยวกับช่องโหว่ที่เกิดขึ้น

19.1.3.5 ต้องเก็บ Log ของเหตุการณ์ที่เกิดขึ้นทั้งหมดเพื่อใช้ในการตรวจสอบ

19.1.3.6 ต้องมีกระบวนการบริหารจัดการช่องโหว่ที่มีการดำเนินการ เช่น การเฝ้าระวังต้อง มั่นใจว่ามีประสิทธิภาพและประสิทธิผล

19.1.3.7 ระบบที่มีความเสี่ยงสูงจะต้องมีการเตรียมการเป็นอันดับแรกตามลำดับความสำคัญและการประเมินความเสี่ยง

19.2 การจำกัดสิทธิ์ในการติดตั้งซอฟต์แวร์

19.2.1 ต้องจัดทำรายการซอฟต์แวร์ที่จำเป็นสำหรับเครื่องผู้ใช้งาน เช่น เครื่องคอมพิวเตอร์, แล็ปท็อป

19.2.2 ต้องทำการตรวจสอบและอนุมัติรายการซอฟต์แวร์ที่จำเป็นสำหรับเครื่องผู้ใช้งาน เพื่อจัดทำเป็นรายการซอฟต์แวร์ที่อนุญาตให้ใช้งานในองค์กรสำหรับเครื่องผู้ใช้งานทั่วไป

19.2.3 ห้ามผู้ใช้งานทำการติดตั้งซอฟต์แวร์ที่เป็นการละเมิดลิขสิทธิ์ รวมถึงซอฟต์แวร์อื่น ๆ ที่ไม่ได้รับอนุญาตให้ใช้งานใน สมอ.

19.2.4 หากผู้ใช้งานต้องการติดตั้งซอฟต์แวร์ที่อยู่นอกเหนือรายการซอฟต์แวร์ที่อนุญาตให้ใช้งาน จะต้องทำการขออนุมัติ ศส. ก่อนการติดตั้ง

19.2.5 การติดตั้งซอฟต์แวร์บนเครื่องผู้ใช้งานจะต้องกระทำโดยผู้ดูแลระบบเท่านั้น โดยผู้ดูแลระบบต้องทำการจำกัดสิทธิ์ในการติดตั้งซอฟต์แวร์บนเครื่องของผู้ใช้งานอย่างเหมาะสม

19.2.6 ต้องทำการตรวจสอบการใช้งานซอฟต์แวร์ที่ไม่ได้รับอนุญาตอย่างน้อยปีละ 1 ครั้ง

20. นโยบายการควบคุมการเปลี่ยนแปลงระบบ (System Change Control Policy)

20.1 ขั้นตอนปฏิบัติสำหรับการควบคุมการเปลี่ยนแปลงระบบอย่างเป็นทางการควรจัดทำเป็นเอกสาร และบังคับใช้เพื่อให้มั่นใจได้ว่าความถูกต้องของระบบ แอปพลิเคชัน และผลิตภัณฑ์ ตั้งแต่ขั้นตอนการออกแบบจนถึงการบำรุงรักษาในปัจจุบัน

20.2 การปรับเปลี่ยนระบบใหม่ หรือ การเปลี่ยนแปลงครั้งใหญ่ ที่มีผลกระทบกับระบบที่ทำงานอยู่ในปัจจุบันควรได้รับอนุญาตตามขั้นตอนตั้งแต่การทำจัดเอกสาร การจัดทำ, การระบุรายละเอียด, การทดสอบ, การควบคุมคุณภาพ และการจัดการสำหรับการติดตั้งระบบ

20.3 ขั้นตอนการควบคุมการเปลี่ยนแปลงต้องรวมการประเมินความเสี่ยง การวิเคราะห์ผลกระทบของการเปลี่ยนแปลง และรายละเอียดการควบคุมความปลอดภัยที่ต้องการ

20.4 ขั้นตอนการควบคุมการเปลี่ยนแปลงต้องมั่นใจได้ว่ามีการควบคุมความปลอดภัยอย่างเหมาะสม เช่น ผู้พัฒนาโปรแกรมควรได้รับสิทธิ์ในการเข้าถึงระบบเท่าที่จำเป็นสำหรับใช้ในการทำงาน และการเปลี่ยนแปลงควรได้รับการอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

21. นโยบายการบริหารจัดการเพื่อสร้างความเนื่องทางธุรกิจ (Information security continuity policy)

21.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

21.1.1 ต้องมีการกำหนดแนวทางในการสร้างความต่อเนื่องด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในกรณีที่เกิดเหตุการณ์ไม่พึงประสงค์ เช่น เหตุฉุกเฉิน หรือ วิกฤต

21.1.2 จัดให้ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ เป็นส่วนหนึ่งของกระบวนการในการบริหารจัดการความต่อเนื่องทางธุรกิจ หรือ กระบวนการในการกู้คืนระบบในภาวะวิกฤต

21.1.3 พิจารณาด้านความมั่นคงปลอดภัยสารสนเทศ ระหว่างการวางแผนความต่อเนื่องทางธุรกิจหรือการกู้คืนระบบในภาวะวิกฤต

21.2 การดำเนินการความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

21.2.1 ต้องจัดตั้งคณะทำงานแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศซึ่ง ประกอบไปด้วยตัวแทนจากหน่วยงาน เจ้าของข้อมูล เจ้าของระบบงาน และหน่วยงานที่ดูแลระบบเครือข่าย เป็นต้น

21.2.2 คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศที่เป็นลายลักษณ์อักษร

21.2.3 กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศต้องประกอบด้วยหัวข้อหลัก ดังนี้

21.2.3.1 การวิเคราะห์ผลกระทบทางธุรกิจ

21.2.3.2 การประเมินความเสี่ยงและการควบคุม

21.2.3.3 การวางกลยุทธ์สำหรับแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

21.2.3.4 การพัฒนาแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

21.2.3.5 การประชาสัมพันธ์และการฝึกอบรม

21.2.3.6 การทดสอบปรับปรุงแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ควรพิจารณาดังนี้

21.2.3.7 การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินภารกิจและการให้บริการ

21.2.3.8 การตอบสนองต่อสถานการณ์ฉุกเฉินเพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุมการแก้ไขสถานการณ์ฉุกเฉิน

21.2.3.9 การดำเนินการเพื่อให้สามารถดำเนินภารกิจได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย

21.2.3.10 ต้องมีการกลับคืนสู่การทำงานปกติเพื่อให้ภารกิจกลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ

21.2.4 แนวทางปฏิบัติของการเก็บรักษาข้อมูลและสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศผู้ใช้งานควรปฏิบัติตามแนวปฏิบัติการสำรองข้อมูลการกู้คืนและรักษาความลับของข้อมูล

21.2.4.1 เจ้าของข้อมูลเป็นผู้จัดเก็บรักษาข้อมูลเกี่ยวกับระบบซึ่งได้แก่ ข้อมูลเกี่ยวกับระบบปฏิบัติการ, ซอฟต์แวร์ระบบงาน (ทั้ง Source Code และ Executable Files) โดยให้เป็นไปตามความต้องการที่เจ้าของข้อมูลในระบบนั้นกำหนดจำนวนครั้งและระยะเวลาในการเก็บรักษาข้อมูลดังกล่าวต้องสอดคล้องกับการประเมินความเสี่ยงของข้อมูลนั้น ๆ ด้วย

21.2.4.2 ก่อนที่จะมีการปรับปรุงหรือเปลี่ยนแปลงระบบ หน่วยงานที่รับผิดชอบต้องทำการสำรองข้อมูลของระบบทุกครั้ง

21.2.4.3 ถ้าการสำรองข้อมูลถูกดำเนินการที่เซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์หลักและเป็นข้อมูลของระบบงานที่สำคัญจะต้องเพิ่มจำนวนครั้งในการสำรองข้อมูลของเซิร์ฟเวอร์นั้นด้วย

21.2.4.4 ข้อมูลและสารสนเทศที่มีความสำคัญมากจะต้องทำการสำรองข้อมูลไว้ทุกวัน และข้อมูลสำรองดังกล่าวต้องมีการจัดเก็บไว้นอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลักอย่างเหมาะสม โดยตรวจสอบให้แน่ใจว่าสถานที่นั้นมีความปลอดภัย

21.2.4.5 ระบบข้อมูลที่สำคัญทั้งหมด ควรมีระบบการประมวลผลสำรองระบบเครือข่ายสำรองเพื่อป้องกันการพึ่งพาระบบหลักเพียงระบบเดียว ในกรณีที่ระบบหนึ่งไม่สามารถทำงาน ได้สามารถใช้งานอีกระบบหนึ่งได้ทันทีเพื่อให้ภารกิจหลักดำเนินต่อไปได้

21.2.4.6 ข้อมูลและสารสนเทศที่ถูกจัดประเภทเป็นข้อมูลธรรมดาซึ่งไม่ส่งผลกระทบต่อการดำเนินกิจการ จำนวนครั้งในการสำรองข้อมูลนั้นขึ้นอยู่กับการพิจารณาของเจ้าของข้อมูล และข้อมูลดังกล่าวจะถูกนำไปจัดเก็บในสถานที่ ๆ มีความปลอดภัย

21.2.5 แนวทางปฏิบัติของการเก็บข้อมูลสำรองนอกสถานที่

21.2.5.1 ศูนย์คอมพิวเตอร์สำรองหรือสถานที่ที่ใช้ในการจัดเก็บข้อมูลสำรองควรตั้งอยู่ไกลจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะแน่ใจได้ว่าเหตุการณ์หรือภัยธรรมชาติชนิดเดียวกัน เช่น ไฟไหม้ หรือเหตุจลาจลต่าง ๆ จะไม่เกิดขึ้นกับศูนย์คอมพิวเตอร์ทั้งสองแห่งพร้อมกัน

21.2.5.2 ศูนย์คอมพิวเตอร์สำรองหรือสถานที่ที่จัดเก็บข้อมูลสำรองนอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลัก ต้องมีการรักษาความปลอดภัยทั้งในด้านกายภาพและสภาพแวดล้อมการควบคุมเช่นเดียวกันกับศูนย์คอมพิวเตอร์หลักหรือปรับเปลี่ยนตามความเหมาะสม

21.3 การตรวจสอบ สอบทาน และวัดผลความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

21.3.1 คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศที่เป็นลายลักษณ์อักษรโดยต้องมีการสอบทานและปรับปรุงแก้ไขให้ ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละหนึ่งครั้ง

22. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

22.1 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Management of Information Security Incidents and Improvements) เพื่อให้มีวิธีการที่สอดคล้อง และได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย

22.1.1 กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ ต้องมีการกำหนดหน้าที่ความรับผิดชอบและกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และขั้นตอนดังกล่าวต้องมีความรวดเร็วได้ผล และมีความเป็นระบบระเบียบที่ดี

22.1.2 การรายงานเหตุการณ์น่าสงสัย / จุดอ่อนด้านความมั่นคงปลอดภัย

22.1.2.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการรายงานเหตุการณ์ทันทีที่สงสัยว่าเป็นเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล

22.1.2.2 ถ้าหากพบเหตุการณ์ที่น่าสงสัยให้แจ้งต่อผู้รับผิดชอบทันทีเช่น เหตุการณ์ต่อไปนี้

(1) พบว่ารหัสผ่านส่วนบุคคลของตนถูกล็อคโดยไม่ทราบสาเหตุ
(2) เวลาการเข้าใช้งานระบบครั้งล่าสุดที่ผิดปกติ
(3) พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน เช่น มีไฟล์ที่ไม่รู้จักการเปลี่ยนแปลงของค่าต่าง ๆ
(4) มีการไม่ปฏิบัติตามขั้นตอนความมั่นคงปลอดภัย
(5) พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล
(6) พบหรือคาดว่าข้อมูลในระบบจะถูกทำลาย แก้ไขหรือลบทิ้ง
(7) มีความพยายามที่จะเข้าใช้ระบบอย่างผิดวิธีไม่ว่าจะสำเร็จหรือไม่
(8) การให้บริการของระบบเกิดการชะงักหรือไม่สามารถให้บริการ
(9) เกิดการละเมิดสิทธิ์เข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล
(10) การแก้ไขค่าความปลอดภัยในระบบเช่น Hardware, Software หรือ Firmware โดยผู้ใช้งานไม่ทราบ

22.1.3 การประเมินเหตุการณ์ด้านความมั่นคงปลอดภัย ผู้ดูแลระบบต้องประเมินขอบเขตและความรุนแรงของปัญหาหากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้าง รุนแรงหรือมีผลต่อชื่อเสียงจะต้องรายงานให้ ผู้บังคับบัญชาทราบโดยด่วนเพื่อหาแนวทางแก้ไขและป้องกันไม่ให้เกิดในครั้งต่อไปควรมีการแบ่งประเภทของปัญหาอย่างเหมาะสม

22.1.4 การตอบโต้ต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดและการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟต์แวร์ เพื่อลดความเสียหายจาก

เหตุการณ์ละเมิดความมั่นคงปลอดภัยและระบบทำงานบกพร่อง เช่น ไวรัสคอมพิวเตอร์แพร่กระจาย ระบบถูกบุกรุก และให้บุคลากรได้เรียนรู้จากประสบการณ์ความเสียหายดังกล่าว

22.1.4.1 หากผู้ใช้งานพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัย และ/หรือจุดอ่อนช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และ/หรือการทำงานที่บกพร่องหรือการทำงานผิดปกติของซอฟต์แวร์ ผู้ใช้งานต้องรายงานสิ่งที่เกิดขึ้นให้แก่ผู้รับผิดชอบทราบโดย เร่งด่วน

22.1.4.2 ในกรณีที่ไม่สามารถติดต่อผู้รับผิดชอบได้ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้น

22.1.4.3 ในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย ให้ปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ดังนี้

(1) ภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง มีความเสี่ยงอย่างมีนัยสำคัญที่ทำให้ระบบคอมพิวเตอร์ หรือการให้บริการของ สมอ. ด้อยประสิทธิภาพลง

(2) ภัยคุกคามทางไซเบอร์ระดับร้ายแรง ถูกโจมตีอย่างมีนัยสำคัญ ทำให้เกิดความเสียหายกับระบบคอมพิวเตอร์ หรือ การให้บริการของ สมอ. จนไม่สามารถทำงานหรือให้บริการได้

(3) ภัยคุกคามทางไซเบอร์ระดับร้ายแรงวิกฤติ ถูกโจมตีในระดับสูงส่งผลกระทบรุนแรงเป็นวงกว้างทำให้ระบบคอมพิวเตอร์ หรือการให้บริการที่ สมอ. ล้มเหลว มีความเสี่ยงที่จะลุกลามไปยังหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

22.1.5 การเรียนรู้จากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

22.1.5.1 ต้องบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย จุดอ่อนช่องโหว่ ภัยคุกคามหรือการทำงานบกพร่องของระบบสารสนเทศรวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

22.1.5.2 ระบบต้องจัดทำสรุปรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัยให้รับทราบ อย่างน้อยเดือนละ 1 ครั้ง

22.1.6 การเก็บรวบรวมหลักฐาน

22.1.6.1 ต้องกำหนดให้มีการรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในการวิเคราะห์สืบสวนหรือเป็นหลักฐานในกระบวนการทางศาลที่เกี่ยวข้องเมื่อพบว่า เหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

22.1.6.2 ส่วนงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่า ได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบหรือข้อบังคับ

ที่ได้กำหนดไว้โดยมีระยะเวลาจัดเก็บตาม ความสำคัญของข้อมูลและกฎหมาย เช่น 90 วัน หรือ 1 ปี

22.1.6.3 ต้องศึกษาถึงลักษณะของหลักฐานที่มีความสมบูรณ์และมีคุณภาพเพื่อสามารถนำไปใช้ในกระบวนการของศาลได้

ภาคผนวก

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ - นามสกุล	ตำแหน่ง	ลายมือชื่อ	วันที่
จัดทำโดย				
ทบทวน				
อนุมัติ				

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

แผนกลยุทธ์และแผนที่นำทาง
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Strategy Plan and Roadmap)

จัดทำโดย บริษัท เอเชี่ยน อินเทลลีเจนท์ อินฟอร์เมชั่น เทคโนโลยี จำกัด

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

แผนการตรวจสอบและประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Audit Plan)

จัดทำโดย บริษัท เอเชี่ยน อินเทลลีเจนท์ อินฟอร์เมชั่น เทคโนโลยี จำกัด

แบบฟอร์มการวางแผนการตรวจประเมิน (Audit Plan Form)

หมายเลขอ้างอิง : .....

1. ขอบเขตการตรวจประเมิน (Audit Scope)

ผู้ตรวจสอบ:	ผู้นำทีม: ทีมผู้ตรวจ: ทีมผู้ตรวจ:
ขอบเขตการตรวจ:	การรักษาความมั่นคงปลอดภัยไซเบอร์ และเอกสารต่าง ๆ ที่เกี่ยวข้อง
มาตรฐานที่ใช้:	พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
พื้นที่การตรวจ:	

2. ข้อมูลผู้ขอรับการตรวจประเมิน (Client Information)

บุคคลติดต่อ:	
สถานที่:	
เบอร์โทรศัพท์:	
อีเมล:	
แผนกที่เกี่ยวข้อง / บริการที่เกี่ยวข้อง	

3. กำหนดการตรวจประเมิน (Audit Schedule)

ช่วงเวลา	พื้นที่	ผู้ตรวจ	ผู้ถูกตรวจ
1st Day: DD/MM/YYYY			
9:00-12.00	ตรวจวิธีการประเมินความเสี่ยง และผลการประเมินความเสี่ยง	ทีมผู้ตรวจ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่เกี่ยวข้อง
12:00-13:00	พักเบรก		
13.00-16.00	ตรวจแผนและผลการควบคุมความเสี่ยงทั้งหมด	ทีมผู้ตรวจ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่เกี่ยวข้อง
2nd Day: DD/MM/YYYY			

ช่วงเวลา	พื้นที่	ผู้ตรวจ	ผู้ถูกตรวจ
09:00-12:00	ตรวจนโยบายและแนวทางปฏิบัติ (เอกสารทั้งหมด)	ทีมผู้ตรวจ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่เกี่ยวข้อง
12:00-13:00	พักเบรก		
13.00-16.00	ตรวจผลการปฏิบัติตามนโยบายและแนวทางปฏิบัติ ในหัวข้อ 1. นโยบายอุปกรณ์แบบพกพา (Mobile device policy) 2. นโยบายการปฏิบัติงานจากระยะไกล (Teleworking Policy) 3. นโยบายการควบคุมการเข้าถึง (Access control policy) 4. นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls) 5. นโยบายการบริหารจัดการกุญแจ (Key Management Policy) 6. นโยบายการควบคุมการเข้าถึงทางกายภาพ (Physical Control Policy) 7. นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy) 8. นโยบายการสำรองข้อมูล (Backup Policy) 9. นโยบายการถ่ายโอนสารสนเทศ (Information transfer policy) 10. นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy) 11. ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)	ทีมผู้ตรวจ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่เกี่ยวข้อง

ช่วงเวลา	พื้นที่	ผู้ตรวจ	ผู้ถูกตรวจ
3rd. Day: DD/MM/YYYY			
09.00-12.00	ตรวจผลการปฏิบัติตามนโยบายและแนวทางปฏิบัติ ในหัวข้อ 12. นโยบายการจัดชั้นความลับ (Information classification policy) 13. นโยบายการจัดการสื่อบันทึกข้อมูล (Media Handling policy) 14. การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software) 15. การบริหารจัดการช่องโหว่ (Technical Vulnerability Management) 16. นโยบายการควบคุมการเปลี่ยนแปลงระบบ (System Change Control Policy) 17. นโยบายการบริหารจัดการเพื่อสร้างความเนื่องทางธุรกิจ (Information security continuity policy)	ทีมผู้ตรวจ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่เกี่ยวข้อง
12:00-13:00	พักเบรก		
13.00-14.00	ตรวจผลการปฏิบัติตามนโยบายและแนวทางปฏิบัติ ในหัวข้อ 18. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)	ทีมผู้ตรวจ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่เกี่ยวข้อง
14.00-15.00	เตรียมรายงานการตรวจ และสรุปผลการตรวจสำหรับประชุมปิดการตรวจ	ทีมผู้ตรวจ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่เกี่ยวข้อง
15.00-16.00	ประชุมปิดตรวจ และสรุปผลการตรวจสอบในเบื้องต้น	ทีมผู้ตรวจ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่เกี่ยวข้อง

สารบัญ

เรื่อง **หน้า**

1. แผนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อ้างอิงมาตรฐาน NIST (National Institute of Standards and Technology)

การระบุ (IDENTIFY)	การป้องกัน (PROTECT)	การตรวจจับ (DETECT)	การตอบสนอง(RESPOND)	การกู้คืน (RECOVERY)
การบริหารจัดการทรัพย์สิน (Asset Management)	การบริหารจัดการผู้ใช้งาน การพิสูจน์ตัวตน และการควบคุมการเข้าถึง (Identity Management, Authentication and Access Control)	ความผิดปกติและเหตุการณ์ (Anomalies and Events)	การวางแผนการตอบสนอง (Response Planning)	การวางแผนการกู้คืน (Recovery Planning)
สภาพแวดล้อมทางธุรกิจ (Business Environment)	การสร้างความตระหนัก และการอบรม (Awareness and Training)	การติดตามความปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring)	การสื่อสาร (Communications)	การปรับปรุง (Improvements)
Governance	ความปลอดภัยของข้อมูล (Data Security)	ขั้นตอนการตรวจจับ (Detection Processes)	การวิเคราะห์ (Analysis)	การสื่อสาร (Communications)
การประเมินความเสี่ยง (Risk Assessment)	ขั้นตอนและแนวทางปฏิบัติในการป้องกันสารสนเทศ (Information Protection Processes & Procedures)	-	การบรรเทา (Mitigation)	-
กลยุทธ์ในการบริหารจัดการความเสี่ยง (Risk Management Strategy)	การซ่อมบำรุง (Maintenance)	-	การปรับปรุง (Improvements)	-

การระบุ (IDENTIFY)	การป้องกัน (PROTECT)	การตรวจจับ (DETECT)	การตอบสนอง(RESPOND)	การกู้คืน (RECOVERY)
Supply Chain Risk Management	เทคโนโลยีในการป้องกัน (Protective Technology)	-	-	-

1.1 กลยุทธ์ที่เกี่ยวข้องกับการระบุสภาพแวดล้อมพื้นฐานเพื่อให้มีความมั่นคงปลอดภัย (IDENTIFY)

การระบุ (IDENTIFY)	เอกสารอ้างอิง
การบริหารจัดการทรัพย์สิน (Asset Management)	- นโยบายการจัดชั้นความลับ - นโยบายการควบคุมการเข้าถึงทางกายภาพ 9.1.6 การจัดเตรียมพื้นที่สำหรับส่งมอบ 9.2.5 การนำทรัพย์สินออกนอกสถานที่ 9.2.6 ความปลอดภัยของอุปกรณ์และทรัพย์สินภายนอกสถานที่
สภาพแวดล้อมทางธุรกิจ (Business Environment)	- ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก
การกำกับดูแล (Governance)	- นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์
การประเมินความเสี่ยง (Risk Assessment)	- แนวทางปฏิบัติการประเมินความเสี่ยง
กลยุทธ์ในการบริหารจัดการความเสี่ยง (Risk Management Strategy)	- แนวทางปฏิบัติการประเมินความเสี่ยง
การบริหารจัดการความเสี่ยงห่วงโซ่อุปทาน (Supply Chain Risk Management)	- แนวทางปฏิบัติการประเมินความเสี่ยง

1.2 กลยุทธ์ที่เกี่ยวข้องกับการป้องกันไม่ให้มีการละเมิดความมั่นคงปลอดภัย (PROTECT)

การป้องกัน (PROTECT)	อ้างอิงเอกสาร
การบริหารจัดการผู้ใช้งาน การพิสูจน์ตัวตน และการควบคุมการเข้าถึง (Identity Management, Authentication and Access Control)	- นโยบายการควบคุมการเข้าถึง
การสร้างความตระหนัก และการอบรม (Awareness and Training)	- จัดให้มีการสร้างความตระหนัก การสื่อสาร ความมั่นคงปลอดภัยไซเบอร์ เป็นประจำ อย่างสม่ำเสมอ
ความปลอดภัยของข้อมูล (Data Security)	- นโยบายการใช้มาตรการเข้ารหัสข้อมูล - นโยบายการบริหารจัดการกุญแจ - นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และการป้องกันหน้าจอคอมพิวเตอร์ - นโยบายการจัดการสื่อบันทึกข้อมูล
ขั้นตอนและแนวทางปฏิบัติในการป้องกันสารสนเทศ (Information Protection Processes & Procedures)	- นโยบายการควบคุมการเข้าถึงทางกายภาพ - นโยบายการสำรองข้อมูล - นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย - นโยบายการควบคุมการเปลี่ยนแปลงระบบ - การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ
การซ่อมบำรุง (Maintenance)	- นโยบายการปฏิบัติงานจากระยะไกล
เทคโนโลยีในการป้องกัน (Protective Technology)	- นโยบายอุปกรณ์แบบพกพา - นโยบายการถ่ายโอนสารสนเทศ

1.3 กลยุทธ์ที่เกี่ยวข้องกับการตรวจจับเหตุการณ์ละเมิดความมั่นคงปลอดภัย (DETECT)

การตรวจจับ (DETECT)	อ้างอิงเอกสาร
ความผิดปกติและเหตุการณ์ (Anomalies and Events)	- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
การติดตามความปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring)	- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ - การบริหารจัดการช่องโหว่
ขั้นตอนการตรวจจับ (Detection Processes)	- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

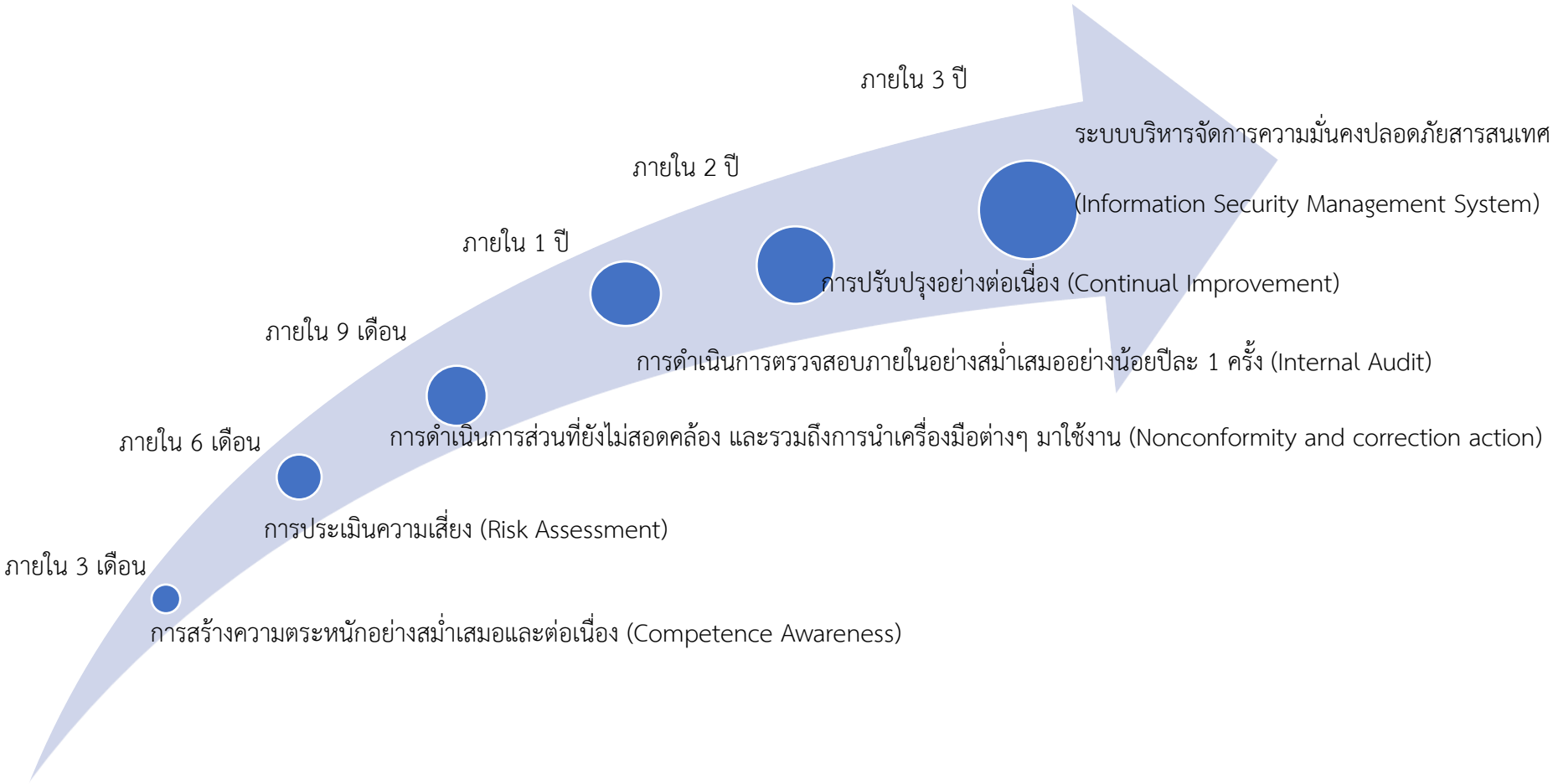
1.4 กลยุทธ์ที่เกี่ยวข้องกับการตอบสนองเหตุการณ์ละเมิดความมั่นคงปลอดภัย (RESPOND)

การตอบสนอง (RESPOND)	อ้างอิงเอกสาร
การวางแผนการตอบสนอง (Response Planning)	- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
การสื่อสาร (Communications)	- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
การวิเคราะห์ (Analysis)	- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
การบรรเทา (Mitigation)	- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
การปรับปรุง (Improvements)	- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

1.5 กลยุทธ์ที่เกี่ยวข้องกับการกู้คืนเพื่อกลับไปสู่สภาวะปกติ (RECOVERY)

การกู้คืน (RECOVERY)	อ้างอิงเอกสาร
การวางแผนการกู้คืน (Recovery Planning)	- นโยบายการบริหารจัดการความต่อเนื่องทางธุรกิจ
การปรับปรุง (Improvements)	- นโยบายการบริหารจัดการความต่อเนื่องทางธุรกิจ
การสื่อสาร (Communications)	- นโยบายการบริหารจัดการความต่อเนื่องทางธุรกิจ

2. แผนที่นำทาง (Roadmap)



2.1 แผนที่นำทางประกอบด้วย

แผนระยะสั้น ในช่วง 3 - 6 เดือน สมอ. ต้องสร้างความตระหนักอย่างสม่ำเสมอและต่อเนื่องตลอดไปให้กับบุคลากรที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศทุกระดับเพื่อให้ความรู้ ความเข้าใจ และเสริมสร้างการป้องกันภัยคุกคามทางไซเบอร์ได้

แผนระยะกลาง ในช่วง 9 เดือน ถึง 2 ปี สมอ. ต้องดำเนินการส่วนที่ยังไม่สอดคล้องจากผลการประเมินความเสี่ยงช่องว่าง (GAP) ทั้งหมดที่เกิดขึ้น รวมถึงการนำ Tool หรือ Technology มาเสริมสร้างการควบคุมและการป้องกันภัยคุกคามไซเบอร์ได้ และต้องการวัดผลการบริหารจัดการในกระบวนการต่าง ๆ เพื่อให้ได้ผลลัพธ์การปฏิบัติงานที่มีประสิทธิภาพและประสิทธิผล และต้องมีการตรวจสอบภายในอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เพื่อเป็นการตรวจสอบการดำเนินการให้มีความสอดคล้องให้มากยิ่งขึ้น

แผนระยะยาว ในช่วง 2 - 3 ปี สมอ. ต้องมีการทบทวนผลการประเมินความเสี่ยง และผลการตรวจสอบภายในเพื่อให้ได้การปรับปรุงอย่างต่อเนื่องและให้ได้ระบบบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์อย่างสมบูรณ์

3. แผนปฏิบัติงาน (Action Plan / Implementation Plan) เพื่อรับมือจากภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ ในระยะสั้น ระยะกลาง และระยะยาว

แผนปฏิบัติงานรับมือภัยคุกคามทางไซเบอร์	ระยะสั้น	ระยะกลาง	ระยะยาว
ภัยคุกคามระดับไม่ร้ายแรง	**People** - จัดเตรียมคนให้มีความรู้เพื่อพร้อมรับมือกับภัยคุกคามทางไซเบอร์	**People** - จัดเตรียมคนให้มีความรู้เพื่อพร้อมรับมือกับภัยคุกคามทางไซเบอร์ **Process** - จัดเตรียมคู่มือปฏิบัติงานสำหรับรับมือกับภัยคุกคามทางไซเบอร์	**People** - จัดเตรียมคนให้มีความรู้เพื่อพร้อมรับมือกับภัยคุกคามทางไซเบอร์ **Process** - จัดเตรียมคู่มือปฏิบัติงานสำหรับรับมือกับภัยคุกคามทางไซเบอร์ **Technology** - จัดเตรียมอุปกรณ์หรือเครื่องมือให้พร้อมรับมือกับภัยคุกคามทางไซเบอร์
ภัยคุกคามระดับร้ายแรง	**People** - จัดเตรียมคนให้มีความรู้และทักษะเพื่อพร้อมรับมือกับภัยคุกคามทางไซเบอร์	**People** - จัดเตรียมคนให้มีความรู้และทักษะเพื่อพร้อมรับมือกับภัยคุกคามทางไซเบอร์	**People** - จัดเตรียมคนให้มีความรู้และทักษะเพื่อพร้อมรับมือกับภัยคุกคามทางไซเบอร์

แผนปฏิบัติงานรับมือภัยคุกคามทางไซเบอร์	ระยะสั้น	ระยะกลาง	ระยะยาว
		Process - จัดเตรียมคู่มือปฏิบัติงานสำหรับรับมือกับภัยคุกคามทางไซเบอร์ - จัดเตรียมแผนรองรับภัยคุกคามทางไซเบอร์	**Process** - จัดเตรียมคู่มือปฏิบัติงานสำหรับรับมือกับภัยคุกคามทางไซเบอร์ - จัดให้มีการซ้อมแผนรองรับภัยคุกคามทางไซเบอร์ **Technology** - จัดเตรียมอุปกรณ์หรือเครื่องมือให้พร้อมรับมือกับภัยคุกคามทางไซเบอร์
ภัยคุกคามระดับวิกฤติ	**People** - จัดเตรียมคนให้มีความรู้และทักษะ รวมถึงประสานงานกับที่ปรึกษาเพื่อให้ข้อมูลสำหรับการรับมือกับภัยคุกคามทางไซเบอร์	**People** - จัดเตรียมคนให้มีความรู้และทักษะ รวมถึงประสานงานกับที่ปรึกษาเพื่อให้ข้อมูลสำหรับการรับมือกับภัยคุกคามทางไซเบอร์ **Process** - จัดเตรียมคู่มือปฏิบัติงานสำหรับรับมือกับภัยคุกคามทางไซเบอร์	**People** - จัดเตรียมคนให้มีความรู้และทักษะ รวมถึงประสานงานกับที่ปรึกษาเพื่อให้ข้อมูลสำหรับการรับมือกับภัยคุกคามทางไซเบอร์ **Process** - จัดเตรียมคู่มือปฏิบัติงานสำหรับรับมือกับภัยคุกคามทางไซเบอร์ - จัดให้มีการซ้อมแผนรองรับภัยคุกคามทางไซเบอร์

แผนปฏิบัติงานรับมือภัยคุกคามทางไซเบอร์	ระยะสั้น	ระยะกลาง	ระยะยาว
		- จัดเตรียมแผนรองรับภัยคุกคามทางไซเบอร์	- จัดให้มีการประเมินความเสี่ยงแผนการรับมือภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง **Technology** - จัดเตรียมอุปกรณ์หรือเครื่องมือให้พร้อมรับมือกับภัยคุกคามทางไซเบอร์