กรมการขนส่งทางราง
Department of Rail Transport

ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมการขนส่งทางราง

โครงการจ้างที่ปรึกษาพัฒนาแนวการกำกับดูแลผู้ให้บริการขนส่งทางรางและจัดทำมาตรการความมั่นคงปลอดภัยไซเบอร์ของกรมการขนส่งทางรางตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มีนาคม ๒๕๖๙

รายละเอียดการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชัน	วันที่อนุมัติ	ผู้อนุมัติ	รายละเอียด
๑	๑.๐	๑๐ มิถุนายน ๒๕๖๗	นายอธิภู จิตรานุเคราะห์ (CISO)	จัดทำเล่มครั้งแรก
๒	๒.๐	๓๐ มีนาคม ๒๕๖๙	นายพิเชฐ คุณาธรรมรักษ์ (DCIO)	ปรับปรุงเอกสาร

สารบัญ

บทสรุปผู้บริหาร (EXECUTIVE SUMMARY) ๑
๑. บทนำ ๓
๑.๑ ความเป็นมาของโครงการ ๓
๒. กรอบแนวคิดในการดำเนินงาน ๙
๒.๑ ความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๙
๒.๒ ความรู้ความเข้าใจด้านการประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และด้านการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ๑๓
๒.๒.๑ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๑๓
๒.๒.๒ การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ๑๕
๓. ประมวลแนวทางปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. ๑๗
บทที่ ๑ บทนำ ๑๗
๑. หลักการและเหตุผล ๑๗
๒. วัตถุประสงค์ ๑๗
๓. ขอบเขต ๑๗
๔. คำนิยาม ๑๗
บทที่ ๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๐
๒.๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) ๒๐
๒.๒ กรอบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System - ISMS) ๒๕
บทที่ ๓ การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity) ๒๙
บทที่ ๔ ประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. ๓๒
(A) แนวทางการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment and Risk Management Strategy) ๓๒
(B) แนวทางการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) ๔๑
(C) การจัดการทรัพย์สิน (Asset Management) ๔๒
(D) การควบคุมการเข้าถึง (Access Control) ๕๒
(E) การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ๖๔
(F) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ๗๖
(G) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ๗๙
(H) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) ๙๓

(I) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)..... ๙๓
(J) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)..... ๙๔
(K) การเชื่อมต่อระยะไกล (Remote Connection)..... ๙๘
(L) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)..... ๑๐๓
(M) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)..... ๑๐๖
(N) การจัดการผู้ให้บริการภายนอก (Third Party Management)..... ๑๑๑
(O) การแบ่งปันข้อมูล (Information Sharing) ๑๒๘
(P) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)..... ๑๓๖
บทที่ ๕ การจำแนกหมวดหมู่ภัยคุกคามทางไซเบอร์ และการรายงานภัยคุกคามทางไซเบอร์..... ๑๔๔
๔. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมการขนส่งทางราง พ.ศ. ๒๕๖๘ ๑๔๗
ข้อ ๑ คำนิยาม..... ๑๔๗
หมวดที่ ๑ นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ๑๕๐
ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)..... ๑๕๐
ส่วนที่ ๒ การบริหารจัดการเข้าถึงของผู้ใช้งาน (User Access Management) ๑๕๓
ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) ๑๕๖
ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Asset Management)..... ๑๕๙
ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)..... ๑๖๓
ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) ๑๖๖
ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)..... ๑๖๘
ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malware).... ๑๗๐
ส่วนที่ ๙ การปฏิบัติงานจากภายนอก ขร. (Teleworking) และการเชื่อมต่อระยะไกล (Remote Connection) ๑๗๒
ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) ๑๗๓
ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)..... ๑๗๔
ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (e-Mail) ๑๗๕
ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)..... ๑๗๖
ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล..... ๑๗๘
ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา และการใช้งานอุปกรณ์คอมพิวเตอร์พกพาและสื่อเก็บข้อมูลแบบถอดได้..... ๑๗๙

ส่วนที่ ๑๖ การป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี (Malicious Code Protection) ๑๘๑
ส่วนที่ ๑๗ การบริหารจัดการข่าวกรองภัยคุกคาม และช่องโหว่ทางเทคนิค (Threat Intelligence and Technical Vulnerability Management) ๑๘๒
ส่วนที่ ๑๘ การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy) ๑๘๕
ส่วนที่ ๑๙ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration) ๑๘๖
ส่วนที่ ๒๐ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และการเฝ้าระวัง (Logging and Monitoring) ๑๘๘
หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูล ข้อมูลและสำรองข้อมูล ๑๘๙
ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล ๑๘๙
ส่วนที่ ๒ การสำรองข้อมูล ๑๙๑
ส่วนที่ ๓ การบริหารจัดการสื่อบันทึกข้อมูลสำรอง (Removeable Media) ๑๙๓
ส่วนที่ ๔ การเข้ารหัสข้อมูล (Cryptography) ๑๙๔
ส่วนที่ ๕ การป้องกันข้อมูลรั่วไหล (Data Leakage Prevention) ๑๙๖
หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ๑๙๗
ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง ๑๙๗
ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ๑๙๙
หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม ๒๐๑
หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ ๒๐๕
ส่วนที่ ๑ การตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศสำหรับ ขร. . ๒๐๕
ส่วนที่ ๒ การควบคุม หรือกำกับดูแล เพื่อตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ และไซเบอร์ ของหน่วยงานที่อยู่ภายใต้การควบคุมหรือกำกับดูแล ๒๐๙
หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ๒๑๑
หมวดที่ ๗ หน้าที่และความรับผิดชอบ ๒๑๓
หมวดที่ ๘ การบริหารจัดการการใช้บริการจากหน่วยงานภายนอก ๒๑๔
หมวดที่ ๙ การบริหารความต่อเนื่อง ๒๑๘
หมวดที่ ๑๐ การเผยแพร่และทบทวน ๒๒๑
๕. แผนรับมือภัยคุกคามทางไซเบอร์ (CYBER INCIDENT RESPONSE PLAN) ของ ขร. ๒๒๒
๑. หลักการและเหตุผล ๒๒๒
๒. วัตถุประสงค์ ๒๒๒
๓. ขอบเขต ๒๒๒
๔. หน้าที่การทบทวนแผน ๒๒๒
๕. หน้าที่ในการดำเนินการตามแผน ๒๒๒

๗. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง ๒๒๓
๘. คำนิยาม ๒๒๔
๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ๒๒๔
๑๐.ลักษณะของภัยคุกคามทางไซเบอร์ และปัจจัยที่ใช้ในการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับ .. ๒๓๒
๑๑. รูปแบบภัยคุกคามไซเบอร์ ๒๓๒
๑๒. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ ๒๓๔
๑๓. ขั้นตอนการรับมือ ๒๓๕
๑๔. การสื่อสารและรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ ๒๔๔
๑๕. การฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ ๒๔๕
เอกสาร และข้อมูลประกอบ ๒๔๖

บทสรุปผู้บริหาร (Executive Summary)

การบริหารจัดการภาครัฐในปัจจุบันมีการผลักดันให้ประเทศไทยไปสู่ยุคดิจิทัล โดยการนำเทคโนโลยีเข้ามาช่วยในการบริหารจัดการ และสนับสนุนการทำงานรวมไปถึงการให้บริการกับประชาชน เพื่อความสะดวก รวดเร็ว และทันต่อเหตุการณ์ต่าง ๆ ทำให้มีการใช้งานอินเทอร์เน็ต ระบบงานต่าง ๆ อย่างแพร่หลาย ซึ่งการนำเทคโนโลยีมาใช้งานทำให้ก่อให้เกิดภัยคุกคามไซเบอร์ และก่อให้เกิดอาชญากรรมในรูปแบบที่หลากหลาย จึงต้องดำเนินการบริหารจัดการข้อมูล กำหนดมาตรการป้องกัน เพื่อไม่ให้ข้อมูลที่เป็นความลับและข้อมูลที่สำคัญเกิดการรั่วไหล หรือการกระทำอื่น ๆ ที่ทำให้เกิดความเสียหายที่ไม่สามารถประเมินค่าได้ หน่วยงานภาครัฐซึ่งเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ จึงต้องดำเนินการกำหนดมาตรการควบคุมทางไซเบอร์ และเพื่อให้การดำเนินการสอดคล้องตามตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงกฎหมายรองที่เกี่ยวข้อง

กรมการขนส่งทางราง (ขร.) ในฐานะหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศด้านการให้บริการขนส่งทางราง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๕ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงการกำหนดหน้าที่ความรับผิดชอบของหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ข้อ ๕ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. ๒๕๖๗

ดังนั้น ขร. จึงจำเป็นต้องจัดทำโครงการร่วมกับที่ปรึกษาดำเนินการจัดทำแนวปฏิบัติ กรอบมาตรฐานสำหรับ ขร. และจัดทำแนวปฏิบัติ กรอบมาตรฐานสำหรับผู้ให้บริการขนส่งทางราง เพื่อให้การดำเนินการสอดคล้องกับอำนาจหน้าที่ตามกฎหมายกำหนด โดยมีรายละเอียดการดำเนินงาน ดังนี้

๑. จัดทำคู่มือปฏิบัติงานของ ขร. ด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับ ขร. ประกอบด้วย
   - ประมวลทางแนวปฏิบัติ
   - กรอบมาตรฐาน
   - คู่มือการใช้งานระบบฐานข้อมูลสำหรับจัดเก็บข้อมูลการติดตามการปฏิบัติงานมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับ ขร.
   - แนวปฏิบัติในการบริหารความเสี่ยง (Risk Management) ด้านความมั่นคงปลอดภัยไซเบอร์
   - จัดทำแนวปฏิบัติสำหรับการจัดทำสรุปรายงานการบริหารความเสี่ยง (Risk Management) ด้านความมั่นคงปลอดภัยไซเบอร์ และสรุปรายงานผลการตรวจสอบ (Audit) ด้านความมั่นคงปลอดภัยไซเบอร์

๒. จัดทำแนวปฏิบัติ และกรอบมาตรฐานสำหรับผู้ให้บริการขนส่งทางราง ประกอบด้วย

๑) มาตรฐานความมั่นคงปลอดภัยไซเบอร์ของระบบการขนส่งทางราง (cybersecurity in railway) และจัดหาระบบ เพื่อจัดเก็บข้อมูลการปฏิบัติงานด้านความมั่นคงปลอดภัย สำหรับผู้ให้บริการขนส่งทางราง พร้อมทั้งจัดทำคู่มือการใช้งานระบบฐานข้อมูลการติดตามการปฏิบัติตามมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร.

๒) คู่มือปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง ประกอบด้วย

- ประมวลแนวทางปฏิบัติ
- กรอบมาตรฐาน
- มาตรฐานขั้นต่ำ
- แบบฟอร์มการตรวจประเมิน

๓) ดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง

๑. บทนำ

๑.๑ความเป็นมาของโครงการ

ด้วยนโยบายด้านการบริหารจัดการภาครัฐ และการผลักดันให้ประเทศไทยไปสู่ยุคดิจิทัล โดยการนำเทคโนโลยีเข้ามาช่วยในการบริหารจัดการ การสนับสนุนการทำงานรวมไปถึงการให้บริการกับประชาชน เพื่อความสะดวกรวดเร็ว และทันต่อเหตุการณ์ต่าง ๆ ทำให้มีการใช้งานอินเทอร์เน็ต ระบบงานต่าง ๆ อย่างแพร่หลาย ทั้งนี้ ข้อมูลต่าง ๆ ของทางภาครัฐได้ถูกเข้าสู่ระบบโลกออนไลน์เป็นจำนวนมาก มีการแลกเปลี่ยน หมุนเวียน และส่งต่อข้อมูลดังกล่าวทุกเวลา อีกทั้ง เทคโนโลยียังถูกนำมาใช้เป็นเครื่องมือในการก่อให้เกิดภัยคุกคามไซเบอร์ การก่อให้เกิดอาชญากรรมในรูปแบบที่หลากหลาย การบริหารจัดการข้อมูล การป้องกัน เพื่อไม่ให้ข้อมูลที่เป็นความลับและข้อมูลที่สำคัญเพื่อไม่ให้ข้อมูลรั่วไหล กระทำการเพื่อให้เกิดความเสียหายที่ไม่สามารถประเมินค่าได้ หน่วยงานภาครัฐซึ่งเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ เมื่อนำเทคโนโลยีมาใช้ในการขับเคลื่อนองค์กร จึงไม่อาจละเลยกับภัยคุกคามด้านไซเบอร์ รวมถึงการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

กรมการขนส่งทางราง (ขร.) ในฐานะหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศด้านการให้บริการขนส่งทางรางต้องปฏิบัติตามกฎหมาย ดังนี้

๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำ หรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าว ยังไม่มี หรือมีแต่ไม่ครบถ้วน หรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

มาตรา ๔๕ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

ในกรณีที่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่อาจดำเนินการหรือปฏิบัติตามวรรคหนึ่งได้ สำนักงานอาจให้ความช่วยเหลือด้านบุคลากรหรือเทคโนโลยีแก่หน่วยงานนั้นตามที่ร้องขอได้

มาตรา ๕๓ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน หากพบว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่ได้มาตรฐาน ให้หน่วยงานควบคุมหรือกำกับดูแลนั้น รีบแจ้งให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต่ำกว่ามาตรฐานแก้ไขให้ได้มาตรฐานโดยเร็ว หากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นยังคงเพิกเฉย ไม่ดำเนินการหรือไม่ดำเนินการให้แล้วเสร็จภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลส่งเรื่องให้ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) พิจารณาโดยไม่ชักช้า

เมื่อได้รับคำร้องเรียนตามวรรคหนึ่ง หาก กกม. พิจารณาแล้วเห็นว่า มีเหตุดังกล่าวและอาจทำให้เกิดภัยคุกคามทางไซเบอร์ ให้ กกม. ดำเนินการ ดังต่อไปนี้

(๑) กรณีเป็นหน่วยงานของรัฐ ให้แจ้งต่อผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหารสั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

(๒) กรณีเป็นหน่วยงานเอกชน ให้แจ้งไปยังผู้บริหารระดับสูงสุดของหน่วยงาน ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว ให้เลขาธิการดำเนินการติดตามเพื่อให้เป็นไปตามความในวรรคสองด้วย

มาตรา ๕๔ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง

ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวัน นับแต่วันที่ดำเนินการแล้วเสร็จ

มาตรา ๕๖ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแลและตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการ หรือ กกม. กำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

มาตรา ๕๗ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ทั้งนี้ กกม. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

๒. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่องหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. ๒๕๖๗ มีการกำหนดหน้าที่ความรับผิดชอบของหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ดังนี้

ข้อ ๕ ให้หน่วยงานควบคุมหรือกำกับดูแล มีหน้าที่ดังต่อไปนี้

(๑) กำหนดมาตรฐานที่เหมาะสมในการรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน โดยต้องสอดคล้องและไม่ต่ำกว่ามาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด

(๒) กำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน เฉพาะบริการที่เป็นภารกิจหรือให้บริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Services) ตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ ของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ให้อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยที่ยอมรับได้ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นและเป็นไปตามมาตรฐานที่เหมาะสมตาม (๑) ของประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. ๒๕๖๗ และมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนดด้วย

(๓) ตรวจสอบการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน ให้เป็นไปตามมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด และจัดทำรายงานสรุปผลการตรวจสอบให้แก่สำนักงานภายใน ๓๐ วัน หลังกระบวนการตรวจสอบเสร็จสิ้น ทั้งนี้ ในการดำเนินการดังกล่าว ให้หน่วยงานควบคุมหรือกำกับดูแล แต่งตั้งกลุ่มบุคคลทำหน้าที่เป็นผู้ตรวจสอบ อันประกอบไปด้วยหัวหน้าทีมผู้ตรวจสอบ (Lead Auditor) และผู้ตรวจสอบ (Auditor) ที่มีความรู้ความเชี่ยวชาญด้านการตรวจสอบเรื่องความมั่นคงปลอดภัยไซเบอร์ ในกรณีที่พบว่าการดำเนินการไม่เป็นไปตามมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแล แจ้งหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแก้ไขให้ได้มาตรฐาน พร้อมทั้งกำหนดเวลาให้ดำเนินการหากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่ดำเนินการภายในระยะเวลาที่กำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้ง กกม. เพื่อดำเนินการตามมาตรา ๕๓ วรรคสอง ของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ต่อไป

(๔) ให้ความช่วยเหลือ สนับสนุน หรือประสานงานในการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน เมื่อมีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ ของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ด้านใดแล้ว ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้งการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านดังกล่าว พร้อมกับรายชื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การดูแลและข้อมูลอื่น ๆ ที่เกี่ยวข้อง ให้สำนักงานทราบภายใน ๓๐ วัน นับแต่วันที่จัดตั้ง

(๕) ให้ความช่วยเหลือ สนับสนุน หรือประสานงานในการประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน

(๖) ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และดำเนินการให้เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด

(๗) จัดทำเอกสารดังต่อไปนี้ของหน่วยงานของตนให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติให้แล้วเสร็จภายในระยะเวลา ๑ ปี นับแต่วันที่ประกาศนี้มีผลใช้บังคับ

(ก) ประมวลแนวทางปฏิบัติ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์

(ข) กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย การระบุความเสี่ยงที่อาจจะเกิดขึ้น มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ และมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

(๘) จัดให้มีการทบทวนเพื่อปรับปรุงหรือแก้ไขเพิ่มเติมนโยบาย มาตรฐานและประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ของหน่วยงาน อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อการปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน

(๙) เข้าร่วมการดำเนินการ ประสานงาน และให้การสนับสนุน กกม. ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖ ของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๑๐) แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ พร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาหกสิบนาที เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปยังสำนักงาน ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงานทราบภายในระยะเวลา ๑๕ วัน นับแต่วันที่มีการเปลี่ยนแปลง

(๑๑) รับแจ้งและเก็บรักษาข้อมูลรายชื่อและข้อมูลการติดต่อของเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ และของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ที่ได้รับจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ปลอดภัย

(๑๒) เก็บรักษาข้อมูลที่จำเป็นของหน่วยงานที่ได้รับการแต่งตั้งหรือถูกยกเลิกจากการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑๓) รับแจ้งข้อมูลจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้ที่อยู่ในการควบคุมหรือกำกับดูแลของตน และดำเนินการรวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และดำเนินการตามที่กำหนดในมาตรา ๕๙ ของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เมื่อปรากฏภัยคุกคามทางไซเบอร์แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกิดขึ้น

(๑๔) ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติ และในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการต่อไปนี้ด้วย

(ก) เก็บรักษาข้อมูลและพยานหลักฐานตามที่กำหนดในขั้นตอนที่ ๒ การตรวจจับและวิเคราะห์ (Detection and Analysis) ของเอกสารแนบ ๓ แนวทางการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อแผนการรับมือภัยคุกคามทางไซเบอร์ และแนวทางการจัดทำ

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อมาตรการเผชิญเหตุ เมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ท้ายประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) แจ้งเหตุไปยังสำนักงานภายในระยะเวลาและปฏิบัติตามหลักเกณฑ์และวิธีการตามที่กำหนดในประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗ ของ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(ค) ให้ความร่วมมือกับพนักงานเจ้าหน้าที่ตาม ในการปฏิบัติการตามมาตรา ๖๖ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงให้ความร่วมมือกับพนักงานเจ้าหน้าที่หรือเจ้าหน้าที่อื่นที่เกี่ยวข้อง ในการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเกี่ยวกับภัยคุกคามทางไซเบอร์

(๑๕) รับทราบและให้ความเห็นหรือข้อเสนอแนะเกี่ยวกับระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำก่อนส่งให้แก่สำนักงาน

(๑๖) จัดทำรายงานประจำปี และส่งรายงานดังกล่าวให้สำนักงาน ภายในวันที่ ๓๑ มกราคม ของปีถัดไป โดยรายงานต้องมีรายละเอียดดังต่อไปนี้

(ก) ระบุจำนวนและลักษณะของเหตุการณ์ภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน ตามแบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี ที่กำหนดท้ายประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(ข) วิเคราะห์สาเหตุหรือผลกระทบที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(ค) ปัญหาและอุปสรรคในการดำเนินงาน

(ง) ข้อเสนอแนะต่าง ๆ ซึ่งรวมถึงข้อเสนอแนะเชิงนโยบายหากหน่วยงานเป็นทั้งหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีภารกิจหรือการให้บริการตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ให้จัดทำรายงานโดยรวมข้อมูลของตนในบทบาทที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้วย

(๑๗) ให้ความช่วยเหลือหรือสนับสนุนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในควบคุมหรือกำกับดูแลของตน ในการจัดทำหรือปรับปรุงมาตรการป้องกัน รับมือ ปราบปรามและระงับภัยคุกคามทางไซเบอร์ ให้มีความเหมาะสมและเป็นปัจจุบัน และเก็บรักษาข้อมูลดังกล่าวให้ปลอดภัย

(๑๘) ให้ความช่วยเหลือหรือสนับสนุนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในควบคุมหรือกำกับดูแลของตน ในการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ และการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

(๑๙) ให้ความร่วมมือ สนับสนุนหรือดำเนินการเพื่อให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในด้านของตนตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในกรณีที่ไม่มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เป็นหน่วยงานของรัฐใดมีความพร้อม และหน่วยงานกำกับหรือดูแลไม่พร้อมทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบ

คอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าว ให้แจ้งเหตุขัดข้องให้สำนักงานทราบถึงเหตุผลที่ยังไม่พร้อมในการทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ลักษณะหน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นไปตามหลักเกณฑ์ที่ กมช. ประกาศกำหนด

(๒๐) ให้ความร่วมมือหรือสนับสนุนแก่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ในการติดตามการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และผลการตอบสนองและรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

(๒๑) ประสานงาน ให้ความร่วมมือ หรือสนับสนุน แก่หน่วยงานควบคุมหรือกำกับดูแลอื่นเพื่อให้การควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีความสอดคล้องกัน

(๒๒) ดำเนินการตามที่ กมช. หรือ กกม. มอบหมายหรือประกาศกำหนด หรือให้ความร่วมมือกับสำนักงานหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ดังนั้น ขร. จึงจำเป็นต้องจ้างที่ปรึกษาเพื่อวิเคราะห์ จัดทำมาตรการด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้สอดรับกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยที่ปรึกษาจะทำการวิเคราะห์บริบทขององค์กรตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อนำไปจัดทำ หรือปรับปรุงนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ขร. พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงแนวทางในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ ขร. มีนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และโครงสร้างการดำเนินงาน เพื่อป้องกัน และพร้อมรับมือกับภัยความมั่นคงปลอดภัยไซเบอร์ และจำเป็นต้องดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในมาตรา ๕๓ ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อขับเคลื่อนการดำเนินงานให้บรรลุผลสำเร็จตามพันธกิจขององค์กร ในการนี้ เพื่อยกระดับการกำกับดูแลการขนส่งทางรางให้เป็นไปตามกฎหมาย กฎระเบียบ มีคุณภาพ การให้บริการที่ดี และปฏิบัติงานตามหลักธรรมาภิบาล จัดทำ หรือปรับปรุงแนวทางการกำหนดมาตรฐานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้สอดคล้องกับบริบทของอุตสาหกรรมการขนส่งทางราง พร้อมทั้งพัฒนาแบบตรวจประเมินแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงสำรวจความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางรางภายใต้การกำกับดูแลของ ขร. และจัดทำรายงานสรุปความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง ภายใต้การกำกับดูแลของ ขร. วิเคราะห์ ปรับปรุงมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สอดรับกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยวิเคราะห์บริบทขององค์กรตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อนำไปจัดทำ หรือปรับปรับปรุงนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ขร. พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงแนวทางในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ ขร. มีนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และโครงสร้างการดำเนินงาน เพื่อป้องกัน และพร้อมรับมือกับภัยความมั่นคงปลอดภัยไซเบอร์

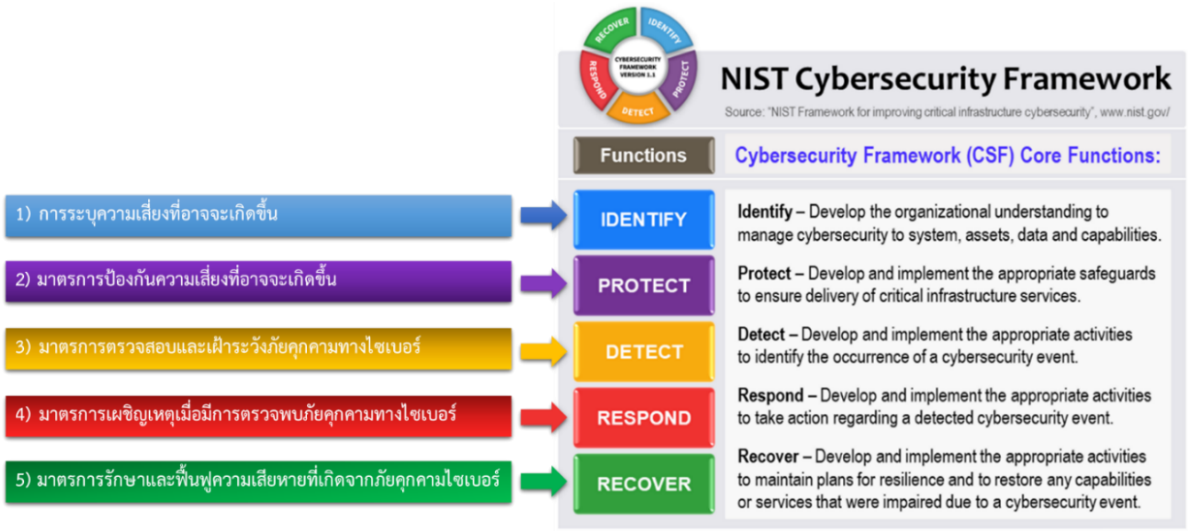
๒. กรอบแนวคิดในการดำเนินงาน

๒.๑ความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

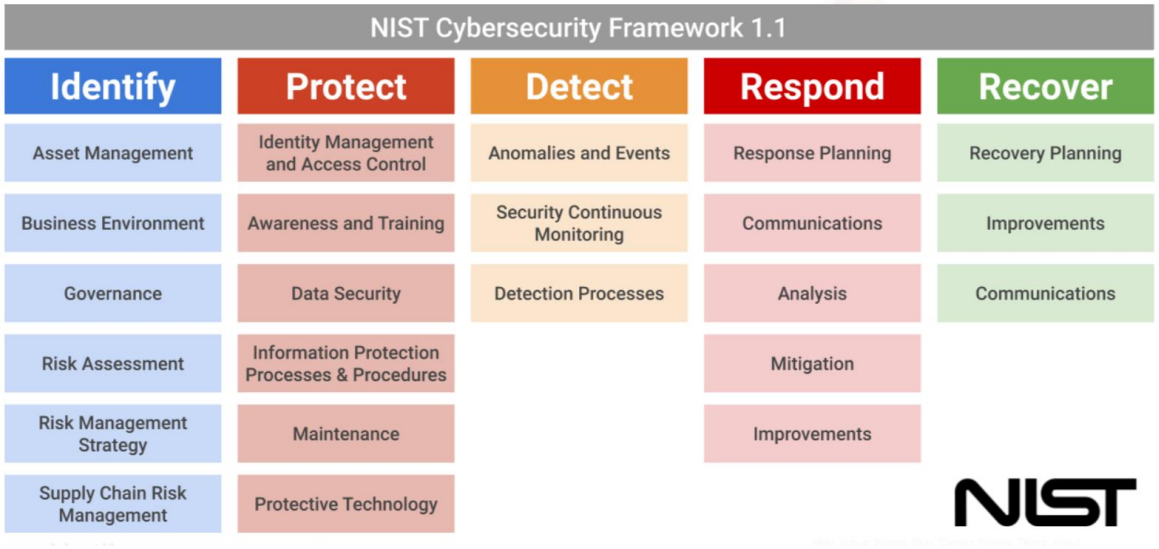
การกำหนดกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดในมาตรา ๑๓ วรรค ๔ ดังนี้

(๔) กำหนด**ประมวลแนวทางปฏิบัติ**และ**กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์** อันเป็นข้อกำหนดขั้นต่ำ ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนด**มาตรการในการประเมินความเสี่ยง** การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบ หรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรง ต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

ในการกำหนดกรอบมาตรฐาน ตามวรรค (๔) จึงต้องคำนึงถึงหลักการบริหารความเสี่ยง โดยต้องประกอบด้วย วิธีการ และมาตรการ ซึ่งสอดคล้องกับ NIST Cybersecurity Framework ดังภาพต่อไปนี้



ทั้งนี้ NIST Security Framework มีรายละเอียดแต่ละฟังก์ชัน ดังต่อไปนี้



Source:
https://www.automatedbuildings.com/news/jan๒๐/articles/newdeal/๑๙๑๒๒๐๑๑๒๐๐๒newdeal.html

๑. **การระบุ (Identify)** การระบุและเข้าใจบริบทต่างๆ ขององค์กร เพื่อการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งประกอบด้วยการประเมินตามหัวข้อย่อยดังต่อไปนี้

- **การบริหารจัดการทรัพย์สิน (Asset Management)** มีการระบุและบริหารจัดการทรัพยากรและทรัพย์สินขององค์กร ได้แก่ ข้อมูล บุคลากร อุปกรณ์ ระบบงาน ให้สอดคล้องกับวัตถุประสงค์ขององค์กร
- **สภาพแวดล้อมขององค์กร (Business Environment)** เข้าใจ และสามารถระบุสภาพแวดล้อมขององค์กร ได้แก่ ภารกิจ วัตถุประสงค์ ผู้มีส่วนได้ส่วนเสีย และกิจกรรมสำคัญขององค์กรได้
- **การกำกับดูแล (Governance)** ต้องมีการกำหนดนโยบาย ขั้นตอน และกระบวนการการจัดการ และติดตามข้อกำหนดด้านกฎระเบียบ กฎหมาย ความเสี่ยง สิ่งแวดล้อม และการปฏิบัติงาน
- **การประเมินความเสี่ยง (Risk Assessment)** เข้าใจในความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีผลต่อการดำเนินงาน
- **การกำหนดกลยุทธ์บริหารจัดการความเสี่ยง (Risk Management Strategy)** กำหนดระดับความความสำคัญ ระดับที่ยอมรับได้ การบริหารจัดการของความเสี่ยง เพื่อใช้ในการสนับสนุน หรือตัดสินใจของผู้บริหาร
- **การบริหารจัดการความเสี่ยงห่วงโซ่อุปทาน (Supply Chain Risk Management)** ลำดับความสำคัญของการยอมรับความเสี่ยง เพื่อสนับสนุนการตัดสินใจในการจัดการความเสี่ยงห่วงโซ่อุปทาน

๒. **การป้องกัน (Protect)** เป็นมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการที่สำคัญ โดยมีวัตถุประสงค์ เพื่อจำกัดระดับผลกระทบและลดโอกาสเกิดความเสี่ยง

- **กำหนดการบริหารจัดการ การพิสูจน์ตัวตน และควบคุมการเข้าถึง (Identify Management, Authentication and Access Control)** การเข้าถึงทรัพย์สินและสิ่งอำนวยความสะดวกที่เกี่ยวข้องเฉพาะผู้ใช้ที่ได้รับอนุญาต และสอดคล้องกับกลยุทธ์ความเสี่ยงขององค์กร
- **การสร้างความตระหนักและการฝึกอบรม (Awareness and Training)** บุคลากรขององค์กร ได้รับการอบรมหรือสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์
- **การกำหนดความมั่นคงปลอดภัยของข้อมูล (Data Security)** มีการบริหารจัดการข้อมูลและบันทึก ให้สอดคล้องกับกลยุทธ์ความเสี่ยงขององค์กร เพื่อปกป้องความลับ ความสมบูรณ์และความพร้อมใช้งานของข้อมูล
- **กระบวนการและแนวทางการปฏิบัติงานเพื่อป้องกันสารสนเทศ (Information Protection Processes and Procedure)** มีการกำหนดนโยบายด้านความมั่นคงปลอดภัย รวมถึงกระบวนการ แนวปฏิบัติ เพื่อป้องกันระบบสารสนเทศ และทรัพย์สินจากภัยคุกคาม
- **กระบวนการบำรุงรักษา (Maintenance)** การบำรุงรักษาส่วนประกอบต่างๆ ระบบสารสนเทศควรสอดคล้องกับนโยบายและแนวปฏิบัติ
- **จัดหาเทคโนโลยีการป้องกัน (Protective Technology)** องค์กรต้องจัดหาระบบสำหรับป้องกัน และการรักษาความมั่นคงปลอดภัย เพื่อเพิ่มประสิทธิภาพในการจัดการความมั่นคงปลอดภัย

๓. **การตรวจจับ (Detect)** เป็นการตรวจหาเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวัง หรือตรวจติดตามอย่างต่อเนื่อง

- **การตรวจจับเหตุการณ์และความผิดปกติ (Anomalies and Events)** สร้างความรู้ความเข้าใจเกี่ยวกับเหตุผลที่ผิดปกติให้ผู้เกี่ยวข้องได้รับทราบ
- **การติดตามด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring)** มีการติดตามประสิทธิภาพกระบวนการในการป้องกันระบบสารสนเทศและทรัพย์สิน
- **กระบวนการตรวจจับ (Detection Processes)** กระบวนการและขั้นตอนการตรวจจับได้รับการบำรุงรักษาและทดสอบ เพื่อให้แน่ใจว่ามีการตระหนักถึงเหตุการณ์ผิดปกติ

๔. **การตอบสนอง (Respond)** การดำเนินการตอบสนองต่อเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

- **การวางแผนการตอบสนอง (Response Planning)** มีกระบวนการและขั้นตอนการตอบสนองที่ใช้ในการวางแผนสำหรับใช้ในการตอบสนองต่อเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้น
- **การสื่อสาร (Communications)** เพื่อประสานงานกับหน่วยงานที่เกี่ยวข้อง และตอบสนองการประสานงานกับผู้มีส่วนได้ส่วนเสีย
- **การวิเคราะห์ (Analysis)** การวิเคราะห์ผลลัพธ์เพื่อให้แน่ใจว่ามีการตอบสนองที่มีประสิทธิภาพและสนับสนุนกิจกรรมการฟื้นฟู
- **การควบคุมดูแลและจำกัด (Mitigation)** การควบคุม จำกัดขอบเขต และลดผลกระทบที่เกิดขึ้น เพื่อป้องกันและแก้ไขเหตุการณ์
- **การปรับปรุง (Improvements)** การปรับปรุงและพิจารณาสิ่งที่ได้เรียนรู้จากกิจกรรมการตรวจจับ การตอบสนอง ในปัจจุบัน และเหตุการณ์ในอดีต

๕. **การคืนสภาพ (Recover)** เป็นการดำเนินการกู้คืนสภาพระบบสารสนเทศที่ได้รับความเสียหายจากการถูกคุกคามด้านไซเบอร์

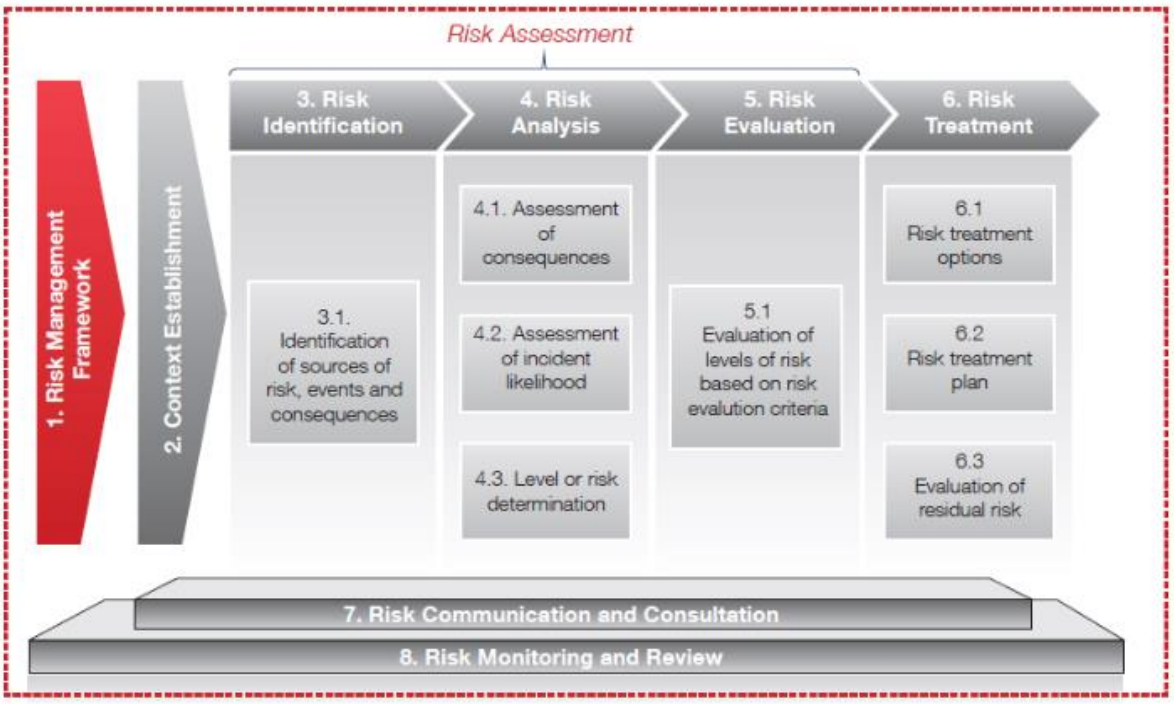
- **การวางแผนการกู้คืน (Recovery Planning)** มีกระบวนการและขั้นตอนการกู้คืนข้อมูลและมีการทบทวนอย่างสม่ำเสมอ เพื่อให้แน่ใจว่าระบบสารสนเทศที่ได้รับผลกระทบได้รับการฟื้นฟู
- **การปรับปรุง (Improvements)** การวางแผนและกระบวนการกู้คืนได้รับการปรับปรุงอย่างสม่ำเสมอ เพื่อรองรับกิจกรรมต่าง ๆ ในอนาคต
- **การสื่อสาร (Communications)** มีการประสานงานกับภายในและภายนอก เพื่อให้กิจกรรมการฟื้นฟูสามารถดำเนินการได้อย่างราบรื่น (เช่น ศูนย์ประสานงาน ผู้ให้บริการอินเทอร์เน็ต เจ้าของระบบโจมตี ผู้ที่ได้รับผลกระทบ CSIRT อื่น ๆ และผู้ขาย)

๒.๒ ความรู้ความเข้าใจด้านการประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และด้านการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ

๒.๒.๑ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การประเมินความเสี่ยงด้านการรักษาความปลอดภัยไซเบอร์ของ ขร. จะอ้างอิงตามมาตรฐาน ISO ๓๑๐๐๐ Risk Management ซึ่งเป็นมาตรฐานสำหรับบริหารจัดการความเสี่ยงด้านสากลระดับนานาชาติ โดยหน่วยงานราชการ รัฐวิสาหกิจ และเอกชน ในประเทศไทย นำมาตรฐานนี้มาใช้ในการดำเนินงานการบริหารความเสี่ยง เช่น สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) กองบัญชาการกองทัพไทย บรรษัทประกันสินเชื่ออุตสาหกรรมขนาดย่อม (บสย.) เป็นต้น

มาตรฐาน ISO ๓๑๐๐๐ มีรายละเอียดกระบวนการสำหรับการบริหารจัดการความเสี่ยงดังต่อไปนี้



Source: PECB (Professional Evaluation and Certification Board)

- **การชี้บ่งความเสี่ยง (Risk Identification)**

การชี้บ่งความเสี่ยง เป็นการระบุแหล่งที่มาของความเสี่ยง และปัจจัยความเสี่ยง ตลอดจนพื้นที่ที่ได้รับผลกระทบจากความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือความเสี่ยงด้านอื่นๆ ที่อาจเกิดขึ้น เหตุการณ์ภัยคุกคาม ช่องโหว่ และเหตุการณ์ความเสี่ยง รวมถึงผลที่จะตามมา โดยเป้าหมายของขั้นตอนนี้ เป็นการจัดทำรายการความเสี่ยงจากเหตุการณ์ที่อาจจะเป็นความเสี่ยงต่อวัตถุประสงค์ขององค์กรที่ตั้งไว้ เช่น เกิดความล้มเหลวต่อการให้บริการหลัก (Core Process) ส่งผลต่อตัวชี้วัดความสำเร็จองค์กร หรือส่งผลให้การดำเนินงานหลักขององค์กรเกิดล่าช้า โดยพิจารณาความเสี่ยงที่อาจเกิดขึ้น จากแหล่งความเสี่ยง ทั้งจากภายในและภายนอกองค์กร ตลอดจนความสัมพันธ์ระหว่างเหตุการณ์ที่อาจเกิดขึ้น

- **การวิเคราะห์ความเสี่ยง (Risk Analysis)**

การวิเคราะห์ความเสี่ยง เป็นข้อมูลในการตัดสินใจจัดการกับความเสี่ยง โดยการพิจารณาถึงโอกาสในการเกิด (Likelihood) และผลกระทบ (Impact) ที่ครอบคลุมด้านภัยคุกคามทางไซเบอร์ และข้อมูลส่วนบุคคล ตามเกณฑ์การประเมินความเสี่ยงด้านโอกาสเกิด (Likelihood Assessment Criteria) และตารางเกณฑ์การประเมินความเสี่ยงด้านผลกระทบ (Impact Assessment Criteria)

- **การประเมินผลความเสี่ยง (Risk Evaluation)**

เป็นการพิจารณาการจัดการความเสี่ยง การควบคุมที่มี และการประเมินโอกาส และผลกระทบของความเสี่ยงที่เหลืออยู่ เพื่อจัดลำดับความสำคัญของความเสี่ยง และกำหนดมาตรการจัดการกับปัจจัยเสี่ยงเหล่านั้นได้อย่างเหมาะสม

- **การจัดการความเสี่ยง (Risk Treatment) และการตอบสนองความเสี่ยง (Risk Response)**

เป็นการกำหนดแผนการจัดการ เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยอาจเลือกใช้วิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรืออาจใช้หลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์เพื่อให้อยู่ในช่วงที่องค์กรยอมรับได้ (Risk Tolerance) โดยพิจารณาแนวทางในการจัดการความเสี่ยง ๔ แนวทาง ดังนี้

๑) การยอมรับความเสี่ยง (Accept /Take Risk) คือ การยอมรับความเสี่ยงภายใต้การควบคุมที่มีอยู่ในปัจจุบัน โดยไม่มีการดำเนินการใด ๆ เพิ่มเติม เนื่องจากการควบคุมที่มีอยู่มีประสิทธิภาพและประสิทธิผล เพียงพอต่อการลดโอกาสหรือผลกระทบของความเสี่ยง หรือการยอมรับความเสี่ยงเนื่องจากค่าใช้จ่ายของการจัดการความเสี่ยงนั้น ไม่คุ้มค่ากับผลที่องค์กรจะได้รับ หรือเป็นการยอมรับความเสี่ยง เพื่อให้ได้รับโอกาสที่สูงกว่าในอนาคตอันใกล้ ซึ่งในกรณีนี้ อาจต้องอาศัยบุคลากรหรือหน่วยงานที่มีความเชี่ยวชาญในการให้คำปรึกษา หรือใช้ข้อมูลสารสนเทศที่เชื่อถือได้มาประกอบการตัดสินใจในการยอมรับความเสี่ยงนั้น

๒) การควบคุม/การลดความเสี่ยง (Treat/Reduce Risk) คือ การกำหนดมาตรการจัดการความเสี่ยง หรือกิจกรรมควบคุม หรือการดำเนินการเพิ่มเติม เพื่อลดโอกาสเกิด หรือลดผลกระทบของความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้อยู่ในระดับที่ยอมรับได้ เช่น การบริหารจัดการบัญชีผู้ใช้งาน การกำหนดสิทธิในการเข้าถึงระบบสารสนเทศ การทบทวนและระงับสิทธิผู้ใช้งาน การตั้งค่าการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ การควบคุมรหัสผ่าน การควบคุมและป้องกันศูนย์ข้อมูล การบริหารจัดการการเปลี่ยนแปลง การสำรองข้อมูล การบำรุงรักษาอุปกรณ์ การเฝ้าระวังและบริหารจัดการเหตุการณ์ผิดปกติ การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ เป็นต้น

๓) การหาผู้ร่วมรับความเสี่ยง (Transfer/Share Risk) คือ การถ่ายโอน/แบ่งปันความเสี่ยงบางส่วน (Transfer/Share) ไปยังบุคคลหรือองค์กรอื่นช่วยรับผิดชอบ เช่น การว่าจ้างผู้ให้บริการภายนอกมาดำเนินการแทน การทำประกันภัย เป็นต้น เพื่อลดโอกาสเกิดหรือลดผลกระทบความเสี่ยงลง

๔) การหลีกเลี่ยงความเสี่ยง (Avoid Risk /Terminate) คือ การดำเนินการเพื่อยกเลิกหรือหลีกเลี่ยงความเสี่ยงที่เกี่ยวกับกิจกรรม/แผนงาน/โครงการ ที่อาจสร้างผลกระทบ หรือความเสียหายอย่างมีนัยสำคัญต่อการดำเนินงาน หรือเสถียรภาพความมั่นคงขององค์กรในระยะยาว โดยการดำเนินการตามแนวทางนี้ อาจต้องมีการทบทวนวัตถุประสงค์ หรือเป้าหมาย หรือแผนกลยุทธ์แรกเริ่มให้สอดคล้องกับบริบทขององค์กร หรือความต้องการ และความคาดหวังของผู้มีส่วนได้ส่วนเสียขององค์กร เพื่อลดโอกาสความเสี่ยงที่อาจเกิดขึ้นได้ในอนาคต

- **การสื่อสารความเสี่ยงและการให้คำปรึกษา (Communication and Consultation)**

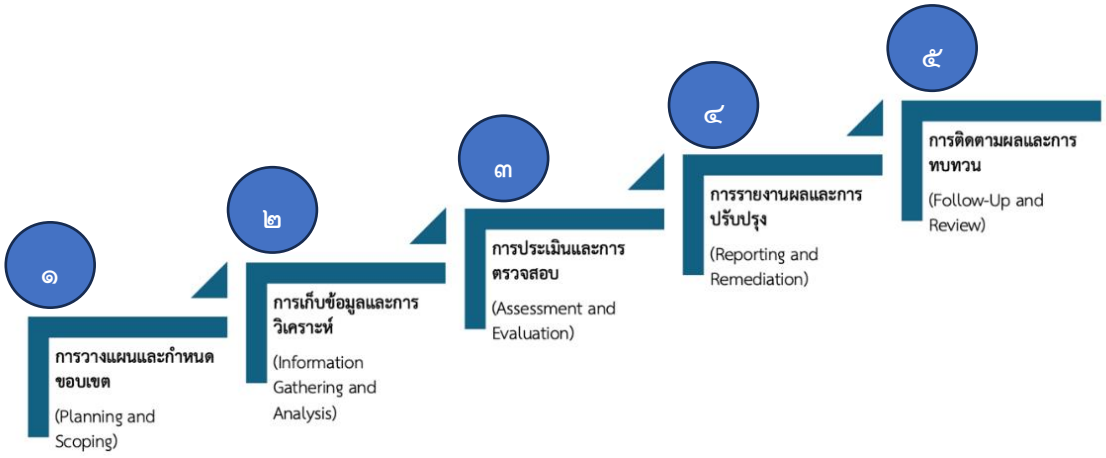
เป็นการสื่อสารกิจกรรมและการดำเนินการจัดการความเสี่ยง ซึ่งจะจัดทำเป็นรายงานผลการบริหารความเสี่ยง ตามแผนบริหารจัดการความเสี่ยง ให้ผู้รับผิดชอบความเสี่ยงพิจารณาผลการดำเนินการ ก่อนรายงานไปยังฝ่ายบริหารที่เกี่ยวข้องตามลำดับต่อไป

- **การติดตามผลและการทบทวนความเสี่ยง (Monitoring and Review)**

เป็นการเฝ้าติดตาม ตรวจสอบและทบทวนความเสี่ยงตามกรอบเวลาที่กำหนดไว้ โดยจะต้องครอบคลุมในทุก ๆ ส่วนของกระบวนการบริหารจัดการความเสี่ยง ซึ่งการดำเนินการนี้ จะเป็นการสร้างความมั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม และการบริหารความเสี่ยงได้นำไปประยุกต์ใช้ในทุกระดับขององค์กร ความเสี่ยงทั้งหมดที่มีผลกระทบสำคัญต่อการบรรลุวัตถุประสงค์ขององค์กรได้รับการรายงานต่อผู้บริหารที่รับผิดชอบ

๒.๒.๒ การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit) หมายถึง กระบวนการประเมินอย่างเป็นระบบ เพื่อประเมินประสิทธิภาพของมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศภายใน ขร. โดยมีวัตถุประสงค์ เพื่อระบุช่องโหว่และความเสี่ยงที่อาจนำไปสู่การโจมตีทางไซเบอร์หรือการรั่วไหลของข้อมูลสำคัญ ซึ่งตามขอบเขตงานของโครงการนี้ ที่ปรึกษาจะดำเนินการตรวจสอบครอบคลุมการประเมิน การปฏิบัติตามนโยบายและมาตรฐานความปลอดภัยที่เกี่ยวข้อง รวมถึงการตรวจสอบระบบควบคุมต่าง ๆ เพื่อให้มั่นใจว่า ขร. ได้ดำเนินตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒



ทั้งนี้ การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ มีกระบวนการในการดำเนินการดังนี้

๑. การวางแผนและกำหนดขอบเขต (Planning and Scoping)

- **กำหนดวัตถุประสงค์** ระบุเป้าหมายหลักของการตรวจสอบ เช่น การประเมินความเสี่ยง การปฏิบัติตามข้อกำหนด หรือการทดสอบช่องโหว่
- **กำหนดขอบเขต** ระบุขอบเขตของระบบ สินทรัพย์ และพื้นที่ ที่จะได้รับการตรวจสอบ เช่น ระบบเครือข่าย ฐานข้อมูล แอปพลิเคชัน หรือโครงสร้างพื้นฐาน
- **ระบุทรัพยากร** กำหนดบุคลากร เครื่องมือ และเทคโนโลยีที่จำเป็นต่อการดำเนินการตรวจสอบ

- **จัดทำแผนการตรวจสอบ** วางแผนตารางเวลาและขั้นตอนการตรวจสอบ โดยรวมถึงการประสานงานกับหน่วยงานที่เกี่ยวข้อง

๒. การเก็บข้อมูลและการวิเคราะห์ (Information Gathering and Analysis)

- **รวบรวมเอกสารและข้อมูล** รวบรวมเอกสารที่เกี่ยวข้อง เช่น นโยบายความมั่นคงปลอดภัย มาตรการควบคุม และรายงานการตรวจสอบก่อนหน้า
- **สัมภาษณ์และสอบถาม** สัมภาษณ์ผู้ที่เกี่ยวข้องใน ขร. เช่น ผู้ดูแลระบบ เจ้าหน้าที่ IT เพื่อทำความเข้าใจเกี่ยวกับกระบวนการและมาตรการความปลอดภัยที่มีอยู่
- **การวิเคราะห์ข้อมูล** วิเคราะห์ข้อมูลที่รวบรวมได้เพื่อระบุช่องโหว่ ความเสี่ยง และส่วนที่ต้องปรับปรุง

๓. การประเมินและการตรวจสอบ (Assessment and Evaluation)

- **ประเมินการปฏิบัติตามมาตรฐาน** ตรวจสอบว่าระบบและกระบวนการของ ขร. เป็นไปตามมาตรฐานความมั่นคงปลอดภัย เช่น ISO ๒๗๐๐๑, NIST หรือ กฎหมาย กฎระเบียบที่เกี่ยวข้อง
- **ตรวจสอบมาตรการควบคุม (Control Testing)** ตรวจสอบว่ามาตรการควบคุมต่างๆ ถูกนำมาใช้และปฏิบัติอย่างถูกต้องและมีประสิทธิภาพ
- **การวิเคราะห์ผลกระทบ** ประเมินผลกระทบของความเสี่ยงและช่องโหว่ที่พบต่อ ขร. รวมถึงการกำหนดระดับความเสี่ยง

๔. การรายงานผลและการปรับปรุง (Reporting and Remediation)

- **จัดทำรายงานผลการตรวจสอบ** จัดทำรายงานที่ระบุผลการตรวจสอบที่พบ รวมถึงความเสี่ยง และข้อเสนอแนะในการปรับปรุง
- **การนำเสนอผลการตรวจสอบ** นำเสนอผลการตรวจสอบต่อผู้บริหารและหน่วยงานที่เกี่ยวข้อง เพื่อให้เข้าใจถึงสถานะความมั่นคงปลอดภัยของ ขร.
- **การวางแผนการปรับปรุง (Remediation Planning)** ร่วมมือกับทีม IT และผู้บริหารในการวางแผนและดำเนินการปรับปรุงมาตรการควบคุมตามข้อเสนอแนะ
- **การติดตามและตรวจสอบซ้ำ** หลังจากดำเนินการปรับปรุงแล้ว ควรมีการตรวจสอบซ้ำเพื่อยืนยันว่าช่องโหว่ได้รับการแก้ไขและมาตรการความมั่นคงปลอดภัยได้รับการปรับปรุง

๕. การติดตามผลและการทบทวน (Follow-Up and Review)

- **ติดตามความคืบหน้า** ติดตามผลการดำเนินการตามแผนการปรับปรุงว่ามีความคืบหน้าและผลลัพธ์ที่เกิดขึ้นเป็นอย่างไร
- **ทบทวนและปรับปรุงกระบวนการ** ทบทวนกระบวนการตรวจสอบและผลลัพธ์ที่ได้เพื่อนำไปปรับปรุงกระบวนการตรวจสอบในอนาคต
- **การตรวจสอบประจำปี** จัดทำการตรวจสอบประจำปี เพื่อประเมินความมั่นคงปลอดภัยไซเบอร์ ขององค์กรอย่างต่อเนื่อง

๓. ประมวลแนวทางปฏิบัติและกรอบมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร.

บทที่ ๑ บทนำ

๑. หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และไปในทิศทางเดียวกัน

กรมการขนส่งทางราง (ขร.) ในฐานะหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล จึงจัดทำกรอบมาตรฐานด้านการรักษาความปลอดภัยไซเบอร์ถือปฏิบัติ โดยอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔

๒. วัตถุประสงค์

เพื่อกำหนดกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์พร้อมทั้งนำไปใช้ในการดำเนินงานและการจัดการระบบงานเทคโนโลยีสารสนเทศของ ขร. ให้มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน

๓. ขอบเขต

๑. เอกสารฉบับนี้ครอบคลุมตามกรอบและวิธีปฏิบัติสำหรับด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งบังคับใช้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒. เอกสารฉบับนี้ใช้บังคับกับกรมการขนส่งทางราง ซึ่งมีฐานะเป็นหน่วยงานกำกับดูแลผู้ให้บริการขนส่งทางราง ซึ่งขอบเขตของการประยุกต์ใช้แบ่งเป็น ๒ ส่วน ดังนี้ ๑. แนวปฏิบัติที่ต้องดำเนินการตามกฎหมายกำหนด และ ๒. แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option) ซึ่งจะระบุไว้ในแต่ละหัวข้อของแนวปฏิบัตินี้

๔. คำนิยาม

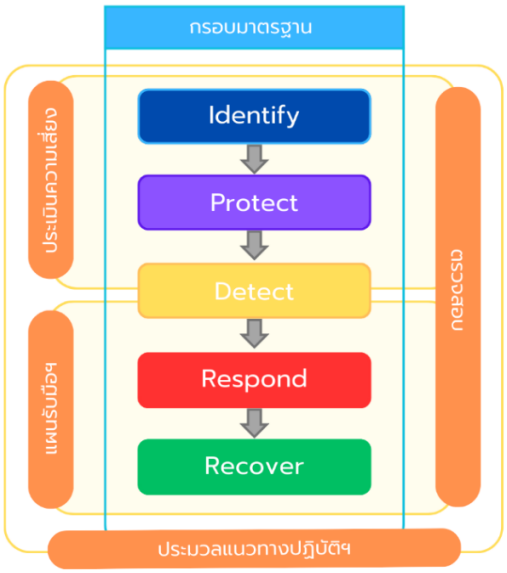
ลำดับ	คำนิยาม	ความหมาย
๑.	หน่วยงาน หรือ องค์กร	กรมการขนส่งทางราง หรือ ขร.
๒.	คณะกรรมการ	คณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์
๓.	กกม.	คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

ลำดับ	คำนิยาม	ความหมาย
๔.	สกมช.	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๕.	ดัชนีชี้วัดความเสี่ยงที่สำคัญ	เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์เหตุการณ์ และความเสี่ยงในอนาคตและเตรียมมาตรการการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย
๖.	คอมไพเลอร์	โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
๗.	แพตซ์	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟแวร์หลายรายได้เผยแพร่แพตซ์ (Patch) ออกมาเป็นระยะเช่น บริษัท Microsoft มีการเผยแพร่แพตซ์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update
๘.	Recovery Time Objective (RTO)	ระยะเวลาในการกู้คืนระบบ
๙.	Recovery Point Objective (RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
๑๐.	Maximum Tolerance Period of Disruption (MTPD)	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
๑๑.	ผู้ใช้งาน	ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างตามสัญญาจ้างในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของ ขร.
๑๒.	บุคคลภายนอก	บุคคลจากหน่วยงานภายนอกที่เข้ามาประชุม หรือปฏิบัติงานร่วมกับหน่วยงาน
๑๓.	หน่วยงานภายนอก	หน่วยงานภายนอกที่หน่วยงานอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ลำดับ	คำนิยาม	ความหมาย
๑๔.	สิทธิ์ของผู้ใช้งาน	สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
๑๕.	ผู้ดูแลระบบ	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบงาน
๑๖.	สินทรัพย์	ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตนอันมีมูลค่าคุณค่าสำหรับหน่วยงาน
๑๘.	การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การขออนุญาต การกำหนดสิทธิ์ หรือมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบสารสนเทศและระบบเครือข่าย
๑๙.	ความมั่นคงปลอดภัยด้านสารสนเทศ	การธำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ
๒๐.	ภัยคุกคาม	สาเหตุที่ทำให้เกิดเหตุไม่พึงประสงค์ที่มีผลเสียหายต่อ ขร.
๒๑.	ช่องโหว่	จุดอ่อนของทรัพย์สิน หรือมาตรการ ที่ภัยคุกคามสามารถใช้ประโยชน์ในการทำให้เกิดความเสียหาย
๒๒.	สื่อบันทึกข้อมูล	สิ่งที่ใช้จัดเก็บข้อมูล ชุดคำสั่ง และสารสนเทศอื่น ๆ เช่น USB drive, SD Card, Memory stick, เทป, CD/DVD, Removable drive, External Hard disk, Flash memory และหน่วยความจำของอุปกรณ์ Router หรือ Switch เป็นต้น
๒๓.	ทรัพย์สิน	ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ หรือสิ่งอื่นใดที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศ
๒๔.	ความเสี่ยง	เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศขององค์กร เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้องค์กรเสียชื่อเสียง
๒๕	ISO/IEC ๒๗๐๐๑	มาตรฐานระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System หรือ ISMS)
๒๖	NIST Cybersecurity Framework	กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework)
๒๗	มาตรฐาน IEC ๖๒๔๔๓	กรอบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของระบบควบคุมอุตสาหกรรม (Industrial Automation and Control Systems: IACS)

บทที่ ๒
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework)

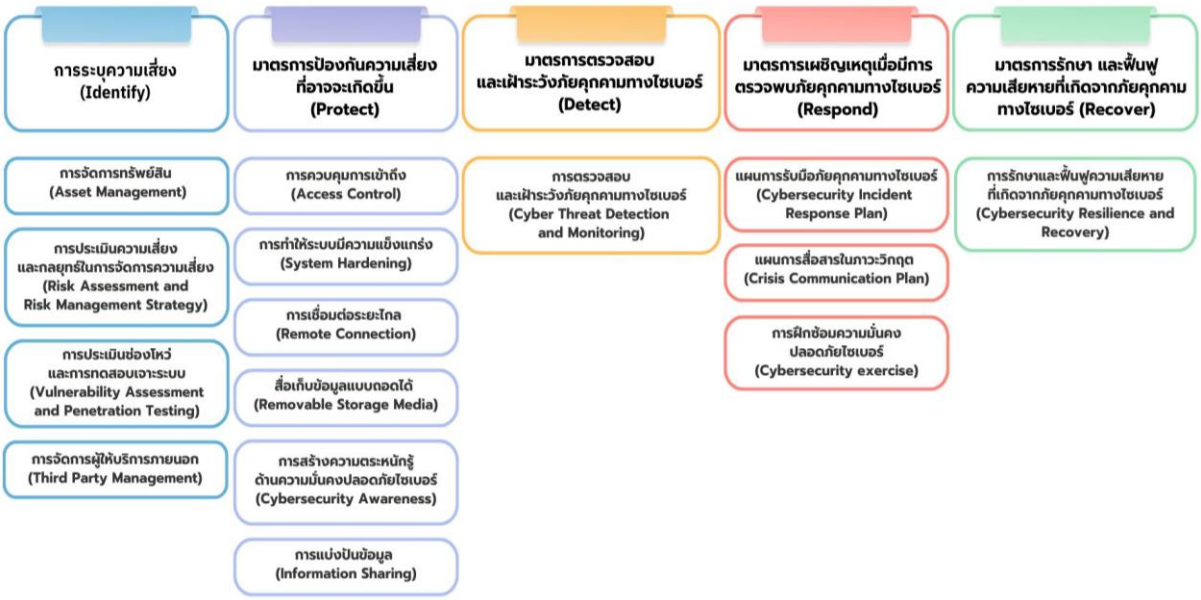


รูปที่ ๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑.๑ บทนำ

NIST Cybersecurity Framework (CSF) เป็นมาตรฐานที่พัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (National Institute of Standards and Technology - NIST) โดยมีวัตถุประสงค์ เพื่อช่วยให้องค์กรสามารถบริหารจัดการความเสี่ยงด้านไซเบอร์ได้อย่างมีประสิทธิภาพ CSF ถูกออกแบบให้ยืดหยุ่น และสามารถนำไปประยุกต์ใช้ได้กับองค์กรทุกประเภท ไม่ว่าจะเป็นภาครัฐ เอกชน หรือองค์กรที่ต้องการเพิ่มความมั่นคงปลอดภัยของระบบสารสนเทศ

ทั้งนี้ ปัจจุบันกรอบมาตรฐานที่เป็นไปตามกฎหมายกำหนดและบังคับใช้ยังคงเป็นฉบับเดิม (Version ๑.๑) ซึ่งปัจจุบันสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (National Institute of Standards and Technology - NIST) ได้มีการพัฒนามาตรฐานขึ้นใหม่เป็นฉบับ ๒.๐ ซึ่งประกาศเมื่อกุมภาพันธ์ ๒๐๒๔ เพื่อให้มาตรฐานมีขอบเขตที่กว้างขึ้น และสนับสนุนให้องค์กรทบทวนและปรับปรุงแนวปฏิบัติด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ รวมถึงให้ความสำคัญกับการประเมินและลดความเสี่ยงที่มาจากผู้ให้บริการและบุคคลที่สาม



รูปที่ ๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Version ๑.๑)

๒.๑.๒ หลักการของมาตรฐาน NIST CSF ๑.๑

หลักการสำคัญที่ใช้เป็นแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ โดยแบ่งออกเป็น ๕ ฟังก์ชันหลัก ได้แก่

๑. ระบุ (Identify)

NIST Framework ในส่วนแรก คือ การที่องค์กรต้องจัดทำรายงานเพื่อระบุความเสี่ยงของอุปกรณ์ต่าง ๆ และจัดลำดับความสำคัญของสินทรัพย์ภายในองค์กรตามความสำคัญ โดยกระบวนการจัดการสินทรัพย์จะต้องทำตั้งแต่เริ่มต้นจนสิ้นสุดการใช้งาน Asset Lifecycle Management (ALM) ต้องมีการตรวจสอบและรวบรวมข้อมูลด้านภัยคุกคาม เพื่อประเมินความเสี่ยงทางไซเบอร์ในปัจจุบันขององค์กรอย่างต่อเนื่อง

- การระบุทรัพย์สินที่สำคัญ (Assets Identification)
- การวิเคราะห์บริบทขององค์กร
- การระบุช่องโหว่และภัยคุกคาม
- การจัดลำดับความสำคัญความเสี่ยง

๒. ป้องกัน (Protect)

NIST Framework ส่วนต่อมาเป็นการใช้มาตรการรักษาความปลอดภัยเพื่อป้องกันระบบและข้อมูลขององค์กร เช่น การกำหนดสิทธิการเข้าถึง การจัดการเกี่ยวกับการยืนยันตัวตน การใช้เทคโนโลยีเพื่อป้องกันระบบ และการฝึกอบรมพนักงานให้ตระหนักถึงภัยคุกคามทางไซเบอร์

- การควบคุมการเข้าถึง (Access Control)
- การฝึกอบรมและการสร้างความตระหนักในด้านความปลอดภัย
- การปกป้องข้อมูลและระบบจากการถูกโจมตี
- การดูแลรักษาโครงสร้างพื้นฐานทางเทคโนโลยี

๓. ตรวจจับ (Detect)

ทุกองค์กรควรจะต้องมีระบบการตรวจสอบทรัพย์สินอย่างต่อเนื่อง เพื่อตรวจจับความผิดปกติและสัญญาณที่แสดงถึงภัยคุกคามที่จะเข้ามาโจมตี การวิเคราะห์เหตุการณ์ ต้องทำอย่างรวดเร็วเพื่อระบุพฤติกรรม หรือสถานการณ์ที่ไม่ปกติ ซึ่งอาจบ่งชี้ถึงการถูกโจมตีทางไซเบอร์ กระบวนการตรวจจับที่มีประสิทธิภาพ จะช่วยให้องค์กรสามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว ลดผลกระทบที่อาจเกิดขึ้นได้อย่างทันท่วงที

- การติดตั้งระบบเพื่อตรวจจับเหตุการณ์ไซเบอร์
- การวิเคราะห์ข้อมูลแบบเรียลไทม์
- การแจ้งเตือนและบันทึกเหตุการณ์ที่ผิดปกติ

๔. ตอบสนอง (Respond)

องค์กรควรมีแผนรับมือเหตุการณ์ด้านความปลอดภัยไซเบอร์ที่ชัดเจนและเป็นระบบ โดยกำหนดนโยบายและขั้นตอน รวมถึงบทบาทและหน้าที่ของผู้เกี่ยวข้องอย่างชัดเจน แผนดังกล่าว จะช่วยให้องค์กรตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นเมื่อเกิดเหตุการณ์ที่ไม่คาดฝัน

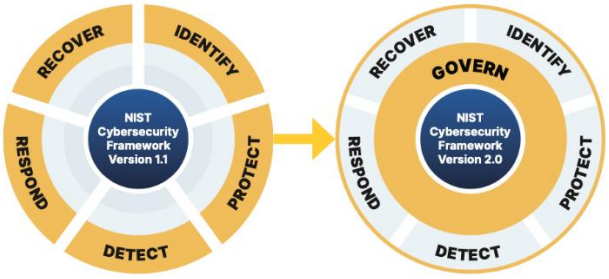
- การวางแผนและดำเนินการตอบสนองต่อเหตุการณ์
- การสื่อสารในช่วงเกิดเหตุการณ์กับผู้มีส่วนเกี่ยวข้อง
- การประเมินผลหลังการตอบสนองเพื่อปรับปรุงกระบวนการ

๕. กู้คืน (Recover)

หากระบบขององค์กรถูกโจมตี NIST Framework มีแนวทางสำหรับการกู้ระบบ คือ การวางแผนการกู้คืนระบบไว้อย่างเป็นขั้นตอน มีการตรวจสอบความครบถ้วนของข้อมูลสำรองที่ใช้ในการกู้คืน จัดทำแผนการสื่อสาร เพื่อแจ้งความคืบหน้าให้ผู้เกี่ยวข้องทราบ เพื่อให้การดำเนินงานสามารถกลับมาเป็นปกติโดยไม่หยุดชะงักและให้จัดทำเอกสารบันทึกรายละเอียดเหตุการณ์ ปัญหาและขั้นตอนการแก้ไข เพื่อนำมาวิเคราะห์และปรับปรุงแนวปฏิบัติสำหรับในอนาคต

- การฟื้นฟูระบบและข้อมูลให้กลับมาสู่สภาพปกติ
- การปรับปรุงความยืดหยุ่นของระบบในอนาคต
- การสื่อสารกับบุคคลภายนอก เช่น ลูกค้าและคู่ค้า

๒.๑.๓ หลักการของมาตรฐาน NIST CSF ๒.๐



รูปที่ ๓ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Version ๒.๐)

๑. การกำกับดูแล (Government)

ฟังก์ชันนี้เป็นส่วนที่เพิ่มเข้ามาใหม่ใน CSF ๒.๐ ซึ่งเน้นย้ำถึงความสำคัญของการกำกับดูแลและความเป็นผู้นำในการบริหารจัดการความเสี่ยงด้านไซเบอร์ในระดับองค์กร โดยมีองค์ประกอบ ดังนี้

- บริบทขององค์กร (Organizational Context) เป็นการทำความเข้าใจสภาพแวดล้อม วัตถุประสงค์ และความต้องการขององค์กรที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์
- กลยุทธ์การบริหารความเสี่ยง (Risk Management Strategy) เป็นการกำหนดแนวทางและเป้าหมายในการจัดการความเสี่ยงด้านไซเบอร์
- บทบาท ความรับผิดชอบ และอำนาจหน้าที่ (Roles, Responsibilities, and Authorities) เป็นการกำหนดผู้รับผิดชอบและขอบเขตอำนาจที่ชัดเจน
- นโยบาย (Policy) ต้องจัดทำนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์
- การกำกับดูแล (Oversight) ต้องมีการตรวจสอบและประเมินผลการดำเนินงานด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง
- การบริหารจัดการความเสี่ยงในห่วงโซ่อุปทาน (Cybersecurity Supply Chain Risk Management - C-SCRM) โดยกำหนดการจัดการความเสี่ยงที่มาจากผู้ให้บริการและบุคคลที่สามในห่วงโซ่อุปทาน

๒. การระบุ (Identify)

มุ่งเน้นที่การทำความเข้าใจและระบุความเสี่ยงด้านไซเบอร์ขององค์กร ซึ่งประกอบด้วย

- การบริหารจัดการสินทรัพย์ (Asset Management) โดยจัดให้มีการระบุและจัดประเภทสินทรัพย์ที่สำคัญขององค์กร (เช่น ระบบ ข้อมูล บุคลากร)
- สภาพแวดล้อมทางธุรกิจ (Business Environment) ซึ่งเป็นการทำความเข้าใจบทบาทของความมั่นคงปลอดภัยไซเบอร์ในการสนับสนุนการดำเนินงานขององค์กร
- การบริหารความเสี่ยง (Risk Assessment) โดยกำหนดให้มีการประเมินความเสี่ยงและช่องโหว่ด้านความมั่นคงปลอดภัย
- การบริหารจัดการความเสี่ยงห่วงโซ่อุปทาน (Supply Chain Risk Management) การระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการและบุคคลที่สาม

๓. การป้องกัน (Protect)

ฟังก์ชันนี้ ครอบคลุมการพัฒนากำหนดและดำเนินกิจกรรมป้องกันเพื่อจำกัดหรือยับยั้งผลกระทบที่อาจเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัย ประกอบด้วย

- การบริหารจัดการข้อมูล (Data Security) โดยจัดให้มีการป้องกันข้อมูลสำคัญจากการเข้าถึง การใช้งาน การเปิดเผย การขัดขวาง การแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาต
- การควบคุมการเข้าถึง (Identity Management, Authentication, and Access Control) เป็นการบริหารจัดการตัวตน การยืนยันตัวตน และการควบคุมการเข้าถึงระบบและข้อมูล
- การป้องกันระบบและข้อมูล (Protective Technology) โดยการนำเทคโนโลยีและมาตรการป้องกันต่างๆ มาใช้ (เช่น ไฟร์วอลล์ การเข้ารหัส ซอฟต์แวร์ป้องกันมัลแวร์)
- การอบรมและสร้างความตระหนัก (Awareness and Training) โดยการให้ความรู้แก่บุคลากรเกี่ยวกับภัยคุกคามและการปฏิบัติงานที่ปลอดภัยจากภัยคุกคามทางไซเบอร์
- กระบวนการป้องกัน (Protective Processes) โดยกำหนดและดำเนินการตามกระบวนการที่ช่วยป้องกันเหตุการณ์ด้านความมั่นคงปลอดภัย

๔. การตรวจจับ (Detect)

ฟังก์ชันนี้เน้นที่การพัฒนากิจกรรมเพื่อระบุการเกิดเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ให้ทันท่วงที ประกอบด้วย

- การตรวจสอบความผิดปกติและเหตุการณ์ (Anomalies and Events) โดยจัดให้มีการตรวจจับกิจกรรมที่ผิดปกติหรือเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์
- การตรวจสอบความปลอดภัย (Security Continuous Monitoring) โดยจัดให้มีการเฝ้าระวังระบบและเครือข่ายอย่างต่อเนื่อง
- กระบวนการตรวจจับ (Detection Processes) โดยกำหนดและดำเนินการตามกระบวนการ เพื่อตรวจจับภัยคุกคาม

๕. การตอบสนอง (Respond)

ฟังก์ชันนี้มุ่งเน้นที่การพัฒนากิจกรรมเพื่อดำเนินการเมื่อตรวจพบเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งประกอบด้วย

- การวางแผนการตอบสนอง (Response Planning) โดยจัดให้มีทำแผนการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์
- การสื่อสาร (Communication) โดยการสื่อสารข้อมูลที่เกี่ยวข้องกับเหตุการณ์ไปยังผู้มีส่วนได้ส่วนเสีย
- การวิเคราะห์ (Analysis) โดยดำเนินการวิเคราะห์เหตุการณ์ เพื่อทำความเข้าใจสาเหตุและขอบเขตของผลกระทบ
- การลดผลกระทบ (Mitigation) โดยดำเนินการตามมาตรการควบคุมขององค์กร เพื่อลดผลกระทบของเหตุการณ์

- การปรับปรุง (Improvements) โดยการนำบทเรียนจากเหตุการณ์ภัยคุกคามทางไซเบอร์มาดำเนินการปรับปรุงกระบวนการและมาตรการป้องกันที่อยู่ปัจจุบัน เพื่อป้องกันการเกิดซ้ำ

๖. การกู้คืน (Recover)

ฟังก์ชันนี้เน้นที่การพัฒนากิจกรรมเพื่อฟื้นฟูระบบและบริการที่ได้รับผลกระทบจากเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งรวมถึง:

- การวางแผนการกู้คืน (Recovery Planning) โดยดำเนินการจัดทำแผนการกู้คืนระบบและข้อมูลจากภัยคุกคามทางไซเบอร์
- การปรับปรุง (Improvements) โดยนำบทเรียนจากการกู้คืนไปปรับปรุงแผนและความสามารถในการฟื้นตัว
- การสื่อสาร (Communications) จัดให้มีการสื่อสารสถานะการกู้คืนกับผู้มีส่วนได้ส่วนเสียรับทราบเป็นระยะ

๒.๒ กรอบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System - ISMS)

๒.๒.๑ บทนำ (Introduction)

ISO/IEC ๒๗๐๐๑ เป็นมาตรฐานสากลสำหรับการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System - ISMS) ที่ออกแบบมาเพื่อช่วยให้องค์กรสามารถปกป้องข้อมูลสำคัญจากภัยคุกคามทางไซเบอร์ และลดความเสี่ยงจากการรั่วไหลของข้อมูล ระบบนี้เป็นโครงสร้างที่ช่วยให้องค์กรสามารถวางแผน ดำเนินการ ตรวจสอบ และปรับปรุงมาตรการรักษาความปลอดภัยของข้อมูลอย่างต่อเนื่อง โดยสามารถนำไปใช้ได้กับทุกประเภทขององค์กร ไม่ว่าจะเป็นภาครัฐ ภาคเอกชน หรือองค์กรที่เกี่ยวข้องกับข้อมูลที่มีความอ่อนไหวสูง

รวมถึงแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบขนส่งทางราง (Guidelines for cyber-security in railway) ที่จัดทำโดยสหภาพรถไฟระหว่างประเทศ (International Union of Railways (UIC)) จัดตั้งที่กรุงปารีส ประเทศฝรั่งเศส มีการนำกรอบมาตรฐาน ISO/IEC ๒๗๐๐๑ นี้ไปจัดทำแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบขนส่งทางราง

รูปที่ ๔ แนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบขนส่งทางราง
(Guidelines for cyber-security in railway)

ทั้งนี้การจัดทำกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมการขนส่งทางราง จึงมีการประยุกต์ใช้มาตรฐาน ISO/IEC ๒๗๐๐๑ เป็นกรอบในการกำหนดประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นทางเลือกในการดำเนินการกำหนดมาตรการป้องกัน และควบคุมภัยคุกคามทางไซเบอร์นอกเหนือจากกฎหมายกำหนด

รูปที่ ๕ กรอบมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ
(Information Security Management System - ISMS)

๒.๒.๒ หลักการของ ISO/IEC ๒๗๐๐๑:๒๐๒๒ (Key Principles)

หลักการสำคัญของมาตรฐาน ISO/IEC ๒๗๐๐๑ อิงตามหลักการสำคัญของความมั่นคงปลอดภัยสารสนเทศที่เรียกว่า CIA Triad ได้แก่

๑. การรักษาความลับของข้อมูล (Confidentiality)

- การป้องกันไม่ให้ข้อมูลถูกเข้าถึง แก้ไข หรือเปิดเผยโดยบุคคลที่ไม่ได้รับอนุญาต เพื่อรักษาความปลอดภัยและลดความเสี่ยงจากการรั่วไหลของข้อมูล

๒. ความถูกต้องครบถ้วนของข้อมูล (Integrity)

- การป้องกันข้อมูลจากการถูกแก้ไข ดัดแปลง หรือทำลายโดยไม่ได้รับอนุญาต เพื่อให้มั่นใจว่าข้อมูลยังคงถูกต้องและน่าเชื่อถือ

๓. ความพร้อมใช้งานของข้อมูล (Availability)

- **การทำให้ข้อมูลสามารถเข้าถึงและใช้งานได้อย่างต่อเนื่อง เมื่อต้องการ โดยไม่มีการหยุดชะงัก**หรือสูญหาย

๒.๒.๓ ข้อกำหนดของ ISO/IEC ๒๗๐๐๑:๒๐๒๒ (Requirements)

ข้อกำหนดใน ISO/IEC ๒๗๐๐๑:๒๐๒๒ ถูกแบ่งออกเป็นส่วนต่าง ๆ ดังนี้

๑. บริบทขององค์กร (Context of the Organization)

- การทำความเข้าใจบริบทภายในและภายนอกที่อาจมีผลกระทบต่อ ISMS
- การระบุและทำความเข้าใจความต้องการของผู้มีส่วนได้ส่วนเสีย
- การกำหนดขอบเขตของ ISMS

๒. ความเป็นผู้นำ (Leadership)

- การสนับสนุนจากผู้บริหารระดับสูงในเรื่องการจัดการ ISMS
- การกำหนดนโยบายความมั่นคงปลอดภัยของข้อมูล
- การมอบหมายบทบาท ความรับผิดชอบ และอำนาจหน้าที่

๓. การวางแผน (Planning)

- การระบุความเสี่ยงและโอกาสที่เกี่ยวข้องกับ ISMS
- การกำหนดวัตถุประสงค์และเป้าหมายด้านความมั่นคงปลอดภัยของข้อมูล
- การวางแผนเพื่อจัดการความเสี่ยงและโอกาส

๔. การสนับสนุน (Support)

- การจัดหาทรัพยากรที่เพียงพอสำหรับ ISMS
- การฝึกอบรมและสร้างความตระหนักในองค์กร
- การสื่อสารที่มีประสิทธิภาพเกี่ยวกับ ISMS

๕. การดำเนินงาน (Operation)

- การวางแผนและควบคุมกระบวนการที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูล
- การประเมินและจัดการความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล
- การจัดการเปลี่ยนแปลงที่มีผลกระทบต่อ ISMS

๖. การประเมินผลการปฏิบัติงาน (Performance Evaluation)

- การติดตาม วัดผล และประเมินผลการปฏิบัติงานของ ISMS

- การตรวจสอบภายใน (Internal Audit)
- การทบทวนโดยผู้บริหาร (Management Review)

๗. การปรับปรุง (Improvement)

- การแก้ไขปัญหาและการปรับปรุงอย่างต่อเนื่องของ ISMS
- การดำเนินการแก้ไขเมื่อมีความไม่สอดคล้อง

รูปที่ ๖ มาตรการควบคุม (Annex A) ตามมาตรฐาน ISO/IEC ๒๗๐๐๑: ๒๐๒๒

๒.๒.๔ ข้อกำหนดภาคผนวก (Annex A Controls)

Annex A ใน ISO/IEC ๒๗๐๐๑:๒๐๒๒ ประกอบด้วย ๙๓ ข้อควบคุม (Controls) แบ่งออกเป็น ๔ หมวดใหญ่ ดังนี้

- **A.๕ มาตรการควบคุมเชิงองค์กร (Organizational Controls) จำนวน ๓๗ ข้อ**
- **A.๖ มาตรการด้านบุคลากร (People Controls) จำนวน ๘ ข้อ**
- **A.๗ มาตรการด้านกายภาพ (Physical Controls) จำนวน ๑๔ ข้อ**
- **A.๘ มาตรการด้านเทคโนโลยี (Technological Controls) จำนวน ๓๔ ข้อ**

ISO/IEC ๒๗๐๐๑ เป็นมาตรฐานที่ช่วยให้องค์กรสามารถบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศได้อย่างมีประสิทธิภาพ ลดความเสี่ยงทางไซเบอร์ และเพิ่มความน่าเชื่อถือให้กับองค์กร การนำมาตรฐานนี้มาใช้ จะช่วยให้สามารถควบคุมความเสี่ยง ปกป้องข้อมูล และปฏิบัติตามข้อกำหนดด้านกฎหมายและกฎระเบียบได้อย่างมีประสิทธิภาพ

บทที่ ๓
การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

รูปที่ ๗ การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense)

ขร. มีการดำเนินการจัดให้มีโครงสร้าง และการกำกับดูแลให้เป็นไปตามกฎหมายกำหนด ดังนี้

๑. ขร. ดำเนินการพิจารณาจัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) โดยจัดให้มีผู้ที่ทำหน้าที่ควบคุม กำกับ และตรวจสอบที่เป็นอิสระและสามารถทำหน้าที่ได้อย่างมีประสิทธิผล ซึ่งควรประกอบด้วย

๑) ผู้ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในชั้นแรก (Business Unit หรือ First Line of Defense) มีหน้าที่ดูแลและปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ที่กำหนดไว้ มีการควบคุมภายใน และมีการจัดการความเสี่ยงอย่างเหมาะสม

๒) หน่วยงานหรือผู้กำกับภายใน (Second Line of Defense) เช่น หน่วยงานบริหารความเสี่ยง (Risk Management) หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance)

๓) หน่วยงานหรือผู้ตรวจสอบภายใน (Internal Audit หรือ Third Line of Defense) เพื่อส่งเสริมให้มีกลไกการตรวจสอบและถ่วงดุลที่เหมาะสม

๒. ขร. ดำเนินการกำหนดให้มีผู้รับผิดชอบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่า โดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้ หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์

ทั้งนี้ ผู้บริหารที่ทำหน้าที่ดังกล่าว ควรมีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) รวมทั้งควรมีบทบาทหน้าที่และความรับผิดชอบให้หน่วยงานดำเนินการ เพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อย ดังนี้

๑) กำหนดให้มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

๒) มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)

๓) บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ให้สอดคล้องกับความเสี่ยงที่องค์กรมี และรายงานนำเสนอความเสี่ยงต่อคณะกรรมการหน่วยงานหรือคณะกรรมการบริหารจัดการความเสี่ยงขององค์กรอย่างสม่ำเสมอเป็นวาระประจำ

๔) ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๕) ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้ เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านภัยคุกคามทางไซเบอร์

๓. ขร. ดำเนินการจัดให้มีผู้บริหารระดับสูง ที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงานผู้ให้บริการขนส่งทางราง

ทั้งนี้ ผู้บริหารระดับสูงที่ทำหน้าที่ที่ปฏิบัติหน้าที่ดังกล่าวควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพ และประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้

๑) ดำเนินการรายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด คณะกรรมการของหน่วยงานผู้ให้บริการขนส่งทางราง และคณะกรรมการที่เกี่ยวข้องโดยตรง

๒) ดำเนินการให้ความเห็นด้านภัยคุกคามไซเบอร์ และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของหน่วยงานผู้ให้บริการขนส่งทางราง คณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือ IT risk committee และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ที่กระทบต่อหน่วยงานผู้ให้บริการขนส่งทางรางอย่างมีนัยสำคัญ

๔. ขร. ดำเนินการแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ พร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาหกสิบ (๖๐) นาที เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน

ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงานทราบภายในระยะเวลาสิบห้า (๑๕) วัน นับแต่วันที่มีการเปลี่ยนแปลง

๕. ขร. ดำเนินการแจ้งรายชื่อหน่วยงานภายในหรือบุคคลที่เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ พร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาหกสิบ (๖๐) นาทีไปยังสำนักงาน โดยบุคคลดังกล่าวต้องเป็นบุคคลผู้ซึ่งรับผิดชอบในการบริหารงานของ ขร.

ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงาน ก่อนการเปลี่ยนแปลงล่วงหน้าไม่น้อยกว่า ๗ วัน เว้นแต่มีเหตุจำเป็นอันไม่อาจล่วงรู้ได้ให้แจ้งภายในระยะเวลาสิบห้าวัน (๑๕) วัน นับแต่วันที่มีการเปลี่ยนแปลง

การเปลี่ยนแปลงข้อมูลให้รวมถึงการดำเนินการที่มีผลเป็นการเปลี่ยนแปลงเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของ ขร. เช่น การเปลี่ยนแปลงหน่วยงานต้นสังกัดของ ขร. การยุบหรือควบรวมกิจการ การเพิ่มหน่วยงานย่อยภายใน ขร.

บทที่ ๔
ประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร.

ขร. ดำเนินการจัดทำประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยมีรายละเอียดแนวปฏิบัติตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีดังนี้

(A) แนวทางการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment and Risk Management Strategy)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

เพื่อให้ ขร. สามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง ขร. จึงกำหนดแนวปฏิบัติการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้าน การรักษาความมั่นคงปลอดภัยไซเบอร์ โดยครอบคลุมกระบวนการอย่างน้อยในเรื่องดังต่อไปนี้

๑. กำหนดบริบทของความเสี่ยง (Establish Risk Context) ประกอบด้วย

๑) กำหนดคำนิยามความเสี่ยง (Define Risk) โดยพิจารณาดังนี้

- เหตุการณ์ภัยคุกคาม (Threat Event) หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม (Threat Actor) ใช้เวกเตอร์ภัยคุกคาม (Threat Vector) กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตรายในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures: TTP) ที่ใช้โดยผู้คุกคาม
- ผู้คุกคาม หมายถึง บุคคลหรือหน่วยงานที่รับผิดชอบต่อเหตุการณ์ที่อาจก่อให้เกิดอันตราย
- เวกเตอร์ภัยคุกคาม หมายถึง เส้นทางที่ผู้คุกคามใช้เพื่อโจมตีเป้าหมาย โดยระบุจุดทั้งหมด ที่สามารถเข้าถึงระบบคอมพิวเตอร์ หรือเครือข่าย
- ช่องโหว่ (Vulnerability) หมายถึง จุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สิน หรือการควบคุมภายในของกระบวนการ
- ผลกระทบที่อาจเกิดขึ้น (Impact) หรือความรุนแรง (Severity) หมายถึง ขนาดหรือระดับของความอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ หรือชุดของช่องโหว่ ความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคลที่เกี่ยวข้องกับ ขร. ทั้งภายในและภายนอก
- ระดับความเสียงที่ยอมรับได้ (Risk Appetite) คือ ความไม่แน่นอน โดยรวมที่ ขร. ยอมรับได้ โดยการดำเนินการตามภาระหน้าที่ความรับผิดชอบยังคงดำเนินการได้บรรลุตามเป้าหมาย
- ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) หมายถึง ขอบเขตของความเบี่ยงเบนที่ยอมรับได้จากเป้าหมายที่ตั้งไว้ หรือจากระดับความเสี่ยงที่กำหนดตามน Risk Appetite
- แนวโน้มหรือโอกาส (Likelihood) หมายถึง แนวโน้มหรือโอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ สามารถใช้ประโยชน์จากช่องโหว่ที่มีอยู่ หรือชุดของช่องโหว่ ซึ่งความน่าจะเป็นนี้สามารถประมาณการได้จากปัจจัยต่าง ๆ ได้แก่ ความสามารถในการค้นพบ (Discoverability) ความสามารถในการหาประโยชน์ (Exploitability) และความสามารถในการทำซ้ำ (Reproducibility)

๒) กำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Determine Risk Appetite) ควรกำหนดให้มีความชัดเจน ดังนี้

- ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) เป็นการกำหนดระดับความเสี่ยงที่ ขร. ยอมรับในการดำเนินงาน ซึ่งอาจพิจารณาจาก วัตถุประสงค์ พันธกิจ หรือวัฒนธรรมความเสี่ยง (Risk Culture) ของ ขร.
- ขีดแบ่งความเสี่ยงที่ไม่สามารถยอมรับได้ (Risk Threshold) เป็นการกำหนดเกณฑ์ที่เป็นเส้นแบ่งของความเสี่ยงที่ยอมรับได้และยอมรับไม่ได้สำหรับความเสี่ยงด้านต่าง ๆ เกณฑ์เหล่านี้ กำหนดจุดที่ความเสี่ยงไม่สามารถยอมรับได้และต้องมีการดำเนินการเพื่อจัดการความเสี่ยงที่เกิดขึ้น
- คำชี้แจงความเสี่ยงด้านความมั่นคงปลอดภัยที่ยอมรับได้ (Risk Appetite Statement) เป็นการจัดทำข้อความที่ชัดเจนและรัดกุมซึ่งแสดงถึงความมุ่งมั่นของ ขร. ที่จะยอมรับความเสี่ยงในด้านต่าง ๆ เช่น ความมั่นคงปลอดภัยทางไซเบอร์ การปกป้องข้อมูล หรือความมั่นคงปลอดภัยทางกายภาพ

ตัวอย่าง กำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Determine Risk Appetite)

- คำชี้แจงความเสี่ยงด้านความมั่นคงปลอดภัย “ในฐานะที่ ขร. มีหน้าที่กำกับดูแล พัฒนา และส่งเสริมระบบการขนส่งทางรางของประเทศไทย” จึงมีความเข้าใจและมุ่งมั่นถึงความสำคัญของข้อมูลที่เกี่ยวข้องกับการกำกับดูแล พัฒนา และส่งเสริมระบบการขนส่งทางราง จึงมีการกำหนดระดับความเสี่ยงที่ยอมรับได้ต่อเหตุการณ์ด้านความมั่นคงปลอดภัย ที่อาจส่งผลต่อความมั่นคงปลอดภัยของข้อมูลที่เกี่ยวข้องกับการกำกับดูแล พัฒนา และส่งเสริมระบบการขนส่งทางรางในระดับต่ำ”
- ระดับความเสี่ยงที่ยอมรับได้ของ ขร. ซึ่งกำหนดระดับความเสี่ยงที่ยอมรับได้เป็น “ระดับต่ำ” ต่อเหตุการณ์ด้านความมั่นคงปลอดภัยต่อข้อมูลที่เกี่ยวข้องกับการกำกับดูแล พัฒนา และส่งเสริมระบบการขนส่งทางราง
- ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) ของ ขร. ซึ่งกำหนดระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) เป็น “ระดับปานกลาง” ต่อเหตุการณ์ด้านความมั่นคงปลอดภัยต่อข้อมูลที่เกี่ยวข้องกับการกำกับดูแล พัฒนา และส่งเสริมระบบการขนส่งทางราง และต้องการดำเนินการกำหนดมาตรการในการควบคุมความเสี่ยงไม่ให้มีระดับที่สูงขึ้น
- การกำหนดเกณฑ์ขีดแบ่งความเสี่ยง ที่ไม่สามารถยอมรับได้สำหรับเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ ดังนี้
  - การละเมิดการรักษาความมั่นคงปลอดภัยของ ขร. ที่อาจนำไปสู่การเข้าถึงพื้นที่รักษาความมั่นคงปลอดภัยโดยไม่ได้รับอนุญาต ถือว่าไม่สามารถยอมรับได้
  - การโจมตีทางไซเบอร์ใด ๆ ที่ส่งผลกระทบต่อข้อมูลที่เกี่ยวข้องกับการกำกับดูแล พัฒนา และส่งเสริมระบบการขนส่งทางรางทำให้ข้อมูลรั่วไหล หรือถูกเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ถือว่าไม่สามารถยอมรับได้
  - เหตุการณ์ด้านความมั่นคงปลอดภัยทางกายภาพใด ๆ ที่เป็นภัยคุกคามต่อความมั่นคงปลอดภัยของข้อมูลที่เกี่ยวข้องกับการกำกับดูแล พัฒนา และส่งเสริมระบบการขนส่งทางราง ถือว่าไม่สามารถยอมรับได้

- การดำเนินการลดความเสี่ยง โดยการควบคุมการเข้าถึงข้อมูล และพื้นที่จัดเก็บข้อมูลที่เข้มงวด และกำหนดให้มีขั้นตอนการคัดกรองความมั่นคงปลอดภัย มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สำหรับระบบที่จัดเก็บข้อมูลที่เกี่ยวข้องกับการกำกับดูแล พัฒนา และส่งเสริมระบบการขนส่งทางราง รวมถึงการตอบสนองเหตุฉุกเฉิน

๓) กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

ดำเนินการกำหนดบทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้องในการประเมินความเสี่ยงให้ชัดเจน เพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องตระหนักถึงบทบาทหน้าที่ที่ได้รับ ซึ่งควรพิจารณาอย่างน้อยดังนี้

- หัวหน้าหน่วยงาน (Head of Organization) มีภาระหน้าที่และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้
- เจ้าของกระบวนการธุรกิจ (Business Owner) มีหน้าที่รับผิดชอบในการตรวจสอบให้แน่ใจว่ากิจกรรมตามภาระหน้าที่บรรลุเป้าหมาย รวมถึงระบุข้อกังวลเกี่ยวกับผลกระทบที่มีต่อการดำเนินการตามภาระกิจหน้าที่ในกรณีที่ระบบมีการหยุดชะงัก
- ผู้รับผิดชอบ หรือผู้ที่ได้รับมอบหมายดำเนินการเกี่ยวกับการบริหารความเสี่ยง (Risk Management Function) มีหน้าที่รับผิดชอบในการบริหารความเสี่ยงทั่วทั้ง ขร. รวมถึงทำหน้าที่เป็นหน่วยงานเชื่อมระหว่างฝ่ายงานอื่น ๆ ของ ขร. ในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยง เพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยงที่สอดคล้องกัน
- ผู้รับผิดชอบ หรือผู้ที่ได้รับมอบหมายดำเนินการด้านเทคโนโลยีและด้านการปฏิบัติ (Technology and Operations Function) มีหน้าที่รับผิดชอบในการบำรุงรักษาและปฏิบัติการเกี่ยวกับโครงสร้างพื้นฐาน ทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชันที่สนับสนุนการทำงานของระบบหรือกิจกรรมตามภาระกิจของ ขร.
- ผู้รับผิดชอบ หรือผู้ที่ได้รับมอบหมายดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function) มีหน้าที่รับผิดชอบในการดำเนินการเกี่ยวกับการบำรุงรักษาและควบคุมความมั่นคงปลอดภัยไซเบอร์ในระบบที่สนับสนุนกิจกรรมตามภาระกิจหน้าที่ของ ขร. และทำหน้าที่ระบุภัยคุกคามที่อาจเกิดขึ้นกับระบบ รวมถึงพิจารณาสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดโอกาสเสี่ยง ตลอดจนแนะนำมาตรการที่เหมาะสมเพื่อจัดการกับภัยคุกคามหรือการโจมตี

๒. ดำเนินการประเมินความเสี่ยง (Conduct Risk Assessment)

๑) การประเมินความเสี่ยง (Risk assessment)

(๑) การระบุความเสี่ยง (Risk identification)

ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าว อาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก โดยสามารถพิจารณาระบุความเสี่ยง (Risk Identification) ดังนี้

๑) ระบุทรัพย์สิน (Identify Asset) ดำเนินการระบุและสร้างทะเบียนทรัพย์สินทั้งหมดที่เป็นส่วนประกอบของระบบที่อยู่ภายในขอบเขตการประเมินความเสี่ยง โดยต้องมีการบันทึกรายการทรัพย์สิน ดังนี้

- ทรัพย์สินสำคัญ ซึ่งเป็นทรัพย์สินที่มีความสำคัญต่อการบรรลุวัตถุประสงค์หลักในการดำเนินการตามภาระกิจหน้าที่ของ ขร.
- ทรัพย์สินที่เกี่ยวข้อง เป็นทรัพย์สินที่ผู้โจมตีต้องการควบคุมและใช้ประโยชน์ เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สินสำคัญ เช่น ในระบบวินโดวส์เครื่องแม่ข่ายที่เป็นระบบบริหารจัดการจากศูนย์กลาง (Active Directory: AD) ที่เก็บรักษาหรือตรวจสอบข้อมูลการรับรองการเข้าสู่ระบบของผู้ใช้มัก
- ดำเนินการสร้างแผนผังสถาปัตยกรรมเครือข่ายที่แสดงให้เห็นถึงภาพของเส้นทางการเชื่อมต่อและการสื่อสารระหว่างทรัพย์สินสำคัญ และทรัพย์สินที่เกี่ยวข้อง และระบุช่องทางการเข้าถึง (Entry Point) ทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายของทรัพย์สินสำคัญและทรัพย์สินที่เกี่ยวข้อง

๒) สร้างแบบจำลองภัยคุกคามทางไซเบอร์ (Threat Modeling)

ดำเนินการระบุเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นจากการที่ผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์จากช่องโหว่ของทรัพย์สินแต่ละรายการ เพื่อทำการวิเคราะห์เชิงลึกทางเทคนิค โดยการสร้างแบบจำลองภัยคุกคามทางไซเบอร์มีขั้นตอนต่อไปนี้

- การระบุขอบเขตและการจำแนกระบบ (Scope Identification and System Decomposition)
- การระบุภัยคุกคามทางไซเบอร์ (Threat Identification) เป็นการระบุเหตุการณ์ที่เป็นไปได้ ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้
- การสร้างแบบจำลองการโจมตี (Attack Modelling) โดยระบุเหตุการณ์ภัยคุกคามทางไซเบอร์ หรือแนวทางการบุกรุกของผู้โจมตีที่เป็นไปได้ให้กับทรัพย์สินแต่ละรายการแล้ว

๓) สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios)

เป็นการพิจารณาถึงสถานการณ์ที่อาจมีสิ่งผิดปกติเกิดขึ้น การสมมติสถานการณ์เหล่านี้ควรจะใกล้เคียงความเป็นจริงและเหมาะสมกับบริบทของ ขร. สภาพแวดล้อมของระบบ และภัยคุกคามทางไซเบอร์ ทีเกี่ยวข้อง โดยการสร้างสถานการณ์ความเสี่ยงควรระบุองค์ประกอบหลัก ๔ ประการ ต่อไปนี้

- ทรัพย์สิน (Asset) คือ ทรัพย์สินที่ได้รับการระบุใน (๑) ระบุทรัพย์สิน (Identify Asset)
- เหตุการณ์ภัยคุกคามทางไซเบอร์ (Threat Event) คือ เหตุการณ์การโจมตีที่ระบุใน (๒) สร้างแบบจำลองภัยคุกคามทางไซเบอร์ (Threat Modeling)
- ช่องโหว่ (Vulnerability) คือ จุดอ่อนในทรัพย์สินหรือกระบวนการสนับสนุนการทำงานที่ผู้ไม่ประสงค์ดีสามารถใช้ช่องโหว่เหล่านั้นในการโจมตีหรือเข้าถึงทรัพย์สินได้ ซึ่งช่องโหว่นี้อาจทราบได้จากการตรวจสอบ (Audit) และหรือการทดสอบการเจาะระบบ หรือจากสภาพแวดล้อมของการใช้งานเทคโนโลยีหรือกระบวนการปฏิบัติงาน
- ผลที่ตามมา (Consequence) คือ ผลลัพธ์โดยตรงที่เกิดจากเหตุภัยคุกคามทางไซเบอร์

ตัวอย่าง เหตุการณ์ความเสี่ยง (Risk Scenario) ของการโจมตีแบบฟิชชิ่ง

- ผู้โจมตีส่งอีเมลฟิชชิ่งแบบเจาะจงกลุ่มเป้าหมายไปยังผู้ใช้ที่ไม่สังเกต ซึ่งเมื่อผู้ใช้คลิกอีเมล แล้วทำให้บัญชีผู้ใช้ดำเนินการตรวจสอบสิทธิ์ SMB กับเครื่องแม่ข่ายที่เป็นอันตรายและเปิดเผยข้อมูลสิ่งที่ใช้รับรองตัวตน ที่แฮชไว้

ตัวอย่าง เหตุการณ์ความเสี่ยง (Risk Scenario) ของการโจมตีแบบ SQL

- ผู้โจมตีทำการแทรก SQL บนเว็บแอปพลิเคชันเก่าที่ไม่ได้แพตช์ เพื่อสร้างโหลดเกินความจำเป็นให้กับฐานข้อมูล ทำให้ฐานข้อมูลและเว็บแอปพลิเคชันทำงานช้าลง หรือหยุดการให้บริการโดยสิ้นเชิง

(๒) การวิเคราะห์ความเสี่ยง (Risk analysis)

ดำเนินการวิเคราะห์ความเสี่ยงโดยวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์ เพื่อดำเนินการกำหนด

๑) กำหนดแนวโน้มหรือโอกาสของสถานการณ์ความเสี่ยง (Determine Likelihood) โดยประเมินความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรพิจารณาจากในแง่ของภัยคุกคามและช่องโหว่ โดยพิจารณาความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

- ความสามารถในการค้นพบ (Discoverability) เป็นปัจจัยที่ใช้พิจารณาว่าผู้โจมตี จะสามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ซึ่งความสามารถในการค้นพบมักขึ้นอยู่กับการเปิดเผยหรือมีข้อมูล เผยแพร่เกี่ยวกับช่องโหว่และทรัพย์สินที่มีช่องโหว่

- ความสามารถในการใช้ประโยชน์ (Exploitability) เป็นปัจจัยที่ใช้พิจารณาว่าผู้โจมตีจะใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ทั้งนี้ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะทางเทคนิคในการโจมตี

- ความสามารถในการทำซ้ำ (Reproducibility) เป็นปัจจัยที่ใช้พิจารณาว่าผู้โจมตีจะสามารถ ทำการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด ซึ่งขึ้นอยู่กับความซับซ้อนของการปรับแต่งวิธีการใช้ประโยชน์ จากช่องโหว่และสภาพแวดล้อมในการดำเนินการโจมตี

ตัวอย่างดังตาราง

ระดับ โอกาสที่จะเกิด	ไม่มีนัยสำคัญ หรือ ต่ำมาก (๑)	ต่ำ (๒)	ปานกลาง (๓)	สูง (๔)	สูงมาก (๕)
(๑) เปอร์เซ็นต์โอกาสที่อาจจะเกิดเหตุการณ์ความเสี่ยง	เกิดขึ้นได้ยากมาก (น้อยกว่า ๑๐%)	มีโอกาสเกิดขึ้นน้อย (๑๑% - ๒๕%)	มีโอกาสเกิดขึ้นได้ในบางครั้ง (๒๖% - ๕๐%)	มีโอกาสเกิดขึ้นค่อนข้างสูง (๕๑% - ๗๕%)	มีโอกาสเกิดขึ้นสูง (มากกว่า ๗๕%)
(๒) โอกาสที่อาจจะเกิดเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ	เหตุการณ์ผิดปกตินี้ไม่เคยเกิดขึ้นเลย หรือ คาดว่าจะมีโอกาสเกิดขึ้น >= ๑ ครั้ง มากกว่า ๓ ปี	เคยเกิดเหตุการณ์ผิดปกติขึ้นแล้ว หรือ คาดว่าจะมีโอกาสเกิดขึ้น >= ๑ ครั้ง ภายใน ๓ ปี	เคยเกิดเหตุการณ์ผิดปกติขึ้นแล้ว หรือคาดกาณ์จะมีโอกาสเกิดขึ้น >= ๑ ครั้ง ภายใน ๑ ปี	เคยเกิดเหตุการณ์ผิดปกติขึ้นแล้ว หรือ คาดว่าจะมีโอกาสเกิดขึ้น >= ๑ ครั้ง ภายใน ๑ เดือน	เคยเกิดเหตุการณ์ผิดปกติขึ้นแล้ว หรือ คาดว่าจะมีโอกาสเกิดขึ้น >= ๑ ครั้ง ภายใน ๑ สัปดาห์
(๓) โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงจากการถูกโจมตีทางไซเบอร์					
๓.๑ Discoverability จุดอ่อนของทรัพย์สิน พิจารณาจาก ผู้ไม่หวังดีสามารถค้นพบจุดอ่อนของทรัพย์สินได้ง่ายแค่ไหน	• สามารถค้นพบได้โดยการอ่าน Source Code หรือ blueprint ของระบบ/โปรแกรม หรือ • สามารถค้นพบและโจมตีได้จากการเข้าถึงด้านกายภาพ	• สามารถค้นพบได้โดยการใช้งานจากการติดตั้งจริง หรือการติดตั้งที่คล้ายกันของเป้าหมาย หรือ • สามารถค้นพบและโจมตีได้จากการเข้าถึงระบบ แบบ Local	• สามารถค้นพบได้จากโดยตรวจสอบการตอบสนองพฤติกรรม และการสื่อสารของเป้าหมาย (network sniffing) หรือ • สามารถค้นพบและโจมตีได้จากภายในเครือข่ายย่อยหรือเครือข่ายเดียวกัน	• สามารถค้นพบได้จากการสแกน Port หรือ • สามารถค้นพบและโจมตีจากเครือข่ายที่อยู่ใกล้เคียง หรือติดกัน (adjacent subnets or network segments)	• สามารถค้นพบได้จากการสแกน Public Domain หรือ • สามารถค้นพบและโจมตีจากเครือข่ายภายนอกได้ (Public Network)
๓.๒ Exploitability การโจมตี พิจารณาจาก ผู้ไม่หวังดีสามารถใช้ประโยชน์จากจุดอ่อนของทรัพย์สินได้ง่ายแค่ไหน	• สามารถโจมตีได้โดยใช้สิทธิพิเศษ (admin/ system/root) ที่ต้องมีการใช้ Multi Factor Authentication ในการเข้าถึง หรือ • สามารถทำได้ด้วยเครื่องมือเฉพาะที่ต้องใช้ความรู้ด้านเทคนิคจากผู้เชี่ยวชาญ หรือ	• สามารถโจมตีได้โดยใช้สิทธิพิเศษ (admin/ system/ root) ในการเข้าถึง หรือ • สามารถโจมตีได้โดยใช้เครื่องมือที่เฉพาะทางที่เผยแพร่เป็นสาธารณะ แต่ต้องใช้ความรู้เทคนิคระดับสูง หรือ	• สามารถโจมตีได้โดยใช้สิทธิการเข้าถึงของเป้าหมายที่มีสิทธิพิเศษ (admin/system/root) หรือ • สามารถโจมตีได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยมีความรู้เทคนิคระดับปานกลาง	• สามารถโจมตีได้โดยใช้สิทธิการเข้าถึงของเป้าหมาย (เช่น User) หรือ • สามารถโจมตีได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยมีความรู้ขั้นพื้นฐาน	• สามารถโจมตีได้โดยไม่มีสิทธิการเข้าถึงของเป้าหมาย หรือ • สามารถโจมตีได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยไม่มีต้องมีความรู้ด้านเทคนิค

ระดับ โอกาสที่จะเกิด	ไม่มีนัยสำคัญ หรือ ต่ำมาก (๑)	ต่ำ (๒)	ปานกลาง (๓)	สูง (๔)	สูงมาก (๕)
	• ต้องการการเชื่อมต่อช่องโหว่หลายอันเพื่อให้สามารถโจมตีได้	• อาจจะต้องทำการเชื่อมต่อช่องโหว่หลายอันเพื่อให้สามารถโจมตีได้			
๓.๓ Reproducibility การโจมตี พิจารณาจาก ผู้ไม่หวังดีสามารถโจมตีซ้ำทรัพย์สินได้ง่ายแค่ไหน	• ไม่สามารถทำซ้ำได้บนเป้าหมาย หรือ • สามารถทำซ้ำได้โดยใช้ช่องโหว่ที่ไม่ได้เผยแพร่เฉพาะเป้าหมาย	• สามารถทำซ้ำได้โดยมีเงื่อนไขเหตุการณ์จากการสุ่ม หรือ • สามารถทำซ้ำได้จากทฤษฎี หรือช่องโหว่ที่มีการพิสูจน์และเผยแพร่สู่สาธารณะ	• สามารถโจมตีซ้ำได้โดยมีเงื่อนไขเหตุการณ์ที่คาดการณ์ได้ หรือ • สามารถโจมตีซ้ำได้ด้วยการปรับแต่งช่องโหว่เฉพาะสำหรับเป้าหมาย	• สามารถโจมตีซ้ำได้หลายครั้งโดยมีการกำหนดค่าบางอย่างในเป้าหมาย หรือ • สามารถโจมตีซ้ำได้ด้วยการปรับแต่งช่องโหว่ที่เผยเล็กน้อย เช่น การเปลี่ยนพารามิเตอร์	• สามารถโจมตีซ้ำได้ตามต้องการโดยไม่จำเป็นต้องมีการกำหนดค่า หรือเงื่อนไขเหตุการณ์ใดๆ หรือ • สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งเครื่องมือโจมตีที่เผยแพร่ไว้

๒) กำหนดผลกระทบที่อาจเกิดขึ้น (Determine Impact) สถานการณ์ที่มีความเสี่ยงอาจเป็นอันตรายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของทรัพย์สิน เช่น ข้อมูล อุปกรณ์ต่าง ๆ และการโจมตีใด ๆ ต่อทรัพย์สินอาจส่งผลกระทบใน ๓ ระดับต่อไปนี้

- ระดับชาติ (National) ซึ่งเป็นผลกระทบที่ถูกมองว่าเป็นอันตรายต่อความมั่นคงและ เศรษฐกิจของประเทศ
- หน่วยงาน (Organizational) ซึ่งเป็นผลกระทบที่ถูกมองว่าเป็นการหยุดชะงักในการดำเนินตามภาระกิจหน้าที่ของ ขร. ซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงและการสูญเสียทางการเงิน
- บุคคล (Individual) ซึ่งเป็นผลกระทบที่สามารถมองได้ว่าเป็นการสูญเสียชีวิตและหรือการได้รับบาดเจ็บ

๓) การประเมินค่าความเสี่ยง (Risk evaluation)

ดำเนินการประเมินค่าความเสี่ยง ประกอบด้วยการดำเนินการ ดังนี้

(๑) กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritize Risk) โดยดำเนินการเปรียบเทียบสถานการณ์ความเสี่ยงกับระดับการยอมรับความเสี่ยงที่กำหนด ซึ่งสถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการตอบสนองต่อความเสี่ยงจนกว่าระดับความเสี่ยงจะอยู่ภายในระดับที่ยอมรับได้ และในการจัดลำดับความสำคัญของความเสี่ยงในการตอบสนองต่อความเสี่ยง ต้องกำหนดระยะเวลาที่คาดหวังในการดำเนินการลดความเสี่ยงให้ชัดเจน

(๒) ดำเนินการจัดทำทะเบียนความเสี่ยง (Document Risk) โดยผลลัพธ์จากการประเมินความเสี่ยงจะต้องได้รับการบันทึกไว้อย่างชัดเจนในทะเบียนความเสี่ยง เพื่อการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย และการจัดทำทะเบียนความเสี่ยงเป็นบันทึกของสถานการณ์ความเสี่ยงทั้งหมดที่ระบุ รวมถึงระดับความเสี่ยงb ที่กำหนด ซึ่งทะเบียนความเสี่ยงเป็นเอกสารที่ต้องได้รับการตรวจสอบและปรับปรุงให้ทันสมัย (Update) เป็นประจำอย่างน้อยปีละ ๑ ครั้ง ซึ่งทะเบียนความเสี่ยงควรมีข้อมูลอย่างน้อยดังต่อไปนี้

- วันที่ระบุสถานการณ์ความเสี่ยง (Identification Date)
- หมวดหมู่ทรัพย์สินที่เกี่ยวข้อง (Asset Group) ตามทะเบียนทรัพย์สิน (Inventory) ที่ได้จัดทำขึ้น
- คำอธิบายของความเสี่ยง (Description of the Risk หรือ Risk Scenario) โดยระบุรายละเอียดของสถานการณ์ที่แสดงให้เห็นว่าเหตุการณ์ภัยคุกคามสามารถใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน
- มาตรการปัจจุบัน (Existing Measures) ที่มีอยู่เพื่อจัดการกับสถานการณ์ความเสี่ยง
- โอกาสที่จะเกิดความเสี่ยง (Likelihood of Occurrence)
- ความรุนแรงของเหตุการณ์ หรือระดับผลกระทบ (Severity of the Occurrence)
- ความเสี่ยงในปัจจุบัน (Current Risk) ของสถานการณ์ความเสี่ยงหลังจากพิจารณามาตรการที่มีอยู่

- เจ้าของความเสี่ยง (Risk Owner) ที่รับผิดชอบในการดูแลความเสี่ยงที่เหลืออยู่ให้อยู่ในระดับที่ยอมรับได้

- ตัวเลือกการจัดการความเสี่ยง (Risk Treatment Option) เช่น ลดความเสี่ยง (Mitigate) โอนย้าย (Transfer) หลีกเลี่ยง (Avoid) ยอมรับความเสี่ยง (Accept)

- แผนจัดการความเสี่ยง (Risk Treatment Plan: RTP) ในกรณีที่การจัดการความเสี่ยงไม่ได้อยู่ในระดับที่ยอมรับได้ ต้องจัดทำ RTP โดยกำหนดกิจกรรมที่จะวางแผนดำเนินการ เช่น การใช้มาตรการควบคุมเพิ่มเติม และระยะเวลาในการจัดการกับความเสี่ยงในปัจจุบันให้อยู่ในระดับที่ยอมรับได้

- ความเสี่ยงที่คงเหลืออยู่ (Residual Risk) หลังจากดำเนินการตามแผนจัดการความเสี่ยง

- สถานะความคืบหน้า (Progress Status) สถานะของการดำเนินการตามแผนจัดการความเสี่ยง

๒. การจัดการความเสี่ยง (Risk Treatment/Respond)

๑) มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

๒) แนวทางการตอบสนองความเสี่ยง (Risk Respond) ควรมีการกำหนดอย่างน้อย ๔ แนวทาง ดังนี้

(๑) การควบคุม/ลดความเสี่ยง (Treat/Reduce)

(๒) การหาผู้ร่วมรับความเสี่ยง (Transfer/Share)

(๓) การหลีกเลี่ยงความเสี่ยง (Avoid/Terminate)

(๔) การยอมรับ (Accept/Take)

นอกจากนี้ ต้องกำหนดดัชนีชี้วัดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ (Key Risk Indicators) ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๓. การติดตามและทบทวนความเสี่ยง (Risk monitoring and review)

กำหนดกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๔. การรายงานความเสี่ยง (Risk reporting)

กำหนดรอบในการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของ ขร. ที่ได้รับมอบหมายเป็นประจำ อย่างน้อยปีละ ๑ ครั้ง

๕. ทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กำหนดให้มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณี

ที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ กรณีที่มีการเปลี่ยนแปลงกระบวนการที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

(B) แนวทางการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้มีการจัดทำและสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ ให้ผู้เกี่ยวข้องทราบและมีการตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของ ขร. อย่างน้อยปีละ ๑ ครั้ง

๒. จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยต้องระบุรายละเอียดอย่างน้อย ดังนี้

๑) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคน และรายละเอียดการติดต่อ

๒) โครงสร้างการรายงานเหตุการณ์ซึ่งกำหนดว่า ขร. จะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายย่อยใดๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้อง

๓) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

๔) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๑) การเรียกใช้งานกระบวนการกู้คืน

(๒) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๓) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึง แต่ไม่จำกัดเพียงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๔) ระเบียบวิธีการมีส่วนร่วม (Engagement protocols) กับบุคคลภายนอกรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์ / การกู้คืน และการบังคับใช้กฎหมาย เพื่อดำเนินคดี

(๕) กระบวนการทบทวนหลังการดำเนินการ (After-action review process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๓. ดำเนินการการทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง นับแต่วันที่แผนได้รับการอนุมัติ โดยเริ่มทบทวนตั้งแต่การจัดทำแผนฯ เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล หรือดำเนินการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงกลยุทธ์และข้อกำหนดของ ขร. ระเบียบข้อบังคับ และกฎหมายที่เกี่ยวข้อง ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และภูมิทัศน์ ภัยคุกคามทางไซเบอร์ และสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของการให้บริการที่สำคัญของ ขร. และควรดำเนินการทบทวนเพิ่มเติมเมื่อมีเหตุการณ์ ดังนี้

(ก) บทเรียนจากการปฏิบัติการตอบสนองต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นจริงในแต่ละวัน

(ข) สิ่งที่ได้จากการฝึกหัด/การอบรม

(ค) ผลที่ได้จากการฝึกซ้อมและข้อเสนอแนะหลังจากการฝึกซ้อมตามแผนการรับมือภัยคุกคามทางไซเบอร์ดังกล่าว

(ง) กลยุทธ์และข้อกำหนดของหน่วยงานที่อาจมีการเปลี่ยนแปลง

(จ) สภาพแวดล้อมของการปฏิบัติการทางไซเบอร์ของการให้บริการในหน่วยงานที่สำคัญที่อาจมีการเปลี่ยนแปลง

(ฉ) ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และภูมิทัศน์ภัยคุกคามทางไซเบอร์ (Threat Landscape) ที่มีการเปลี่ยนแปลง

(ช) ระเบียบ ข้อบังคับ และกฎหมายใหม่

(ซ) เทคโนโลยีใหม่

(ฌ) การเปลี่ยนแปลงยุทธศาสตร์ระดับชาติที่เกี่ยวข้องกับลำดับความสำคัญของระบบสารสนเทศหรือของการดำเนินงานตามภารกิจของหน่วยงาน

(ญ) ข้อมูลที่ได้จากระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence: CTI)

๔. ดำเนินการฝึกซ้อมแผนการรับมือภัยคุกคามไซเบอร์ที่กำหนดขึ้น อย่างน้อยปีละ ๑ ครั้ง

(C) การจัดการทรัพย์สิน (Asset Management)

๑. กำหนดให้มีการบริหารจัดการทรัพย์สิน โดยพิจารณาอย่างน้อยดังนี้

๑) กำหนดให้มีการจัดทำบัญชีทรัพย์สิน (Asset Inventory) หรือนำระบบการบริหารจัดการทรัพย์สินมาช่วยในการบริหารจัดการทรัพย์สิน ที่ระบุทรัพย์สินของบริการที่สำคัญ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยการจัดทำบัญชีทรัพย์สินครอบคลุมทั้ง ข้อมูลและสารสนเทศ (Information) ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) เครือข่าย (Network) บุคลากร (Personnel) สถานที่ (Site) Cloud Assets เป็นต้น ซึ่งทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

(๑) ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. เช่น ชื่อและคำอธิบายข้อมูลกำหนด คุณลักษณะของฮาร์ดแวร์ เครื่องเสมือน ซอฟต์แวร์ อุปกรณ์เครือข่าย

(๒) หมวดหมู่ทรัพย์สิน (Asset Group) โดยหน่วยงานอาจจัดให้ทรัพย์สินที่เกี่ยวข้องกันอยู่ในหมวดหมู่เดียวกัน (เช่น กลุ่มของฮาร์ดแวร์และซอฟต์แวร์ที่ใช้สำหรับการให้บริการแต่ละบริการ) หรือจัดหมวดหมู่ทรัพย์สินตามประเภททรัพย์สินย่อย (Asset Subtype)

(๓) ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. โดยหากเกิดการแก้ไข เสียหาย สูญเสียไปแล้วจะมีผลต่อการปฏิบัติงานตามภารกิจของ ขร.

(๔) การระบุและการจัดลำดับความสำคัญของของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร.

(๕) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร.

(๖) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. แต่ละรายการ

(๗) การขึ้นต่อกันของทรัพย์สินของของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. บนระบบ/เครือข่ายภายใน และ/หรือภายนอก เช่น เครื่องแม่ข่ายให้บริการเบิกสวัสดิการผู้ปฏิบัติงานต้องดึงข้อมูลจากเครื่องแม่ข่ายที่ให้บริการฐานข้อมูลผู้ปฏิบัติงาน และต้องส่งข้อมูลผ่านสวิตช์หลัก

๒) ระบุขอบเขตเครือข่ายของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface) เช่น โซน Demilitarized (DMZ) สำหรับให้ผู้ใช้ภายนอกสามารถเข้าถึงได้ และโซนที่อยู่ภายในที่ป้องกันไม่ให้ผู้ใช้ภายนอกเข้าถึง โดยการพิจารณาระบุขอบเขตของเครือข่ายของบริการที่สำคัญ ควรพิจารณาดำเนินการ ดังนี้

- พิจารณาทุกทรัพย์สินของทุกบริการที่สำคัญ เพื่อระบุจุดที่ข้อมูลไหลเข้าและออกจากเครือข่าย (Entry and Exit Point) เช่น จุดที่มีการเชื่อมต่ออินเทอร์เน็ต จุดที่ยอมให้มีการเข้าถึงจากระยะไกล (Remote Access) และจุดที่มีการเชื่อมต่อกับหน่วยงานอื่นที่เป็นหน่วยงานพันธมิตร (Partner)
- พิจารณาเทียบกับแผนภาพเครือข่าย (Network Diagram) ที่มีอยู่ เพื่อนำมาสร้างแผนภาพขอบเขตของเครือข่ายของบริการที่สำคัญ ซึ่งแสดงถึงอุปกรณ์เครือข่าย ไฟร์วอลล์ ระบบตรวจจับการบุกรุก ระบบป้องกันการบุกรุก และเครือข่ายเสมือน รวมถึงการเชื่อมต่อของแต่ละทรัพย์สินที่เกี่ยวข้องกับบริการที่สำคัญ ทั้งการเชื่อมต่อทางกายภาพ และการเชื่อมต่อเชิงตรรกะ (Physical and Logical Connection)
- ดำเนินการตรวจสอบ และทบทวนขอบเขตของเครือข่าย รวมถึงปรับปรุงทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. โดยพิจารณาหัวข้อในการตรวจสอบ และทบทวน ดังนี้

(๑) ตรวจสอบความถูกต้องของข้อมูลในทะเบียน โดยตรวจสอบและทบทวน ชื่อ คำอธิบาย หมวดหมู่ ทรัพย์สิน ลำดับความสำคัญ เจ้าของ ตำแหน่ง และการขึ้นต่อกันของทรัพย์สิน เช่น การปรับปรุงเวอร์ชันของซอฟต์แวร์ การปรับระดับความสำคัญของระบบสารสนเทศให้สูงขึ้นในกรณีที่กฎหมายใหม่มีผลบังคับใช้ หรือการเชื่อมต่ออุปกรณ์ใหม่เข้ากับทรัพย์สินในทะเบียน

(๒) จำนวนของทรัพย์สิน (Inventory Status) เช่น การตรวจนับจำนวนทรัพย์สิน

(๓) สถานะเชิงคุณภาพของทรัพย์สิน เช่น การตรวจสอบทรัพย์สินที่ชำรุด เสื่อมสภาพ สูญไป หรือทรัพย์สินที่ไม่จำเป็นต้องใช้ ในกรณีที่ทรัพย์สินอยู่ในสถานะชำรุด เสื่อมสภาพ หรือสูญไป ต้องดำเนินการสอบหาสาเหตุ พร้อมทั้งระบุผู้ที่เข้าข่ายต้องรับผิดชอบต่อความเสียหาย

(๔) ข้อกำหนดด้านความมั่นคงปลอดภัยของทรัพย์สิน (Security Requirement) เช่น กฎหมาย หรือมาตรฐานที่เปลี่ยนแปลงไปหรือที่ถูกกำหนดขึ้นใหม่ การเปลี่ยนแปลงของระยะเวลาการกู้ข้อมูลที่ยอมรับได้ ระยะเวลาสูงสุดที่ยอมให้การดำเนินการตามภาระกิจหน้าที่หยุดชะงัก (Maximum Tolerable Downtime) ระยะเวลาในการกู้คืนระบบ (Recovery Time Objective) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective)

(๕) กลยุทธ์และมาตรการควบคุม เพื่อการป้องกันทรัพย์สินและบริการ เช่น การกำหนดให้ใช้การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-factor Authentication) สำหรับการเข้าถึงระบบสารสนเทศที่มีความเสี่ยงต่อการถูกโจมตีมากขึ้น การกำหนดวิธีการเข้ารหัสข้อมูลที่มีความอ่อนไหวให้มีความปลอดภัยมากขึ้น โดยการเพิ่มจำนวนบิตที่ใช้การเข้ารหัส การใช้เทคโนโลยีใหม่ที่สามารถกู้ข้อมูลได้เร็วขึ้น

(๖) กลยุทธ์และแผนความต่อเนื่องให้กับทรัพย์สินและบริการ เช่น การทบทวนแผนความต่อเนื่อง (Continuity Plan) และแผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan)

ทั้งนี้ การตรวจสอบ และทบทวนทรัพย์สินต้องกำหนดให้มีการนำเสนอสถานะปัจจุบันของทรัพย์สินต่อผู้บริหารระดับสูงอย่างสม่ำเสมอตามรอบที่กำหนด

๓) กำหนดให้มีการบริหารจัดการทรัพย์สิน (Asset Management) ตั้งแต่เริ่มจัดทำรายการทรัพย์สินจนถึงการบำรุงรักษา (Maintaining) รายการทรัพย์สินให้ถูกต้องครบถ้วน ซึ่งข้อมูลที่นำมาจัดทำรายการทรัพย์สินสามารถข้อมูลนำมาจากฐานข้อมูลการจัดการทรัพย์สินของ ขร. หรือดำเนินการสำรวจข้อมูลที่กับหน่วยงานภายในที่เกี่ยวข้องกับบริการที่สำคัญ หรือระบบงานที่สำคัญ หรือจากรายการทรัพย์สินของผู้ให้บริการภายนอกในกรณีที่มีการใช้บริการผู้ให้บริการภายนอกจัดหา ทั้งนี้ต้องจัดให้มีการบริหารจัดการทรัพย์สินด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ควรมีการพิจารณาดำเนินการ ดังนี้

(๑) ดำเนินการบริหารความเสี่ยง (Risk Management) โดยการทำความเข้าใจและดำเนินการจัดการความเสี่ยงทางไซเบอร์ที่เกี่ยวข้องอยู่กับทรัพย์สินของบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. ตามลำดับความสำคัญของความเสี่ยง รวมถึงติดตาม ทบทวนความเสี่ยงอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๒) การบริหารจัดการทรัพย์สินล้าสมัย (Managing Legacy) หากซอฟต์แวร์และฮาร์ดแวร์ล้าสมัยการใช้ทรัพย์สินหรือผลิตภัณฑ์นั้นอาจก่อให้เกิดความเสี่ยงหรือต้นทุนสำหรับการลดความเสี่ยงเพิ่มขึ้น จึงควรมีการดำเนินการจัดการทรัพย์สินติดตามการสนับสนุนทรัพย์สินหรือผลิตภัณฑ์เป็นระยะ เพื่อติดตามการประกาศการให้การสนับสนุนได้สิ้นสุดลง (End of Support) ของผู้ผลิตและดำเนินการวางแผนปรับปรุงเปลี่ยนแปลงล่วงหน้า

(๓) กำหนดให้มีการจัดการข้อมูลประจำตัวและการเข้าถึง (Identity and Access Management) ทรัพย์สินนั้น ๆ โดยให้มีการระบุผู้ใช้และอุปกรณ์ที่ใช้งาน เพื่อควบคุมการเข้าถึง (Access Control) ทรัพย์สิน และทรัพยากรของ ขร.

(๔) กำหนดให้มีการดำเนินการประเมินช่องโหว่และการจัดการแพตช์ (Vulnerability and Patch Management) อย่างสม่ำเสมอ

(๕) กำหนดให้มีการเฝ้าระวังการใช้งานทรัพย์สิน (Monitoring) โดยการตรวจจับ (Detect) และสืบสวน (Investigate) การบุกรุกที่อาจเกิดขึ้นก่อนดำเนินการลดภัยคุกคาม

(๖) การจัดการเหตุภัยคุกคามทางไซเบอร์การตอบสนองและการฟื้นฟู (Incident Management, Response and Recovery) โดยดำเนินการวางแผน ตอบสนอง และกู้คืนจากเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เพื่อลดการหยุดชะงักการให้บริการ (Minimize Disruption)

๔) ในกณีที่มีการพิจารณานำระบบการจัดการทรัพย์สินมาใช้บริหารจัดการ ควรมีการดำเนินพิจารณาการออกแบบระบบให้สามารถดำเนินการได้ ดังนี้

- การค้นหาทรัพย์สิน (Asset Discovery) เพื่อสแกนสภาพแวดล้อมของ ขร. เพื่อหาทรัพย์สินใหม่หรือลบรายการทรัพย์สินเก่าออกอย่างสม่ำเสมอและต่อเนื่อง
- เก็บข้อมูลจากแหล่งข้อมูลที่เชื่อถือ และข้อมูลที่ถูกต้อง (Authoritative Source of Information & Accurate Source of Information) โดยการกำหนดมาตรฐานสำหรับทะเบียนทรัพย์สินเพื่อหลีกเลี่ยงการบันทึกข้อมูลที่ซ้ำซ้อน และออกแบบระบบให้ผู้ใช้สามารถเข้าถึงข้อมูลได้ง่ายขึ้น รวมถึงข้อมูล

ทรัพย์สินควรถูกรวบรวมและอัปเดตอย่างสม่ำเสมอ และควรดำเนินการจัดทำรายการความถี่ในการอัปเดตข้อมูลตามความ เหมาะสมหรือระดับการเปลี่ยนแปลงของประเภททรัพย์สิน เช่น

(ก) เครื่องแม่ข่าย (Server) ดำเนินการอัปเดตข้อมูลเป็นรายเดือนหรือรายไตรมาส เนื่องจากมีการเปลี่ยนแปลงไม่บ่อย

(ข) เครื่องเดสก์ท็อป (Desktop) ดำเนินการอัปเดตข้อมูลเป็นรายสัปดาห์หรือรายเดือน เพื่อรองรับการจัดการค่ากำหนด (Configuration) และการจัดการช่องโหว่ (Vulnerability Management) การกำหนดรอบการอัปเดตตามระดับความสำคัญของระบบ

- ความพร้อมใช้งานของข้อมูลทรัพย์สิน (Availability of Asset Information) โดยจัดให้มีการบริหารจัดการกำหนดค่าฐานข้อมูล (Configuration Management Database: CMDB) รวมถึงกำหนดให้มีการตรวจสอบ และปรับปรุงค่าที่กำหนดอย่างสม่ำเสมอ
- พิจารณาการนำไปใช้งานของผู้ใช้งาน (Human Factors) เช่น ความสะดวกในการใช้งาน (Usability) และความสะดวกในการเข้าถึง (Accessibility) รวมถึงนำแนวทางที่เน้นปฏิบัติงานที่ใช้ได้จริง (Pragmatic Approach) มาเป็นหลักการในการพัฒนาหรือจัดหาระบบ
- พิจารณาใช้ระบบอัตโนมัติ (Automation) เป็นกลไกในการปรับปรุงรายการทรัพย์สินที่ถูกใช้งานได้จริงให้เป็นปัจจุบัน
- การทำงานของระบบครอบคลุม (Comprehensive Visibility) ตามจุดประสงค์และวิธีการใช้ข้อมูลทรัพย์สินที่ ขร. กำหนดขึ้น และมีข้อมูลที่ละเอียดเพียงพอตามวัตถุประสงค์ของ ขร. เช่น การระบุเวอร์ชันของซอฟต์แวร์ทั้งหมดที่ติดตั้งในเครื่องคอมพิวเตอร์ของ ขร.
- สามารถตรวจจับการเปลี่ยนแปลง (Change Detection) ข้อมูลทรัพย์สินได้รับการบันทึก และใช้แหล่งข้อมูลหลายแหล่งเพื่อระบุความไม่สอดคล้อง กัน (Identify Inconsistencies) เช่น พบอุปกรณ์ใหม่บนเครือข่ายและยังไม่ได้ถูกลงทะเบียน
- การรักษาความลับ (Confidentiality) โดยพิจารณาให้สามารถกำหนดให้มีการเข้าถึงได้ตามสิทธิ์การเข้าถึงตามหน้าที่ความรับผิดชอบ เพื่อดำเนินการการป้องกันและการจำกัดการเข้าถึงที่เหมาะสมกับระดับความอ่อนไหว รวมถึงกำหนดให้มีการเฝ้าระวังการเข้าถึงข้อมูลทรัพย์สิน เช่น ตรวจสอบ log เข้าถึงอย่างสม่ำเสมอ หรือเมื่อมีเหตุผิดปกติ
- สามารถจัดประเภททรัพย์สิน (Asset Classification) โดยกำหนดประเภททรัพย์สินและจำแนกทรัพย์สินให้สอดคล้องกับแนวทางการบริหารความเสี่ยงของ ขร. เช่น การจัดประเภทตามความอ่อนไหวของข้อมูลที่ประมวลผล หรือความสำคัญของระบบต่อภารกิจหน้าที่ของ ขร.

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑) กำหนดภาระหน้าที่ความรับผิดชอบบริหารจัดการต่อทรัพย์สินอย่างชัดเจน และกำหนดให้มีการลงนามยอมรับข้อตกลงการใช้งานทรัพย์สิน เช่น คอมพิวเตอร์แบบพกพา (Notebook) พร้อมทั้งกำหนดให้มีการอบรมแนวทางการใช้และดูแลรักษาทรัพย์สินก่อนการใช้งาน

๒) กำหนดให้มีผู้รับผิดชอบถือครองทรัพย์สินที่ชัดเจน เพื่อรับผิดชอบในการดูแลติดตาม และรายงานการสูญหายหรือชำรุด

๓) กำหนดให้มีการใช้ทรัพย์สินอย่างเหมาะสม โดยการพิจารณาให้มีมาตราการควบคุมอย่างน้อย ดังนี้

(๑) ใช้ทรัพย์สินตามวัตถุประสงค์ทางราชการ หรือขององค์กร ภายใต้หน้าที่ความรับผิดชอบที่ได้รับมอบหมายเท่านั้น

(๒) ห้ามติดตั้งซอฟต์แวร์หรือเชื่อมต่อกับอุปกรณ์ส่วนตัวโดยไม่ได้รับอนุญาต

(๓) กำหนดให้มีแนวปฏิบัติการใช้งานเทคโนโลยีสารสนเทศ (Acceptable Use Policy) และกฎระเบียบด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

๔) กำหนดให้มีการควบคุมการคืนทรัพย์สิน โดยพิจารณาอย่างน้อย ดังนี้

(๑) เมื่อผู้ใช้งานลาออก เปลี่ยนตำแหน่ง หรือพ้นจากหน้าที่ความรับผิดชอบ ต้องดำเนินการคืนทรัพย์สินให้กับองค์ตามกระบวนการ หรือขั้นตอนการคืนทรัพย์สินขององค์กร พร้อมทั้งกำหนดให้มีการจัดเก็บหลักฐานการคืนทรัพย์สิน และการตรวจสอบทรัพย์สินก่อนรับทรัพย์สินคืน

(๒) หากทรัพย์สินนั้นมีข้อมูลสำคัญ ต้องมีการดำเนินการกำหนดให้มีการลบข้อมูล (Sanitization) ก่อนส่งต่อหรือก่อนนำไปทำลาย

๕) กำหนดให้มีการบริหารจัดการนำทรัพย์สินขององค์กรออกนอกสถานที่ (Off-site Asset Control and Security Management) ต้องดำเนินการขออนุมัติจากผู้มีอำนาจก่อนนำทรัพย์สินออกนอกสถานที่ และกำหนดให้มีหลักฐานการขอนำทรัพย์สินออกนอกสถานที่ (Asset Movement Request Form) รวมถึงระบุรายละเอียดอย่างน้อย ดังนี้ ประเภทอุปกรณ์, หมายเลขทรัพย์สิน, ผู้ใช้งาน, จุดประสงค์, ระยะเวลาใช้งาน และสถานที่ปลายทาง เป็นต้น รวมถึงบันทึกทะเบียนการนำทรัพย์สินออกนอกสถานที่

๖) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของอุปกรณ์ โดยพิจารณาอย่างน้อย ดังนี้

(๑) ดำเนินการติดตั้งระบบรักษาความปลอดภัยพื้นฐาน เช่น Antivirus, Firewall, Full-disk Encryption เป็นต้น

(๒) อุปกรณ์ต้องมีรหัสผ่านหรือวิธีการพิสูจน์ตัวตนตามระดับความเสี่ยงของการนำไปใช้งาน เช่น MFA

(๓) ห้ามเก็บข้อมูลสำคัญในอุปกรณ์โดยไม่มีการเข้ารหัส

(๔) ห้ามใช้อุปกรณ์ขององค์กรร่วมกับเครือข่ายที่ไม่ปลอดภัยโดยไม่มี VPN หรือระบบรักษาความปลอดภัย

๗) กำหนดให้มีการควบคุมในระหว่างใช้งาน โดยพิจารณาอย่างน้อยดังนี้

(๑) ผู้ใช้งานต้องไม่ปล่อยให้อุปกรณ์ถูกทิ้งไว้โดยไม่มีการดูแล หรือใช้งานในพื้นที่สาธารณะที่มีความเสี่ยง

(๒) หากเกิดการสูญหาย หรือถูกขโมย ต้องดำเนินการรายงานต่อฝ่ายเทคโนโลยีสารสนเทศภายใน ๒๔ ชั่วโมง

(๓) ห้ามติดตั้งซอฟต์แวร์ใด ๆ เพิ่มเติม หรือเปลี่ยนแปลงการตั้งค่าโดยไม่ได้รับอนุญาต

๘) กำหนดให้มีการส่งคืนและตรวจสอบ โดยพิจารณาอย่างน้อยดังนี้

(๑) หลังสิ้นสุดการใช้งานนอกสถานที่ ต้องส่งคืนทรัพย์สินให้ฝ่ายเทคโนโลยีสารสนเทศ หรือฝ่ายที่ได้รับมอบหมายภายในเวลาที่กำหนด

(๒) ดำเนินการตรวจสอบความสมบูรณ์ของอุปกรณ์ และล้างข้อมูลที่ไม่จำเป็นออกจากอุปกรณ์

(๓) อัปเดตสถานะในทะเบียนสินทรัพย์ เพื่อบันทึกการคืนและความสมบูรณ์ของทรัพย์สิน

๙) กำหนดให้มีการกำจัดหรือทำลายอุปกรณ์ที่หมดอายุการใช้งาน โดยพิจารณาอย่างน้อย ดังนี้

(๑) ดำเนินการตรวจสอบและบันทึกข้อมูลในทะเบียนสินทรัพย์ก่อนทำลายหรือถ่ายโอน

(๒) ดำเนินการล้างข้อมูลอย่างปลอดภัย (Data Sanitization) ด้วยวิธีการที่รับรองได้ เช่น

๑) การเขียนทับหลายรอบ (Overwrite)

๒) การล้างด้วยซอฟต์แวร์มาตรฐาน (Wipe tools)

๓) การทำลายทางกายภาพ เช่น การบด การเผา หรือการเจาะ

(๓) จัดให้มีหลักฐานการทำลาย เช่น แบบฟอร์มยืนยัน, ภาพถ่าย, รายงานการทำลายจากผู้รับจ้าง เป็นต้น

(๔) ดำเนินการโดยบุคลากรที่ได้รับอนุญาต หรือผู้ให้บริการที่มีข้อตกลงความมั่นคงปลอดภัยที่ชัดเจน เช่น NDA, SLA เป็นต้น

๑๐) กำหนดให้มีการควบคุมการนำอุปกรณ์ไปใช้งานซ้ำ (Reuse/Repurpose) โดยพิจารณาอย่างน้อย ดังนี้

(๑) ดำเนินการตรวจสอบให้แน่ใจว่าได้ล้างข้อมูลจากอุปกรณ์อย่างครบถ้วนก่อนการนำอุปกรณ์ไปใช้งาน

(๒) อัปเดตทะเบียนสินทรัพย์ และระบุการเปลี่ยนแปลงผู้ใช้งาน หรือหน่วยงานที่ได้รับอุปกรณ์ไปใช้งาน

(๓) กำหนดให้มีการตั้งค่าความมั่นคงปลอดภัยพื้นฐาน (Baseline Configuration) ก่อนการแจกจ่ายให้กับหน่วยงาน รวมถึงปรับระดับสิทธิและการเข้าถึงให้เหมาะสมกับผู้ใช้งานใหม่

๑๑) กำหนดให้มีการจัดการอุปกรณ์ที่ถูกปล่อยทิ้ง (Unattended Equipment) โดยพิจารณาอย่างน้อย ดังนี้

(๑) อุปกรณ์ที่พบนอกพื้นที่ควบคุม หรือถูกทิ้งไว้โดยไม่มีเจ้าของชัดเจน ต้องถูกนำมาจับเก็บในพื้นที่ปิด และมีการควบคุม

(๒) ผู้ที่พบเห็น หรือผู้ดูแลพื้นที่ต้องรายงานต่อฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายทันที

(๓) ดำเนินการตรวจสอบความเสี่ยง เช่น การเชื่อมต่อเครือข่าย หรือข้อมูลในเครื่อง เป็นต้น

(๔) จัดเก็บอุปกรณ์ในที่ปลอดภัย และเก็บบันทึกการตรวจพบและดำเนินการไว้สำหรับตรวจสอบย้อนหลัง

๑๒) กำหนดให้มีการกำหนดระดับชั้นความลับของทรัพย์สินสารสนเทศ โดยพิจารณาอย่างน้อย ดังนี้

(๑) พิจารณากำหนดระดับชั้นความลับของข้อมูล โดยกำหนดให้มีระดับชั้นความลับอย่างต่ำ ๓-๔ ระดับชั้น เช่น ลับที่สุด ลับมาก ลับ และสาธารณะ พร้อมทั้งคำอธิบายในการเข้าถึงแต่ละระดับชั้นความลับ

(๒) กำหนดให้มีการบ่งชี้ระดับชั้นความลับของสารสนเทศ (Labeling & Marking) โดยการพิจารณาอย่างน้อย ดังนี้

(๒.๑) ข้อมูลที่ถูกจัดระดับชั้นความลับต้องมี สัญลักษณ์ระบุระดับชั้นความลับ (Label) เช่น บนหัวกระดาษ, ชื่อไฟล์, Metadata หรือ Watermark เป็นต้น และในกรณีที่เป็นเอกสารหรือข้อมูลในรูปแบบอิเล็กทรอนิกส์ไฟล์ ให้พิจารณากำหนดให้มีข้อความระบุระดับความลับที่ชัดเจนทุกหน้า

(๒.๒) พิจารณาใช้ระบบช่วยในการชี้บ่งระดับชั้นความลับ (Tag) อัตโนมัติ เช่น DLP, Microsoft Purview, Data Classification Tool เป็นต้น

(๒.๓) พิจารณากำหนดการจัดการทรัพย์สินตามชั้นความลับ เช่น ข้อมูลที่เป็น "ลับมากที่สุด" ต้องจัดให้มีการเข้ารหัสระหว่างจัดเก็บและส่งต่อ (Encryption at rest/in transit) กำหนดให้มีการจัดเก็บในระบบที่มีการควบคุมการเข้าถึง ห้ามนำข้อมูลลับใส่ USB โดยไม่ได้รับอนุญาต เป็นต้น รวมถึงการทำลายข้อมูลต้องกำหนดวิธีที่เหมาะสมตามระดับชั้นความลับ เช่น Overwrite, Degauss, Physical Destruction เป็นต้น

๑๓) กำหนดให้มีการบริหารจัดการเข้ารหัสข้อมูลตามระดับชั้นความลับ โดยพิจารณาใช้อัลกอริทึมที่สอดคล้องกับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการเกี่ยวกับการเข้ารหัสข้อมูลเป็นไปในทิศทางเดียวกัน

๑๔) จัดให้มีและปฏิบัติตามขั้นตอนปฏิบัติการบริหารจัดการกุญแจเข้ารหัสข้อมูล เพื่อให้มีกระบวนการที่รัดกุมตลอดช่วงเวลาการใช้งาน (Key management whole life cycle) โดยมีการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของกุญแจเพื่อเข้ารหัส การจัดเก็บ การใช้งาน และการยกเลิกการใช้งานกุญแจรหัส

๑๕) มีการอนุญาตการเข้าถึงรหัสลับเฉพาะผู้ที่ รับผิดชอบเท่านั้น เพื่อป้องกันการถูกแก้ไข หรือเปิดเผยรวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามขั้นตอนปฏิบัติดังกล่าวอย่างเคร่งครัด

๑๖) กำหนดให้มีการบริหารจัดการความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล โดยระบุข้อมูลส่วนบุคคลและการทำบันทึกรายการประมวลผล (ROPA) ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

๑๗) กำหนดให้มีหลักการประมวลผลข้อมูลส่วนบุคคล โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

(๑) กำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่ชัดเจน และใช้ข้อมูลเท่าที่จำเป็น (Data Minimization)

(๒) ใช้ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสม เช่น ความยินยอม (Consent) สัญญา หรือภาระหน้าที่ทางกฎหมาย เป็นต้น

(๓) กำหนดให้มีการแจ้งวัตถุประสงค์ต่อเจ้าของข้อมูล (Privacy Notice) ก่อนดำเนินการจัดเก็บหรือใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์

(๔) กำหนดให้มีการจัดเก็บข้อมูลให้นานเท่าที่จำเป็น และระบุระยะเวลาที่สามารถระบุได้ รวมถึงทำลายข้อมูลอย่างเหมาะสมตามระดับชั้นความลับของข้อมูลเมื่อหมดวัตถุประสงค์

๑๘) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

(๑) กำหนดให้มีการเข้ารหัสข้อมูล (Encryption) และควบคุมสิทธิการเข้าถึงข้อมูลเท่าที่จำเป็นตามหน้าที่ความรับผิดชอบ (Role-Based Access Control: RBAC) รวมถึงมาตรการควบคุมที่เหมาะสม เช่น การพิสูจน์ตัวตนก่อนเข้าถึงข้อมูล เป็นต้น

(๒) กำหนดให้มีแผนสำรองและกู้คืนข้อมูลในกรณีเกิดเหตุฉุกเฉินด้านความมั่นคงปลอดภัย (Backup & Recovery)

๑๙) กำหนดให้มีสิทธิของเจ้าของข้อมูล (Data Subject Rights) ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนด เช่น สิทธิการเข้าถึง สิทธิขอลบข้อมูล เป็นต้น รวบถึงกำหนดกระบวนการบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล

๒๐) กำหนดให้มีการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Management) โดยกำหนดให้การจัดทำแผนการตอบสนองต่อเหตุการณ์ข้อมูลรั่วไหล รวมถึงกำหนดให้มีการแจ้งฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย ในกรณีที่พบเหตุการรั่วไหลของข้อมูลส่วนบุคคลภายใน ๒๔ ชั่วโมง เมื่อทราบเหตุ

๒๑) กำหนดให้มีการบริหารจัดการถ่ายโอนสารสนเทศ โดยจัดทำข้อตกลงการถ่ายโอนโดยพิจารณาอย่างน้อย ดังนี้

(๑) กำหนดข้อตกลงการถ่ายโอนข้อมูลโดยพิจารณาจากวัตถุประสงค์การถ่ายโอน ประเภทของข้อมูล ความสำคัญของข้อมูล และระดับความลับของข้อมูล

(๒) จัดให้มีข้อตกลงในการถ่ายโอนข้อมูล (Information Sharing Agreement / Data Transfer Agreement) กรณีที่ต้องดำเนินการส่งข้อมูลให้บุคคลภายนอก

(๓) ระบุสิทธิ์และบทบาทของผู้ส่งและผู้รับในการรักษาข้อมูล เช่น ห้ามส่งต่อ ห้ามใช้ซ้ำ โดยไม่ได้รับอนุญาต เป็นต้น

(๔) กำหนดช่องทางในการถ่ายโอนข้อมูลที่ชัดเจน เช่น ผ่านช่องทางอีเมลที่กำหนดโดยเฉพาะ หรือระบบคลาวด์ที่มีการเข้ารหัสข้อมูลและกำหนดสิทธิในการเข้าถึงเฉพาะผู้ที่มีสิทธิเข้าถึงเท่านั้น รวมถึงจัดให้มีการเก็บรักษาหลักฐานการถ่ายโอนข้อมูล (Transfer Log)

(๕) ตรวจสอบความสมบูรณ์ของข้อมูลหลังการรับ-ส่ง หากพบการเปลี่ยนแปลงหรือสูญหายต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายทันที

(๖) ไม่อนุญาตให้มีการถ่ายโอนข้อมูลผ่านอุปกรณ์พกพาส่วนตัวโดยไม่มีการขออนุมัติ และมาตรการควบคุม

(๗) จัดให้มีช่องทางในการรายงานเหตุการณ์ผิดปกติจากการถ่ายโอน เช่น ข้อมูลหลุด ข้อมูลสูญหาย เป็นต้น รวมถึงวิเคราะห์เหตุการณ์และทบทวนมาตรการ เพื่อป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำ

๒๒) กำหนดให้มีมาตรการเพิ่มเติมสำหรับการถ่ายโอนข้อมูลส่วนบุคคล โดยพิจารณาอย่างน้อย ดังนี้

(๑) ดำเนินการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA) หากมีการส่งข้อมูลส่วนบุคคลจำนวนมากหรือข้อมูลส่วนบุคคลละเอียดอ่อน

(๒) พิจารณาใช้ระบบป้องกันข้อมูลรั่วไหล (Data Loss Prevention – DLP) เพื่อควบคุมการส่งข้อมูลส่วนบุคคลไปยังภายนอก

(๓) พิจารณาใช้เทคนิค Masking หรือ Anonymization ในกรณีที่จำเป็นต้องถ่ายโอนข้อมูลส่วนบุคคลไปยังภายนอก

๒๓) จัดให้มีการบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ โดยพิจารณาอย่างน้อย ดังนี้

(๑) จัดทำทะเบียนซอฟต์แวร์ (Software Inventory) ที่มีการบันทึกรายละเอียด เช่น ชื่อซอฟต์แวร์, เวอร์ชัน, หมายเลขลิขสิทธิ์ (License Key), วันที่หมดอายุ และสถานะการใช้งาน และทบทวนปรับปรุงอย่างสม่ำเสมอ

(๒) กำหนดให้มีการจัดซื้อและติดตั้งซอฟต์แวร์ผ่านช่องทางที่ได้รับการรับรองหรือผู้จำหน่ายที่ได้รับอนุญาตเท่านั้น และห้ามติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตโดยเด็ดขาด

(๓) กำหนดให้มีการตรวจสอบการใช้งานซอฟต์แวร์ในระบบอย่างสม่ำเสมอ เช่น ทุก ๖ เดือน หรือปีละ ๑ ครั้ง

(๔) กำหนดให้มีการควบคุมสิทธิ์การติดตั้งซอฟต์แวร์ โดยอนุญาตเฉพาะผู้มีอำนาจ เช่น ผู้ดูแลระบบ (System Administrator) เป็นต้น

(๕) กำหนดให้มีนโยบายการใช้งานซอฟต์แวร์ (Software Usage Policy) และเผยแพร่ให้บุคลากรที่เกี่ยวข้องรับทราบ

๒๔) กำหนดให้มีการบริหารจัดการสิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights Management) ซึ่งต้องจัดทำบัญชีทะเบียนทรัพย์สินทางปัญญา (IP Inventory) โดยระบุประเภทเจ้าของสิทธิ ข้อกำหนดการใช้งาน และสถานะสิทธิ์ รวมถึงทบทวนปรับปรุงรายการทรัพย์สินทางปัญญาอย่างสม่ำเสมอ เช่น ทุก ๖ เดือน เป็นต้น

๒๕) กำหนดให้มีการควบคุมการเข้าถึงและการใช้งาน โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

(๑) กำหนดสิทธิการเข้าถึงทรัพย์สินทางปัญญาตามหลัก Least Privilege และ Need to Know

(๒) ควบคุมการคัดลอก การแจกจ่าย หรือการเผยแพร่ทรัพย์สินทางปัญญา ทั้งภายในและภายนอกองค์กร

(๓) พิจารณาให้มีการใช้มาตรการด้านเทคโนโลยีในการควบคุม เช่น การเข้ารหัสไฟล์ การใช้งานระบบ Digital Rights Management (DRM) และระบบ Watermarking สำหรับงานสำคัญ เป็นต้น

(๔) ไม่อนุญาตให้ติดตั้งหรือใช้งานซอฟต์แวร์ละเมิดลิขสิทธิ์ (Pirated Software)

(๕) กำหนดให้มีการตรวจสอบ เพื่อให้แน่ใจว่าซอฟต์แวร์ที่ใช้ในองค์กรมีลิขสิทธิ์ถูกต้องตามกฎหมาย

(๖) พิจารณาจัดให้มีสัญญา Non-Disclosure Agreement (NDA) สำหรับผู้ปฏิบัติงานหรือบุคคลภายนอกที่เข้าถึงข้อมูลทรัพย์สินทางปัญญา

๒๖) จัดให้มีการบริหารจัดการป้องกันโปรแกรมไม่ประสงค์ดี (Malware Protection) โดยพิจารณาอย่างน้อย ดังนี้

(๑) จัดให้มีการติดตั้งและอัปเดตโปรแกรมป้องกันไวรัส/มัลแวร์ (Antivirus/Antimalware Software) อย่างสม่ำเสมอ

(๒) กำหนดให้มีการใช้งานระบบป้องกันแบบ Real-time และกำหนดให้มีการสแกนอัตโนมัติอย่างน้อยวันละครั้ง

(๓) กำหนดมาตรการควบคุมการนำเข้าข้อมูลผ่านสื่อบันทึกข้อมูลภายนอก (เช่น USB, External HDD)

(๔) กำหนดให้มีการตั้งค่าให้ระบบปฏิบัติการและซอฟต์แวร์ที่ใช้งานทำการอัปเดตแพตช์ (Security Patches) โดยอัตโนมัติหรือภายในระยะเวลาที่กำหนด

(๕) จำกัดสิทธิ์การใช้งานระบบ (Privilege Management) เพื่อลดความเสี่ยงจากการติดตั้งโปรแกรมไม่ประสงค์ดี

(D) การควบคุมการเข้าถึง (Access Control)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้การควบคุมการเข้าถึงบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. ถูกจำกัดไว้ที่

๑) บุคลากร/เจ้าหน้าที่ ที่ปฏิบัติงานให้ ขร. และกิจกรรมที่ได้รับอนุญาตจาก ขร.

๒) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตจาก ขร.

๒. กำหนดให้แต่ละบุคลากร/เจ้าหน้าที่ กิจกรรมและกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. ต้องมีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร.

๓. กำหนดให้มีการจัดเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกการเข้าถึงควรสอดคล้องกับความถี่หรือความสม่ำเสมอของกิจกรรมการเข้าถึงบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร.

๔. กำหนดให้ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. เช่น USB, พอร์ตอนุกรม ซึ่งเป็นจุดที่ผู้ใช้หรืออุปกรณ์ภายนอกสามารถเชื่อมต่อเข้ากับระบบ โดยต้องควบคุมการเข้าถึงอย่างเข้มงวด เช่น การกำหนดให้มีการอนุญาตเฉพาะบุคลากรของ ขร. ที่มีสิทธิ์ในการเข้าถึงเท่านั้น หรือการใช้มาตรการที่ช่วยป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การใช้ระบบการยืนยันตัวตนก่อนการเข้าถึง

๕. กำหนดให้ตรวจสอบการเข้าถึงทางลอจิคอล (Logical) ให้อยู่ภายใต้การดูแลของ ขร. เท่านั้น โดยการควบคุมการเข้าถึงระบบและข้อมูลที่อยู่ในระบบคอมพิวเตอร์ เช่น การเข้าสู่ระบบปฏิบัติการหรือแอปพลิเคชัน และจัดให้มีการกำหนดบทบาทและสิทธิ์การเข้าถึง (Role-based Access Control) เพื่อให้แน่ใจว่าบุคคลมีสิทธิ์เข้าถึงข้อมูลหรือระบบตามที่จำเป็นเท่านั้น และกำหนดบุคลากรที่รับผิดชอบดูแลการเข้าถึงอินเทอร์เฟซ และระบบในช่วงที่ผู้ให้บริการภายนอกมาปฏิบัติงาน เช่น หากมีการเชื่อมต่ออุปกรณ์ภายนอก (USB) ต้องจัดให้มีการตรวจสอบและควบคุมโดยบุคลากรภายใน ขร. รวมถึงควรพิจารณาให้ดำเนินการในสถานที่ของ ขร. (หากเป็นไปได้) และพิจารณาติดตามและเฝ้าระวังการเข้าถึงด้วยเครื่องมือที่สามารถตรวจสอบและแจ้งเตือนอัตโนมัติเมื่อมีเหตุการณ์ที่ผิดปกติ เช่น Security Event Manager หรือ USB Defender

๖. กำหนดให้มีการดำเนินการจัดการดูแลระบบให้มีความมั่นคงปลอดภัย (Principles of Secure System Administration) โดยพิจารณาดำเนินการตามหลักการ ๕ หลักการ ดังนี้

(๑) ดำเนินการตรวจสอบและป้องกันไม่ให้อุปกรณ์ที่ใช้ในการดูแลระบบ (Gain Trust in your Management Devices) เช่น อุปกรณ์จัดการเซิร์ฟเวอร์ระบบควบคุมการเข้าถึง หรืออุปกรณ์เครือข่ายถูกโจมตีหรือถูกใช้ในทางที่ผิด โดยการรักษาความมั่นคงปลอดภัยของอุปกรณ์ สามารถพิจารณาได้ ดังนี้

- ดำเนินการตั้งค่ารหัสผ่านอุปกรณ์การจัดการทั้งหมด และใช้รหัสผ่านที่มีความยาวและซับซ้อน เช่น การใช้ตัวเลข ตัวอักษร และอักขระพิเศษ รวมทั้งการเปลี่ยนรหัสผ่านเป็นระยะ ตัวอย่างเช่น

ตั้งรหัสผ่านที่ยาวกว่า ๑๒ ตัวอักษร และหลีกเลี่ยงการใช้รหัสผ่านที่เดาง่าย เช่น “๑๒๓๔๕๖” หรือ “password” เป็นต้น

- พิจารณาใช้การยืนยันตัวตนด้วยหลายปัจจัย (Multi-Factor Authentication - MFA) เช่น การยืนยันตัวตนผ่านรหัสผ่านและรหัส OTP (One-Time Password) ที่ส่งไปยังมือถือ เช่น ใช้ระบบที่มีการส่งรหัส OTP ผ่านแอปพลิเคชัน (เช่น Google Authenticator) หรือ SMS เพื่อยืนยันตัวตน
- พิจารณาการควบคุมการเข้าถึง (Access Control) อุปกรณ์โดยจำกัดเฉพาะผู้ที่ได้รับอนุญาต เช่น ผู้ดูแลระบบ หรือบุคลากรที่จำเป็นต้องทำงานกับอุปกรณ์เท่านั้น เช่น ใช้การตั้งค่า Role-based Access Control (RBAC) เพื่อให้ผู้ที่มีบทบาทเฉพาะสามารถเข้าถึงอุปกรณ์ที่เกี่ยวข้องเท่านั้น
- พิจารณาเข้ารหัสข้อมูล (Encryption) ที่ถูกส่งหรือเก็บในอุปกรณ์การจัดการควรถูกเข้ารหัส เพื่อป้องกันการดักจับ หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เช่น ใช้การเข้ารหัสไฟล์ข้อมูลด้วย AES-๒๕๖ หรือการเชื่อมต่อแบบ SSL/TLS สำหรับ การส่งข้อมูลผ่านเครือข่าย
- พิจารณาบันทึกและเฝ้าระวังการเข้าถึง (Logging and Monitoring) โดยติดตั้งระบบการบันทึกและเฝ้าระวังการเข้าถึงอุปกรณ์การจัดการ เพื่อสามารถตรวจสอบการเข้าถึงที่ผิดปกติหรือไม่สามารถตรวจสอบได้ เช่น ใช้ระบบ Security Information and Event Management (SIEM)
- พิจารณาอัปเดตซอฟต์แวร์และแพตช์ (Software Updates and Patching) อุปกรณ์การจัดการอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ที่อาจเกิดขึ้นจากซอฟต์แวร์ที่ล้าสมัย เช่น ตั้งค่าให้อุปกรณ์จัดการอัปเดตแพตช์อัตโนมัติ เพื่อป้องกันช่องโหว่ที่อาจถูกใช้ ในการโจมตี
- พิจารณาจำกัดการใช้งานในช่วงเวลาที่จำเป็น โดยจำกัดการเข้าถึงอุปกรณ์การจัดการเฉพาะในเวลาที่จำเป็น เช่น เมื่อมีการตรวจสอบหรือบำรุงรักษาเท่านั้น และทำการล็อกการเข้าถึงในเวลาที่ไม่ได้ใช้งาน เช่น ใช้การกำหนดเวลาเข้าถึงระบบให้สามารถเข้าถึงเครื่องแม่ข่ายการจัดการ ได้เฉพาะในช่วงเวลาทำการเท่านั้น
- ดำเนินการตรวจสอบสิทธิ์การเข้าถึง (Access Review) อุปกรณ์การจัดการอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เช่น ทบทวนสิทธิ์การเข้าถึงของผู้ใช้ในทุก ๆ ไตรมาส รวมถึงใช้มาตรการอื่นที่เข้มงวดร่วมกัน เช่น การใช้รหัสผ่านที่แข็งแรง การยืนยันตัวตนด้วยหลายปัจจัย การควบคุมการเข้าถึงที่จำกัด และการตรวจสอบการเข้าถึงอย่างสม่ำเสมอ

ในกรณีที่มีการพิจารณาใช้ระบบ Cloud ต้องพิจารณาดำเนินการเลือกผู้ให้บริการ Cloud ที่มีการรับรองมาตรฐานความปลอดภัย เช่น ISO/IEC ๒๗๐๐๑, SOC๒ เป็นต้น และพิจารณาให้มีการควบคุมความมั่นคงปลอดภัยภายในบริการ Cloud ดังนี้

- มีการใช้การเข้ารหัส (Encryption) ข้อมูลทั้งในขณะที่เก็บ (Data at Rest) และขณะส่ง (Data in Transit) ข้อมูล แม้ว่าอุปกรณ์จะเชื่อมต่อผ่านอินเทอร์เน็ต เช่น บริการ Cloud ที่ใช้การเข้ารหัส AES-๒๕๖ เพื่อปกป้องข้อมูลที่จัดเก็บบนคลาวด์ และการเข้ารหัส SSL/TLS ในการส่งข้อมูล
- มีการควบคุมการเข้าถึง (Access Control) โดยตั้งค่าการควบคุมการเข้าถึงบริการ Cloud โดยใช้เทคนิค Multi-Factor Authentication (MFA) และ Role-based Access Control (RBAC)

เช่น การตั้งค่าให้เฉพาะผู้ที่ผ่านการยืนยันตัวตนหลายขั้นตอน เช่น รหัสผ่านและ OTP ถึงจะสามารถเข้าถึงระบบได้

- มีการตรวจสอบและบันทึกข้อมูล (Logging and Monitoring) โดยใช้ระบบตรวจสอบและบันทึกกิจกรรมในระบบ Cloud เพื่อให้สามารถติดตามและตรวจสอบเหตุการณ์ที่เกิดขึ้น เช่น การตรวจสอบกิจกรรมที่ผิดปกติหรือการเข้าถึงที่ไม่เหมาะสม เช่น การใช้เครื่องมือ Security Information and Event Management (SIEM) เพื่อตรวจจับการพยายามเข้าถึงโดยไม่ได้รับอนุญาตหรือการเปลี่ยนแปลงที่ผิดปกติในระบบ Cloud

- มีการแยกข้อมูลและการควบคุมภายในระบบ (Segmentation and Internal Controls) Cloud โดยแยกข้อมูล (data segmentation) และจัดแบ่งข้อมูลในพื้นที่ที่มีการควบคุมที่แตกต่างกัน เช่น การจัดเก็บข้อมูลที่สำคัญในสภาพแวดล้อมที่แยกออกจากข้อมูลที่ไม่สำคัญ เช่น บริการ Cloud ที่ให้จัดการกับ Virtual Private Cloud (VPC) เพื่อให้ระบบต่าง ๆ ที่เชื่อมต่อกันในพื้นที่แยกต่างหากและมีการควบคุมที่ดีขึ้น

- มีการจัดการช่องโหว่ (Vulnerability Management) โดยการตรวจสอบและป้องกันช่องโหว่ในระบบ Cloud ด้วยการอัปเดตแพตช์ซอฟต์แวร์และการใช้เครื่องมือในการทดสอบเจาะระบบ (Penetration Testing) เช่น การใช้เครื่องมือเช่น Qualys หรือ Tenable ในการตรวจสอบความเสี่ยงและช่องโหว่ในระบบ Cloud

(๒) ออกแบบระบบให้มีการปกป้องช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบ (Protect your Administration Interfaces) โดยให้สิทธิ์การดำเนินงานพิเศษแก่ผู้ใช้ที่เข้าถึงระบบผ่านช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบและบริการของ ขร. เท่านั้น (Administration Interfaces) และอนุญาตให้เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่จะเข้าถึงช่องทางหรือระบบที่กำหนด เช่น

- การใช้รหัสผ่านที่เข้มงวดและการยืนยันตัวตนหลายขั้นตอน (Multi-Factor Authentication: MFA) ใช้ระบบที่ต้องการทั้งรหัสผ่านและรหัส OTP (One-Time Password) เพื่อเพิ่มความมั่นคงปลอดภัย เมื่อเข้าถึงช่องทางการเชื่อมต่อสำหรับการจัดการ เช่น เมื่อผู้ดูแลระบบต้องการเข้าถึงเครื่องแม่ข่ายเซิร์ฟเวอร์ หรือระบบสำคัญ ผู้ดูแลต้องใช้รหัสผ่านร่วมกับรหัส OTP ที่ส่งไปยังมือถือ เพื่อยืนยันตัวตนก่อนการเข้าถึง

- การตั้งค่าการเข้าถึงที่จำกัด (Access Control) กำหนดให้การเข้าถึงเครื่องมือการจัดการดูแล ระบบสามารถทำได้เฉพาะผู้ที่ได้รับอนุญาต เช่น ผู้ดูแลระบบเท่านั้น เช่น จำกัดการเข้าถึง SSH (Secure Shell) หรือ Remote Desktop (RDP) โดยผู้ที่มีบทบาทในการดูแลระบบหรือผู้มีสิทธิ์พิเศษเท่านั้น

- การใช้ช่องทางการเชื่อมต่อที่มั่นคงปลอดภัยสูง เช่น การเข้ารหัสการเชื่อมต่อ (SSL/TLS) สำหรับการเข้าถึงระบบจากภายนอก เช่น ใช้ Virtual Private Network (VPN) หรือ SSH สำหรับการเข้าถึงเครื่องแม่ข่าย หรือฐานข้อมูลภายใน เพื่อป้องกันการดักจับข้อมูลระหว่างทาง เช่น

ตัวอย่างการใช้โค้ดและการตั้งค่าในการจัดการระบบ

- การใช้โค้ดสำหรับการติดตั้งและอัปเดตซอฟต์แวร์ หน่วยงานอาจใช้ Automated Scripts หรือ Configuration Management Tools เช่น Ansible, Puppet, หรือ Chef เพื่อจัดการติดตั้งและอัปเดตซอฟต์แวร์โดยอัตโนมัติ โดยไม่ต้องเข้าถึงระบบด้วย การเชื่อมต่อแบบตรง ตัวอย่างเช่น ใช้โค้ดหรือ

สคริปต์ในการติดตั้งแอปพลิเคชันบนเซิร์ฟเวอร์หลายเครื่องในคราว เดียว โดยไม่ต้องใช้การเข้าถึงทางกายภาพหรือการเชื่อมต่อจากระยะไกล

- การจัดการการตั้งค่าผ่านไฟล์คอนฟิก โดยใช้ Configuration Files เช่น JSON หรือ YAML ในการกำหนดค่าของระบบต่าง ๆ การกำหนดสิทธิการเข้าถึงระบบผ่านไฟล์คอนฟิกที่ได้รับการตรวจสอบและบันทึกไว้ เช่น การตั้งค่าผู้ใช้ การตั้งค่าความมั่นคงปลอดภัย หรือการตั้งค่าฐานข้อมูล
- การใช้โค้ดในการควบคุมการเข้าถึง เช่น เซิร์ฟเวอร์, เครือข่าย, ฐานข้อมูล, Storage, Load Balancer, Firewall, และการตั้งค่าต่างๆ ด้วยการเขียนโค้ด (Code) โดยใช้แนวคิดและวิธีการจัดการโครงสร้างพื้นฐานด้านไอที (Infrastructure as Code (IaC)) เช่น

- Terraform ซึ่งใช้ในการจัดเตรียมและจัดการทรัพยากรบน Cloud Provider ต่างๆ เช่น AWS, Azure, GCP และ On-Premises
- Ansible ซึ่งเน้นการจัดการ Configuration Management เช่น ติดตั้งซอฟต์แวร์, ตั้งค่าเซิร์ฟเวอร์ และ Automation
- Puppet, Chef, Salt Stack เป็นเครื่องมือเน้น Configuration Management คล้าย Ansible
- AWS CloudFormation ซึ่งเป็นเครื่องมือ IaC เฉพาะสำหรับ Amazon Web Services (AWS)
- Azure Resource Manager (ARM) Templates เป็นเครื่องมือ IaC เฉพาะสำหรับ Microsoft Azure
- Google Cloud Deployment Manager: เป็นเครื่องมือ IaC เฉพาะสำหรับ Google Cloud Platform (GCP)

(๓) จัดการดูแลและการบริหารความเสี่ยงโดยใช้ระดับชั้น (Risk Manage Administration Using Tiers) โดยประยุกต์การบริหารความเสี่ยงที่ใช้ในทางปฏิบัติกับการจัดการดูแลระบบของ ขร. ให้สอดคล้องกับระดับชั้น (Tiered Administration) โดยพิจารณาดำเนินการ ดังนี้

๑) ดำเนินการระบุและประเมินความเสี่ยงของช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบ (Identify and Assess the Risks your Administration Interfaces) ในแต่ละระดับชั้น (Tier) โดยช่องทางการเชื่อมต่อแบ่งเป็น ๓ ส่วนหลัก ๆ ดังนี้

(๑) การเชื่อมต่อผ่านเครือข่าย (Network-based Connection) ได้แก่

- Secure Shell (SSH) ซึ่งเป็นโปรโตคอลที่ใช้ในการเข้าถึงและจัดการเซิร์ฟเวอร์หรืออุปกรณ์เครือข่ายระยะไกลได้อย่างปลอดภัย โดยมีการเข้ารหัสข้อมูล เหมาะสำหรับการบริหารจัดการ Linux/Unix server และอุปกรณ์ network เช่น Router, Switch
- Remote Desktop Protocol (RDP) ใช้สำหรับเข้าถึงและควบคุมเครื่องคอมพิวเตอร์ Windows ระยะไกลแบบกราฟิก (GUI) ทำให้ผู้ดูแลระบบสามารถทำงานบนเครื่องนั้นได้เหมือนนั่งอยู่หน้าจอ
- Virtual Network Computing (VNC) มีลักษณะคล้ายกับ RDP แต่สามารถใช้งานได้หลากหลายแพลตฟอร์ม (Windows, Linux, macOS) เพื่อเข้าถึงและควบคุมเดสก์ท็อประยะไกล

- Web-based Interface (Console/Management Portal) เป็นอุปกรณ์เครือข่ายและซอฟต์แวร์หลายตัวมีหน้าเว็บสำหรับจัดการทำให้ผู้ดูแลระบบสามารถเข้าถึงและกำหนดค่าผ่านเว็บเบราว์เซอร์ได้จากทุกที่ที่มีอินเทอร์เน็ต เช่น เราเตอร์, สวิตช์, ไฟร์วอลล์, หรือแพลตฟอร์มคลาวด์.

- SNMP (Simple Network Management Protocol) เป็นโปรโตคอลที่ใช้ในการตรวจสอบและจัดการอุปกรณ์เครือข่ายผู้ดูแลระบบสามารถใช้เครื่องมือ SNMP เพื่อรวบรวมข้อมูลสถานะของอุปกรณ์, ตั้งค่าการแจ้งเตือน, และควบคุมการทำงานบางอย่างได้

- APIs (Application Programming Interfaces) ใช้สำหรับระบบที่มีความซับซ้อนและต้องการการจัดการแบบอัตโนมัติ (Automation) ผู้ดูแลระบบสามารถใช้ API เพื่อเขียนสคริปต์หรือโปรแกรมในการสั่งการและรวบรวมข้อมูลจากระบบได้โดยตรง

(๒) การเชื่อมต่อแบบกายภาพ (Physical Connection) ได้แก่

- Console Port/Serial Port เป็นอุปกรณ์เครือข่ายหลายตัว เช่น Router, Switch มีพอร์ต Console ที่ใช้สายเคเบิล Serial เช่น RJ๔๕ to DB๙ สำหรับการเชื่อมต่อโดยตรงจากคอมพิวเตอร์เพื่อเข้าถึง Command Line Interface (CLI) ในการกำหนดค่าเริ่มต้นหรือแก้ไขปัญหาเมื่อการเชื่อมต่อเครือข่ายยังไม่พร้อมใช้งาน

- Keyboard, Video, Mouse (KVM) Switch ใช้สำหรับควบคุมเซิร์ฟเวอร์หลายเครื่องจากชุดคีย์บอร์ด, จอภาพ, และเมาส์ชุดเดียว เหมาะสำหรับศูนย์ข้อมูลหรือห้องเซิร์ฟเวอร์ที่มีอุปกรณ์จำนวนมาก

- Out-of-Band Management (OOB) เป็นช่องทางการจัดการที่แยกออกจากเครือข่ายหลัก มักใช้ในกรณีที่เครือข่ายหลักมีปัญหา เช่น IPMI (Intelligent Platform Management Interface) บนเซิร์ฟเวอร์ที่ช่วยให้สามารถควบคุมเปิด-ปิด, รีบูต, หรือเข้าถึงคอนโซลของเซิร์ฟเวอร์ได้แม้จะไม่มีระบบปฏิบัติการทำงานอยู่

(๓) เครื่องมือและแพลตฟอร์มเฉพาะ ได้แก่

- Google Admin, Family Link เป็นแพลตฟอร์มสำหรับการจัดการบัญชีและอุปกรณ์ของผู้ใช้ในบริบทเฉพาะ เช่น Google Workspace, บัญชีครอบครัว

- Managed Network Services เช่น จาก UIH เป็นบริการจากผู้ให้บริการภายนอกที่ดูแลจัดการระบบเครือข่ายทั้งหมดให้องค์กร โดยผู้ดูแลระบบขององค์กรจะเชื่อมต่อกับแพลตฟอร์มหรือทีมงานของผู้ให้บริการเพื่อจัดการ

๒) ดำเนินการระบุระดับชั้นการจัดการดูแลระบบ (Identify your Administration Tiers) ซึ่งควรใช้ผลจากการประเมินความเสี่ยง เพื่อกำหนดระดับชั้นของช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบ เช่น

- ระดับชั้น ๐ (Tier ๐) เป็นระดับชั้นที่เป็นรากฐานในการดำเนินการจัดการดูแลอื่น ๆ ดังนั้น หากผู้โจมตีสามารถโจมตีรากฐานได้ผู้โจมตีสามารถเข้าถึงส่วนประกอบในระดับชั้นอื่น ๆ เช่น

- ผู้ดูแลระบบที่มีสิทธิสูงสุดในการเข้าถึงและจัดการทรัพยากรทั้งหมดในโดเมน (Root Domain Administrators) รวมถึงสามารถสร้างบัญชีที่มีสิทธิพิเศษ (Highly Privilege Accounts) เพิ่มเติมได้

- บัญชีรูท (Root Account) ในบริการคลาวด์ที่จัดการสิทธิของบัญชีอื่น ๆ ทั้งหมด (Manages the Privileges of all Other Accounts)

- โครงสร้างพื้นฐานแบบออฟไลน์ (Offline Infrastructure) เพื่อสร้างเอกสาร อุปกรณ์หรือ เครื่องมือใด ๆ ที่มีข้อมูลเกี่ยวกับการเข้ารหัส และมีความสำคัญต่อการเข้ารหัส ถอดรหัส หรือการยืนยันตัวตน ของการสื่อสารทางไกลการเข้ารหัส (Cryptographic Material)

- ระดับชั้น ๑ (Tier ๑) เป็นระดับชั้นของโครงสร้างพื้นฐานที่ช่วยให้สามารถดำเนินการที่ต้องใช้สิทธิพิเศษ (Highly Privileged Functions) ต่อระบบที่สำคัญได้ ซึ่งการโจมตีโครงสร้างพื้นฐานในระดับชั้น ๑ อาจก่อให้เกิดการหยุดชะงักในวงกว้าง เช่น

- ผู้ดูแลระบบของฐานข้อมูลที่สำคัญ เนื่องจากจัดเก็บข้อมูลที่อ่อนไหวจำนวนมาก ซึ่งระบบอื่น จำเป็นต้องใช้ฐานข้อมูลนี้ในการดำเนินงานด้วย

- ความสามารถในการควบคุมและจัดการบริการที่สำคัญจำนวนมากในสภาพแวดล้อมแบบคลาวด์

- โครงสร้างพื้นฐานที่ใช้ในการกำหนดค่าขีดแบ่งให้แก่ระบบควบคุมที่สำคัญ (Set Operational Thresholds on Critical Control Systems)

- ระดับชั้น ๒ (Tier ๒) เป็นระดับชั้นของโครงสร้างพื้นฐานที่ช่วยให้ดำเนินการที่ต้องใช้สิทธิพิเศษ (Privileged Functions) ได้ และเป็นการดำเนินการต่อส่วนประกอบจำนวนน้อย “ส่วนประกอบ” ซึ่งหมายถึง ฟังก์ชันหรือบริการที่เกี่ยวข้องกับการเข้าถึงและการดำเนินการของผู้ดูแลระบบ เช่น การเข้าถึงแอปพลิเคชันสำคัญ การจัดการเครื่องแม่ข่าย หรือการปรับค่าระบบในลักษณะที่มีผลกระทบต่อการทำงานของระบบ แต่ไม่ได้ส่งผลกระทบสูงต่อการดำเนินงานตามภาระกิจหน้าที่ของ ขร. เช่น

- การเข้าถึงแอปพลิเคชันสนับสนุนธุรกิจที่สำคัญ (Important Business Support Application) ของผู้ดูแลระบบ

- การเข้าถึงระดับรูทบนเว็บเครื่องแม่ข่ายเว็บส่วนหน้า (Front End Web Server) ซึ่งเป็นส่วนหนึ่ง ของสถาปัตยกรรมระบบคลาวด์ที่เป็นระบบใหญ่

- การจัดการดูแลแผงควบคุม (Dashboard) ที่หน่วยงานใช้เฝ้าระวังระบบควบคุมอุตสาหกรรม (Monitoring an Industrial Control System)

- ระดับชั้น ๓ (Tier ๓) เป็นระดับชั้นของโครงสร้างพื้นฐานที่อนุญาตให้ดำเนินการได้อย่างจำกัด (A Constrained Set of Functions) และเป็นการดำเนินการต่อส่วนประกอบเดียวหรือจำนวนน้อย ซึ่งผลกระทบของการโจมตีโครงสร้างพื้นฐานในระดับนี้เป็นสิ่งที่ไม่ต้องการให้เกิด เนื่องจากอาจส่งผลถึงชื่อเสียงของ ขร. แต่ไม่ส่งผลเสียหายต่อการดำเนินการมากนัก เช่น

- บุคลากรฝ่ายสนับสนุนด่านหน้า (First Line Support staff) ใช้คำสั่งรีเซ็ตรหัสผ่าน

- ความสามารถในการทริกเกอร์หรือกระตุ้น (Trigger) การกระทำที่กำหนดไว้ล่วงหน้า (Predefined Action) ในสภาพแวดล้อมระบบคลาวด์ เช่น การใช้ฟีเจอร์โค้ดใหม่ในสภาพแวดล้อมที่ใช้งานจริง

- การปรับเปลี่ยนค่าในระบบควบคุมอุตสาหกรรมที่ถูกจำกัดขอบเขตไว้ด้วยส่วนประกอบ หรือด้วยผู้ดูแลระบบในระดับที่ต่ำกว่า

๓) กำหนดกลยุทธ์การจัดการดูแลระบบ (Define an Administration Strategy) เมื่อระบบมีผู้ใช้งานมากขึ้นและผลกระทบจากการโจมตีมีความสำคัญมากขึ้น โดยทบทวนกลยุทธ์การจัดการดูแลระบบในแต่ละระดับชั้น (Tier) ให้เหมาะสมกับความเสี่ยงที่เพิ่มขึ้น โดยให้ความสำคัญกับการจัดการสิทธิพิเศษในระดับชั้น ๐ (Tier ๐) และลดความเสี่ยงในระดับชั้นที่ต่ำกว่า

๔) ดำเนินการตามกลยุทธ์การจัดการดูแล (Implement your Administration Strategy) โดยกำหนดมาตรการควบคุมทางเทคนิคที่เหมาะสมสำหรับแต่ละระดับชั้น เช่น การใช้การพิสูจน์ตัวตนหลายปัจจัย (MFA) ในระดับชั้น ๐ (Tier ๐) และการใช้การควบคุมสิทธิพิเศษ (Privileged Access Management) โดยควรคำนึงถึงการให้สิทธิน้อยที่สุด (Least Privilege) และการรักษาความสมดุลระหว่างความเสี่ยงและความคล่องตัวในการจัดการ

๕) ปรับแต่งกลยุทธ์ (Evolve and Refine your Strategy) โดยใช้ข้อมูลจากการบันทึก (Logging Data) และการทำงานร่วมกับผู้ดูแลระบบในแต่ละระดับชั้น เพื่อปรับปรุงและพัฒนากลยุทธ์การจัดการดูแลระบบอย่างต่อเนื่อง โดยปรับให้เหมาะสมกับความเสี่ยงที่เพิ่มขึ้นในแต่ละระดับ

๖) สนับสนุนผู้ดูแลระบบ (Support your Administrators) โดยส่งเสริมให้มีการดำเนินการทำงานร่วมกับผู้ดูแลระบบในแต่ละระดับชั้น เพื่อกำหนดนโยบายและการดำเนินการที่โปร่งใส และช่วยสนับสนุนการดำเนินการให้ผู้ดูแลระบบสามารถทำงานได้อย่างมีประสิทธิภาพ โดยให้การควบคุมที่เหมาะสมตามระดับความสำคัญของแต่ละชั้น

(๔) จัดการการเข้าถึงด้วยสิทธิพิเศษ (Use Privileged Access Management) โดยการอนุญาตให้บุคคลเข้าถึงระบบหนึ่ง ๆ เป็นการอนุญาตให้เข้าถึง ณ เวลาใด ด้วยเหตุผลและวิธีการใด รวมถึงให้สิทธิน้อยที่สุด (Least Privilege) แก่ผู้ดูแลระบบ (Privileged User) และยกเลิกสิทธิ เมื่อผู้ดูแลระบบไม่จำเป็นต้องใช้สิทธินั้น โดยพิจารณาดำเนินการ ดังนี้

- ยอมให้เข้าถึงจากอุปกรณ์ที่ได้รับอนุญาตเท่านั้น (Only Allow Permitted Devices) โดยกำหนดมาตรการควบคุมทางสถาปัตยกรรม และยอมให้อุปกรณ์ได้รับอนุญาตสามารถเข้าถึง (Privileged Access Management: PAM) และช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบได้เท่านั้น
- ยอมให้เฉพาะผู้ใช้ที่ได้รับอนุญาตสามารถร้องขอข้อมูลประจำตัว (Only Allow Permitted Users) โดยกำหนดให้มีการพิสูจน์ตัวตนที่รัดกุม (Strong Authentication) และยอมให้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้นเข้าสู่ระบบ เพื่อขอข้อมูลประจำตัวชั่วคราวสำหรับการจัดการดูแลระบบ
- แจ้งเหตุผลอันสมควรในการจัดการดูแล (Justify Administration Intent) กำหนดให้ผู้ดูแลระบบต้องแสดงเหตุผลในการจัดการดูแลระบบ เพื่อเป็นข้อมูลของกระบวนการร้องขอในการพิจารณาอนุมัติหรือยับยั้งบุคคลภายในที่เป็นอันตรายที่จะเข้าถึงระบบ
- กำหนดให้มีการอนุมัติที่เหมาะสม (Use Appropriate Approvals) โดยพิจารณาคำร้องขอและกฎสำหรับการอนุมัติการเข้าถึงช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบอย่างรอบคอบ โดยพิจารณาจากระดับความเสี่ยงของระบบ รวมถึงผลกระทบจากเหตุการณ์ ที่ผู้โจมตีสามารถเข้าถึงช่องทางการเชื่อมต่อ

- กำหนดให้รับรองตัวตนที่มีความมั่นคงปลอดภัยและรัดกุม (Use Secure and Strong Credentials) โดยเข้ารหัสระหว่างการส่งข้อมูลประจำตัว และเข้ารหัสข้อมูลประจำตัวที่ยากต่อการปลอมแปลงและถอดรหัส

- จำกัดระยะเวลาการใช้งานสิ่งที่ใช้รับรองตัวตน (Constrain Credential Validity Period) โดยจัดให้มีการดำเนินการกำหนดกรอบเวลาการใช้งานข้อมูลประจำตัวของผู้ดูแลระบบของแต่ละระบบตามความต้องการในการใช้งานข้อมูลประจำตัว

- ให้สิทธิน้อยที่สุดแก่ผู้ที่มีบทบาทในการจัดการดูแลระบบ (Use Least Privilege on Administration Roles) ให้กับผู้ดูแลระบบ เพื่อทำงานที่จำเป็นสำเร็จเท่านั้น

- ในกรณีที่มีการพิจารณาใช้ระบบ PAM (Protect the PAM System) ต้องดำเนินการพิจารณามาตรการปกป้องระบบ PAM (Protect the PAM System) ใช้มาตรการควบคุมทางสถาปัตยกรรม เช่น การป้องกันหลายชั้น (Defense in Depth) หลักการให้สิทธิ์น้อยที่สุด (Principle of Least Privilege) การแบ่งแยกหน้าที่ (Separation of Duties) เป็นต้น รวมถึงติดตั้งแพตช์เป็นประจำ และกำหนดให้ระบบ PAM อยู่ในกลยุทธ์การเฝ้าระวังความมั่นคงปลอดภัย (Security Monitoring Strategy)

- พิจารณาความพร้อมใช้งานของ PAM (Consider PAM Availability) ให้มีสภาพพร้อมใช้งานสูง (High Availability) และกำหนดกระบวนการสำรองฉุกเฉิน (Emergency Backup Process) สำหรับการเข้าถึงระบบต่าง ๆ

(๕) บันทึกและตรวจสอบกิจกรรมการจัดการดูแลระบบ (Log and Audit Administration Activities) ที่เกี่ยวข้องกับการจัดการดูแลระบบ และตรวจสอบบันทึกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าผู้ดูแลระบบได้ดำเนินการตามขั้นตอนที่ได้รับอนุมัติและไม่เกิดการกระทำที่ผิดพลาดหรือไม่เหมาะสม โดยพิจารณาดำเนินการ ดังนี้

- ดำเนินการเฝ้าระวังโดยพิจารณาผลประเมินความเสี่ยง และภัยคุกคามที่อาจเกิดขึ้น เพื่อระบุช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบที่อาจตกเป็นเป้าหมายการโจมตี ทั้งนี้สามารถนำข้อมูลผลประเมินความเสี่ยง และภัยคุกคามที่อาจเกิดขึ้น มากำหนดกลยุทธ์การรวบรวมบันทึกและการเฝ้าระวังความมั่นคงปลอดภัย

- ดำเนินการรวบรวมข้อมูลที่ถูกต้อง (Collect the Right Data) โดยพิจารณาข้อมูลที่จำเป็นต้องใช้ เพื่อสนับสนุนการตรวจสอบและการเฝ้าระวัง และดำเนินการรวบรวมข้อมูลนั้น

- กำหนดนิยามสถานะปกติ (Define Normal) เพื่อใช้เป็นข้อมูลพื้นฐานสำหรับการเฝ้าระวังความมั่นคงปลอดภัย

- ทำงานร่วมกับนักวิเคราะห์ความมั่นคงปลอดภัย (Work with Security Analysis) เพื่อให้เข้าใจการทำงานของระบบ และสถานะปกติของระบบ เพื่อให้นักวิเคราะห์สามารถระบุพฤติกรรมที่น่าสงสัยได้ถูกต้อง

- ทดสอบการเฝ้าระวัง (Test your Monitoring) โดยการตรวจสอบประสิทธิภาพการทำงานของช่องทางการเชื่อมต่อ สำหรับการจัดการดูแลระบบ โดยฝึกซ้อมการโจมตีร่วมกับฝึกการป้องกัน (Run Red and Blue Team Exercises) ที่ช่องทางการเชื่อมต่อ

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการควบคุมสิทธิการเข้าถึงเครือข่ายและบริการเครือข่าย โดยพิจารณาอย่างน้อย ดังนี้

๑) จัดกลุ่มผู้ใช้งานและอุปกรณ์เครือข่ายตามบทบาทหน้าที่ และกำหนดสิทธิการเข้าถึงเครือข่ายแยกตาม VLAN หรือ Segment รวมถึงกำหนดให้มีการบังคับใช้นโยบายการเข้าถึงเท่าที่จำเป็น (Least Privilege)

๒) พิจารณาใช้ระบบควบคุมการเข้าถึงเครือข่าย (NAC – Network Access Control) เพื่อตรวจสอบสถานะของอุปกรณ์ก่อนเชื่อมต่อ

๓) กำหนดให้ผู้ใช้งานต้องยืนยันตัวตนด้วยรหัสผ่านที่รัดกุม หรือ Multi-Factor Authentication (MFA)

๔) กำหนดให้มีการใช้งาน VPN พร้อมทั้งกำหนดให้มีการตรวจสอบสิทธิ์ ในกรณีที่มีผู้ใช้งานภายนอกต้องการเข้าถึงระบบ เช่น พาร์ตเนอร์ หรือผู้รับจ้าง เป็นต้น

๕) กำหนดให้มีการจำกัดเวลาการเชื่อมต่อและ Session Timeout สำหรับการเข้าถึงจากภายนอก

๖) กำหนดให้มีการแยกเครือข่ายที่สำคัญไว้ใน Zone ที่มีมาตรการควบคุมเคร่งครัด เช่น DMZ เป็นต้น

๗) กำหนดให้มีการเปิดใช้งานเฉพาะพอร์ต หรือโปรโตคอลที่จำเป็น (Port Management) และปิดพอร์ตที่ไม่ได้ใช้งาน

๘) กำหนดให้มีการบันทึก Log การเข้าถึงเครือข่ายทุกประเภท เช่น การพิสูจน์ตัวตน การเชื่อมต่อและการปฏิเสธการเข้าถึง

๙) กำหนดให้มีการตรวจสอบและวิเคราะห์ Log อย่างสม่ำเสมอ เพื่อค้นหาพฤติกรรมผิดปกติ

๑๐) พิจารณาติดตั้งระบบ IDS/IPS หรือ Firewall ที่มีความสามารถในการตรวจจับการรุกล้ำ

๒. กำหนดให้มีการบริหารจัดการอุปกรณ์พกพาและอุปกรณ์ส่วนบุคคล (BYOD) โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีการขออนุมัติ พร้อมทั้งลงทะเบียนอุปกรณ์พกพาและอุปกรณ์ส่วนบุคคล ในกรณีที่มีการนำอุปกรณ์ส่วนบุคคลมาใช้งาน

๒) จำกัดการเข้าถึงของอุปกรณ์พกพาและอุปกรณ์ส่วนบุคคล เฉพาะเครือข่าย Guest หรือ VLAN ที่แยกจากเครือข่ายหลัก

๓) ห้ามเชื่อมต่ออุปกรณ์ IoT ที่ไม่ได้รับอนุญาตเข้ากับเครือข่ายหลัก

๓. กำหนดให้มีการบริหารจัดการลงทะเบียนการเข้าถึงระบบของผู้ใช้งาน ก่อนที่จะได้รับอนุญาตให้เข้าใช้งานระบบ ตามสิทธิหน้าที่ความรับผิดชอบของผู้ใช้งาน หากในกรณีที่มีสิทธิพิเศษที่นอกเหนือหน้าที่ความรับผิดชอบ ต้องได้รับอนุญาตจากเจ้าของระบบ หรือผู้มีอำนาจก่อนได้รับสิทธิ

๔. ห้ามใช้งานบัญชีร่วมกัน ยกเว้นกรณีจำเป็น และต้องกำหนดมาตรการควบคุมการเข้าถึงให้สามารถชี้บ่งถึงตัวบุคคลที่เข้าถึงระบบในแต่ละช่วงเวลา

๕. กำหนดให้มีการบริหารจัดการถอดถอนสิทธิการเข้าถึงทันที หรือกำหนดระยะเวลาภายใน ๒๔ ชั่วโมง หลังได้รับแจ้ง ในกรณีที่ผู้ปฏิบัติงานลาออก, พ้นจากอำนาจหน้าที่, โยกย้ายตำแหน่ง, หรือครบกำหนดตามสัญญา เป็นต้น

๖. ในกรณีที่บัญชีมีความจำเป็นต้องเก็บไว้ เพื่อการสอบสวน หรือตรวจสอบ ต้องมีมาตรการควบคุมพิเศษให้ผู้ใช้งานไม่สามารถเข้าถึงได้ พร้อมทั้งระบุเหตุผลให้ชัดเจน

๗. กำหนดให้มีการบันทึก Log การเข้าถึงระบบอย่างน้อย ๙๐ วัน รวมถึงกำหนดให้มีการตรวจสอบ log อย่างน้อยปีละ ๑ ครั้งในระบบงานที่สำคัญ หรือบริการที่สำคัญ

๘. กำหนดให้มีการบริหารจัดการบัญชีผู้ใช้งานชั่วคราว (Temporary Access) โดยกำหนดอายุบัญชีผู้ใช้งานชั่วคราว (Account Expiry) ให้ชัดเจน และเมื่อครบกำหนดต้องมีการลบบัญชีหรือยกเลิกสิทธิอัตโนมัติ รวมถึงห้ามแปลงบัญชีชั่วคราวเป็นบัญชีถาวรโดยไม่มีการอนุมัติใหม่

๙. กำหนดให้มีการบันทึก Log การเปิด หรือปิดบัญชีผู้ใช้งานชั่วคราว และกำหนดให้มีการทบทวนหรือตรวจสอบบัญชีผู้ใช้งานชั่วคราวที่ไม่มีการใช้งานเป็นระยะเวลานาน เช่น เกินกว่า ๔๕ วัน หรือ ๙๐ วัน เพื่อตัดสิทธิ์หรือปิดบัญชีผู้ใช้งานชั่วคราว

๑๐. กำหนดให้มีการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน โดยพิจารณาอย่างน้อยดังนี้

๑) พิจารณาให้มีการพิสูจน์ตัวตนโดยใช้รูปแบบ Multi-Factor Authentication (MFA) สำหรับระบบงานที่สำคัญ หรือบริการที่สำคัญ

๒) กำหนดให้มีการตั้งรหัสผ่านตามแนวทางการบริหารจัดการรหัสผ่าน และห้ามนำรหัสผ่านที่เหมือนกันไปใช้งานซ้ำในหลายระบบ

๓) การจัดเก็บข้อมูลความลับสำหรับการพิสูจน์ตัวตน ต้องพิจารณาให้มีมาตรการควบคุมอย่างน้อย ดังนี้

(๑) ต้องเข้ารหัสด้วยอัลกอริทึมที่เหมาะสม เช่น PBKDF๒, bcrypt, Argon๒ เป็นต้น

(๒) ห้ามแชร์ข้อมูลลับผ่านช่องทางที่ไม่ปลอดภัย เช่น อีเมล หรือ Line เป็นต้น

๔) กำหนดให้มีการเปลี่ยนรหัสผ่าน เมื่อมีเหตุบ่งชี้ว่ารหัสถูกเปิดเผย หรือถูกใช้ผิดปกติ รวมถึงห้ามใช้รหัสเดียวกันตลอดไป

๕) กำหนดให้มีการตรวจสอบบัญชีที่มีความพยายามเข้าสู่ระบบผิดซ้ำ ๆ หรือเข้าสู่ระบบผิดเวลาปกติ

๑๑. กำหนดให้มีการบริหารจัดการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดรอบการทบทวนสิทธิการเข้าถึงของผู้ใช้งานทุกคน อย่างน้อยปีละ ๑ ครั้ง

๒) กำหนดให้มีการทบทวนสิทธิสำหรับบัญชีที่มีสิทธิพิเศษ เช่น Admin, Root, Cloud Admin อย่างน้อย ทุก ๖ เดือน

๓) ในกรณีที่มีการเปลี่ยนแปลงผู้ใช้งาน เช่น เปลี่ยนตำแหน่ง, ย้ายหน่วยงาน, ลาออก ต้องทบทวนสิทธิทันทีหลังจากได้รับแจ้ง

๔) จัดให้มีหลักฐานในการทบทวนสิทธิตามรอบที่กำหนด เช่น จัดทำรายงานการทบทวนสิทธิ

๑๒. กำหนดให้มีการกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดบทบาทหน้าที่ความรับผิดชอบ โดยจัดหมวดหมู่ผู้ใช้งานให้ชัดเจน เช่น ผู้ใช้งานทั่วไป (End User) เจ้าของระบบ (Data Owner) ผู้ดูแลระบบ (Admin) เป็นต้น

๒) พิจารณาจัดทำ Role Responsibility Matrix (RACI) หรือ user Matrix ให้สอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งานในแต่ละหมวดหมู่ และสิทธิ์ในการเข้าถึงระบบ

๓) กำหนดให้มีการทบทวน Role Responsibility Matrix (RACI) หรือ user Matrix อย่างสม่ำเสมอ

๑๓. กำหนดให้มีการพิสูจน์ตัวตนที่ปลอดภัย (Authentication Control) โดยพิจารณากำหนดให้มีการบังคับใช้รหัสผ่านที่ปลอดภัยตามแนวทางการบริหารจัดการรหัสผ่าน

๑๔. กำหนดให้มีการควบคุมพฤติกรรมการเข้าสู่ระบบ โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีการจำกัดจำนวนครั้งของการพยายามเข้าสู่ระบบ หากเกินจำนวนครั้งที่กำหนดให้ระบบทำการล็อคบัญชีไว้ชั่วคราว

๒) กำหนดให้มีการตั้งค่า Session Timeout เมื่อไม่มีการใช้งานระบบ

๓) กำหนดเงื่อนไข Context-based เช่น ไม่อนุญาต Login ข้ามประเทศ หรือข้ามเวลาทำการในระบบงานที่สำคัญ

๑๕. กำหนดให้มีมาตรการควบคุมการเข้าสู่ระบบแบบปลอดภัยสำหรับผู้ดูแลระบบ โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากบัญชีผู้ดูแลระบบ (Admin) อย่างชัดเจน

๒) กำหนดให้มีการบันทึกกิจกรรมการเข้าระบบ (Log) ของผู้ดูแลระบบทุกครั้งที่มีการเข้าสู่ระบบ

๑๖. กำหนดให้มีมาตรการควบคุมการบันทึกและตรวจสอบการเข้าสู่ระบบ โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีการบันทึกกิจกรรมการเข้าถึงระบบ (Log) เช่น วันเวลา, ชื่อผู้ใช้, IP, สถานะ (สำเร็จ/ล้มเหลว) การเข้าถึงระบบ

๒) กำหนดให้มีการจัดเก็บบันทึกกิจกรรมการเข้าถึงระบบ (Log) อย่างน้อย ๙๐ วัน หรือมากกว่าสำหรับระบบงานที่สำคัญ หรือบริการที่สำคัญ

๓) กำหนดให้มีการตรวจสอบบันทึกกิจกรรมการเข้าถึงระบบ (Log) เป็นประจำ เพื่อตรวจหาเหตุผิดปกติ เช่น brute-force หรือการเข้าระบบ (Login) จากตำแหน่งผิดปกติ เป็นต้น

๑๗. กำหนดให้มีการบริหารจัดการจำกัดการเข้าถึงข้อมูล โดยพิจารณาอย่างน้อยดังนี้

๑) กำหนดให้มีการจำแนกระดับข้อมูล เพื่อกำหนดการเข้าถึงข้อมูลตามระดับความสำคัญของข้อมูล

๒) จัดให้มีการระบุเจ้าของข้อมูล (Data Owner) เพื่อควบคุมการเข้าถึงและการปรับปรุงสิทธิ์

๓) ดำเนินการควบคุมสิทธิ์การเข้าถึง โดยพิจารณาหลักการ ดังนี้

(๑) กำหนดให้มีการใช้หลัก Least Privilege โดยให้ผู้ใช้งานเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้องกับภาระหน้าที่งานเท่านั้น

(๒) ควบคุมการเข้าถึงโดยใช้หลัก Role-Based Access Control (RBAC) หรือ Attribute-Based Access Control (ABAC)

(๓) กำหนดให้ระบบต้องสามารถกำหนดสิทธิ์การเข้าถึง โดยแยกตามโฟลเดอร์ ไฟล์ หรือฐานข้อมูล เป็นต้น

(๔) กำหนดให้การขอเข้าถึงข้อมูลนอกเหนือจากอำนาจหน้าที่ต้องได้รับอนุมัติจากเจ้าของข้อมูลหรือผู้ที่ได้รับมอบอำนาจก่อนการเข้าถึง

(๕) กำหนดให้มีการทบทวนสิทธิ์การเข้าถึงข้อมูลอย่างน้อยปีละ ๑ ครั้ง

(๖) กำหนดให้มีการบันทึกกิจกรรมการเข้าถึงข้อมูล (Log) โดยบันทึกข้อมูล ดังนี้ ผู้ใช้ เวลา ข้อมูลที่เข้าถึง

(๗) พิจารณานำระบบ DLP (Data Loss Prevention) หรือ SIEM ตรวจจับพฤติกรรมเสี่ยงในการเข้าถึงข้อมูล

๑๘. กำหนดให้มีการบริหารจัดการรหัสผ่าน โดยพิจารณาตามแนวทางมาตรฐานสากล เช่น NIST SP ๘๐๐-๖๓B หรือ ISO๒๗๐๐๑ โดยกำหนดมาตรการ อย่างน้อยดังนี้

๑) รหัสผ่านต้องมีความยาวอย่างน้อย ๘ ตัวอักษร และสามารถใช้ได้สูงสุดถึง ๖๔ ตัวอักษร

๒) เน้นรหัสผ่านที่จำง่าย แต่ยากต่อการคาดเดา เช่น วลี หรือประโยคสั้นๆ ที่มีความหมายเฉพาะตัว ตัวอย่าง: “chanrakmaw ๓ tuamakmak” “ฉันชอบกินข้าวผัดกะเพราไข่ดาว”

๓) เปลี่ยนรหัสผ่านเมื่อมีเหตุผล เช่น เมื่อสงสัยว่ารหัสผ่านอาจรั่วไหล หรือเมื่อมีการเปลี่ยนแปลงบทบาทในองค์กร

๔) หลีกเลี่ยงการใช้รหัสผ่านที่เป็น Common password หรือ Default password หรือรหัสผ่านที่รั่วไหลจากฐานข้อมูลที่ถูกแฮก หรือสิ่งที่สามารถคาดเดาได้ง่าย หรือข้อมูลส่วนตัวที่สามารถหาได้จากโซเชียลมีเดีย ตัวอย่าง: "password๑๒๓", "admin๑๒๓๔“ “วันเกิด” “หมายเลขโทรศัพท์”

๕) ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้ เช่น ใช้รหัส OTP ที่ส่งมาทาง SMS หรือแอปพลิเคชัน Authenticator หรือการยืนยันผ่าน Biometric (เช่น ลายนิ้วมือหรือใบหน้า)

๖) ไม่ควรใช้รหัสผ่านซ้ำกันในแต่ละระบบ และไม่ควรบอกรหัสผ่านแก่ผู้อื่น

๑๙. กำหนดให้มีการบริหารจัดการใช้โปรแกรมอรรถประโยชน์ โดยพิจารณามาตรการควบคุมอย่างน้อยดังนี้

๑) จัดทำ Whitelist ของ โปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานในองค์กร

๒) ห้ามติดตั้งหรือใช้งานโปรแกรมอรรถประโยชน์ที่ไม่ได้รับอนุญาต โดยเฉพาะจากแหล่งที่ไม่น่าเชื่อถือ

๓) จำกัดสิทธิ์ในการใช้งานโปรแกรมตามหลัก Least Privilege

๔) บันทึก Log การเปิดใช้งานและคำสั่งที่รันจากโปรแกรมอรรถประโยชน์ โดยเฉพาะโปรแกรมที่มีผลต่อระบบหรือข้อมูล

๕) พิจารณาใช้ระบบ SIEM หรือ Endpoint Detection & Response (EDR) ตรวจจับพฤติกรรมเสี่ยง หรือพฤติกรรมผิดปกติ เช่น การรัน PowerShell ผิดปกติ

๖) ตรวจสอบ Log อย่างสม่ำเสมอ และพิจารณาเปิดการแจ้งเตือนเมื่อมีการใช้งานโปรแกรมต้องสงสัย

๗) ห้ามผู้ใช้งานทั่วไปติดตั้งโปรแกรมอรรถประโยชน์ด้วยตนเอง

๘) โปรแกรมที่ไม่ใช้งานอีกต่อไปต้องถูกถอนการติดตั้งหรือล็อกการใช้งาน

๙) กำหนดให้มีการทบทวนรายชื่อผู้ใช้งานและสิทธิ์การใช้โปรแกรมอรรถประโยชน์อย่างน้อย ปีละ ๑ ครั้ง

๑๐) ดำเนินการถอนโปรแกรมอรรถประโยชน์ทันที เมื่อพนักงานพ้นหน้าที่ หรือไม่มีความจำเป็นในการใช้งาน

(E) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้ดำเนินการจัดทำขั้นตอนของการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัย ประกอบด้วย ๔ ขั้นตอนหลัก ดังนี้

(๑) การวางแผน (Planning) โดยจัดให้มีการวางแผน และพัฒนานโยบายและกระบวนการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัยของระบบ (Security-Focused Configuration Management: SecCM) รวมถึงการนำนโยบายและกระบวนการที่กำหนดนำเข้าผนวกกับแผนเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยที่มีอยู่ รวมถึงระบุขอบเขตหรือการบังคับใช้กระบวนการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัยของระบบ (Security-Focused Configuration Management: SecCM) และดำเนินการเผยแพร่นโยบายและกระบวนการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัยของระบบ (Security-Focused Configuration Management: SecCM) ซึ่งนโยบายที่จัดทำขึ้นควรพิจารณาเนื้อหาครอบคลุมอย่างน้อย ดังนี้ การนำแผนการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัยของระบบ (Security-Focused Configuration Management: SecCM) ไปใช้ การรวมเข้ากับแผนความมั่นคงปลอดภัยที่มีอยู่ คณะกรรมการควบคุมการกำหนดค่า (CCB) กระบวนการควบคุมการเปลี่ยนแปลงการกำหนดค่า เครื่องมือและเทคโนโลยี การใช้การกำหนดค่าความมั่นคงปลอดภัยทั่วไป และการกำหนดค่าขั้นต่ำ การเฝ้าระวัง และชี้วัดสำหรับการปฏิบัติตามข้อกำหนด

(๒) จัดให้มีการระบุและใช้งานการกำหนดค่า (Identifying and Implementing Configuration) หลังจากกิจกรรมการวางแผนและการจัดเตรียมเสร็จสิ้น โดยดำเนินการพัฒนา สอบทาน อนุมัติ และนำการกำหนดค่าขั้นต่ำที่มั่นคงปลอดภัยสำหรับระบบไปใช้การกำหนดค่าขั้นต่ำที่ได้รับอนุมัติสำหรับระบบและส่วนประกอบที่เกี่ยวข้อง (Associated Component) ซึ่งต้องสอดคล้องกับข้อกำหนดและข้อจำกัดในการปฏิบัติงาน รวมถึงระบุการกำหนดค่าขั้นต่ำที่มั่นคงปลอดภัย (Secure Baseline) สำหรับระบบทั่วไป ควรพิจารณากำหนดให้มีการตั้งค่าคอนฟิกูเรชัน (Configuration Setting) การโหลดซอฟต์แวร์ (Software Load) ระดับแพตช์ (Patch Level) วิธีการจัดระบบข้อมูลทางกายภาพหรือทางตรรกะ วิธีการควบคุมความมั่นคงปลอดภัยต่าง ๆ ที่ถูกนำมาใช้รวมถึงคู่มือหรือเอกสารประกอบ

ทั้งนี้ อาจใช้ระบบอัตโนมัติโดยตั้งค่าให้เครื่องมือสามารถทำงานร่วมกัน (Interoperability) และกำหนดค่าขั้นต่ำของระบบต่าง ๆ ในรูปแบบเดียวกัน (Uniformity)

(๓) กำหนดให้มีการบริหารจัดการควบคุมการเปลี่ยนแปลงการกำหนดค่าที่มั่นคงปลอดภัย (Controlling Configuration Change) เมื่อมีการเปลี่ยนแปลงที่สำคัญที่เกิดขึ้น เพื่อรักษาระดับพื้นฐานที่มั่นคงปลอดภัย โดยต้องดำเนินการอย่างน้อย ดังนี้ ระบุถึงการเปลี่ยนแปลงค่าที่ปลอดภัย นำเสนอ สอบทานและวิเคราะห์ผลกระทบด้านความมั่นคงปลอดภัย รวมถึงดำเนินการทดสอบ และนำขออนุมัติอย่างเป็นทางการก่อนนำไปใช้งาน

(๔) การเฝ้าระวัง (Monitoring) เป็นกิจกรรมการตรวจสอบ และติดตามการปฏิบัติตามนโยบายและกระบวนการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัยของระบบ (Security-Focused Configuration Management: SecCM) โดยการสุ่มตรวจสอบการตั้งค่าของระบบต่าง ๆ ที่มีความสำคัญเทียบกับเอกสาร การกำหนดการตั้งค่าระบบ (System Configuration Management) รวมถึงกำหนดให้

รายงานสถานะความมั่นคงปลอดภัยของการจัดการกำหนดค่าแต่ละรายการที่ดำเนินการตรวจสอบ และนำข้อมูลการไม่ดำเนินการตามนโยบายและกระบวนการที่กำหนดเป็นข้อมูลตั้งต้นในการดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยต่อไป

๒. การจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) โดยอ้างอิงข้อกำหนดการตั้งค่าระบบจากแหล่งที่น่าเชื่อถือ เช่น ISO/IEC ๒๗๐๐๒, Center for Internet Security (CIS), Security Technical Implementation Guides (STIG), NIST, ENISA หรือตามคำแนะนำของเจ้าของผลิตภัณฑและจัดทำเป็นเอกสารอย่างเป็นลายลักษณ์อักษร โดยมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒) แบ่งแยกหน้าที่ (Separation of Duties)

๓) บังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๔) ลบบัญชีที่ไม่ได้ใช้

๕) ลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น ลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๖) ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗) การป้องกันมัลแวร์ (Malware)

๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

๙) ปิดการใช้งานอัลกอริทึมที่ไม่มีความปลอดภัย เช่น ๓DES, RC๔, SSLv๒, SSlv๓

ตัวอย่างการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย

มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคง ปลอดภัย	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด	N/A	สิทธิพิเศษในการเข้าถึงน้อยที่สุดต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติ และทบทวน การแบ่งแยกหน้าที่ (Separation of Duties) อย่างน้อยปีละ ๑ ครั้ง	สิทธิพิเศษในการเข้าถึงน้อยที่สุดต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติโดยมีการ กำหนดสิทธิจากส่วนกลาง และทบทวนการแบ่งแยก หน้าที่ (Separation of Duties)อย่างน้อยปีละ ๑ ครั้ง
๒) แบ่งแยกหน้าที่	N/A	การแบ่งแยกหน้าที่ต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติ และ	การแบ่งแยกหน้าที่ต้องมี การได้รับอนุมัติเป็น ลายลักษณ์อักษร และนำมา ปฏิบัติโดยมีการกำหนดสิทธิ จากส่วนกลาง

มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคง ปลอดภัย	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
		ทบทวนการแบ่งแยกหน้าที่อย่างน้อยปีละ ๑ ครั้ง	และทบทวน การแบ่งแยกหน้าที่ อย่าง น้อยปีละ ๑ ครั้ง
๓) บังคับใช้นโยบายความซับซ้อนของรหัสผ่าน	รหัสผ่านต้องยาวกว่า ๘ ตัวอักษร	รหัสผ่านต้องยาวกว่า ๑๐ ตัวอักษรและควรมีการใช้ การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication)	รหัสผ่านต้องยาวกว่า ๑๒ ตัวอักษรและต้องมีการใช้ การยืนยันตัวตนโดยใช้ หลายปัจจัย (Multi-Factor Authentication)
๔) ลบบัญชีที่ไม่ได้ใช้	ลบบัญชีที่ไม่ได้ใช้หรือปิดการใช้งานไว้ (Disable) ภายใน ๗๒ ชั่วโมงเมื่อสิ้นสุดกิจกรรม	ลบบัญชีที่ไม่ได้ใช้หรือปิด การใช้งานไว้ (Disable) ภายใน ๔๘ ชั่วโมงเมื่อสิ้นสุด กิจกรรม	ลบบัญชีที่ไม่ได้ใช้หรือหรือ ปิดการใช้งานไว้ (Disable) ทันทีเมื่อสิ้นสุดกิจกรรม
๕) ลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น ลบคอมไพเลอร์ และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก	ตรวจสอบการลบบริการและแอปพลิเคชัน ที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ และแอป พลิเคชันสนับสนุน ผู้ให้บริการภายนอก ก่อนนำมา ใช้งาน และตรวจสอบ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ที่มีนัยสำคัญ	ตรวจสอบการลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ และแอปพลิเคชันสนับสนุน ผู้ให้บริการภายนอก ก่อนนำมา ใช้งาน และตรวจสอบอย่างน้อย ไตรมาสละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ที่มีนัยสำคัญ	ตรวจสอบการลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ และแอปพลิเคชันสนับสนุน ผู้ให้บริการภายนอก ก่อนนำมา ใช้งาน และตรวจสอบ อย่างน้อยเดือนละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ที่มีนัยสำคัญ
๖)ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน	ปิดพอร์ตเครือข่ายที่ไม่ได้ ใช้งาน และมีการป้องกัน การเข้าถึงพอร์ต ทางกายภาพ	ปิดพอร์ตเครือข่ายที่ไม่ได้ ใช้งาน มีการป้องกันการเข้าถึงพอร์ตทางกายภาพ มีการป้องกันการเข้าถึงทางกายภาพ เช่น มีกรงกั้น มีรั้ว และการควบคุม การเข้าถึงทางกายภาพ	ปิดพอร์ตเครือข่ายที่ไม่ได้ ใช้งานโดยควบคุมจาก ส่วนกลาง เช่น ระบบบริหาร จัดการจากศูนย์กลาง (Active Directory: AD) เป็นต้น มีการป้องกันการเข้าถึง พอร์ตทางกายภาพ มีการป้องกันการเข้าถึง ทางกายภาพ เช่น มีกรงกั้น มีรั้ว และการควบคุม การเข้าถึงทางกายภาพ
๗)การป้องกันมัลแวร์ (Malware)	อัพเดทฐานข้อมูลสำหรับการตรวจสอบรูปแบบมัลแวร์ (Signature) และเวอร์ชันของซอฟต์แวร์สำหรับการป้องกันมัลแวร์อยู่อย่างสม่ำเสมอ	อัพเดทฐานข้อมูลสำหรับ การตรวจสอบรูปแบบ มัลแวร์ (Signature) และ เวอร์ชันของซอฟต์แวร์ สำหรับการป้องกันมัลแวร์ อยู่อย่างสม่ำเสมอ	อัพเดทฐานข้อมูลสำหรับ การตรวจสอบรูปแบบ มัลแวร์ (Signature) และ เวอร์ชันของซอฟต์แวร์ สำหรับการป้องกันมัลแวร์ อยู่อย่างสม่ำเสมอและมีการ ส่งบันทึก (Log) ไปยังระบบ ส่วนกลาง เพื่อตรวจจับและ วิเคราะห์ความผิดปกติ รวมถึงมี

มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคง ปลอดภัย	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
			เทคโนโลยีขั้นสูงอื่น ๆ เช่น IDS, IPS, EDR เป็นต้น
๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม	ปรับปรุงซอฟต์แวร์ และแพตช์ (Patch) ความมั่นคงปลอดภัยของ ระบบภายใน ๗ วัน เมื่อมีแพตช์ระดับวิกฤต	ปรับปรุงซอฟต์แวร์ และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบภายใน ๗๒ ชั่วโมง เมื่อมีแพตช์ระดับวิกฤต	ปรับปรุงซอฟต์แวร์ และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบภายใน ๔๘ ชั่วโมง เมื่อมีแพตช์ระดับวิกฤต

๓. กำหนดให้มีการตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ ตามตัวอย่างดังตาราง

ทรัพย์สิน	รายการที่ต้องดำเนินการ	การตั้งค่า ตามมาตรฐานการกำหนดค่าขั้นต่ำ	สถานะการตรวจสอบ
เครื่องแม่ข่ายที่จะเชื่อมต่อกับบริการที่สำคัญ	ตั้งรหัสผ่าน BIOS/เฟิร์มแวร์	รหัสผ่านต้องยาวมากกว่า ๑๒ ตัวอักษร	Yes/no
	ตั้งรหัสผ่านบูตโหลดเดอร์ (Boot Loader)	รหัสผ่านต้องยาวมากกว่า ๑๒ ตัวอักษร	Yes/no
	กำหนดค่าสำหรับการพิสูจน์ตัวตน เพื่อเข้าถึงระบบปฏิบัติการ (Configure OS User Authentication)	- รหัสผ่านของบัญชีผู้ใช้ต้องยาวมากกว่า ๑๒ ตัวอักษร - สร้างบัญชีผู้ใช้ตามที่ได้รับอนุญาตเท่านั้น หรือต้องดำเนินการด้วยระบบ LDAP หรือRADIUS ของหน่วยงานเท่านั้น - ห้ามการเข้าถึงจากระยะไกลด้วยบัญชี Root	Yes/no
	กำหนดเทคโนโลยีการพิสูจน์ตัวตน และเทคโนโลยีการเข้ารหัส	- กำหนดการเข้าถึงโปรแกรมประยุกต์ ที่สำคัญต้องทำผ่านการยืนยันตัวตนด้วย สองปัจจัยเป็นอย่างน้อย (๒-FA) - เปิดใช้งานการเข้ารหัส TLS ๑.๓ ขึ้นไป สำหรับ Web services และโปรแกรม ประยุกต์	Yes/no

๔. กำหนดให้มีการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๕. กำหนดให้มีการบริหารจัดการการเปลี่ยนแปลง โดยจัดทำเป็นเอกสาร ซึ่งควรประกอบด้วยขั้นตอน ดังนี้ การร้องขอการเปลี่ยนแปลง โดยใช้แบบฟอร์มการร้องขอการเปลี่ยนแปลง (Change Request) เพื่อประเมินผลกระทบการเปลี่ยนแปลงก่อนดำเนินการเปลี่ยนแปลง โดยระบุข้อมูลอย่างน้อย ดังนี้

วัตถุประสงค์, ขอบเขต, รายละเอียดการเปลี่ยนแปลง, ความเสี่ยง, แผนการดำเนินงาน, ผู้รับผิดชอบ, แผนทดแทน และแผนย้อนกลับ (Rollback Plan) และนำขออนุมัติก่อนดำเนินการเปลี่ยนแปลง

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการประเมินผลกระทบและความเสี่ยง โดยวิเคราะห์ผลกระทบต่อระบบสารสนเทศความต่อเนื่องในการให้บริการ และความมั่นคงปลอดภัยของข้อมูล

๒. กำหนดให้มีการอนุมัติการเปลี่ยนแปลง โดยพิจารณาให้มีการประชุม เพื่อพิจารณาอนุมัติหรือปฏิเสธการเปลี่ยนแปลงที่สำคัญ

๓. กำหนดให้ต้องมีการจัดแผน Rollback ที่สามารถดำเนินการได้ทันทีหากเกิดปัญหาในการเปลี่ยนแปลง

๔. กำหนดให้มีการติดตามผลและการปิดการเปลี่ยนแปลง พร้อมทั้งจัดทำรายงาน Post-Implementation Review (PIR) หรือ Lessons Learned และบันทึกข้อมูลการเปลี่ยนแปลงอย่างเป็นระบบ

๕. กำหนดให้มีการบริหารจัดการพัฒนาซอฟต์แวร์ โดยจัดให้มีการกำหนดความต้องการด้านความมั่นคงปลอดภัย โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) จัดให้มีการเก็บข้อมูลความต้องการด้านความมั่นคงปลอดภัย เช่น การพิสูจน์ตัวตน, การเข้ารหัส, การควบคุมสิทธิ์ เป็นต้น

๒) ดำเนินการวิเคราะห์ภัยคุกคาม (Threat Modeling) และความเสี่ยงของระบบก่อนเริ่มพัฒนาซอฟต์แวร์

๓) จัดให้มีรายการตรวจสอบข้อกำหนดด้านความมั่นคงปลอดภัย (Security Requirement Checklist) และจัดเก็บเอกสารไว้เป็นหลักฐานการตรวจสอบ

๖. กำหนดให้มีการบริหารจัดการวงจรชีวิตของระบบ (System Lifecycle Security Management) โดยวางแผน วิเคราะห์และออกแบบ รวมถึงความต้องการด้านความมั่นคงปลอดภัย โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) ดำเนินการประเมินความเสี่ยงเบื้องต้นของระบบ พร้อมทั้งระบุระดับความสำคัญของข้อมูลและระดับผลกระทบ (Impact Level) เพื่อกำหนดมาตรการควบคุมที่เหมาะสม

๒) นำหลักการ "Security by Design" และ "Privacy by Design" ผนวกเข้ากับการออกแบบระบบ โดยพิจารณาอย่างน้อย ดังนี้

(๑) กำหนดมาตรการควบคุมด้านการพิสูจน์ตัวตน การเข้ารหัสข้อมูล และการตรวจสอบการเข้าถึง

(๒) ดำเนินการวิเคราะห์ผลกระทูลด้านข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) ในกรณีที่ระบบมีการจัดเก็บข้อมูลส่วนบุคคล

๗. กำหนดให้มีการพัฒนาและทดสอบความปลอดภัยของระบบ โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) ปฏิบัติตามแนวทางการพัฒนาซอฟต์แวร์อย่างปลอดภัย (Secure Software Development Lifecycle - SSDLC) โดยจัดให้มีการดำเนินการทดสอบความมั่นคงปลอดภัยของระบบ เช่น Penetration

Test, Vulnerability Scan พร้อมทั้งจัดทำเอกสารด้านความมั่นคงปลอดภัย เช่น Secure Configuration Guidelines เป็นต้น

๘. กำหนดให้มีการบริหารจัดการติดตั้งระบบ โดยดำเนินการติดตั้งระบบตามมาตรฐานความปลอดภัยที่กำหนด (Security Baseline) ขององค์กร และกำหนดให้มีการดำเนินการตรวจสอบความมั่นคงปลอดภัยก่อนนำระบบขึ้นใช้งานจริง (Go-live Security Assessment) รวมถึงจัดทำแผนตอบสนองต่อเหตุการณ์ (Incident Response Plan) และแผนบริหารความต่อเนื่อง (BCP/DRP)

๙. กำหนดให้มีการบริหารจัดการบำรุงรักษาและติดตาม โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) กำหนดให้มีการตรวจสอบและติดตามการใช้งานระบบอย่างสม่ำเสมอ (Monitoring and Logging)

๒) กำหนดให้มีการจัดการอัปเดตซอฟต์แวร์ แพตช์ รวมถึงกำหนดให้มีการเปลี่ยนแปลงระบบอย่างปลอดภัย (Patch and Change Management)

๓) กำหนดให้มีการประเมินและทบทวนความเสี่ยงอย่างต่อเนื่องตลอดอายุการใช้งานของระบบ

๑๐. กำหนดให้มีการบริหารจัดการควบคุมความเสี่ยงในกรณีที่มีการยกเลิกใช้งานระบบ (Disposal Phase) โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) กำหนดให้มีการวางแผนการยกเลิกใช้งานระบบอย่างปลอดภัย (Secure Decommissioning Plan)

๒) ดำเนินการวางแผนลบข้อมูลหรือทำลายข้อมูลอย่างปลอดภัย (Secure Data Erasure) ตามมาตรฐาน เช่น NIST SP ๘๐๐-๘๘ เป็นต้น

๓) ดำเนินการถอดถอนระบบงานออกจากการใช้งาน และอัปเดตบัญชีสินทรัพย์ไอที (IT Asset Inventory)

๑๑. กำหนดให้มีการออกแบบและพัฒนาอย่างปลอดภัย โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) กำหนดให้มีการจัดการช่องโหว่ในไลบรารีและส่วนประกอบซอฟต์แวร์ โดยจัดให้มีกระบวนการตรวจหาไลบรารีภายนอก เช่น frameworks, packages, modules เป็นต้น ที่นำมาใช้ในซอฟต์แวร์ เพื่อตรวจสอบช่องโหว่ด้านความมั่นคงปลอดภัย (vulnerabilities) พร้อมทั้งอัปเดตให้เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอ

๒) กำหนดให้มีการตรวจสอบความมั่นคงปลอดภัยของโค้ด (Security Code Review) ก่อนนำระบบขึ้นใช้งานจริง (Production)

๑๒. กำหนดให้มีการดำเนินการทดสอบความมั่นคงปลอดภัย เช่น Static Application Security Testing (SAST) Dynamic Application Security Testing (DAST) หรือ Penetration Testing เป็นต้น พร้อมทั้งจัดทำบันทึกผลการทดสอบและแก้ไขช่องโหว่ก่อนขึ้นใช้งานจริง

๑๓. กำหนดให้มีการควบคุมเวอร์ชันและการเปลี่ยนแปลง โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) จัดเก็บซอร์สโค้ดและเวอร์ชันใน Git หรือระบบควบคุมเวอร์ชันที่ปลอดภัย

๒) บังคับใช้แนวปฏิบัติการควบคุมการเปลี่ยนแปลง ในกรณีที่ระบบมีการเปลี่ยนแปลง พร้อมทั้งบันทึกการเปลี่ยนแปลงโค้ด และเหตุผลในการเปลี่ยนแปลงรวมถึงผู้รับผิดชอบ (Change Log)

๑๔. กำหนดให้มีการควบคุมในกรณีที่มีการจ้างหน่วยงานภายนอกพัฒนา โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) ระบุข้อกำหนดด้านความมั่นคงปลอดภัยในสัญญาให้ชัดเจน (Security Clause in Contract)

๒) กำหนดให้มีการตรวจสอบผลทดสอบช่องโหว่ก่อนรับมอบงาน

๓) ห้ามผู้พัฒนาภายนอกเข้าถึงระบบงาน (Production) โดยตรง ในกรณีที่ความจำเป็นต้องเข้าถึงระบบงาน (Production) ต้องมีกระบวนการอนุมัติ และกำหนดสิทธิการเข้าถึงให้ชัดเจน รวมถึงระยะเวลาในการเข้าถึง

๑๕. กำหนดให้มีการควบคุมข้อมูลในสภาพแวดล้อมพัฒนา โดยพิจารณาให้มีการดำเนินการอย่างน้อยดังนี้

๑) ห้ามใช้ข้อมูลจริงในการพัฒนาระบบ รวมถึงการทดสอบระบบ โดยไม่มีการปกปิดข้อมูล (Masking/Anonymization)

๒) กำหนดให้มีการควบคุมการนำข้อมูลออกนอกระบบพัฒนา เช่น ผ่าน USB, Cloud Drive, หรือ Email ส่วนตัว เป็นต้น

๓) กำหนดให้มีการบันทึกกิจกรรม (Log) รวมถึงการติดตามบันทึกกิจกรรม (Log) การเข้าถึงและการทำงานในระหว่างการพัฒนาระบบอย่างต่อเนื่อง

๑๖. กำหนดให้มีการบริหารจัดการข้อจำกัดการติดตั้งซอฟต์แวร์ โดยกำหนดสิทธิ์ในการติดตั้งซอฟต์แวร์ โดยพิจารณาอย่างน้อยดังนี้

๑) อนุญาตให้ติดตั้งซอฟต์แวร์เฉพาะโดยผู้ปฏิบัติงานฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ปฏิบัติที่ได้รับมอบหมายตามหน้าที่ความรับผิดชอบ

๒) ไม่อนุญาตให้ผู้ใช้งานทั่วไปมีสิทธิ์ในการติดตั้งซอฟต์แวร์บนอุปกรณ์

๓) ซอฟต์แวร์ที่อนุญาตให้ติดตั้ง หรือใช้งานต้องผ่านการประเมินความมั่นคงปลอดภัย ความเข้ากันได้กับระบบ และการตรวจสอบลิขสิทธิ์

๔) กำหนดให้มีการจัดทำ “บัญชีซอฟต์แวร์ที่ได้รับอนุญาต” (Approved Software List) เพื่อใช้ในการควบคุมการติดตั้งซอฟต์แวร์

๕) กำหนดให้มีรายการตรวจสอบการติดตั้งซอฟต์แวร์ พร้อมทั้งจัดทำบันทึกการติดตั้งเป็นหลักฐาน

๖) พิจารณาใช้ระบบตรวจจับและป้องกันการใช้งานซอฟต์แวร์ต้องห้าม เช่น Application Whitelisting หรือ Endpoint Detection and Response (EDR) เป็นต้น พร้อมทั้งตั้งค่าระบบให้แจ้งเตือนเมื่อมีการพยายามติดตั้งโปรแกรมจากแหล่งที่ไม่ได้รับอนุญาต

๗) กำหนดให้มีการตรวจสอบรายงานการใช้งานซอฟต์แวร์อย่างน้อยปีละ ๑ ครั้ง และดำเนินการลบหรือล็อกการใช้งาน ในกรณีที่พบสิ่งผิดปกติ

๘) จัดให้มีการเก็บบันทึก (Logs) การติดตั้งและถอนการติดตั้งซอฟต์แวร์ เพื่อใช้ในการตรวจสอบย้อนหลัง

๙) กำหนดให้มีการถอนการติดตั้งและจัดการซอฟต์แวร์ เมื่อเลิกใช้งานหรือหมดอายุการใช้งาน โดยต้องถอนการติดตั้งซอฟต์แวร์ทันที และในกรณีที่ซอฟต์แวร์ที่ไม่มีการอัปเดตจากผู้ผลิต หรือไม่มีความจำเป็นต้องใช้งาน ต้องพิจารณาเลิกใช้งาน เพื่อบริหารจัดการความเสี่ยงจากช่องโหว่ของซอฟต์แวร์

๑๗. กำหนดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่าย โดยการออกแบบโครงสร้างเครือข่ายที่ปลอดภัย โดยคำนึงถึงการพิจารณา อย่างน้อย ดังนี้

๑) จัดแบ่งเครือข่ายออกเป็นโซนตามระดับความสำคัญและความอ่อนไหวของข้อมูล เช่น โซนอินเทอร์เน็ต โซนเครือข่ายภายใน โซนเซิร์ฟเวอร์ และโซนข้อมูลสำคัญ

๒) จัดให้มีการป้องกันหลายชั้น โดยไม่พึ่งพาเพียงกลไกป้องกันเดียว (Defense-in-Depth)

๓) กำหนดโซน DMZ สำหรับเซิร์ฟเวอร์ที่ต้องเชื่อมต่อกับเครือข่ายภายนอก

๑๘. กำหนดให้มีการติดตั้งและการกำหนดค่าอุปกรณ์เครือข่าย โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) ปิดพอร์ตและบริการที่ไม่จำเป็นต่อการทำงาน

๒) อัปเดตเฟิร์มแวร์ของอุปกรณ์เครือข่ายให้เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอ

๓) กำหนดให้ใช้การพิสูจน์ตัวตนหลายปัจจัยสำหรับการเข้าถึงอุปกรณ์สำคัญ

๔) กำหนดมาตรฐานการตั้งค่าความปลอดภัยสำหรับอุปกรณ์แต่ละประเภท

๕) สำรองและจัดเก็บการกำหนดค่าของอุปกรณ์อย่างปลอดภัย

๑๙. กำหนดให้มีการเข้ารหัสข้อมูลในการส่งผ่านเครือข่าย โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้ใช้ TLS/SSL สำหรับการสื่อสารผ่านเว็บ

๒) กำหนดนโยบายการใช้ VPN สำหรับการเข้าถึงจากระยะไกล

๓) กำหนดให้ใช้การพิสูจน์ตัวตนหลายปัจจัยสำหรับการเชื่อมต่อ VPN

๒๐. กำหนดให้มีการตรวจสอบและการตรวจจับภัยคุกคาม โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) กำหนดนโยบายบันทึกเหตุการณ์จากอุปกรณ์เครือข่าย

๒) ใช้ระบบรวมศูนย์การเก็บบันทึกเหตุการณ์ เช่น SIEM (Security Information and Event Management)

๓) ดำเนินการสแกนช่องโหว่ของระบบเครือข่ายอย่างสม่ำเสมอ

๔) จัดให้มีการทดสอบเจาะระบบเครือข่ายโดยผู้เชี่ยวชาญอย่างน้อยปีละครั้ง

๒๑. กำหนดให้มีการควบคุมการเข้าถึงเครือข่าย โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) จำกัดสิทธิ์การเข้าถึงเครือข่ายตามหน้าที่และความรับผิดชอบ

๒) ทบทวนสิทธิ์การเข้าถึงเครือข่ายเป็นประจำ

๒๒. กำหนดให้มีการบริหารจัดการรักษาความปลอดภัยฐานข้อมูล โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีการจัดทำแนวปฏิบัติการบริหารจัดการฐานข้อมูลที่ครอบคลุมการควบคุมการเข้าถึง การปกป้องข้อมูล และการติดตามตรวจสอบ

๒) กำหนดให้มีการจัดทำแนวปฏิบัติการจัดการบัญชีผู้ใช้ และสิทธิ์การเข้าถึงฐานข้อมูล (Database Access Control Policy)

๓) กำหนดให้มีการจัดทำแนวปฏิบัติการสำรองและกู้คืนข้อมูลฐานข้อมูล (Database Backup and Recovery Policy)

๔) การบริหารจัดการควบคุมการเข้าถึงฐานข้อมูล ต้องประกอบไปด้วย

(๑) จำกัดการเข้าถึงเฉพาะผู้ที่มีหน้าที่เกี่ยวข้องตามหลัก Least Privilege

(๒) กำหนดให้มีการแยกหน้าที่ความรับผิดชอบระหว่างผู้ดูแลระบบและผู้พัฒนา (Segregation of Duties) อย่างชัดเจน

(๓) กำหนดให้ใช้การพิสูจน์ตัวตนแบบเข้มงวด เช่น การใช้รหัสผ่านที่ซับซ้อน, Multi-Factor Authentication (MFA) เป็นต้น

(๔) กำหนดระยะเวลา Session Timeout สำหรับการเชื่อมต่อฐานข้อมูล

๒๓. การบริหารจัดการปกป้องข้อมูลในฐานข้อมูล ต้องประกอบไปด้วย

๑) กำหนดให้มีการเข้ารหัสข้อมูลที่สำคัญทั้งขณะจัดเก็บ (Encryption at Rest) และขณะส่งข้อมูล (Encryption in Transit)

๒) กำหนดให้ใช้เทคนิคการ Masking หรือ Anonymization กับข้อมูลที่ใช้ในระบบทดสอบ (Test Data Protection)

๓) กำหนดให้ใช้มาตรการควบคุมความสมบูรณ์ของข้อมูล เช่น ตรวจสอบค่า Hash หรือใช้การทำ Data Integrity Verification

๔) กำหนดนโยบายการจัดการข้อมูลที่หมดอายุหรือไม่จำเป็น เช่น การลบหรือทำลายข้อมูลอย่างปลอดภัย (Secure Deletion)

๒๔. การบริหารจัดการติดตามและตรวจสอบการใช้งานฐานข้อมูล ต้องประกอบไปด้วย

๑) กำหนดให้มีการเปิดใช้งานระบบบันทึกการทำงาน (Database Auditing) เพื่อบันทึกกิจกรรมที่สำคัญ เช่น การเข้าใช้ การอ่าน การแก้ไข และการลบข้อมูล

๒) พิจารณาใช้เครื่องมือวิเคราะห์และตรวจจับพฤติกรรมผิดปกติ (Database Activity Monitoring: DAM)

๓) กำหนดการทบทวน Log การใช้งานฐานข้อมูลอย่างสม่ำเสมอ และแจ้งเตือนเมื่อพบกิจกรรมต้องสงสัย

๔) พิจารณาตั้งค่าระบบแจ้งเตือน (Alert System) สำหรับเหตุการณ์ผิดปกติที่มีความเสี่ยงสูง

๒๕. การบริหารจัดการสำรองและการกู้คืนฐานข้อมูล ต้องประกอบไปด้วย

๑) กำหนดให้มีการสำรองฐานข้อมูลอย่างสม่ำเสมอ และกำหนดระยะเวลาการสำรองข้อมูลให้เป็นไปตามระดับความสำคัญของข้อมูล

๒) กำหนดให้มีกระบวนการกู้คืนข้อมูล (Recovery Test) อย่างสม่ำเสมอ เช่น ไตรมาสละ ๑ ครั้ง เป็นต้น

๓) กำหนดให้มีการจัดเก็บข้อมูลสำรองแยกจากระบบปฏิบัติการหลัก และปกป้องข้อมูลสำรองด้วยการเข้ารหัสและควบคุมการเข้าถึง

๒๖. กำหนดให้มีการบริหารจัดการความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม โดยกำหนดมาตรการควบคุมการเข้า - ออก เพื่อดูแลรักษาความปลอดภัย โดยบุคคลที่ต้องการสิทธิในการเข้า - ออก ต้องขออนุญาตเป็นลายลักษณ์อักษร

๒๗. ต้องทำการยืนยันตัวตนก่อนเข้าพื้นที่ทุกครั้ง เพื่อป้องกันการเข้า - ออกโดยไม่ได้รับอนุญาต

๒๘. ควบคุมการลงชื่อ บันทึกวัน เวลา และวัตถุประสงค์การเข้า - ออก ของผู้ใช้งาน และบุคคลภายนอก (Visitors) ทุกครั้ง

๒๙. ตรวจสอบการเข้าถึงอาคารต่าง ๆ ที่มีระบบสารสนเทศที่สำคัญอย่างต่อเนื่อง รวมถึงการจัดให้มีอุปกรณ์หรือเครื่องมือแจ้งเตือน เพื่อตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต หรือพฤติกรรมที่น่าสงสัย

๓๐. ดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอก (Visitors) ในขณะที่ปฏิบัติงาน จนกระทั่งเสร็จสิ้นภารกิจและออกจากศูนย์คอมพิวเตอร์ เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๓๑. กำหนดให้มีการบริหารจัดการระบบและอุปกรณ์สนับสนุนการทำงาน ต้องดำเนินการวางแผนและติดตั้งอุปกรณ์ โดยพิจารณาอย่างน้อยดังนี้

๑) ต้องติดตั้งอุปกรณ์สนับสนุนในพื้นที่ควบคุมที่มีการออกแบบตามมาตรฐานความปลอดภัย เช่น TIA-๙๔๒ หรือ Uptime Tier เป็นต้น

๒) ดำเนินการตรวจสอบให้มั่นใจว่าอุปกรณ์ที่ติดตั้งมีคุณสมบัติรองรับภาระงานของระบบ และมีระบบสำรองหากเกิดความล้มเหลว รวมถึงควบคุมการเข้าถึงพื้นที่ที่มีอุปกรณ์สำคัญ

๓๒. กำหนดให้มีการบำรุงรักษาและตรวจสอบสภาพการทำงาน โดยพิจารณาอย่างน้อยดังนี้

๑) จัดทำ แผนบำรุงรักษาเชิงป้องกัน (Preventive Maintenance Plan) สำหรับอุปกรณ์ทั้งหมด โดยกำหนดความถี่ที่เหมาะสม เช่น รายเดือน รายไตรมาส เป็นต้น

๒) พิจารณาให้มีการตรวจสอบสถานะการทำงานของอุปกรณ์แบบเรียลไทม์ด้วยระบบ Monitoring พร้อมแจ้งเตือนเมื่อเกิดเหตุผิดปกติ รวมถึงบันทึกผลการบำรุงรักษาและเหตุขัดข้องในระบบ Log สำหรับการตรวจสอบย้อนหลัง

๓) ติดตั้งระบบสำรองไฟ เช่น UPS Generator เป็นต้น และทดสอบการทำงานของระบบสำรองอย่างสม่ำเสมอ

๔) ตรวจสอบระบบดับเพลิงอัตโนมัติ เช่น FM-๒๐๐ CO_2 หรือระบบ Clean Agent เป็นต้น พร้อมทั้งตรวจสอบระบบดับเพลิงตามรอบระยะเวลา เช่น ทุก ๓ เดือน หรือ ๖ เดือน เป็นต้น

๕) กำหนดให้มีการใช้เซ็นเซอร์ตรวจจับความชื้น น้ำรั่ว และอุณหภูมิภายในห้องเซิร์ฟเวอร์ พร้อมตั้งค่าการแจ้งเตือน และกำหนดให้มีการตรวจสอบอย่างสม่ำเสมอ

๖) กำหนดให้มีการสำรองอุปกรณ์ หรือจัดทำแผนรองรับฉุกเฉิน ในกรณีที่อุปกรณ์สำคัญล้มเหลว

๗) จำกัดการเข้าถึงห้องระบบเฉพาะผู้มีหน้าที่รับผิดชอบ หรือผู้ที่ได้รับมอบหมาย โดยใช้ระบบควบคุมการเข้าออก เช่น การใช้บัตรผ่านเข้า-ออก หรือใช้ข้อมูล Biometric สำหรับการควบคุมการเข้า-ออก เป็นต้น และเก็บข้อมูลการเข้า-ออก อย่างน้อย ๙๐ วัน

๘) ในกรณีที่มีการเข้าถึงจากผู้ให้บริการภายนอก บุคคลภายนอก หรือผู้ที่ไม่มีสิทธิการเข้าถึงตามหน้าที่ความรับผิดชอบต้องจัดให้มีการลงทะเบียนเข้า-ออก และปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร

๓๓. กำหนดให้มีการบริหารความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร โดยการออกแบบและติดตั้งสายสัญญาณและสายสื่อสาร ควรพิจารณาอย่างน้อย ดังนี้

๑) การเดินสายสัญญาณและสายสื่อสารต้องวางแผนตามมาตรฐานอุตสาหกรรม เช่น TIA/EIA-๕๖๘, ISO/IEC ๑๑๘๐๑ เป็นต้น

๒) แยกสายสัญญาณข้อมูลออกจากสายไฟฟ้าแรงสูง เพื่อป้องกันการรบกวนทางแม่เหล็กไฟฟ้า (EMI) และพิจารณาใช้สายที่มีฉนวนหุ้มป้องกันการดักฟัง (Shielded Cable / Armored Fiber) ในพื้นที่สำคัญ

๓) กำหนดให้มีการใช้ท่อหรือรางสาย (Cable Conduit/Duct) ที่สามารถป้องกันการเข้าถึงสายสัญญาณและสายสื่อสารจากภายนอก

๔) ต้องมีการควบคุมการเข้า-ออก ในพื้นที่ที่ติดตั้งสาย เช่น ห้อง Data Center เป็นต้น รวมถึงจัดให้มีการเก็บบันทึกการเข้าออก

๕) กำหนดสิทธิเฉพาะผู้ที่ได้รับมอบหมาย หรือมีหน้าที่ความรับผิดชอบที่ชัดเจนในการปรับเปลี่ยน ดัดแปลง หรือซ่อมบำรุงรักษา

๖) จัดทำแผนผังการเดินสาย (Cabling Layout) และอัปเดตเมื่อมีการเปลี่ยนแปลง

๗) กำหนดรอบการตรวจสอบความสมบูรณ์ และการทำงานของสาย เช่น ทุก ๖ หรือ ๑๒ เดือน เป็นต้น และแยกการทดสอบสายสื่อสารในระบบสำคัญออกจากระบบที่ใช้งานทั่วไป รวมถึงจัดให้มีบันทึกการตรวจสอบ และบำรุงรักษา

๓๔. กำหนดให้มีการบริหารจัดการบำรุงรักษาและซ่อมบำรุงอุปกรณ์ (Equipment Maintenance and Repair Security Management) โดยการวางแผนและบันทึกประวัติการบำรุงรักษา ควรพิจารณาอย่างน้อย ดังนี้

๑) จัดทำแผนบำรุงรักษาเชิงป้องกัน (Preventive Maintenance Plan) รายปี โดยระบุอุปกรณ์ ช่วงเวลา และผู้รับผิดชอบ เป็นต้น

๒) บันทึกการดำเนินการทุกครั้งที่มีการเปลี่ยนแปลง เช่น รายการอุปกรณ์ที่บำรุงรักษา วันเวลา รายชื่อผู้ดำเนินการ และผลการตรวจสอบ เป็นต้น

๓) ดำเนินการแยกบันทึกสำหรับอุปกรณ์สำคัญ (Critical Assets) และกำหนดระดับความเร่งด่วนหากพบข้อบกพร่อง

๓๕. กำหนดให้มีการควบคุมการเข้าถึงในระหว่างการซ่อมบำรุง โดยพิจารณาอย่างน้อยดังนี้

๑) อนุญาตให้เฉพาะบุคลากรที่มีสิทธิหรือผู้ให้บริการที่ผ่านการตรวจสอบเข้าไปยังพื้นที่อุปกรณ์

๒) ผู้ให้บริการภายนอกต้องลงทะเบียนเวลาเข้า-ออก และต้องมีเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายควบคุมดูแลขณะดำเนินการ

๓) ห้ามคัดลอกข้อมูล หรือถ่ายภาพหน้าจอ หรือการตั้งค่าระบบ โดยไม่ได้รับอนุญาต

๓๖. กำหนดให้มีมาตรการด้านข้อมูลระหว่างการซ่อมบำรุง โดยพิจารณาอย่างน้อยดังนี้

๑) กรณีต้องส่งอุปกรณ์ซ่อมภายนอกต้องดำเนินการล้างข้อมูล หรือเข้ารหัสข้อมูลก่อนส่งอุปกรณ์เข้าซ่อม

๒) หากจำเป็นต้องเปิดระบบให้เข้าถึงข้อมูล ควรใช้บัญชีควบคุมพิเศษ และปิดใช้งานทันทีหลังดำเนินการ

๓) ห้ามนำอุปกรณ์ทดแทนที่ไม่ผ่านการรับรองเข้าระบบโดยไม่มีการตรวจสอบด้านความปลอดภัยล่วงหน้า

๓๗. กำหนดให้มีมาตรการตรวจสอบหลังการซ่อม โดยพิจารณาอย่างน้อยดังนี้

๑) ตรวจสอบความสมบูรณ์ของระบบหลังจากการบำรุงรักษา เช่น การทำงานของระบบปฏิบัติการ ความสมบูรณ์ของไฟล์ Log และการเชื่อมต่อเครือข่าย เป็นต้น

๒) กรณีที่ต้องดำเนินการเปลี่ยนอะไหล่ หรืออุปกรณ์ต้องบันทึกหมายเลขซีเรียลใหม่และอัปเดตทะเบียนสินทรัพย์

๓) หากพบสิ่งผิดปกติต้องรายงานต่อฝ่ายเทคโนโลยีสารสนเทศ หรือฝ่ายที่ได้รับมอบหมายเพื่อพิจารณาดำเนินการเพิ่มเติม

๓๘. กำหนดให้มีการบริหารการติดตั้งและป้องกันอุปกรณ์ (Installation and Protection of Equipment Management) โดยการวางแผนและการติดตั้งอุปกรณ์ ควรพิจารณาอย่างน้อยดังนี้

๑) การติดตั้งอุปกรณ์ต้องอยู่ภายใต้การอนุมัติและดำเนินการตามแบบแปลนที่ได้รับอนุมัติ

๒) ตำแหน่งติดตั้งต้องคำนึงถึงความปลอดภัยทางกายภาพ ความร้อน ความชื้น และความเสี่ยงต่อไฟฟ้าลัดวงจร

๓) อุปกรณ์ที่มีความสำคัญควรติดตั้งในห้องควบคุมพิเศษ เช่น Server Room, Data Center เป็นต้น และต้องมีการดำเนินการควบคุมการเข้า-ออกอย่างเคร่งครัด เช่น บัตรพนักงาน หรือระบบสแกนชีวมิติ เป็นต้น รวมถึงจัดเก็บ log การเข้าถึง

๔) การเชื่อมต่อสายสัญญาณและพลังงานต้องพิจารณาให้เป็นไปตามมาตรฐานด้านความปลอดภัยไฟฟ้าและสื่อสาร

๕) จัดให้มีแผนบำรุงรักษาอุปกรณ์ตามระยะเวลา (Preventive Maintenance Schedule) เช่น ทุก ๖ เดือน หรือ ๑ ปี เป็นต้น

๖) พิจารณาติดตั้งระบบตรวจสอบสถานะการทำงานของอุปกรณ์ (Monitoring Tools) และแจ้งเตือนเมื่อเกิดเหตุผิดปกติ รวมถึงเก็บประวัติการติดตั้ง ซ่อมบำรุง และเปลี่ยนอุปกรณ์ในระบบทะเบียนสินทรัพย์ (Asset Register)

๓๙. กำหนดให้มีการบริหารจัดการเมื่อถอดถอน หรือย้ายอุปกรณ์ โดยพิจารณาอย่างน้อยดังนี้

๑) กำหนดให้การย้ายอุปกรณ์ต้องมีบันทึกการเคลื่อนย้าย พร้อมทั้งได้รับอนุมัติก่อนการเคลื่อนย้าย

๒) ต้องจัดให้มีการดำเนินการ Backup ข้อมูลก่อนถอดถอน และล้างข้อมูล (Data Sanitization) ในกรณีที่ต้องดำเนินการส่งคืน หรือจำหน่าย

๓) ดำเนินการปรับปรุงทะเบียนสินทรัพย์ให้เป็นปัจจุบัน

(F) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. จัดให้มีการกำหนดนโยบายการสร้างความตระหนัก โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สาม ที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(๑) มีกิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่ พนักงานใหม่ (New Employees) ผู้ใช้และระดับบริหาร (Users and Management) เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

(๒) เผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร.

(๓) ให้ความรู้ด้านกฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๔) การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ ผลกระทบและการบรรเทาผลกระทบ

(๕) กำหนดให้การสร้างความตระหนักเป็นกิจกรรมที่ดำเนินการต่อเนื่องเป็นประจำทุกปี

(๖) การสร้างความตระหนักต้องผนวกรวมเข้าเป็นส่วนหนึ่งของวัฒนธรรมองค์กรและกระบวนการบริหารจัดการความเสี่ยง

(๗) ดำเนินการทบทวนแผนงาน/กิจกรรมในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

๒. จัดให้มีแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือมาตรการในการพัฒนาศักยภาพบุคลากรของ ขร. ในด้านทักษะของบุคลากร โดยให้มีการส่งเสริมและสนับสนุนการเรียนรู้ และการพัฒนาบุคลากรอย่างต่อเนื่อง รวมถึงจัดให้มีโครงการพัฒนาศักยภาพผู้ปฏิบัติงานของ ขร. และหลักสูตร หรือโครงการสร้างความตระหนักรู้และการฝึกอบรม และแผนงานที่เกี่ยวข้อง โดยต้องดำเนินการจัดประเภทของผู้ปฏิบัติงาน โครงการ หลักสูตร และกำหนดแผนงานให้เหมาะสมกับผู้ปฏิบัติงานแต่ละประเภท เพื่อเป็นการยกระดับทักษะความรู้และความเชี่ยวชาญของบุคลากรของ ขร. ซึ่งประกอบไปด้วย

๑) ขอบเขตการพัฒนาผู้ปฏิบัติงาน ประกอบด้วย

(๑) ทักษะของบุคลากร (Skillsets) เพื่อกำหนดแนวทางการพัฒนาผู้ปฏิบัติงานของ ขร. หรือบุคลากรอื่นที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ให้มีทักษะที่จำเป็นเหมาะสมในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงต้องประเมินและวางแผนการพัฒนาอย่างต่อเนื่อง

(๒) สภาพแวดล้อมและระบบการทำงานที่ส่งเสริมและสนับสนุนการเรียนรู้และการพัฒนาบุคลากรอย่างต่อเนื่อง เพื่อส่งเสริมและเอื้อต่อการเรียนรู้และการพัฒนากรอบความคิดและกรอบทักษะสำหรับการทำงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

๒) การพัฒนาทักษะของบุคลากร โดยกำหนดแนวทางการสร้างความตระหนักรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งประกอบด้วยแนวทางการส่งเสริมการเรียนรู้ ดังนี้

(๑) การสร้างความตระหนักรู้ (Awareness)

(๒) การฝึกอบรม (Training)

(๓) การศึกษา (Education)

ซึ่งควรนำทั้ง ๓ แนวทางการส่งเสริมการเรียนรู้มากำหนดให้มีความต่อเนื่องในการดำเนินการพัฒนาทักษะของบุคลากร โดยเริ่มจากการสร้างความตระหนักรู้ สร้างการฝึกอบรม และพัฒนาไปสู่การศึกษา

๓) บุคคลที่เกี่ยวข้องกับการพัฒนาทักษะของผู้ปฏิบัติงานของ ขร. ประกอบด้วย

(๑) หัวหน้าหน่วยงาน

(๒) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

(๓) หัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ หรือผู้บริหารระดับสูงที่มีหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) ที่ได้รับการแต่งตั้งให้ดำเนินการเป็นหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์

(๔) หัวหน้าส่วนงาน

(๕) ผู้ใช้งาน ประกอบด้วย บุคคลภายใน ขร. และ บุคคลภายนอก ขร.

๔) ขั้นตอนการพัฒนาทักษะของผู้ปฏิบัติงานของ ขร. ซึ่งประกอบด้วย

(๑) ขั้นตอนที่ ๑ การออกแบบแผนงาน หรือโครงการสร้างความตจระหนักรู้และการฝึกอบรม

(๒) ขั้นตอนที่ ๒ การพัฒนาเอกสาร สื่อ เนื้อหาสำหรับแผนงาน หรือโครงการสร้างความตระหนักรู้ และการฝึกอบรม

(๓) ขั้นตอนที่ ๓ การดำเนินการแผนงาน หรือโครงการ

(๔) ขั้นตอนที่ ๔ หลังดำเนินการแผนงาน หรือโครงการ

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. จัดให้มีการกำหนดกิจกรรมส่งเสริมความตระหนัก โดยพิจารณาอย่างน้อย ดังนี้

๑) จัดอบรมและสัมมนาเชิงปฏิบัติการเกี่ยวกับภัยคุกคามไซเบอร์และวิธีการป้องกันอย่างน้อยปีละ ๑ ครั้ง

๒) จัดทำสื่อประชาสัมพันธ์ เช่น Infographic, Video Clip, E-Newsletter ที่เกี่ยวกับการรักษาความปลอดภัยของข้อมูล เป็นต้น

๓) จัดกิจกรรม Cybersecurity Awareness Campaign เช่น การจัดกิจกรรมรายสัปดาห์แห่งความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

๔) จัดทำหลักสูตร e-Learning และแบบทดสอบออนไลน์ เพื่อวัดระดับความเข้าใจของบุคลากร

๕) จัดให้มีกิจกรรมตอบคำถาม หรือแข่งขันด้านความรู้ความปลอดภัยไซเบอร์ เพื่อกระตุ้นการมีส่วนร่วม

๖) กำหนดให้มีการแจ้งเตือนภัยคุกคามใหม่ ๆ ผ่านช่องทางภายใน เช่น Intranet, Email Notification เป็นต้น

๒. จัดให้มีการกำหนดเนื้อหาหลักในการสร้างความตระหนัก โดยพิจารณาอย่างน้อย ดังนี้

๑) ความสำคัญของการรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล (CIA Triad)

๒) วิธีป้องกันภัยฟิชชิง (Phishing), มัลแวร์ (Malware), และการโจมตีทางไซเบอร์รูปแบบต่าง ๆ

๓) แนวทางการใช้รหัสผ่านอย่างปลอดภัยและการจัดการบัญชีผู้ใช้ (Password and Account Management)

๔) การรักษาความปลอดภัยของอุปกรณ์พกพา และการทำงานจากระยะไกล (Mobile and Remote Working Security)

๕) นโยบายการใช้งานอินเทอร์เน็ต อีเมล และอุปกรณ์เทคโนโลยีสารสนเทศภายในองค์กร

๖) กระบวนการรายงานเหตุการณ์ผิดปกติหรือเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Reporting)

๓. จัดให้มีการประเมินผลและปรับปรุง โดยพิจารณาอย่างน้อย ดังนี้

๑) ประเมินผลการสร้างความตระหนักผ่านการสอบหลังการอบรม การสัมภาษณ์ หรือแบบสอบถาม

๒) กำหนดให้มีการติดตามผลและวิเคราะห์พฤติกรรมการใช้งานระบบของบุคลากรอย่างต่อเนื่อง

๓) นำผลการประเมินไปปรับปรุงกิจกรรมและเนื้อหาให้เหมาะสมกับภัยคุกคามและบริบทขององค์กรที่เปลี่ยนแปลง

๔. กำหนดให้มีการบริหารจัดการควบคุมการส่งข้อความอิเล็กทรอนิกส์ โดยพิจารณาให้มีการควบคุมอย่างน้อย ดังนี้

๑) กำหนดให้มีการควบคุมและเข้ารหัสข้อมูลสำคัญหรือข้อมูลส่วนบุคคลที่ส่งผ่านข้อความอิเล็กทรอนิกส์ และ จำกัดสิทธิ์การแนบไฟล์ หรือส่งลิงก์ไปยังผู้ใช้งานภายนอก

๒) พิจารณาติดตั้งระบบ Email Security Gateway เพื่อคัดกรอง spam และ phishing

๓) กำหนดให้มีการควบคุมและจำกัดสิทธิ์การส่งข้อความอิเล็กทรอนิกส์ โดยการห้ามใช้ email ส่วนตัว ในการส่งข้อมูลขององค์กร เว้นแต่ได้รับอนุญาต

๔) กำหนดให้มีการบันทึกและตรวจสอบการรับ - ส่งข้อความอิเล็กทรอนิกส์ โดยพิจารณาอย่างน้อย ดังนี้

(๑) กำหนดให้มีการบันทึกกิจกรรมระบบ (Log) การรับ-ส่งข้อความอิเล็กทรอนิกส์ เช่น ผู้ส่ง, ผู้รับ, เวลา, ขนาดไฟล์แนบ เป็นต้น และจัดเก็บไว้อย่างน้อย ๙๐ วัน

(๒) กำหนดให้มีการตรวจสอบพฤติกรรมผิดปกติ เช่น ส่งข้อมูลจำนวนมากผิดเวลา, แนบไฟล์น่าสงสัย เป็นต้น

๕) กำหนดให้มีการอบรมผู้ใช้งานข้อความอิเล็กทรอนิกส์ โดยให้ความรู้เกี่ยวกับความเสี่ยงจากการใช้ข้อความอิเล็กทรอนิกส์ เช่น Social Engineering, Business Email Compromise (BEC) เป็นต้น พร้อมทั้งกำหนดช่องทางแจ้งเตือนหรือรายงานอีเมลต้องสงสัย

(G) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้มีการสร้าง การทบทวน หรือปรับปรุงมาตรการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และขีดความสามารถในการจัดเก็บข้อมูลจราจร (Implementing a Cybersecurity Monitoring and Logging Capability) โดยพิจารณากำหนดกระบวนการ ๗ ขั้นตอน ดังนี้

๑) กำหนดให้มีการพัฒนาแผนการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร (Develop a Cybersecurity Monitoring and Logging) โดยพิจารณาสำรวจสมรรถนะในการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และความต้องการในการเก็บข้อมูลจราจรของ ขร. รวมถึงส่วนประกอบอื่นที่เกี่ยวข้อง เช่น งบประมาณ ทรัพยากร และวิธีดำเนินการเก็บข้อมูลจราจรที่ต้องการหรือคาดหวังและนำขออนุมัติจากผู้บริหารระดับสูง หรือคณะกรรมการที่ได้รับมอบหมาย ทั้งนี้ การพิจารณาแนวทางที่ดีสำหรับการวางแผนการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร สามารถพิจารณาออกเป็น ๔ ประเภทหลัก ดังนี้

(๑) วัตถุประสงค์ที่ชัดเจน (Clear Purpose) เช่น ตั้งเป้าหมายที่ชัดเจน ระบุประโยชน์ของการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร สำรวจบริบทของ ขร. เพื่อกำหนดวัตถุประสงค์ ของ ขร.

(๒) การดำเนินการตามกระบวนการที่ขับเคลื่อนด้วยความเสี่ยง (Risk-driven, Process-based Approach) เช่น ใช้แนวทางการประเมินความเสี่ยงในการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร สามารถเชื่อมโยงข้อมูลข่าวกรองความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นจริงกับการประเมินความเสี่ยง เป็นต้น

(๓) ให้ความสำคัญกับการวิเคราะห์ภัยคุกคามมากขึ้น (More Focused Threat Analysis) เช่น นำเครื่องมือในการจัดการกับข้อมูลจราจรมาใช้อย่างเหมาะสมกับภัยคุกคามและความเสี่ยงของ ขร. ศึกษาพฤษติกรรมปกติ และผิดปกติของระบบหรือเครือข่าย • กำหนดกระบวนการที่สามารถเข้าถึงข้อมูลแหล่งที่มาของภัยคุกคามได้ทันเวลา บูรณาการและใช้งานข้อมูล ข่าว และข่าวกรองภัยคุกคามได้

(๔) การจัดสรรทรัพยากรที่ดีขึ้น (Better Resourcing) เช่น ลงทุนในการสร้างทักษะให้แก่บุคลากร ดำเนินการจัดสรรเวลาหรือทรัพยากรอย่างต่อเนื่อง และสร้างความร่วมมือกับผู้ให้บริการด้านการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และบริการเก็บข้อมูลจราจรข้อมูล

๒) กำหนดข้อกำหนดเบื้องต้น สำหรับการเฝ้าระวังและการเก็บข้อมูลจราจรความมั่นคงปลอดภัยไซเบอร์ (Carry out Prerequisites for Cybersecurity Monitoring and Logging) และดำเนินการตาม ซึ่งข้อกำหนด ควรพิจารณาประกอบด้วย

- วัตถุประสงค์และขอบเขตและสินทรัพย์ที่ต้องตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Agreeing Objectives and Scope) การเฝ้าระวังและการเก็บข้อมูลจราจรความมั่นคงปลอดภัยไซเบอร์ เช่น เช่น บริการที่สำคัญ หรือระบบงานที่สำคัญ ระบบเครือข่าย (Network Infrastructure) เป็นต้น
- กำหนดทรัพย์สินหลักหรือทรัพย์สินที่สำคัญ และการกำหนดตำแหน่งที่อยู่ของทรัพย์สินนั้น
- ระบุจุดเชื่อมต่อไปยังภายนอก เช่น อินเทอร์เน็ต
- พิจารณาลักษณะการโจมตีการรักษาความมั่นคงปลอดภัยไซเบอร์ในทรัพย์สินที่สำคัญ

- พิจารณาหามาตรการเพื่อลดเส้นทางการโจมตีไปยังทรัพย์สิน และกำหนดมาตรการควบคุมทางเทคนิคที่สำคัญและลดขอบเขตการโจมตี
- ทบทวนและปรับปรุงมาตรการควบคุมความมั่นคงปลอดภัยทางไซเบอร์ (Reviewing and Revising Cybersecurity Controls) และอื่น ๆ ให้เหมาะสมกับเป้าหมายของ ขร.

๓) ระบุแหล่งที่มาของสัญญาณเตือนเหตุภัยคุกคามทางไซเบอร์ (Signs of Cybersecurity Incidents) รวมถึงการกำหนดให้มีการแยก “สัญญาณเตือน” (Signal) ที่แท้จริงออกจาก “สัญญาณรบกวน” (Noise) แหล่งข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการวิเคราะห์ตัวบ่งชี้ถึงการบุกรุก (IOC) เช่น

- พิจารณาใช้บริการโดยผู้ให้บริการภายนอกที่ให้บริการซอฟต์แวร์รักษาความมั่นคงปลอดภัย เช่น IDS, IPS, DLP, SIEM, ซอฟต์แวร์ป้องกันไวรัส และ สแปม, ซอฟต์แวร์ตรวจสอบความสมบูรณ์ของไฟล์และบริการเฝ้าระวัง (Monitoring Services)
- พิจารณาใช้เครื่องมือที่สามารถแยกมัลแวร์และเทคนิคการสืบสวนสอบสวน (Malware Isolation and Investigation Techniques) เช่น การทำแซนด์บ็อกซ์ (Sandboxing) หรือเอ็นจิ้นการดำเนินการเสมือน (Virtual Execution Engines)
- พิจารณาให้มีข้อมูลบันทึกการใช้งาน เช่น ข้อมูลการจราจรระบบปฏิบัติการ บันทึกบริการและแอปพลิเคชัน บันทึกอุปกรณ์เครือข่าย และการไหลของข้อมูลในเครือข่าย
- พิจารณาแยกข้อมูลที่เปิดเผยต่อสาธารณะ เช่น ข้อมูลเกี่ยวกับการแสวงหาประโยชน์ใหม่ ๆ (Information on New Exploits) ที่ต้องเปิดเผยต่อบุคคลหรือหน่วยงานที่สาม

๔) ดำเนินการออกแบบความสามารถในการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร (Design Your Cybersecurity Monitoring and Logging Capability) เมื่อข้อกำหนดต่าง ๆ เสร็จสมบูรณ์ และได้ระบุแหล่งที่มาของสัญญาณเตือนเหตุภัยคุกคามทางไซเบอร์ (Signs of Cybersecurity Incidents) แล้วเสร็จ โดยดำเนินการพิจารณาออกแบบการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์โดยรวมและความสามารถในการเก็บข้อมูลจราจร โดยพิจารณาด้านต่าง ๆ ดังนี้

- บุคคลการ (People) ที่ต้องรับผิดชอบในการวิเคราะห์ข้อมูล ซึ่งต้องมีทักษะโดยเฉพาะ
- กระบวนการ (Process) เช่น กำหนดกระบวนการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์และกระบวนการตอบสนองต่อเหตุการณ์ กระบวนการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ ซึ่งประกอบด้วย ๔ ขั้นตอนหลัก เช่น ๑. รวบรวมข้อมูลเหตุการณ์ที่เกี่ยวข้อง ๒. หลอมรวมข้อมูลเข้าด้วยกัน ๓. พิจารณาวิเคราะห์เหตุการณ์ที่ผิดปกติ ๔. ดำเนินการจัดการเหตุการณ์ที่ผิดปกติ
- เทคโนโลยี (Technology) โดยพิจารณาใช้เครื่องมือ SIEM และเครื่องมือในการจัดการเก็บข้อมูลจราจรและการวิเคราะห์เหตุการณ์ที่หลากหลายร่วมกัน
- ข้อมูล (Information) โดยพิจารณาข่าวกรองความมั่นคงปลอดภัยไซเบอร์ที่เชื่อถือได้ (Reliable) และเป็นปัจจุบัน

๕) พิจารณาสร้างหรือซื้อบริการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร (Build or Buy Cybersecurity Monitoring and Logging Services) โดยพิจารณาวิธีการใช้งานอย่างมีประสิทธิภาพ และมีค่าใช้จ่ายที่สมเหตุสมผลกับ ขร. ซึ่งควรมีการพิจารณา ดังนี้

- การดำเนินการโดยภายในหน่วยงาน (In-sourced Service)
- การใช้ระบบคลาวด์และอุปกรณ์ หรือซอฟต์แวร์ในฐานะผู้ให้บริการ (Cloud & Appliance Based/ Software as a Service Provider)
- การใช้บริการจากผู้ให้บริการเครือข่าย หรือผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือผู้ให้บริการจัดการการรักษาความมั่นคงปลอดภัย (Managed Security Services Provider: MSSP)
- การใช้โมเดลแบบผสม (Hybrid Model)

ทั้งนี้ ในกรณีที่เลือกใช้บริการจากผู้ให้บริการภายนอก ควรมีการพิจารณาข้อกำหนด ดังนี้

(๑) เข้าใจถึงประโยบขน์ของการใช้บริการผู้ให้บริการภายนอก

(๒) พิจารณาว่าควรจ้างกิจกรรมใดบ้างจากผู้ให้บริการภายนอก

(๓) กำหนดเกณฑ์การคัดเลือกผู้ให้บริการภายนอก

(๔) แต่งตั้ง และกำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกที่ได้รับการคัดเลือก

๖) บูรณาการความสามารถในการเฝ้าระวังและการเก็บข้อมูลจราจรเข้ากับกรอบความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Integrate the Capability into Your Cybersecurity Framework) โดยนำระบบต่างๆที่เกี่ยวข้องมาร่วมกันจัดเก็บข้อมูล และวิเคราะห์ข้อมูล เช่น ระบบที่จัดเก็บข้อมูลจราจร และระบบ SIEM เพื่อจัดเก็บ และวิเคระห์ข้อมูลจราจร

๗) ดำเนินการรักษาระดับความสามารถในการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร (Maintain the Cybersecurity Monitoring and Logging Capability) อย่างต่อเนื่อง โดยดำเนินการรักษาความสามารถในการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจรของ ขร. และติดตาม รวมถึงพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง รวมถึงกำหนดให้มีการศึกษาแนวโน้มเทคโนโลยีหรือการดำเนินการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ และการเก็บข้อมูลจราจรที่จะเกิดในอนาคตตามความต้องการตามเป้าหมายของ ขร. ซึ่งการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร ควรพิจารณาให้ความสำคัญ ๓ ส่วนหลัก ดังนี้

(๑) การบริหารจัดการข้อมูลจราจร (Log Management)

(๒) การตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident Response)

(๓) การบริหารจัดการข่าวกรองความมั่นคง ปลอดภัยไซเบอร์และการรับรู้สถานการณ์ (Cybersecurity Intelligence and Situational Awareness)

๒. กำหนดให้มีกลไกและกระบวนการเพื่อตรวจจับ จัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ พร้อมทั้งจัดให้มีการวิเคราะห์ภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. โดยพิจารณาดำเนินการ ดังนี้

๑) จัดหาเทคโนโลยีสำหรับการรวบรวมข้อมูล (Technologies for Data Gathering) โดยใช้เครื่องมือที่มีความสามารถในการสังเกต ตรวจจับ ป้องกัน หรือบันทึกภัยคุกคามทางไซเบอร์และช่องโหว่ที่รู้จักและหรือแก้ไขหรือจัดการด้านต่าง ๆ ของการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่นำมาใช้ เพื่อจัดการกับภัย

คุกคามและช่องโหว่ และพิจารณาจากวัตถุประสงค์ในการเฝ้าติดตามและความสามารถของสถาปัตยกรรมของ ขร. และมาตรการการเฝ้าติดตามอย่างต่อเนื่อง ดังนี้

- การจัดการช่องโหว่ (Vulnerability Management)
- การจัดการแพตช์ (Patch Management)
- การจัดการเหตุการณ์ (Event Management)
- การจัดการเหตุภัยคุกคามทางไซเบอร์ (Incident Management) • การตรวจจับมัลแวร์ (Malware Detection)
- การจัดการทรัพย์สิน (Asset Management)
- การจัดการกำหนดค่า (Configuration Management)
- การจัดการเครือข่าย (Network Management)
- การจัดการไลเซนส์ (License Management)
- การจัดการสารสนเทศ (Information Management)
- การรับประกันซอฟต์แวร์ (Software Assurance)

๒) พิจารณาเทคโนโลยีสำหรับการรวบรวมและการวิเคราะห์ (Technologies for Aggregation and Analysis) โดยนำเทคโนโลยีที่มีความสามารถในการรวบรวมข้อมูลดิบที่ได้จากการควบคุมความมั่นคงปลอดภัยอย่างน้อยหนึ่งรายการหรือจากเทคโนโลยีการรวบรวมข้อมูลโดยตรงอื่น ๆ มาทำการเชื่อมโยง วิเคราะห์ และแสดงข้อมูลดิบในลักษณะที่ให้มุมมองที่มีความหมายมากขึ้นเกี่ยวกับประสิทธิภาพของการรักษาความมั่นคงปลอดภัย เช่น การจัดการเหตุการณ์และสารสนเทศความมั่นคงปลอดภัย (Security Information and Event Management: SIEM) รวมถึงจัดให้มีแดชบอร์ดการจัดการความมั่นคงปลอดภัย หรือข้อมูลสรุปการควบคุมการจัดการสารสนเทศความมั่นคงปลอดภัย โดยรวบรวมและสื่อสารข้อมูลที่เกี่ยวข้องกับสถานะความมั่นคงปลอดภัยของหน่วยงานแบบเรียลไทม์ และรายงานไปยังผู้เกี่ยวข้องในการจัดการความมั่นคงปลอดภัย เช่น ผู้ดูแลระบบทางเทคนิค CISO ผู้บริหารความเสี่ยง เป็นต้น และแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในกฎหมาย ข้อบังคับ และนโยบาย ในกรณีที่ไม่มีวิธีการทำงานที่เป็นมาตรฐานและเป็นไปโดยอัตโนมัติ

ทั้งนี้ ควรพิจารณาใช้เครื่องมือที่สามารถทำงานโดยอัตโนมัติ เพื่อให้สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

- สแกนหาช่องโหว่และใช้แพตช์ที่เหมาะสมโดยอัตโนมัติ
- เปิดใช้งานการกำหนดค่าความมั่นคงปลอดภัยโดยอัตโนมัติตามรายการตรวจสอบการตั้งค่าความมั่นคงปลอดภัย (Checklist of Security Settings)
- สแกนหาความสอดคล้องกับรายการตรวจสอบการตั้งค่าความมั่นคงปลอดภัยที่กำหนดไว้ล่วงหน้า
- รวบรวมตัวชี้วัดความมั่นคงปลอดภัยจากเครื่องมือและรายงานไปยังแผงควบคุมสำหรับการจัดการ (Management Console) ในรูปแบบมาตรฐาน

๓) จัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ เมื่อได้รับการแจ้งเตือนการเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์จากกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยวิเคราะห์ และคัดแยกเหตุภัยคุกคามทางไซเบอร์ (Incident Triage) กำหนดประเภทและขอบเขตของเหตุการณ์กับความสัมพันธ์กับเหตุการณ์อื่น ๆ และเรียงลำดับเหตุการณ์ เพื่อดำเนินการแก้ไขตามลำดับความร้ายแรงของผลกระทบ ซึ่งควรพิจารณากำหนดกระบวนการคัดแยกเหตุการณ์ (Triage Process) อย่างชัดเจน ซึ่งควรประกอบด้วยกระบวนการหลัก ดังนี้

(๑) ดำเนินการระบุเหตุการณ์ (Event Identification) โดยทีมรักษาความมั่นคงปลอดภัยที่ได้รับมอบหมายดำเนินการระบุเหตุการณ์ที่มีการแจ้งเตือนเหตุการณ์

(๒) ดำเนินการประเมินเบื้องต้น (Initial Assessment) เพื่อพิจารณาการแจ้งเตือนเป็นเท็จ (False Positive) หรือเป็นภัยคุกคามทางไซเบอร์ที่แท้จริง ทั้งที่จะเกิดขึ้น ในอนาคต หรือกำลังเกิดขึ้นในขณะนี้ โดยการตรวจสอบข้อมูลจราจร ตรวจสอบการรับส่งข้อมูลเครือข่าย หรือดำเนินการประเมินช่องโหว่ เป็นต้น

(๓) ดำเนินการจัดประเภท (Classification) โดยจำแนกประเภทของเหตุการณ์ และวิเคราะห์เหตุภัยคุกคามทางไซเบอร์นั้นเป็นภัยคุกคามอย่างไร ตามที่กำหนดในประกาศความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

(๔) ดำเนินการจัดลำดับความสำคัญ (Prioritization) โดยอิงกับผลการประเมินเบื้องต้นและผลการจัดประเภท เพื่อทราบถึงความเร่งด่วน และวางแผนการดำเนินการ

(๕) ดำเนินการระงับ (Containment) เพื่อจำกัดขอบเขต และระงับภัยคุกคามทางไซเบอร์

(๖) ดำเนินการทางนิติเวชและการสืบสวน (Forensics and Investigation) โดยละเอียดเพื่อหาหลักฐาน ระบุที่มาของการจู่โจม ประเมินข้อมูลที่ได้รับผลกระทบ และการสูญเสียข้อมูลที่อาจเกิดขึ้น

(๗) ดำเนินการสื่อสาร (Communication) กับบุคลากรที่ได้รับผลกระทบ เช่น เจ้าหน้าที่เทคโนโลยีสารสนเทศ ฝ่ายบริหาร เพื่อแจ้งให้ทราบเกี่ยวกับเหตุการณ์ และให้คำแนะนำในการรักษาความมั่นคงปลอดภัย

(๘) ดำเนินการแก้ไข (Resolution) ตามมาตการเพื่อแก้ไขปัญหาที่อาจเกิดขึ้นอีก

(๙) จัดทำเอกสารประกอบ (Documentation) และเก็บรักษาเอกสารอย่างละเอียดตลอดกระบวนการตอบสนองต่อเหตุการณ์ รวมถึงการดำเนินการและการสำรวจ

(๑๐) ดำเนินการทบทวนและนำมาเป็นบทเรียน (Review and Lessons Learned) เพื่อนำมาประเมินปัญหา และอุปสรรคที่เกิดขึ้น พร้อมทั้งปรับปรุงแก้ไข

ตัวอย่างของการดำเนินการตามกระบวนการคัดแยกระหว่างเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัย ไซเบอร์และเหตุภัยคุกคามทางไซเบอร์ (Security Event and an Incident)

เหตุการณ์ที่ ๑ ตัวอย่างเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๑.๑ คำอธิบายเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์กิจกรรมที่ผิดปกติบนเครื่องแม่ข่าย (Unusual Activity on a Server)

- ระบบตรวจสอบความมั่นคงปลอดภัยของหน่วยงานจะสร้างการแจ้งเตือนเกี่ยวกับกิจกรรมที่ ผิดปกติบนเครื่องแม่ข่ายให้บริการเว็บไซต์ของบริษัทหนึ่ง
- การแจ้งเตือนบ่งชี้ว่ามีการรับส่งข้อมูลเครือข่ายเพิ่มขึ้นอย่างมากและการพยายามเข้าสู่ระบบ ล้มเหลวหลายครั้งภายในกรอบเวลาอันสั้น
- ไม่พบหลักฐานโดยตรงของการเข้าถึงโดยไม่ได้รับอนุญาตหรือการละเมิดข้อมูล

๑.๒ ตัวอย่างกระบวนการคัดแยก (Triage Process)

๑. การระบุเหตุการณ์ (Event Identification) ทีมรักษาความมั่นคงปลอดภัยจะระบุเหตุการณ์ เมื่อระบบตรวจสอบสร้างการแจ้งเตือน

๒. การประเมินเบื้องต้น (Initial Assessment) ทีมรักษาความมั่นคงปลอดภัยจะเริ่มการประเมินเหตุการณ์เบื้องต้น และตรวจสอบการแจ้งเตือนและรวบรวมข้อมูลเกี่ยวกับเครื่องแม่ข่ายลักษณะของกิจกรรม และตัวบ่งชี้ที่เป็นไปได้ของการโจมตี

๓. การจัดประเภท (Classification) จากการประเมินเบื้องต้นทีมปฏิบัติงานจัดประเภทเหตุการณ์นี้เป็นเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แทนที่จะเป็นเหตุภัยคุกคามทางไซเบอร์ เนื่องจากยังไม่มีหลักฐานที่เป็นรูปธรรมของการละเมิดความมั่นคงปลอดภัย จึงถือเป็นงานรักษาความมั่นคงปลอดภัยเนื่องจากมีกิจกรรมที่ผิดปกติ

๔. การจัดลำดับความสำคัญ (Prioritization) เหตุการณ์นี้จัดอยู่ในลำดับความสำคัญต่ำถึงปานกลาง เนื่องจากไม่มีข้อบ่งชี้ถึงการละเมิดในทันทีมีการติดตามอย่างใกล้ชิดแต่ไม่ต้องการการตอบสนองอย่างเร่งด่วน

๕. เอกสารประกอบ (Documentation) รายละเอียดของเหตุการณ์ รวมถึงการแจ้งเตือน การประเมินเบื้องต้น และการจัดหมวดหมู่ ได้รับการบันทึกไว้เพื่อใช้อ้างอิงและการวิเคราะห์ในอนาคต

เหตุการณ์ที่ ๒ ตัวอย่างเหตุภัยคุกคามทางไซเบอร์ (Incident)

๒.๑ คำอธิบายเหตุภัยคุกคามทางไซเบอร์การละเมิดข้อมูล (Data Breach)

- หลายวันต่อมา ทีมรักษาความมั่นคงปลอดภัยตรวจพบการถ่ายโอนข้อมูลที่น่าสงสัยจากเครื่องแม่ข่ายที่ถูกบุกรุกไปยังที่อยู่ IP ภายนอก
- การตรวจสอบเพิ่มเติมเผยให้เห็นการเข้าถึงข้อมูลลูกค้าที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต
- มีการยืนยันการมีอยู่ของมัลแวร์บนเครื่องแม่ข่ายที่ถูกบุกรุก

๒.๒ กระบวนการคัดแยก

๑. การระบุเหตุภัยคุกคามทางไซเบอร์ (Incident Identification) ทีมรักษาความมั่นคงปลอดภัย จะระบุเหตุการณ์เมื่อยืนยันการเข้าถึงโดยไม่ได้รับอนุญาตและการขโมยข้อมูล

๒. การประเมินเบื้องต้น (Initial Assessment) การประเมินอย่างละเอียดจะดำเนินการเพื่อทำ ความเข้าใจขอบเขตและผลกระทบของเหตุการณ์ รวบรวมหลักฐาน และระบุว่าการละเมิดเกิดขึ้นได้อย่างไร

๓. การจำแนกประเภท (Classification) ขณะนี้เหตุการณ์นี้ถูกจัดว่าเป็นเหตุภัยคุกคามทางไซเบอร์ (Incident) เนื่องจากการเข้าถึงที่ไม่ได้รับอนุญาตและการละเมิดข้อมูลได้รับการยืนยัน

๔. การจัดลำดับความสำคัญ (Prioritization) เหตุการณ์นี้จัดอยู่ในประเภทวิกฤติ โดยต้องมีการ ดำเนินการทันทีเพื่อหยุดการละเมิด แยกระบบที่ได้รับผลกระทบ และเริ่มการสืบสวนสอบสวนโดยละเอียด

๕. การระงับ (Containment) ทีมรักษาความมั่นคงปลอดภัยจะดำเนินการทันทีเพื่อควบคุม เหตุการณ์ เช่น การแยกเครื่องแม่ข่ายที่ถูกบุกรุกออกจากเครือข่าย และการปิดกั้นการขโมยข้อมูลเพิ่มเติม

๖. นิติเวชและการสืบสวน (Forensics and Investigation) มีการดำเนินการสืบสวนสอบสวน โดยละเอียดเพื่อระบุสาเหตุที่แท้จริง วิเคราะห์มัลแวร์ และกำหนดขอบเขตของการละเมิดข้อมูล

๗. การสื่อสาร (Communication) ผู้มีส่วนได้ส่วนเสีย รวมถึงผู้บริหารระดับสูง ทีมกฎหมาย และลูกค้าที่ได้รับผลกระทบ จะได้รับแจ้งเกี่ยวกับเหตุการณ์ดังกล่าวตามแผนการตอบสนองต่อเหตุการณ์ ของหน่วยงาน

๘. การแก้ไข (Resolution) ทีมรักษาความมั่นคงปลอดภัยทำงานเพื่อแก้ไขปัญหา ลบมัลแวร์ แก้ไขช่องโหว่ และใช้มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์เพิ่มเติมเพื่อป้องกันการละเมิดในอนาคต

๙. เอกสารประกอบ (Documentation) มีการเก็บรักษาเอกสารโดยละเอียดตลอดกระบวนการ ตอบสนองต่อเหตุการณ์ รวมถึงการดำเนินการ การสำรวจ และบทเรียนที่ได้รับ

๑๐. การทบทวนและบทเรียนที่ได้รับ (Review and Lessons Learned) หลังจากแก้ไขเหตุการณ์แล้ว การทบทวนหลังเหตุการณ์จะดำเนินการเพื่อประเมินการตอบสนองของหน่วยงาน ระบุพื้นที่สำหรับการปรับปรุง และปรับปรุงขั้นตอนการตอบสนองต่อเหตุการณ์ให้สอดคล้องกัน ตัวอย่างนี้แสดงให้เห็นถึงความแตกต่างระหว่างเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และเหตุภัยคุกคามทางไซเบอร์ และวิธีที่กระบวนการคัดแยกแตกต่างกันตามลักษณะของสถานการณ์ รวมถึงความเป็นไปได้ที่เหตุการณ์อาจหรือไม่อาจบานปลายไปสู่เหตุการณ์ต่าง ๆ ในกรณีที่เหตุการณ์ได้รับการ ยืนยันว่ามีการละเมิดความมั่นคงปลอดภัยไซเบอร์ หน่วยงานต้องใช้ความพยายามตอบสนองในทันที

เหตุการณ์ที่ ๓ การจราจรขาออกที่ผิดปกติพุ่งสูงขึ้น

๓.๑ คำอธิบายเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

- บันทึกไฟร์วอลล์ของหน่วยงานแสดงให้เห็นว่าการรับส่งข้อมูลขาออกจากเวิร์กสเตชันแห่งใด แห่งหนึ่งพุ่งสูงขึ้นอย่างกะทันหัน
- จากการสืบสวนสอบสวน พบว่าพนักงานกำลังดาวน์โหลดการอัพเดทซอฟต์แวร์ขนาดใหญ่ ส่งผลให้มีการรับส่งข้อมูลเพิ่มขึ้น

๓.๒ กระบวนการคัดแยก

๑. การระบุเหตุการณ์ ทีมรักษาความมั่นคงปลอดภัยจะระบุเหตุการณ์เมื่อสังเกตเห็นปริมาณการ รับส่งข้อมูลที่เพิ่มขึ้นอย่างรวดเร็วในบันทึกไฟร์วอลล์

๒. การประเมินเบื้องต้น การประเมินเบื้องต้นจะดำเนินการเพื่อทำความเข้าใจสาเหตุ ของการจราจรที่เพิ่มขึ้นอย่างรวดเร็ว จากการตรวจสอบพบว่าไม่เป็นอันตรายและเกี่ยวข้องกับการอัพเดทซอฟต์แวร์ที่ถูกต้องตามกฎหมาย

๓. การจัดประเภท เหตุการณ์ดังกล่าวจัดเป็นเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ แต่ไม่ใช่เหตุภัยคุกคามทางไซเบอร์ เนื่องจากไม่มีข้อบ่งชี้ถึงการเข้าถึงโดยไม่ได้รับอนุญาตหรือกิจกรรมที่เป็นอันตราย

๔. การจัดลำดับความสำคัญ เนื่องจากไม่ใช่เหตุภัยคุกคามทางไซเบอร์ จึงได้รับมอบหมายลำดับ ความสำคัญต่ำและไม่ต้องการการตอบสนองอย่างเร่งด่วน

๕. เอกสารประกอบ รายละเอียดของเหตุการณ์ รวมถึงผลการสืบสวนสอบสวน ได้รับการบันทึก ไว้เพื่อใช้อ้างอิง

เหตุการณ์ที่ ๔ การโจมตีแบบฟิชชิ่ง

๔.๑ คำอธิบายเหตุภัยคุกคามทางไซเบอร์

- พนักงานหลายคนรายงานว่าได้รับอีเมลที่น่าสงสัยพร้อมไฟล์แนบ
- การสืบสวนสอบสวนพบว่าอีเมลเหล่านี้ เป็นส่วนหนึ่งของแคมเปญฟิชชิ่งที่พยายามขโมยข้อมูล รับรองการเข้าสู่ระบบ

๔.๒ กระบวนการคัดแยก

๑. การระบุเหตุการณ์ ทีมรักษาความมั่นคงปลอดภัยจะระบุเหตุการณ์เมื่อพนักงานหลายคนรายงานอีเมลที่น่าสงสัย

๒. การประเมินเบื้องต้น การประเมินเบื้องต้นจะดำเนินการเพื่อประเมินอีเมล ระบุเจตนาร้าย และประเมินผลกระทบที่อาจเกิดขึ้น

๓. การจัดประเภท เหตุการณ์นี้จัดเป็นเหตุภัยคุกคามทางไซเบอร์ (Incident) เนื่องจากเกี่ยวข้อง กับการโจมตีแบบฟิชชิ่งที่ได้รับการยืนยันแล้วซึ่งอาจมีผลกระทบด้านความมั่นคงปลอดภัยไซเบอร์

๔. การจัดลำดับความสำคัญ เหตุการณ์นี้จัดอยู่ในลำดับความสำคัญปานกลาง แม้ว่าจะไม่เร่งด่วน เท่ากับเหตุการณ์ร้ายแรง แต่ก็จำเป็นต้องดำเนินการทันทีเพื่อลดภัยคุกคามทางไซเบอร์

๕. การระงับ ผู้ใช้ที่ได้รับผลกระทบจะได้รับคำสั่งไม่ให้เปิดไฟล์แนบที่น่าสงสัย และตัวกรองอีเมล จะได้รับการอัพเดทเพื่อปิดกั้นอีเมลฟิชชิ่งที่คล้ายกัน

๖. นิติเวชและการสืบสวนสอบสวน มีการดำเนินการสืบสวนสอบสวนโดยละเอียดเพื่อระบุแหล่งที่มาของอีเมลฟิชชิ่ง ประเมินว่าข้อมูลประจำตัวใด ๆ ถูกบุกรุกหรือไม่ และระบุการสูญเสียข้อมูลที่อาจเกิดขึ้น

๗. การสื่อสาร ทีมตอบสนองต่อเหตุการณ์จะสื่อสารกับพนักงานที่ได้รับผลกระทบ เจ้าหน้าที่ เทคโนโลยีสารสนเทศ และฝ่ายบริหารเพื่อแจ้งให้ทราบเกี่ยวกับเหตุการณ์ดังกล่าวและให้คำแนะนำในการ รักษาความมั่นคงปลอดภัยไซเบอร์

๘. การแก้ไข มีการใช้มาตรการเพื่อลบเนื้อหาที่เป็นอันตราย อัพเดทการกำหนดค่าความมั่นคง ปลอดภัยของอีเมล และให้ความรู้แก่พนักงานเกี่ยวกับภัยคุกคามทางไซเบอร์กรณีฟิชชิ่ง

๙. เอกสารประกอบ มีการเก็บรักษาเอกสารอย่างละเอียดตลอดกระบวนการตอบสนองต่อเหตุการณ์ รวมถึงการดำเนินการและการสำรวจ

๑๐. การทบทวนและบทเรียนที่ได้รับ หลังจากแก้ไขเหตุการณ์แล้ว จะมีการดำเนินการทบทวน หลังเหตุการณ์เพื่อประเมินการตอบสนองของหน่วยงาน ระบุพื้นที่สำหรับการปรับปรุง และปรับปรุงมาตรการ ต่อต้านการฟิชชิ่ง ตัวอย่างเหล่านี้แสดงให้เห็นถึงความแตกต่างระหว่างเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ไซเบอร์และเหตุภัยคุกคามทางไซเบอร์ โดยอิงตามลักษณะของกิจกรรมที่สังเกตได้ วิธีที่กระบวนการคัดแยก จะแตกต่างกันไป หน่วยงานต้องสอบสวนเหตุการณ์ แม้ว่าเหตุการณ์อาจไม่เกี่ยวข้องกับการโจมตีทางไซเบอร์ ในกรณีที่ได้รับการยืนยันว่าเป็นเหตุภัยคุกคามทางไซเบอร์หรือกิจกรรมที่เป็นอันตรายหน่วยงานต้อง ตอบสนองอย่างเร่งด่วน

๔) ดำเนินการระบุถึงเหตุภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ โดยดำเนินการวิเคราะห์ข้อมูล ดังนี้

- จำนวนผู้ได้รับผลกระทบ
- ผลกระทบที่เกิดขึ้น
- ระยะเวลาที่คาดว่าจะใช้ดำเนินการแก้ไขเหตุภัยคุกคามทางไซเบอร์
- บริการที่ได้รับผลกระทบเป็นบริการที่สำคัญหรือไม่ หากใช่ให้พิจารณาว่าเป็นเหตุการณ์ที่ต้องแจ้งไปยังหน่วยงานกำกับดูแล และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหรือไม่

๕) ดำเนินการทบทวนกลไกและกระบวนการตรวจจับเหตุภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อปรับเปลี่ยนกฎ (Rules) ของระบบที่มีการทำงานอิงตามกฎ (Rule-based) ให้มีความเหมาะสม และตรงกับนโยบายความมั่นคงปลอดภัยของ ขร. หรือในกรณีที่การทำงานของระบบอิงกับพฤติกรรมของการจู่โจม (Behavior-based) อาจปรับเปลี่ยนค่า Baseline เพื่อให้มีความเหมาะสมกับพฤติกรรมการใช้งานที่แท้จริง รวมถึงการปรับปรุงความถี่ในการตรวจสอบ ปรับปรุงรายการการตรวจสอบ (Checklist) ในการวิเคราะห์ และปรับกระบวนการต่าง ๆ เป็นต้น

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการเก็บบันทึกและวิเคราะห์เหตุการณ์ (Log Management and Analysis) โดยจัดเก็บ Log จากระบบต่าง ๆ เช่น firewall, IDS/IPS, endpoint, server และกำหนดให้มีการจัดเก็บ log อย่างน้อย ๙๐ วัน หรือพิจารณาระยะเวลาจัดเก็บตามระดับความเสี่ยงของบริการที่สำคัญ หรือระบบงานที่สำคัญ

๒. พิจารณาใช้เครื่องมือ SIEM (Security Information and Event Management) เพื่อวิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์

๓. กำหนดให้มีการประเมินความเสี่ยงจากภัยคุกคามใหม่ที่เกิดขึ้นอย่างสม่ำเสมอ รวมถึงทบทวนรายการภัยคุกคามและแนวโน้มใหม่ที่เกิดขึ้นอย่างน้อยทุกไตรมาส

๔. จัดให้มีการอบรมให้กับผู้ปฏิบัติงานที่เกี่ยวข้อง โดยมีเนื้อหาที่เกี่ยวข้องกับภัยคุกคามใหม่ๆ

๕. กำหนดให้มีการบริหารจัดการข้อมูลจราจรคอมพิวเตอร์ (Log) โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) จัดให้มีการกำหนดประเภทของข้อมูลจราจรที่ต้องจัดเก็บ ประกอบด้วยข้อมูลอย่างน้อย ดังนี้

(๑) ข้อมูลการพิสูจน์ตัวตน (Authentication Logs) เช่น การเข้าใช้งานระบบ (Login) และการออกจากระบบ (Logout) เป็นต้น

(๒) ข้อมูลการรับส่งข้อมูล (Access Logs, Traffic Logs) เช่น URL ที่เข้าใช้งาน ปริมาณการรับส่งข้อมูล เป็นต้น

(๓) ข้อมูลการเปลี่ยนแปลงระบบ (System Change Logs) เช่น การติดตั้ง/ถอนการติดตั้งโปรแกรม การแก้ไขสิทธิ์ผู้ใช้งาน เป็นต้น

(๔) ข้อมูลการใช้งานทรัพยากร (Resource Usage Logs) เช่น การใช้ CPU, Memory, Storage เป็นต้น

(๕) ข้อมูลเหตุการณ์ผิดปกติด้านความปลอดภัย (Security Event Logs) เช่น การถูกโจมตี การตรวจจับมัลแวร์ เป็นต้น

๒) จัดให้มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยพิจารณาอย่างน้อยดังนี้

(๑) กำหนดให้มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์อย่างน้อย ๙๐ วัน ตามกฎหมายกำหนด

(๒) ระบบที่มีข้อมูลสำคัญหรือระบบที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ให้พิจารณาเก็บ ไม่น้อยกว่า ๑๘๐ วัน ถึง ๑ ปี ตามระดับความเสี่ยง

(๓) ใช้ระบบกลางในการรวบรวมข้อมูล (เช่น Centralized Log Server, SIEM) เพื่อให้การจัดเก็บ วิเคราะห์ และสำรองข้อมูลเป็นไปอย่างมีประสิทธิภาพ

(๔) ข้อมูล Log ต้องมีการประทับเวลาที่ถูกต้อง (Time Synchronization) กับแหล่งเวลาอ้างอิงที่น่าเชื่อถือ (เช่น NTP Server)

๓) จัดให้มีแนวทางการรักษาความปลอดภัยของข้อมูลจราจรคอมพิวเตอร์ โดยพิจารณาอย่างน้อยดังนี้

(๑) จำกัดสิทธิ์การเข้าถึงข้อมูลจราจรเฉพาะผู้ที่มีหน้าที่รับผิดชอบ (Role-Based Access Control)

(๒) เข้ารหัสข้อมูลระหว่างการรับส่งและขณะจัดเก็บ (Encryption In Transit and At Rest)

(๓) กำหนดมาตรการป้องกันการแก้ไข ลบ หรือเข้าถึงข้อมูล Log โดยมิชอบ

(๔) ดำเนินการสำรองข้อมูลจราจร (Log Backup) อย่างสม่ำเสมอ และเก็บรักษาในสถานที่ปลอดภัย

๔) กำหนดให้มีการตรวจสอบและการใช้ประโยชน์จากข้อมูลจราจรคอมพิวเตอร์ โดยพิจารณาอย่างน้อยดังนี้

(๑) จัดให้มีการตรวจสอบข้อมูลจราจรอย่างสม่ำเสมอ เพื่อค้นหาความผิดปกติ เช่น รายสัปดาห์ รายเดือน หรือรายไตรมาส เป็นต้น

(๒) กำหนดกระบวนการให้ข้อมูลจราจรแก่หน่วยงานภายนอกตามกฎหมาย พร้อมการอนุมัติจากผู้มีอำนาจ

๖. กำหนดให้มีการบริหารจัดการตั้งนาฬิการะบบให้ถูกต้อง โดยพิจารณาอย่างน้อยดังนี้

๑) จัดให้มีการกำหนดแหล่งเวลาสำหรับเวลาที่ใช้ในการอ้างอิงการตั้งเวลาระบบให้ชัดเจน เช่น กรมอุทกศาสตร์ กองทัพเรือ

๒) จัดให้มีการจัดการสำหรับระบบที่แยกขาดหรือมีความปลอดภัยสูง โดยดำเนินการใช้ NTP Server ภายในที่อ้างอิงกับ GPS หรือ Atomic Clock หรือกำหนดให้มีการตรวจสอบความถูกต้องของเวลาของระบบความปลอดภัยสูงทุกวัน

๗. กำหนดให้มีการบริหารจัดการขีดความสามารถของระบบ (System Capacity Management) โดยวางแผนขีดความสามารถของระบบ และดำเนินการประเมินความต้องการของระบบในระยะสั้น กลาง และยาว และทบทวนอย่างสม่ำเสมอ โดยพิจารณาปัจจัยสำคัญ เช่น จำนวนผู้ใช้งานพร้อมกัน ปริมาณข้อมูลที่จัดเก็บ ปริมาณการร้องขอบริการต่อวินาที

๘. กำหนดให้มีการตรวจสอบ ติดตาม และประเมินความมั่นคงปลอดภัย โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) ติดตามสถานะการใช้งาน CPU, RAM, Storage, Bandwidth อย่างสม่ำเสมอ

๒) กำหนดให้มีการตั้งค่าการแจ้งเตือน (Alert) หากการใช้ทรัพยากรเข้าใกล้หรือเกินกว่าค่ากำหนด (Threshold)

๓) ทบทวนขีดจำกัดของอุปกรณ์รักษาความปลอดภัย เช่น Firewall, SIEM หรือ Antivirus Server อย่างสม่ำเสมอ

๙. กำหนดให้มีการบริหารจัดการทดสอบซอฟต์แวร์ ซึ่งต้องดำเนินการวางแผนการทดสอบ โดยพิจารณาอย่างน้อยดังนี้

๑) จัดทำแผนการทดสอบ (Test Plan) โดยรวมถึงการทดสอบความมั่นคงปลอดภัย เช่น การทดสอบ input validation, access control, error handling เป็นต้น

๒) กำหนดให้มีการแยกสภาพแวดล้อมการทดสอบออกจากระบบงานจริง

๓) กำหนดบทบาทหน้าที่ และสิทธิของผู้ทดสอบ, ผู้พัฒนา และผู้ดูแลระบบ ออกจากกันอย่างชัดเจน

๔) กำหนดให้มีการควบคุมการใช้ข้อมูลในการทดสอบ โดยห้ามใช้ข้อมูลจริง (Production Data) ในการทดสอบระบบทดสอบ หากจำเป็นต้องใช้ข้อมูลจริงต้องดำเนินการกำหนดมาตรการควบคุม เช่น Approval, NDA, และมาตรการป้องกันข้อมูลส่วนบุคคล เป็นต้น

๑๐. กำหนดให้มีการทดสอบความมั่นคงปลอดภัยของซอฟต์แวร์ เช่น

๑) การทดสอบความมั่นคงปลอดภัยของแอปพลิเคชันโดยการวิเคราะห์ซอร์สโค้ดหรือไบนารีแบบไม่ต้องรันโปรแกรม เพื่อค้นหาช่องโหว่ด้านความปลอดภัยตั้งแต่ระยะเริ่มต้นของการพัฒนา (Static Application Security Testing (SAST))

๒) การทดสอบความมั่นคงปลอดภัยของแอปพลิเคชันขณะกำลังทำงานจริง โดยจำลองการโจมตีจากภายนอกเพื่อค้นหาช่องโหว่ด้านความปลอดภัยจากพฤติกรรมของระบบ (Dynamic Application Security Testing (DAST))

๓) การวิเคราะห์ส่วนประกอบของซอฟต์แวร์ เช่น ไลบรารีโอเพ่นซอร์ส เพื่อระบุช่องโหว่ที่รู้จักและความเสี่ยงด้านลิขสิทธิ์ที่อาจส่งผลต่อความมั่นคงปลอดภัยของระบบ (Software Composition Analysis (SCA))

๔) การทดสอบระบบแบบองค์รวมเพื่อยืนยันว่าระบบทำงานสอดคล้องตามข้อกำหนดทางธุรกิจและความต้องการของผู้ใช้งาน ก่อนการนำระบบไปใช้งานจริง (System acceptance testing)

๕) การประเมินความมั่นคงปลอดภัยของระบบโดยรวม เพื่อตรวจสอบมาตรการควบคุมด้านความปลอดภัย เช่น การตรวจสอบสิทธิ์ การเข้ารหัส และการป้องกันการบุกรุก ว่ามีประสิทธิภาพและเหมาะสมกับความเสี่ยงที่คาดการณ์ไว้ (System security testing)

๑๑. กำหนดให้มีการควบคุมสภาพแวดล้อมการทดสอบ โดยพิจารณาอย่างน้อยดังนี้

๑) จำกัดการเข้าถึงระบบทดสอบ โดยให้เข้าถึงเฉพาะผู้มีสิทธิ์ รวมถึงพิจารณาใช้การยืนยันตัวตนที่มั่นคงปลอดภัย เช่น MFA, Role-based Access เป็นต้น

๒) กำหนดให้มีการบันทึก Log การเข้าถึงและการเปลี่ยนแปลงระบบในช่วงทดสอบ

๓) ตรวจสอบให้แน่ใจว่าไม่มีข้อมูลหรือรหัสสำคัญค้างอยู่ในระบบหลังดำเนินการทดสอบแล้วเสร็จ

๑๒. กำหนดให้มีการประเมินผลและจัดการช่องโหว่ก่อนนำระบบไปใช้งานจริง และหากพบข้อบกพร่องหรือช่องโหว่ในการทดสอบ ต้องดำเนินการประเมินความเสี่ยงและกำหนดระดับความรุนแรง พร้อมทั้งแก้ไขและทำการทดสอบซ้ำ (Retesting) ก่อนส่งมอบระบบ

๑๓. จัดทำรายงานการทดสอบ (Test Report) และรายการข้อบกพร่อง (Defect List) เพื่อใช้ในการตรวจสอบภายหลัง

๑๔. กำหนดให้มีการบริหารจัดการพิสูจน์การทดสอบและการตรวจรับงาน โดยกำหนดให้วางแผนการทดสอบ โดยพิจารณาอย่างน้อยดังนี้

๑) จัดทำแผนการทดสอบ (Test Plan) โดยกำหนดให้มีการทดสอบ อย่างน้อย ดังนี้

(๑) การทดสอบส่วนย่อยที่สุดของโปรแกรม เช่น ฟังก์ชันหรือเมธอด เพื่อให้มั่นใจว่าทำงานได้ถูกต้องตามที่ออกแบบไว้ โดยไม่ขึ้นกับส่วนอื่นของระบบ (Unit Test)

(๒) การทดสอบการทำงานร่วมกันของหน่วยโปรแกรมต่าง ๆ หรือระบบย่อยหลายระบบ เพื่อให้แน่ใจว่ามีการสื่อสารและทำงานร่วมกันได้ถูกต้อง (Integration Test)

(๓) การทดสอบโดยผู้ใช้งานหรือผู้แทนของธุรกิจ เพื่อประเมินว่าระบบตอบสนองต่อความต้องการและสามารถใช้งานได้จริงตามวัตถุประสงค์ก่อนนำไปใช้งานจริง (UAT)

(๔) การทดสอบเพื่อประเมินความมั่นคงปลอดภัยของระบบ โดยมุ่งตรวจสอบช่องโหว่ ความเสี่ยง และความสามารถของระบบในการป้องกันภัยคุกคามทางไซเบอร์ (Security Testing) เช่น SAST, DAST, Vulnerability Scan, Penetration Test เป็นต้น

๒) กำหนดผู้รับผิดชอบ ช่วงเวลา เครื่องมือ และเกณฑ์การผ่าน (Acceptance Criteria)

๓) กำหนดให้มีหลักฐานการทดสอบที่ชัดเจน เช่น รายการตรวจทดสอบ พร้อมผลการทดสอบ เป็นต้น

๑๕. กำหนดให้มีการทดสอบด้านความมั่นคงปลอดภัย โดยประกอบด้วย อย่างน้อยดังนี้

๑) ทำการทดสอบความปลอดภัยในขั้นตอน UAT หรือก่อนขึ้นระบบ (Go-live)

๒) เครื่องมือ หรือบริการที่ใช้ในการทดสอบต้องผ่านการรับรอง เช่น OWASP ZAP, Burp Suite, Nessus เป็นต้น

๓) หากพบความเสี่ยงระดับสูงหรือช่องโหว่สำคัญ ต้องแก้ไขก่อนอนุมัติการตรวจรับงาน

๑๖. กำหนดให้มีการบันทึกผลและจัดทำรายงานผลการทดสอบไว้เป็นหลักฐานการทดสอบ

๑๗. กำหนดให้มีการทบทวนภายหลังการขึ้นระบบงาน (Post-Acceptance Review) โดยดำเนินการอย่างน้อย ดังนี้

๑) ตรวจสอบความเสถียรและความมั่นคงปลอดภัยหลังจากที่มีการใช้งานระบบ ๓๐ วันนับจากที่มีการขึ้นระบบ ในกรณีที่พบปัญหาต้องดำเนินการบันทึกปัญหา การแก้ไข และแจ้งกลับผู้พัฒนาระบบ เพื่อนำไปปรับปรุงระบบ

๒) ดำเนินการสรุปปัญหา ผลการวิเคราะห์ และวิธีการแก้ไข เพื่อนำไปเป็นบทเรียน (Lessons Learned) สำหรับใช้ปรับปรุงในอนาคต

๑๘. กำหนดให้มีการจำกัดการปรับแต่งซอฟต์แวร์สำเร็จรูป โดยพิจารณาให้มีการดำเนินการประเมินก่อนปรับแต่งซอฟต์แวร์สำเร็จรูป โดยดำเนินการอย่างน้อย ดังนี้

๑) วิเคราะห์ความจำเป็นในการปรับแต่ง เทียบกับความสามารถมาตรฐานของซอฟต์แวร์ (Out-of-the-box)

๒) ประเมินผลกระทบด้านความมั่นคงปลอดภัย ความเข้ากันได้กับแพตช์ และ SLA การบำรุงรักษาของซอฟต์แวร์

๓) พิจารณาทางเลือกอื่น เช่น การปรับกระบวนการองค์กรให้สอดคล้องกับระบบ แทนที่จะปรับระบบให้สอดคล้องกับองค์กร

๑๙. กำหนดให้มีการควบคุมขอบเขตการปรับแต่งซอฟต์แวร์สำเร็จรูป โดยพิจารณาให้มีการควบคุมอย่างน้อย ดังนี้

๑) จำกัดการปรับแต่งเฉพาะฟังก์ชันที่ปลอดภัย และสามารถแยกออกจากซอฟต์แวร์หลัก เช่น ผ่าน API, Extension Framework เป็นต้น

๒) ห้ามแก้ไขซอร์สโค้ดของระบบหลักโดยตรง เว้นแต่ได้รับอนุญาตจากผู้ผลิต และไม่กระทบกับการดำเนินการด้านความมั่นคงปลอดภัยของระบบหลัก

๓) ในกรณีที่มีการเปลี่ยนแปลงต้องดำเนินการจัดเก็บ Script, Code และ Log การเปลี่ยนแปลงทั้งหมด พร้อมทั้ง Version Control และจัดทำ Change Log เป็นลายลักษณ์อักษร

๔) กำหนดให้มีการขออนุมัติการปรับแต่งซอฟต์แวร์สำเร็จรูปจากเจ้าของระบบ และฝ่ายเทคโนโลยีสารสนเทศ หรือฝ่ายที่ได้รับมอบหมาย

๕) กำหนดสิทธิการเข้าถึงเฉพาะผู้ที่ได้รับอนุมัติ หรืออนุญาตให้มีสิทธิปรับแต่งซอฟต์แวร์สำเร็จรูปเท่านั้น พร้อมทั้งจัดทำบันทึกประวัติการเข้าถึง หรือบันทึกกิจกรรมการเข้าถึง (Log)

๖) กำหนดให้มีกระบวนการทดสอบในระบบ UAT/Sandbox แยกจาก Production พร้อมทั้งต้องมีแผน Rollback ที่สามารถใช้คืนระบบสู่สภาพเดิมได้หากเกิดข้อผิดพลาด

๗) ในกรณีที่มีการอัปเดตแพตช์จากผู้ผลิต ต้องมีการดำเนินการตรวจสอบผลกระทบของการปรับแต่งก่อนดำเนินการ

๘) ในกรณีที่มีการปรับปรุงเวอร์ชันใหม่ของซอฟต์แวร์ ผู้ดูแลระบบและผู้ที่ได้รับมอบหมายให้ดำเนินการปรับแต่งซอฟต์แวร์ต้องร่วมกันประเมินผลกระทบต่อประสิทธิภาพของการใช้งาน

๒๐. กำหนดให้มีการจัดการทบทวนทางเทคนิคของแอปพลิเคชันหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) กำหนดให้มีการลงทะเบียนการเปลี่ยนแปลงตามกระบวนการเปลี่ยนแปลงขององค์กร พร้อมทั้ง พร้อมทั้งระบุรายละเอียดการเปลี่ยนแปลง เช่น ประเภทของการเปลี่ยนแปลง ช่วงเวลา ระบบที่เกี่ยวข้อง และแอปพลิเคชันที่คาดว่าจะได้รับผลกระทบจากการเปลี่ยนแปลง เป็นต้น

๒) กำหนดให้มีการประเมินผลกระทบเชิงเทคนิค เช่น การเชื่อมต่อระบบภายนอก/ภายใน (IP, Port, Firewall) การเรียกใช้งาน API, Library, หรือบริการ (Service) ที่ได้รับผลกระทบ และตรวจสอบความเข้ากันได้ของเวอร์ชันใหม่กับซอฟต์แวร์ หรือเฟรมเวิร์กของแอปพลิเคชัน เป็นต้น

๓) กำหนดให้มีการทดสอบก่อนและหลังการนำไปใช้งาน โดยจัดให้มีการทดสอบฟังก์ชันที่สำคัญในแอปพลิเคชันในสภาพแวดล้อมสำหรับการทดสอบ เช่น Sandbox, UAT เป็นต้น รวมถึงทดสอบการเชื่อมต่อ ความเร็ว การพิสูจน์ตัวตน และการเข้าถึงข้อมูลหลังจากการเปลี่ยนแปลง

๔) กำหนดให้มีการตรวจประเมินความมั่นคงปลอดภัยหลังจากที่มีการเปลี่ยนแปลงโครงสร้างพื้นฐาน เช่น สแกนช่องโหว่ (Vulnerability Scanning) ทดสอบสิทธิและการควบคุมการเข้าถึง ประเมินผลกระทบต่อมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (PDPA) หรือการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC ๒๗๐๐๑)

๕) จัดให้มีรายงาน Application Review Result ที่แสดงผลการตรวจสอบและทดสอบ รวมถึงผลการติดตามการแก้ไขในกรณีที่พบข้อบกพร่อง พร้อมทั้งจัดเก็บไว้เป็นหลักฐาน

(H) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้มีการจัดทำแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) โดยดำเนินการอย่างน้อย ดังนี้

๑) มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดวัตถุประสงค์ของแผนการสื่อสารในภาวะวิกฤต และครอบคลุมการสื่อสารภายในและการสื่อสารไปยังภายนอกให้ครบถ้วน รวมถึงมีการระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง

๒) กำหนดและวิเคราะห์กลุ่มผู้มีส่วนได้ส่วนเสีย (Stakeholder) ทั้งภายใน และภายนอก รวมทั้งระบุกลุ่มเป้าหมายที่ต้องสื่อสารเมื่อเกิดเหตุการณ์วิกฤต โดยพิจารณาจากสถานการณ์ จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๓) จัดโครงสร้างของทีมสื่อสารในภาวะวิกฤตพร้อมทั้งหน้าที่ความรับผิดชอบ ให้สอดคล้องกับบริบทของ ขร. โดยทีมสื่อสารในภาวะวิกฤตอาจประกอบด้วย ผู้บริหาร เจ้าหน้าที่ ฝ่ายประชาสัมพันธ์ เจ้าหน้าที่ฝ่ายทรัพยากรมนุษย์ เจ้าหน้าที่ฝ่ายกฎหมาย เป็นต้น

๔) จัดเตรียมร่างข้อความที่ใช้สื่อสารเมื่อเกิดภาวะวิกฤต และกำหนดโฆษกหลัก และผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กร เมื่อมีการกล่าวแถลงกับสื่อมวลชน

๕) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๖) ตรวจสอบแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ เพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๗) ดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงที และมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(I) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้มีการจัดเตรียมบุคคลกรสำหรับฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) โดยดำเนินการอย่างน้อย ดังนี้

๑) สนับสนุนบุคลากรและเจ้าหน้าที่ ให้เข้าร่วมฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ ทั้งในระดับชาติหรือระดับภาคส่วน โดยบุคลากรและเจ้าหน้าที่ที่อยู่ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

๒) เข้าร่วมฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ตามที่คณะกรรมการกำหนด อย่างน้อยปีละ ๑ ครั้ง

๓) ปฏิบัติตามคำขอของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ เพื่อวัตถุประสงค์ในการวางแผน และดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์ และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้น

๔) จัดทำตารางรายการตรวจสอบ (Checklist) โดยรวบรวมรายชื่อผู้ที่อยู่ในแผนการรับมือภัยคุกคามทางไซเบอร์ และดำเนินการตรวจสอบว่าบุคคลดังกล่าวตามรายชื่อมีการเข้าร่วมฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์หรือไม่ รวมถึงจัดให้มีการรายงานให้ผู้บริหารรับทราบ

๒. กำหนดให้มีการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) โดยดำเนินการอย่างน้อย ดังนี้

๑) กำหนดนโยบายในการฝึกซ้อม ประกอบด้วยเป้าหมาย ขอบเขตของการใช้งาน การบังคับใช้ ผู้ที่เกี่ยวข้องในการฝึกซ้อมแผน เป็นต้น

๒) กำหนดบทบาทหน้าที่และความรับผิดชอบ (Identify Roles and Responsibilities) ในการดูแลโปรแกรมการฝึกซ้อม ซึ่งพิจารณากำหนดเป็นบุคคลหรือทีมที่รับผิดชอบในการวางแผนการฝึกซ้อม รวมถึงทำหน้าที่ในการประสานงานกิจกรรมต่าง ๆ และดูแลบำรุงรักษาแผนการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

๓) กำหนดตารางการฝึกซ้อม โดยพิจารณาข้อกำหนดหรือกฎหมายที่เกี่ยวข้องในการระบุความถี่ในการทบทวนหรือทดสอบแผน รวมทั้งความถี่ในการฝึกซ้อม พร้อมทั้งดำเนินการภายในระยะเวลาที่กำหนด

๔) กำหนดให้มีการจัดทำเอกสารที่เกี่ยวข้องกับการวางแผนการฝึกซ้อม ประกอบด้วย

(๑) การกำหนดหัวข้อ และขอบเขตของกิจกรรม ระบุวัตถุประสงค์พื้นฐานตามหัวข้อและขอบเขตที่จะทำการฝึกซ้อม และกำหนดบุคลากรที่ควรเข้าร่วมกิจกรรม รวมถึงกำหนดให้ผู้ดูแลโปรแกรมการฝึกซ้อม ดำเนินการพิมพ์เอกสาร การเตรียมห้องฝึกซ้อม อาหาร และอุปกรณ์เครื่องเสียงหรือวิดีโอ

(๒) การจัดทำเอกสารในการดำเนินกิจกรรม เช่น คู่มือสำหรับผู้เข้าร่วมฝึก แผนการทดสอบ สคริปต์ เกณฑ์การประเมิน เป็นต้น

(๓) จัดทำรายงานผลของการฝึกอบรมหรือทดสอบตามกิจกรรมที่ได้ออกแบบ

(๔) ดำเนินการประเมินกิจกรรมที่จัดขึ้น หรืออุปสรรคที่เกิดขึ้นระหว่างการดำเนินการ รวมถึงรับฟังความคิดเห็นของผู้เข้าร่วมกิจกรรมที่จัดขึ้น เพื่อใช้ในการปรับปรุงแผนและปรับปรุงการดำเนินงาน

(J) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยผู้บริหารสูงสุด หรือผู้ที่ได้รับมอบอำนาจของ ขร. ก่อนดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

๒. กำหนดให้มีการพิจารณผู้ตรวจสอบตามเกณฑ์การพิจารณาข้างต้น อย่างน้อย ดังนี้ ความเป็นอิสระ และความสามารถของผู้ตรวจสอบ

๓. กำหนดให้ทีมตรวจสอบและผู้ตรวจสอบที่ได้รับการแต่งตั้ง ควรมีคุณลักษณะ ดังนี้

ก. ไม่อยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of Interest) โดยผลประโยชน์ทับซ้อนหมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของผู้ตรวจสอบอาจก่อให้เกิดการแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบจนทำให้การดำเนินการตรวจสอบไม่เป็นอิสระหรือไม่มีตรงกับหลักฐานที่ปรากฏ

ข. มีความสามารถทางเทคนิคที่จำเป็นต่อการดำเนินการตรวจสอบ เช่น มีคุณวุฒิวิชาชีพ ใบรับรอง ทักษะ ความรู้และประสบการณ์ที่เกี่ยวข้อง

๔. ในกรณีที่ไม่มีบุคคลที่มีคุณสมบัติตรงตามเกณฑ์ที่กำหนด สำหรับการเป็นผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สามารถพิจารณาดำเนินการได้ ดังนี้

(๑) พิจารณาพัฒนาและอบรมบุคลากรภายใน (Internal Development) โดยพิจารณา ดังนี้

- จัดอบรมและพัฒนาทักษะบุคลากรภายในให้มีคุณสมบัติที่เหมาะสม เช่น การฝึกอบรมหลักสูตรเกี่ยวกับการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ หรือการสอบใบรับรองวิชาชีพที่เกี่ยวข้อง เช่น CISA, ISO ๒๗๐๐๑ Lead Auditor, CISSP
- จัดทำแผนพัฒนาบุคลากรโดยให้พนักงานเข้ารับการฝึกอบรมเป็นระยะ หรือส่งพนักงานเข้าร่วมโครงการพี่เลี้ยง (Mentorship) จากผู้เชี่ยวชาญ

(๒) พิจารณาว่าจ้างผู้ตรวจสอบภายนอก (External Hiring) โดยพิจารณา ดังนี้

- ว่าจ้างผู้ตรวจสอบภายนอก (Third-Party Auditor) หรือสำนักงานตรวจสอบที่ได้รับการรับรอง ซึ่งมีคุณสมบัติตรงตามที่กำหนด
- ใช้บริการที่ปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์ที่มีประสบการณ์ในการตรวจสอบ

(๓) พิจารณาใช้ทีมตรวจสอบภายในจากหน่วยงานอื่น (Internal Rotation or Collaboration) โดยพิจารณา ดังนี้

- หากหน่วยงานมีหลายแผนกอาจพิจารณาส่งบุคลากรจากแผนกอื่นที่ไม่มีผลประโยชน์ทับซ้อนมาทำหน้าที่ตรวจสอบ
- ขอความร่วมมือจากพันธมิตรที่สามารถส่งบุคลากรที่มีคุณสมบัติเข้ามาตรวจสอบได้

(๔) พิจารณากำหนดข้อยกเว้นและแผนระยะยาว (Exception Handling & Long-Term Plan) โดยพิจารณา ดังนี้

- ในกรณีที่ไม่สามารถหาได้จริงอาจดำเนินการกำหนดข้อยกเว้นชั่วคราว เช่น ใช้บุคลากรที่มีความรู้พื้นฐานและให้มีการตรวจสอบเพิ่มเติมโดยผู้เชี่ยวชาญภายนอก
- จัดทำแผนระยะยาวในการพัฒนาทีมตรวจสอบภายในเพื่อให้มีบุคลากรที่เพียงพอในอนาคต

๕. กำหนดให้มีการดำเนินการจัดทำขั้นตอนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ หรือประยุกต์ใช้ขั้นตอนการตรวจสอบเดิมของ ขร. และเพิ่มเติมขั้นตอนที่เกี่ยวข้องสอดคล้องกับข้อกำหนดกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์

๖. กำหนดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ ขร. โดยดำเนินการ ดังนี้

๑) กำหนดให้มีการจัดทำแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และดำเนินการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตของการตรวจสอบ อย่างน้อยประกอบด้วย

(๑) การวิเคราะห์ผลการวิเคราะห์ผลกระทบทางการดำเนินการตามภาระกิจหน้าที่ (Business Impact Analysis: BIA) ประกอบด้วยข้อมูล ดังนี้

- ผลการวิเคราะห์ผลกระทบทางการดำเนินการตามภาระกิจหน้าที่ (Business Impact Analysis: BIA) ที่ผู้มีส่วนได้ส่วนเสียพิจารณาร่วมกัน และได้รับอนุมัติ จากผู้บริหารสูงสุดของ ขร. หรือบุคคลหรือคณะกรรมการที่ได้รับมอบหมาย
- รายการกระบวนการทางธุรกิจ พร้อมระบุระดับผลกระทบ ระยะเวลาสูงสุดที่ยอมให้การดำเนินการตามหน้าที่ความรับผิดชอบหยุดชะงัก ระยะเวลาในการกู้คืนระบบ ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย และคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศที่เกี่ยวข้อง
- ทรัพยากรที่ต้องใช้ดำเนินการแก้ปัญหาการหยุดชะงัก

- บริการที่สำคัญที่ได้จากผลกระทบทางการดำเนินการตามภาระกิจหน้าที่ (Business Impact Analysis: BIA) โดยบริการที่สำคัญต้องมีความเชื่อมโยงกับวัตถุประสงค์ และพันธกิจของ ขร.

(๒) บริการที่สำคัญที่ ขร. เป็นเจ้าของและใช้บริการ ตามผลกระทบทางการดำเนินการตามภาระกิจหน้าที่ (Business Impact Analysis: BIA) ซึ่งต้องมีการตรวจสอบตามนโยบาย การกำหนดหน้าที่รับผิดชอบ ฮาร์ดแวร์และซอฟต์แวร์ที่เกี่ยวข้อง แผนและผลของการปรับปรุงของการดำเนินการตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ซึ่งประกอบด้วยรายการอย่างน้อย ดังนี้

- การจัดทำทะเบียนทรัพย์สิน และการจัดทำขอบเขตเครือข่ายของบริการที่สำคัญ
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมบริการที่สำคัญ
- การประเมินช่องโหว่ และแผนการจัดการช่องโหว่ที่ครอบคลุมบริการที่สำคัญ
- การจัดการผู้ให้บริการภายนอกที่เกี่ยวข้องกับบริการที่สำคัญ
- การควบคุมการเข้าถึงบริการที่สำคัญ
- การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ที่ครอบคลุมถึงบริการที่สำคัญ
- การควบคุมเชื่อมต่อระยะไกล (Remote Connection) ที่เชื่อมต่อมายังบริการที่สำคัญ
- การควบคุมสื่อเก็บข้อมูลแบบถอดได้ (Removable Media) ที่เชื่อมต่อกับบริการที่สำคัญ
- การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลที่เกี่ยวข้องกับบริการที่สำคัญ
- การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ให้กับบริการที่สำคัญ
- การจัดแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)

(๓) การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์และประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรฐานการปฏิบัติงาน และทิศทางที่คณะกรรมการประกาศกำหนด

ทั้งนี้ ผู้ตรวจสอบสามารถพิจารณาตรวจสอบตามความเสี่ยงได้จากการพิจารณาผลการตรวจสอบครั้งที่ผ่านมา การเกิดเหตุภัยคุกคามทางไซเบอร์ครั้งล่าสุดที่ส่งผลกระทบต่อ ขร. และข้อร้องเรียนของผู้ใช้บริการ ผลการประเมินช่องโหว่หรือผลการทดสอบเจาะระบบ (Vulnerability Assessment or Penetration Testing Report) เหตุละเมิดข้อมูลส่วนบุคคลที่ผ่านมาการไม่ปฏิบัติการตามกฎหมายกฎระเบียบ (Noncompliance) ผลการประเมินความเสี่ยง

๒) กำหนดระดับผลการตรวจสอบ โดยแบ่งหมวดหมู่ของความสอดคล้องเป็น ๓ ระดับ ดังนี้

- ความไม่สอดคล้องที่สำคัญ (Major Non-Conformity: Major NC) หมายถึง พบว่าไม่นำข้อกำหนดกฎหมายข้อใดข้อหนึ่งหรือทั้งหมดไปปฏิบัติ และทำให้ระบบการจัดการล้มเหลว หรือมีความเสี่ยงสูงหรือมีเหตุนำมาซึ่งความเสียหายอย่างร้ายแรงต่อระบบ หรือผู้ตรวจสอบพบความไม่สอดคล้องย่อย (Minor Non-Conformity) หลาย ๆ จุดในข้อกำหนดเดียว ซึ่งเมื่อพิจารณาแล้วมีผลกระทบต่อระบบการจัดการโดยรวม

- ความไม่สอดคล้องย่อย (Minor Non-Conformity: Minor NC) หมายถึง พบว่าไม่ปฏิบัติการตามข้อกำหนดกฎหมายบางส่วน มีการละเลยการดำเนินการเพียงบางส่วน หรือปฏิบัติไม่ครอบคลุมซึ่งจะไม่ทำให้ระบบการจัดการล้มเหลว หรือไม่ได้เป็นเหตุที่จะนำมาซึ่งความเสียหายอย่างร้ายแรงต่อระบบ

- การดำเนินการสอดคล้อง (Conformity: C) หมายถึง พบว่าหน่วยงานดำเนินการตามที่ประกาศกำหนดทั้งหมด

๓) ในกรณีที่ผู้ตรวจสอบพบข้อสังเกต (Observation: OBS) ที่อาจมีผลกระทบ โดยไม่ถือเป็นความไม่สอดคล้องย่อย แต่หากหน่วยงานปล่อยทิ้งไว้ หรือละเลยอาจนำไปสู่ความไม่สอดคล้องได้ (Potential Non-Conformity) จึงควรปรับปรุงตามข้อสังเกต เพื่อป้องกันความไม่สอดคล้องมิให้เกิดขึ้น หรือในกรณีที่ผู้ตรวจสอบอาจพบโอกาสในการปรับปรุง (Opportunity for Improvement: OFI) ซึ่งหมายความว่าข้อเสนอแนะหรือโอกาสเพื่อการปรับปรุงในการปฏิบัติให้ดียิ่งขึ้น หรือเพื่อป้องกันความไม่สอดคล้อง

๔) กำหนดให้มีการดำเนินการสรุปผลการตรวจสอบ (Audit Conclusion) โดยผู้ตรวจสอบต้องให้ความเห็นและข้อสรุป โดยมีประเด็นอย่างน้อย ดังนี้

ก. ความเหมาะสมของการตอบสนองต่อผลการตรวจสอบจากฝ่ายบริหาร

ข. ประสิทธิผลและความเหมาะสมของมาตรการควบคุมของ ขร. เพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และโอกาสในการปรับปรุง เพื่อรักษาความมั่นคงปลอดภัยของ ขร.

๕) กำหนดให้มีการดำเนินการจัดทำรายงานการตรวจสอบ ประกอบไปด้วยหัวข้อ อย่างน้อย ดังนี้

- บทสรุปผู้บริหาร (Executive Summary)
- วัตถุประสงค์ (Purpose)
- เกณฑ์ในการตรวจสอบ (Audit Criteria)
- ขอบเขตการตรวจสอบ (Audit Scope)
- วันเวลาที่ตรวจสอบ
- ผู้ตรวจสอบ
- ผู้มีส่วนได้ส่วนเสีย (Stakeholders)
- วิธีการและแนวทาง การตรวจสอบ (Audit Methodology and Approach)
- สิ่งที่พบจากการตรวจสอบ (Audit Finding)
- สรุปการตรวจสอบ (Audit Conclusion)

๖) รายงานผลดำเนินการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยสานสนเทศและไซเบอร์ต่อคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในกรณีที่มีการร้องขอจากสำนักงาน ภายใน ๓๐ วัน

๗) ในกรณีที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้ ขร. ดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) กำหนด

๘) เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) ขร. จะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้เสร็จสิ้นภายในระยะเวลาตามที่ระบุไว้ในแผนดังกล่าว

๗. กำหนดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ผู้ให้บริการขนส่งทางราง โดยดำเนินการดังนี้

๑) ดำเนินการแต่งตั้งกลุ่มบุคคลทำหน้าที่เป็นผู้ตรวจสอบ อันประกอบไปด้วย หัวหน้าทีมผู้ตรวจสอบ (Lead Auditor) และผู้ตรวจสอบ (Auditor) ที่มีความรู้ความเชี่ยวชาญด้านการตรวจสอบเรื่องความมั่นคงปลอดภัยไซเบอร์

๒) ดำเนินการตรวจสอบการดำเนินการของผู้ให้บริการขนส่งทางที่อยู่ภายใต้การควบคุมหรือกำกับดูแล ให้เป็นไปตามมาตรฐานขั้นต่ำที่กำหนด

๓) จัดทำรายงานสรุปผลการตรวจสอบให้แก่สำนักงานภายใน ๓๐ วัน หลังกระบวนการตรวจสอบเสร็จสิ้น

๔) ในกรณีที่พบว่าการดำเนินการไม่เป็นไปตามมาตรฐานขั้นต่ำที่กำหนด ขร. ต้องดำเนินการแจ้งผู้ให้บริการขนส่งทางราง แก้ไขให้ได้มาตรฐานขั้นต่ำ ภายในระยะเวลา ๓๐ วัน หลังจากได้รับแจ้งจาก ขร.

๕) ในกรณีที่พบว่าผู้ให้บริการขนส่งทางรางไม่ดำเนินการภายในระยะเวลาที่กำหนด ขร. ต้องดำเนินการแจ้ง กกม. เพื่อดำเนินการตามมาตรา ๕๓ วรรคสอง

(K) การเชื่อมต่อระยะไกล (Remote Connection)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้มีการพิจารณาด้านความมั่นคงปลอดภัยของกลไกหรือเครื่องมือสำหรับการทำงานจากระยะไกลและการเข้าถึงจากระยะไกล (Security Considerations for the Telework and Remote Access Life Cycle) โดยแบ่งวงจรชีวิตออกเป็น ๕ ขั้นตอน ดังนี้

๑) ขั้นตอนเริ่มต้น (Initiation)

กำหนดนโยบายความมั่นคงปลอดภัยของการทำงานจากระยะไกล (Telework Security Policy) เป็นส่วนหนึ่งในแผนการรักษาความมั่นคงปลอดภัยของระบบ (System Security Plan) รวมถึงควรครอบคลุมข้อกำหนด ดังนี้

๑.๑) กำหนดประเภทของกลไกหรือเครื่องมือสำหรับการเข้าถึงจากระยะไกลที่อนุญาตให้เข้าถึงได้จากระยะไกล เช่น การติดตั้งซอฟต์แวร์สำหรับการทำงานจากระยะไกล (Software Already Installed on Telework Device) ที่สามารถใช้สำหรับการเข้าถึงจากระยะไกล รวมถึงไม่ควรอนุญาตให้ใช้ประเภทการเข้าถึงจากระยะไกลที่ไม่สอดคล้องกับนโยบาย

๑.๒) ข้อจำกัดเกี่ยวกับอุปกรณ์หรือโปรแกรมสำหรับการขอใช้บริการสำหรับการทำงานจาก ระยะไกลและระดับการเข้าถึงจากระยะไกล (Restrictions on Telework Client Devices and Remote Access Levels) โดยกำหนดประเภทของไคลเอนต์และระดับชั้นการเข้าถึงที่อนุญาตให้เข้าถึง โดยอิงตามระดับความเสี่ยงของทรัพยากรที่เกี่ยวข้อง ดังนี้

(๑) การกำหนดข้อจำกัดทั่วไปด้านความมั่นคงปลอดภัยในการทำงานจากระยะไกลที่มี ควรพิจารณาดังนี้

- การเข้าถึงข้อมูลหรือทรัพยากรที่มีความอ่อนไหวต้องมีการข้อกำหนดที่เข้มงวดมากขึ้น (Restrictive Requirement) เช่น การอนุญาตให้ใช้เฉพาะอุปกรณ์การทำงานจากระยะไกลที่ควบคุมโดย ขร. เท่านั้นเข้าถึงข้อมูลที่มีความอ่อนไหว
- กำหนดค่าของอุปกรณ์สำหรับการทำงานจากระยะไกล เพื่อให้มั่นใจในความมั่นคงปลอดภัยในระดับต้น ในกรณีที่อุปกรณ์ที่ไม่ได้ควบคุมโดย ขร. (Non-Organization-Controlled Device) สามารถใช้เครื่องแม่ข่ายสำหรับการเข้าถึงจากระยะไกล (Remote Access Server) เพื่อตรวจสอบอุปกรณ์ที่ร้องขอใช้บริการให้เป็นตามข้อกำหนดของ ขร. ได้ รวมถึงสร้างความตระหนักถึงความรับผิดชอบของ

ผู้ร้องขอเข้าถึงจากระยะไกลให้มีความระมัดระวัง และคำนึงถึงการรักษาความมั่นคงปลอดภัยของอุปกรณ์ตลอดเวลา

ทั้งนี้ อุปกรณ์ที่ควบคุมโดยบุคคลหรือผู้ให้บริการภายนอก ต้องมีข้อกำหนดบังคับให้บุคคลหรือผู้ให้บริการภายนอกปฏิบัติตามนโยบาย และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของ ขร. ผ่านข้อกำหนดในสัญญา

- ข้อจำกัดทางเทคนิค (Technical Limitation) ในการทำงานจากระยะไกลอาจจำเป็นต้องใช้อุปกรณ์เฉพาะเครื่องแม่ข่ายที่ให้บริการการเข้าถึงจากระยะไกลบางประเภท ซึ่งสามารถรองรับการเชื่อมต่อผ่านโปรแกรมไคลเอนต์เฉพาะ (Custom Client) เท่านั้น
- การกำหนดให้ต้องปฏิบัติตามข้อกำหนดเกี่ยวกับการทำงานจากระยะไกลให้เป็นไปตามนโยบายการเข้าถึงข้อมูลจากระยะไกล และนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของ ขร.

(๒) การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยในการทำงานจากระยะไกลที่มีความเสี่ยงสูงเป็นพิเศษ ควรพิจารณา ดังนี้

- อนุญาตการทำงานจากระยะไกลที่มีความเสี่ยงสูงจากอุปกรณ์ระยะไกลที่ ขร. จัดหา ให้เป็นการเฉพาะเท่านั้นและมีมาตรการความมั่นคงปลอดภัย (Organization-Issued and Secured Telework Device)
- พิจารณาให้ใช้การยืนยันตัวตนด้วยหลายปัจจัย (Multi-factor Authentication) สำหรับการเข้าถึงอุปกรณ์การทำงานจากระยะไกล และการเข้าถึงจากระยะไกล
- กำหนดให้มีการเข้ารหัสที่เก็บข้อมูล (Use Storage Encryption) บนอุปกรณ์การทำงานจากระยะไกล เพื่อปกป้องข้อมูลที่มีความอ่อนไหวทั้งหมด เช่น กำหนดให้เข้ารหัสดิสก์เต็มรูปแบบ เพื่อลดความเสี่ยงจากผู้โจมตีที่ได้รับสิทธิเข้าถึงทางกายภาพ รวมกับการเข้ารหัสดิสก์เสมือน (Virtual Disk) หรือการเข้ารหัสไฟล์/โฟลเดอร์ และกำหนดให้มีการเข้ารหัสข้อมูลที่เกิดจากการทำงานจากระยะไกล (Telework Data) ที่อยู่ในสื่อเก็บข้อมูลแบบถอดได้ (Removable Media)
- โอนย้ายทรัพยากรที่มีความเสี่ยงสูงไปยังเครื่องแม่ข่ายที่มีความสามารถในการปกป้องทรัพยากร ดังกล่าว (Migrate High-Risk Resources to Servers that Assume Responsibility for Protecting Them) เช่น กำหนดให้ผู้ปฏิบัติงานจากระยะไกลต้องเชื่อมต่อกับเครื่องแม่ข่ายเทอร์มินัลที่เก็บข้อมูลสำคัญที่ผู้ปฏิบัติงานจากระยะไกลจำเป็นต้องใช้
- จัดเก็บและอนุญาตเข้าถึงข้อมูลที่จำเป็นเท่านั้น (Store and Access Only the Minimum Data Necessary) ในกรณีที่ให้บุคลากรยืมอุปกรณ์ ต้องดำเนินการล้าง (Wipe) ข้อมูลทั้งหมดก่อนและหลังการทำงานจากระยะไกลที่มีความเสี่ยงสูง เช่น บุคลากรทำงานขณะการเดินทางไปต่างจังหวัดหรือต่างประเทศ และใส่เฉพาะข้อมูลและแอปพลิเคชันที่ได้รับอนุญาตและจำเป็นสำหรับการทำงานจากระยะไกลเท่านั้นในอุปกรณ์ และไม่อนุญาตเชื่อมต่อกับเครือข่ายภายในของ ขร.
- ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (System Command) เช่น คำสั่ง Start, Stop, Restart/Reboot, Shutdown, Disable/Enable, Rollback,

Upgrade, Reset, FactoryReset ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างชัดเจน เนื่องจากมีความจำเป็นต่อการดำเนินงานภาระกิจ และหน้าที่ของ ขร.

- จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ เช่น การเปิดบริการ หรือฟังก์ชันบนเครื่องแม่ข่ายให้แก่การทำงานจากระยะไกลเฉพาะบริการหรือฟังก์ชันที่จำเป็นเท่านั้น รวมถึงการกำหนดสิทธิการเข้าถึงข้อมูล เช่น ไม่ให้ส่งไฟล์ไปยังเครื่องแม่ข่าย ไม่ให้เข้าถึงข้อมูลอ่านข้อมูลได้อย่างเดียว หรือ อ่านและเขียนได้ รวมถึงตั้งค่า Firewall เพื่ออนุญาตการเชื่อมต่อกับบริการหรือฟังก์ชันบนเครื่องแม่ข่ายในกรณีที่จำเป็นเท่านั้น

ทั้งนี้ ในกรณีที่อยู่ในสถานการณ์ที่มีความเสี่ยงสูง ขร. อาจพิจารณาห้ามการทำงานจากระยะไกล และห้ามการเข้าถึงจากระยะไกล โดยเฉพาะที่ต้องเข้าถึงข้อมูลบางประเภท เช่น ข้อมูลที่ระบุตัวตนได้ และมีความอ่อนไหว เป็นต้น

(๓) การกำหนดแนวทางการกำหนดระดับการเข้าถึง (Access Tier) จากระยะไกลให้แก่อุปกรณ์ ไคลเอนต์ สามารถพิจารณาแบ่งได้เป็น ๗ ประเภท ดังนี้

- อุปกรณ์ที่ ขร. จัดหา (Furnished Equipment: FE) และอยู่ในสำนักงาน
- อุปกรณ์ที่ ขร. จัดหาสำหรับการทำงานจากระยะไกล (FE in Telework)
- อุปกรณ์ส่วนตัว BYOD ที่ผู้ใช้นำมาใช้งานในสำนักงานของ ขร. (BYOD in office)
- อุปกรณ์ส่วนตัว BYOD ที่ผู้ใช้นำมาใช้ทำงานจากระยะไกล (BYOD in Telework)
- อุปกรณ์ของผู้ให้บริการภายนอก, พันธมิตรทางธุรกิจ (Contractor, Partner, Vendor in Office)
- อุปกรณ์ของผู้ให้บริการภายนอก, พันธมิตรทางธุรกิจ ที่นำมาใช้เข้าถึงข้อมูลหรือบริการของหน่วยงานจากระยะไกล (Contractor, Partner, Vendor in Telework)
- อุปกรณ์อื่น ๆ ของบุคคลที่สาม เช่น อุปกรณ์ของอินเทอร์เน็ตคาเฟ่หรือโรงแรม

ทั้งนี้ ต้องกำหนดให้มีการเฝ้าระวังความมั่นคงปลอดภัยของเครือข่ายส่วนบุคคลไร้สาย (Wireless Personal Area Networks: WPAN) ซึ่งเป็นอุปกรณ์เครือข่ายไร้สายขนาดเล็กที่ไม่ใช่โครงสร้างพื้นฐานสำหรับการทำงาน เช่น การใช้แป้นพิมพ์หรือเมาส์ไร้สายกับคอมพิวเตอร์ การพิมพ์แบบไร้สาย การเชื่อมต่อสมาร์โฟนกับคอมพิวเตอร์ และการเชื่อมต่อชุดหูฟังหรือหูฟังไร้สายกับสมาร์ทโฟน โดยต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลควรปิดใช้งานเทคโนโลยี WPAN เมื่อไม่ได้ใช้งาน เพื่อป้องกันการใช้งานในทางที่ผิด โดยไม่ได้รับอนุญาต

๒) ขั้นตอนการพัฒนา (Development)

การพัฒนากลไกหรือเครื่องมือ เพื่อรองรับการทำงานจากระยะไกลควรมีการพิจารณาด้านความมั่นคงปลอดภัยทางเทคนิคที่สำคัญ อย่างน้อยดังนี้

๒.๑) สถาปัตยกรรม (Architecture)

ดำเนินการพิจารณาการออกแบบสถาปัตยกรรมรวมถึงการจัดวางเครื่องแม่ข่ายการเข้าถึงจากระยะไกล (Placement of the Remote Access Server) การเลือกซอฟต์แวร์ไคลเอนต์การเข้าถึงจากระยะไกล (Remote Access Client Software) และการออกแบบเซ็กเมนต์เครือข่ายของ ขร. (Organization Network Segment) เฉพาะสำหรับการเชื่อมต่อกับอุปกรณ์ไคลเอนต์ที่ไม่ได้ควบคุมโดย ขร. (non-Organization-Controlled Client Device) ซึ่งอาจพิจารณาออกแบบให้มีเซ็กเมนต์เพียงเซ็กเมนต์เดียวหรือหลายเซ็กเมนต์ตามความเหมาะสมและวัตถุประสงค์ของ ขร.

๒.๒) การพิสูจน์ตัวตน (Authentication)

ดำเนินการคัดเลือกเทคโนโลยีหรือวิธีการพิสูจน์ตัวตนการเข้าถึงจากระยะไกล และกำหนดวิธีการใช้ส่วนประกอบของเทคโนโลยี การใช้งานไคลเอนต์ และการใช้งานเครื่องแม่ข่าย รวมถึงขั้นตอนสำหรับการเริ่มใช้งานและการรีเซ็ตค่าการใช้งานของเทคโนโลยี (Issuing and Resetting Authenticator) และขั้นตอนการจัดเตรียมเทคโนโลยีให้กับผู้ใช้และอุปกรณ์ของผู้ใช้งาน

๒.๓) พิจารณาวิทยาการการเข้ารหัสลับ (Cryptography) รวมถึงการเลือกอัลกอริทึมสำหรับการเข้ารหัส (Encryption) การป้องกันความถูกต้องครบถ้วน (Integrity Protection) ของการสื่อสารการเข้าถึงจากระยะไกล และการตั้งค่าความแข็งแกร่งของคีย์สำหรับอัลกอริทึมที่รองรับความยาวของคีย์หลายรายการ (Support Multiple Key Length)

๒.๔) กำหนดให้มีการควบคุมการเข้าถึง (Access Control) โดยการกำหนดว่าการเข้าถึงจากระยะไกลประเภทไหนที่อนุญาตให้เข้าถึง หรือปฏิเสธการเข้าถึง

๒.๕) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง (Endpoint Security) สำหรับการทำงานจากระยะไกล และอุปกรณ์ไคลเอนต์ รวมถึงพิจารณาถึงการจัดการหรือการตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident) ที่เกี่ยวข้องกับการทำงานจากระยะไกลและการเข้าถึงจากระยะไกล และระบุไว้ในแผนความมั่นคงปลอดภัยของระบบให้ชัดเจน

๓) ขั้นตอนการนำไปใช้งาน (Implementation)

๓.๑) การเชื่อมต่อ (Connectivity) โดยจัดให้มีการตรวจสอบให้มั่นใจว่าผู้ทำงานจากระยะไกลสามารถเชื่อมต่อกับทรัพยากรทั้งหมดที่ได้รับอนุญาต และไม่สามารถเชื่อมต่อกับทรัพยากรอื่นได้และเข้าถึงข้อมูล และระบบตามสิทธิ์ที่ได้รับ

๓.๒) การป้องกัน (Protection) โดยจัดให้มีการตรวจสอบให้มั่นใจว่าข้อมูลที่ถูกส่งในเครือข่ายจะได้รับการป้องกันสอดคล้องกับข้อกำหนดของ ขร. ซึ่งรวมถึงข้อมูลที่ถูกส่งระหว่างอุปกรณ์ไคลเอนต์ สำหรับการทำงานจากระยะไกล (Telework Client Device) และเครื่องแม่ข่ายการเข้าถึงจากระยะไกล และข้อมูลที่ถูกส่งระหว่างเครื่องแม่ข่ายและทรัพยากรภายใน ขร. เช่น การเฝ้าติดตามการรับส่งข้อมูลเครือข่าย (Monitoring Network Traffic) หรือการตรวจสอบข้อมูลจราจรการรับส่งข้อมูล (Checking Traffic Log)

๓.๓) การพิสูจน์ตัวตน (Authentication) โดยกำหนดให้มีการบังคับใช้นโยบายการพิสูจน์ตัวตนทุกครั้งที่มีการเชื่อมต่อ และจัดให้มีการตรวจสอบให้มั่นใจว่าการพิสูจน์ตัวตนสามารถป้องกันการถูกโจมตีหรือถูกละเมิด เพื่อลดความเสี่ยงการเข้าถึงทรัพยากรภายในของ ขร.

๓.๔) แอปพลิเคชัน (Application) สำหรับการทำงานจากระยะไกลที่นำมาใช้งานต้องไม่ขัดขวางการทำงานของอุปกรณ์ไคลเอนต์สำหรับการทำงานจากระยะไกล เช่น ไคลเอนต์ VPN ที่ต้องทำงานร่วมกับไฟร์วอลล์บนโฮสต์ (Host-Based Firewall)

๓.๕) การจัดการ (Management) กำหนดให้ผู้ดูแลระบบต้องกำหนดค่ามั่นคงปลอดภัยและการทำงานของแอปพลิเคชัน (Application) สำหรับการทำงานจากระยะไกลให้มีประสิทธิภาพ รวมถึงส่วนประกอบอื่น ๆ เช่น เครื่องแม่ข่ายการเข้าถึงจากระยะไกล การพิสูจน์ตัวตน (Authentication Services) และซอฟต์แวร์ไคลเอนต์ การปรับใช้และการกำหนดค่า เช่น สามารถกำหนดค่าไคลเอนต์อัตโนมัติเต็มรูปแบบ (Fully Automated Client Configuration) ได้แทนการกำหนดค่าไคลเอนต์แต่ละเครื่องด้วยตัวผู้ดูแลระบบเอง

๓.๖) การเก็บข้อมูลจราจร (Logging) จัดให้มีการเก็บข้อมูลจราจรเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Event) ตามนโยบาย และแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของ ขร. รวมถึงพิจารณาให้มีการจัดเก็บข้อมูลอื่น ๆ เช่น การบันทึกการใช้งานแอปพลิเคชันแต่ละแอปพลิเคชัน

๓.๗) การตรวจสอบประสิทธิภาพ (Performance) โดยจัดให้มีการตรวจสอบประสิทธิภาพ และความเพียงพอสำหรับปริมาณการใช้งานปกติ และสำหรับปริมาณการใช้งานสูงสุด รวมถึงพิจารณาถึงประสิทธิภาพของอุปกรณ์ที่เป็นตัวกลาง เช่น เราเตอร์และไฟร์วอลล์ และส่วนประกอบต่าง ๆ โดยเฉพาะในช่วงการอัปเดตซอฟต์แวร์ขนาดใหญ่ ผ่านการทำงานและการเข้าถึงจากระยะไกล ซึ่งการดำเนินการทดสอบประสิทธิภาพ ควรพิจารณาทดสอบโดยการใช้ปริมาณงานที่สร้างขึ้นไว้เป็นต้นแบบ (Load of a Prototype) โดยใช้ตัวสร้างข้อมูลในเครือข่าย (Traffic) จำลองบนเครือข่ายทดสอบ (Live Test Network) เพื่อเลียนแบบลักษณะที่แท้จริงของทราฟฟิกที่คาดหวังและใกล้เคียงการใช้งานจริงที่สุด ซึ่งการทดสอบนี้ต้องรวมปริมาณงานของแอปพลิเคชันต่าง ๆ ที่จะถูกใช้ร่วมกับการทำงานและการเข้าถึงจากระยะไกล

๓.๘) ความมั่นคงปลอดภัยของการดำเนินการ (Security of the Implementation) ต้องจัดให้มีการอัปเดตด้วยแพตช์ล่าสุด และกำหนดค่าตามแนวทางปฏิบัติด้านความมั่นคงปลอดภัย รวมถึงการตรวจสอบค่าเริ่มต้น (Default Setting) อย่างละเอียดสำหรับการตั้งค่าการเข้าถึงจากระยะไกลแต่ละรายการ และแก้ไขการตั้งค่าตามความจำเป็น เพื่อรองรับข้อกำหนดด้านความมั่นคงปลอดภัย และจัดให้มีการประเมินช่องโหว่ของส่วนประกอบของระบบสำหรับการเข้าถึงจากระยะไกล

๔) ขั้นตอนการดำเนินงานและการบำรุงรักษา (Operation and Maintenance) เป็นกระบวนการดำเนินงาน (Operational Processes) เกี่ยวกับการดูแลระบบการทำงานหรือการเข้าถึงจากระยะไกลให้มีความมั่นคงปลอดภัย ๆ อย่างน้อยทุก ๖ เดือน หรือทุก ๑ ปี ตามระดับความเสี่ยงของการอนุญาตให้มีการทำงานระยะไกล โดยดำเนินการ ดังนี้

๔.๑) ดำเนินการตรวจสอบเจ้าของผลิตภัณฑ์เกี่ยวกับการอัปเดตโปรแกรม ในกรณีที่มีการประกาศการอัปเดตโปรแกรมรุ่นล่าสุดแล้ว ให้ ขร. หรือผู้ดูแลผลิตภัณฑ์ดำเนินการจัดหา (Acquiring) ทดสอบ (Testing) และใช้งานโปรแกรมรุ่นล่าสุด (Deploying)

๔.๒) ตรวจสอบให้แน่ใจว่าองค์ประกอบโครงสร้างพื้นฐานการเข้าถึงจากระยะไกลแต่ละรายการ เช่น เครื่องแม่ข่าย เกตเวย์ เครื่องแม่ข่ายการพิสูจน์ตัวตน ฯลฯ มีการตั้งเวลาที่ถูกต้อง เพื่อให้การประทับเวลา (Timestamp) ตรงกับระบบตั้งค่าเวลา

๔.๓) ดำเนินการตรวจสอบ และปรับเปลี่ยนการตั้งค่าการควบคุมการเข้าถึง (Access Control Setting) ตามความจำเป็น ตามเหตุการณ์ต่าง ๆ เช่น มีการเปลี่ยนแปลงนโยบาย มีการเปลี่ยนแปลงเทคโนโลยี มีข้อแนะนำหรือการสำรวจช่องโหว่ (Gap) จากการตรวจสอบ (Audit Findings) หรือมีความต้องการด้านความมั่นคงปลอดภัยใหม่

๔.๔) ตรวจจับและบันทึกความผิดปกติที่ตรวจพบภายในโครงสร้างพื้นฐานสำหรับการทำงาน หรือเข้าถึงจากระยะไกล ในกรณีที่พบความผิดปกติต้องนำรายงานไปยังผู้ดูแลระบบ และผู้ดูแลระบบอื่นที่เกี่ยวข้อง และดำเนินการประเมินการดำเนินงานเป็นระยะ ๆ อย่างน้อยทุก ๖ เดือน หรือทุก ๑ ปี ตามระดับความเสี่ยงของการอนุญาตให้มีการทำงานระยะไกล เช่น การประเมินอาจเป็นแบบแพสซิฟ (Passive) เช่น การตรวจสอบบันทึก หรือการประเมินแบบแอ็กทิฟ (Active) เช่น การสแกนช่องโหว่และการทดสอบการเจาะระบบ เป็นต้น

๕) ขั้นตอนการกำจัด (Disposal) กำหนดให้มีการลบข้อมูลที่มีความอ่อนไหวออกจากอุปกรณ์ไคลเอนต์หรือเครื่องแม่ข่ายสำหรับการเข้าถึงจากระยะไกลก่อนที่จะดำเนินการกำจัดหรือเลิกใช้อุปกรณ์ เช่น สัญญาเช่าเครื่องแม่ข่ายหมดอายุ หรือเมื่อเครื่องคอมพิวเตอร์ที่ล้าสมัยกำลังถูกรีไซเคิล เป็นต้น รวมถึงกำหนดให้มีการล้าง (Wipe) ข้อมูลออกจากอุปกรณ์ที่ถูกยืมโดยผู้ปฏิบัติงานจากระยะไกล โดยเฉพาะอย่างยิ่งเป็นการยืมสำหรับการเดินทาง และตรวจสอบให้แน่ใจว่าการล้างข้อมูลได้ดำเนินการล้างข้อมูลทุกจุดที่สามารถจัดเก็บข้อมูลได้ เช่น ซอฟต์แวร์ที่ทำงานภายใต้ Microsoft Windows มักจะเก็บข้อมูลที่อาจมีความสำคัญไว้ในรีจิสทรีของ Windows ในกรณีที่มีการจัดจ้างให้ผู้ให้บริการภายนอกดำเนินการล้างข้อมูลต้องกำหนดให้มีกรตรวจสอบการดำเนินการของผู้ให้บริการภายนอกหลังดำเนินการแล้วเสร็จ และจัดทำเอกสารการตรวจสอบไว้เป็นหลักฐาน

(L) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้มีการบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. โดยใช้มาตรการอย่างน้อย ดังนี้

๑) สื่อบันทึกข้อมูลทุกประเภท และทุกชนิด ต้องได้รับอนุญาตก่อนนำมาเชื่อมต่อทั้งหมด และห้ามนำสื่อบันทึกข้อมูลส่วนตัวมาเชื่อมต่อกับอุปกรณ์องค์กรโดยไม่ได้รับอนุญาต

๒) กำหนดให้มีการลงทะเบียนสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media Register) ก่อนนำไปใช้งาน รวมถึงกำหนดให้มีการบำรุงรักษา และการตรวจสอบการลงทะเบียนของสื่อเก็บข้อมูล แบบถอดได้เป็นประจำ อย่างน้อยทุก ๓ เดือน หรือ ๖ เดือนตามระดับความเสี่ยงที่นำไปใช้งานกับระบบหรือข้อมูล พร้อมทั้งจัดทำบันทึกการติดตามและตรวจสอบปรับปรุงทะเบียนทรัพย์สินนสำหรับสื่อเก็บข้อมูลแบบถอดได้ที่ได้รับอนุญาต

๓) ดำเนินการติดฉลากให้แก่สื่อเก็บข้อมูลแบบถอดได้ (ยกเว้นสื่อเก็บข้อมูลแบบถอดที่ติดตั้งถาวรภายใน อุปกรณ์ ICT) เพื่อให้ทราบถึงระดับความอ่อนไหว หรือชั้นความลับของข้อมูล รวมถึงช่วยให้มั่นใจ

ว่ามีการใช้มาตรการที่เหมาะสมในการจัดเก็บ การจัดการ และการนำไปใช้งาน โดยอาจจะดำเนินการติดป้ายสีเพื่อระบุความสำคัญแทนการติดเป็นข้อความ รวมถึงจัดการฝึกอบรมการใช้งานให้แก่บุคลากรอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๔) กำหนดให้มีการใช้สื่อเก็บข้อมูลแบบถอดได้เฉพาะกับระบบที่ได้รับอนุญาตให้ประมวลผล จัดเก็บหรือส่งข้อมูล โดยใช้สื่อเก็บข้อมูลแบบถอดเท่านั้น

๕) กำหนดให้มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญ บนสื่อบันทึกข้อมูลแบบถอดได้ รวบถึงหากเป็นในระดับชั้นความลับ ลับมากที่สุด ลับมาก ต้องพิจารณาดำเนินการอย่างน้อยดังนี้ เข้ารหัส (Encryption) ระบุผู้รับผิดชอบ (ผู้ถือครอง) และบันทึก ในทะเบียนสื่อบันทึกข้อมูล รวมถึงกำหนดให้มีการทบทวนการกำหนดระดับชั้นความลับให้กับสื่อเก็บข้อมูลแบบถอดได้อย่างสม่ำเสมอ

๒. กำหนดให้มีมาตรการในการปกป้องข้อมูล และความเป็นส่วนตัวให้กับข้อมูลที่จัดเก็บบนสื่อบันทึกข้อมูลที่ถอดได้ ดังนี้

๑) ติดตั้งโปรแกรมป้องกันไวรัสที่สามารถสแกนหาไวรัสและลบไวรัสออกจาก สื่อเก็บข้อมูลแบบถอดได้ หากมีการใช้สื่อใหม่ เช่น แฟลชไดรฟ์ USB หรือการ์ดหน่วยความจำ รวมถึงกำหนดให้ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมด ไม่มีมัลแวร์ (Malware) ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร.

๒) ปิดการใช้งานคุณสมบัติการเล่นอัตโนมัติและการเปิดใช้งานอัตโนมัติของคอมพิวเตอร์ (Disable Computer's Autoplay and Auto-Run Features) ก่อนที่จะเชื่อมต่อสื่อแบบถอดได้เข้ากับคอมพิวเตอร์ เพื่อป้องกันคอมพิวเตอร์จากการเปิดโฟลเดอร์ที่มีไวรัส โดยอัตโนมัติ

๓) จัดให้มีการใส่รหัสผ่านป้องกันอุปกรณ์สื่อเก็บข้อมูลแบบถอดได้ (Password Protect Removable Storage Media Devices) เพื่อควบคุมการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต รวมถึงตรวจสอบให้แน่ใจว่าการใช้รหัสผ่านมีความรัดกุมและป้องกันรหัสผ่านไม่ให้รั่วไหล

๔) ไม่ทิ้งสื่อบันทึกข้อมูลไว้โดยไม่มีบุคคลดูแล หรือถูกเก็บในที่ที่อาจถูกขโมยได้ง่าย เช่น โต๊ะทำงาน รวมถึงทำให้มั่นใจว่าการเข้าถึงสื่อบันทึกข้อมูลต้องใช้รหัสผ่านเสมอ

๕) กำหนดให้มีการเข้ารหัสข้อมูล หากมีข้อมูลที่อ่อนไหวหรือความลับในสื่อเก็บข้อมูลแบบถอดได้ เช่น ข้อมูลที่มีชั้นความลับในระดับลับมากหรือระดับลับที่สุดของ ขร. หรือข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ เช่น ข้อมูลการตั้งค่าระบบ เป็นต้น

๖) กำหนดเจ้าของสื่อเก็บข้อมูลแบบถอดได้ให้ชัดเจน เช่น ชื่อบุคคลที่รับผิดชอบ ชื่อหน่วยงานที่รับผิดชอบ และห้ามบุคลากรที่ไม่เกี่ยวข้องใช้สื่อเก็บข้อมูลแบบถอดได้ และหากสื่อเก็บข้อมูลไม่สามารถระบุเจ้าของหรือบุคลากรที่รับผิดชอบได้ ไม่อนุญาตให้ใช้งานสื่อบันทึกนั้น

๗) ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

๘) กำหนดให้มีการทำลายสื่อบันทึกข้อมูล โดยพิจารณาดำเนินการดังนี้

(๑) ดำเนินการประเมินระดับชั้นความลับของข้อมูลก่อนทำลาย

(๒) กำหนดวิธีการทำลายข้อมูลให้สอดคล้องกับระดับชั้นความลับของข้อมูลในแต่ละลำดับชั้น พร้อมทั้งจัดให้มีหลักฐานการทำลายข้อมูล พร้อมทั้งกำหนดให้มีการลงนามโดยผู้มีอำนาจอนุมัติทำลายข้อมูล

(๓) ในกรณีที่มีการจัดจ้างผู้ให้บริการภายนอกทำลายสื่อบันทึก ควรพิจารณาจัดจ้างผู้ให้บริการที่ได้รับการรับรอง พร้อมทั้งกำหนดให้มีการกำหนดรูปแบบการทำลาย พร้อมวิธีการทำลายให้ฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายก่อนดำเนินการทำลาย

๙) กำหนดให้ใช้สื่อเก็บข้อมูลแบบถอดได้แบบเขียนครั้งเดียว (Write-once Media) ในการถ่ายโอนข้อมูลระหว่างระบบที่อยู่โดเมนความปลอดภัยที่แตกต่างกัน และกำหนดมาตรการป้องกันข้อมูลรั่วไหลหรือเข้าถึงโยไม่ได้รับอนุญาตอย่างเหมาะสม เช่น การใช้คอมแพคดิสก์ที่ไม่สามารถเขียนซ้ำได้ (Non-Rewritable Compact Discs) เป็นต้น ในกรณีที่ไม่สามารถใช้สื่อเก็บข้อมูลแบบถอดได้บันทึกแบบครั้งเดียวในการถ่ายโอนข้อมูลระหว่างระบบ ควรตรวจสอบให้แน่ใจว่าระบบปลายทางมีกลไกการเข้าถึงแบบอ่านอย่างเดียวได้ (Read-only Access) เช่น ผ่านอุปกรณ์แบบอ่านอย่างเดียวหรือตัวบล็อกการเขียนด้วยฮาร์ดแวร์ (Read-only Device or Hardware Write-blocker) และควรกำหนดให้มีการลบ (Sanitize) ข้อมูลทั้งหมดจากสื่อยบันทึกข้อมูลหลังการถ่ายโอนข้อมูลแต่ละครั้ง

๑๐) กำหนดบุคลากรที่มีหน้าที่ตรวจสอบการเชื่อมต่อให้ชัดเจน โดยมีหน้าที่ อย่างน้อยดังนี้

(๑) ทบทวนและตอบสนองต่อข้อมูลที่แจ้งเกี่ยวกับการเชื่อมต่อที่ผิดปกติ เช่น ข้อมูลการแจ้งเตือนจากระบบปฏิบัติการ จาก Endpoint Detection and Response (EDR) หรือจาก Security Information and Event Management (SIEM)) ภายในระยะเวลาที่เหมาะสม

(๒) ดำเนินการปรับปรุง (Update) ซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ตามนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ขร.

(๓) จัดทำรายงานการตรวจสอบการเชื่อมต่อสื่อบันทึกข้อมูล เพื่อให้ผู้บังคับบัญชาทบทวนหลังจากที่การดำเนินการตรวจสอบแล้วเสร็จภายใน ๑ สัปดาห์

๑๑) กำหนดให้มีการตรวจสอบการควบคุมการเชื่อมต่อของสื่อบันทึกข้อมูลแบบถอดได้กับบริการที่สำคัญ เพื่อให้แน่ใจว่ามีการดำเนินการ อย่างน้อย ดังนี้

ก) ในกรณีที่สามารถปิดใช้งานได้ ให้ปิดใช้งานพอร์ตสำหรับการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และเปิดใช้งานก็ต่อเมื่อจำเป็นเท่านั้น

(ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตและกำหนดไว้ในนโยบายหรือแนวปฏิบัติของหน่วยงานเท่านั้น

(ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้ทั้งหมดไม่มีไวรัสหรือมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ง) กำหนดให้ผู้ปฏิบัติงานทำการตรวจสอบ โดยเปรียบเทียบการตั้งค่าการใช้งานพอร์ตและการอนุญาตให้ชื่อสื่อบันทึกข้อมูลตามมาตรการข้อ (ก) และ (ค)

(จ) มีซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ พร้อมตั้งค่าให้ทำงานทุกครั้งที่มีการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ กับบริการที่สำคัญของ ขร.

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. ในกรณีที่มีการขนย้ายสื่อบันทึกข้อมูล ควรพิจารณาดำเนินการดังนี้

(๑) จัดให้มีบรรจุภัณฑ์ที่มั่นคงและปิดผนึก

(๒) กำหนดให้ใช้วิธีการเคลื่อนย้ายที่สามารถตรวจสอบได้ เช่น มีหลักฐานการรับ และหลักฐานการส่งสื่อบันทึกข้อมูลโดยการลงนามรับและส่ง เป็นต้น

(๓) ข้อมูลที่อยู่ในระดับชั้นความลับในชั้น “ลับมากที่สุด” “ลับมาก” ควรดำเนินการขนย้ายโดยผู้ปฏิบัติงานที่ได้รับมอบหมายโดยเฉพาะ พร้อมทั้งบันทึกเส้นทางการเคลื่อนย้าย

(๔) ห้ามทิ้งสื่อบันทึกข้อมูลไว้ โดยไม่มีผู้ดูแลในพื้นที่สาธารณะหรือยานพาหนะ

(ม) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้ดำเนินการจัดทำขั้นตอนการประเมินช่องโหว่ของระบบ ประกอบด้วยอย่างน้อย ๖ ขั้นตอน ดังนี้

(๑) การกำหนดขอบเขต (Scoping) โดยขอบเขตการประเมินต้องได้รับความเห็นชอบจากผู้ดำเนินการประเมินและผู้รับการประเมิน โดยจะต้องระบุรายละเอียดเกี่ยวกับทรัพย์สินที่จะตรวจสอบ กฎของการประเมิน และความต้องการของผู้รับการประเมิน ซึ่งขอบเขตของการประเมินควรครอบคลุมดังนี้

- การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review) เพื่อให้แน่ใจว่าสอดคล้องกับการดำเนินงานของ ขร. ต้องรวมถึงสถาปัตยกรรมของระบบสารสนเทศที่เกี่ยวข้องกับบริการสำคัญ เช่น เครื่องคอมพิวเตอร์แม่ข่าย (Server), เครื่องคอมพิวเตอร์ลูกข่าย (Client), ระบบเครือข่าย และการแบ่งแยกเครือข่าย (Network Segmentation)
- การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment) ที่เกี่ยวข้องกับบริการสำคัญ
- การประเมินความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ (Host Security Assessment) แม่ข่ายที่มีความสำคัญและเป็นเป้าหมายของการโจมตี

(๒) ขั้นตอนการสแกน (Scanning) เป็นการตรวจสอบทรัพย์สินเพื่อหาช่องโหว่หรือส่วนที่ไม่ปฏิบัติตามข้อกำหนด และอาจเป็นอันตรายต่อความมั่นคงปลอดภัยของสารสนเทศ ซึ่งการทดสอบความมั่นคงปลอดภัยของคอมพิวเตอร์ ระบบเครือข่าย ซอฟต์แวร์ หรือระบบอื่น ๆ สามารถทำได้ทั้งด้วยเครื่องมือสแกนอัตโนมัติ หรือการประเมินด้วยตนเอง โดยสามารถพิจารณาดำเนินการดังนี้

- การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review) สามารถดำเนินการได้ ดังนี้

o ตรวจสอบผังกระบวนการหรือไดอะแกรมที่แสดงการเข้าถึงบริการสำคัญและการเชื่อมโยงไปยังระบบต่าง ๆ

o พิจารณาสถาปัตยกรรมของระบบสารสนเทศที่เกี่ยวข้องกับบริการสำคัญ เช่น ระบบเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์ต่าง ๆ

o ใช้มาตรการป้องกันหลายชั้น ตามหลักการป้องกันเชิงลึก (Defense in Depth) เพื่อลดความเสี่ยง

o พิจารณาการแบ่งแยกเครือข่าย (Network Segmentation) เพื่อให้เครือข่ายของบริการสำคัญมีอุปกรณ์ที่เกี่ยวข้องและมีความปลอดภัยเข้ามาในเครือข่ายเท่านั้น

o พิจารณาออกแบบระบบให้มีความพร้อมใช้สูง (High Availability: HA) เพื่อให้บริการมีความเสถียรและไม่หยุดชะงัก

- การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment ควรกำหนดขอบเขตการประเมิน ดังนี้

o การประเมินนโยบายและแนวปฏิบัติเพื่อป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต ทั้งในเครือข่ายส่วนตัว (Private Network) และเครือข่ายสาธารณะ (Public Network)

o การระบุทรัพย์สินที่ไม่ได้ลงทะเบียน

o การระบุข้อผิดพลาดในการตั้งค่า

o การป้องกันการเข้าถึงเครือข่าย

- การประเมินความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ (Host Security Assessment)

o ประเมินช่องโหว่อิงตามข้อมูลช่องโหว่ของแต่ละผลิตภัณฑ์ซึ่งประกาศโดยผู้ผลิต หรือจากช่องโหว่ที่เคยเกิดขึ้นมาแล้วจากข้อมูลข่าวกรอง (Threat Intelligence)

o ขอบเขตการประเมินควรรวมถึงการเรียกข้อมูลระบบปฏิบัติการและแพตช์ของแอปพลิเคชัน การระบุการกำหนดสิทธิในระบบไฟล์ที่ไม่ถูกต้อง การตรวจสอบนโยบายบัญชี และรหัสผ่าน การวิเคราะห์การตั้งค่าควบคุมต่าง ๆ (Configuration) เป็นต้น

(๓) ขั้นตอนการประเมิน (Evaluation) โดยดำเนินการจัดหมวดหมู่ตามความรุนแรงของภัยคุกคาม และการจัดลำดับความสำคัญ (Prioritization) หลังจากที่ช่องโหว่ถูกค้นพบในระหว่างการสแกนช่องโหว่ ซึ่งขั้นตอนการจัดลำดับความสำคัญของช่องโหว่ด้านระบบสารสนเทศอาจใช้ Common Vulnerability Scoring System (CVSS) โดยระบุคะแนนเกี่ยวกับความรุนแรงของข้อบกพร่อง รวมถึงข้อมูลวิธีการหาประโยชน์จากข้อบกพร่อง

(๔) ขั้นตอนการรายงาน (Reporting) เป็นขั้นตอนที่ดำเนินการเมื่อการประเมินเสร็จสมบูรณ์ โดยรายละเอียดของรายงานจะระบุช่องโหว่ที่พบ มาตรการแก้ไขที่สามารถเลือกได้ รวมถึงเป็นหลักฐานในการดำเนินการประเมินช่องโหว่ของระบบ

(๕) ขั้นตอนการแก้ไข (Remediation) เป็นการดำเนินการแก้ไขช่องโหว่ หรือยอมรับความเสี่ยงหากไม่สามารถแก้ไขได้ โดยรายละเอียดในรายงานจะแสดงมาตรการแก้ไขสำหรับช่องโหว่ที่พบ ซึ่งช่องโหว่จะต้องได้รับการแก้ไข และแพตช์ตามระดับความวิกฤต และช่องโหว่ที่มีความวิกฤตสูงควรได้รับการแก้ไขทันที

(๖) ขั้นตอนการสแกนซ้ำ (Rescanning) เมื่อช่องโหว่ได้รับการแก้ไขและแพตช์แล้ว ต้องดำเนินการถูกสแกนซ้ำ เพื่อตรวจสอบให้แน่ใจว่าไม่มีช่องโหว่เพิ่มเติม

๒. กำหนดให้ดำเนินการสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ เช่น ตรวจสอบสถานะของการแก้ไขช่องโหว่ และปรับปรุงรายงานการตรวจสอบช่องโหว่ และดำเนินการสแกนซ้ำหลังจากการแก้ไขช่องโหว่ รวมถึงจัดให้มีการสำรองข้อมูล เพื่อป้องกันความสูญเสียที่อาจเกิดขึ้นระหว่างการแก้ไขช่องโหว่ และกำหนดให้มีการเรียนรู้จากช่องโหว่ที่พบ เพื่อป้องกันไม่ให้เกิดขึ้นอีก เป็นต้น

๓. กำหนดให้มีการสแกนช่องโหว่ (Vulnerability Scanner) อย่างปีละ ๑ ครั้ง หรือขึ้นอยู่กับความสำคัญของบริการ หรือระบบตามระดับความเสี่ยงประเมินช่องโหว่ของบริการที่สำคัญ และระบบงานที่สำคัญของ ขร. โดยอ้างอิงตามหลักการบริหารความเสี่ยงของ ขร. อย่างปีละ ๑ ครั้ง เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญ และระบบงานที่สำคัญของ ขร.

๔. ประเมินช่องโหว่ของบริการที่สำคัญ และระบบงานที่สำคัญของ ขร. เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี โดยพิจารณาดำเนินการอย่างน้อย ดังนี้

(๑) วิเคราะห์ผลกระทบของช่องโหว่ที่มีต่อระบบ และข้อมูล รวมถึงจัดลำดับความสำคัญของการแก้ไขช่องโหว่

(๒) กำหนดหลักเกณฑ์ที่ชัดเจน เช่น Critical, High, Medium, Low เพื่อนำมากำหนดระดับเร่งด่วนในการแก้ไขช่องโหว่

(๓) ดำเนินการอัปเดตแพตช์หรือเปลี่ยนแปลงการตั้งค่าอย่างเหมาะสม เพื่อแก้ไขช่องโหว่

(๔) ดำเนินการทดสอบแพตช์ในระบบทดสอบก่อนนำไปใช้งานจริง (Patch Testing & Rollout Plan)

(๕) จัดให้มีการบันทึกผลการดำเนินการบริหารจัดการช่องโหว่ตั้งแต่เริ่มต้น จนถึงการรายงานผลการติดตามการจัดการช่องโหว่

๕. กำหนดให้มีการทดสอบเจาะระบบ (Penetration Testing) โดยพิจารณาอย่างน้อยดังนี้

๑) พิจารณาจัดทำขั้นตอนสำหรับการทดสอบการเจาะระบบ (Penetration Testing Phases) ซึ่งประกอบด้วย ขั้นตอนดังนี้ การวางแผน การสำรวจ การโจมตี และการรายงาน

๒) พิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) สำหรับบริการที่สำคัญ และระบบงานที่สำคัญของ ขร. โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบ

๓) ตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ โดยเฉพาะอย่างยิ่งทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๔) พิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อย ๑ ปีครั้ง ตามความจำเป็น เช่น มีการเปลี่ยนแปลงระดับความเสี่ยงเพิ่มขึ้นเกินกว่าระดับความเสี่ยงที่ยอมรับได้มีการเปลี่ยนแปลงลักษณะของภัย

คุกคามทางไซเบอร์ เป็นต้น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ซึ่งในการดำเนินการทดสอบเจาะระบบอาจเกิดจากกรณี ดังนี้

- ก่อนทำการทดสอบระบบใหม่
- เพิ่มโครงสร้างพื้นฐาน เครือข่าย หรือแอปพลิเคชันใหม่
- อัพเกรดหรือการปรับเปลี่ยนที่สำคัญที่จะนำไปใช้กับโครงสร้างพื้นฐานหรือแอปพลิเคชันของบริการที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี
- จัดตั้งสำนักงานแห่งใหม่
- ใช้แพตช์ใหม่ในการรักษาความมั่นคงปลอดภัย
- การเปลี่ยนแปลงนโยบายด้านการรักษาความมั่นคงปลอดภัย เป็นต้น

๕) ตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบ และผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ

ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบต้องได้รับการรับรองมาตรฐานผู้ทดสอบระดับบริหารจัดการ และระดับปฏิบัติการที่ยอมรับ โดยทั่วไปมีดังต่อไปนี้

- ระดับบริหารจัดการ (Security Management level) เช่น
  (๑) Certified Information Systems Security Professional (CISSP)
  (๒) Certified Information Security Manager (CISM)
  (๓) Certified Information Systems Auditor (CISA)
- ระดับปฏิบัติการ (Penetration Tester Level) เช่น
  (๑) ประกาศนียบัตรการรับรองจากสถาบัน CompTIA เช่น CompTIA Pentest+ เป็นต้น
  (๒) ประกาศนียบัตรการรับรองจากสถาบัน EC-Council เช่น EC-Council’s Certified Penetration Testing Professional (C|PENT), Certified Ethical Hacker (CEH), Licensed Penetration Tester (LPT) เป็นต้น
  (๓) ประกาศนียบัตรการรับรองจากสถาบัน ISACA เช่น CSX Cybersecurity Practitioner (CSX-P) เป็นต้น
  (๔) ประกาศนียบัตรการรับรองจากสถาบัน Mile๒ เช่น CERTIFIED Penetration Testing Engineer (C)PTE) เป็นต้น
  (๕) ประกาศนียบัตรการรับรองจากสถาบัน Council for Registered Ethical Security Testers (CREST) เช่น CREST Registered Penetration Tester, CREST Certified Web Application Tester, CREST Certified Infrastructure Tester เป็นต้น
  (๖) ประกาศนียบัตรการรับรอง จากสถาบัน Offensive Security เช่น OSCP, OSWP, OSCE, OSEE และ OSWE เป็นต้น

(๗) ประกาศนียบัตรการรับรองจากสถาบัน Global Information Assurance Certification (GIAC) เช่น GCIH, GMOB, GPEN, GXPN, GAWN และ GWAPT

๖) ตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมด โดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของ ขร.

๗) จัดให้มีกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไข

๘) หากได้รับการร้องขอจาก กกม. หรือ สกมช. ให้ดำเนินการส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ ตามระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ ขร. ไปยัง สกมช. ขร. จะดำเนินการภายในกำหนด ๓๐ วัน นับแต่วันที่ได้รับหนังสือด้วย

๖. เมื่อการทดสอบแล้วเสร็จ (Post-testing Activity) ต้องดำเนินการตามขั้นตอนแก้ไข และติดตามช่องโหว่ เพื่อแก้ไขช่องโหว่ที่ได้พบ โดยทำการวิเคราะห์ผลลัพธ์จากการสแกนช่องโหว่ และดำเนินการจัดหามาตรการแก้ไข และจัดทำรายงานที่ระบุถึงช่องโหว่ของระบบ ช่องโหว่ของเครือข่าย และช่องโหว่อื่น ๆ พร้อมกับข้อแนะนำในการดำเนินการแก้ไข หรือลดผลกระทบโดยเปรียบเทียบการดำเนินการลดผลกระทบที่อาจเกิดขึ้นกับข้อกำหนดในการปฏิบัติงาน รวมถึงจัดเก็บไว้เป็นหลักฐานให้กับผู้ที่เกี่ยวข้อง เช่น ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (Chief Information Security Officer: CISO) และเจ้าหน้าที่ด้านการรักษาความมั่นคงปลอดภัยตลอดจนเจ้าของระบบที่เกี่ยวข้องสามารถเข้าถึงได้

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการค้นหาและตรวจสอบช่องโหว่ โดยพิจารณาอย่างน้อยดังนี้

๑) ติดตามข้อมูลช่องโหว่จากมาตรฐาน หรือหน่วยงานสากลที่น่าเชื่อถือ เช่น CVE, NVD, CERT และ Vendor Advisory เป็นต้น

๒) ตรวจสอบข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่มีการประกาศบนเว็บไซต์หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่าง ๆ ที่มีการใช้งานบนระบบสารสนเทศของหน่วยงาน หรือจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติ (ThaiCERT)

๓) กำหนดให้มีการการควบคุมช่องโหว่ที่ยังไม่สามารถแก้ไขได้ทันที โดยพิจารณาอย่างน้อย ดังนี้

(๑) กำหนดมาตรการลดความเสี่ยง (Compensating Controls) เช่น ปิดพอร์ตชั่วคราว แยกระบบจากเครือข่ายหลัก หรือเปิดใช้งานระบบเฝ้าระวัง (IDS/IPS) เป็นต้น

(๒) ดำเนินการติดตามสถานะของช่องโหว่ที่ยังไม่ได้รับการแก้ไข หรือจัดการจนกว่าจะสามารถดำเนินการแก้ไขได้อย่างถาวร พร้อมทั้งจัดให้มีการรายงานการติดตามช่องโหว่ที่ยังไม่ได้รับการแก้ไข

(N) การจัดการผู้ให้บริการภายนอก (Third Party Management)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้ดำเนินการรแยกประเภทห่วงโซ่อุปทานของผู้ให้บริการภายนอกด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Supply Chain) เช่น IT and cybersecurity service providers, Telecommunications service providers, Cloud platforms, OT hardware products, IoT /IIOT hardware products, IT hardware products (e.g., firewalls, computers, mobile devices), IT software products (e.g., enterprise software, cybersecurity software, database technologies, operating systems) และที่ไม่ใช่ด้านความมั่นคงปลอดภัยไซเบอร์ (Non-Cyber Supply Chain) เช่น Providers of consumables (e.g., stationery, catering, food), Office furniture (e.g., desks, chairs, cabinets), Contractors and service providers ที่ไม่ได้ให้บริการโดยตรงเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น การบริหารจัดการอาคาร

๒. กำหนดให้ต้องดำเนินการการกำกับดูแลการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกอย่างต่อเนื่อง และสอดคล้องตามกรอบและกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ ขร. (IT Risk Management) เพื่อให้ความเสี่ยงอยู่ในระดับที่หน่วยงานยอมรับได้ และกำหนดให้มีระเบียบวิธีปฏิบัติที่ชัดเจนและเป็นลายลักษณ์อักษรครอบคลุมวัฏจักรการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Life Cycle) ตั้งแต่การประเมินความเสี่ยง การคัดเลือกผู้ให้บริการภายนอก การจัดทำสัญญาหรือข้อตกลง การติดตามผลการปฏิบัติงานอย่างต่อเนื่องและการยกเลิก/สิ้นสุดสัญญาหรือข้อตกลง รวมถึงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๓. กำหนดมีการจัดทำนโยบายการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกอย่างชัดเจนเป็นลายลักษณ์อักษร และสอดคล้องกับนโยบายอื่นที่เกี่ยวข้องของ ขร. เช่น นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น ซึ่งการจัดทำนโยบายการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกอาจเป็นนโยบายที่จัดทำขึ้นเฉพาะ หรืออาจจะกำหนดอยู่ในนโยบายอื่นที่มีอยู่แล้วของ ขร.

๔. นโยบายการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกควรครอบคลุมประเด็น ดังต่อไปนี้

๑) โครงสร้างการกำกับดูแล และบทบาทหน้าที่ของผู้เกี่ยวข้องในการกำกับดูแลและบริหารจัดการ ความเสี่ยงจากผู้ให้บริการภายนอก

๒) หลักเกณฑ์การจัดระดับความเสี่ยงและระดับความสำคัญของบริการหรือข้อมูลที่เปิดให้ผู้ให้บริการภายนอกเข้าใช้ เชื่อมต่อหรือเข้าถึง

๓) การบริหารจัดการความเสี่ยงที่ครอบคลุมวงจรการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Life Cycle) และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่ครอบคลุมตามหลักการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วนของข้อมูล และความพร้อมใช้งาน (Availability)

๔) หลักเกณฑ์การขออนุมัติความเห็นชอบ และการรายงานต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย ซึ่งหมายถึง กระบวนการที่หน่วยงานต้องดำเนินการเพื่อขออนุมัติจากผู้มีอำนาจ เช่น คณะกรรมการหรือผู้บริหารระดับสูงก่อนที่จะดำเนินการใด ๆ ที่เกี่ยวข้องกับการใช้บริการจากผู้ให้บริการภายนอก โดยจะต้องมีการรายงานรายละเอียดต่าง ๆ ที่เกี่ยวข้องกับการใช้บริการ เช่น ข้อมูลเกี่ยวกับบริการที่

ให้ผู้ให้บริการภายนอกเข้าถึง ความเสี่ยงที่อาจเกิดขึ้น วิธีการจัดการความเสี่ยง และแนวทางการบริหารจัดการการเชื่อมต่อหรือการเข้าถึงข้อมูลของ ขร. ซึ่งกระบวนการนี้จะช่วยให้ผู้บริหารและคณะกรรมการสามารถตัดสินใจได้อย่างมีข้อมูลครบถ้วน และสามารถตรวจสอบความเหมาะสมของการใช้บริการภายนอกได้อย่างมีประสิทธิภาพ เพื่อให้มั่นใจว่าไม่มีความเสี่ยงที่อาจเกิดขึ้นจากการให้ผู้ให้บริการภายนอกเข้าถึงข้อมูลหรือระบบที่สำคัญของ ขร.

๕) การตรวจสอบการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก

๖) การเตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อ ขร. อย่างมีนัยสำคัญ เพื่อให้ ขร. สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ซึ่งรวมถึงการเตรียมข้อมูลให้พร้อมใช้สำหรับการดำเนินธุรกิจและการให้บริการแก่ผู้ใช้งาน หรือผู้รับบริการของ ขร. ได้อย่างต่อเนื่อง

๗) การคุ้มครองผู้ใช้งาน หรือผู้รับบริการของ ขร.

๕. นโยบายการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกต้องได้รับการอนุมัติจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๖. กำหนดให้มีการสื่อสารนโยบายให้ผู้ที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง และควบคุมดูแลให้ผู้ที่เกี่ยวข้องปฏิบัติตามนโยบายอย่างเคร่งครัด

๗. จัดให้มีมาตรฐานและระเบียบวิธีปฏิบัติ เพื่อสนับสนุนการดำเนินการตามนโยบายการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกให้สอดคล้องกับระดับความเสี่ยง และระดับความสำคัญของบริการหรือข้อมูลที่เปิดให้ผู้ให้บริการภายนอกเข้าใช้ เชื่อมต่อหรือเข้าถึง รวมถึงสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป

๘. การประเมินความเสี่ยงจากการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก ต้องพิจารณาดำเนินการ ดังนี้

๑) ต้องประเมินความเสี่ยงและผลกระทบทั้งก่อนการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมถึงดำเนินการประเมินเป็นประจำอย่างน้อยปีละ ๑ ครั้ง โดยต้องมีผลการประเมินเป็นลายลักษณ์อักษร และคำนึงถึงความเสี่ยงดังต่อไปนี้

(๑) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ซึ่งหมายถึง ความเสี่ยงที่เกิดขึ้นจากการตัดสินใจ หรือการดำเนินกลยุทธ์ที่ไม่เหมาะสม หรือการเปลี่ยนแปลงในสภาพแวดล้อมทางบริบทของ ขร. ที่อาจส่งผลกระทบต่อความสามารถในการบรรลุเป้าหมายและวัตถุประสงค์ของ ขร. เช่น การเลือกใช้ผู้ให้บริการภายนอก ที่ไม่ตรงกับเป้าหมาย และวัตถุประสงค์การดำเนินการของ ขร. หรือการเปลี่ยนแปลงของการดำเนินการตามภาระกิจหน้าที่ของ ขร. ที่ไม่สามารถตอบสนองต่อความต้องการ หรือคาดหวังของการเปลี่ยนแปลงที่เกิดขึ้นได้ ตัวอย่างของความเสี่ยงด้านกลยุทธ์ เช่น การเลือกใช้ผู้ให้บริการภายนอกที่ไม่สามารถปรับตัวได้ตามความต้องการของ ขร. หรือไม่สามารถพัฒนาเทคโนโลยีใหม่ ๆ ตามที่ ขร. ต้องการ, การเปลี่ยนแปลงกลยุทธ์ของ ขร. ที่ทำให้บริการจากผู้ให้บริการภายนอกไม่ตอบสนองต่อทิศทางใหม่ของ ขร., ความไม่ตรงกับวิสัยทัศน์ระยะยาวของ ขร. จากการเลือกผู้ให้บริการภายนอก หรือพันธมิตรที่ไม่เหมาะสม

(๒) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการผู้ให้บริการภายนอกที่ไม่ครอบคลุมทุกขั้นตอนที่ผู้ให้บริการภายนอกดำเนินการ

(๓) ความเสี่ยงด้านชื่อเสียง (Reputation Risk) เช่น ความขัดข้องของระบบหรือบริการที่ดำเนินการร่วมกับผู้ให้บริการภายนอกอาจส่งผลกระทบต่อการให้บริการ รวมถึงชื่อเสียงและความน่าเชื่อถือของหน่วยงาน เป็นต้น

(๔) ความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ เช่น ระบบขัดข้อง หรือหยุดบริการ โดยมีสาเหตุจากผู้ให้บริการภายนอก ระบบของผู้ให้บริการภายนอกมีช่องโหว่ด้านความปลอดภัย ทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล ผู้ให้บริการภายนอกเข้าใช้งานด้วยสิทธิสูงเกินกว่าที่ได้รับอนุญาต การจัดเตรียมทรัพยากรระบบมีไม่เพียงพอต่อการใช้งาน เป็นต้น

(๕) ความเสี่ยงด้านกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น การปฏิบัติไม่ถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติลิขสิทธิ์ และ The EU General Data Protection Regulation (GDPR) เป็นต้น

(๖) ความเสี่ยงของประเทศที่ผู้ให้บริการภายนอกตั้งอยู่หรือประกอบธุรกิจ (Country /Cross Border Risk) เช่น การไม่สามารถเข้าถึงข้อมูลอันเนื่องมาจากการขัดข้องหรือการปิดกั้นเครือข่ายการสื่อสาร ระหว่างประเทศ เป็นต้น

(๗) ความเสี่ยงที่เกี่ยวข้องกับสัญญาหรือข้อตกลง เช่น ความไม่ครอบคลุม ความไม่ชัดเจน และความไม่ครบถ้วนสมบูรณ์ของสัญญาหรือข้อตกลง เป็นต้น

(๘) ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีของผู้ให้บริการหรือพันธมิตรทางธุรกิจ (Partner) และข้อจำกัดของ ขร. ในการนำระบบหรือข้อมูลกลับมาดำเนินการ

(๙) ความเสี่ยงจากการกระจุกตัว (Concentration Risk) เช่น หน่วยงานที่มีภารกิจหน้าที่ในลักษณะเดียวกันมีการใช้บริการจากผู้ให้บริการภายนอกเพียงรายเดียว (Single Provider) เป็นต้น

(๑๐) ความเสี่ยงจากผู้ให้บริการภายนอกโดยมีผู้ว่าจ้างผู้อื่นมาดำเนินการแทน (Subcontractor) เช่น Subcontractor มีการปฏิบัติงานที่เกิดข้อบกพร่อง เป็นต้น

๒) ต้องจัดให้มีการควบคุมและบริหารจัดการความเสี่ยงที่สามารถครอบคลุมวัฏจักรการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Life Cycle) ตั้งแต่การคัดเลือก การจัดทำสัญญาหรือข้อตกลงการติดตามผลการปฏิบัติงานอย่างต่อเนื่อง ตลอดจนการยกเลิก/สิ้นสุดสัญญา หรือข้อตกลง รวมถึงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๓) ต้องมีการกำหนดหลักเกณฑ์ที่ชัดเจนสำหรับการจัดระดับความเสี่ยง และระดับความสำคัญเพื่อวางแผนการจัดการความเสี่ยง

๔) ต้องจัดทำทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องให้ครอบคลุมครบถ้วนตามที่กำหนดในหัวข้อ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการใช้บริการ การเชื่อมต่อหรือการเข้าถึง ข้อมูลจากผู้ให้บริการภายนอก ข้อ ๑) จัดทำทะเบียนการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้หน่วยงานสามารถ ใช้ดำเนินการบริหารจัดการความเสี่ยง ติดตาม และตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอกได้ครบถ้วนและมีความต่อเนื่อง

๕) ดำเนินการประเมินความเสี่ยง โดยอาจพิจารณาใช้ทั้งการประเมินจากภายใน และการประเมินจากภายนอก รวมถึงพิจารณาใช้ระบบสำหรับการประเมินความเสี่ยง และดำเนินการติดตาม และประเมินผลการประเมินอย่างต่อเนื่องระหว่างการใช้บริการ ดังต่อไปนี้

(๑) การประเมินจากภายในหน่วยงาน (Internal Assessment) หมายถึง การรวบรวมข้อมูลจากบุคลากรภายในหน่วยงาน เช่น การสัมภาษณ์หรือการกรอกแบบสอบถาม โดยพิจารณาดำเนินการดังนี้

- จัดให้มีแพลตฟอร์มและมาตรฐานคำถามที่ชัดเจน (Standard Template) สำหรับสร้างแบบสอบถามที่สามารถปรับแต่งให้เหมาะสมกับบริบทของ ขร. เช่น แบบสอบถามเกี่ยวกับความเสี่ยงที่เกิดจากการใช้บริการจากผู้ให้บริการภายนอก เป็นต้น
- จัดให้มีแบบสอบถามสำหรับเหตุการณ์เฉพาะ (Event-specific Questionnaires) โดยการสร้างแบบสอบถามที่เกี่ยวข้องกับเหตุการณ์ใหม่ ๆ ที่อาจเกิดขึ้น เช่น เมื่อมีข่าวภัยคุกคามใหม่ ๆ เช่น การค้นพบช่องโหว่ใหม่ๆ การแก้ไขช่องโหว่ใหม่ๆที่เกิดขึ้นของผู้ให้บริการภายนอก เป็นต้น

(๒) การประเมินจากภายนอกด้วยการตรวจสอบพื้นผิวการโจมตี (External Assessment with Attack Surface Testing) หมายถึง การตรวจสอบระบบจากภายนอกหน่วยงาน เพื่อหาจุดอ่อนที่อาจถูกโจมตี ซึ่งจะทำได้โดยวิธีที่ไม่เป็นการบุกรุก (Non-intrusive) ดังนี้

- ดำเนินการตรวจสอบพื้นผิวการโจมตี เช่น การค้นหาจากโดเมน หรือการตรวจสอบกลุ่ม IP Address ที่ใช้งานอยู่ในระบบ โดยตัวอย่างการสำรวจช่องโหว่ที่อาจเกิดขึ้น เช่น
  - ใบรับรอง TLS ที่ไม่มีความน่าเชื่อถือ
  - การขาด Web Application Firewall (WAF) ในระบบที่สำคัญ
  - การเปิดเผยข้อมูลในแอปพลิเคชันที่ไม่ได้รับการแพตช์
- ดำเนินการอัปเดตข้อมูลและฐานข้อมูลอย่างต่อเนื่อง เพื่อให้มั่นใจว่าได้ข้อมูลที่ถูกต้องและทันสมัย
- พิจารณาใช้เครื่องมือที่สามารถตั้งค่าการแจ้งเตือน เมื่อมีการเปลี่ยนแปลงที่สำคัญหรือคะแนนความเสี่ยงลดลง
- ดำเนินการจัดกลุ่มหรือประเภทการประเมิน เพื่อให้การประเมินมีขอบเขตที่ชัดเจนและเป็นระเบียบ โดยการตรวจสอบพื้นผิวการโจมตีของผู้ให้บริการภายนอก หรือการได้รับข้อมูลจากผู้ให้บริการภายนอกเกี่ยวกับผลการตรวจสอบที่ดำเนินการ เช่น
  - การประเมินพื้นผิวการโจมตีดิจิทัล (Digital Attack Surface) มุ่งเน้นการประเมินไปที่สินทรัพย์ดิจิทัลที่เข้าถึงได้จากอินเทอร์เน็ต เช่น เว็บแอปพลิเคชันและเว็บไซต์ (Web Applications & Websites) ระบบการเข้าถึงระยะไกล (Remote Access Systems) เป็นต้น
  - การประเมินพื้นผิวการโจมตีทางกายภาพ (Physical Attack Surface) ซึ่งเป็นการประเมินความเสี่ยงทางกายภาพที่ผู้โจมตีสามารถใช้เพื่อเข้าถึงระบบดิจิทัลได้ เช่น การเข้าถึงอาคารโดยไม่ได้รับอนุญาตเพื่อติดตั้งอุปกรณ์ หรือการขโมยอุปกรณ์ เป็นต้น

o การประเมินพื้นผิวการโจมตีทางสังคม (Social/Human Attack Surface) ซึ่งเป็นการประเมินเกี่ยวข้องกับช่องโหว่ที่เกิดจากพฤติกรรมมนุษย์ รวมถึงการตรวจสอบข้อมูลที่เปิดเผยสาธารณะที่สามารถนำไปใช้ในการโจมตีแบบ Social Engineering เช่น Phishing, Spear Phishing เป็นต้น

๙. การคัดเลือกผู้ให้บริการภายนอก

๑) กำหนดให้มีระเบียบวิธีปฏิบัติและหลักเกณฑ์ในการพิจารณาคัดเลือกผู้ให้บริการภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร โดยให้มีข้อมูลที่เพียงพอสำหรับการพิจารณาตัดสินใจเลือกใช้บริการและอนุญาตให้ผู้ให้บริการภายนอกเชื่อมต่อหรือเข้าถึงข้อมูลของ ขร. เพื่อให้สามารถทำการคัดเลือกผู้ให้บริการภายนอกที่มีความเหมาะสมตามวัตถุประสงค์สำหรับการดำเนินการของ ขร.

๒) การตัดสินใจเลือกใช้บริการที่ผู้ให้บริการภายนอกต้องเชื่อมต่อหรือเข้าถึงข้อมูลที่มีความเสี่ยงอย่างมีนัยสำคัญต้องได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

๓) กำหนดให้ดำเนินการประเมินศักยภาพของผู้ให้บริการภายนอก (Due Diligence) โดยการประเมินกระบวนการ การตรวจสอบ และประเมินความเหมาะสมของผู้ให้บริการภายนอกอย่างละเอียด เพื่อให้มั่นใจว่าผู้ให้บริการมีความสามารถและมีคุณสมบัติเหมาะสมในการให้บริการ ตามต้องการ ซึ่งควรมีการพิจารณาการประเมินให้ครอบคลุมตามระดับความสำคัญและระดับความเสี่ยงที่เกี่ยวข้องของการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกในประเด็นต่าง ๆ เช่น

(๑) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์และความสามารถในการ ให้บริการของผู้ให้บริการภายนอก

(๒) ธรรมาภิบาลและวัฒนธรรมภายในองค์กรของผู้ให้บริการภายนอก

(๓) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน

(๔) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอก

(๕) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือจากภัยหรือเหตุการณ์ต่าง ๆ เช่น การตรวจสอบจากการได้รับรองมาตรฐาน ISO หรือเอกสารรายงานการรับมือภัยคุกคามทางไซเบอร์

(๖) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง และการปฏิบัติตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ เช่น การเข้าตรวจสอบเอกสาร หลักฐาน หรือใบรับรองจากผู้ให้บริการภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง หรือการได้รับการรองรับตามมาตรฐาน ISO/IEC ๒๗๐๐๑ เป็นต้น ซึ่งขอบเขตการรับรองตามมาตรฐานสากลของผู้ให้บริการภายนอกควรพิจารณาจากการรับรองการให้บริการในส่วนที่สำคัญ เช่น ศูนย์คอมพิวเตอร์ หรือ ได้รับการรับรองที่ครอบคลุมทั้งหน่วยงาน เป็นต้น

(๗) ปัจจัยภายนอกที่อาจกระทบต่อการให้บริการของผู้ให้บริการภายนอก เช่น ข้อจำกัดด้านกฎหมายของประเทศที่ผู้ให้บริการภายนอกตั้งอยู่หรือประกอบธุรกิจ

(๘) การใช้เทคโนโลยีแบบเปิด (Open Technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (Interoperability) และสามารถลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยีของผู้ให้บริการหรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการ เองภายใต้การ

ดำเนินการของ ขร. เช่น การใช้รูปแบบการรับส่งข้อมูลกับผู้ให้บริการภายนอกที่เป็นมาตรฐานการใช้เทคโนโลยีแบบเปิด (Open Standard หรือ Open Source) เป็นต้น

๑๐. การจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก

๑) กำหนดให้มีการจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร โดยอาจทำในรูปแบบของกระดาษหรือโดยวิธีการทางอิเล็กทรอนิกส์ และจัดเก็บสัญญาหรือข้อตกลงดังกล่าวไว้ที่ ขร. เพื่อสามารถใช้เป็นหลักฐานตามกฎหมายและเป็นการเตรียมข้อมูลให้พร้อมสำหรับการตรวจสอบ หรือเมื่อมีการร้องขอโดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒) กำหนดให้มีการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญในสัญญาหรือข้อตกลงกับผู้ให้บริการภายนอกอย่างชัดเจน โดยต้องคำนึงถึงรายละเอียด ดังนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่อนุญาตให้เข้าถึงทรัพย์สินของบริการที่สำคัญของ ขร. ตามความต้องการในการดำเนินการตามภาระกิจหน้าที่ของ ขร. และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดย ขร. ต้องระบุรายละเอียด และสิทธิการเข้าถึงทรัพย์สินของบริการที่สำคัญ เช่น ไม่อนุญาตให้ผู้ให้บริการภายนอกประเภทที่เป็นผู้รับช่วงต่อเข้าถึงระบบงานหลักที่มีความเสี่ยงสูง

(ข) กำหนดภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของ ขร. จากภัยคุกคามทางไซเบอร์ โดยต้องระบุรายละเอียดบทบาทหน้าที่ในการจัดการเทคโนโลยี การจัดการความเสี่ยงและการควบคุมทางไซเบอร์ (Managing Cyber Risks and Controls) เช่น ขร. เป็นผู้ควบคุมการเข้าถึงข้อมูล และผู้ให้บริการภายนอกทำหน้าที่เป็นผู้ให้บริการหลักของบริการตามมาตรการที่กำหนด และต้องแจ้ง ขร. เมื่อมีการดำเนินการตามภาระหน้าที่ หรือเมื่อมีเหตุการณ์อื่นใดที่ก่อให้เกิดความเสี่ยงอย่างมีนัยสำคัญต่อ ขร. เป็นต้น

(ค) กำหนดให้มีการบริหารความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์โดยระบุรายละเอียดการติดตาม และควบคุมความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก เช่น ผู้ให้บริการภายนอกต้องแจ้งการเปลี่ยนแปลง หรือเหตุการณ์ที่สำคัญให้รายงานปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากห่วงโซ่อุปทาน กำหนดให้มีข้อตกลงการเข้ารหัสที่สำคัญ และข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ เป็นต้น

(ง) สิทธิของหน่วยงานในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก เช่น กำหนดสิทธิของ ขร. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหรือผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากหน่วยงานหรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของผู้ให้บริการภายนอกในส่วนที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกของ ขร. ทั้งนี้ควรพิจารณาระบุรายละเอียดอื่น ๆ ในข้อตกลงหรือสัญญา เช่น

- ขอบเขตการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก โดยระบุ รายละเอียด เช่น ความถี่ของการใช้บริการ เนื้อหาและรูปแบบของการใช้บริการ ระยะเวลาของการ

เชื่อมต่อตามสัญญา สถานที่ตั้งทางกายภาพของบริการ และบริการเสริม เช่น ซอฟต์แวร์หรือการสนับสนุนเทคโนโลยี อื่น ๆ การบำรุงรักษา และการบริการ

- การคุ้มครองข้อมูลส่วนบุคคลทั้งข้อมูลของ ขร. และข้อมูลของผู้ใช้บริการของ ขร. โดยต้องกำหนดให้เป็นไปตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น ควรมีการจัดทำข้อตกลงเกี่ยวกับการใช้หรือประมวลผลข้อมูลส่วนบุคล (Data Processing Agreement: DPA) ให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

- มาตรฐานการปฏิบัติงานขั้นต่ำของผู้ให้บริการภายนอก เช่น มาตรฐานการควบคุมภายใน มาตรฐานการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษา สภาพพร้อมใช้งาน (Availability) ต้องสอดคล้องกับมาตรฐานขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยของ ขร. เช่น หาก ขร. ได้รับการรับรองตาม ISO/IEC ๒๗๐๐๑, ISO/IEC ๒๗๐๑๗ หรือ CSA-STAR ขร. ต้องดำเนินการกำหนดให้ผู้ให้บริการภายนอกได้รับการรับรองมาตรฐานในระดับใกล้เคียงกัน เป็นต้น

- แผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan) สำหรับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก โดยเฉพาะอย่างยิ่งสำหรับกรณีที่เกิดการหยุดชะงักของระบบ ซึ่งผู้ให้บริการภายนอกควรมีระบบการสื่อสารสำรอง เพื่อรองรับการดำเนินการของ ขร. ให้สามารถดำเนินการได้ภายในระยะเวลาที่กำหนดหลักจากระบบหยุดชะงัก

- ข้อกำหนดในการดำเนินการทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก เช่น การกำหนดให้ผู้ให้บริการภายนอกต้องออกหนังสือรับรองการทำลายข้อมูลหลังจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลได้สิ้นสุดลง

- เงื่อนไขหรือสิทธิของ ขร. ในการขอเปลี่ยนแปลง ยุติหรือยกเลิกสัญญาหรือข้อตกลงกรณีที่เกิดการเปลี่ยนแปลงหรือเกิดการละเมิดสัญญาหรือข้อตกลง เช่น เมื่อผู้ให้บริการภายนอกมีการเปลี่ยนเจ้าของ การละเมิดความปลอดภัยหรือการรักษาความลับ หรือผู้ให้บริการภายนอกอยู่ระหว่างกระบวนการพิทักษ์ทรัพย์/การชำระบัญชี/การล้มละลาย เป็นต้น

๓) กรณีการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing) อย่างมีนัยสำคัญ โดยอาจมีผลกระทบต่อความเสี่ยงหรือผลลัพธ์ที่สำคัญที่สามารถส่งผลต่อการดำเนินงาน ความมั่นคงปลอดภัย หรือความสามารถในการปฏิบัติตามข้อกำหนดของ ขร. ซึ่งควรสงวนสิทธิในการพิจารณาอนุมัติ ในกรณีผู้ให้บริการภายนอกว่าจ้างผู้รับเหมาช่วง (Subcontract) และข้อกำหนดที่ผู้ให้บริการภายนอกต้องรับผิดชอบต่อผลการปฏิบัติงานของผู้รับเหมาช่วง เช่น

- บริการที่อาจก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัย หากการใช้บริการจากผู้ให้บริการภายนอกเกี่ยวข้องกับข้อมูลหรือระบบที่สำคัญ เช่น ระบบที่ใช้จัดการข้อมูลผู้ใช้บริการหรือข้อมูลทางการเงิน การให้ผู้รับเหมาช่วงเข้ามามีส่วนร่วมอาจเพิ่มความเสี่ยงในการเข้าถึงข้อมูลสำคัญ

- บริการที่เกิดความเสี่ยงด้านการดำเนินงาน หากผู้ให้บริการภายนอกมีการจ้างผู้รับเหมาช่วงในการ ดำเนินงานบางส่วน แต่ไม่สามารถควบคุมหรือประเมินการดำเนินการของผู้รับเหมาช่วงได้อย่างเต็มที่อาจทำ ให้เกิดการปฏิบัติงานที่ไม่ได้มาตรฐานหรือล่าช้า ซึ่งมีผลกระทบต่อการให้บริการของ ขร.

- บริการที่อาจก่อให้เกิดผลกระทบต่อการควบคุมและการติดตาม การอนุญาตให้ผู้รับเหมาช่วงเข้ามาทำงานแทนผู้ให้บริการหลัก อาจทำให้ ขร. ขาดการควบคุมและตรวจสอบการดำเนินการที่เกิดขึ้นภายใต้การทำงานของผู้รับเหมาช่วง

- การดำเนินการที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและการปฏิบัติตามมาตรฐาน ซึ่งผู้ให้บริการภายนอกที่เลือกใช้ผู้รับเหมาช่วงต้องรับผิดชอบต่อการปฏิบัติตามข้อกำหนดกฎหมาย และมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้อง เพื่อป้องกันปัญหาทางกฎหมายหรือข้อบังคับที่อาจเกิดขึ้นในภายหลัง

๔) ในกรณีที่ผู้ให้บริการภายนอกได้ว่าจ้างผู้รับเหมาช่วง (Subcontract) และผู้ให้บริการภายนอกมีสิทธิเข้าใช้บริการงานด้านเทคโนโลยีสารสนเทศที่สำคัญ ขร. ควรกำหนดสิทธิในการพิจารณาอนุมัติในกรณีผู้ให้บริการภายนอกว่าจ้างผู้รับเหมาช่วง (Subcontract) และแจ้งถึงข้อกำหนดที่ผู้ให้บริการภายนอกต้องรับผิดชอบต่อผลการปฏิบัติงานของผู้รับเหมาช่วง

๕) กรณีการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกที่ตั้งอยู่ในต่างประเทศ สัญญาหรือข้อตกลงในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกควรพิจารณาถึงความเสี่ยงและอุปสรรคที่อาจเกิดขึ้นจากประเทศที่ผู้ให้บริการภายนอกตั้งอยู่หรือประกอบการดำเนินการตามภาระหน้าที่ของผู้ให้บริการภายนอก (Country Risk)

ทั้งนี้ ในการจัดทำสัญญาหรือข้อตกลงการใช้บริการ ขร. ควรมอบหมายให้ผู้ที่มีอำนาจตัดสินใจเข้าร่วมในการเจรจา โดยวัตถุประสงค์ของการเจรจาคือการมีข้อตกลงร่วมกัน และสอดคล้องกับการเปลี่ยนแปลงตามกฎหมายภายใต้เงื่อนไขที่ดีที่สุดสำหรับทั้งสองฝ่าย

๑๑. กำหนดให้สร้างกระบวนการในการตรวจสอบ ติดตามผลปฏิบัติงานอย่างต่อเนื่อง (Monitoring) เพื่อตรวจสอบความถูกต้องของผู้ให้บริการภายนอกในการดำเนินการให้สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุเป็นเงื่อนไขในสัญญาที่ครอบคลุมการตรวจสอบการปฏิบัติตามข้อกำหนดด้านความปลอดภัยทางไซเบอร์และข้อตกลงระดับการให้บริการ (Service Level Agreement) การตรวจสอบการเปลี่ยนแปลงสถานะต่างๆ ของผู้ให้บริการภายนอก เช่น การเงิน กฎหมาย ความเป็นเจ้าของ รวมถึงการตรวจสอบเรื่องการจัดการความเสี่ยงตามที่ระบุตามกรอบเวลาการแก้ไขข้อตกลงร่วมกัน ซึ่งกระบวนการตรวจสอบ ติดตามผู้ให้บริการภายนอก ควรพิจารณาให้มีขั้นตอน ดังนี้

๑) กำหนดผู้รับผิดชอบและจัดการติดตามผลการปฏิบัติงานของผู้ให้บริการภายนอกอย่างต่อเนื่อง โดยพิจารณาตามระดับความเสี่ยงและระดับความสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก เช่น กำหนดให้ผู้ให้บริการภายนอกรายงานผลการปฏิบัติงานอย่างสม่ำเสมอ กำหนดการประชุมติดตามอย่างสม่ำเสมอและต่อเนื่อง กำหนดการเข้าสังเกตการณ์การดำเนินงานของผู้ให้บริการภายนอก เป็นต้น

๒) กำหนดให้ผู้ให้บริการภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของ ขร. เพื่อให้ ขร. รับทราบอย่างทันการณ์และสามารถประเมินผลกระทบที่มีต่อ ขร. และหาก ขร. ประเมินแล้วพบว่าผลกระทบที่เกิดขึ้นมีผลต่อการดำเนินการของ ขร. อย่างมีนัยสำคัญ ต้องกำหนดให้ ขร. มีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติที่เกิดขึ้น

๓) ดำเนินการตรวจสอบความถูกต้องของผู้ให้บริการภายนอก โดย ขร. ตามสิทธิ์การตรวจสอบที่กำหนดในข้อกำหนด โดยการพิจารณาวิธีการประเมินอย่างใดอย่างหนึ่ง หรือใช้วิธีการร่วมกัน ดังนี้

- วิธีการประเมินตนเอง (Self–assessment) โดยการกำหนดให้ผู้ให้บริการภายนอกบันทึก ประเด็นปัญหาความเสี่ยง ข้อมูลความเสียหาย รวมถึงเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานด้วย ตนเอง เพื่อให้หน่วยงานตรวจสอบและกำกับได้เมื่อมีการร้องขอ

- วิธีการประเมินโดยบุคคลที่สาม (Third-party Assessment) โดยให้หน่วยงานที่เป็นบุคคลที่สาม และมีความสามารถในการประเมินที่เป็นที่น่าเชื่อถือมาเป็นผู้ประเมินคุณภาพการดำเนินงานของผู้ให้บริการภายนอก

- วิธีการตรวจสอบผลิตภัณฑ์ โดยการทดสอบผลิตภัณฑ์ที่ผู้ให้บริการภายนอกใช้ในการดำเนินงาน เช่น การทดสอบความเร็วในการเชื่อมต่อของอุปกรณ์เครือข่าย การทดสอบการตรวจจับมัลแวร์ การตรวจสอบช่องโหว่ เป็นต้น

๔) ดำเนินการทบทวนการประเมินศักยภาพ การประเมินผลการปฏิบัติงาน และการประเมินความเสี่ยงของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกทั้งในด้านประสิทธิภาพ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการปฏิบัติตามกฎหมาย เมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่ ขร.กำหนด รวมถึงควรดำเนินการทบทวนการประเมินอย่างน้อยปีละ ๑ ครั้ง รวมถึงให้รายงานผลการประเมินต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

๑๒. การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง

๑) จัดให้มีมาตรฐานหรือระเบียบเกี่ยวกับการปฏิบัติว่าด้วยการยกเลิกและสิ้นสุดสัญญา หรือข้อตกลง เพื่อเป็นกรอบแนวทางการยกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลง โดยคำนึงถึงความต่อเนื่องในการให้บริการและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงบทบาทหน้าที่ของคณะกรรมการและหน่วยงานที่เกี่ยวข้องกับ กระบวนการและการควบคุมภายใน เช่น การสำรองข้อมูลก่อนการยกเลิก การลบหรือการเรียกคืนทรัพย์สินสำคัญของ ขร. กลับมาทำลาย เช่น กุญแจการเข้ารหัสข้อมูล และบัญชีผู้ใช้งาน เป็นต้น

๒) พิจารณาดำเนินการประเมินผล กระทบและความเสี่ยงที่อาจเกิดขึ้นจากการยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง และดำเนินการตามมาตรฐาน หรือระเบียบเกี่ยวกับการปฏิบัติว่าด้วยการยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง และกำหนดกลยุทธ์ และแผนงาน การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง (Exit Strategy and Exit Plan) ที่ชัดเจน เพื่อให้มั่นใจว่าการยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลงนั้นเป็นไปอย่างมีประสิทธิภาพและได้เตรียมความพร้อมต่อผลกระทบที่อาจจะเกิดขึ้น เช่น การหยุดให้บริการของระบบที่ส่งผลกระทบกับผู้ใช้บริการ และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

๑๓. การเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ ในกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ซึ่งอาจปรับเปลี่ยนระดับของรายละเอียดหรือความครอบคลุมของข้อตกลง และส่งผลต่อสัญญาปัจจุบันให้เกิดความเสี่ยงเพิ่มขึ้น และไม่สามารถยอมรับความเสี่ยงได้ ขร. ควรพิจารณาขอเจรจาแก้ไขข้อกำหนดของสัญญาเพิ่มเติม หรือขอแก้ไขรายละเอียด เพื่อให้สอดคล้องกับข้อกำหนดหรือความเสี่ยงที่เปลี่ยนแปลง และในการเจรจาต่อรองเงื่อนไขของสัญญาจ้างต้องทำ

ความเข้าใจสิทธิและหน้าที่ความรับผิดชอบของแต่ละฝ่าย รวมถึงขอบเขตอำนาจในการเจรจาต่อรองในเงื่อนไขการบอกเลิกสัญญา หรือการรับผิดที่อาจตามมา และพิจารณารายละเอียดของขอบเขตงาน ความซับซ้อนในการดำเนินการ รวมถึงระยะเวลาในการดำเนินการที่เพิ่มขึ้น ซึ่งควรดำเนินการตรวจสอบจากที่ปรึกษาทางกฎหมายก่อนการเริ่มต้นเจรจาสัญญา

ในกรณีไม่สามารถตกลงกันได้ภายใต้เงื่อนไขใหม่อาจต้องพิจารณาจัดหาผู้ให้บริการรายอื่นมาดำเนินการในส่วนที่มีการเปลี่ยนแปลงแก้ไขต่อไป

๑๔. กำหนดให้ผู้ให้บริการภายนอกต้องมีมาตราการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ตามกรอบหลักการ ที่สำคัญ ๓ ประการ คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) และสอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ ขร. (IT Security Policy) หรือมาตรฐานสากลด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เช่น ISO/IEC ๒๗๐๐๑, ISO/IEC ๒๗๐๑๗ เป็นต้น

ในกรณีที่มีการใช้บริการ Cloud Computing ต้องนำแนวปฏิบัติที่ดีของผู้ให้บริการ Cloud Computing มาเป็นแนวทางในการปฏิบัติงานและควบคุมดูแล เพื่อให้ระบบที่ใช้บริการ Cloud Computing มีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยต้องกำหนดให้บุคลากรที่เกี่ยวข้องในการปฏิบัติงานปฏิบัติตามแนวปฏิบัติด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของ ขร. รวมถึงเป็ยไปตามมาตรฐานสากลทางด้านการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่เป็นที่ยอมรับโดยทั่วไป และพิจารณาให้สอดคล้องตามระดับความเสี่ยงและระดับความสำคัญของบริการหรือข้อมูลที่เปิดให้ผู้ให้บริการภายนอกเข้าใช้เชื่อมต่อหรือเข้าถึง ซึ่งควรกำหนดมาตรการเพิ่มเติม ดังนี้

๑) จัดทำทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง โดยพิจารณาดำเนินการ ดังนี้

(๑) จัดให้มีผู้รับผิดชอบในการจัดทำ และปรับปรุงทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้สามารถนำมาใช้ระบุความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกได้อย่างชัดเจน และสามารถบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างปลอดภัยและทันการณ์

(๒) ทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง ควรครอบคลุมรายละเอียด ดังนี้

- ชื่อผู้ให้บริการภายนอก
- ประเภทของผู้ให้บริการภายนอก เช่น ประเภทที่อยู่ภายนอกกลุ่มของหน่วยงาน ประเภท ที่อยู่ภายในกลุ่มของหน่วยงาน และ Regulator เป็นต้น
- ชื่อบริการ/ระบบงาน
- ลักษณะและขอบเขตของงาน
- ประเภทของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก เช่น IT Outsourcing Cloud Computing บริการร่วมกับพันธมิตร การใช้บริการเครือข่ายสาธารณะ เป็นต้น

- ระดับความเสี่ยงและระดับความสำคัญของบริการหรือข้อมูลที่เปิดให้ผู้ให้บริการภายนอก เข้าใช้ เชื่อมต่อหรือเข้าถึง
- ที่ตั้งศูนย์คอมพิวเตอร์หลักและสำรองข้อมูลของผู้ให้บริการภายนอกที่ประมวลผล จัดเก็บข้อมูล หรือดำเนินการใด ๆ ที่เกี่ยวข้องกับข้อมูลหรือระบบงานให้แก่ ขร.
- วันเริ่มต้นและวันสิ้นสุดสัญญาหรือข้อตกลงของการใช้บริการ การเชื่อมต่อหรือการเข้าถึง ข้อมูลจากผู้ให้บริการภายนอก
- การรับรองตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง (ถ้ามี)
- รายละเอียดทรัพย์สินที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก เช่น ข้อมูลที่นำไปจัดเก็บหรือประมวลผล ระดับชั้นความลับข้อมูล เป็นต้น

๒) การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

(๑) กำหนดให้ต้องแบ่งระดับความสำคัญของข้อมูล (Information Classification) ตามการบริหารจัดการทรัพย์สิน (Asset Management) ของกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ก่อนที่จะนำข้อมูลไปใช้ จัดเก็บหรือประมวลผลโดยผู้ให้บริการภายนอก โดยต้องพิจารณาจัดเก็บข้อมูลหรือระบบสารสนเทศที่มีผลกระทบระดับสูงไว้ในประเทศ (Data Localization) ซึ่งอ้างอิงตามประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูล หรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗

(๒) เข้ารหัสข้อมูลที่อยู่ภายใต้การดูแลของผู้ให้บริการภายนอกให้เป็นไปตามนโยบาย และมาตรฐานของ ขร. ตามประเภทและระดับชั้นความลับของข้อมูล (Information Classification) ให้สอดคล้องกับนโยบาย และแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศของ ขร. รวมถึงพิจารณาการเข้ารหัสให้ครอบคลุมทั้งข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data at Endpoint) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (Data in Transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (Data at Rest) ซึ่งรวมถึงข้อมูลสำรอง

(๓) กำหนดให้มีการควบคุมทุกขั้นตอนตลอดวงจรการบริหารจัดการกุญแจการเข้ารหัส (Lifecycle of Cryptographic Keys) ตั้งแต่ การสร้าง การจัดเก็บ การใช้งาน การสำรอง การเพิกถอน และการต่ออายุของกุญแจเข้ารหัสข้อมูล ภายใต้การดูแลของ ขร.

(๔) กำหนดให้ ขร. ดำเนินการสร้างกุญแจการเข้ารหัสด้วยตนเอง ซึ่งในกรณีที่ ขร. ไม่สามารถสร้างกุญแจการเข้ารหัสด้วยตนเอง ขร. ต้องกำหนดให้มีการควบคุมผู้ให้บริการภายนอกไม่ให้นำกุญแจการเข้ารหัสที่สร้างขึ้นโดยผู้ให้บริการภายนอกไปใช้ร่วมกับผู้ใช้บริการรายอื่น รวมถึงต้องทราบถึงรายละเอียดของระบบการบริหารจัดการกุญแจเข้ารหัสข้อมูลของผู้ให้บริการภายนอก ดังนี้

- ประเภทของกุญแจเข้ารหัสข้อมูล
- รายละเอียดของระบบ รวมถึงกระบวนการควบคุมการเข้ารหัสข้อมูลในแต่ละขั้นตอน ตลอดวงจรการบริหารจัดการกุญแจการเข้ารหัส
- ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล

(๕) กำหนดให้มีการเก็บกุญแจการเข้ารหัสข้อมูลในอุปกรณ์รักษาความปลอดภัย เช่น Hardware Security Module (HSM) เป็นต้น และดูแลรักษาความปลอดภัยของอุปกรณ์ HSM ด้วยการจัดตั้งในโซนเครือข่ายที่มีความปลอดภัยและจำกัดการเชื่อมต่อกับระบบงานอื่นที่ไม่เกี่ยวข้อง

(๖) กำหนดให้มีการสอบทานการปฏิบัติงานการบริหารจัดการเข้ารหัสข้อมูลทั้งที่ดำเนินการภายใต้การดูแลของ ขร. และโดยผู้ให้บริการภายนอกให้ครอบคลุมการสอบทานช่องโหว่และความเสี่ยงของการเข้ารหัสข้อมูล โดยพิจารณาให้มีความปลอดภัยและมีความสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป เช่น ใช้อัลกอริธึมการเข้ารหัส (Encryption Algorithm) และขนาดความยาวของกุญแจเข้ารหัสข้อมูลที่ได้รับการยอมรับ เป็นต้น

๓) การควบคุมการเข้าถึง (Access Control)

(๑) กำหนดกระบวนการจัดการและควบคุมการเบิกใช้สิทธิและการเข้าถึงระบบและข้อมูลของ ขร. ที่ชัดเจนเป็นลายลักษณ์อักษรเป็นไปตามนโยบาย และแนวการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่กำหนด รวมทั้งตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป เช่น NIST, ISO/IEC๒๗๐๐๑ เป็นต้น

(๒) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้มีสิทธิเข้าใช้งานระบบและผู้ใช้งานที่ได้รับสิทธิสูงสุด (Privilege Account) ให้ชัดเจน

(๓) ควบคุมดูแลการให้สิทธิแก่ผู้ให้บริการภายนอก โดยจำกัดสิทธิตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน รวมถึงมีการอนุมัติการเบิกใช้งาน เพื่อไม่ให้บุคคลใดบุคคลหนึ่งมีสิทธิปฏิบัติงานได้ตั้งแต่เริ่มกระบวนการจนจบกระบวนการ (Separation of Duties)

(๔) มีระบบหรือกระบวนการติดตามระหว่างการใช้งานบัญชีของผู้ใช้งานที่มีสิทธิสูงสุด รวมทั้งควรติดตามและสอบทานสถานะสิทธิและการใช้งานหรือการเข้าถึงระบบข้อมูลที่สอดคล้องกับความเสี่ยงและระดับของสิทธิ (Privilege Level) สม่ำเสมออย่างน้อยทุก ๖ เดือน เพื่อให้มั่นใจว่าการใช้งานสิทธิเป็นไปตามขอบเขต และความจำเป็นในการใช้งาน

(๕) กำหนดวิธีการระบุและพิสูจน์ตัวตนของผู้ใช้งานด้วยวิธีการที่รัดกุมเพียงพอ และสอดคล้องกับนโยบายแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของ ขร.

(๖) ในกรณีที่ผู้ให้บริการภายนอกต้องดำเนินการเชื่อมต่อ เพื่อเข้าถึงระบบงานของ ขร. ผ่านช่องทางการเข้าถึงระบบงานระยะไกล (System Remote Access) ต้องมีการกำหนดกระบวนการบริหารจัดการการเข้าถึงระยะไกลด้วยวิธีการที่ปลอดภัย ดังนี้

- มีการขออนุมัติก่อนการเข้าถึงระบบงานระยะไกล (System Remote Access)
- ผู้ใช้งานที่ได้รับสิทธิระดับสูง (Privilege Account) ให้ใช้เข้าถึงระบบงานเฉพาะกรณีที่มีความจำเป็นและภายในระยะเวลาที่อนุมัติเท่านั้น
- กำหนดให้มีการพิสูจน์ตัวตนของผู้ใช้งานแบบ Two-Factors Authentication และการเชื่อมต่อผ่าน Virtual Private Network (VPN)
- มีการควบคุมการเข้าใช้งาน โดยจำกัดการเข้าใช้งานเฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้น หรือใช้เทคโนโลยีเข้ามาบริหารจัดการเครื่องคอมพิวเตอร์แบบเสมือน (Virtual Desktops Infrastructure) เพื่อลดความเสี่ยงจากการติด Malware หรือการเข้าถึงระบบงานที่ไม่เหมาะสม

- สามารถระบุและสอบทานอุปกรณ์หรือระบบปลายทางที่มีการเชื่อมต่อกับระบบเครือข่ายของ ขร. แบบระยะไกลว่าเป็นอุปกรณ์ที่ได้รับอนุญาต
- มีการสอบทานการเข้าถึงระบบงานระยะไกล โดยบัญชีผู้ใช้งานที่ได้รับสิทธิระดับสูงด้วยบุคคล หรือหน่วยงานที่มีความเป็นอิสระและมีความรู้ความเชี่ยวชาญเพียงพอ

(๗) กำหนดให้มีการจัดเก็บบันทึกข้อมูลประวัติของการพิสูจน์ตัวตนและการเข้าถึง (Access Log) บันทึกการดำเนินงาน (Activity Log) อย่างน้อย ๙๐ วัน และจัดให้มีการสอบทานข้อมูลการบันทึกสม่ำเสมออย่างน้อยทุก ๖ เดือน ให้สอดคล้องกับความเสี่ยงและความสำคัญของระบบ และข้อมูล

๔) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

(๑) กำหนดให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์ในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารกับผู้ให้บริการภายนอกให้เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของ ขร. รวมถึงให้เป็นไปตามมาตรฐานสากลที่ยอมรับโดยทั่วไป

(๒) กำหนดให้ผู้ให้บริการภายนอกมีระบบหรือกระบวนการสำหรับการคัดกรองข้อมูลที่ส่งผ่านระบบเครือข่าย (Traffic) ที่สามารถตรวจจับแจ้งเตือนและสามารถยับยั้งการบุกรุกหรือตอบโต้การโจมตีได้ โดยอัตโนมัติแบบต่อเนื่องบนระบบเครือข่ายให้เพียงพอเหมาะสมตามระดับความเสี่ยงและระดับความสำคัญของบริการหรือข้อมูลที่ผู้ให้บริการภายนอกเข้าใช้ เชื่อมต่อ หรือเข้าถึงได้ ดังนี้

- เครื่องมือตรวจหาและแจ้งเตือน ที่สามารถยับยั้งการบุกรุก หรือตอบโต้การโจมตีได้โดยอัตโนมัติบนระบบเครือข่าย (Network Intrusion Detection and Prevention Systems: NIDPS)
- เครื่องมือป้องกันการโจมตีเว็บไซต์ (Web Application Firewall: WAF)
- มาตรการป้องกันการโจมตีแบบ Distributed Denial of Services (DDoS)
- ระบบป้องกัน ข้อมูลรั่วไหล (Data Leakage Prevention Systems: DLPS)
- ซอฟต์แวร์การตรวจจับไวรัส หรือมัลแวร์ ต่าง ๆ ที่อาจทำการบุกรุกเข้าสู่เครือข่าย

(๓) กรณีที่หน่วยงานใช้บริการ Cloud Computing ต้องกำหนดมาตรการที่ชัดเจนในการแยกแยะข้อมูลและแยกสภาพแวดล้อมบน Cloud ของ ขร. ออกจากผู้ใช้บริการรายอื่นที่ใช้บริการจากผู้ให้บริการ Cloud เดียวกัน เช่น การแยกแยะสภาพแวดล้อมโดยการใช้ Virtual Private Cloud (VPC) หรือการสร้างบัญชีผู้ใช้แยกต่างหาก

๕) การบริหารจัดการการเปลี่ยนแปลง (Change Management)

(๑) จัดทำกระบวนการและแนวทางบริหารจัดการการเปลี่ยนแปลง โดยกำหนดให้ผู้ให้บริการภายนอก และผู้ที่ได้รับมอบหมายของ ขร. ดำเนินการกำหนดกระบวนการและแนวทางร่วมกัน หรืออาจให้กระบวนการบริหารจัดการการเปลี่ยนของ ขร. ที่มีอยู่มาบังคับใช้ร่วมกัน และดำเนินการสื่อสารให้ผ้ให้บริการภายนอกรับทราบ และปฏิบัติตาม เพื่อให้สามารถประเมินผลกระทบ และเตรียมแนวทางรองรับผลกระทบที่จะเกิดขึ้น เช่น ผู้ให้บริการ Cloud Computing ต้องแจ้ง ขร. เมื่อผู้ให้บริการภายนอกต้องการเปลี่ยนแปลงระบบของผู้ให้บริการภายนอกและอาจส่งผลกระทบกับการให้บริการ

(๒) กำหนดให้ผู้ให้บริการภายนอกแจ้งการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่อาจมีผลกระทบกับการให้บริการของ ขร. โดยให้แจ้งล่วงหน้าในระยะเวลาที่กำหนด เพื่อให้ ขร. สามารถพิจารณาแนวทางการลดผลกระทบต่อการให้บริการระบบ และข้อมูลที่จะได้รับผลกระทบที่จะเกิดขึ้น

๖) การบริหารจัดการการตั้งค่าระบบ (System Configuration Management) ในกรณีที่ผู้ให้บริการภายนอกมีหน้าที่ตั้งค่าระบบงาน ขร. ต้องกำหนดมาตรฐานการตั้งค่าระบบงานให้ปลอดภัยเพียงพอตามมาตรฐานด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศของ ขร. เช่น ค่า System Configuration ของระบบปฏิบัติการและการตั้งค่าความปลอดภัยของอุปกรณ์เครือข่าย เป็นต้น

๗) การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

(๑) กำหนดกระบวนการติดตาม ประเมินประสิทธิภาพและความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลโดยผู้ให้บริการภายนอกอย่างเพียงพอและต่อเนื่อง ตลอดจนรายงานผลการติดตามและประเมินให้แก่คณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างสม่ำเสมอ รวมถึงกำหนดแนวทางลดความเสี่ยงได้ทันการณ์ เช่น ติดตามและประเมินการใช้งานบริการของหน่วยงานเทียบกับทรัพยากรของระบบ และเครือข่ายของผู้ให้บริการ เช่น หน่วยประมวลผล (CPU) หน่วยความจำ (RAM) หรือความกว้างแถบความถี่ (Bandwidth) มีความพอเพียงในการใช้บริการหรือไม่

(๒) กำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (Threshold และ Trigger) ในระดับต่าง ๆ และกำหนดกระบวนการรายงานและแจ้งเตือนปัญหาหรือเหตุการณ์ที่มีความผิดปกติที่เกิดจากการให้บริการหรือเชื่อมต่อกับผู้ให้บริการภายนอก รวมถึงกำหนดแนวทางการประสานงานกับหน่วยงานทั้งภายใน และภายนอกในกรณีเกิดเหตุขัดข้องให้เหมาะสมตามระดับความเสี่ยงและระดับความสำคัญของบริการ

๘) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ในกรณีที่ ขร. ไม่สามารถเก็บข้อมูลบันทึกเหตุการณ์ได้ด้วยตนเอง เช่น การใช้บริการ Cloud Computing ขร. ต้องควบคุม และตรวจสอบให้ผู้ให้บริการภายนอกดำเนินการจัดเก็บข้อมูลให้ครบถ้วน เพียงพอ และปลอดภัย เพื่อใช้ในการติดตามตรวจสอบเกี่ยวกับร่องรอยการเข้าถึงและการใช้งาน ระบบหรือข้อมูลของผู้ใช้งาน รวมทั้งใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด

๙) การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring)

(๑) กำหนดให้ผู้ให้บริการภายนอกดำเนินการติดตามดูแลระบบและเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง รวมทั้งมีการตรวจจับเหตุการณ์ที่ผิดปกติที่เกิดขึ้นอย่างมีนัยสำคัญกับระบบหรือการบริการที่สำคัญ ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ทั้งในระดับระบบ (System) เครือข่าย (Network) และแอปพลิเคชัน (Application) เพื่อรับมือภัยคุกคามไซเบอร์ได้ทันการณ์

(๒) กำหนดให้มีการวิเคราะห์ข้อมูลบันทึกเหตุการณ์ (Logging) ของระบบ การบริการที่ใช้หรือเชื่อมต่อกับผู้ให้บริการภายนอก เพื่อให้สามารถป้องกันและตรวจจับการบุกรุกได้ทันการณ์

๑๐) การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Testing)

(๑) กำหนดให้ผู้ให้บริการภายนอกมีการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Testing) ตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป และสอดคล้องกับนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของ ขร.

(๒) ดำเนินการสอบทานขอบเขตและผลการทดสอบเจาะระบบของผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าการทดสอบครอบคลุมระบบทั้งหมดที่ ขร. ใช้บริการหรือเชื่อมต่อกับผู้ให้บริการภายนอก และครอบคลุมภัยคุกคามไซเบอร์ที่สำคัญ

๑๑) กำหนดให้มีกระบวนการหรือขั้นตอนการสำรองข้อมูล (Data Backup) ในกรณีที่ ขร. ใช้บริการหรือเชื่อมต่อกับผู้ให้บริการภายนอก และมีการจัดเก็บข้อมูลของ ขร. หรือข้อมูลผู้ใช้บริการของ ขร. โดยครอบคลุมเนื้อหา ดังนี้

- ขอบเขต และรายละเอียดของการสำรองข้อมูลและรอบเวลาสำรองข้อมูล
- วิธีการ หรือเทคโนโลยีการสำรองข้อมูลและรูปแบบข้อมูล (Data Format)
- ระยะเวลาในการเก็บรักษาข้อมูลสำรอง
- การตรวจสอบความถูกต้องครบถ้วนของข้อมูลสำรอง
- ขั้นตอนและวิธีการกู้ข้อมูล
- การทดสอบความสามารถในการกู้คืนข้อมูลจากอุปกรณ์สำรองข้อมูล (Restoration Test)
- สถานที่จัดเก็บข้อมูลสำรอง

๑๒) การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident Management)

(๑) ระบุหน้าที่และความรับผิดชอบของ ขร. และผู้ให้บริการภายนอกที่เกี่ยวกับการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศอย่างชัดเจน ซึ่งต้องรวมถึงหน้าที่การกำหนดระดับความรุนแรงของเหตุการณ์ผิดปกติ และหน้าที่ของผู้ให้บริการภายนอกที่ต้องแจ้งให้ ขร. ทราบถึงเหตุการณ์ผิดปกติที่เกิดขึ้นและเกี่ยวข้องกับ ขร. ภายในระยะเวลา ๒๔ ชม.

(๒) หากเหตุการณ์ผิดปกติที่เกิดขึ้นนั้นมีผลกระทบต่อการดำเนินการตามภาระกิจหน้าที่ของ ขร. อย่างมีนัยสำคัญ ต้องดำเนินการร่วมกับผู้ให้บริการภายนอก เพื่อตัดสินใจแก้ไขเหตุการณ์ผิดปกติที่เกิดขึ้น

(๓) กำหนดให้ผู้ให้บริการภายนอกจัดให้มีช่องทาง ระบบ หรือเครื่องมือ เพื่อรองรับกรณี ขร. ตรวจพบและต้องการรายงานเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศให้ผู้ให้บริการภายนอกทราบ รวมถึงติดตามสถานการณ์และการแก้ไขของผู้ให้บริการภายนอกต่อเหตุการณ์ผิดปกติที่เกิดขึ้นได้อย่างทันการณ์

(๔) กำหนดให้ผู้ให้บริการภายนอกมีผู้ประสานงานอย่างเป็นทางการ เพื่อประสานงานกับ ขร. ในการตอบสนองต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศได้อย่างทันการณ์

๑๓) การบริหารความต่อเนื่อง (Business Continuity Management)

(๑) กำหนดให้ผู้ให้บริการภายนอกจัดทำแผนความต่อเนื่อง (Business Continuity Plan) และแผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan) ที่ครอบคลุมถึงการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก เพื่อให้มีแนวทางรองรับต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อการให้บริการอย่างมีนัยสำคัญ และสามารถดำเนินการให้บริการได้อย่างต่อเนื่อง

(๒) แผนความต่อเนื่องและแผนฟื้นฟูจากภัยพิบัติที่ผู้ให้บริการภายนอกจัดทำขึ้นต้องคำนึงถึงปัจจัยสำคัญ หรือความเสี่ยงที่อาจเกิดขึ้นและส่งผลต่อการหยุดชะงักจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก ผลกระทบที่มีต่อการดำเนินการตามภาระกิจของ ขร. และการติดต่อสื่อสารระหว่างผู้ให้บริการภายนอกกับ ขร. รวมถึงการรายงานปัญหาหรือเหตุการณ์ผิดปกติให้

คณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างทันการณ์ตามความสำคัญและระดับความรุนแรงหรือผลกระทบของเหตุการณ์

(๓) ประเมินและทดสอบการปฏิบัติตามแผนความต่อเนื่อง และแผนฟื้นฟูจากภัย พิบัติ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความ สอดคล้องกับแผนของ ขร. เช่น ความสอดคล้องกันของขอบเขต คำนิยามและการกำหนดระยะเวลาที่สำคัญ เช่น ระยะเวลาการหยุดชะงักสูงสุดที่ยอมรับได้ (Maximum Tolerable Period of Disruption: MTPD)ระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective, RPO) เป็นต้น

(๔) กำหนดให้มีการเข้าร่วมทดสอบแผนความต่อเนื่อง และแผนฟื้นฟูจากภัยพิบัติกับผู้ให้บริการภายนอก ในกรณีที่สามารถเข้าร่วมได้ เพื่อประเมินความพร้อมของผู้ให้บริการภายนอกในการกู้คืนระบบงานตามกรอบ MTPD, RTO และ RPO ที่กำหนดไว้

(๕) กำหนดให้มีการสื่อสารรายละเอียดแผนความต่อเนื่อง และแผนฟื้นฟูจากภัยพิบัติกับผู้ให้บริการภายนอก ให้กับทีมบริหารจัดการในสภาวะวิกฤติ (Crisis Management Team) ของ ขร. ได้รับทราบและเตรียมความพร้อมในการบริหารจัดการในส่วนที่เกี่ยวข้อง

(๖) ดำเนินการรวบรวมปัญหาที่พบระหว่างการทดสอบแผนความต่อเนื่อง และแผนฟื้นฟูจากภัยพิบัติกับผู้ให้บริการภายนอก ในกรณีที่ไม่ได้เข้าร่วมการซ้อมแผน ต้องกำหนดให้ผ้ให้ยริการภายนอกจัดทำรายงานการซ้อมแผนความต่อเนื่อง และแผนฟื้นฟูจากภัยพิบัติส่งให้ ขร. ตรวจสอบ และปรับปรุงแก้ไขร่วมกับผู้ให้บริการภายนอก

๑๕. กำหนดให้มีการตรวจสอบผู้ให้บริการภายนอกในส่วนที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของหน่วยงาน เช่น ระบุเงื่อนไขในสัญญาหรือข้อตกลง เป็นต้น ซึ่งอาจเป็นการตรวจสอบจาก ขร. หรือดำเนินการแต่งตั้งหน่วยงานให้เข้าตรวจสอบแทนให้สอดคล้องกับระดับ ความเสี่ยงและระดับความสำคัญของบริการหรือข้อมูลที่เปิดให้ผู้ให้บริการภายนอกเข้าใช้ เชื่อมต่อหรือเข้าถึง โดยการใช้บริการการเชื่อมต่อหรือการเข้าถึงบริการหรือข้อมูลที่สำคัญควรได้รับการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อพบเหตุการณ์ผิดปกติเกิดขึ้นอย่างมีนัยสำคัญ

ในกรณีที่มีเหตุจำเป็นที่ทำให้ไม่สามารถดำเนินการตรวจสอบผู้ให้บริการภายนอกได้ ต้องระบุสิทธิหรือเงื่อนไขการตรวจสอบในสัญญาหรือข้อตกลง หรือดำเนินการตรวจสอบได้จากผลการตรวจสอบด้านเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอกที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล เช่น ผลการตรวจสอบตาม ISO/IEC ๒๗๐๐๑ หรือ CSA-STAR ที่ถูกรายงานให้คณะกรรมการ หรือผู้บริหารระดับสูงที่ได้รับมอบหมายรับทราบแล้ว

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการอบรม และสร้างความตระหนักด้านความปลอดภัยสำหรับบุคลากรของผู้ให้บริการอย่างสม่ำเสมอ

๒. ในกรณีที่มีการจัดจ้างผู้ให้บริการภายนอกดำเนินการพัฒนาระบบควรพิจารณาข้อกำหนดด้านความมั่นคงปลอดภัย ในเรื่องดังนี้

๑) สิทธิในทรัพย์สินทางปัญญาสำหรับชุดคำสั่ง (Source Code) ในการพัฒนา

๒) การตรวจสอบด้านคุณภาพและความถูกต้องของระบบสารสนเทศ

๓) การตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์

๔) ข้อจำกัดในการเปิดเผยข้อมูลขององค์กร

๕) มาตรฐานและคุณภาพการให้บริการด้านความมั่นคง

๖) การทดสอบระบบสารสนเทศ

๓. ในกรณีที่มีการจัดจ้างผู้ให้บริการภายนอกดำเนินการพัฒนาระบบไม่อนุญาตให้นำข้อมูลสำคัญของ ขร. เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล หรือข้อมูลใช้ภายในเท่านั้น ไปใช้ในการทดสอบกับระบบงาน เพื่อป้องกันการรั่วไหลของข้อมูล เว้นแต่ได้รับการอนุมัติจากผู้บริหารที่มีอำนาจหน้าที่รับผิดชอบ หรือได้รับความยินยอมโดยชัดแจ้ง หรือมีการแจ้งเจ้าของข้อมูลส่วนบุคคลตามแต่กรณีไว้ก่อนแล้ว

๔. กำหนดให้มีการบริหารจัดการข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ โดยจัดทำข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับก่อนเริ่มดำเนินการใด ๆ ที่อาจมีการเปิดเผยข้อมูล และครอบคลุมเนื้อหาอย่างน้อย ดังนี้

๑) หน้าที่ความรับผิดชอบของผู้จัดทำข้อตกลง และผู้ที่ยินยอมรับทราบข้อตกลง

๒) ขอบเขตของข้อมูลที่ถือว่าเป็นความลับ เช่น ข้อมูลส่วนบุคคล ข้อมูล Source code ของระบบ ข้อมูลรายละเอียดโครงสร้างระบบเครือข่าย (Network diagram) หรือการตั้งค่าความปลอดภัย เป็นต้น

๓) ระยะเวลาการรักษาความลับ และระยะเวลาต่อเนื่องที่ต้องรักษาความลับหลังสิ้นสุดภาระหน้าที่ความรับผิดชอบ

๔) ข้อตกลงในการจำกัดการเปิดเผย การทำสำเนา และการส่งต่อข้อมูล

๕) บทลงโทษในกรณีละเมิดไม่ปฏิบัติตามข้อตกลง

๕. กำหนดให้มีการบริหารจัดเก็บ และควบคุมข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับอย่างน้อย ดังนี้

๑) ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA) ที่ลงนามแล้ว ต้องถูกจัดเก็บในระบบการบริหารจัดการเอกสารขององค์กร (Document Control Management) โดยจัดเก็บแยกตามบุคคล/หน่วยงาน พร้อมระบุวันเริ่มต้น–สิ้นสุด และเลขอ้างอิง พร้อมทั้งกำหนดให้มีการควบคุมการเข้าถึงเอกสารข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA) ได้เฉพาะผู้มีสิทธิ์การเข้าถึงตามหน้าที่ความรับผิดชอบ พร้อมทั้งจัดให้มีการติดตามอายุของข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA)

๒) กำหนดให้มีการติดตาม และทบทวนสถานะของข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA) อย่างสม่ำเสมอ เช่น อย่างน้อยปีละ ๑ ครั้ง

๓) กำหนดให้มีการติดตามการละเมิดข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA) โดยการกำหนดขั้นตอนการแจ้งเหตุละเมิดข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับหรือปฏิบัติตามขั้นตอนการแจ้งเหตุละเมิดขององค์กร

๔) ในกรณีที่พบเหตุการณ์ละเมิดข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA) ต้องดำเนินการบันทึกเหตุการณ์ตามขั้นตอนการแจ้งเหตุละเมิดข้อตกลงการรักษาความลับหรือ

การไม่เปิดเผยความลับ หรือปฏิบัติตามขั้นตอนการแจ้งเหตุละเมิดขององค์กร พร้อมทั้งดำเนินการลงโทษ และหามาตรการป้องกันการเกิดเหตุการณ์ซ้ำเดิม

(O) การแบ่งปันข้อมูล (Information Sharing)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการ เพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญ และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญ) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

๒. การกำหนดขั้นตอนการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์และภัยคุกคามไซเบอร์ควรประกอบไปด้วย

๑) กำหนดเป้าหมายและวัตถุประสงค์ของการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์และภัยคุกคามไซเบอร์ ก่อนดำเนินการแบ่งปันข้อมูล

๒) จัดให้มีการระบุแหล่งที่มาของข้อมูลภัยคุกคาม (Identify Potential Sources) เช่น เป็นข้อมูลที่มาจากภายในหน่วยงาน แหล่งข้อมูลจากศูนย์ประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ เครื่องมือที่ใช้ในการเก็บข้อมูล และตำแหน่งของเครื่องมือจัดเก็บข้อมูล

๓) จัดให้มีการระบุประเภทข้อมูลที่สามารถแบ่งปันได้ เช่น Indicator of Compromise (IOC) Tactics Techniques and Procedures (TTPs) เป็นต้น และกำหนดระดับความลับของข้อมูล

๔) ระบุขอบเขตผู้รับข้อมูล เช่น หน่วยงานภายในองค์กร ผู้ให้บริการที่เกี่ยวข้อง (Third Parties) พันธมิตรด้านความมั่นคงไซเบอร์ (Trusted Partners) หน่วยงานของรัฐ หน่วยงานกำกับดูแลหรือสาธารณะ (เฉพาะข้อมูลที่เปิดเผยได้) รวมถึงการเข้าถึงข้อมูล และเงื่อนไขการรักษาความลับ

๕) กำหนดมาตรการป้องกันความเป็นส่วนตัว เช่น ลบหรือปกปิดข้อมูลให้สามารถระบุตัวบุคคลได้ (PII) เพื่อปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๖) กำหนดเกณฑ์การแบ่งปันข้อมูล (Sharing Designations) ตามระดับประเภทของข้อมูล (Traffic Light Protocol: TLP) ซึ่งมี ๕ ระดับ ดังนี้

ระดับชั้นข้อมูล (TLP)	ข้อมูลในระดับความลับมาก
คำอธิบายระดับชั้นข้อมูล	๑. เป็นข้อมูลที่ไม่สามารถเปิดเผยหรือเผยแพร่ได้ และจำกัดเฉพาะผู้ที่มีสิทธิได้รับข้อมูลเท่านั้น ๒. การนำไปใช้งานเมื่อข้อมูลมีความเกี่ยวข้องกับข้อมูลส่วนบุคคล หรือส่งผลกระทบต่อการดำเนินงาน หรือความเป็นส่วนตัว หรือ ชื่อเสียงของบุคคล หน่วยงาน หรือภาครัฐ หากข้อมูลถูกนำไปใช้ในทางที่ผิด
การเปิดหรือเผยแพร่	ผู้ได้รับข้อมูลต้องไม่เปิดเผยหรือ เผยแพร่ข้อมูลให้กับบุคคลใด ๆ นอกเหนือจาก ที่ผู้ส่งข้อมูลได้ระบุไว้

ตัวอย่างข้อมูล	• การรั่วไหลของข้อมูล (Data Breach) หรือการโจมตีเข้าถึงข้อมูลของลูกค้ารายบุคคล (Specific Customer) • ข้อมูลส่วนบุคคล (Personal Identifiable Information) • รหัสผ่าน Password ต่าง ๆ • Blocking Rules ที่เปิดเผยไม่ได้เพราะอาจมีผลกระทบอย่างรุนแรงต่อความสามารถในการปกป้องข้อมูลลูกค้า • ช่องโหว่ของระบบสารสนเทศของหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูล หรือผู้ส่งข้อมูลที่ยังไม่มีการเผยแพร่สู่สาธารณะ • Example of Attack Code สำหรับใช้ในการโจมตีช่องโหว่ของระบบข้อมูล ของหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูลที่ยังไม่มีการ เผยแพร่สู่สาธารณะ • ข้อมูลที่อาจทำให้ Attackers รู้ตัวว่าอยู่ระหว่างภายใต้การตรวจสอบ (Under Surveillance)
ระดับชั้นข้อมูล (TLP)	ข้อมูลในระดับความลับ
คำอธิบายระดับชั้นข้อมูล	๑. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้อย่าง จำกัด ซึ่งผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะภายในหน่วยงาน หรือหน่วยงานของผู้มีสิทธิได้รับข้อมูล เท่านั้น ๒. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่สำหรับการสนับสนุนในการดำเนินการแก้ไขหรือ ป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ แต่อาจส่งผลกระทบต่อการดำเนินงาน หรือความเป็นส่วนตัว หรือชื่อเสียงของบุคคล หน่วยงาน หากถูกเผยแพร่ออกไปภายนอกหน่วยงาน หรือหน่วยงานของผู้ได้รับข้อมูล
การเปิดหรือเผยแพร่	• ผู้ได้รับข้อมูลสามารถเปิดเผย หรือเผยแพร่ข้อมูลจำกัดเฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น • ผู้ได้รับข้อมูลสามารถเปิดเผย หรือเผยแพร่ข้อมูลกับผู้ที่เกี่ยวข้องใน หน่วยงานหรือหน่วยงานที่เกี่ยวข้องโดยตรงกับข้อมูล เพื่อปกป้องอันตรายที่อาจเกิดขึ้น • ผู้ส่งข้อมูลมีสิทธิที่จะระบุข้อจำกัดใน การเปิดเผยหรือเผยแพร่ข้อมูลเพิ่มเติมซึ่งผู้ได้รับข้อมูลจะต้องปฏิบัติตามโดยเคร่งครัด
ตัวอย่างข้อมูล	• ขั้นตอนหรือการกระทำย่อยๆ ที่ใช้เพื่อทำให้กลยุทธ์นั้นเป็นจริง เป็นส่วนหนึ่งของกลยุทธ์ที่ระบุว่าเราจะทำอย่างไรเพื่อให้บรรลุเป้าหมายที่วางไว้ Tactics Techniques and Procedures (TTPs) ของ Specific Attacker หรือ เฉพาะกลุ่มของ Threat Actors ที่มี TTP เป็นลักษณะเฉพาะเจาะจง ในการโจมตีหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น • Blocking Rules เช่น IP Blacklist หรือ WAF (Web Application Firewall) Rules ที่มีข้อมูลเป็นลักษณะเฉพาะเจาะจงของหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น

	• Software Security Vulnerability (ช่องโหว่ความปลอดภัยของซอฟต์แวร์) ที่มีข้อมูลเป็นลักษณะเฉพาะเจาะจงหรือมีผลกระทบกับหน่วยงาน หรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น • Security Incident Information ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น • System Logs ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูล หรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น • การโจมตีในรูปแบบต่าง ๆ ที่เกี่ยวข้องกับ Cybersecurity ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับ ข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะภายในหน่วยงานหรือหน่วยงาน ของผู้มีสิทธิได้รับข้อมูลเท่านั้น • ข้อมูลเกี่ยวกับ Identified (หรือ Acting) Botnet Networks ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น • ตัวอย่างมัลแวร์ (Malware Sample) ของหน่วยงานหรือหน่วยงาน ของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูลที่ยังไม่มีการเผยแพร่สู่สาธารณะ ที่สามารถระบุ หน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับ หน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับ ข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะภายในหน่วยงานหรือหน่วยงาน ของผู้มีสิทธิได้รับข้อมูลเท่านั้น • ข้อมูลที่เตรียมทำเป็นข่าว ก่อนการแถลง ประกาศ หรือ เปิดเผย (Press Releases Before Announcement) ซึ่งต้องการให้ผู้รับข้อมูลสามารถ เผยแพร่ข้อมูลเฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิ ได้รับข้อมูลเท่านั้น
ระดับชั้นข้อมูล (TLP)	ข้อมูลในระดับใช้ภายใน
คำอธิบายระดับชั้นข้อมูล	๑. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้อย่าง จำกัด ซึ่งผู้รับข้อมูลสามารถเผยแพร่ข้อมูลชนิดนี้ได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น ๒. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่สำหรับ การสนับสนุนในการดำเนินการแก้ไขหรือ ป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมี ประสิทธิภาพ แต่อาจส่งผลกระทบต่อการดำเนินงาน หรือความเป็นส่วนตัว หรือชื่อเสียงของบุคคล หน่วยงาน หากถูกเผยแพร่ออกไปภายนอกหน่วยงาน หรือหน่วยงานของผู้ได้รับข้อมูล

การเปิดหรือเผยแพร่	• ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่จำกัดเฉพาะเมื่อจำเป็นต้องรู้ (Need to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น • ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลกับหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูล เพื่อปกป้องตนเองหรือ ป้องกันอันตรายที่อาจเกิดขึ้น • ผู้ส่งข้อมูลมีสิทธิที่จะระบุข้อจำกัดในการเปิดเผยหรือเผยแพร่ข้อมูลเพิ่มเติม ซึ่งผู้ได้รับข้อมูลจะต้องปฏิบัติตามโดยเคร่งครัด
ตัวอย่างข้อมูล	• ขั้นตอนหรือการกระทำย่อยๆ ที่ใช้เพื่อทำให้กลยุทธ์นั้นเป็นจริง เป็นส่วนหนึ่งของกลยุทธ์ที่ระบุว่าเราจะทำอย่างไรเพื่อให้บรรลุเป้าหมายที่วางไว้ Tactics Techniques and Procedures (TTPs) ของ Specific Attacker หรือ เฉพาะกลุ่มของ Threat Actors ที่มี TTP เป็นลักษณะเฉพาะเจาะจง ในการโจมตีหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็น ต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลนี้เท่านั้น • Blocking Rules เช่น IP Blacklist หรือ WAF (Web Application Firewall) Rules ที่มีข้อมูลเป็นลักษณะเฉพาะเจาะจงของหน่วยงานหรือหน่วยงานของ ผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น • Software Security Vulnerability (ช่องโหว่ความปลอดภัยของซอฟต์แวร์) ที่มีข้อมูลเป็นลักษณะเฉพาะเจาะจงหรือมีผลกระทบกับหน่วยงาน หรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น • Security Incident Information ที่สามารถระบุหน่วยงานหรือหน่วยงานของ ผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น • System Logs ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูล หรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น • การโจมตีในรูปแบบต่าง ๆ ที่เกี่ยวข้องกับ Cybersecurity ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับ ข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น

	• ข้อมูลเกี่ยวกับ Identified (หรือ Acting) Botnet Networks ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น • ตัวอย่างมัลแวร์ (Malware Sample) ของหน่วยงานหรือหน่วยงาน ของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูลที่ยังไม่มีการเผยแพร่สู่สาธารณะ ที่สามารถระบุ หน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับ หน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น • ข้อมูลที่เตรียมทำเป็นข่าว ก่อนการแถลง ประกาศ หรือ เปิดเผย (Press Releases Before Announcement) ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลชนิดนี้ได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น
ระดับชั้นข้อมูล (TLP)	ข้อมูลในระดับเปิดเผยระหว่างหน่วยงานสมาชิก หรือกลุ่มบุคคลที่มีสิทธิ์เข้าถึงและเกี่ยวข้อง
คำอธิบายระดับชั้นข้อมูล	๑. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้จำกัด เฉพาะระหว่างหน่วยงานหรือหน่วยงานที่เป็นสมาชิกเท่านั้น ๒. เป็นข้อมูลที่เป็นประโยชน์กับสมาชิก ในการสร้างความตระหนักให้กับหน่วยงานหรือผู้ที่เกี่ยวข้อง
การเปิดหรือเผยแพร่	• ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลเฉพาะระหว่างหน่วยงานหรือหน่วยงานของสมาชิกศูนย์ประสานการรักษาความ มั่นคงปลอดภัยระบบคอมพิวเตอร์ ในด้านเดียวกับหน่วยงานเท่านั้น และ ต้องไม่เผยแพร่สู่สาธารณะ โดยการส่งต่อข้อมูลต้องไม่ใช้ช่องทางสาธารณะ ที่ทำให้ข้อมูลแพร่กระจายในวงกว้าง • ในกรณีที่หน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลมีบริษัทใหญ่ หรือบริษัทย่อย หรือบริษัทร่วมหรือ บริษัทย่อยลำดับเดียวกัน ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลได้เฉพาะการนำข้อมูลที่ได้รับไปใช้ เพื่อวัตถุประสงค์ในการป้องกันภัยคุกคาม ทางไซเบอร์ของหน่วยงานหรือของ หน่วยงานของสมาชิกที่อยู่ในขอบเขตของ สกมช. หรือหน่วยงานควบคุมหรือ กำกับดูแล หรือภาคส่วนเท่านั้น เช่น บริษัท A เป็นบริษัทผู้ประกอบกิจการเกี่ยวกับบริการขนส่งทางรางเป็นสมาชิกของศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ บริษัท A สามารถนำข้อมูลที่อยู่ในระดับสีเขียวไปใช้ได้กับหน่วยงานหรือส่วนงานที่ IT Security Officer (หรือเทียบเท่า) ของบริษัท A รับผิดชอบเท่านั้น หากบริษัท A มี บริษัทใหญ่ชื่อบริษัท B ซึ่งไม่ได้อยู่ในภาคระบบการขนส่งทางรางและมีหน่วยงาน หรือส่วนงาน IT Security ของบริษัท B เองแล้วนั้น บริษัท A จะไม่สามารถ แชร์ข้อมูลที่อยู่ในระดับสีเขียวให้ บริษัท B ได้

ตัวอย่างข้อมูล	ข้อมูลทั่วไปเกี่ยวกับสถิติของ Cybersecurity Incidents ที่ไม่ใช่เป็นข้อมูลสาธารณะ หรือจากแหล่งข้อมูลสาธารณะ • ข้อมูลการวิเคราะห์สถิติหรือแนวโน้ม Malware หรือภัยคุกคามทางไซเบอร์ เฉพาะกลุ่มอุตสาหกรรม ที่ไม่ใช่เป็นข้อมูลสาธารณะ หรือจากแหล่งข้อมูล สาธารณะ • รายชื่อ Websites, URLs, Hash ที่เป็นอันตราย (Malicious) หรือข้อมูลเกี่ยวกับ Indicator of Compromise (IoC) ที่สร้างโดย สกมช. หรือหน่วยงานควบคุม หรือกำกับดูแล หรือ ที่ไม่ใช่เป็นข้อมูลสาธารณะ หรือจากแหล่งข้อมูลสาธารณะ • ตัวอย่างมัลแวร์ (Malware Sample) ของหน่วยงานหรือหน่วยงานของผู้ได้รับ ข้อมูลหรือผู้ส่งข้อมูลที่ยังไม่มีการเผยแพร่สู่สาธารณะ • ข้อมูลการติดต่อ สกมช. หรือหน่วยงานควบคุมหรือกำกับดูแล
ระดับชั้นข้อมูล (TLP)	ข้อมูลในระดับเปิดเผยสู่สาธารณะ
คำอธิบายระดับชั้นข้อมูล	๑. เป็นข้อมูลที่สามารถเปิดเผยหรือเผยแพร่สู่สาธารณะได้โดยไม่มีข้อจำกัด ๒. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่สู่ สาธารณะแล้วไม่ส่งผลกระทบต่อการดำเนินงาน หรือความเป็นส่วนตัว หรือชื่อเสียงของบุคคล หน่วยงาน หรือภาครัฐใด ๆ ตลอดจนการเผยแพร่สู่สาธารณะต้องสอดคล้องกับหลักกฎหมายระหว่างประเทศหรือกฎหมายภายในประเทศ ที่เกี่ยวข้อง
การเปิดหรือเผยแพร่	ผู้ได้รับข้อมูลสามารถเปิดเผยหรือ เผยแพร่ข้อมูลสู่สาธารณะได้ภายใต้หลักกฎหมายระหว่างประเทศ หรือกฎหมายภายในประเทศที่เกี่ยวข้อง
ตัวอย่างข้อมูล	• ข้อมูลที่เปิดเผยทั่วไปใน Public Domain • รายชื่อ Websites, URLs, Hash ที่เป็นอันตราย (Malicious) หรือ ข้อมูลเกี่ยวกับ Indicator of Compromise (IoC) ที่สร้างโดย สกมช. หรือ ขร. และกำหนดให้เป็นข้อมูลสาธารณะ หรือจากแหล่งข้อมูลสาธารณะ • ตัวอย่างมัลแวร์ (Malware Sample) จากแหล่งข้อมูลสาธารณะ • ข้อมูลที่เป็นข่าว หลังการแถลง, ประกาศ หรือ เปิดเผย (Press Releases After Announcement)

๗) กำหนดช่องทางแบ่งปันที่ชัดเจน และปลอดภัย และใช้ช่องทางที่กำหนดในการแบ่งปันข้อมูลเท่านั้น เช่น ผ่าน CERT ระบบ Threat Intelligence Sharing Platform เป็นต้น

๘) กำหนดให้มีการจัดเก็บประวัติการแบ่งปันข้อมูลและผู้รับข้อมูล เพื่อให้สามารถตรวจสอบย้อนหลังได้ในกรณีที่ข้อมูลถูกนำไปใช้ไม่เหมาะสม

๓. กำหนดให้มีการอนุมัติการแบ่งปันข้อมูลก่อนทำข้อตกลงในการแบ่งปันข้อมูล จากผู้บริหารระดับสูง หรือผู้ที่ได้รับมอบหมายในการอนุมัติการแบ่งปันข้อมูล รวมถึงขอความเห็นชอบในการดำเนินการทีมกฎหมายหรือผู้มีอำนาจในการทำสัญญา เจ้าหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคลและผู้มีส่วนได้ส่วนเสียหลักอื่น ๆ ที่มีบทบาท ในการรวบรวม นำเข้า จัดเก็บ วิเคราะห์ เผยแพร่ หรือปกป้องข้อมูลภัยคุกคามทางไซเบอร์ รวมถึงกำหนดให้มีผู้ตรวจสอบข้อมูลก่อนดำเนินการแบ่งปันข้อมูล

๔. เมื่อได้รับการแจ้งเตือนด้านความมั่นคงปลอดภัยไซเบอร์ ขร. ต้องดำเนินการพิจารณาว่าการแจ้งเตือนนั้น มาจากแหล่งที่เชื่อถือได้หรือไม่ เมื่อการแจ้งเตือนมาจากแหล่งที่ไม่รู้จักหรือไม่น่าเชื่อถือ หน่วยงานอาจต้องใช้เวลา ตรวจสอบข้อเท็จจริงมากขึ้น หรือขอการยืนยันที่เป็นอิสระ (Independent Confirmation)

ก่อนที่จะดำเนินการ และหากการแจ้งเตือนมีความน่าเชื่อถือและเกี่ยวกับระบบ แอปพลิเคชัน หรือฮาร์ดแวร์ที่ ขร. เป็นเจ้าของ หรือดำเนินการ ขร. ต้องกำหนดขั้นตอนในการตอบสนองต่อการแจ้งเตือนความมั่นคงปลอดภัยไซเบอร์ เพื่อแบ่งปันหรือเผยแพร่ข้อมูลการแจ้งเตือนความมั่นคงปลอดภัยไซเบอร์ให้สมาชิกในกลุ่มทราบถึงช่องโหว่ การใช้ประโยชน์ และปัญหาด้านความมั่นคงปลอดภัยอื่น ๆ ที่เกิดขึ้นใหม่ ข้อมูลที่มักปรากฏในการแจ้งเตือนด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การแจ้งเตือนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและแถลงการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และจัดทำรายงาน ซึ่งประกอบด้วยข้อมูลอย่างน้อย ดังนี้

- ภาพรวมโดยย่อ/บทสรุปสำหรับผู้บริหารและคำอธิบายโดยละเอียด ซึ่งจะรวมถึง สิ่งบอกเหตุการณ์ต่าง ๆ
- แพลตฟอร์มที่ได้รับผลกระทบ (เช่น ระบบปฏิบัติการ แอปพลิเคชัน ฮาร์ดแวร์)
- ผลกระทบ (เช่น ระบบล่ม การขโมยข้อมูล การปล้นแอปพลิเคชัน)
- การจัดระดับความรุนแรง (เช่น Common Vulnerability Scoring System (CVSS))
- ตัวเลือกวิธีการลดผลกระทบ รวมถึงการแก้ไขถาวรหรือวิธีแก้ปัญหาชั่วคราว
- การอ้างอิงสำหรับข้อมูลเพิ่มเติม
- คำอธิบายรายละเอียดของข้อมูลการแจ้งเตือน (Alert Metadata) เช่น วันที่สร้างและวันที่แก้ไขการแจ้งเตือน การรับทราบ

๕. กำหนดให้มีการจัดเก็บข้อมูลภัยคุกคามทางไซเบอร์ และจัดทำเป็นระเบียบฐานความรู้ โดยระบุข้อมูลดังนี้

- แหล่งที่มาของภัยคุกคามทางไซเบอร์ เช่น แหล่งเก็บข้อมูลแบบเปิด (Open Source) และหน่วยงานพันธมิตร
- กฎที่ควบคุมการใช้หรือการแบ่งปันสิ่งบอกเหตุการณ์
- วันที่หรือเวลาที่มีการรวบรวมสิ่งบอกเหตุการณ์
- ระยะเวลาที่ยังคงถือว่าสิ่งบอกเหตุการณ์ความถูกต้อง
- หน่วยงานหรือภาคส่วนที่เป็นเป้าหมายของการโจมตีที่เกี่ยวข้องกับสิ่งบอกเหตุการณ์
- ช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ (Common Vulnerability Enumeration: CVE), แพลตฟอร์มฮาร์ดแวร์ ซอฟต์แวร์ และเฟิร์มแวร์ (Common Platform Enumeration: CPE), จุดอ่อนของซอฟต์แวร์หรือระบบคอมพิวเตอร์ (Common Weakness Enumeration: CWE), การตั้งค่า (Common Configuration Enumeration: CCE) ที่เกี่ยวข้องกับสิ่งบอกเหตุการณ์
- กลุ่มหรือผู้คุกคามที่เกี่ยวข้องกับสิ่งบอกเหตุการณ์
- นามแฝงของผู้คุกคามที่เกี่ยวข้อง
- TTPs ที่ผู้คุกคามใช้กันทั่วไป
- แรงจูงใจหรือเจตนาของผู้คุกคามที่เกี่ยวข้อง
- บุคคลหรือประเภทของบุคคลที่ตกเป็นเป้าหมายในการโจมตีที่เกี่ยวข้อง

- ระบบที่เป็นเป้าหมายในการโจมตี

๖. กำหนดให้ระบุระยะเวลาการเก็บรักษาข้อมูล (Retention Requirement) ให้อยู่ในสภาพพร้อมใช้งาน ซึ่งแยกเป็น การจัดเก็บในระยะสั้น (ออนไลน์) และระยะยาว (ออฟไลน์) ในการจัดการและการเก็บรักษาข้อมูลอาจเปลี่ยนแปลงได้เมื่อข้อมูลภัยคุกคามถูกใช้ประกอบหลักฐาน ตัวอย่างเช่น หลักฐานที่ได้มาระหว่างการสืบสวนสอบสวนเหตุการณ์ภัยคุกคามใด ๆ ควรได้รับการรวบรวม และเก็บรักษาไว้โดยใช้แนวทางปฏิบัติที่ดีที่สุดในการเก็บรักษาข้อมูลตามข้อกำหนดของห่วงโซ่การครอบครองวัตถุพยาน (Chain of Custody) และกฎหมายอื่น ๆ ที่เกี่ยวข้องกับการส่งหลักฐาน โดยพิจารณาเทคนิคทางนิติวิทยาศาสตร์ที่เกี่ยวข้องกับห่วงโซ่การครอบครองวัตถุพยานและการรักษา ความสมบูรณ์ของข้อมูล (Preserving Information Integrity)

๗. การจัดทำและเผยแพร่ข้อมูลภัยคุกคามทางไซเบอร์ที่ ขร. พบและดำเนินการตอบสนองต่อภัยคุกคามนั้น โดยการจัดทำคำอธิบายรายละเอียดของข้อมูลภัยคุกคามทางไซเบอร์ (Metadata) ประกอบด้วยข้อมูลอย่างน้อย ดังนี้ แหล่งที่มา ประเภทข้อมูล เหตุการณ์ สถานะการดำเนินการจัดการ ข้อเสนอแนะการจัดการภัยคุกคาม และการปรับปรุงกฎการแบ่งปันข้อมูล เป็นต้น

ตัวอย่างจัดทำคำอธิบายรายละเอียดของข้อมูลภัยคุกคามทางไซเบอร์ (Metadata)

- การโจมตีแบบกระจายเพื่อให้ระบบปฏิเสธการให้บริการ (Distributed Denial of Service Attacks)
  - วันที่โจมตี(Attack Date)
  - บริการเป้าหมาย (Target Service)
  - เวลาเริ่มการโจมตี(Attack Start)
  - เวลาสิ้นสุดการโจมตี(Attack End)
  - ประเภทการโจมตี(Attack Type)
  - ปริมาณการโจมตี(Attack Volume)
  - ผลกระทบจากการโจมตี(Attack Impact)
  - สถานะการดำเนินการจัดการ
  - ข้อเสนอแนะการจัดการภัยคุกคาม
- การประกาศขอความร่วมมือให้ช่วยกันจู่โจมแบบฟิชชิงหรือสเปียร์ฟิชชิง (Phishing or Spear Phishing Campaigns)
  - คำอธิบายการขอความร่วมมือให้ช่วยกันจู่โจม (Campaign Description)
  - ที่อยู่ผู้ส่ง (Sender Address)
  - ที่อยู่ IP ผู้ส่ง (Sender IP)
  - หัวข้ออีเมล (Email Subject)
  - ไฟล์แนบ/ ชื่อลิงก์/ แฮช (Attachment/ Link Name/ Hash)
  - รายละเอียดข้อมูลในแพ็คเก็ตของการจู่โจม (Payload) และสิ่งบอกเหตุการณ์การโจมตี (Indicators of Compromise: IOCs)
  - สถานะการดำเนินการจัดการ
  - ข้อเสนอแนะการจัดการภัยคุกคาม

๘. กำหนดให้มีการทบทวนกฎระเบียบ ข้อกำหนดของการแบ่งปันข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง โดยพิจารณาจากปัจจัย ดังนี้

- การเปลี่ยนแปลงข้อกำหนดด้านกฎระเบียบหรือกฎหมาย
- การปรับปรุงนโยบายของหน่วยงาน
- บริบทขององค์กร เช่น โครงสร้างการดำเนินการขององค์กร
- การแนะนำแหล่งข้อมูลใหม่ ๆ
- การเปลี่ยนแปลงด้านการยอมรับความเสี่ยง
- การเปลี่ยนแปลงด้านกรรมสิทธิของข้อมูล
- การเปลี่ยนแปลงสภาพแวดล้อมของการดำเนินงาน
- การเปลี่ยนแปลงของภัยคุกคาม
- การควบรวม หรือการปรับเปลี่ยนของหน่วยงาน

ทั้งนี้ ในกรณีที่ สกมช. มีการประกาศกำหนดหลักเกณฑ์และวิธีการ แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงาน และสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้ดำเนินการตามประกาศกำหนดนั้น

๙. กำหนดให้มีการให้ความรู้ความเข้าใจผู้รับผิดชอบในการแบ่งปันข้อมูล ให้สามารถดำเนินการตามแนวทาง การแบ่งปันข้อมูลอย่างปลอดภัย อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

(P) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้มีการจัดทำแผนบริหารความต่อเนื่อง (BCP) เป็นกรอบการบริหารความต่อเนื่องโดยใช้โมเดลวางแผน-ดำเนินการ-ตรวจสอบ-ปรับปรุง (Plan-Do-Check-Act Model) เพื่อการวางแผน การจัดทำการดำเนินการ การติดตาม การทบทวน และการปรับปรุง ประสิทธิผลของแผนความต่อเนื่อง ดังนี้

(๑) ขั้นตอนการวางแผน (Plan) พิจารณาดำเนินการตามรายละเอียด ดังนี้

(๑.๑) ทำความเข้าใจบริบทของ ขร. รวมถึงระบุประเด็นภายนอกและภายในที่อาจส่งผลกระทบต่อความสามารถในการดำเนินงานตามพันธกิจของ ขร. อย่างต่อเนื่อง โดยพิจารณาจากประเด็นเหล่านี้

- วัตถุประสงค์ เป้าหมาย พันธกิจ และหน้าที่ของ ขร.
- การให้บริการของ ขร.
- จำนวนและประเภทของความเสี่ยงของ ขร.
- ความต้องการ และความคาดหวังของผู้ที่มีส่วนเกี่ยวข้องกับการบริหารความต่อเนื่อง
- กฎหมายและระเบียบที่หน่วยงานต้องปฏิบัติตาม

(๑.๒) หลังจากที่ดำเนินการวิเคราะห์บริบทของ ขร. เรียบร้อยแล้ว ให้ดำเนินการกำหนดขอบเขตของการดำเนินงานด้านความต่อเนื่อง และบันทึกขอบเขตในแผนบริหารความต่อเนื่อง โดยขอบเขตอาจระบุถึง

- ส่วนของหน่วยงานที่อยู่ในแผนบริหารความต่อเนื่อง รวมถึงระบุสถานที่ ขนาด ความซับซ้อนของการดำเนินการ เป็นต้น
- กระบวนการหรือบริการที่อยู่ในขอบเขตของการดำเนินการตามแผนบริหารความต่อเนื่อง

(๑.๓) กำหนดบทบาทของผู้บริหารที่ได้รับการแต่งตั้งหรือมอบหมายให้ดำเนินการด้านความต่อเนื่องจะประสบความสำเร็จได้ ซึ่งประกอบด้วยบทบาทหน้าที่อย่างนี้ดังนี้

(๑) กำกับดูแลให้มีการกำหนดนโยบายการจัดการความต่อเนื่อง และกำหนดให้การดำเนินการด้านความต่อเนื่องเป็นส่วนหนึ่งของการบริหารความเสี่ยงแบบองค์รวมขององค์กร รวมถึงจัดทำเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุมัติจากผู้บริหารระดับสูง

(๒) พิจารณาจัดสรรทรัพยากรที่พอเพียงต่อการดำเนินงานด้านความต่อเนื่อง

(๓) สื่อสารให้บุคลากรใน ขร. ทุกคนตระหนักถึงความสำคัญของการดำเนินงานด้านความต่อเนื่องให้มีประสิทธิภาพ

(๔) ส่งเสริมให้มีการปรับปรุงการดำเนินงานตามแผนบริหารความต่อเนื่องอย่างสม่ำเสมอ

(๑.๔) ผู้บริหารระดับสูง หรือผู้ได้รับมอบหมายดำเนินการจัดทำนโยบายความต่อเนื่องที่เหมาะสมกับวัตถุประสงค์ของ ขร. และวัตถุประสงค์ในการบริหารความต่อเนื่อง รวมถึงข้อกำหนดต่าง ๆ ที่เกิดจากการวิเคราะห์บริบทของ ขร. พร้อมทั้งจำให้อยู่ในรูปแบบที่เป็นเอกสาร และสื่อสารให้บุคลากรรับทราบและพร้อมสำหรับการนำไปปฏิบัติ

(๑.๕) กำหนดบทบาทและความรับผิดชอบทีมตอบสนองต่อภัยคุกคาม เช่น ทีมเจ้าหน้าที่ความมั่นคงปลอดภัยไซเบอร์ ทีมสนับสนุนด้านเทคโนโลยีสารสนเทศ ทีมงานปฏิบัติการ (Operation Team) ทีมกฎหมาย และทีมสื่อสารประชาสัมพันธ์ โดยผู้บริหารระดับสูงดำเนินการมอบหมายความรับผิดชอบและอำนาจหน้าที่ให้แก่บุคลากรที่ได้รับการแต่งตั้ง และสื่อสารบทบาทหน้าที่ให้ผู้ปฏิบัติงาน และผู้ได้รับมอบหมายรับทราบปฏิบัติ

(๑.๖) ผู้บริหารระดับสูงดำเนินการแต่งตั้งคณะกรรมการบริหารความต่อเนื่อง ซึ่งประกอบด้วย หัวหน้าหน่วยงาน หัวหน้าส่วนงาน ผู้อำนวยการฝ่ายบริหารความเสี่ยง ผู้เชี่ยวชาญเฉพาะด้าน เป็นต้น เพื่อทำหน้าที่ ดำเนินการบริหารความต่อเนื่อง ดังนี้

(๑) จัดทำระเบียบวิธีปฏิบัติและกระบวนการในการจัดการความต่อเนื่อง รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม

(๒) กำกับดูแลให้มีการกำหนดแผนความต่อเนื่องที่ครอบคลุมเหตุภัยคุกคามทางไซเบอร์ที่อาจ เกิดขึ้น และควรพิจารณาให้เหมาะสมสอดคล้องกับลักษณะการดำเนินภาระกิจของ ขร. ความซับซ้อนของ เทคโนโลยี ความเสี่ยงที่เกี่ยวข้องและภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้น

(๓) พิจารณาขอบเขต ลักษณะวิกฤตการณ์และประเมินสถานการณ์ที่เกิดขึ้น

(๔) พิจารณาประกาศใช้แผนบริหารความต่อเนื่อง และดำเนินการแก้ไขเหตุการณ์ด้านความต่อเนื่องจนกว่าจะเข้าสู่สถานการณ์ปกติ

(๕) แต่งตั้งคณะทำงานย่อยเพื่อสนับสนุนการดำเนินงานได้ความความเหมาะสมและจำเป็น เช่น ทีมจัดการเหตุขัดข้อง ทีมกอบกู้ทรัพยากร

(๖) กำกับดูแลสนับสนุนและติดตามผลการใช้แผนบริหารความต่อเนื่อง เช่น

- ผลการจัดการความต่อเนื่องที่ครอบคลุมเหตุภัยคุกคามทางไซเบอร์
- ผลการทดสอบแผนบริหารความต่อเนื่อง
- ข้อมูลหรือปัญหาที่เกี่ยวข้องกับปัญหาหรือเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก รวมถึงภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๗) กำหนดให้มีการฝึกซ้อมแผนบริหารความต่อเนื่อง และนำผลการซ้อมมาทบทวนนโยบาย ระเบียบวิธีปฏิบัติ การดำเนินงาน และแผนบริหารความต่อเนื่องอย่างน้อยปีละ ๑ ครั้งตามปีปฏิทิน

(๘) กำกับดูแลให้มีการจัดอบรมให้ความรู้แก่คณะกรรมการบริษัท ผู้บริหาร และบุคลากรที่ทำหน้าที่ ปฏิบัติงานตามแผนการบริหารความต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มีความรู้ ความเข้าใจและทักษะที่เพียงพอต่อการกำกับดูแลหรือปฏิบัติงาน

(๙) รายงานผลการปฏิบัติงานต่อผู้บริหารระดับสูง

(๑.๗) การวางแผนเพื่อการจัดทำแผนบริหารความต่อเนื่อง

(๑) กำหนดให้มีการพิจารณาผลการประเมินความเสี่ยงที่เกี่ยวข้องกับการวิเคราะห์บริบทของ ขร. และความต้องการของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งภายใน และภายนอกมาประกอบการวางแผนการบริหารความต่อเนื่อง

(๒) การกำหนดวัตถุประสงค์ความต่อเนื่อง (Business Continuity Objectives) หน่วยงานควรกำหนดวัตถุประสงค์ความต่อเนื่อง (Business Continuity Objectives) ที่มีความสอดคล้องกับนโยบายความต่อเนื่อง รวมถึงสามารถวัดความสำเร็จของวัตถุประสงค์ได้ และตอบสนองต่อผลการวิเคราะห์บริบทของ ขร. และความต้องการของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งภายใน และภายนอก พร้อมทั้งกำหนดให้มีการบันทึกวัตถุประสงค์เป็นลายลักษณ์อักษร เพื่อใช้สื่อสารไปยังบุคลากรที่เกี่ยวข้อง และติดตามการดำเนินงาน ทั้งนี้ วัตถุประสงค์ควรมีเนื้อหาต่อไปนี้

ก) สิ่งที่ต้องทำ

ข) ทรัพยากรที่จำเป็น

ค) ผู้รับผิดชอบ

ง) กำหนดการที่ต้องทำให้เสร็จ และ

จ) วิธีการประเมินผลลัพธ์ของวัตถุประสงค์ที่กำหนดขึ้น

(๓) กำหนดให้มีการวางแผนสำหรับการเปลี่ยนแปลงการดำเนินการตามแผนการบริหารความต่อเนื่อง โดยต้องมีการวางแผนสำหรับการเปลี่ยนแปลง โดยพิจารณาหัวข้อ ดังนี้

ก) วัตถุประสงค์ของการเปลี่ยนแปลงและผลที่อาจเกิดตามมา

ข) ความสมบูรณ์ของการดำเนินงานตามแผนบริหารความต่อเนื่อง

ค) ความพร้อมของทรัพยากร

ง) การจัดสรรอำนาจหน้าที่และความรับผิดชอบ

(๑.๘) กำหนดให้มีวางแผน และจัดเตรียมทรัพยากรและกลไกสนับสนุนที่จำเป็นเพื่อให้บรรลุ วัตถุประสงค์ในการบริหารความต่อเนื่อง รวมถึงการจัดเตรียมบุคลากรให้มีความรู้ และความตระหนักในการดำเนินการตามแผนบริหารความต่อเนื่อง

(๒) ขั้นตอนการดำเนินงาน (Do) เพื่อควบคุมให้เป็นไปตามแผนบริหารความต่อเนื่อง และมีประสิทธิภาพ ควรพิจารณาดำเนินการ ดังนี้

(๒.๑) กำหนดให้ผู้ที่เกี่ยวข้องในการบริหารจัดการความต่อเนื่องปฏิบัติตามแผนการดำเนินการที่ได้วางไว้ และควบคุมกระบวนการที่จำเป็นต่อการบริหารความต่อเนื่อง เพื่อให้เป็นไปตามข้อกำหนด และสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นควรกำหนดข้อมูลเพื่อให้การดำเนินการมีประสิทธิภาพ อย่างน้อยดังนี้

ก) ข้อมูลและเวลาที่ต้องใช้สำหรับการดำเนินการบริหารจัดการความต่อเนื่องในแต่ละกระบวนการที่สำคัญ

ข) วิธีควบคุมกระบวนการที่สำคัญให้ได้ตามกำหนดเวลาของแต่ละกระบวนการ

ค) การเก็บรักษาเอกสารสารสนเทศตามขอบเขต เพื่อให้มั่นใจว่ากระบวนการต่าง ๆ ได้ดำเนินการตามแผนที่วางไว้

ง) ควบคุมการเปลี่ยนแปลงตามแผนบริหารความต่อเนื่อง และทบทวนผลที่ตามมาจากการเปลี่ยนแปลงที่ไม่คาดหมาย เพื่อเป็นการลดผลกระทบที่ไม่พึงประสงค์ใด ๆ

(๒.๒) ในกรณีที่มีการใช้บริการของผู้ให้บริการภายนอก ต้องดำเนินการให้มั่นใจว่ากระบวนการที่ดำเนินการโดยผู้ให้บริการภายนอก และห่วงโซ่อุปทานได้รับการควบคุม เช่น การสอบทานแผนบริหารความต่อเนื่องของผู้ให้บริการภายนอกที่เกี่ยวข้องกับการบริหารความต่อเนื่อง เพื่อพิจารณาความสอดคล้องกับแผนความต่อเนื่องของ ขร. ซึ่งควรพิจารณาอย่างน้อย ดังนี้

ก) สอบทานความสอดคล้องกันของขอบเขต และคำนิยาม

ข) สอบทานการกำหนดระยะเวลาที่สำคัญ เช่น ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerable Downtime: MTD) ระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO)

(๒.๓) กำหนดให้มีการวิเคราะห์ผลกระทบต่อการดำเนินการตามภาระกิจหน้าที่ของ ขร. (Business Impact Analysis: BIA) ซึ่งการวิเคราะห์ผลกระทบต่อการดำเนินการตามภาระกิจหน้าที่ของ ขร. (Business Impact Analysis: BIA) ช่วยให้ ขร. สามารถระบุลักษณะต่าง ๆ ของส่วนประกอบของระบบสารสนเทศ รวมทั้งภารกิจหรือการดำเนินงานสำคัญของ ขร. ได้รับสนับสนุนจากระบบสารสนเทศ รวมถึงการพึ่งพาซึ่งกันและกันของระบบสารสนเทศและการดำเนินงานต่าง ๆ ของ ขร.

(๒.๔) การกำหนดกลยุทธ์ในการบริหารความต่อเนื่อง โดยนำผลลัพธ์จากการวิเคราะห์ผลกระทบต่อการดำเนินการตามภาระกิจหน้าที่ของ ขร. (Business Impact Analysis: BIA) และการประเมินความเสี่ยงของ ขร. มาดำเนินการกำหนดกลยุทธ์ในการบริหารความต่อเนื่อง ให้ครอบคลุมการดำเนินการก่อน ระหว่างและหลังการหยุดชะงักที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ซึ่งกลยุทธ์ในการบริหารความต่อเนื่องมีการพิจารณาในประเด็นดังต่อนี้

ก) กลยุทธ์เป็นไปตามข้อกำหนดด้านเวลาและทรัพยากรที่ต้องใช้ในการกู้ระบบ เพื่อแก้ไขเหตุการณ์ ตามแผนการบริหารความต่อเนื่อง เช่น ข้อกำหนดด้านระยะเวลาสูงสุดที่ยอมให้การดำเนินการของ ขร. หยุดชะงัก เพื่อให้ ขร. สามารถดำเนินการได้อย่างต่อเนื่อง และสามารถฟื้นฟูบริการที่สำคัญให้อยู่ในสภาพพร้อมใช้งานได้ในระดับที่กำหนดภายในกรอบระยะเวลาที่กำหนด

ข) กลยุทธ์ที่สามารถการปกป้องการดำเนินงานที่สำคัญของ ขร. ให้สามารถดำเนินการได้ เช่น การกำหนดให้มีพื้นที่สำรองในการดำเนินงานที่สำคัญของ ขร. ในกรณีเกิดเหตุที่พื้นที่ให้บริการหลักเป็นต้น

ค) กลยุทธ์ที่สามารถลดโอกาสที่จะเกิดการหยุดชะงักได้ เช่น การกำหนดให้มีระบบเครือข่ายสำรอง เพื่อป้องกันการหยุดชะงักในการให้บริการ เป็นต้น

ง) กลยุทธ์ที่สามารถลดระยะเวลาของการหยุดชะงัก เช่น กลยุทธ์ในการย้ายการทำงานไปที่ระบบสำรอง เป็นต้น

จ) กลยุทธ์ที่สามารถจำกัดผลกระทบของการหยุดชะงัก เช่น กลยุทธ์ในการสื่อสารและสร้าง ความสัมพันธ์กับผู้มีส่วนได้ส่วนเสียอยู่เสมอ เพื่อช่วยจำกัดผลกระทบของการหยุดชะงักที่มีต่อผู้รับบริการ เป็นต้น

ฉ) กลยุทธ์ที่สามารถรักษาทรัพยากรให้อยู่ในสภาพพร้อมใช้งานได้อย่างเพียงพอ เช่น การกำหนดให้มีเครื่องคอมพิวเตอร์สำรอง การเก็บข้อมูลสำคัญไว้ที่ศูนย์ข้อมูลสำรอง เป็นต้น

ช) กลยุทธ์ในการบริหารจัดการทรัพยากร โดยระบุความต้องการด้านทรัพยากรที่ต้องใช้ดำเนินการแก้ไขปัญหาด้านความต่อเนื่อง เช่น ทรัพยากรบุคคล ข้อมูล โครงสร้าง พื้นฐานทางกายภาพ เช่น อาคาร สถานที่ทำงาน หรือสิ่งอำนวยความสะดวกอื่น ๆ และระบบสาธารณูปโภคที่เกี่ยวข้อง อุปกรณ์และวัสดุสิ้นเปลือง ระบบเทคโนโลยีสารสนเทศและการสื่อสาร การขนส่งและโลจิสติกส์ การเงิน และผู้ให้บริการภายนอก เป็นต้น

(๒.๕) การจัดทำแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ควรมีรายละเอียดอย่างน้อย ดังนี้

ก) ขอบเขต และวัตถุประสงค์ของแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP)

ข) ขั้นตอนการปฏิบัติงานและผู้รับผิดชอบการดำเนินการบริหารความต่อเนื่อง รวมถึงกำหนดหน้าที่และความรับผิดชอบของผู้ปฏิบัติงานแต่ละรายอย่างชัดเจน และจัดให้มีการสื่อสารและซักซ้อมความเข้าใจถึงหน้าที่ที่ต้องปฏิบัติ ตลอดจนกำหนดรายละเอียดวิธีปฏิบัติงานที่สามารถเข้าใจและปฏิบัติตามได้

ค) ข้อมูลสนับสนุนที่จำเป็นต้องใช้ สำหรับการเรียกใช้งานแผนบริหารความต่อเนื่อง เช่น เกณฑ์และสิทธิ์การเรียกใช้งาน เป็นต้น

ง) ข้อมูลการพึ่งพา (Dependencies) เช่น ข้อมูลหน่วยงานภายนอกหรือผู้ให้บริการภายนอก รวมถึงข้อมูลการพึ่งพาซึ่งกันและกันของการดำเนินงานหรือบริการต่าง ๆ

จ) จัดให้มีทรัพยากรที่จำเป็นสำหรับการปฏิบัติงาน การสื่อสาร และการรายงาน เช่น การจัดหาหรือกำหนดบุคลากรที่จะปฏิบัติงานแทนทั้งระดับ พนักงานและผู้บริหาร แหล่งเงินทุน อุปกรณ์สำนักงาน คอมพิวเตอร์ เครื่องใช้สำนักงาน ระบบเทคโนโลยีสารสนเทศ เป็นต้น หรืออาจพิจารณาจัดตั้งศูนย์ปฏิบัติงานสำรอง (Alternate Site) เพื่อป้องกันผลกระทบจากเหตุฉุกเฉินที่เกิดขึ้นในบริเวณกว้าง

ฉ) กำหนดแนวทางในการสำรองข้อมูล (Backup System) เพื่อทำให้สามารถกู้คืนข้อมูลได้อย่างถูกต้องและรวดเร็ว โดยต้องมีความสอดคล้องกับระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objectives: RPO) โดยต้องกำหนดความถี่ในการสำรองข้อมูลให้เป็นไปตามนโยบาย และแผนการบริหารความต่อเนื่องที่กำหนดขึ้น

ช) การกำหนดผู้ที่มีอำนาจตัดสินใจหรืออนุมัติประกาศใช้แผนบริหารความต่อเนื่อง ซึ่งทำหน้าที่ ตัดสินใจหรืออนุมัติประกาศใช้แผนบริหารความต่อเนื่อง ซึ่งควรเป็นคณะกรรมการหรือผู้บริหารระดับสูง หรือเป็นผู้ที่ได้รับมอบอำนาจจากคณะกรรมการหรือผู้บริหารระดับสูงให้ปฏิบัติหน้าที่แทน

(๒.๖) กำหนดให้มีการดำเนินการซ้อมแผนบริหารความต่อเนื่อง อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เพื่อตรวจสอบความถูกต้อง พร้อมทั้ง จับเวลาในการดำเนินการตามแผนบริหารความต่อเนื่อง เพื่อวัดประสิทธิผลของกลยุทธ์ที่กำหนดซึ่งการดำเนินการฝึกซ้อมแผนบริหารความต่อเนื่องควรมีการพิจารณา ดังนี้

ก) ความสอดคล้องกับวัตถุประสงค์ตามแผนการบริหารความต่อเนื่องที่กำหนดขึ้น

ข) กำหนดวิธีการฝึกซ้อมที่เหมาะสม มีเป้าหมายและวัตถุประสงค์ที่ชัดเจน เช่น หากใช้วิธีการ ฝึกซ้อมด้วยวิธีการแบบอิงการอภิปราย (Discussion-based Exercises) ต้องกำหนดสถานการณ์ (Scenarios) ที่เหมาะสม โดยจำลองจากสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นจริง ซึ่งอิงจากโครงสร้างพื้นฐานของ ขร. เช่น อาคาร วัสดุอุปกรณ์ ระบบสารสนเทศต่าง ๆ และพิจารณานำช่องโหว่ที่อาจเป็นสาเหตุทำให้เกิดสถานการณ์ ฉุกเฉินมากำหนดเป็นสถานการณ์จำลอง และกำหนดบทบาทของมีผู้ที่มีส่วนเกี่ยวข้อง เพื่อเข้าร่วมฝึกซ้อม รวมถึงการเขียนบทสถานการณ์ต้องทำให้ผู้เข้าร่วมฝึกซ้อมได้ปฏิบัติการตอบโต้กับสถานการณ์ได้ฝึกตัดสินใจ ตอบสนองต่อเหตุการณ์ ซึ่งโจทย์สถานการณ์ต้องสามารถเชื่อมโยงกับการปฏิบัติของผู้เข้าร่วมฝึกในแต่ละบทบาท เป็นต้น

ค) การตรวจสอบประสิทธิภาพของกลยุทธ์และแนวทางแก้ไขตามแผนบริหารความต่อเนื่อง

จ) กำหนดให้มีการจัดทำรายงานหลังการฝึกอย่างเป็นทางการ ซึ่งประกอบด้วยผลลัพธ์ คำแนะนำ และการดำเนินการปรับปรุง

(๓) ขั้นตอนการติดตามและทบทวน (Check) เพื่อดำเนินการติดตามและทบทวนผลการปฏิบัติงานตามนโยบายและวัตถุประสงค์ในการบริหารความต่อเนื่อง และกำหนดให้มีการรายงานผลให้ฝ่ายบริหารทบทวน เพื่อกำหนด และอนุมัติการดำเนินการเพื่อแก้ไขและปรับปรุง รวมถึงต้องกำหนดให้มีการเก็บรักษาเอกสารรายงานผลการวิเคราะห์และประเมินผลการดำเนินการตามแผนบริหารความต่อเนื่อง ซึ่งควรพิจารณาให้มีการดำเนินการติดตาม และทบทวนอย่างน้อย ดังนี้

๑) กำหนดกระบวนการที่ต้องติดตามและวัดผลการดำเนินการตามแผนบริหารความต่อเนื่อง

๒) กำหนดวิธีการติดตาม การวัด การวิเคราะห์ และการประเมินผล ตามความเหมาะสม เช่น การจับเวลาขณะซ้อมแผน รวมถึงการจับเวลาการกู้คืนระบบหรือบริการ เป็นต้น

๓) กำหนดผู้ที่มีหน้าที่รับผิดชอบดำเนินการติดตาม และเก็บผลการดำเนินการ

๔) กำหนดผู้ที่มีหน้าที่รับผิดชอบวิเคราะห์และประเมินผลการติดตาม และกำหนดการการส่งผลการวิเคราะห์และประเมินผล

(๔) ขั้นตอนการปรับปรุง (Act) ซึ่งเป็นขั้นตอนในการรักษาและปรับปรุงแผนบริหารความต่อเนื่อง โดยดำเนินการแก้ไขตามผลการทบทวนของฝ่ายบริหาร รวมถึงผลการประเมินและทบทวนขอบเขต และวัตถุประสงค์ของแผนบริหารความต่อเนื่อง ซึ่งควรพิจารณาดังนี้

(๔.๑) การดำเนินการปรับปรุง (Improvement)

๑) กำหนดช่วงเวลาสำหรับการดำเนินการปรับปรุงความไม่สอดคล้องและดำเนินการแก้ไข (Nonconformity and Corrective Action) เมื่อเกิดสิ่งที่ไม่เป็นไปตามแผนการบริหารความต่อเนื่อง วัตถุประสงค์ในการบริหารความต่อเนื่อง หรือบริบทของ ขร. ซึ่งการกำหนดช่วงเวลาในการปรับปรุงหรือแก้ไขต้องเหมาะสมกับผลกระทบที่เกิดขึ้น ซึ่งควรพิจารณาให้มีการดำเนินการ ดังนี้

ก) ตอบสนองต่อสิ่งไม่เป็นไปตามแผนการบริหารความต่อเนื่อง วัตถุประสงค์ในการบริหารความต่อเนื่อง หรือบริบทของ ขร. โดยจัดให้มีการดำเนินการควบคุมและแก้ไข พร้อมทั้งจัดการกับผลที่ตามมา

ข) ประเมินความจำเป็นในการดำเนินการ เพื่อกำจัดสาเหตุที่แท้จริง (Root Cause) ของสิ่งที่ไม่เป็นไปตามแผนการบริหารความต่อเนื่อง วัตถุประสงค์ในการบริหารความต่อเนื่อง หรือบริบทของ ขร. เพื่อไม่ให้เกิดขึ้นซ้ำ หรือไม่ให้เกิดขึ้นที่อื่น โดยหาสาเหตุ และพิจารณาว่ามีสิ่งที่ไม่เป็นไปตามข้อกำหนดที่คล้ายกันอาจเกิดขึ้นที่ใดได้อีก

ค) ทบทวนประสิทธิผลของการดำเนินการแก้ไขที่ได้ดำเนินการเรียบร้อยแล้ว

ง) หากมีความจำเป็น ต้องดำเนินการเปลี่ยนแปลงวิธีปฏิบัติหรือขั้นตอนการดำเนินการในการบริหารความต่อเนื่อง ต้องเก็บรักษาเอกสารข้อมูลที่ระบุรายละเอียดของสิ่งที่ไม่เป็นไปตามแผนการบริหารความต่อเนื่อง วัตถุประสงค์ในการบริหารความต่อเนื่อง หรือบริบทของ ขร. รวมถึงการดำเนินการแก้ไขและผลลัพธ์ของการดำเนินการแก้ไขนั้น ๆ ไว้เพื่อเป็นหลักฐาน

(๔.๒) กำหนดให้มีการปรับปรุงอย่างต่อเนื่อง (Continual Improvement) เหมาะสมกับบริบทของ ขร. และปรับปรุงประสิทธิผลของการดำเนินงานตามแผนบริหารความต่อเนื่อง ทั้งเชิงคุณภาพและเชิงปริมาณ หลังจากพิจารณาผลการวิเคราะห์และการประเมินผล รวมถึงผลจากการทบทวนของผู้บริหาร

๒. กำหนดให้มีการวิเคราะห์ภัยคุกคามหรืออันตรายที่จะเกิดต่อการดำเนินงานที่สำคัญต่อพันธกิจของ ขร. โดยแยกกระบวนการดำเนินการพันธกิจของ ขร. โดยดำเนินการวิเคราะห์ผลกระทบในการดำเนินการตามพันธกิจของ ขร. (BIA) ซึ่งมี ๕ ขั้นตอน ดังนี้

๑) ระบุกระบวนการดำเนินการตามพันธกิจของ ขร. (BIA) โดยคำนึงถึงความสำคัญของกระบวนการหรือบริการที่มีต่อบริการตามพันธกิจของ ขร. เช่น กระบวนการควบคุมและกำกับดูแลผู้ให้บริการขนส่งทางราง กระบวนการตรวจสอบผู้ให้บริการขนส่งทางราง การให้บริการงานด้าน IT ภายในหน่วยงานเป็นต้น

๒) พิจารณาผลกระทบจากการหยุดชะงักของกระบวนการหรือบริการที่สำคัญ

๓) กำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerable Downtime) โดยระยะเวลาดังกล่าวควรเป็นเวลาสูงสุดที่หน่วยงานที่เกี่ยวข้องกับกระบวนการใน ขร. สามารถยอมให้ระบบหรือกระบวนการหยุดชะงักภายใต้เงื่อนไขที่ต้องดำเนินการตามภารกิจหรือการให้บริการที่สำคัญของ ขร. ให้สามารถดำเนินการต่อไปได้

๔) กำหนดทรัพยากรของระบบที่จำเป็นต้องกู้คืนระบบ หรือกระบวนการที่จำเป็น เช่น สถานที่, บุคลากร, อุปกรณ์, ซอฟต์แวร์ ไฟล์ข้อมูลของระบบสารสนเทศ ส่วนประกอบของระบบ และเอกสารบันทึกข้อมูลสำคัญต่าง ๆ ที่เกี่ยวข้อง เพื่อให้หน่วยงานสามารถกลับมาดำเนินการหรือให้บริการที่สำคัญให้ได้ให้เร็วที่สุด

๕) ดำเนินการเชื่อมโยงทรัพยากรที่จำเป็นต่อการกู้คืนระบบกับกระบวนการหรือบริการที่สำคัญของ ขร. เพื่อกำหนดระดับความสำคัญของทรัพยากร และเรียงลำดับการดำเนินการกู้คืนระบบ

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการจัดทำแนวปฏิบัติการบริหารจัดการสำรองข้อมูล โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) จัดทำแนวปฏิบัติการบริหารจัดการสำรองข้อมูล (Backup Policy) และแผนการดำเนินการสำรองข้อมูล (Backup Plan)

๒) กำหนดประเภทของข้อมูลที่ต้องสำรอง เช่น ข้อมูลสำคัญ (Critical Data), ข้อมูลส่วนบุคคล, ข้อมูลทางการเงิน เป็นต้น

๓) กำหนดความถี่ในการสำรองข้อมูล เช่น รายวัน รายสัปดาห์ หรือรายเดือน ตามระดับความสำคัญของข้อมูล (Backup Frequency)

๔) กำหนดพื้นที่การสำรองข้อมูล เช่น External Storage หรือ Cloud Backup เป็นต้น

๕) พิจารณาการสำรองข้อมูลแบบต่าง ๆ ตามความเหมาะสม เช่น สำรองข้อมูลทั้งหมด (Full Backup) สำรองเฉพาะข้อมูลที่เปลี่ยนแปลงตั้งแต่ครั้งล่าสุด (Incremental Backup) หรือสำรองข้อมูลที่เปลี่ยนแปลงตั้งแต่ Full Backup ครั้งล่าสุด (Differential Backup)

๖. กำหนดให้มีมาตรการด้านความปลอดภัยของข้อมูลสำรอง โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) เข้ารหัสข้อมูลสำรอง (Backup Encryption) ทั้งขณะจัดเก็บ (At Rest) และขณะส่งข้อมูล (In Transit)

๒) กำหนดสิทธิ์การเข้าถึงข้อมูลสำรองเฉพาะผู้มีอำนาจเท่านั้น (Access Control)

๓) จัดเก็บข้อมูลสำรองในสถานที่ปลอดภัย และพิจารณาการเก็บข้อมูลสำรองนอกสถานที่ (Offsite Backup) หรือในระบบ Cloud ที่มีมาตรฐานความปลอดภัยสูง

๔) ตั้งค่าการเก็บรักษาข้อมูล (Retention Policy) ให้สอดคล้องกับข้อกำหนดทางกฎหมายและนโยบายขององค์กร เช่น เก็บข้อมูลเป็นระยะเวลา ๕ ปี หรือ ๑๐ ปี เป็นต้น

๗. กำหนดให้มีการทดสอบและการกู้คืนข้อมูล โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) กำหนดแผนการกู้คืนข้อมูล (Data Recovery Plan) ให้สอดคล้องกับแผนความต่อเนื่องทางธุรกิจ (BCP)

๒) ดำเนินการทดสอบการกู้คืนข้อมูล (Backup Restoration Test) อย่างสม่ำเสมอ เช่น ไตรมาสละ ๑ ครั้ง หรืออย่างน้อยปีละ ๑ ครั้ง

๓) บันทึกผลการทดสอบการกู้คืนข้อมูลเพื่อใช้ในการปรับปรุงกระบวนการ

บทที่ ๕
การจำแนกหมวดหมู่ภัยคุกคามทางไซเบอร์ และการรายงานภัยคุกคามทางไซเบอร์

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนดหลักเกณฑ์และวิธีการรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบ ซึ่งในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของ ขร. ขึ้น ขร. ต้องดำเนินการตามกฎหมายกำหนด ดังนี้

๑) ดำเนินการจำแนกหมวดหมู่ภัยคุกคามทางไซเบอร์ ตามตาราง ดังนี้

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

๒) กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่

(๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของ ขร. มีประสิทธิภาพลดลง

(๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีการให้บริการของ ขร. และการโจมตีนั้น มีผลทำให้ระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของ ขร. ไม่สามารถทำงานหรือให้บริการได้

(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤต หมายถึง ภัยคุกคามทางไซเบอร์ที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของ ขร. ในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของ ขร. ที่ให้กับประชาชนล้มเหลวทั้งระบบ จนไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้ และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือ การสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์

ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุข ของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัด หรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

๓) รายงานภัยคุกคามทางไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยดำเนินการ ดังนี้

(๑) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของ ขร. ให้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องของข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ และเป็นภัยคุกคามระดับใด หากตรวจพบต้องดำเนินการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแนวปฏิบัติแผนการรับมือภัยคุกคามทางไซเบอร์ และดำเนินการรายงานไปยัง กกม. โดยใช้เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง โดยอ้างอิงระยะเวลาการแจ้งและรายงานตามข้อ (๓)

(๒) ในกรณีที่มีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของ ขร. ให้จัดทำและส่งรายงานเหตุภัยคุกคามทางไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยอ้างอิงระยะเวลาการแจ้งและรายงานตามข้อ (๓) หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์ โดยใช้เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

(๓) ดำเนินการแจ้ง หรือรายงานภัยคุกคามทางไซเบอร์ ตามระยะเวลา ดังนี้

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	ทุกเหตุการณ์	๓๐ นาที	๔ ชั่วโมง
๒	ทุกเหตุการณ์	๓๐ นาที	๘ ชั่วโมง
๓	ทุกเหตุการณ์	๓๐ นาที	๘ ชั่วโมง
๔	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๘ ชั่วโมง
๕	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๔ ชั่วโมง
๖	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๔ ชั่วโมง
๗	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๑๐ นาที	๑ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๘ ชั่วโมง
๘	-	๒๐ นาที	๔ ชั่วโมง
๙	-	-	๑๒ ชั่วโมง

(๔) จัดทำรายงานประจำปี และส่งรายงานดังกล่าวให้สำนักงาน ภายในวันที่ ๓๑ มกราคม ของปีถัดไป โดยรายงานต้องมีรายละเอียดดังต่อไปนี้

(ก) ระบุจำนวนและลักษณะของเหตุการณ์ภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน ตามแบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี ที่กำหนดท้ายประกาศ ที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗

(ข) วิเคราะห์สาเหตุหรือผลกระทบที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(ค) ปัญหาและอุปสรรคในการดำเนินงาน

(ง) ข้อเสนอแนะต่าง ๆ ซึ่งรวมถึงข้อเสนอแนะเชิงนโยบาย

๔. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมการขนส่งทางราง พ.ศ. ๒๕๖๘

ตามประกาศกรมการขนส่งทางราง เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางราง กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางราง เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมการขนส่งทางรางเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อกรมการขนส่งทางรางนั้น

กรมการขนส่งทางราง จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

ข้อ ๑ คำนิยาม

“ขร.” หมายถึง กรมการขนส่งทางราง (ขร.)

“ผู้ใช้งาน” หมายถึง ผู้บริหารของ ขร. ข้าราชการ พนักงานราชการ ลูกจ้าง (ประจำ/ตามสัญญาจ้างของ ขร.) ผู้ดูแลระบบ ผู้รับบริการ ผู้ใช้งานทั่วไป หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องมือคอมพิวเตอร์และระบบเครือข่ายของ ขร.

“ผู้บริหาร” หมายถึง ผู้มีอำนาจในการบังคับบัญชาใน ขร. ได้แก่ อธิบดีกรมการขนส่งทางราง รองอธิบดีกรมการขนส่งทางราง ผู้อำนวยการสำนัก/กอง เป็นต้น

“ผู้บริหารระดับสูง” หมายถึง อธิบดีกรมการขนส่งทางราง หรือผู้ที่อธิบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของ ขร.

“ผู้ดูแลระบบ (System Administrator)” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“เจ้าของข้อมูล” หมายถึง ผู้ได้รับมอบอำนาจจากผู้บริหารระดับสูง ขร. ให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“สิทธิ์ของผู้ใช้งาน” หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของ ขร. โดย ขร. จะเป็นผู้พิจารณาสิทธิ์ในการใช้สินทรัพย์

“สินทรัพย์” หมายถึง ข้อมูล ระบบข้อมูล ระบบเครือข่าย และทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ ขร. ถือครอง (ทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับ ขร.)

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ ขร. ได้ ได้แก่ ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless Lan)

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

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

“เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)” หมายถึง การเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Expected) ซึ่งอาจทำให้ระบบของ ขร. ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“ระบบอินเทอร์เน็ต (Internet)” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของ ขร. เข้ากับเครือข่ายอินเทอร์เน็ตสากล

“ระบบสารสนเทศ” หมายถึง ระบบของ ขร. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่ ขร. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการ ติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ข้อมูลสารสนเทศ เป็นต้น

“หน่วยงานภายนอก” หมายถึง องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของ ขร. โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจ หน้าที่ และต้องรับผิดชอบในการรักษาความลับข้อมูล

“จดหมายอิเล็กทรอนิกส์ (e-Mail)” หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

“สื่อบันทึกพกพา” หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

“ชื่อผู้ใช้ (Username)” หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้น เพื่อใช้ใน การเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

“รหัสผ่าน (Password)” หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“การเข้ารหัส (Encryption)” หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

“อุปกรณ์จัดเส้นทาง (Router)” หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

“การพิสูจน์ยืนยันตัวตน (Authentication)” หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

“SSID (Service Set Identifier)” หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

“WEP (Wired Equivalent Privacy)” หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับ – ส่งข้อมูลถึงกันจึง ต้องรู้ค่าชุดตัวเลขนี้

“WPA (Wi-Fi Protected Access)” หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

“MAC Address (Media Access Control Address)” หมายถึง หมายเลขเฉพาะที่ใช้ อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหลายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้ จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

“VPN (Virtual Private Network)” หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

“แผนผังระบบเครือข่าย (Network Diagram)” หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของ ขร.

หมวดที่ ๑ นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิ์ และการมอบอำนาจของ ขร. ของรัฐ

๓. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับ ขร. ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑ ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบและธุรกรรมตามความจำเป็นต่อการใช้งานเท่านั้น

ข้อ ๒ บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของ ขร. ให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูง หรือเลขานุการกรม/ผู้อำนวยการกอง/หัวหน้า แล้วแต่กรณีเพื่อให้ความเห็นชอบและอนุญาตก่อน

ข้อ ๓ กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์ใดที่มีผลต่อการเข้าถึงข้อมูลและระบบงาน เพื่อให้การเข้าถึงข้อมูลและระบบงานเป็นไปอย่างเหมาะสม โดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิ์ตามอนุญาตนั้น ดังนี้

๓.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

๓.๒ กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๓.๓ ผู้ดูแลระบบ มีหน้าที่ ควบคุมดูแลการเข้าถึงระบบสารสนเทศและปฏิบัติงานตามผู้บริหารระดับสูง ขร. มอบหมาย ดังนี้

๓.๓.๑ อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของ ขร. จะกระทำได้ต่อเมื่อได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๓.๒ กำหนดสิทธิ์ของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิ์การเข้าถึงนั้นอย่างสม่ำเสมอ

๓.๓.๓ ติดตั้งระบบการบันทึกและติดตามการใช้งานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศของ ขร. อย่างสม่ำเสมอ

ข้อ ๔ จัดแบ่งประเภทของข้อมูล การจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลระดับชั้นการเข้าถึง เวลาเข้าถึง และช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจนโดยใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวถือเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยกำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

๔.๑ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๔.๒ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย อย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย อย่างร้ายแรงมาก
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๔.๓ จัดแบ่งประเภทของข้อมูล

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการให้บริการ เช่น ข้อมูลปริมาณผู้โดยสารขนส่งทางราง ข้อมูลการร้องเรียน ข้อมูลการสมัครงาน ข้อมูลการขอใบอนุญาต เป็นต้น

๔.๔ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นในบังคับบัญชาใน ขร. นั้น
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้หรือได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิ์ที่ได้รับมอบหมายตามอำนาจหน้าที่

๔.๕ รูปแบบของเอกสารอิเล็กทรอนิกส์ให้ถือตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

ข้อ ๕ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

๕.๑ ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบ

๕.๒ กำหนดบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้งานข้อมูลในแต่ละชั้นความลับ

๕.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๕.๔ การกำหนดให้เปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดความสำคัญของข้อมูลแต่ละระดับ

๕.๕ การรับ-ส่งข้อมูลด้วย SSL, VPN หรือ XML Encryption ผ่านระบบเครือข่ายต้องเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๕.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ของ ขร. ออกนอก ขร. รวมถึงการบำรุงรักษาตรวจซ่อมให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึก

๕.๗ กำหนดเวลาการเข้าถึงระบบสารสนเทศ ในบางระบบสารสนเทศหากมีการบันทึกแก้ไขข้อมูลจะทำการประมวลผลตอนเที่ยงคืน หากต้องการเรียกรายงานแบบสมบูรณ์สามารถดำเนินการในเวลาเช้าวันรุ่งขึ้นในวันถัดไป

๕.๘ การกำหนดระยะเวลาการเชื่อมต่อ (Limitation Of Connection Time) สำหรับการใช้งานระบบสารสนเทศบางระบบให้เป็นไปตามช่วงเวลาการทำงานที่ ขร. กำหนด ส่วนระบบสารสนเทศที่มีความสำคัญสูงให้ทำการตัดระบบและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีการใช้งานภายในช่วงระยะเวลา ๑๕ นาที

ข้อ ๖ มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

๖.๑ ควบคุมการเข้าถึงสารสนเทศโดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิ์เกี่ยวข้องกับระบบสารสนเทศ

๖.๒ ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๗ การกำหนดระบบและอุปกรณ์สนับสนุนการปฏิบัติงาน ดังนี้

๗.๑ มีระบบสนับสนุนการทำงานของระบบสารสนเทศของ ขร. ที่เพียงพอต่อความต้องการใช้งาน คือ ระบบรักษาความปลอดภัย (Security) ระบบสำรองกระแสไฟฟ้า (UPS) ระบบระบายอากาศ ระบบปรับอากาศและควบคุมความชื้น

๗.๒ ตรวจสอบหรือทดสอบระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าทำงานได้ปกติและลดความเสี่ยงจากความล้มเหลวในการทำงาน

๗.๓ ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (Data Center) เมื่อมีการทำงานเครื่องผิดปกติหรือหยุดทำงาน

๗.๔ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงจากบุคคลภายนอกและให้แยกอุปกรณ์ที่มีความสำคัญเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

๗.๕ ตรวจสอบ สอดส่องดูแลสภาพแวดล้อมภายในห้องและตรวจสอบระดับอุณหภูมิความชื้นให้อยู่ระดับปกติเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ภายในห้องศูนย์ข้อมูล (Data Center)

๗.๖ การเดินสายไฟสายสัญญาณเครือข่ายของ ขร. และสายเคเบิลอื่นที่จำเป็นต้องทำการวางผ่านเข้าไปในบริเวณที่บุคคลภายนอกเข้าถึงได้นั้นให้ร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสัญญาณ อันจะทำให้เกิดความเสียหายต่อระบบเครือข่ายใช้งานไม่ได้ รวมถึงเพื่อป้องกันจากหนู กระรอก แมลงสาบและสัตว์อื่นกัดสายไฟด้วย

๗.๗ จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนถูกต้อง โดยสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน แล้วให้จัดเก็บสายสัญญาณต่าง ๆ ไว้ในตู้ Rack และปิดใส่สลักกุญแจให้สนิท เพื่อป้องกันการเข้าถึงจากบุคคลภายนอกหรือผู้ที่ไม่มีส่วนเกี่ยวข้อง

ส่วนที่ ๒ การบริหารจัดการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๘ ผู้ดูแลระบบ กำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

๘.๑ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีและสารสนเทศ

๘.๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน ไม่ให้มีการลงทะเบียนซ้ำซ้อน

๘.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ (ตามข้อ ๓)

๘.๔ ผู้ดูแลระบบต้องกำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีและสารสนเทศ

ข้อ ๙ ผู้ดูแลระบบ ต้องกำหนดการใช้งานระบบเทคโนโลยีและสารสนเทศที่สำคัญ โดยมีระบบที่เกี่ยวข้อง คือ บัญชีผู้ใช้งานบนระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศและโปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

ข้อ ๑๐ ผู้ดูแลระบบต้องเก็บบันทึกการปฏิบัติงานของผู้ใช้งาน ได้แก่ บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกอย่างน้อย ๙๐ วัน

ข้อ ๑๑ ผู้ดูแลระบบต้องมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอทุก ๖ เดือน

ข้อ ๑๒ ผู้ดูแลระบบต้องป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิในการเข้าถึงบันทึกเหล่านั้นได้เฉพาะผู้ดูแลระบบเท่านั้น

ข้อ ๑๓ ผู้ดูแลระบบต้องทำการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการโยกย้าย เปลี่ยนตำแหน่ง ลาออกหรือสิ้นสุดการจ้างโดยปฏิบัติตามแนวทาง ดังนี้

๑๓.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามสำนัก/กอง/กลุ่ม

๑๓.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของ ขร. เพื่อดำเนินการทบทวนรายชื่อ และสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

๑๓.๓ ดำเนินการแก้ไขข้อมูลสิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากสำนัก/กอง/กลุ่ม

๑๓.๔ ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง และทบทวนสำหรับผู้ที่มีสิทธิ์ในระดับสูงด้วยความถี่มากกว่าผู้ใช้งาน

๑๓.๕ เมื่อเจ้าหน้าที่มีการโยกย้าย เปลี่ยนตำแหน่ง ลาออก สิ้นสุดการจ้างงาน หรือเปลี่ยนหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้ถอดถอนสิทธิ์ภายใน ๒ วันทำการ

ข้อ ๑๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๑๔.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๑๔.๒ กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๑๔.๓ ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

๑๔.๔ กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

๑๔.๕ กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

๑๔.๖ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๑๔.๗ กำหนดให้มีการตั้งรหัสผ่าน ตามหลักเกณฑ์ ดังนี้

๑๔.๗.๑ รหัสผ่านต้องมีความยาวอย่างน้อย ๖ ตัวอักษร สำหรับผู้ใช้งานที่ได้รับสิทธิปกติ (Regular Users)

๑๔.๗.๒ รหัสผ่านต้องมีความยาวอย่างน้อย ๑๐ ตัวอักษร สำหรับผู้ใช้งานที่ได้รับสิทธิพิเศษ (Privileged Users)

๑๔.๗.๓ รหัสผ่านต้องประกอบด้วยตัวอักษร (a-z) หรือตัวเลข (๐-๙)

๑๔.๗.๔ รหัสผ่านต้องไม่ซ้ำกับบัญชีรายชื่อผู้ใช้ระบบงาน (User ID)

๑๔.๗.๕ เมื่อมีการเปลี่ยนแปลงรหัสผ่านต้องไม่ทำการเปลี่ยนรหัสผ่านโดยการใช้รหัสเดิม (Recycle Password)

๑๔.๗.๖ ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านทุก ๙๐ วัน

๑๔.๘ ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้ยากต่อการคาดเดาและผู้ดูแลระบบ ต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ในการเข้าใช้งานระบบในครั้งแรก

ข้อ ๑๕ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๑๕.๑ ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีทำลายข้อมูลแต่ละประเภทชั้นความลับ (หากข้อมูลมีความลับ)

๑๕.๒ เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑๕.๓ ผู้ดูแลระบบควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงข้อมูลโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับข้อมูล

๑๕.๔ การรับ – ส่ง ข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ VPN

๑๕.๕ มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “การใช้งานรหัสผ่านผู้ใช้งาน”

๑๕.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอก ขร. เช่น บำรุงรักษา การตรวจซ่อมให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๑๕.๗ เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑๕.๘ หากมีการกระทำความผิดเกิดขึ้นจากชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของบุคคลใดบุคคลนั้น ต้องเป็นผู้รับผิดชอบต่อการกระทำความผิดนั้นตามกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง

ข้อ ๑๖ ระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business Information Systems) ให้ผู้บริหารระดับสูงพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่าง ขร. กับกระทรวง หรือหน่วยงานอื่น ๆ ดังนี้

๑๖.๑ กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

๑๖.๒ พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

๑๖.๓ พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

๑๖.๔ พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

๑๖.๕ ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๗ การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

๑๗.๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password)

๑๗.๒ กำหนดรหัสผ่าน ประกอบด้วย ตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวอักษร (Alphabet) ตัวใหญ่ผสมตัวเล็ก ตัวเลข (Numerical Character) และตัวอักษรพิเศษ (Special Character)

๑๗.๓ หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อหรือนามสกุลของตนเอง หรือตรงกับคำในพจนานุกรม

๑๗.๔ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๑๗.๕ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลแบบอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

๑๗.๖ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๑๗.๗ กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการคาดเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

๑๗.๘ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๙๐ วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๑๗.๙ ผู้ใช้งานจะต้องไม่เปิดเผยรหัสผ่านส่วนตัวให้ผู้อื่นทราบหรือนำไปใช้งานแทน

ข้อ ๑๘ การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เหมาะสมและเป็นมาตรฐานสากล

ข้อ ๑๙ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๒๐ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของ ขร. และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดีหรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

๒๐.๑ การเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ของ ขร. คอมพิวเตอร์ทุกประเภทการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

๒๐.๒ การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวต้น และมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๒๐.๓ เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

๒๐.๔ ผู้ใช้งานต้องตั้งเวลาพักหน้าจอ (Screen Saver) หลังจากไม่ได้ใช้งานเป็นเวลา ๑๐ นาที และต้องใส่รหัสผ่าน (Password) ให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

ข้อ ๒๑ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของ ขร. หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๒๒ เอกสารที่เป็นความลับหรือมีระดับความสำคัญ ซึ่งพิมพ์ออกจากเครื่องพิมพ์ (Printer) ตลอดจนข้อมูลที่เป็นความลับในรูปแบบอิเล็กทรอนิกส์ ผู้ใช้งานต้องปฏิบัติให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการ ดังนี้

๒๒.๑ จัดหมวดหมู่เอกสารที่เป็นความลับหรือที่มีระดับความสำคัญสูงไว้ต่างหาก

๒๒.๒ จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ

๒๒.๓ การเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย ต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่เป็นเจ้าของ

๒๒.๔ ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน

๒๒.๕ ทำลายเอกสารที่เป็นความลับ หรือมีระดับความสำคัญสูงเมื่อหมดความจำเป็นในการใช้งาน

ข้อ ๒๓ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของ ขร. และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๔ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๒๕ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร ขร. จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่ ขร. ต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับ ขร. ซึ่ง ขร. อาจแต่งตั้งผู้ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๖ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า

แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของเครื่องคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่อง File Server หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิตทอร์เรนต์ (Bittorrent) หรือ อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูง

ข้อ ๒๗ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง ในระหว่างเวลาปฏิบัติราชการ เช่น การดูหนัง ฟังเพลง เล่นเกม เป็นต้น

ข้อ ๒๘ ห้ามใช้สินทรัพย์ของ ขร. ที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพหรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม กฎหมาย ความมั่นคงของประเทศหรือกระทบต่อภารกิจของ ขร.

ข้อ ๒๙ ห้ามใช้สินทรัพย์ของ ขร. เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อศีลธรรมและกฎหมาย หรือกระทบต่อภารกิจของ ขร.

ข้อ ๓๐ ห้ามใช้สินทรัพย์ของ ขร. เพื่อประโยชน์ทางการค้า

ข้อ ๓๑ ห้ามกระทำใด ๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของ ขร. โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๓๒ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของ ขร. ต้องหยุดชะงัก

ข้อ ๓๓ ห้ามใช้ระบบสารสนเทศของ ขร. เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓๔ ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๕ ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของ ขร. โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓๖ ห้ามผู้ใช้งานกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศชาติ ความปลอดภัยสาธารณะความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะหรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

ข้อ ๓๗ ห้ามผู้ใช้งานทำการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงของชาติเข้าสู่ระบบคอมพิวเตอร์ซึ่งอาจเป็นผลกระทบกับความมั่นคงแห่งราชอาณาจักรหรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

ข้อ ๓๘ ห้ามผู้ใช้งานทำการเผยแพร่ข้อมูลที่เท็จเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมหรือเป็นเท็จไม่ว่าทั้งหมดหรือบางส่วนโดยที่น่าจะเกิดความเสียหายแก่ผู้อื่น

ข้อ ๓๙ ห้ามผู้ใช้งานทำการเผยแพร่ภาพตัดต่อที่เป็นการหมิ่นหรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูล คอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการใด ๆ

ข้อ ๔๐ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

ข้อ ๔๑ ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๐ นาที หรือต่ำกว่านั้น และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

ข้อ ๔๒ ผู้ใช้งานต้องล็อคอุปกรณ์เครื่องคอมพิวเตอร์ที่สำคัญหรือติดตั้งอยู่ในบริเวณที่เข้าถึงได้ยาก เมื่อไม่ได้ถูกใช้งาน

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Asset Management)

ข้อ ๔๓ เจ้าของระบบงานจัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญหรือระบบงานที่สำคัญตามที่กำหนดขึ้น โดยระบุหัวข้อดังนี้

(ก) ชื่อ/คำอธิบายทรัพย์สินของระบบงานที่สำคัญ หรือบริการที่สำคัญ

(ข) ฟังก์ชันที่สำคัญของระบบงานที่สำคัญ หรือบริการที่สำคัญ

(ค) การระบุและการจัดลำดับความสำคัญของทรัพย์สินของระบบงานที่สำคัญ หรือบริการที่สำคัญ

(ง) เจ้าของหรือผู้ดำเนินการของทรัพย์สินของระบบงานที่สำคัญ หรือบริการที่สำคัญ

(จ) ตำแหน่งทางกายภาพของทรัพย์สินของระบบงาน หรือบริการที่สำคัญแต่ละรายการ

(ฉ) การขึ้นต่อกันของทรัพย์สินของระบบงานที่สำคัญ หรือบริการที่สำคัญทางสารสนเทศบนระบบ/เครือข่ายภายใน/หรือภายนอก

ข้อ ๔๔ ผู้ดูแลระบบตรวจสอบทะเบียนทรัพย์สินที่จัดทำขึ้นตามกฎหมายกำหนดอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของ ขร.

ข้อ ๔๕ ผู้ดูแลระบบระบุระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface) ของ ขร. หลังจากที่มีการกำหนดบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร.

ข้อ ๔๖ ผู้ดูแลระบบดำเนินการทบทวนบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. พร้อมทั้งระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญของ ขร.

ข้อ ๔๗ ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) ซึ่งเป็นสถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์บริหารจัดการเครือข่าย ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๘ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๙ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือเครื่องมืออื่นใด เชื่อมเข้าเครือข่ายเพื่อกิจส่วนบุคคล

ข้อ ๕๐ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ ๕๑ ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญและ

ข้อมูลอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์นั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การตัดฝอยด้วยเครื่องทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย ไม่สามารถเข้าถึงสื่อได้
แผ่น CD/DVD	ใช้การตัดฝอยด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย ไม่สามารถเข้าถึงสื่อได้หรือเผาทำลาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย ไม่สามารถเข้าถึงสื่อได้หรือเผาทำลาย

ข้อ ๕๒ ผู้ใช้งาน มีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่ ขร. มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยรายการสินทรัพย์ (Asset List) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์จะถูกบันทึกและตรวจสอบทุกครั้ง โดยเจ้าหน้าที่ที่ ขร. มอบหมาย

ข้อ ๕๓ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมสินทรัพย์ ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงหรือผู้ดูแลที่ได้รับมอบหมาย

ข้อ ๕๔ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของ ขร. ที่ได้รับมอบหมาย

ข้อ ๕๕ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๕๖ ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่ ขร. จัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของ ขร. เท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่ ขร. ไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อ ขร.

ข้อ ๕๗ ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๕๖ ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ข้อ ๕๘ ให้มีการบำรุงรักษาทรัพย์สินสารสนเทศให้มีสภาพพร้อมใช้งานและรองรับการดำเนินงานของ ขร. ได้อย่างต่อเนื่อง พร้อมทั้งวางแผนรองรับทรัพย์สินสารสนเทศที่ใกล้จะสิ้นสุดอายุการใช้งาน (End of Life) หรือสิ้นสุด การสนับสนุนหรือให้บริการจากผู้ผลิต (End of Support) ได้อย่างเหมาะสมทันการณ์ พร้อมทั้งมีมาตรการควบคุมความเสี่ยง ในกรณีที่มีความจำเป็นต้องใช้ทรัพย์สินที่สิ้นสุดอายุการใช้งานหรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต

ข้อ ๕๙ จัดประเภทข้อมูลตามระดับชั้นความลับ และจัดประเภททรัพย์สินสารสนเทศอื่น ๆ ตามระดับความสำคัญ เพื่อให้ทรัพย์สินสารสนเทศได้รับการปกป้องในระดับที่เหมาะสมตามระดับชั้นความลับหรือระดับความสำคัญ โดยกำหนดและจำแนกชั้นความลับของข้อมูลออกเป็น ๔ ประเภท ที่เหมาะสมในการจัดการเอกสาร ทั้งเอกสารตีพิมพ์และเอกสารอิเล็กทรอนิกส์ และการรักษาความปลอดภัยของข้อมูล ซึ่งเอกสารที่ไม่ต้องควบคุม คือ ประเภทเปิดเผย (Public) การจัดระดับชั้นความลับให้พิจารณาจากความสำคัญของข้อมูลในเนื้อความของเอกสารนั้นเป็นหลัก ซึ่งผู้ที่สามารถกำหนดระดับชั้นความลับคือ “เจ้าของข้อมูล” หรือ “เจ้าของระบบ” โดยจะแบ่งระดับชั้นความลับของข้อมูล ดังนี้

Classification	รายละเอียด
ลับที่สุด (Top Secret)	ข้อมูลที่มีการประเมินในด้าน กฎหมาย มูลค่าของข้อมูล ความสำคัญ หรือความอ่อนไหว แล้วว่าหากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วนโดยไม่ได้รับอนุญาต หรือถูกละเมิดความปลอดภัยจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด ทั้งในรูปการเงินและที่ไม่ใช่การเงิน ซึ่งส่งผลกระทบต่อการดำเนินงานของ ขร. การเข้าถึงข้อมูล อนุญาตเป็นรายบุคคล ซึ่งโดยส่วนมากจะเป็นบุคคลหรือกลุ่มคนที่ได้รับมอบหมายหน้าที่พิเศษเท่านั้น หากมีการเข้าถึงจำเป็นต้องมีการลงนามข้อตกลง ไม่เปิดเผยข้อมูล (NDA)
	ตัวอย่างข้อมูล ข้อมูลกลยุทธ์, รหัสสูงสุดของอุปกรณ์สำคัญ เช่น Core Switch, Root ระบบ VM
ลับมาก (Secret)	ข้อมูลที่มีการประเมินในด้าน กฎหมาย มูลค่าของข้อมูล ความสำคัญ หรือความอ่อนไหว แล้วว่าหากมีการเปิดเผยโดยไม่ได้รับอนุญาตหรือถูกละเมิดความปลอดภัยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง ทั้งในรูปการเงินและที่ไม่ใช่การเงิน ซึ่งส่งผลกระทบต่อการดำเนินงานของ ขร. การเข้าถึงข้อมูล อนุญาตเป็นรายบุคคล ซึ่งโดยส่วนมากจะเป็นบุคคลหรือกลุ่มคนที่มีหน้าที่รับผิดชอบในการปฏิบัติงานเฉพาะด้านเท่านั้น
	ตัวอย่างข้อมูล ข้อมูลโครงสร้างเครือข่ายที่ระบุ IP Address ข้อมูลสำรองค่า Configuration ของอุปกรณ์เครือข่าย และ Network Diagram
ลับ (Confidential)	ข้อมูลที่มีการประเมินแล้วว่าเปิดเผยได้เฉพาะภายใน ขร. และบุคคลภายนอกที่มีความสัมพันธ์ในการปฏิบัติภาระกิจของ ขร. ที่ได้รับสิทธิเท่านั้น ไม่เหมาะที่จะเปิดเผย ต่อสาธารณชนเป็นการทั่วไป หากมีการเปิดเผยโดยไม่ได้รับอนุญาต หรือถูกละเมิด ความปลอดภัยทั้งหมด หรือเพียงบางส่วน อาจส่งผลกระทบต่อการดำเนินการของ ขร. การเข้าถึงข้อมูล อนุญาตให้บุคลากรภายใน ขร. หรือบุคคลภายนอกที่มีความสัมพันธ์ในการปฏิบัติภาระกิจของ ขร. ที่สามารถเข้าถึงได้ โดยต้องได้รับอนุญาตจากเจ้าของข้อมูลหรือผู้ดูแลข้อมูล

Classification	รายละเอียด
	ตัวอย่างข้อมูล ข้อมูล Log จากระบบ Network Monitoring ข้อมูลการรายงานผลการตรวจความพร้อมของระบบ Database, Log Database คู่มือปฏิบัติ และคู่มือการให้บริการ
เปิดเผย (Public)	ข้อมูลข่าวสารทั่วไป ซึ่งสามารถเปิดเผยต่อสาธารณชนหรือบุคคลภายใน ขร. การเข้าถึงข้อมูล อนุญาตให้หน่วยงานภายใน ขร. หรือบุคคลทั่วไปเข้าถึงได้
	ตัวอย่างข้อมูล คู่มือการให้บริการ

ข้อ ๖๐ กำหนดให้มีการแสดงระดับชั้นความลับ โดยเจ้าของข้อมูล เพื่อให้ผู้ที่มีสารสนเทศหรือเอกสารสามารถจัดการกับเอกสารหรือสารสนเทศได้อย่างเหมาะสม โดยการแสดงระดับชั้นความลับให้พิจารณา ดังนี้

ประเภทของการแสดงระดับชั้นความลับ	รายละเอียด
การแสดงระดับชั้นความลับทางกายภาพ	- สำเนาถาวร (Hardcopy) ให้ใช้ตัวอักษรตามชั้นความลับที่ขนาดใหญ่กว่าตัวอักษรธรรมดา โดยใช้สีแดงหรือสีอื่นที่สามารถมองเห็นได้เด่นและชัดเจน ที่ กลางหน้ากระดาษ ทั้งด้านบนและด้านล่างของทุกหน้าเอกสารนั้น ถ้าเอกสารเข้าปกให้แสดงไว้ที่ด้านนอกของปกหน้าปกหลังด้วย เพื่อแยกประเภทเอกสารตามระดับชั้นความลับ โดยเจ้าของข้อมูลเป็นผู้กำหนดระดับชั้นความลับของเอกสารนั้น - สื่อบันทึกข้อมูล (Media) เขียนระบุระดับชั้นความลับตรงที่สามารถเห็นได้ชัดเจน โดยเจ้าของข้อมูลเป็นผู้กำหนดระดับชั้นความลับของสื่อนั้น - ข้อมูลข่าวสารที่มีสภาพเป็นจานบันทึก แถบบันทึก ฟิล์มบันทึกภาพทุกประเภท หรือสิ่งบันทึกที่สามารถแสดงผลหรือสื่อความหมายโดยกรรมวิธีใด ๆ ให้แสดงชั้นความลับไว้ที่ต้นและปลายม้วนฟิล์ม หรือต้นและปลายของข้อมูลข่าวสารหรือบนวัสดุ หรือบนภาชนะที่บรรจุ ถ้าไม่สามารถแสดงชั้นความลับไว้ในที่ดังกล่าวได้ให้เก็บในกล่องหรือหีบห่อ ซึ่งมีเครื่องหมายแสดงชั้นความลับนั้น
การแสดงระดับชั้นความลับทางอิเล็กทรอนิกส์	- สำเนาอิเล็กทรอนิกส์ (Soft File) ระบุระดับชั้นความลับ โดยเจ้าของข้อมูลเป็นผู้กำหนดระดับชั้นความลับของเอกสารนั้น - ให้แสดงชั้นความลับไว้ที่ต้นและปลายของสื่อประสม (Multimedia) เช่น วีดีโอ เป็นต้น

หมายเหตุ การแสดงระดับชั้นความลับทางกายภาพ อาจใช้เป็นรหัสแทนข้อความของประเภทระดับชั้นความลับ เพื่อป้องกันผู้ที่ไม่ได้รับอนุญาตล่วงรู้ระดับชั้นความลับของทรัพย์สินนั้น ๆ

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๖๑ มาตรการควบคุมการเข้า-ออก ห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) ดังนี้

๖๑.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor) แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๖๑.๒ ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน และต้องได้รับการอนุญาตจากหัวหน้ากลุ่มเทคโนโลยีและสารสนเทศ และผู้อำนวยการกองยุทธศาสตร์และแผนงานตามลำดับ

๖๑.๓ ผู้ดูแลระบบหรือผู้ได้รับมอบหมาย ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก และแบบฟอร์มการขออนุญาตเข้าออกกับเจ้าหน้าที่กับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อ ๖๒ ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของ ขร. ต้องได้รับอนุญาตจากผู้บริหารระดับสูงและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย”

ข้อ ๖๓ การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่ ขร. รับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารระดับสูง และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ

ข้อ ๖๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๖๕ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๖๕.๑ ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๖๕.๒ ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๖๕.๓ ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

๖๕.๔ ระบบเครือข่ายทั้งหมดของ ขร. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก ขร. ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๖๕.๕ ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention Systems/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของ ขร. ในลักษณะที่ผิดปกติ

๖๕.๖ การเข้าสู่ระบบเครือข่ายภายใน ขร. โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๖๕.๗ ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของ ขร.

๖๕.๘ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๖๕.๙ การระบุอุปกรณ์เครือข่าย

- ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
- อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย
- ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
- อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของต้นทางและปลายทางได้
- ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” โดยดาวน์โหลดผ่านเว็บไซต์ของ ขร.
- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวจนทุกครั้งที่ใช้อุปกรณ์

๖๕.๑๐ กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่ายเมื่อเว้นว่างจากการใช้งานเป็นเวลานาน

ข้อ ๖๖ ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๖๗ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

ข้อ ๖๘ กำหนดให้มีการจัดเก็บซอร์สโค้ด (Source Code) ไลบรารี่ (Library) และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ ๖๙ การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไม่น้อยกว่า ๙๐ วัน เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุตัวบุคคลได้ตามแนวทางพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ข้อ ๗๐ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบตามแนวทางปฏิบัติ ดังต่อไปนี้

๗๐.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของ ขร. จะต้องมีหนังสือขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บริหารระดับสูง

๗๐.๒ มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๗๐.๓ วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้บริหารระดับสูง

๗๐.๔ การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับ ขร. อย่างเพียงพอ

๗๐.๕ การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศใน ขร. จากระยะไกล ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๗๑ กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

๗๑.๑ Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

๗๑.๒ Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

ข้อ ๗๒ กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ ๗๓ ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอก ขร. ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ ๗๔ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของ ขร. ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ข้อ ๗๕ IP Address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้ ขร. ภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ข้อ ๗๖ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๗๗ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของ ขร. (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๓) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายใน ขร. เป็นต้น

ข้อ ๗๘ กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

๗๘.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๗๘.๒ หลังจากระบบติดตั้งเสร็จ ต้องมีระบบบริหารจัดการรหัสผ่าน ที่สามารถทำงานเชิงโต้ตอบหรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการเปลี่ยนรหัสผ่านของผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๗๘.๓ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๗๘.๔ ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการลงบันทึกเข้าใช้งาน (Login) ทุกครั้ง

๗๘.๕ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของ ขร. ร่วมกัน

๗๘.๖ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๗๘.๗ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูง

๗๘.๘ ซอฟต์แวร์ที่ ขร. ใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

๗๘.๙ ซอฟต์แวร์ที่ ขร. จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๗๘.๑๐ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของ ขร. เพื่อประโยชน์ทางการค้า

๗๘.๑๑ ห้ามผู้ใช้งาน นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้งานมีสิทธิ์ในการนำข้อมูลข่าวสารขึ้นบนเว็บไซต์หรือนำเข้าข้อมูลสู่ระบบสารสนเทศหรือบนเครือข่ายคอมพิวเตอร์

๗๘.๑๒ ห้ามผู้ใช้งานของ ขร. ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูง

ข้อ ๗๙ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งานแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง โดยปฏิบัติตามแนวทางที่กำหนดไว้ในข้อ ๑๔

ข้อ ๘๐ การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งาน โปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการ ดังนี้

๘๐.๑ การใช้งานโปรแกรมยูทิลิตี้ ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน

๘๐.๒ โปรแกรมยูทิลิตี้ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

๘๐.๓ ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

๘๐.๔ มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

๘๐.๕ ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

ข้อ ๘๑ การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

๘๑.๑ กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน เมื่อมีการว่างเว้นจากการใช้งาน เป็นเวลา ๓๐ นาทีเป็นอย่างน้อย ต้องยุติการใช้งานระบบสารสนเทศ (Session Time-out) นั้น

๘๑.๒ ระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นตามความเหมาะสม หรือเป็นเวลา ๑๐ นาที

ข้อ ๘๒ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

๘๒.๑ ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศ หรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัย ดังนี้

- กำหนดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับระบบสารสนเทศ หรือแอปพลิเคชันที่มีความเสี่ยง หรือมีความสำคัญสูง เพื่อให้ผู้ใช้งาน สามารถใช้งานได้นานที่สุด ภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้ได้ ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง

- กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร มีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุและพิสูจน์ตัวตน เพื่อเข้าใช้งานใหม่ทุกครั้ง

๘๒.๒ กำหนดให้ระบบสารสนเทศ ที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอก ขร.) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ ภายใน ๓๐ นาที

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ข้อ ๘๓ ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๓) เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายใน ขร. เป็นต้น

ข้อ ๘๔ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บริหารระดับสูงเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๘๕ ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกิน ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

ข้อ ๘๖ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

๘๖.๑ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๘๖.๒ กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๘๖.๓ กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๘๖.๔ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารระดับสูง โดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้ รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๘๗ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๘๗.๑ ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๘๗.๒ ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

๘๗.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๘๗.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

๘๗.๕ กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๘๗.๖ กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๘๗.๗ ต้องสำรองข้อมูลและระบบ และทดสอบการกู้คืนข้อมูลและระบบอย่างสม่ำเสมอ โดยกำหนดความถี่ในการดำเนินงานอย่างชัดเจนในแต่ละระบบ

๘๗.๘ ไม่เก็บข้อมูลสำคัญขององค์กรไว้บนอุปกรณ์แบบพกพา เว้นแต่มีความจำเป็น และข้อมูลดังกล่าวจะต้องมีการเข้ารหัสข้อมูลที่เป็นมาตรฐาน

๘๗.๙ ข้อมูลที่มีชั้นความลับที่ต้องส่งออกไปนอกองค์การ โดยถูกจัดเก็บไว้บนอุปกรณ์แบบพกพาหรือถูกส่งผ่านระบบเครือข่ายไร้สาย ต้องผ่านการอนุมัติจากเจ้าของระบบงาน และธุรกรรม และทำการเข้ารหัสข้อมูลและระบบเครือข่ายไร้สายก่อนเท่านั้น

๘๗.๑๐ การเคลื่อนย้ายข้อมูลที่มีชั้นความลับ ต้องกระทำโดยบุคคลที่เจ้าของระบบงานและธุรกรรมกำหนด และจะต้องทำลายข้อมูลดังกล่าวทันทีเมื่อไม่มีการใช้งานแล้ว

ข้อ ๘๘ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

๘๘.๑ ระบบที่ไวต่อการรบกวน โดยมีผลกระทบและมีความสำคัญสูง ได้แก่ ระบบบริหารงานบุคคล ที่เป็นข้อมูลส่วนบุคคลของเจ้าหน้าที่ภายใน (ข้อมูลประวัติ การลา การสแกนหน้า/นิ้วเข้า-ออกปฏิบัติงาน) ระบบฐานข้อมูลผู้ประกอบการและการออกใบอนุญาตด้านการขนส่งทางรางผ่านระบบดิจิทัล (e-License R)

๘๘.๒ ต้องมีการควบคุมสภาพแวดล้อมของระบบที่ไวต่อการรบกวนโดยเฉพาะ

- กำหนดสิทธิ์ให้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว (ในทางกายภาพสามารถแยกเป็นสัดส่วน)

- ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่นและกำหนดสิทธิ์ในการเข้าถึงข้อมูล

๘๘.๓ ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร

ข้อ ๘๙ การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

๘๙.๑ ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

๘๙.๒ ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

๘๙.๓ เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

๘๙.๔ เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

๘๙.๕ หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malware)

ข้อ ๙๐ ขร. ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น ซอฟต์แวร์ที่ ขร. อนุญาตให้ใช้งานหรือที่ ขร. มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๙๑ ซอฟต์แวร์ (Software) ที่ ขร. ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาต จากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ ๙๒ คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่ ขร. ได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากผู้บริหารระดับสูง

ข้อ ๙๓ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๙๔ ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๙๕ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๙๖ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๙๗ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของ ขร. หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูง

ข้อ ๙๘ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของ ขร. สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการ ดังนี้

๙๘.๑ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูล บุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

๙๘.๒ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

๙๘.๓ พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๙๘.๔ พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

๙๘.๕ นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีผู้ใช้งานมีสิทธิ์ในการนำข้อมูลข่าวสารขึ้นบนเว็บไซต์หรือนำเข้าข้อมูลสู่ระบบสารสนเทศหรือบนเครือข่ายคอมพิวเตอร์

ข้อ ๙๙ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software Development)

๙๙.๑ จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๙๙.๒ พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๙๙.๓ พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๙๙.๔ ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๙๙.๕ หลังจากการส่งมอบการพัฒนาซอฟแวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

๙๙.๖ ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องลงนามในสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ก่อนดำเนินการ

๙๙.๗ ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องถือปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของ ขร.

๙๙.๘ ในกรณีผู้รับจ้างที่ให้บริการจากภายนอกมีการเข้าใช้ระบบคอมพิวเตอร์ภายใน ขร. ผู้รับจ้างที่ให้บริการจากภายนอก จะต้องแจ้งรายชื่อผู้ที่จะเข้ามาใช้ระบบคอมพิวเตอร์ล่วงหน้า และต้องมีการลงชื่อเข้าใช้งานห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ทุกครั้งที่มีการเข้าใช้งาน นอกจากนี้ หากผู้รับจ้างที่ให้บริการจากภายนอกต้องใช้งานห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ ในวันหยุดหรือนอกเวลาราชการจะต้องขออนุญาตจากผู้รับผิดชอบหรือผู้ดูแลระบบล่วงหน้า

๙๙.๙ หน่วยงานภายนอกต้องทำการบันทึกค่า Config และ/หรือซอร์สโค้ดเดิม ทุกครั้งที่จะมีการแก้ไขค่า Config ซอร์สโค้ดระบบงานสารสนเทศบนระบบ Production หากการแก้ไขมีปัญหาเกิดขึ้น ผู้รับจ้างที่ให้บริการจากภายนอกจะสามารถใช้ค่าและ/หรือซอร์สโค้ดเดิม เพื่อให้ระบบสามารถกลับมาใช้งานได้

๙๙.๑๐ ซอฟต์แวร์ที่ถูกพัฒนาจากหน่วยงานภายนอก หากมีการติดตั้งบริการผ่านระบบเครือข่ายคอมพิวเตอร์ภายใน ขร. จะมีการจัดให้ทำ Penetration Test อย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นการตรวจสอบหาช่องโหว่บนระบบซอฟต์แวร์ดังกล่าว เพื่อนำข้อมูลที่ได้มาปรับปรุงการรักษาความปลอดภัยให้กับระบบซอฟต์แวร์ดังกล่าว เพื่อลดความเสี่ยงในการถูกโจมตีจากผู้ไม่ประสงค์ดีจากภายนอก

ส่วนที่ ๙ การปฏิบัติงานจากภายนอก ขร. (Teleworking) และการเชื่อมต่อระยะไกล (Remote Connection)

ข้อ ๑๐๐ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของ ขร. จากระยะไกล มีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่ ขร. กำหนด

ข้อ ๑๐๑ ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

ข้อ ๑๐๒ ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตนก่อนการใช้งาน เพื่อเพิ่มความปลอดภัย เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ข้อ ๑๐๓ ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ ขร. จากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของ ขร.

ข้อ ๑๐๔ ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่าง ๆ ของ ขร. ที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

ข้อ ๑๐๕ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิในการเข้าถึงระบบสารสนเทศ และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

ข้อ ๑๐๖ ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระบบระยะไกลทั้งหมดมายังบริการที่สำคัญของ ขร. มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต และในการกำหนดมาตรการควบคุมในการรักษาความมั่นคงปลอดภัยสำหรับปฏิบัติงานจากระยะไกลนั้น ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(๑) ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกลเมื่อจำเป็นเท่านั้น

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

(๓) กำหนดให้มีการเข้ารหัสที่เก็บข้อมูล (Use Storage Encryption) บนอุปกรณ์การทำงานจากระยะไกล เพื่อปกป้องข้อมูลที่มีความอ่อนไหวทั้งหมด เช่น กำหนดให้เข้ารหัสดิสก์เต็มรูปแบบ เพื่อลดความเสี่ยงจากผู้โจมตีที่ได้รับสิทธิเข้าถึงทางกายภาพ รวมกับการเข้ารหัสดิสก์เสมือน (Virtual Disk) หรือการเข้ารหัสไฟล์/โฟลเดอร์ และกำหนดให้มีการเข้ารหัสข้อมูลที่เกิดจากการทำงานจากระยะไกล (Telework Data) ที่อยู่ในสื่อเก็บข้อมูลแบบถอดได้ (Removable Media)

(๔) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของ ขร. เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ

(๕) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ สำหรับการเชื่อมต่อ เช่น การเปิดบริการ หรือฟังก์ชันบนเครื่องแม่ข่ายให้แก่การทำงานจากระยะไกลเฉพาะบริการหรือฟังก์ชันที่จำเป็นเท่านั้น รวมถึงการกำหนดสิทธิการเข้าถึงข้อมูล เช่น ไม่ให้ส่งไฟล์ไปยังเครื่องแม่ข่าย ไม่ให้

เข้าถึงข้อมูล อ่านข้อมูลได้อย่างเดียว หรือ อ่านและเขียนได้ รวมถึงตั้งค่า Firewall เพื่ออนุญาตการเชื่อมต่อกับบริการหรือฟังก์ชันบนเครื่องแม่ข่ายในกรณีที่จำเป็นเท่านั้น

ข้อ ๑๐๗ ผู้ดูแลระบบต้องกำหนดให้มีการเก็บบันทึกการเข้าถึงระบบจากระยะไกล โดยในการบันทึกจะต้องประกอบด้วยข้อมูลที่สำคัญที่จำเป็นต้องทราบ เช่น ชื่อสกุลของผู้ที่ต้องการเข้าถึงระบบจากระยะไกล ระยะเวลาในการเข้าถึง และสาเหตุที่ต้องการเข้าถึง โดยจะต้องหมั่นตรวจสอบข้อมูลที่มีการบันทึกไว้อย่างสม่ำเสมอ

ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ ๑๐๘ ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๑๐๙ ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน และกำหนดให้ซ่อน SSID (Service Set Identifier) โดยเฉพาะระบบงานที่เป็นชั้นความลับ ดังกล่าวด้วย

ข้อ ๑๑๐ ผู้ดูแลระบบ ต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) หรือที่ดีกว่า ในการเข้ารหัสข้อมูลระหว่างเครื่องลูกข่าย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) และกำหนดค่าโดยไม่ให้แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๑๑๑ ผู้ดูแลระบบ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และหรือบัญชีผู้ใช้งาน โดยอนุญาตเฉพาะผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สายตามที่กำหนดไว้ เท่านั้น

ข้อ ๑๑๒ ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๑๑๓ ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๑๑๔ ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

ข้อ ๑๑๕ ผู้ดูแลระบบ ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานต่อผู้บังคับบัญชาทราบทันที

ข้อ ๑๑๖ ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบเครือข่ายและระบบสารสนเทศภายในหน่วยงาน

ข้อ ๑๑๗ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ ขร. จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

ข้อ ๑๑๘ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งทำการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ข้อ ๑๑๙ การสร้างบัญชีการใช้งานระบบเครือข่ายไร้สายให้กับบุคคลภายนอกนั้น จะต้องทำการกำหนดให้ ๑ บัญชี ไม่สามารถใช้ได้เกินกว่า ๑-๒ อุปกรณ์เท่านั้น เพื่อเป็นการป้องกันการนำบัญชีดังกล่าวไปแจกจ่ายยังบุคคลภายนอกอื่น ๆ ที่ไม่ได้ทำการขออนุญาต

ข้อ ๑๒๐ ผู้ดูแลระบบต้องทำการกำหนดช่วงระยะเวลาการหมดอายุ (Session Timeout) ในการใช้งานระบบเครือข่ายไร้สายของบุคคลภายนอกทุกครั้งโดยไม่มีข้อยกเว้น ในกรณีที่บุคคลภายนอกดังกล่าวมีความต้องการใช้งานเพิ่มเติมให้ทำการแจ้งความประสงค์ในการใช้งานมายังผู้ดูแลระบบเพื่อทำการขยายเพิ่มเติมระยะเวลาในการใช้งาน

ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๑๒๑ หน่วยงานมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

ข้อ ๑๒๒ การกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

ข้อ ๑๒๓ ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดย Firewall

ข้อ ๑๒๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

ข้อ ๑๒๕ การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่าง ๆ ของ Firewall

ข้อ ๑๒๖ การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๑๒๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๒๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากหน่วยงานก่อน

ข้อ ๑๒๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่ายต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการกองยุทธศาสตร์และแผนงาน โดยต้องระบุข้อมูล ดังนี้

๑๒๙.๑ หมายเลข Port ที่ต้องการขอให้เปิด

๑๒๙.๒ หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๑๒๙.๓ วัตถุประสงค์ หรือชื่อแอปพลิเคชันที่ต้องการใช้งานผ่าน Port นั้น ๆ

ข้อ ๑๓๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ป้องกันเครือข่าย (Firewall) เป็นประจำทุกเดือนและทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ ๑๓๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ภายในหน่วยงานที่มีลักษณะที่เป็นอินทราเน็ตจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๓๒ หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดหรือเสี่ยงต่อความปลอดภัยของระบบเครือข่ายส่วนรวม หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๑๓๓ การเชื่อมต่อในลักษณะของการควบคุมระยะไกล (Remote Login) จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน ต้องดำเนินการ ดังนี้

๑๓๓.๑ ขออนุญาตการใช้งานเป็นลายลักษณ์อักษร

๑๓๓.๒ เก็บข้อมูล Logfile ที่ Firewall

๑๓๓.๓ เก็บ Logfile จากตัว Application

ข้อ ๑๓๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการให้บริการทันทีจนกว่าจะได้รับการแก้ไข

ข้อ ๑๓๕ ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (e-Mail)

ข้อ ๑๓๖ ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (e-Mail) ต้องทำการกรอกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-Mail) โดยยื่นคำขอกับเจ้าหน้าที่ ขร.

ข้อ ๑๓๗ รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ “๐” ในการพิมพ์แต่ละตัวอักษร

ข้อ ๑๓๘ เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ให้เปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ ๑๓๙ ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ เช่น ไม่เกิน ๓ ครั้ง

ข้อ ๑๔๐ ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๑๔๑ เปลี่ยนรหัสผ่าน (Password) ทุก ๙๐ วัน

ข้อ ๑๔๒ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-Mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (e-Mail) ของตน

ข้อ ๑๔๓ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๑๔๔ การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล e-Mail ที่หน่วยงานกำหนดไว้ และให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ e-Mail ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๑๔๕ ห้ามส่งจดหมายอิเล็กทรอนิกส์ (e-Mail) ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail) หรือจดหมายลูกโซ่ (Chain Letter) หรือที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น หรือที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๔๖ ให้ระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ (e-Mail) ทุกฉบับที่ส่งไป

ข้อ ๑๔๗ ให้ทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ (e-Mail) ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ ๑๔๘ ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๔๙ ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

ข้อ ๑๕๐ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ ๑๕๑ ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Inbox) ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๑๕๒ ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อ ๑๕๓ ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ภาครัฐ สำหรับใช้รับ-ส่งข้อมูลในระบบราชการตามมติคณะรัฐมนตรีเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet)

ข้อ ๑๕๔ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากผู้บริหารระดับสูงเป็นลายลักษณ์อักษร

ข้อ ๑๕๕ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ ๑๕๖ ในการรับ-ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการตรวจจับไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูล

ข้อ ๑๕๗ ห้ามใช้เครือข่ายอินเทอร์เน็ตของ ขร. เพื่อกระทำการต่อไปนี้

๑๕๗.๑ หาประโยชน์ในเชิงธุรกิจส่วนตัว

๑๕๗.๒ เพื่อความบันเทิง ได้แก่ การเล่นเกม ดูภาพยนตร์ ฟังเพลง

๑๕๗.๓ กระทำการที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงขององค์กร เช่น การเผยแพร่ข้อมูลที่อาจก่อความเสียหายต่อองค์กร หรือข้อมูลสำคัญที่เป็นความลับขององค์กร

๑๕๗.๔ กระทำผิดกฎหมาย เช่น

- นำเข้าหรือเผยแพร่ข้อมูลหรือชุดโปรแกรมที่ละเมิดลิขสิทธิ์
- แพร่กระจายโปรแกรมไม่ประสงค์ดี (Malware) เช่น ไวรัสคอมพิวเตอร์
- กระทำการที่ไม่เหมาะสมขัดต่อศีลธรรม เช่น การเล่นพนันออนไลน์ การนำเข้าหรือเผยแพร่สื่อลามก อนาจาร
- กระทำการที่ส่งผลร้ายกระทบกับความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เช่น การก่อการร้าย
- กระทำการข่มขู่ คุกคาม หรือละเมิดสิทธิ์ของผู้อื่นให้ได้รับความเสียหาย เช่น การนำเข้าหรือเผยแพร่ภาพ เสียง สื่อผสมภาพและเสียง (Multimedia) ของผู้อื่น ทั้งที่เป็นข้อมูลจริงหรือข้อมูลเท็จอันเกิดจากการสร้าง ตัดต่อ แต่งเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่ทำให้ผู้อื่นนั้นเสีย ชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
- กระทำการเป็นภัยต่อสังคม เช่น การนำเข้าหรือเผยแพร่ ข้อมูลที่มีลักษณะอันเป็นเท็จเพื่อสร้างความสับสนวุ่นวาย หรือเพื่อการหลอกลวงให้เกิดความเสียหายต่าง ๆ

ข้อ ๑๕๘ ในการใช้งานระบบเครือข่ายอินเทอร์เน็ต ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของ ขร. หรือเกี่ยวกับงานของ ขร. ที่ซึ่งยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๑๕๙ ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๑๖๐ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ ขร. การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

ข้อ ๑๖๑ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

ข้อ ๑๖๒ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๑๖๓ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ข้อ ๑๖๔ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ/หรือกฎหมาย ระเบียบ วิธีปฏิบัติทางคอมพิวเตอร์ อื่น ๆ ที่เกี่ยวข้อง อย่างเคร่งครัด

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ข้อ ๑๖๕ แนวทางปฏิบัติการใช้งานทั่วไป

๑๖๕.๑ เครื่องคอมพิวเตอร์ที่ ขร. อนุญาตให้ใช้งานเป็นสินทรัพย์ของ ขร. เพื่อใช้ในงานราชการ

๑๖๕.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่ ขร. ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๖๕.๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของ ขร.

๑๖๕.๔ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของ ขร. หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับ ขร. เท่านั้น

๑๖๕.๕ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๑๖๕.๖ ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๑๖๕.๗ ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๑๖๕.๘ ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

๑๖๕.๙ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวบุคคลที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของ ขร. โดยไม่มีการติดตั้งโปรแกรมป้องกันไวรัสอย่างเหมาะสม และต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ขร. อย่างเคร่งครัด ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของ ขร. ก่อนการใช้งาน

ข้อ ๑๖๖ การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทาง “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน” ที่ระบุไว้ในเอกสารส่วนที่ ๓

ข้อ ๑๖๗ การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๑๖๗.๑ ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๑๖๗.๒ ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๑๖๗.๓ ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ ๑๖๘ การสำรองข้อมูลและการกู้คืน

๑๖๘.๑ ผู้ใช้งาน ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น External Hard Disk เป็นต้น

๑๖๘.๒ ผู้ใช้งาน มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๖๘.๓ ผู้ใช้งาน ต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงานเพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของ ขร.

ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา และการใช้งานอุปกรณ์คอมพิวเตอร์พกพา และสื่อเก็บข้อมูลแบบถอดได้

ข้อ ๑๖๙ แนวทางปฏิบัติการใช้งานทั่วไป

๑๖๙.๑ เครื่องคอมพิวเตอร์แบบพกพาที่ ขร. อนุญาตให้ใช้งาน เป็นสินทรัพย์ของ ขร. เพื่อใช้ในงานราชการ

๑๖๙.๒ กำหนดให้มีการลงทะเบียนสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media Register) ก่อนนำไปใช้งาน รวมถึงกำหนดให้มีการบำรุงรักษา และการตรวจสอบการลงทะเบียนของสื่อเก็บข้อมูล แบบถอดได้เป็นประจำ อย่างน้อยทุก ๓ เดือน หรือ ๖ เดือนตามระดับความเสี่ยงที่นำไปใช้งานกับระบบหรือข้อมูล พร้อมทั้งจัดทำบันทึกการติดตามและตรวจสอบปรับปรุงทะเบียนทรัพย์สินสำหรับสื่อเก็บข้อมูลแบบถอดได้ที่ได้รับอนุญาต

๑๖๙.๓ ดำเนินการติดฉลากให้แก่สื่อเก็บข้อมูลแบบถอดได้ ยกเว้นสื่อเก็บข้อมูลแบบถอดที่ติดตั้งถาวรภายใน อุปกรณ์ ICT เพื่อให้ทราบถึงระดับความอ่อนไหว หรือชั้นความลับของข้อมูล รวมถึงช่วยให้มั่นใจว่ามีการใช้มาตรการที่เหมาะสมในการจัดเก็บ การจัดการ และการนำไปใช้งาน โดยอาจจะดำเนินการติดป้ายสี เพื่อระบุความสำคัญแทนการติดเป็นข้อความ รวมถึงจัดการฝึกอบรมการใช้งานให้แก่บุคลากรอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๑๖๙.๔ กำหนดให้มีการใช้สื่อเก็บข้อมูลแบบถอดได้เฉพาะกับระบบที่ได้รับอนุญาตให้ประมวลผล จัดเก็บหรือส่งข้อมูล โดยใช้สื่อเก็บข้อมูลแบบถอดเท่านั้น

๑๖๙.๕ กำหนดให้มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญ บนสื่อบันทึกข้อมูลแบบถอดได้ รวบถึงหากเป็นในระดับชั้นความลับ ลับมากที่สุด ลับมาก ต้องพิจารณาดำเนินการอย่างน้อยดังนี้ เข้ารหัส (Encryption) ระบุผู้รับผิดชอบ (ผู้ถือครอง) และบันทึก ในทะเบียนสื่อบันทึกข้อมูล รวมถึงกำหนดให้มีการทบทวนการกำหนดระดับชั้นความลับให้กับสื่อเก็บข้อมูลแบบถอดได้อย่างสม่ำเสมอ

๑๖๙.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่ ขร. ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๖๙.๓ ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๑๖๙.๔ ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๑๖๙.๕ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

๑๖๙.๖ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑๖๙.๗ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๑๖๙.๘ การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๑๖๙.๙ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑๖๙.๑๐ การย้ายอุปกรณ์คอมพิวเตอร์พกพาที่เป็นโน้ตบุ๊กขณะที่เปิดใช้งานอยู่ ให้ยกเครื่องจากฐานบริเวณใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๖๙.๑๑ กำหนดให้มีการทำลายสื่อบันทึกข้อมูล โดยพิจารณาดำเนินการดังนี้

(๑๖๙.๑๑.๑) ดำเนินการประเมินระดับชั้นความลับของข้อมูลก่อนทำลาย

(๑๖๙.๑๑.๒) กำหนดวิธีการทำลายข้อมูลให้สอดคล้องกับระดับชั้นความลับของข้อมูลในแต่ละลำดับชั้น พร้อมทั้งจัดให้มีหลักฐานการทำลายข้อมูล พร้อมทั้งกำหนดให้มีการลงนามโดยผู้มีอำนาจอนุมัติทำลายข้อมูล

(๑๖๙.๑๑.๓) ในกรณีที่มีการจัดจ้างผู้ให้บริการภายนอกทำลายสื่อบันทึก ควรพิจารณาจัดจ้างผู้ให้บริการที่ได้รับการรับรอง พร้อมทั้งกำหนดให้มีการกำหนดรูปแบบการทำลาย พร้อมวิธีการทำลายให้ฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายก่อนดำเนินการทำลาย

ข้อ ๑๗๐ ความปลอดภัยทางด้านกายภาพ

๑๗๐.๑ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๑๗๐.๒ ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อ ๑๗๑ การควบคุมการเข้าถึงระบบปฏิบัติการ

๑๗๑.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

๑๗๑.๒ ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๑๗๑.๓ ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

๑๗๑.๔ ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ ๑๗๒ การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

ข้อ ๑๗๓ การสำรองข้อมูลและการกู้คืน

๑๗๓.๑ ผู้ใช้งาน ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

๑๗๓.๒ ผู้ใช้งาน มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๗๓.๓ แผ่นสื่อข้อมูลสำรองที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๑๗๓.๔ ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของ ขร.

ส่วนที่ ๑๖ การป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี (Malicious Code Protection)

ข้อ ๑๗๔ ดูแลระบบต้องจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัสเวอร์ชั่นล่าสุด บนระบบปฏิบัติการทุกเครื่องใน ขร. ทั้งเครื่องแม่ข่ายและเครื่องลูกข่าย

ข้อ ๑๗๕ ผู้ดูแลระบบต้องจัดให้มีการปรับปรุงโปรแกรมป้องกันไวรัส รวมไปถึงฐานข้อมูลโปรแกรมป้องกันไวรัสให้เป็นรุ่นล่าสุดอยู่เสมอ

ข้อ ๑๗๖ ผู้ดูแลระบบต้องกำหนดให้โปรแกรมป้องกันไวรัสทำงานพร้อมกับการเริ่มทำงานของระบบประมวลผลหรือระบบปฏิบัติการทุกครั้ง

ข้อ ๑๗๗ ผู้ดูแลระบบต้องกำหนดให้โปรแกรมป้องกันไวรัส มีการสแกนสื่อบันทึกข้อมูลของเครื่องคอมพิวเตอร์ (Hard disk) อยู่เป็นประจำ เพื่อทำการค้นหาและจัดการกับชุดคำสั่งประสงค์ร้ายที่อยู่ในสื่อบันทึกข้อมูลนั้น ๆ

ข้อ ๑๗๘ ขร. ไม่อนุญาตให้มีการถอดถอน (Remove/Uninstall) หรือปิดบริการ (Disable services) ระบบป้องกันไวรัส หรือระบบป้องกันชุดคำสั่งประสงค์ร้าย โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๑๗๙ ผู้ดูแลระบบต้องกำหนดแนวทางในการเฝ้าระวังเครือข่ายและเครื่องคอมพิวเตอร์เพื่อติดตาม วิเคราะห์ และหาแนวทางป้องกันปัญหาที่อาจจะเกิดขึ้นจากการแพร่ระบาดของไวรัสภายใน ขร.

ข้อ ๑๘๐ ผู้ดูแลระบบจะต้องให้คำแนะนำในการใช้งานโปรแกรมป้องกันไวรัสแก่ผู้ใช้งาน และแจ้งให้ผู้ใช้งานหมั่นทำการ Update Signature ของโปรแกรมป้องกันไวรัส รวมทั้งทำการตรวจสอบไวรัสบน เครื่องคอมพิวเตอร์ภายใต้การดูแลเป็นประจำอย่างน้อยเดือนละ ๑ ครั้ง

ข้อ ๑๘๑ ผู้ใช้งานต้องทำการตรวจหาไวรัสของไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต รวมไปถึงไฟล์ที่มาจากสื่อบันทึกข้อมูลต่างๆ ได้แก่ Thumb Drive, CD หรือ Diskette ก่อนนำไปใช้งาน

ข้อ ๑๘๒ ผู้ใช้งานห้ามรับหรือทำการติดตั้งโปรแกรมที่ไม่ทราบแหล่งที่มาหรือมีแหล่งที่มาไม่น่าเชื่อถือ

ข้อ ๑๘๓ ห้ามผู้ใช้งานทำการพัฒนาชุดคำสั่งประสงค์ร้ายหรือนำชุดคำสั่งประสงค์ร้ายมาใช้ภายใน ขร. หรือเผยแพร่สู่ภายนอกด้วยเครือข่ายหรือทรัพยากรที่เป็นของ ขร.

ข้อ ๑๘๔ หากผู้ใช้งานที่ใช้งานเครื่องคอมพิวเตอร์พบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัสให้รีบแจ้งผู้ดูแลระบบเพื่อทำการตรวจสอบและแก้ไขในทันที

ข้อ ๑๘๕ ขร. ต้องมีการตรวจสอบเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารของ ขร. เพื่อให้มั่นใจว่าได้ปฏิบัติตามนโยบายการป้องกันชุดคำสั่งประสงค์ร้ายอย่างสม่ำเสมอ

ข้อ ๑๘๖ เมื่อมีผู้ใช้งานจากภายนอกนำเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารมาขออนุญาตใช้งานระบบเครือข่ายสารสนเทศภายใน ขร. ผู้ดูแลระบบจะต้องทำการตรวจสอบก่อนว่ามีระบบรักษาความปลอดภัยหรือมีการติดตั้งใช้งานโปรแกรมป้องกันไวรัสบนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารหรือไม่ หากพบว่าไม่มีระบบรักษาความปลอดภัยหรือติดตั้งใช้งานโปรแกรมป้องกันไวรัส ผู้ดูแลระบบไม่ควรอนุญาตให้ทำการใช้งานระบบเครือข่ายสารสนเทศภายใน ขร. เป็นอันขาด

ข้อ ๑๘๗ ผู้บริหารควรมีความตระหนักในภัยโจมตีทางไซเบอร์ในรูปแบบใหม่ๆ พร้อมแนะนำและกำหนดแนวทางในการวางแผนเพื่อบริหารจัดการสำหรับการป้องกัน และแก้ไขสำหรับวิกฤติภัยโจมตีประเภทต่างๆ ทั้งปัจจุบัน และอนาคต

ส่วนที่ ๑๗ การบริหารจัดการข่าวกรองภัยคุกคาม และช่องโหว่ทางเทคนิค (Threat Intelligence and Technical Vulnerability Management)

ข้อ ๑๘๘ ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. อ้างอิงตามหลักการบริหารความเสี่ยงของ ขร. เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญของหรือระบบงานที่สำคัญของ ขร. อย่างน้อยปีละ ๑ ครั้ง โดยต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย

๑๘๘.๑ การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

๑๘๘.๒ การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

๑๘๘.๓ การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

ข้อ ๑๘๙ ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และควบคุมก่อนที่จะทำการทดสอบระบบใดๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบสำคัญใดๆ กับบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

ข้อ ๑๙๐ ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

ข้อ ๑๙๑ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ต (Internet Facing)

ข้อ ๑๙๒ ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยสารสนเทศของบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. ก่อนทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

ข้อ ๑๙๓ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลหรือตามที่กฎหมายที่เกี่ยวข้องกำหนด ดังนี้

- ระดับบริหารจัดการ (Security Management level) เช่น
  (๑) Certified Information Systems Security Professional (CISSP)
  (๒) Certified Information Security Manager (CISM)
  (๓) Certified Information Systems Auditor (CISA)
- ระดับปฏิบัติการ (Penetration Tester Level) เช่น
  (๑) ประกาศนียบัตรการรับรองจากสถาบัน CompTIA เช่น CompTIA Pentest+ เป็นต้น
  (๒) ประกาศนียบัตรการรับรองจากสถาบัน EC-Council เช่น EC-Council’s Certified Penetration Testing Professional (C|PENT), Certified Ethical Hacker (CEH), Licensed Penetration Tester (LPT) เป็นต้น
  (๓) ประกาศนียบัตรการรับรองจากสถาบัน ISACA เช่น CSX Cybersecurity Practitioner (CSX-P) เป็นต้น
  (๔) ประกาศนียบัตรการรับรองจากสถาบัน Mile๒ เช่น CERTIFIED Penetration Testing Engineer (C)PTE) เป็นต้น
  (๕) ประกาศนียบัตรการรับรองจากสถาบัน Council for Registered Ethical Security Testers (CREST) เช่น CREST Registered Penetration Tester, CREST Certified Web Application Tester, CREST Certified Infrastructure Tester เป็นต้น

(๖) ประกาศนียบัตรการรับรอง จากสถาบัน Offensive Security เช่น OSCP, OSWP, OSCE, OSEE และ OSWE เป็นต้น

(๗) ประกาศนียบัตรการรับรองจากสถาบัน Global Information Assurance Certification (GIAC) เช่น GCIH, GMOB, GPEN, GXPN, GAWN และ GWAPT

ข้อ ๑๙๔ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของ ขร.

ข้อ ๑๙๕ ต้องสร้างกระบวนการเพื่อติดตามและจัดการช่องโหว่ที่ระบุในผลประเมินช่องโหว่ และในผลการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

ข้อ ๑๙๖ หากได้รับการร้องขอจาก กกม. หรือ สกมช. ทาง ขร. ต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ ขร. ไปยัง สกมช. ภายใน ๓๐ วัน นับแต่วันที่ได้รับหนังสือ ทั้งนี้ รูปแบบรายงานสรุปผลการ ทดสอบเจาะระบบให้เป็นไปตามหลักเกณฑ์และวิธีการที่ สกมช. ประกาศกำหนด

ข้อ ๑๙๗ หากการตรวจสอบช่องโหว่และการทดสอบเจาะระบบนั้นดำเนินการโดยผู้ให้บริการภายนอกให้ ขร. ดำเนินการควบคุม ดังนี้

๑๙๗.๑ จัดทำสัญญารักษาความลับ (Non-Disclosure Agreement: NDA) และกำหนดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมในสัญญาว่าจ้างหรือเอกสารแนบท้ายสัญญาว่าจ้างอันเป็นส่วนหนึ่งของสัญญาดังกล่าว

๑๙๗.๒ ต้องได้รับความเห็นชอบจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรมก่อนดำเนินการเสมอ และมีการวางแผนก่อนดำเนินการ ซึ่งครอบคลุมถึงการดำเนินการนอกเวลางาน

๑๙๗.๓ หากมีการสำเนาข้อมูล ต้องทำลายสำเนาข้อมูลทั้งหมดทันทีที่การดำเนินงานเสร็จสิ้นลง แต่ไม่รวมไปถึงรายงานการดำเนินการ

๑๙๗.๔ ในกรณีเจ้าหน้าที่ของ ขร. ทำการตรวจสอบระบบเอง โดยใช้ซอฟต์แวร์หรือเครื่องมือเข้าช่วย ต้องทำการเก็บรักษาซอฟต์แวร์หรือเครื่องมือนั้นไว้ในที่มั่นคงปลอดภัย เช่น เก็บไว้ในเครื่องคอมพิวเตอร์ที่มีรหัสผ่านปกป้อง เป็นต้น เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิสามารถนำเอาซอฟต์แวร์หรือเครื่องมือดังกล่าวไปใช้งานโดยไม่ได้รับอนุญาต

๑๙๗.๕ เมื่อดำเนินการเสร็จสิ้น หากมีบัญชีผู้ใช้งานและรหัสผ่านที่กำหนดให้ผู้เชี่ยวชาญจากภายนอกใช้ในการดำเนินการ ต้องถูกลบหรือยกเลิก

๑๙๗.๖ จัดเก็บรายงานผลการดำเนินการไว้เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถตรวจสอบย้อนหลังได้อย่างน้อย ๕ ปี

ข้อ ๑๙๘ ต้องจัดให้มีการติดตามข้อมูลข่าวสารจากแหล่งข้อมูลต่างๆ ที่เชื่อถือได้ เช่น เว็บไซต์ของเจ้าของผลิตภัณฑ์หรือผู้ให้บริการ เป็นต้น เกี่ยวกับโปรแกรมแก้ไขข้อบกพร่องของซอฟต์แวร์และระบบปฏิบัติการ (Patch) ตลอดจนอุปกรณ์อื่นๆ ที่เกี่ยวข้อง และดำเนินการติดตั้งโปรแกรมดังกล่าวตามขั้นตอนปฏิบัติงานที่ ขร. กำหนดซึ่งรวมไปถึงกระบวนการบริหารการเปลี่ยนแปลง (Change Management)

ข้อ ๑๙๙ ให้ความช่วยเหลือ สนับสนุน หรือประสานงานในการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน

ข้อ ๒๐๐ จัดให้มีการรวบรวมและวิเคราะห์ข้อมูลข่าวกรองภัยคุกคามด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ขร.

ส่วนที่ ๑๘ การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

ข้อ ๒๐๑ IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศและข้อมูลบนเครือข่ายภายในหน่วยงาน ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาท และความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๒๐๒ IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของหน่วยงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

ข้อ ๒๐๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะ จะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

ข้อ ๒๐๔ ระบบทั้งหมดใน DMZ (Demilitarized Zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

ข้อ ๒๐๕ โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

ข้อ ๒๐๖ ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำและทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

ข้อ ๒๐๗ ต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรมและบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

ข้อ ๒๐๘ เครื่องแม่ข่ายที่มีการติดตั้ง Host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

ข้อ ๒๐๙ จะต้องรายงานพฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ให้ผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ทราบทันทีที่ตรวจพบ

ข้อ ๒๑๐ การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๒๑๑ ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

ข้อ ๒๑๒ หน่วยงานมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

ข้อ ๒๑๓ ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของ ขร. การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของหน่วยงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ส่วนที่ ๑๙ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

ข้อ ๒๑๔ การปรับปรุงระบบปฏิบัติการ (Operating System Update)

๒๑๔.๑ ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

๒๑๔.๒ ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

๒๑๔.๓ กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบและชื่อผู้ใช้งาน (User)

๒๑๔.๔ กำหนดค่าติดตั้ง ชื่อเครื่อง (Computer Name) / IP Address

๒๑๔.๕ ปรับปรุง/กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)

ข้อ ๒๑๕ การบริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management)

๒๑๕.๑ กำหนดชื่อและรหัสผ่าน ผู้ดูแลระบบ (System Administrator)

๒๑๕.๒ กำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

๒๑๕.๓ บันทึกบัญชีผู้ใช้งานและสิทธิ์การเข้าใช้ระบบ

ข้อ ๒๑๖ การปรับปรุงการรักษาความปลอดภัย/Antivirus (System Security & Antivirus Update)

๒๑๖.๑ ติดตาม เฝ้าระวัง ระบบการทำงานของคอมพิวเตอร์ การเข้าใช้ระบบ

๒๑๖.๒ Performance ของระบบ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

๒๑๖.๓ ปรับปรุง/กำหนดค่าระบบความปลอดภัยให้เหมาะสมกับปัญหา

๒๑๖.๔ ปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

๒๑๖.๕ ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์เป็นประจำ

ข้อ ๒๑๗ ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation)

๒๑๗.๑ ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบสารสนเทศ

๒๑๗.๒ กำหนดค่าระบบหรือโปรแกรมฐานข้อมูล ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพ ตามข้อกำหนดของระบบฐานข้อมูล

๒๑๗.๓ สร้างและกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้งานอื่นและสิทธิ์การใช้

๒๑๗.๔ ปรับปรุง/กำหนดค่าระบบให้เหมาะสม ทันสมัยหรือป้องกันการเกิดปัญหาเป็นประจำ

ข้อ ๒๑๘ ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่างๆ/กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการ หรือเข้าถึงฐานข้อมูล

๒๑๘.๑ ติดตั้งโปรแกรมระบบงานตามความต้องการ หรือการพัฒนา

๒๑๘.๒ กำหนดค่า หรือโปรแกรม หรือบริการ ให้ทำงานร่วมกับระบบปฏิบัติการ เป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

๒๑๘.๓ ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามระบบงาน

๒๑๘.๔ แจ้งผู้ใช้งาน หรือเจ้าของระบบงาน โดยแจ้งรายชื่อ รหัสผ่านและสิทธิ์การเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้

๒๑๘.๕ กำหนดเกณฑ์การสำรอง/สำเนา/ทดสอบกู้คืน (Restore Test)

๒๑๘.๖ บันทึกข้อกำหนด ค่าติดตั้งและบัญชีชื่อผู้ใช้งาน แต่ละระบบทุกครั้งที่มีการสร้าง/ปรับปรุง

ข้อ ๒๑๙ การสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงานหรือแอปพลิเคชัน และอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายทั้งหมดของบริการที่สำคัญของ ขร. ให้สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. โดยต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังนี้

๒๑๙.๑ สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒๑๙.๒ การแบ่งแยกหน้าที่ (Separation of Duties)

๒๑๙.๓ การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๒๑๙.๔ การลบบัญชีที่ไม่ได้ใช้

๒๑๙.๕ การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพลเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๒๑๙.๖ การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๒๑๙.๗ การป้องกันมัลแวร์ (Malware)

๒๑๙.๘ การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

๒๑๙.๙ การแสดงข้อความแจ้งเตือนต้องไม่เกินความจำเป็น หรือบ่งชี้อย่างเจาะจงว่าข้อมูลส่วนใดส่วนหนึ่งผิดพลาด เช่น ใช้ถ้อยคำว่า "ชื่อผู้ใช้งานหรือรหัสผ่านไม่ถูกต้อง" แทนการแจ้งเตือนว่า "รหัสผ่านไม่ถูกต้อง" เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีคาดเดาได้รวมทั้งต้องไม่แสดงข้อมูลภายในของระบบ เช่น เวอร์ชัน และ ยี่ห้อ ของระบบงาน IP Address และ Path เป็นต้น

ข้อ ๒๒๐ ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. รวมทั้งต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการ

ที่สำคัญ หรือระบบงานที่สำคัญของ ขร. อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

ข้อ ๒๒๑ ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร. โดยต้องดำเนินการอย่างน้อย ดังนี้

(๑) กำหนดให้ต้องมีการบริหารจัดการการเปลี่ยนแปลง โดยร้องขอการเปลี่ยนแปลง โดยใช้แบบฟอร์มการร้องขอการเปลี่ยนแปลง (Change Request) เพื่อประเมินผลกระทบการเปลี่ยนแปลงก่อนดำเนินการเปลี่ยนแปลง โดยระบุข้อมูลอย่างน้อย ดังนี้ วัตถุประสงค์, ขอบเขต, รายละเอียดการเปลี่ยนแปลง, ความเสี่ยง, แผนการดำเนินงาน, ผู้รับผิดชอบ, แผนทดแทน และแผนย้อนกลับ (Rollback Plan)

(๒) กำหนดให้มีการประเมินผลกระทบและความเสี่ยง โดยวิเคราะห์ผลกระทบต่อระบบสารสนเทศ ความต่อเนื่องในการให้บริการ และความมั่นคงปลอดภัยของข้อมูล

(๓) กำหนดให้มีการอนุมัติการเปลี่ยนแปลง โดยพิจารณาให้มีการประชุม เพื่อพิจารณาอนุมัติหรือปฏิเสธการเปลี่ยนแปลงที่สำคัญ

(๔) กำหนดให้ต้องมีการจัดแผน Rollback ที่สามารถดำเนินการได้ทันทีหากเกิดปัญหาในการเปลี่ยนแปลง

(๕) กำหนดให้มีการติดตามผลและการปิดการเปลี่ยนแปลง พร้อมทั้งจัดทำรายงาน Post-Implementation Review (PIR) หรือ Lessons Learned และบันทึกข้อมูลการเปลี่ยนแปลงอย่างเป็นระบบ

ส่วนที่ ๒๐ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และการเฝ้าระวัง (Logging and Monitoring)

ข้อ ๒๒๒ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

ข้อ ๒๒๓ ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ ๒๒๔ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๒๒๕ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ ๒๒๖ กำหนดให้มีการตรวจสอบและการใช้ประโยชน์จากข้อมูลจราจรคอมพิวเตอร์ โดยจัดให้มีการตรวจสอบข้อมูลจราจรอย่างสม่ำเสมอ เพื่อค้นหาความผิดปกติ เช่น รายสัปดาห์ รายเดือน หรือรายไตรมาส เป็นต้น และกำหนดกระบวนการให้ข้อมูลจราจรแก่หน่วยงานภายนอกตามกฎหมาย พร้อมการอนุมัติจากผู้มีอำนาจ

ข้อ ๒๒๗ เวลาของระบบ เครื่องแม่ข่ายและเครื่องคอมพิวเตอร์ ตลอดจนอุปกรณ์ด้านความมั่นคงปลอดภัยต่าง ๆ เช่น Access Control Device, CCTV เป็นต้น ต้องถูกต้องตรงกัน โดยต้องมีการเทียบเวลา (Clock Synchronization) กับเวลามาตรฐานของแหล่งที่เชื่อถือได้ โดยให้ตรงกับเวลาอ้างอิงสากล

หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูล ข้อมูลและสำรองข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๒. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑ กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

๑.๑ จัดทำบัญชีฐานข้อมูล การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

๑.๒.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

๑.๒.๒ กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือ ผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

๑.๓.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการให้บริการ เช่น ข้อมูลการรับสมัครงาน ข้อมูลผู้ประกอบการขนส่งทางราง เป็นต้น

๑.๓.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๑.๓.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๑.๓.๔ จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๑.๓.๕ การกำหนดเวลาที่ได้เข้าถึง

๑.๓.๖ การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ ๒ ข้อมูลข่าวสารสารสนเทศทุกประเภทในฐานข้อมูล ต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่นๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓ การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวดที่ ๑ ข้อ ๑๕

ข้อ ๔ หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใดๆ กับข้อมูลนั้นได้ตามสิทธิ์และจัดให้มีแฟ้มลงบันทึกเข้าออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจากส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่าง ขร. กับหน่วยงานภายนอก ดังต่อไปนี้

๕.๑ กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

๕.๒ กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกันหรือแลกเปลี่ยนข้อมูล เช่น วิธีการรับ-ส่ง เป็นต้น

๕.๓ กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

๕.๔ กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูล เพื่อเป็นการป้องกันการปฏิเสธ

๕.๕ กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่นๆ กับข้อมูลนั้น

๕.๖ กำหนดสิทธิ์การเข้าถึงข้อมูล

๕.๗ กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๕.๘ กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่นๆ ที่มีความสำคัญ เช่น กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๖ ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย

ข้อ ๗ ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

ข้อ ๘ ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ ต้องกำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

๙.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๙.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล

๙.๓ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๙.๔ ตรวจสอบค่าคอนฟิกกูเรชันต่างๆ ของระบบการสำรองข้อมูล

๙.๕ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๙.๖ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

๙.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๙.๘ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๙.๙ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๙.๑๐ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น

๙.๑๑ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ ๑๐ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยมีข้อปฏิบัติอย่างน้อย ดังนี้

๑๐.๑ มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๑๐.๒ มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๑๐.๓ มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๑๐.๔ มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๑๐.๕ มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๑๐.๖ การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

ข้อ ๑๑ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อ ๑๓ มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๔ ต้องกำหนดข้อตกลงระดับการให้บริการ (Service Level Agreement-SLA) สำหรับการกู้คืนข้อมูลของแต่ละระบบสารสนเทศของ ขร. ซึ่งระยะเวลาในการกู้คืนควรสอดคล้องกับความสำคัญ และความสามารถของระบบสารสนเทศที่มีอยู่

ข้อ ๑๕ ต้องกำหนดอำนาจอนุมัติในการกู้คืนข้อมูลอย่างเป็นลายลักษณ์อักษรและในการกู้คืนข้อมูลทุกครั้ง ต้องได้รับการอนุมัติจากผู้มีอำนาจที่ได้มีการกำหนดไว้เท่านั้น

ข้อ ๑๖ จัดให้มีการทดสอบการกู้คืนข้อมูลอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๗ จัดทำรายละเอียดการทดสอบกู้คืนข้อมูล สำหรับแต่ละระบบสารสนเทศของ ขร. โดยให้ครอบคลุมเนื้อหา ดังนี้

- ความถี่ในการทดสอบ
- รูปแบบการทดสอบ
- ระยะเวลาในการทดสอบและการตรวจทานผลการทดสอบ

- รายชื่อ รายละเอียดบทบาทและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ปฏิบัติงานที่เกี่ยวข้อง
- รายละเอียดเอกสารที่เกี่ยวข้องกับการทดสอบ
- การประเมินผลการทดสอบ เพื่อรายงานผู้บริหารของ ขร. รับทราบ

ข้อ ๑๘ ผู้ดูแลระบบที่รับผิดชอบต้องทำการตรวจสอบความพร้อมในการใช้งานของสื่อบันทึกข้อมูลอย่างสม่ำเสมอ ตามที่กำหนดในรายละเอียดการทดสอบกู้คืนข้อมูล เพื่อให้แน่ใจได้ว่าสื่อบันทึกข้อมูลอยู่ในสถานะพร้อมใช้งาน

ส่วนที่ ๓ การบริหารจัดการสื่อบันทึกข้อมูลสำรอง (Removeable Media)

ข้อ ๑๙ สื่อบันทึกที่ใช้ในการบันทึกข้อมูลสำรองที่เป็นข้อมูลความลับ ต้องได้รับการปกป้องอย่างเหมาะสมกับระดับความสำคัญของข้อมูล ทั้งนี้ หากมิได้มีการกำหนดไว้เป็นอื่น ให้ถือว่าสื่อบันทึกข้อมูลสำรองมีระดับความสำคัญของข้อมูลเป็นข้อมูลลับ (Confidential)

ข้อ ๒๐ จัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆ ที่เกี่ยวข้องไว้ภายนอก สถานที่ปฏิบัติงานของ ขร. เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าว ต้องมีระบบควบคุมสภาพแวดล้อมที่เหมาะสม และมีความมั่นคงปลอดภัยทางกายภาพที่ดี เช่น มีระบบควบคุม อุณหภูมิและความชื้น มีระบบควบคุมการเข้าออก ระบบตรวจจับผู้บุกรุก และระบบป้องกันอัคคีภัย เป็นต้น

ข้อ ๒๑ สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ตลอดจนสื่อบันทึกแบบอื่นๆ (เช่น External HDD, CD-ROM, Floppy Disk) ที่มาจากแหล่งภายนอก หรือที่เคยถูกนำไปใช้งานภายนอก ขร. ต้องได้รับการตรวจหามัลแวร์ก่อนที่จะถูกนำมาใช้งานภายใน ขร. หากไฟล์ในสื่อบันทึกถูกเข้ารหัส ผู้ใช้งานต้องทำการถอดรหัส ข้อมูลก่อนการตรวจหามัลแวร์ทุกครั้ง รวมถึงมีมาตรการรักษาความปลอดภัยของสื่อบันทึกข้อมูลระหว่างการขนส่ง (physical media transfer)

ข้อ ๒๒ สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ที่จัดเก็บข้อมูลของ ขร. ต้องใช้ในการจัดเก็บข้อมูลของ ขร. เท่านั้น และใช้เฉพาะการปฏิบัติงานให้กับ ขร. ห้ามใช้สื่อบันทึกข้อมูลดังกล่าวกับผู้ที่ไม่มีสิทธิเข้าถึงข้อมูลที่จัดเก็บนั้น

ข้อ ๒๓ การขอใช้งานสื่อบันทึกข้อมูลสำรองที่มีข้อมูลสำรองอยู่ภายใน เช่น ขอใช้งานเพื่อทำการกู้ข้อมูล เป็นต้น ต้องได้รับการอนุมัติจากผู้มีอำนาจ

ข้อ ๒๔ ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนของบริการที่สำคัญของ ขร. ที่ถูกจัดเก็บบนสื่อบันทึกข้อมูลแบบถอดได้

ข้อ ๒๕ จัดให้มีการทำลายข้อมูลสำคัญและสื่อบันทึกที่ไม่ได้ใช้งานแล้วอย่างเหมาะสม เพื่อให้แน่ใจว่าข้อมูลสำคัญจะไม่สามารถถูกกู้กลับคืนมาได้โดยไม่ได้รับอนุญาต

ส่วนที่ ๔ การเข้ารหัสข้อมูล (Cryptography)

ข้อ ๒๖ กำหนดมาตรฐานวิธีการเข้ารหัสข้อมูล (Cryptographic Algorithm) ให้เป็นไปตามมาตรฐานสากล และกำหนดความรับผิดชอบของหน่วยงานหรือบุคลากรที่เกี่ยวข้อง เพื่อให้การเข้ารหัสข้อมูลมีความมั่นคงปลอดภัยเหมาะสมกับระดับความสำคัญของข้อมูล และทบทวนเพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานอยู่ยังมีความมั่นคงเพียงพอในการรักษาความปลอดภัยของข้อมูล อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒๗ การเข้ารหัสข้อมูล มีแนวทางดำเนินการ ดังนี้

๒๗.๑ ใช้งานโปรโตคอลมีความมั่นคงความปลอดภัยสำหรับการสื่อสารผ่านเครือข่ายอินเทอร์เน็ต โดยใช้โปรโตคอลความปลอดภัยสำหรับการส่งข้อมูล (Transport Layer Security: TLS) เป็นอย่างน้อย

๒๗.๒ ใช้มาตรฐานที่เป็นที่ยอมรับในการเข้ารหัส เช่น Triple DES, AES, PGP, RSA, ECC เป็นต้น

๒๗.๓ การเข้ารหัสแบบสมมาตร (Symmetric algorithm) ควรใช้ความยาวกุญแจ (Key) ที่เหมาะสมและปลอดภัย เพื่อป้องกันการถูกถอดรหัสโดยผู้ไม่ประสงค์ดี โดยใช้ AES-๑๐๒๔ bits เป็นอย่างน้อย

๒๗.๔ การเข้ารหัสแบบอสมมาตร (Asymmetric algorithm) ควรใช้ความยาวกุญแจที่เหมาะสมและปลอดภัย เช่น PGP-๑๐๒๔-bit, RSA-๑๐๒๔ bits, ECC-๑๙๒-bit เป็นอย่างน้อย

๒๗.๕ การแทนค่าข้อมูลด้วยฟังก์ชันแฮชเข้ารหัส (Cryptographic hash function) ควรใช้มาตรฐาน SHA-๒ หรือมาตรฐานอื่นที่เทียบเท่าหรือดีกว่า และ ใช้ความยาวกุญแจอย่างน้อย ๒๕๖ bits เป็นอย่างน้อย

๒๗.๖ กรณีที่ไม่มีเครื่องมือในการเข้ารหัสอื่นๆ ผู้ใช้งานต้องใช้โปรแกรมบีบอัดไฟล์ เช่น Zip ๗ip เป็นต้น พร้อมเข้ารหัส โดยรหัสผ่านต้องเป็นไปตามมาตรฐานที่บริษัทฯ กำหนด และต้องได้รับการอนุมัติจากเจ้าของข้อมูล ก่อนส่งข้อมูลให้บุคคลภายนอก หรือส่งข้อมูลสำคัญ ข้อมูลความลับ หรือข้อมูลส่วนบุคคลผ่านระบบ อีเมล หรือช่องทางอื่นๆ รวมถึงการเคลื่อนย้ายสื่อบันทึกข้อมูล

๒๗.๗ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. เข้ารหัสช่องทางการรับ-ส่งข้อมูลบนระบบหรือเว็บไซต์ที่ให้บริการกับบุคคลภายนอก ซึ่งกุญแจเข้ารหัสต้องมีอายุไม่เกิน ๑ ปี โดยจะมีการต่ออายุแบบปีต่อปี และความยาวของรหัสต้องเป็นมาตรฐานและเป็นที่ยอมรับ

ข้อ ๒๘ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. กำหนดกุญแจที่ใช้ในการเข้ารหัสกุญแจให้แตกต่างจากกุญแจที่ใช้ในการเข้ารหัสข้อมูล

ข้อ ๒๙ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. ควบคุมสภาพแวดล้อมและกระบวนการในการสร้างกุญแจเข้ารหัสให้รัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (Certification authority) ที่น่าเชื่อถือ ทำลายข้อมูลที่ใช้ในกระบวนการเข้ารหัสเพื่อควบคุมความเสี่ยงจากการเข้าถึงหรือกู้คืนกุญแจ เข้ารหัสข้อมูลโดยไม่ได้รับอนุญาต เป็นต้น

ข้อ ๓๐ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. จัดเก็บกุญแจที่ใช้ในการเข้ารหัสข้อมูลให้มีความปลอดภัยทั้งด้านกายภาพ (Physical) และระบบ (Logical) เช่น การใช้อุปกรณ์การบริหารจัดการกุญแจดิจิทัล (Hardware Security Module: HSM) หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน เป็นต้น

ข้อ ๓๑ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. ควบคุมการเข้าถึงกุญแจที่ใช้ในการเข้ารหัสข้อมูลให้สามารถเข้าถึงได้เฉพาะบุคคลที่จำเป็นเท่านั้น และต้องมีการแบ่งแยกหน้าที่ความรับผิดชอบของบุคคลที่มีสิทธิในการเข้าถึงกุญแจที่ใช้ในการเข้ารหัส โดยการควบคุมนี้จะใช้กับบุดคลใดก็ตามที่มีหน้าที่เกี่ยวข้องกับการใช้งานกุญแจที่ใช้ในการเข้ารหัส หรือบุคคลที่มีสิทธิในการเข้าถึงพื้นที่ที่ใช้ในการประมวลผลที่เกี่ยวข้องกับการเข้ารหัสข้อมูล

ข้อ ๓๒ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. ควบคุมการแลกเปลี่ยนกุญแจให้ดำเนินการผ่านกระบวนการและช่องทางที่ปลอดภัย

ข้อ ๓๓ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. สำรองข้อมูลของกุญแจที่ใช้ในการเข้ารหัสข้อมูลไฟล์และการสำรองข้อมูลการตั้งค่าของระบบ เพื่อป้องกันการสูญหายของข้อมูลกุญแจที่ใช้ในการเข้ารหัสและ/หรือการถอดรหัส โดยวิธีการเก็บรักษาข้อมูลกุญแจเข้ารหัสชุดสำรองต้องมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสชุดหลัก

ข้อ ๓๔ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. เพิกถอนกุญแจที่ใช้เข้ารหัสทันที เมื่อทราบว่ากุญแจมีความเสี่ยงที่จะก่อให้เกิดการละเมิดทางด้านความมั่นคงปลอดภัย เช่น เมื่อกุญแจส่วนตัว (Private Key) รั่วไหลไปยังบุคคลอื่น หรือกรณีกุญแจเข้ารหัสหมดอายุการใช้งาน ทั้งนี้ กุญแจที่ใช้เข้ารหัสจะต้องมีอายุไม่เกิน ๑ ปี โดยให้ต่ออายุปีต่อปี

ข้อ ๓๕ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. เพิกถอนกุญแจด้วยกระบวนการทำลายกุญแจ เพื่อให้มั่นใจว่าจะไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก อาจเพิกถอนโดยการใช้ช่องทางอัตโนมัติ ผ่านรายการเพิกถอนใบรับรอง (Certificate Revocation List: CRL) ออนไลน์

ข้อ ๓๖ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. แจ้งให้ผู้เกี่ยวข้องกับกุญแจหรือผู้ที่ใช้งานกุญแจทราบถึงการเพิกถอนกุญแจที่ใช้เข้ารหัส พร้อมเหตุผลของการเพิกถอน วันที่และเวลาที่ถูกเพิกถอน

ข้อ ๓๗ ฝ่ายเทคโนโลยีสารสนเทศของขร. จัดเก็บข้อมูลบันทึกเหตุการณ์กิจกรรมสำคัญที่เกี่ยวกับกุญแจเข้ารหัส เช่น การสร้างกุญแจ การสำรองกุญแจ การเข้าถึงหรือใช้งานกุญแจ และการเพิกถอนกุญแจ เป็นต้น

ข้อ ๓๘ กรณีไม่สามารถสร้างกุญแจเข้ารหัสด้วยตนเอง หรือมีความจำเป็นต้องใช้กุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ฝ่ายเทคโนโลยีสารสนเทศของ ขร. ต้องทำให้มั่นใจว่ากุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอกไม่มีการนำมาใช้งานร่วมกับผู้ใช้บริการรายอื่นและมีความมั่นคง ปลอดภัย โดยพิจารณาเงื่อนไขหรือรายละเอียดของการให้บริการ ดังนี้

๓๘.๑ ประเภทของกุญแจเข้ารหัส

๓๘.๒ รายละเอียดของระบบ และกระบวนการบริหารจัดการกุญแจเข้ารหัส

๓๘.๓ ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล

ข้อ ๓๙ ฝ่ายเทคโนโลยีสารสนเทศของขร. กำหนดแผนรับมือเมื่อเกิดการรั่วไหลของกุญแจเข้ารหัส เช่น การติดต่อหน่วยงานและผู้ที่เกี่ยวข้องกับชุดข้อมูลที่ใช้กุญแจเข้ารหัสชุดดังกล่าว การตรวจสอบชุดข้อมูล ที่มีความเสี่ยงในการรั่วไหล การเปลี่ยนหรือเพิกถอนกุญแจการเข้ารหัสข้อมูล เป็นต้น

ข้อ ๔๐ ฝ่ายเทคโนโลยีสารสนเทศของ ขร. ทบทวนรายการกุญแจที่มีการใช้งานอย่างน้อยทุก ๖ เดือน

ส่วนที่ ๕ การป้องกันข้อมูลรั่วไหล (Data Leakage Prevention)

ข้อ ๔๑ กำหนดสิทธิการเข้าถึงข้อมูลตามหน้าที่และความรับผิดชอบ

ข้อ ๔๒ ต้องเฝ้าระวังช่องทางที่อาจจะทำให้เกิดเหตุการณ์ข้อมูลรั่วไหล เช่น การรับส่งข้อมูลทางอิเล็กทรอนิกส์รวมถึงเหตุการณ์การรักษาความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๔๓ เมื่อพบเหตุการณ์ข้อมูลรั่วไหลต้องแจ้งต่อหน่วยงานที่เกี่ยวข้อง และดำเนินการตามแผนภัยคุกคามทางไซเบอร์

ข้อ ๔๔ สร้างความตระหนักรู้ให้แก่พนักงาน ผู้ให้บริการภายนอกในการป้องกันข้อมูลรั่วไหล และปกป้องข้อมูลให้เหมาะสมกับระดับชั้นความลับ

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

ข้อ ๑ กำหนดให้มีการดำเนินการจัดทำขั้นตอนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ หรือประยุกต์ใช้ขั้นตอนการตรวจสอบเดิมของ ขร. และเพิ่มเติมขั้นตอนที่เกี่ยวข้องสอดคล้องกับข้อกำหนดกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์

ข้อ ๒ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคง ปลอดภัยสารสนเทศ โดยมีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

๒.๑ จัดลำดับความสำคัญของความเสี่ยง

๒.๒ ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง

๒.๓ ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง

๒.๔ สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้

๒.๕ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๒.๖ มีมาตรการในการตรวจสอบ หรือตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

๖.๑ จัดทำแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมระบบงานที่สำคัญ หรือบริการที่สำคัญที่ ขร. กำหนดขึ้น โดยมีขอบเขตของการตรวจสอบ ดังนี้

(๑) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(๒) บริการที่สำคัญที่ ขร. เป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (๑)

(๓) การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และแนวนโยบายและแนวปฏิบัติฉบับนี้

ข้อ ๖.๒ ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยผู้บริหารสูงสุด หรือผู้ที่ได้รับมอบอำนาจของ ขร. ก่อนดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ รวมถึงผู้ตรวจสอบต้องมีคุณสมบัติเบื้องต้น ดังนี้ มีความเป็นอิสระ และมีความสามารถของผู้ตรวจสอบ

ข้อ ๖.๓ กำหนดให้ทีมตรวจสอบและผู้ตรวจสอบที่ได้รับการแต่งตั้ง ควรมีคุณลักษณะ ดังนี้

ก. ไม่อยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of Interest) โดยผลประโยชน์ทับซ้อนหมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของผู้ตรวจสอบอาจก่อให้เกิดการแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบจนทำให้การดำเนินการตรวจสอบไม่เป็นอิสระหรือไม่มีตรงกับหลักฐานที่ปรากฏ

ข. มีความสามารถทางเทคนิคที่จำเป็นต่อการดำเนินการตรวจสอบ เช่น มีคุณวุฒิวิชาชีพใบรับรอง ทักษะ ความรู้และประสบการณ์ที่เกี่ยวข้อง

ข้อ ๖.๔ กำหนดให้มีการดำเนินการจัดทำรายงานการตรวจสอบ ประกอบไปด้วยหัวข้อ อย่างน้อย ดังนี้

- บทสรุปผู้บริหาร (Executive Summary)
- วัตถุประสงค์ (Purpose)
- เกณฑ์ในการตรวจสอบ (Audit Criteria)
- ขอบเขตการตรวจสอบ (Audit Scope)
- วันเวลาที่ตรวจสอบ
- ผู้ตรวจสอบ
- ผู้มีส่วนได้ส่วนเสีย (Stakeholders)
- วิธีการและแนวทาง การตรวจสอบ (Audit Methodology and Approach)
- สิ่งที่พบจากการตรวจสอบ (Audit Finding)
- สรุปการตรวจสอบ (Audit Conclusion)

๖.๕ ทบทวนแผนตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบถึงบริการที่สำคัญของ ขร.

๖.๖ ในกรณีที่การตรวจสอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. ในบริการที่สำคัญ พบสิ่งที่ไม่เป็นไปตามกฎหมาย และประกาศที่เกี่ยวข้อง ต้องจัดให้มีการดำเนินการปรับปรุงแก้ไข และดำเนินการตรวจสอบการแก้ไขอีกครั้ง

๖.๗ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๖.๘ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๖.๙ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๖.๑๐ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึก Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

๖.๑๑ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนาและมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่างๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่างๆ ได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงักหรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพได้ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

๑. จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจ การใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้อย่างมีประสิทธิภาพยิ่งขึ้น ทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

๒. จัดทำ Infographic หรือหนังสือแจ้งเวียน เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Virus) หนอนอินเทอร์เน็ต (Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

๑. ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก

๒. ติดตั้งซอฟต์แวร์ Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ และติดตั้งอุปกรณ์ในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) ดังนี้

๑. ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

๒. ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนเพื่อทราบ และรีบเข้าระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

๓. ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

<u>ประเภทที่ ๔</u> ภัยจากน้ำหรือน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำหรือน้ำท่วม จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๑. ติดตั้งอุปกรณ์ตรวจจับน้ำรั่วซึม (Water Leak) ในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center)

๒. เฝ้าระวังภัยอันเกิดจากน้ำท่วม โดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยากรณีน้ำท่วม

๓. ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรกเกอร์เครื่องปรับอากาศเพื่อป้องกันเครื่องควบคุมเสียหายและป้องกันภัยจากไฟฟ้า

๔. เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูงหรือจัดเก็บในที่ปลอดภัย

๕. กรณีน้ำลดลงเรียบร้อยแล้ว ให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่าย ว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

๖. ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

๗. เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวปฏิบัติ

ข้อ ๑ อาคาร สถานที่และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒ ห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) เป็นสถานที่ควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

๒.๑ กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะ โดยพิจารณาตามความสำคัญแล้วแต่กรณี

๒.๒ ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก

๒.๓ ต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

๒.๔ ต้องปิดล็อค หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

๒.๕ หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว

๒.๖ ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าวเป็นอันขาด

๒.๗ จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๓ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๓.๑ มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

๓.๒ กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔ การควบคุมการเข้า-ออก อาคารสถานที่

๔.๑ กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๔.๒ การเข้าถึงอาคารของ ขร. ของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

๔.๓ ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

๔.๔ ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๔.๕ บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๔.๖ จัดเก็บบันทึกการเข้า-ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๔.๗ ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญ จนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๔.๘ มีกลไกการอนุญาตบุคคลภายนอกเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญ ต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๔.๙ สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอก เข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๔.๑๐ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญ ทั้งดำเนินการจัดเก็บแล้วหรือประมวลผลอยู่

๔.๑๑ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ เว้นแต่ได้รับการอนุญาต

๔.๑๒ มีการพิสูจน์ตัวตน เช่น การสแกนนิ้ว/สแกนหน้า การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

๔.๑๓ จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๔.๑๔ จัดให้มีการทบทวนหรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๕.๑ มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- ระบบปรับอากาศและควบคุมความชื้น
- ระบบตรวจจับควันไฟ
- ระบบตรวจจับน้ำรั่วซึม
- ระบบดับเพลิงชนิดก๊าซอัตโนมัติ

๕.๒ ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๕.๓ ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือน กรณีที่ระบบสนับสนุนการทำงานภายในห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center) ทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๖ การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security)

๖.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๖.๒ ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๖.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๖.๔ ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๖.๕ จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

๖.๖ ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักหรือกุญแจให้สนิทเพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๖.๗ พิจารณาใช้งานสายไฟเบอร์ออปติกแทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

๖.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๗ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๗.๑ ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๗.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๗.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๗.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๗.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๗.๖ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๘.๑ ให้มีการขออนุญาต ก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๘.๒ กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๘.๓ กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๘.๔ เมื่อมีการนำอุปกรณ์ส่งคืนให้ตรวจสอบว่า สอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๘.๕ บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises)

๙.๑ กำหนดมาตรการความปลอดภัย เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๙.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๙.๓ เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment)

๑๐.๑ ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๑๐.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

ส่วนที่ ๑ การตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศสำหรับ ขร.

ข้อ ๑ ระบบป้องกันผู้บุกรุก

ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมีดังต่อไปนี้

๑.๑ มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด

๑.๒ ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่

๑.๓ ระดับความรุนแรงมากน้อยเพียงใด

๑.๔ หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

ข้อ ๒ ระบบไฟร์วอลล์

๒.๑ ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

๒.๒ ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบ มีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพีของเครือข่ายใดถูก Block เป็นจำนวนมาก

๒.๓ กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งผู้บังคับบัญชาทราบทันที และรายงานต่อผู้บริหารระดับสูง เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ ๓ ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

๓.๑ ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใดและถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายใน ขร. ไปยังภายนอกหรือไม่

๓.๒ ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของ ขร.

๓.๓ ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอกต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

ข้อ ๔ ต้องจัดทำแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศอย่างไร ซึ่งรวมไปถึงความมั่นคงปลอดภัยไซเบอร์ โดยแผนดังกล่าวต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๔.๑ โครงสร้างทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Response Team: IRT) โดยทีมดังกล่าวมีหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ด้วย นอกจากนี้ ต้องกำหนดบทบาท และความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ

๔.๒ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่า ขร. จะปฏิบัติตามภาระหน้าที่ในการรายงานใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองที่ตราขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย นั้นๆ และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับการปกป้องคุ้มครองบริการที่สำคัญหรือระบบงานที่สำคัญของ ขร.

๔.๓ เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ IRT

๔.๔ ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๕ การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

๔.๖ ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

๔.๗ ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่นๆ เพื่อสนับสนุนการสอบสวน

๔.๘ ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติ การบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

๔.๙ กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

ข้อ ๕ ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญ หรือระบบงานที่สำคัญของ ขร.

ข้อ ๖ ต้องทบทวนแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย อย่างน้อยปีละ ๑ ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งแก้ไขปรับปรุงแผน หากเห็นสมควรว่าการแก้ไขปรับปรุงดังกล่าวทำให้การรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยมีประสิทธิภาพและประสิทธิผล

ข้อ ๗ ต้องมีการทดสอบแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย อย่างน้อยปีละ ๑ ครั้ง โดยต้องครอบคลุมถึงการทดสอบการบริหารจัดการเหตุการณ์ด้านภัยคุกคามทางไซเบอร์ (Cybersecurity Drill) มีการจัดเก็บประกอบด้วยข้อมูล ดังนี้

๗.๑ สถานการณ์ ความเสี่ยง (Risk Scenario) รูปแบบการทดสอบ วัน เวลา สถานที่ ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้องที่ใช้ในการทดสอบ

๗.๒ สรุปผลการทดสอบ ผลการประเมิน และ ผลการทบทวนขั้นตอนการบริหารจัดการเหตุการณ์

ข้อ ๘ ต้องมีการวิเคราะห์หาสาเหตุที่แท้จริง (Root Cause) ของเหตุการณ์ด้านความมั่นคงปลอดภัย และนำองค์ความรู้ที่ได้มาใช้ในการวางแผนและเตรียมการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจจะ เกิดขึ้นในอนาคต

ข้อ ๙ ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) เพื่อตอบสนองต่อวิกฤต ที่เกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัย ซึ่งอย่างน้อยต้องระบุเนื้อหาดังต่อไปนี้

๙.๑ จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

๙.๒ ระบุสถานการณ์จำลองเหตุการณ์ด้านความมั่นคงปลอดภัยที่เป็นไปได้และแผนการดำเนินการ ที่เกี่ยวข้อง (๓) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ด้านความมั่นคง ปลอดภัยแต่ละประเภท

๙.๓ ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนของ ขร. เพื่อกล่าวแถลงกับสื่อมวลชน

๙.๔ ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

ข้อ ๑๐ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่าย ที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

ข้อ ๑๑ ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถ สื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๑๒ ต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ (Cybersecurity Exercise) เมื่อได้รับคำสั่งเป็นลายลักษณ์อักษรจาก กมช. การฝึกซ้อมดังกล่าวอาจดำเนินการได้ทั้งในระดับชาติหรือระดับภาคส่วน โดย ขร. ต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยมีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

ข้อ ๑๓ ต้องปฏิบัติตามคำขอใดๆ ของ กมช. กกม. และ สกมช. เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่ กมช. กกม. และ สกมช. อาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย และแผนการสื่อสารในภาวะวิกฤต ขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร.

ข้อ ๑๔ กำหนดให้มีการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์และภัยคุกคามไซเบอร์ ในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และบริการที่สำคัญของ ขร. รวมทั้งมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบ เช่น ผู้ใช้งาน ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญของ ขร. เป็นต้น เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้ โดยรายละเอียด แนวทาง และรูปแบบใดการแบ่งปันข้อมูล ดังนี้

๑) จัดให้มีการระบุประเภทข้อมูลที่สามารถแบ่งปันได้ เช่น Indicator of Compromise (IOC) Tactics Techniques and Procedures (TTPs) เป็นต้น และกำหนดระดับความลับของข้อมูล

๒) ระบุขอบเขตผู้รับข้อมูล เช่น หน่วยงานภายในองค์กร ผู้ให้บริการที่เกี่ยวข้อง (Third Parties) พันธมิตรด้านความมั่นคงไซเบอร์ (Trusted Partners) หน่วยงานของรัฐ หน่วยงานกำกับดูแล หรือสาธารณะ (เฉพาะข้อมูลที่เปิดเผยได้) รวมถึงการเข้าถึงข้อมูล และเงื่อนไขการรักษาความลับ

๓) กำหนดให้มีผู้ตรวจสอบข้อมูลก่อนดำเนินการแบ่งปัน โดยเฉพาะข้อมูลที่มาจากบุคคลที่สาม

๔) กำหนดมาตรการป้องกันความเป็นส่วนตัว เช่น ลบหรือปกปิดข้อมูลให้สามารถระบุตัวบุคคลได้ (PII) เพื่อปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๕) กำหนดช่องทางแบ่งปันที่ชัดเจน และปลอดภัย และใช้ช่องทางที่กำหนดในการแบ่งปันข้อมูลเท่านั้น เช่น ผ่าน CERT ระบบ Threat Intelligence Sharing Platform เป็นต้น

๖) กำหนดให้มีการจัดเก็บประวัติการแบ่งปันข้อมูลและผู้รับข้อมูล เพื่อให้สามารถตรวจสอบย้อนหลังได้ในกรณีที่ข้อมูลถูกนำไปใช้ไม่เหมาะสม

๗) ให้ความรู้ความเข้าใจผู้รับผิดชอบในการแบ่งปันข้อมูล ให้สามารถดำเนินการตามแนวทาง การแบ่งปันข้อมูลอย่างปลอดภัย

ทั้งนี้ ในกรณีที่ สกมช. มีการประกาศกำหนดหลักเกณฑ์และวิธีการ แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงาน และสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้ดำเนินการตามประกาศกำหนดนั้น

ข้อ ๑๕ ต้องแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ พร้อมด้วยข้อมูลการติดต่อในกรณีมีเหตุฉุกเฉินภายในระยะเวลาหกสิบนาที เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยัง สกมช. หากมีการเปลี่ยนแปลงข้อมูล ให้แจ้งข้อมูลที่เปลี่ยนแปลงไปยัง สกมช. ภายใน ๑๕ วัน นับแต่วันที่มีการเปลี่ยนแปลง

ข้อ ๑๖ จัดทำรายงานประจำปี และส่งรายงานดังกล่าวให้สำนักงาน ภายในวันที่ ๓๑ มกราคมของปีถัดไป โดยรายงานต้องมีรายละเอียดดังต่อไปนี้

๑๖.๑ ระบุจำนวนและลักษณะของเหตุการณ์ภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน ตามแบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี ที่กำหนดท้ายประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗

๑๖.๒ วิเคราะห์สาเหตุหรือผลกระทบที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

๑๖.๓ ปัญหาและอุปสรรคในการดำเนินงาน

๑๖.๔ ข้อเสนอแนะต่างๆ ซึ่งรวมถึงข้อเสนอแนะเชิงนโยบาย

ข้อ ๑๗ ในกรณีที่มีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของ ขร. ให้แจ้งเหตุและส่งรายงานภัยคุกคามทางไซเบอร์ต่อ สกมช. ภายในระยะเวลา ๒๔ ชั่วโมงหลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์ โดยแบบรายงานภัยคุกคามทางไซเบอร์ให้เป็นไปตามที่ กกม. ประกาศกำหนด ให้ ขร. พิจารณาส่งข้อมูลสำคัญที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้อง กับนโยบายหรือแนวปฏิบัติว่าด้วยการรักษาความลับของ ขร. และต้องปรับปรุงข้อมูลในรายงานเหตุภัยคุกคามทางไซเบอร์และสถานะการตอบสนองภัยคุกคามทางไซเบอร์ให้สอดคล้องกับข้อมูลอันเป็นปัจจุบันที่ ขร. ได้สืบทราบเพิ่มมากขึ้นในระหว่างการดำเนินการรับมือเหตุภัยคุกคาม รวมทั้งจัดส่งรายงานปิดเหตุการณ์ภัยคุกคามต่อ สกมช.

ข้อ ๑๘ ให้ความร่วมมือกับ กกม. หรือพนักงานเจ้าหน้าที่ที่ได้รับคำสั่งจาก กกม. ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ข้อ ๑๙ ประสานงาน แจ้งเตือน ให้ความร่วมมือ หรือสนับสนุน แก่หน่วยงานควบคุมหรือกำกับดูแลอื่นเพื่อให้การควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีความสอดคล้องกัน

ข้อ ๒๐ ดำเนินการตามที่ กมช. หรือ กกม. มอบหมายหรือประกาศกำหนด เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๒๑ แต่งตั้งกลุ่มบุคคลทำหน้าที่เป็นผู้ตรวจสอบอันประกอบไปด้วยหัวหน้าทีมผู้ตรวจสอบ (Lead Auditor) และผู้ตรวจสอบ (Auditor) ที่มีความรู้ความเชี่ยวชาญด้านการตรวจสอบเรื่องความมั่นคงปลอดภัย ไซเบอร์ เพื่อดำเนินการตรวจสอบการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแล

ส่วนที่ ๒ การควบคุม หรือกำกับดูแล เพื่อตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศและไซเบอร์ ของหน่วยงานที่อยู่ภายใต้การควบคุมหรือกำกับดูแล

ข้อ ๒๒ กำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน เฉพาะบริการที่เป็นภารกิจหรือให้บริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Services) ให้อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยที่ยอมรับได้ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นและเป็นไปตามมาตรฐานที่เหมาะสม และสอดคล้องกับมาตรฐานขั้นต่ำที่กำหนด

ข้อ ๒๓ ตรวจสอบการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแล ให้เป็นไปตามมาตรฐานขั้นต่ำที่กำหนด และจัดทำรายงานสรุปผลการตรวจสอบให้แก่สำนักงานภายใน ๓๐ วัน หลังกระบวนการตรวจสอบเสร็จสิ้น

ข้อ ๒๔ ในกรณีที่พบว่าการดำเนินการไม่เป็นไปตามมาตรฐานขั้นต่ำที่กำหนด ให้แจ้งหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแก้ไขให้ได้มาตรฐาน พร้อมทั้งกำหนดเวลาให้ดำเนินการ

หากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ดำเนินการภายในระยะเวลาที่กำหนด ให้ผู้ที่ได้รับมอบหมายควบคุมหรือกำกับดูแลของ ขร. ดำเนินการแจ้ง กกม. เพื่อดำเนินการ

ข้อ ๒๕ ให้ความช่วยเหลือ สนับสนุน หรือประสานงานในการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแล

ข้อ ๒๖ ให้ความช่วยเหลือ สนับสนุน หรือประสานงานในการประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแล

ข้อ ๒๗ รับทราบและให้ความเห็นหรือข้อเสนอแนะเกี่ยวกับระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำก่อนส่งให้แก่สำนักงาน

ข้อ ๒๘ รับแจ้งและเก็บรักษาข้อมูลรายชื่อและข้อมูลการติดต่อของเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ และของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ที่ได้รับจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ปลอดภัย

ข้อ ๒๙ เก็บรักษาข้อมูลที่จำเป็นของหน่วยงานที่ได้รับการแต่งตั้งหรือถูกยกเลิกจากการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ข้อ ๓๐ รับแจ้งข้อมูลจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้ที่อยู่ในการควบคุมหรือกำกับดูแล และดำเนินการรวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์

ข้อ ๓๑ แจ้งเตือน ให้ความช่วยเหลือ หรือสนับสนุนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในควบคุมหรือกำกับดูแล ในการจัดทำหรือปรับปรุงมาตรการป้องกัน รับมือ ปราบปรามและระงับภัยคุกคามทางไซเบอร์ ให้มีความเหมาะสมและเป็นปัจจุบัน และเก็บรักษาข้อมูลดังกล่าวให้ปลอดภัย

ข้อ ๓๒ ให้ความช่วยเหลือหรือสนับสนุนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในควบคุมหรือกำกับดูแล ในการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ และการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

ข้อ ๓๓ ให้ความร่วมมือ สนับสนุนหรือดำเนินการเพื่อให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ข้อ ๓๔ ให้ความร่วมมือหรือสนับสนุนแก่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ในการติดตามการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และผลการตอบสนองและรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

ข้อ ๓๕ ความร่วมมือกับสำนักงานหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของ ขร.

๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้น จากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

แนวปฏิบัติ

ข้อ ๑ จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรม โดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

ข้อ ๓ จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนามีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ ๔ ติดประกาศประชาสัมพันธ์หรือ Infographic ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๕ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตามและประเมินผล ตลอดจนสำรวจความต้องการของผู้ใช้งาน

ข้อ ๖ ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ พร้อมทั้งให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

ข้อ ๗ สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของ ขร.

ข้อ ๘ ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบของ ขร. และข้อตกลงระหว่างประเทศ (ถ้ามี) อย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๙ ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๙.๑ กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ดังนี้

๙.๑.๑ พนักงานใหม่ (New Employees)

๙.๑.๒ ผู้ใช้และระดับบริหาร (Users and Management)

๙.๑.๓ ผู้ขาย ผู้รับเหมา และผู้ให้บริการภายนอก (Vendors, Contractors and Service Providers)

๙.๒ การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร.

๙.๓ การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งานและการเข้าถึงบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร.

๙.๔ การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ

ข้อ ๑๐ ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

หมวดที่ ๗ หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

แนวปฏิบัติ

ข้อ ๑ **ระดับนโยบาย** ผู้รับผิดชอบ ได้แก่ ผู้บริหารระดับสูงสุด (Chief Executive Office : CEO) ของ ขร. และมีรองอธิบดีกรมการขนส่งทางราง เป็นผู้ช่วย

๑.๑ รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตามกำกับดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับบริหารและระดับปฏิบัติ

๑.๒ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒ **ระดับบริหาร** ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการกองยุทธศาสตร์และแผนงาน หรือผู้อำนวยการกองที่กำกับดูแลด้านเทคโนโลยีและสารสนเทศ

ข้อ ๓ **ระดับปฏิบัติ** ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากผู้บริหารระดับสูงและ/หรือผู้อำนวยการกองยุทธศาสตร์และแผนงาน หรือผู้อำนวยการกองที่กำกับดูแลด้านเทคโนโลยีและสารสนเทศ เช่น นักวิชาการคอมพิวเตอร์ เป็นต้น

๓.๑ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๒ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓.๓ รับผิดชอบควบคุม ดูแลรักษาความปลอดภัยและบำรุงรักษาระบบเครื่องคอมพิวเตอร์ระบบเครือข่ายและห้องปฏิบัติการศูนย์ข้อมูลกลาง (Data Center)

๓.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๓.๕ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๓.๖ รับผิดชอบในการรักษาความปลอดภัยระบบอินเทอร์เน็ต

๓.๗ ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ขร.

หมวดที่ ๘ การบริหารจัดการการใช้บริการจากหน่วยงานภายนอก

วัตถุประสงค์

เพื่อให้หน่วยงานภายนอก ได้ปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ ขร. ทำให้ระบบสารสนเทศดำเนินไปได้อย่างต่อเนื่องและมีประสิทธิภาพ

แนวปฏิบัติ

ข้อ ๑ ต้องทำการคัดเลือก ตรวจสอบคุณสมบัติและประเมินความสามารถของผู้ให้บริการภายนอกที่จะคัดเลือกเข้าทำงานร่วมกับ ขร. อย่างเหมาะสม ตามลักษณะของงานที่ทำการจ้าง และระดับความสำคัญของข้อมูลและระบบเทคโนโลยีสารสนเทศที่ผู้ให้บริการภายนอกนั้นๆ ต้องเข้าถึงหรือใช้งาน ทั้งนี้ วิธีการดำเนินการ ตรวจสอบคุณสมบัติต้องไม่ขัดต่อกฎหมาย กฎระเบียบ และจริยธรรม และต้องแจ้งต่อผู้ให้บริการภายนอกที่ถูกตรวจสอบอย่างเหมาะสมทุกครั้งก่อนดำเนินการ โดยการตัดสินใจในการใช้บริการ การเชื่อมต่อหรือการเข้าถึง ข้อมูลจากผู้ให้บริการภายนอกที่มีความเสี่ยงหรือมีนัยสำคัญ ควรได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

ข้อ ๒ ต้องมีการกำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกผู้ให้บริการภายนอก โดยคำนึงถึงเรื่องดังนี้

๒.๑ ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการในช่วงที่ผ่านมา และระบบการบริหารงานภายใน

๒.๒ การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน

๒.๓ การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่างๆ

๒.๔ การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

๒.๕ การปฏิบัติตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ ซึ่งรวมไปถึงการรักษาความมั่นคงปลอดภัยสารสนเทศ

๒.๖ การใช้เทคโนโลยีสารสนเทศแบบเปิด (Open Technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (Interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยีสารสนเทศ ผู้ให้บริการหรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง

๒.๗ การที่ผู้ให้บริการภายนอกมอบหมายการปฏิบัติงานที่สำคัญ ให้กับบุคคลอื่นต่อ (Sub-Contracting to Another Supplier)

ข้อ ๓ ต้องมีการประเมินด้านคุณภาพและความน่าเชื่อถือของบุคคลภายนอก โดยพิจารณาจากประสบการณ์ คุณภาพของบริการและผลงานที่ส่งมอบ ตลอดจนมาตรฐานด้านความปลอดภัยสารสนเทศที่เกี่ยวข้องกับสินค้าและบริการ และจัดทำเป็นรายชื่อบุคคลภายนอกที่เชื่อถือได้ (Trusted third-party/Trusted vendor) เพื่อใช้เป็นส่วนหนึ่งของเกณฑ์การคัดเลือกผู้ให้บริการในอนาคต

ข้อ ๔ ต้องจัดให้ผู้ให้บริการภายนอกทุกรายลงนามในเอกสารต่อไปนี้ ตามความเหมาะสมก่อนเริ่มปฏิบัติงาน

๔.๑ สัญญาการปฏิบัติงาน (Contract) และ/หรือ สัญญาบริการ (Service Level Agreement)

๔.๒ สัญญารักษาความลับ (Non-Disclosure Agreement: NDA) ขององค์กรระหว่างหน่วยงานและหน่วยงานภายนอกที่เข้ามาปฏิบัติงานก่อนเปิดให้ใช้บริการระบบเสมอ

ข้อ ๕ สัญญาระหว่าง ขร. และหน่วยงานภายนอกในการให้บริการต้องระบุถึงหัวข้อต่างๆ ดังต่อไปนี้เป็นอย่างน้อย

- ขอบเขตการให้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก
- ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของ ขร. ตามความต้องการของ ขร. และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- บทบาท หน้าที่ และความรับผิดชอบในการปกป้องบริการที่สำคัญ หรือระบบงานที่สำคัญของ ขร. จากเหตุการณ์ด้านความมั่นคงปลอดภัย
- รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ
- มาตรฐานขั้นต่ำในการปฏิบัติงานของผู้ให้บริการภายนอก
- ข้อตกลงระดับการให้บริการ (Service Level Agreement)
- หน้าที่และความรับผิดชอบขององค์การและหน่วยงานภายนอก ในการให้บริการในครั้งนี้
- ระยะเวลาในการให้บริการและการตรวจรับงานบริการในครั้งนี้
- ราคาและเงื่อนไขการชำระเงิน
- ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อหรือพัฒนาขึ้น (ถ้ามี)
- การรักษาความลับของข้อมูลที่ได้รับจากการให้บริการแก่องค์การ
- การติดตามและรายงานผลการปฏิบัติงานของผู้ให้บริการภายนอก
- ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์
- รายชื่อ และช่องทางการติดต่อในกรณีเกิดปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- การทำลายข้อมูลเมื่อสิ้นสุดสัญญาหรือข้อตกลง
- เงื่อนไขหรือสิทธิของ ขร. ในการเปลี่ยนแปลง ยุติ หรือยกเลิกสัญญาหรือข้อตกลง กับผู้ให้บริการภายนอก
- การจัดให้มีแผนฉุกเฉินด้านความมั่นคงปลอดภัยสารสนเทศ
- สิทธิ์ของ ขร. ในการเข้าตรวจสอบการปฏิบัติงาน และการปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่ ขร. กำหนด
- ความรับผิดชอบต่อความเสียหายที่เกิดจากผู้ให้บริการภายนอก
- เงื่อนไขเกี่ยวกับการจ้างช่วง

- การรายงานการเปลี่ยนแปลงที่สำคัญของผู้ให้บริการภายนอก ที่อาจมีผลกระทบต่อความสามารถในการปฏิบัติตามสัญญา เช่น การเปลี่ยนแปลงการบริการของผู้ให้บริการภายนอก เป็นต้น

- การแจ้งล่วงหน้าต่อ ขร. เป็นลายลักษณ์อักษรกรณีที่ผู้ให้บริการภายนอกมีการดำเนินการเปลี่ยนแปลงใดๆ ที่อาจส่งผลกระทบต่อการให้บริการตามสัญญาจ้างหรือข้อตกลงอื่นๆ เพื่อให้ ขร. ทำการพิจารณาอนุมัติวิเคราะห์ผลกระทบ และหาวิธีในการแก้ไขควบคุมความเสี่ยงได้อย่างเหมาะสม โดยมีการประเมินความเสี่ยงและแนวทางควบคุมความเสี่ยง พร้อมทั้งขออนุมัติยกเว้นจากผู้มีอำนาจ หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาข้อตกลงหรือสัญญาการให้บริการระหว่าง ขร. และผู้ให้บริการภายนอกที่เป็นผู้ให้บริการงานด้านเทคโนโลยีสารสนเทศรายที่มีนัยสำคัญ มีการระบุสิทธิให้ ขร. และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจาก ขร. สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของผู้ให้บริการภายนอก กรณีที่ไม่สามารถระบุสิทธิข้างต้น การเลือกใช้ผู้ให้บริการภายนอกจะมีการพิจารณาอย่างรัดกุม และเหมาะสมกับความเสี่ยง เช่น พิจารณาจากผลการตรวจสอบด้านเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอก ที่ดำเนินการโดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล

ข้อ ๖ ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

ข้อ ๗ การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของหน่วยงานจากหน่วยงานภายนอก ต้องมีการขออนุญาตอย่างเป็นทางการ และได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

ข้อ ๘ การบริการและการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่างๆ ของ ขร.

ข้อ ๙ ผู้ดูแลระบบต้องให้สิทธิ์การเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น

ข้อ ๑๐ ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดำเนินงาน และวิธีการดำเนินงานเป็นอย่างน้อย เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการให้เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และเป็นไปตามขอบเขต ที่ได้กำหนดไว้

ข้อ ๑๑ ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

ข้อ ๑๒ ต้องควบคุมให้ผู้ให้บริการภายนอกเก็บรักษาข้อมูลทุกประเภทที่ได้รับหรือรับทราบจาก ขร. ไว้เป็นความลับ โดยอนุญาตให้ใช้ข้อมูลเพื่อการปฏิบัติงานให้แก่ ขร. เท่านั้น

ข้อ ๑๓ ต้องจัดให้มีการบันทึกรายการของอุปกรณ์และซอฟต์แวร์ทั้งหมด รวมถึงบันทึกการเข้าถึงอุปกรณ์ และการเชื่อมต่อกับระบบเครือข่ายของ ขร. ในกรณีที่ ขร. มีการตั้งอุปกรณ์และซอฟต์แวร์ของ ขร. ไว้ในสถานที่ของผู้ให้บริการภายนอก

ข้อ ๑๔ ต้องกำหนดให้ผู้ให้บริการภายนอกแจ้งรายชื่อของเจ้าหน้าที่ที่จะเข้าปฏิบัติงานต่อ ขร. ก่อนเริ่มปฏิบัติงาน และทุกครั้งที่มีการเปลี่ยนแปลงบุคคลที่เข้าปฏิบัติงาน

ข้อ ๑๕ ต้องควบคุมให้ผู้ให้บริการภายนอก เข้าถึงและใช้งานข้อมูล และระบบเทคโนโลยีสารสนเทศของ ขร. ตามวิธีปฏิบัติตามที่ ขร. กำหนดไว้

ข้อ ๑๖ ต้องมีการกำหนดระยะเวลาของสิทธิของผู้ให้บริการภายนอก ในการเข้าใช้งานระบบสารสนเทศ ของ ขร. อย่างชัดเจน โดย ขร. ต้องกำหนดให้ผู้ให้บริการภายนอก ได้รับสิทธิในการเข้าถึงเฉพาะระบบสารสนเทศ ที่ได้รับอนุญาตเท่านั้น

ข้อ ๑๗ ต้องจัดให้มีการบันทึกและตรวจสอบสิทธิในการเข้าถึงระบบต่างๆ ของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

ข้อ ๑๘ ต้องกำหนดให้ผู้ให้บริการภายนอก รายงานสิ่งผิดปกติหรือเหตุละเมิดความมั่นคงปลอดภัย (Security Incident) ต่อ ขร. ทันทีที่พบเหตุ

ข้อ ๑๙ ผู้ดูแลระบบและพนักงานผู้ติดต่อประสานงานกับผู้ให้บริการภายนอก มีหน้าที่ดูแล ควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอก ที่เกี่ยวข้องให้เป็นไปตามเอกสารสัญญา ข้อตกลง รวมถึง กฎระเบียบ นโยบาย ขั้นตอนการปฏิบัติงานและวิธีการปฏิบัติงานต่างๆ ของ ขร. อย่างเคร่งครัด

ข้อ ๒๐ ต้องมีการควบคุมการจ้างช่วงของผู้ให้บริการภายนอกให้เป็นไปตามระเบียบของ ขร.

ข้อ ๒๑ มีการประเมินผลการปฏิบัติงานหรือผลการให้บริการของผู้ให้บริการภายนอก ทั้งในด้านประสิทธิภาพของบริการ การรักษาความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง เมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่ ขร. กำหนด รวมถึง มีการทบทวนคุณสมบัติผู้ให้บริการภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกยังคงมีคุณสมบัติที่เหมาะสม

ข้อ ๒๒ ต้องมีการเตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย และปัญหา ด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจ ได้อย่างต่อเนื่อง

ข้อ ๒๓ เมื่อสิ้นสุดสัญญาการปฏิบัติงาน มีการเปลี่ยนแปลงสัญญา ยกเลิกสัญญา หรือ มีการเปลี่ยนแปลง บุคคลที่เข้าปฏิบัติงานของผู้ให้บริการภายนอก พนักงานผู้ติดต่อประสานงาน ผู้ดูแลระบบที่เกี่ยวข้อง หรือพนักงาน ที่ได้รับมอบหมาย ต้องทำการควบคุมดูแลให้มีการส่งคืนทรัพย์สินต่างๆ ของ ขร. และเพิกถอนสิทธิในการเข้า ระบบต่างๆ อย่างเหมาะสม

หมวดที่ ๙ การบริหารความต่อเนื่อง

วัตถุประสงค์

เพื่อให้องค์กรสามารถตอบสนองต่อเหตุการณ์ไม่คาดคิดที่อาจส่งผลกระทบต่อการดำเนินงาน และมั่นใจว่าบริการและกระบวนการหลักยังคงดำเนินต่อไปได้ในระหว่างเกิดวิกฤต รวมถึงลดความเสียหายทางการเงิน ชื่อเสียง และผลกระทบอื่นๆ ที่อาจเกิดจากการหยุดชะงักของการให้บริการของ ขร. และสามารถกลับสู่ภาวะปกติได้อย่างรวดเร็ว

แนวปฏิบัติ

ข้อ ๑ กำหนดให้มีการบริหารความต่อเนื่องและการประเมินความเสี่ยงโดยพิจารณาจากกระบวนการดำเนินงาน การวิเคราะห์ผลกระทบทางธุรกิจเพื่อระบุเหตุการณ์ที่สามารถทำให้บริการด้านระบบเทคโนโลยีสารสนเทศหยุดชะงักลงได้ ทั้งนี้ กำหนดให้มีการทบทวนความเสี่ยง และผลกระทบทางธุรกิจอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงสำคัญ หรืออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ การพัฒนาและจัดทำแผนการบริหารความต่อเนื่องทางธุรกิจรวมถึงความมั่นคงปลอดภัยของข้อมูล โดยกำหนดให้แผนการบริหารความต่อเนื่องต้องประกอบด้วยหัวข้ออย่างน้อย ดังต่อไปนี้

๒.๑ มีการระบุกระบวนการดำเนินการที่มีความสำคัญของ ขร. การใช้งานทรัพยากรร่วมกันหรือความต่อเนื่องกันของกระบวนการที่มีความสำคัญทั้งหมด

๒.๒ กำหนดลำดับความสำคัญของกระบวนการที่ต้องกู้คืน

๒.๓ ระบุหน้าที่ความรับผิดชอบและการเตรียมการสำหรับกรณีฉุกเฉินทั้งในส่วนของผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน พนักงานทั่วไป และหน่วยงานภายนอก

๒.๔ กำหนดกลยุทธ์ที่ใช้ในการกู้คืนและทรัพยากรที่ต้องการ เช่น สถานที่ปฏิบัติงานสำรอง ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายสำรองข้อมูลที่ได้สำรองไว้ เป็นต้น

๒.๕ ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายสำรองที่กำหนดในแผนการบริหารความต่อเนื่องจะต้องมีการทดสอบความพร้อมใช้งาน และความเข้ากันได้กับระบบปฏิบัติงานจริง อย่างสม่ำเสมอ หรือทดสอบอย่างน้อยปีละ ๑ ครั้ง

๒.๖ การจัดเตรียมเอกสาร ขั้นตอนต่างๆ ที่ได้ระบุไว้ในแผนการบริหารความต่อเนื่องทางธุรกิจ

๒.๗ กำหนดให้มีการทบทวนความสอดคล้องของแผนการบริหารความต่อเนื่องทางธุรกิจและปรับปรุงให้ทันสมัยอยู่เสมอ หรือทบทวนอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๓ จัดให้มีการทดสอบด้านการบริหารความต่อเนื่องของธุรกิจอย่างน้อยปีละ ๑ ครั้ง โดยกำหนดวิธีทดสอบ เกณฑ์ที่ใช้ ก่อนดำเนินการจริง พร้อมทั้งติดตามข้อบกพร่องที่พบในระหว่างการทดสอบ เพื่อให้มีการปรับปรุงประสิทธิภาพ

ข้อ ๔ ขร. กำหนดให้มีการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้การดำเนินการกู้คืนระบบการให้บริการที่สำคัญ จึงได้กำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ ที่เกี่ยวข้องกับบริการที่สำคัญ ดังนี้

๑) กำหนดบทบาทหน้าที่ความรับผิดชอบให้ชัดเจน

๒) กำหนดเป้าหมายการกู้คืนระบบที่เกี่ยวข้องกับบริการที่สำคัญ โดยระยะเวลาเป้าหมายการกู้คืนระบบการให้บริการที่สำคัญ มีดังนี้

(๑) ระยะเวลาเป้าหมายสำหรับการกู้คืนกระบวนการที่มีความสำคัญ (RTO) ๒๔ ชั่วโมง

(๒) ระยะเวลามากที่สุดที่ยอมให้ข้อมูลสูญหายนับจากมีการแจ้งเหตุฯ (RPO) ๓ วัน

(๓) ระยะเวลานานที่สุดที่องค์กรยอมรับได้หากมีการหยุดชะงัก (MTPD) ๒๔ ชั่วโมง

๓) ความเสี่ยงและมาตรการลดความเสี่ยง อ้างอิงเอกสาร การประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของ ขร.

๔) แผนกู้คืนระบบที่เกี่ยวข้องกับบริการที่สำคัญ

(กรณีที่ ๑) เมื่อเกิดเหตุการณ์ที่มีการบุกรุกจากภายนอก โดยประเมินแล้ว เหตุการณ์มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการตามแผนกู้คืนดังนี้

(๑) ตรวจสอบ log และการตั้งค่า Firewall เพื่อวิเคราะห์หาสาเหตุการเข้ามาและผลกระทบที่เกิดขึ้น

(๒) แจ้งให้หัวหน้ากลุ่มเทคโนโลยีและสารสนเทศทราบ

(๓) ดำเนินการการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ถูกบุกรุกเข้ามา

(กรณีที่ ๒) เมื่อเกิดเหตุการณ์ที่มีการมีการแพร่กระจายของไวรัส (Virus) มัลแวร์ (Malware) มัลแวร์เรียกค่าไถ่ หรือแรนซัมแวร์ (Ransomware) โดยประเมินแล้วเหตุการณ์มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการตามแผนกู้คืนดังนี้

(๑) ตัดการเชื่อมต่อทางเครือข่าย สำหรับเครื่องคอมพิวเตอร์ที่โดนมัลแวร์ (Malware) ระบบสำรองข้อมูล รวมถึงตัดการเชื่อมต่ออุปกรณ์จัดเก็บข้อมูลภายนอก และระบบสารสนเทศที่อยู่ในเครือข่ายเดียวกัน

(๒) แจ้งให้หัวหน้ากลุ่มเทคโนโลยีและสารสนเทศทราบ

(๓) ตรวจสอบเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายเดียวกับเครื่องที่ติดมัลแวร์ (Malware) เพื่อประเมินสถานการณ์ด้วยวิธีการดังนี้

- ตรวจสอบความผิดปกติภายในเครื่องคอมพิวเตอร์
- Full Scan ใน Anti-Virus และ Anti-Malware

(๔) ประสานเพื่อขอความช่วยเหลือไปยังสำนักงานคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เบอร์ติดต่อ ๐๒-๑๔๒๖๘๘๘ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ผ่านทางโทรศัพท์ เบอร์ติดต่อ ๐๒-๑๒๓๑๒๑๒

(๕) ปฏิบัติตามคำแนะนำของผู้เชี่ยวชาญ

(๖) กรณีเครื่อง Client ใช้คอมพิวเตอร์สำรอง ข้อมูลที่ถูกสำรองไว้ หรือข้อมูลบน Cloud ในการทำงาน โดยไม่ยุ่งเกี่ยวกับข้อมูลหรือเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ (Malware) จนกว่าการแก้ไขสถานการณ์จะสิ้นสุดลง

(๗) กรณีเครื่อง Server ประสานงานผู้ให้บริการภายนอก เพื่อดำเนินการกู้คืนข้อมูลจากอุปกรณ์ที่ได้ดำเนินการ Backup ไว้

๕) การกลับสู่ภาวะปกติ

(๑) กรณี Client ทำการล้างเครื่องทั้งหมดแบบ Clean format ไม่ให้มีข้อมูลหลงเหลือใน Hard Disk ก่อนทำการลงเครื่องใหม่ ทั้งหมด

(๒) กรณี Server ทำการ Restore Backup Data, Application and Configuration

(๓) ดำเนินการ Test Restore

(๔) ตั้งค่าระบบ การกำหนด Vhost เพื่อให้ผู้ใช้งานสามารถใช้เข้าใช้งานได้ตามปกติ

(๕) ทดสอบความพร้อมใช้งานของระบบและความครบถ้วนของข้อมูลที่กู้คืน

(๖) รายงานผลการกู้คืนให้หัวหน้ากลุ่มเทคโนโลยีและสารสนเทศรับทราบ

ข้อ ๕ กำหนดให้มีการวิเคราะห์ภัยคุกคามหรืออันตรายที่จะเกิดต่อการดำเนินงานที่สำคัญต่อพันธกิจของ ขร. โดยแยกกระบวนการดำเนินการพันธกิจของ ขร. โดยดำเนินการวิเคราะห์ผลกระทบในการดำเนินการตามพันธกิจของ ขร. (BIA) ซึ่งมี ๕ ขั้นตอน ดังนี้

๑) ระบุกระบวนการดำเนินการตามพันธกิจของ ขร. (BIA) โดยคำนึงถึงความสำคัญของกระบวนการหรือบริการที่มีต่อบริการตามพันธกิจของ ขร. เช่น กระบวนการควบคุมและกำกับดูแลผู้ให้บริการขนส่งทางราง กระบวนการตรวจสอบผู้ให้บริการขนส่งทางราง การให้บริการงานด้าน IT ภายในหน่วยงาน เป็นต้น

๒) พิจารณาผลกระทบจากการหยุดชะงักของกระบวนการหรือบริการที่สำคัญ

๓) กำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerable Downtime) โดยระยะเวลาดังกล่าวควรเป็นเวลาสูงสุดที่หน่วยงานที่เกี่ยวข้องกับกระบวนการใน ขร. สามารถยอมให้ระบบหรือกระบวนการหยุดชะงักภายใต้เงื่อนไขที่ต้องดำเนินการตามภารกิจหรือการให้บริการที่สำคัญของ ขร.ให้สามารถดำเนินการต่อไปได้

๔) กำหนดทรัพยากรของระบบที่จำเป็นต้องกู้คืนระบบ หรือกระบวนการที่จำเป็น เช่น สถานที่, บุคลากร, อุปกรณ์, ซอฟต์แวร์ ไฟล์ข้อมูลของระบบสารสนเทศ ส่วนประกอบของระบบ และเอกสารบันทึกข้อมูลสำคัญต่าง ๆ ที่เกี่ยวข้อง เพื่อให้หน่วยงานสามารถกลับมาดำเนินการหรือให้บริการที่สำคัญให้ได้ให้เร็วที่สุด

๕) ดำเนินการเชื่อมโยงทรัพยากรที่จำเป็นต่อการกู้คืนระบบกับกระบวนการหรือบริการที่สำคัญของ ขร. เพื่อกำหนดระดับความสำคัญของทรัพยากร และเรียงลำดับการดำเนินการกู้คืนระบบ

หมวดที่ ๑๐ การเผยแพร่และทบทวน

๑. นโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางราง ต้องทำการเผยแพร่ตามช่องทางที่กำหนดไว้ เพื่อให้ผู้ที่เกี่ยวข้องทั้งภายใน และภายนอกของ ขร. ได้รับทราบและถือปฏิบัติตามหลักเกณฑ์นี้อย่างเคร่งครัด

๒. นโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางราง ต้องถูกทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๓. นโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการขนส่งทางราง ต้องได้รับการดำเนินการตรวจสอบ และประเมินตามระยะเวลาอย่างน้อยปีละ ๑ ครั้ง

๕. แผนรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) ของ ขร.

๑. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมการขนส่งทางราง ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ (๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามแผนการตรวจสอบและการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วย

๒. วัตถุประสงค์

๑. เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในกรมการขนส่งทางราง โดยเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่าง ๆ ภายใต้ ขร. การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของ ขร.

๒. เพื่อสร้างความเชื่อมั่นให้ผู้ใช้งานระบบเครือข่ายของ ขร. ถึงการได้รับการปกป้องต่อภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ

๓. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของ ขร. รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity incident Response Team Committee : CSIRT) มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) และ ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO) อย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลต่อแผนรับมือฯ อย่างมีนัยสำคัญ

๕. หน้าที่ในการดำเนินการตามแผน

หน่วยงานที่ดูแลด้านระบบสารสนเทศของ ขร. มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย กองยุทธศาสตร์และแผนงาน รวมถึงกลุ่มเทคโนโลยีและสารสนเทศ และหน่วยงานภายในกรมต่อไปนี้ สำนักงานเลขานุการกรม, กองกฎหมาย, กองมาตรฐานความปลอดภัยและบำรุงทาง, กองกำกับกิจการขนส่งทางราง, กลุ่มพัฒนาระบบบริหาร และกลุ่มตรวจสอบภายใน

๖. รายละเอียดการบังคับใช้เอกสาร

ขร. ได้ระบุรายละเอียดที่เกี่ยวข้องกับเอกสาร ดังต่อไปนี้

๖.๑ รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	นายศรัทธา พันธ์พุทธ
ผู้ดำเนินการตามเอกสาร (Owner)	นายภูวิศ รักษาแก้ว, นายมนตรี สุดสาย, นายศรัทธา พันธ์พุทธ
วันที่จัดทำเอกสาร (Date created)	๑ มีนาคม ๒๕๖๗
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	นางสาววรกร พุ่มเรือง
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	มีนาคม ๒๕๖๗
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	นายอธิภู จิตรานุเคราะห์ (CISO)
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	มีนาคม ๒๕๖๗

๖.๒ การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
๑.๐	มีนาคม ๒๕๖๗	นายอธิภู จิตรานุเคราะห์ (CISO)	ร่างเอกสาร

๗. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

๗.๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร.

๗.๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร.

๗.๓ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

๘. คำนิยาม

เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ทรัพย์สินสำคัญทางสารสนเทศ หมายความว่า ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญหรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ตามที่หน่วยงานพิจารณาแล้วเห็นว่ามีความจำเป็นต้องเฝ้าระวัง หรือดำเนินมาตรการป้องกัน รับมือ และแก้ไขภัยคุกคามทางไซเบอร์

แนวปฏิบัติพื้นฐาน (Security Control Baselines) หมายความว่า แนวปฏิบัติพื้นฐานที่กำหนดไว้สำหรับการดำเนินมาตรการป้องกันรับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

๙.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายใน ขร.

ขร. ระบุข้อมูลการติดต่อของผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายใน ขร. กรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยมีผู้รับแจ้งเหตุฯ หลักรวมถึงช่องทางหลักในการติดต่อ และเตรียมผู้รับแจ้งเหตุฯ คนที่สอง รวมถึงช่องทางสำรองสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้ โดย ขร. กำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุฯ คลอบคลุมตลอดระยะเวลา ๒๔ ชั่วโมง/๗ วัน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	คุณภูวิศ รักษาแก้ว	๐๘.๓๐ – ๑๖.๓๐	๐๘๒๗๙๑๕๘๒๖	ผู้ประสานงานหลัก	ผู้ประสานด้านความมั่นคงลอดภัยไซเบอร์ของ ขร.
๒	คุณณัฐวีร์ พูลสมบัติภิญโญ	๐๘.๓๐ – ๑๖.๓๐	๐๙๑ ๗๗๑ ๒๗๕๕	ผู้รับผิดชอบโครงการ	- ดูแลเว็บไซต์ ขร. - ดูแลระบบสำนักงานอัตโนมัติ (E-office) - ดูแลระบบสำนักงานอัตโนมัติ (E-office) ระยะที่ ๒
๓	บริษัท กันโด้	๐๐.๐๐ – ๒๓.๕๙	๐๙๒ ๔๙๕ ๓๖๕๑	ผู้รับจ้างพัฒนาระบบ	ดูแลเว็บไซต์ ขร.
๔	บริษัท K&O	๐๐.๐๐ – ๒๓.๕๙	๐๘๑ ๔๙๔ ๖๕๔๔	ผู้รับจ้างพัฒนาระบบ	ดูแลระบบสำนักงานอัตโนมัติ (E-office)
๕	บริษัท CDG	๐๐.๐๐ – ๒๓.๕๙	๐๒ ๖๗๘ ๐๙๗๘	ผู้รับจ้างพัฒนาระบบ	ดูแลระบบสำนักงานอัตโนมัติ (E-office) ระยะที่ ๒
๖	นายกิจติศักดิ์ รำไพรุจิพงศ์	๐๘.๓๐ – ๑๖.๓๐	๐๘๙ ๙๒๑ ๖๓๖๓	ผู้รับผิดชอบโครงการ	E-License R
๗	อาจารย์ศุภวุฒิ มาลัยกฤษณะชาลี	๐๐.๐๐ – ๒๓.๕๙	๐๘๖ ๐๘๔ ๒๔๔๔	ผู้พัฒนาระบบ	E-License R
๘	คุณพลากร กลัดเจริญ	๐๘.๓๐ – ๑๖.๓๐	๐๙๖ ๘๕๘ ๗๒๓๓	ผู้รับผิดชอบโครงการ	DRT Crossing
๙	นางสมปรารถนา มาลัยกฤษณะชลี	๐๐.๐๐ – ๒๓.๕๙	๐๙๔ ๕๑๔ ๕๙๕๔	ผู้รับจ้างดูแลระบบ	DRT Crossing
๑๐	คุณภูวิศ รักษาแก้ว	๐๘.๓๐ – ๑๖.๓๐	๐๘๒๗๙๑๕๘๒๖	ผู้รับผิดชอบโครงการ	ดูแลระบบเครือข่าย ขร.
๑๑	บริษัท เอ็นพีร่า	๐๐.๐๐ – ๒๓.๕๙	๐๘๗ ๗๕๘ ๗๕๐๐	ผู้รับจ้างดูแลระบบเครือข่าย	ดูแลระบบเครือข่าย ขร.

๙.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

กรมการขนส่งทางราง ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ โดยมีการกำหนดบทบาทหน้าที่หลัก และโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) ดังนี้

๙.๒.๑ หน้าที่ความรับผิดชอบหลักของทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) ดังนี้

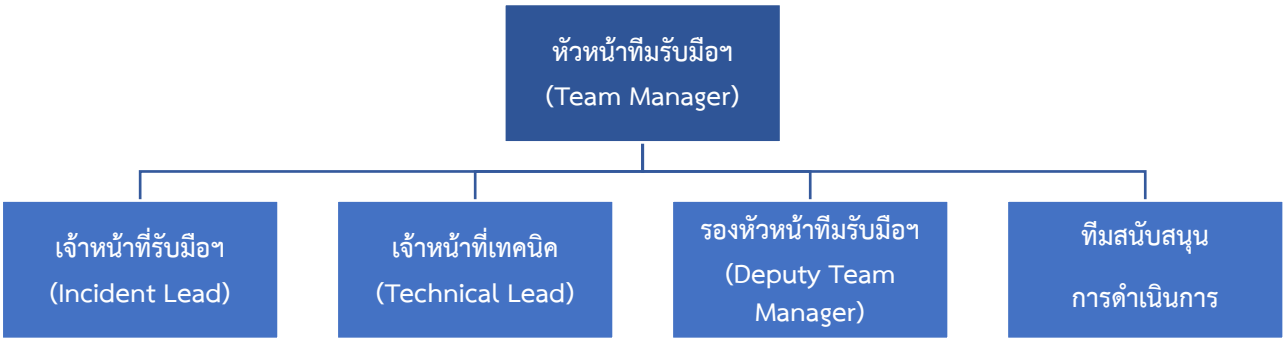
๑) การเฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ (Intrusion Detection)

๒) ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวข้องกับการใช้งานเทคโนโลยี (Advisory Distribution) เกี่ยวกับ จุดอ่อน การป้องกัน ข้อควรระมัดระวัง รวมทั้งแจ้งเตือนภัยคุกคามเกิดใหม่ เพื่อให้ทุกคนในองค์กรมีความตระหนัก

๓) การฝึกอบรมเพื่อสร้างความตระหนัก (Education and Awareness) เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับบุคลากรทุกระดับ เพื่อให้ทุกคนในองค์กรตระหนักรู้ถึงความผิดปกติและช่วยในการสอดส่องดูแลให้กับองค์กรในการตรวจจับและแจ้งเหตุการณ์ที่ผิดปกติ

๔) การมีส่วนร่วมกับหน่วยงานภายนอกองค์กร (Information Sharing) ควรกำหนดขั้นตอนการสื่อสารและประเภทข้อมูล ที่สามารถนำไปแบ่งปันได้กับบุคคลภายนอก ทั้งหน่วยงานบังคับใช้กฎหมาย หน่วยงานกำกับดูแล องค์กรอื่น หรือการติดต่อเพื่อขอความช่วยเหลือจากผู้เชี่ยวชาญจากภายนอกองค์กรที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ เช่น TI-CERT, TCM CERT, TB CERT และ Thai CERT เป็นต้น เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์ เพื่อช่วยให้การป้องกันและตอบสนองต่อภัยคุกคามได้เร็วยิ่งขึ้น

๙.๒.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) ประกอบด้วย



ลำดับ	ชื่อ นามสกุล รายละเอียดการติดต่อ	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	คุณวรกร พุ่มเรือง		หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของ ขร.
๒	คุณภูวิศ รักษาแก้ว	๐๘๒ ๗๙๑ ๕๘๒๖	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	คุณณัฐวีร์ พูลสมบัติภิญโญ	๐๙๑ ๗๗๑ ๒๗๕๕	เจ้าหน้าที่รับมือฯ (Incident Team)	ทำหน้าที่ช่วยเหลือ ขร. ให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
	คุณสุกฤษฎิ์ คำหอมกุล	๐๘๘ ๖๓๘ ๐๘๗๐		
	คุณมนตรี สุดสาย	๐๘๕ ๑๑๘ ๙๐๙๘		
	คุณศรัทธา พันธ์พุทธ	๐๖๓ ๖๙๑ ๐๖๑๔		
	คุณธีรพัฒน์ ยิ้มเจริญ	๐๘๖ ๖๘๑ ๑๕๗๕		
	คุณธรรมสรณ์ อยู่ไพศาล	๐๘๒ ๔๘๙ ๖๕๘๒		
๔	คุณภูวิศ รักษาแก้ว	๐๘๒ ๗๙๑ ๕๘๒๖	เจ้าหน้าที่เทคนิค (Technical)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับที่	ชื่อ นามสกุล	หน้าที่	ความรับผิดชอบ
๑	คุณวรกร พุ่มเรือง	เจ้าหน้าที่จาก ขร.	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๒	Pentest สกมช.	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตามแผนรับมือภัยคุกคามทางไซเบอร์ของ ขร.
๓	ผู้อำนวยการกองกฎหมาย	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่ตามแผนรับมือภัยคุกคามทางไซเบอร์ของ ขร.
๔	คุณขวัญสิรี ช่วงวิไล	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตามแผนรับมือภัยคุกคามทางไซเบอร์ของ ขร.
๕	คุณธีรพัฒน์ ยิ้มเจริญ	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตามแผนรับมือภัยคุกคามทางไซเบอร์ของ ขร.
๖	คุณภูวิศ รักษาแก้ว	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ตามแผนรับมือภัยคุกคามทางไซเบอร์ของ ขร.

คุณสมบัติและทักษะด้านเทคนิค (Technician) ที่พึงมี ประกอบด้วย

ศักยภาพด้านบุคคล

- ยืดหยุ่น มีความคิดสร้างสรรค์ และทำงานเป็นทีม
- มีทักษะการวิเคราะห์ที่ดีเยี่ยม
- สามารถอธิบายข้อมูลเชิงเทคนิคให้ผู้อื่นเข้าใจได้ง่าย
- มีความมั่นใจสูงและทำงานอย่างเป็นระบบ
- อดทนต่อความกดดัน
- มีทักษะด้านการติดต่อสื่อสารและการเขียนดีเยี่ยม
- เปิดใจและพร้อมที่เรียนรู้สิ่งใหม่

ศักยภาพด้านเทคนิค

- มีความรู้ทางด้านเทคโนโลยีอินเทอร์เน็ตและโปรโตคอลอย่างกว้างขวาง
- มีความรู้ทางด้านระบบ Linux, Unix และ Windows
- มีความรู้ทางด้านอุปกรณ์โครงสร้างเครือข่าย
- มีความรู้ทางด้านแอพพลิเคชันและบริการบนอินเทอร์เน็ต เช่น SMTP, HTTP(s), Social Media และอื่นๆ
- มีความรู้ทางด้านภัยคุกคาม เช่น DDoS, Phishing, Defacing, Malware และอื่นๆ
- มีความรู้ทางด้านการประเมินความเสี่ยงและการวางระบบ
- มีความรู้ทางด้านการวิเคราะห์ข้อมูลแบบ Big Data และ Malware

ศักยภาพด้านอื่น ๆ

- พร้อมทำงานแบบ ๗/๒๔ หรือพร้อมรับการติดต่อตลอดเวลา
- มีประสบการณ์การทำงานในสาย IT Security

๙.๓ หน่วยงานภายนอกที่เกี่ยวข้อง

ขร. ได้จัดให้มีข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หน่วยงานกำกับดูแล (Regulator) THAI – CERT และผู้ให้บริการภายนอกของหน่วยงาน เช่น หน่วยงานผู้ให้บริการด้านการตรวจสอบพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic Investigator) เป็นต้น

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	สำนักงาน คณะกรรมการ การรักษาความมั่นคง ปลอดภัยไซเบอร์ แห่งชาติ (สกมช.)	เบอร์โทรศัพท์ : ๐๒ ๑๔๒ ๖๘๘๘ Email : thaicert@ncsa.or.th ที่อยู่สำนักงาน : ๑๒๐ หมู่ ๓ อาคารรัฐ- ประศาสนภักดี (อาคารบี) ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กทม. ๑๐๒๑๐	สำนักงาน คณะกรรมการการ รักษาความมั่นคง ปลอดภัยไซเบอร์ แห่งชาติ (สกมช.)	หน่วยงานหลัก
๒	กระทรวงคมนาคม	เบอร์โทรศัพท์ : ๐๒ ๒๘๓ ๓๐๐๐ email : saraban@mot.go.th ที่อยู่ : ๓๘ ถนนราชดำเนินนอก แขวงวัดโสมนัส เขตป้อมปราบศัตรูพ่าย กทม. ๑๐๑๐๐	กระทรวงคมนาคม	หน่วยงาน ต้นสังกัด
๓	คุณพิมพ์รพัชร์ ขัติวงค์	เบอร์โทรศัพท์มือถือ : ๐๖๑ ๔๙๔ ๖๕๔๔ Email : hrm@ko.in.th ที่อยู่ : ๑๕ Q-Doc Studio ๑๗ ซ.กรุงธนบุรีซอย ๔ แขวงบางลำพูล่าง เขตคลองสาน กทม. ๑๐๖๐๐	K&O Systems and Consulting Co.,Ltd.	E-Office
๔	คุณชัยสิริ ธนสถิรชัย	เบอร์โทรศัพท์ : ๐๒ ๖๗๘ ๐๙๗๘ email : marcom.cdgs@cdg.co.th ที่อยู่ : ๒๐๒ อาคารซีดีจีเฮ้าท์ ถนนนางลิ้นจี่ แขวงช่องนนทรี เขตยานนาวา กทม. ๑๐๑๒๐	CDG Systems Ltd.	E-Office๒
๕	คุณกันต์กมล เสนานนท์	เบอร์โทรศัพท์มือถือ : ๐๘๗ ๗๕๘ ๗๕๐๐ Email : info@npera.co.th ที่อยู่สำนักงาน : ๑๓๘/๔๙ ถนนรังสิต-ปทุมธานี ต.บ้านกลาง อ.เมือง จ.ปทุมธานี ๑๒๐๐๐	บริษัท เอ็นพีร่า จำกัด	MA แม่ข่าย และระบบ เครือข่าย
๖	คุณกันต์นนท์ จงพีร์เพียง	เบอร์โทรศัพท์มือถือ : ๐๙๒ ๔๙๕ ๓๖๕๑ Email : P@gundodigital.com ที่อยู่สำนักงาน : ๕๘๔/๑ สุขุมวิท ๖๕ ถนนสุขุมวิท แขวงพระโขนงเหนือ เขตวัฒนา กทม. ๑๐๑๑๐	บริษัท กันโด้ จำกัด	เว็บไซต์กรมฯ
๗	อาจารย์ศุภวุฒิ มาลัยกฤษณะชาลี	เบอร์โทรศัพท์มือถือ : ๐๘๖ ๐๘๔ ๒๔๔๔ Email : fengshm@ku.ac.th ที่อยู่สำนักงาน : ๕๐ ถนนงามวงศ์วาน แขวงลาดยาว เขตจตุจักร กทม. ๑๐๙๐๐	มหาวิทยาลัย เกษตรศาสตร์	E-License R

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๘	นางสมปรารถนา มาลัยกฤษณะชลี	เบอร์โทรศัพท์มือถือ : ๐๙๔ ๕๑๔ ๕๙๕๔ Email : sompratana.j@gmail.com ที่อยู่สำนักงาน : ๒๙๙/๑๒๔ หมู่บ้านวิสต้า ปาร์ควิภาวดี ถนนวิภาวดีรังสิต แขวงตลาดบางเขน เขตหลักสี่ กทม. ๑๐๒๑๐	บริษัท มันตาวิศวกรรมและเทคโนโลยี จำกัด	DRT Crossing
๙	รองศาสตราจารย์ ดร. วเรศรา วีระวัฒน์	เบอร์โทรศัพท์มือถือ : Email : waressara.wee@mahidol.ac.th ที่อยู่สำนักงาน : คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล	มหาวิทยาลัยมหิดล	BKK Rail
๑๐	การรถไฟแห่งประเทศไทย	เบอร์โทรศัพท์ : ๑๖๙๐ Email : sarabanklang@railway.co.th ที่อยู่สำนักงาน : เลขที่ ๑ ถนนรองเมือง แขวงรองเมือง เขตปทุมวัน กทม.๑๐๓๓๐	การรถไฟแห่งประเทศไทย	หน่วยงานที่เกี่ยวข้อง
๑๑	การรถไฟขนส่งมวลชนแห่งประเทศไทย	เบอร์โทรศัพท์ : ๐๒ ๗๑๖ ๔๐๐๐ Email : saraban@mrta.co.th ที่อยู่สำนักงาน : ๑๗๕ ถนนพระราม ๙ เขตห้วยขวาง แขวงห้วยขวาง กทม. ๑๐๓๑๐	การรถไฟขนส่งมวลชนแห่งประเทศไทย	หน่วยงานที่เกี่ยวข้อง
๑๒	บริษัท รถไฟฟ้า ร.ฟ.ท. จำกัด	เบอร์โทรศัพท์ : ๑๖๙๐ Email : cus.redline@srtet.co.th ที่อยู่สำนักงาน : สถานีกลางกรุงเทพอภิวัฒน์ เลขที่ ๑๐ ถนนกำแพงเพชร แขวงจตุจักร เขตจตุจักร กทม.๑๐๙๐๐	บริษัท รถไฟฟ้า ร.ฟ.ท. จำกัด	หน่วยงานที่เกี่ยวข้อง
๑๓	บริษัท ระบบขนส่งมวลชนกรุงเทพ จำกัด	เบอร์โทรศัพท์ : ๐๒ ๖๑๗ ๗๓๐๐ Email : nuduan@bts.co.th ที่อยู่สำนักงาน : อาคารบีทีเอส ๑๐๐๐ ถนนพหลโยธิน แขวงจอมพล เขตจตุจักร กทม. ๑๐๙๐๐	บริษัท ระบบขนส่งมวลชนกรุงเทพ จำกัด	หน่วยงานที่เกี่ยวข้อง

<u>๙.๔ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)</u>

ขร. จัดทำแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก เป็นต้น รวมถึงกำหนดว่า หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ซึ่งมีรายละเอียดของขั้นตอนการปฏิบัติเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ดังนี้

ขั้นตอน	ผู้รับผิดชอบ
๑. การแจ้งเหตุ	ผู้พบเห็น/ผู้ที่ได้รับผลกระทบจาก incident
๒. ขั้นการเตรียมการ (Preparation) ๒.๑ นโยบายหรือแนวปฏิบัติที่เกี่ยวข้อง ๒.๒ จัดเตรียมทรัพยากรที่ใช้ในการดำเนินงาน ๒.๓ เตรียมการป้องกันและแจ้งเตือน ๒.๔ เตรียมรายละเอียดช่องทางการ ติดต่อสื่อสาร ๒.๕ การให้ความรู้ และวิธีปฏิบัติ ๒.๖ ทดสอบการตอบสนองต่อภัยคุกคามทางไซเบอร์	ทีมรับมือและตอบสนองต่อ incident (CSIRT Team) และเจ้าของระบบฯ
๓. ขั้นการตรวจจับและวิเคราะห์ภัยคุกคาม (Detection & Analysis) ๓.๑ รับแจ้งเหตุ ๓.๒ วิเคราะห์ความผิดปกติเมื่อได้รับแจ้ง ๓.๓ บันทึกข้อมูลเหตุการณ์ภัยคุกคาม ๓.๔ จัดลำดับความสำคัญของ incident ๓.๕ ติดต่อประสานงานกับหน่วยงานภายใน และภายนอก	ผู้รับแจ้งเหตุ IT Team ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ (SOC) ผู้รับแจ้งเหตุ IT Team ทีมรับมือและตอบสนองต่อ incident (CSIRT Team) และเจ้าของระบบฯ ทีมรับมือและตอบสนองต่อ incident (CSIRT Team) และเจ้าของระบบฯ
๔. การระงับภัยคุกคามทางไซเบอร์ (Containment) ๔.๑ ควบคุมความเสียหาย ๔.๒ จัดเก็บและดูแลหลักฐานทางดิจิทัล	ทีมรับมือและตอบสนองต่อ incident (CSIRT Team) และเจ้าของระบบฯ
๕. การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟู (Eradication & Recovery) ๕.๑ แก้ไขสาเหตุ และผลกระทบจากการโจมตี ๕.๒ กู้คืนระบบ ข้อมูล และภาพลักษณ์จากความเสียหาย	ทีมรับมือและตอบสนองต่อ incident (CSIRT Team) และเจ้าของระบบฯ
๖. การดำเนินการภายหลังการแก้ปัญหาภัยคุกคาม (Post-incident) ๖.๑ เก็บรักษาหลักฐานและบันทึกการ ดำเนินงาน ๖.๒ ปรับปรุงและพัฒนากระบวนการ กลไก แนวปฏิบัติในการรับมือ	ทีมรับมือและตอบสนองต่อ incident (CSIRT Team) และเจ้าของระบบฯ

๑๐.ลักษณะของภัยคุกคามทางไซเบอร์ และปัจจัยที่ใช้ในการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับ

ในการพิจารณาระบุระดับของภัยคุกคามทางไซเบอร์ หน่วยงานโครงสร้างสำคัญทางสารสนเทศควรพิจารณาจากเหตุการณ์ต่าง ๆ ที่เป็นพฤติกรรมแวดล้อม ผลกระทบที่เกิดขึ้น ความเสี่ยงหรือแนวโน้มที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ในกรณีต่าง ๆ เพื่อพิจารณาว่าลักษณะของภัยคุกคามทางไซเบอร์นั้นอยู่ในระดับใด โดยให้พิจารณาจากปัจจัยที่ใช้ในการประเมินทั้ง ๔ ปัจจัย ดังนี้

(๑) ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน

(๒) ลักษณะผลกระทบต่อข้อมูลในระบบ

(๓) แนวโน้มในการกู้คืนระบบ

(๔) ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ

การพิจารณาเพื่อระบุระดับของภัยคุกคามทางไซเบอร์แต่ละระดับนั้น หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรพิจารณาให้ครบทั้ง ๔ ปัจจัย ตามที่ได้ระบุไว้ข้างต้น โดยหากปรากฏข้อเท็จจริงว่าลักษณะภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้นเข้าลักษณะหรือมีแนวโน้มเป็นภัยคุกคาม ทางไซเบอร์ในระดับใด ให้ถือเอาระดับสูงสุดที่ประเมินได้เป็นเกณฑ์ในการระบุระดับของภัยคุกคามไซเบอร์ในครั้งนั้น ๆ นอกจากนี้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอาจพิจารณากำหนดปัจจัยที่ใช้ในการประเมินและลักษณะภัยคุกคามทางไซเบอร์เพิ่มเติมร่วมกับหน่วยงานควบคุมหรือกำกับดูแลเพื่อให้มีแนวทางในการจำแนกระดับของภัยคุกคามทางไซเบอร์ที่เหมาะสม โดยจะต้องมีรายละเอียดไม่น้อยกว่าหรือเทียบเท่ากับแนวทางการพิจารณาที่กำหนดไว้ตามเอกสารแนบท้ายตารางที่ ๑

อย่างไรก็ดี เพื่อให้การดำเนินการรับมือ ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับมีความเหมาะสมและสอดคล้องกับสถานการณ์โดยรวมที่เกิดขึ้น คณะกรรมการอาจพิจารณาปรับเปลี่ยนหรือยกระดับของภัยคุกคามทางไซเบอร์ที่ได้รับรายงานเป็นอย่างอื่นได้ หากปรากฏข้อเท็จจริงเพิ่มเติมหรือพบว่าภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้นมีแนวโน้มที่จะลุกลามหรือก่อให้เกิดความเสียหายมากขึ้น

อนึ่ง เพื่อให้สอดคล้องกับสภาวการณ์ที่เปลี่ยนแปลงไป คณะกรรมการหรือผู้ที่ได้รับมอบหมายจากคณะกรรมการอาจพิจารณาทบทวนลักษณะภัยคุกคามทางไซเบอร์ ปรับปรุงปัจจัยที่ใช้ในการประเมินหรือนำเงื่อนไขอื่น ๆ มาประกอบการพิจารณาเพิ่มเติมที่เห็นสมควร

๑๑. รูปแบบภัยคุกคามไซเบอร์

๑. ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือที่เรียกโดยทั่วไปว่า มัลแวร์ (Malware) ซึ่งเป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

๒. ไวรัสคอมพิวเตอร์(Computer Virus) เป็นมัลแวร์ชนิดหนึ่ง ที่สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ซึ่งไวรัสคอมพิวเตอร์จะแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยใช้พาหะ เช่น แฟลชไดร์ฟติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

๓. หนอนคอมพิวเตอร์ (Computer Worm) เป็นมัลแวร์ชนิดหนึ่ง สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต โดยหนอนคอมพิวเตอร์จะต่างกับไวรัสตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์

จะใช้วิธีสแกน เครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอปพลิเคชัน จากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังตัวโดยใช้ช่องโหว่ดังกล่าว

๔. ม้าโทรจัน (Trojan Horse) เป็นมัลแวร์ชนิดหนึ่ง ที่มีจุดประสงค์เพื่อบุกรุก เข้าถึง และควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูลดังกล่าวส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการอาจเป็น ชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่น ๆ ลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัยพาหะ ซึ่งอาจมาจากแฟลชไดร์ฟ หรือทางอีเมล

๕. สปายแวร์ (Spyware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

๖. ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีพฤติกรรมเข้ารหัสไฟล์ต่าง ๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลย หากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนกลับมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ

๗. ประตูหลัง (Backdoor) เป็นช่องทางพิเศษที่ใช้เข้าถึงระบบงานคอมพิวเตอร์โดยที่ไม่ต้องผ่านการพิสูจน์ทราบตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลังเอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบงานคอมพิวเตอร์ในภายหลัง

๘. Rootkit เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ทั้งนี้ นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ด้วย

๙. การโจมตีแบบ DoS/DDoS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงานหากเครื่องคอมพิวเตอร์ที่โจมตีมีเครื่องเดียว เรียกว่า การโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมีมากกว่าหนึ่งเครื่องและกระทำพร้อม ๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจจะเรียกว่า การโจมตีแบบ Distributed Denial of Service (DDoS)

๑๐. Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่นๆ เพื่อรอรับคำสั่งจากผู้บุกรุก (Hacker) โดยผู้บุกรุกจะนำ Botnet ที่มีไปใช้ในการโจมตีที่มีขนาดใหญ่ขึ้น เช่น การทำ DDoS เป็นต้น

๑๑. Spam Mail หรืออีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการและสร้างความเดือดร้อน ความรำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด Phishing แฝงเข้ามาด้วย ด้วยเหตุนี้ จึงควรติดตั้งระบบ Anti-Spam หรือ หากใช้ฟรีอีเมลก็จะมีโปรแกรมคัดกรองอีเมลขยะในชั้นหนึ่งแล้ว

๑๒. Phishing คือ การหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลข บัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่ Phishing กล่าวถึง

๑๓. Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่ง ไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่ผู้บุกรุกระบบนิยมใช้

๑๔. Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรม ด้วยวัตถุประสงค์ต่างๆ กัน ทั้งนี้ โดยทั่วไปแล้วการ Hacking เป็นสิ่งที่ผิดกฎหมาย แต่อย่างไรก็ตาม หากได้รับอนุญาตก็ไม่ใช่สิ่งผิดกฎหมาย โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบเพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่าย

๑๕. ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่างๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหาย จากผู้บุกรุกเป็นภัยคุกคามที่หนัก โดยการจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

ทั้งนี้ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์ให้เป็นไปตาม *ภาคผนวก ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์*

๑๒. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์

เพื่อให้ ขร. มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ จึงจะดำเนินการเตรียมความพร้อมในด้านต่าง ๆ ดังนี้

๑๒.๑ การเตรียมพร้อมด้านอุปกรณ์

เพื่อให้ระบบเทคโนโลยีสารสนเทศที่สำคัญสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ จึงควรมีการจัดหาอุปกรณ์และซอฟต์แวร์ที่มีความจำเป็น ดังนี้

๑๒.๑.๑ อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ซึ่งใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท DoS/DDoS, BOTNET, Phishing, Sniffing, Hacker เช่น อุปกรณ์ป้องกันระบบเครือข่ายนี้ นอกจากจะต้องมีความสามารถในการทำหน้าที่เป็น Firewall แล้วยังควรมีความสามารถอื่นเพิ่มเติม เช่น การตรวจจับการบุกรุก (IPS), การคัดกรองเว็บไซต์อันตราย (Web filtering) และการควบคุมการใช้งานซอฟต์แวร์ (Application Control) เป็นต้น

๑๒.๑.๒ ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจสอบและจับความผิดปกติภายในระบบเครือข่ายคอมพิวเตอร์กลาง และยังสามารถดำเนินการสำรองข้อมูลแบบเข้ารหัส โดยเก็บข้อมูลไว้ที่ฐานข้อมูลของกรมการขนส่งทางราง (ขร.)

๑๒.๑.๓ ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) เพื่อให้เครื่องคอมพิวเตอร์ (PC), เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์แม่ข่าย มีความปลอดภัยจากภัยคุกคามไซเบอร์ต่าง ๆ เช่น Malware, Computer Virus, Computer worm, Trojan, Spyware, Ransomware, BOTNET, Spam Mail จึงควรมีการจัดหาและติดตั้งซอฟต์แวร์ป้องกันไวรัสแบบคอร์ปอเรตเพื่อเสริมความแข็งแกร่งในการป้องกันเหล่านี้

๑๒.๒ แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์ สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา ต้องมีการประเมินความเสี่ยงด้านรักษาความมั่นคงปลอดภัยไซเบอร์และการตรวจสอบ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้ อาจสามารถค้นพบ

ภัยคุกคามไซเบอร์ หรือช่องโหว่ในระบบหรือกระบวนการ เพื่อสามารถปิดแก้ไขประเด็นที่พบว่ามีความเสี่ยงต่อภัยคุกคามทางไซเบอร์ หรือยกระดับการเตรียมพร้อมต่อภัยคุกคามทางไซเบอร์ให้แข็งแรงยิ่งขึ้น

๑๒.๓ การเตรียมพร้อมด้านบุคลากร

๑๒.๓.๑ การให้ความรู้เพื่อให้บุคลากรของกรมการขนส่งทางราง (ขร.) มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ จะดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากร

๑๒.๓.๒ ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Respond Capability Testing)

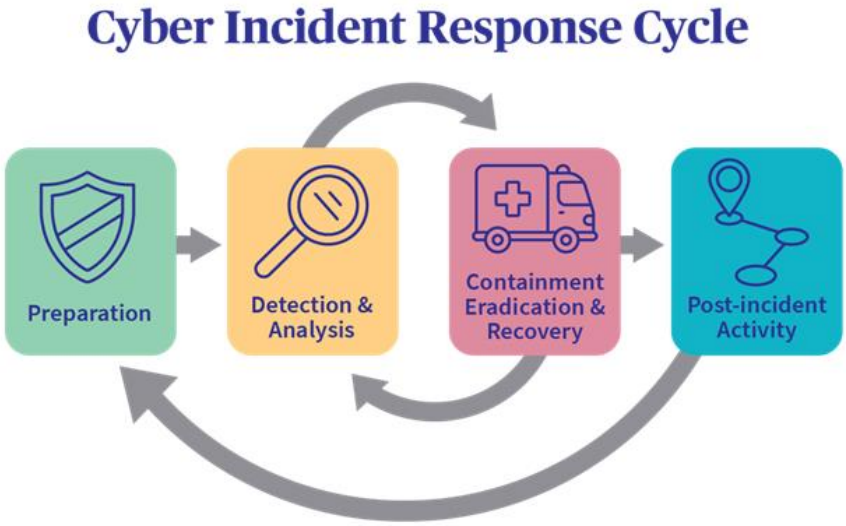
๑๒.๓.๓ มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลาง และระบบที่ดูแลโดยโครงการบริการคลาวด์ภาครัฐ (Government Cloud Service)

๑๒.๓.๔ การเตรียมพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรองในกรณีที่ภัยคุกคามทางไซเบอร์ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์กลางอย่างมาก จนไม่สามารถทำงานได้เป็นเวลานานจะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางสามารถใช้งานได้อย่างรวดเร็วที่สุด

ทั้งนี้ แนวทางในการกู้คืนข้อมูลและ การใช้ระบบคอมพิวเตอร์สำรองจะกำหนดอยู่ในแอกสารแผนสำรองและกู้คืนระบบ

๑๓. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔, ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖ รวมถึงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ขร. ดังนี้



๑๓.๑ ขั้นการเตรียมการ (preparation)

ขร. จะต้องดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

๑. กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ ๙.๒

๒. กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ ๙.๔

๓. กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

๔. จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปกรณ์ติดต่อสื่อสารของบุคลากร กลไกรายงานเหตุการณ์ ห้องประชุมWar room เป็นต้น

๕. จัดเตรียมอุปกรณ์ ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

๖. จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

๗. จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของ ขร. โดย ขร.ได้ทำการจัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ไว้ (รายละเอียดปรากฏตามภาคผนวก ๑)

นอกจากนี้ ขร. จะพิจารณาดำเนินการตามเอกสารแนบท้าย ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๓.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

ขร. จะต้องดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้ ขร. สามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ประกอบด้วยการดำเนินการตามตารางที่ ๓ ตามในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ในตารางที่ ๒.๒

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้วก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่และสามารถแจ้งเตือนได้อย่างทันท่วงที เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

๑๓.๒.๑ ขร. จะต้องดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน (Common Attack Vectors/ Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น

๑๓.๒.๒ ขร. ดำเนินการจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น รวมถึงการตรวจจับ incident จะขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายามโจมตี และกลไกในการปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์หาความผิดปกติและมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบ ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับ แบ่งได้เป็น ๒ ประเภท

- Precursor เป็นข้อมูลบ่งบอกว่า incident จะเกิดขึ้นในอนาคต
- Indicator เป็นข้อมูลบ่งบอกว่า incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับ ต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการแจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

๑. ประเภท Alert

๑) IDPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือนเมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

๒) SIEM ระบบตรวจจับความผิดปกติโดยใช้ข้อมูล Log จากระบบอื่น ๆ เพื่อนำมาวิเคราะห์ โดยต้องตั้งค่า Rule set โดยผู้เชี่ยวชาญ และเหมาะสมกับสภาพแวดล้อมที่เชื่อมต่ออยู่กับ SIEM (จะจัดหาในปีงบประมาณ ๒๕๖๗)

๓) Anti-Malware ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่าย และ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งที่กำลังพยายามโจมตีและการโจมตีได้สำเร็จแล้ว

๔) Third-Party บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบ หรือระบบของหน่วยงาน ถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กร ซึ่งบ่งบอกได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดี และนำไปใช้สร้างความเสียหาย

๒. ประเภท Log

๑) Operating System and Application Log ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วย การบันทึกเหตุการณ์หลายประเภท สามารถถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

๒) Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

๓. ข้อมูลจากแหล่งสาธารณะ ข้อมูลช่องโหว่ และวิธีการโจมตีระบบรูปแบบให้ไม่สามารถถูกใช้เป็นข้อบ่งชี้ภัยคุกคามได้

๔. บุคคลที่ทำหน้าที่แจ้งเตือนบุคคลภายในองค์กร บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝน เพื่อช่วยสอดส่องดูแล

๑๓.๒.๓ ขร. ต้องดำเนินการจัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้องเช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น โดยใช้แนวทางการวิเคราะห์ความผิดปกติ เมื่อได้รับแจ้งเหตุ ดังนี้

๑. log Retention Policy คือ การใช้ Log จากอุปกรณ์ต่าง ๆ เช่น IPS, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และบันทึกเหตุการณ์เก็บไว้เพื่อหลักฐานทางกฎหมายหรือเรียกดูในอนาคต จึงต้องมีการเก็บรักษาไว้เป็นอย่างดี และตามระยะเวลาตามกฎหมายกำหนด

๒. Clock Synchronization อุปกรณ์ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ตรงกันอยู่เสมอ เพื่อทำให้การ Correlate Event ทำได้ง่าย

๓. Sniff and Analyze Network Data ทำการดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ข้อมูล

๔. Seek Assistance เมื่อทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ incident เพื่อหาสาเหตุ ที่แท้จริงได้เพื่อกำจัดผู้บุกรุกออกจากระบบ จะใช้บริการให้คำแนะนำปรึกษาจากภายนอก เช่น CERT ต่างๆ

๑๓.๒.๔ ขร. ต้องดำเนินการจัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๒)

๑๓.๒.๕ ขร. ต้องจัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดย ขร. บันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่

เกิดเหตุและระยะเวลาที่ใช้ด้วยบันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ ควรลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสมโดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์ม (รายละเอียดปรากฏตามภาคผนวก ๓)

๑๓.๒.๖ การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจเชิงกลยุทธ์เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่อย่างจำกัดและลดผลกระทบทางธุรกิจให้น้อยลงที่สุด การกำหนดแนวทางในการวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident โดยอย่างน้อยควรครอบคลุมในด้านผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อข้อมูล (Information Impact) และความสามารถในการฟื้นฟูระบบ (Recoverability)

๑. ผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อการให้บริการ และการดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม พิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาสเกิดขึ้น หากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันที ซึ่งรวมถึงผลกระทบทางด้านการปฏิบัติงานของระบบการให้บริการต่าง ๆ ซึ่งส่งผลโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหายต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมีผลเสียมากยิ่งขึ้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีผลกระทบในการให้บริการหรือดำเนินงานตามปกติ
- Low มีผลน้อยมากต่อกระบวนการทำงานหลัก ทำให้ช้าลงบ้างแต่ผลที่ได้ยังครบถ้วนสมบูรณ์
- Medium ไม่สามารถให้บริการที่ครบถ้วนสมบูรณ์กับผู้ใช้งานบางกลุ่ม ทั้งภายในและภายนอก
- High ไม่สามารถให้บริการกับผู้ใดได้อีกต่อไป เป็นการหยุดชะงักโดยสมบูรณ์

๒. ผลกระทบต่อข้อมูล (Information Impact) ผลกระทบต่อข้อมูลควรพิจารณา ๓ ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อมใช้ (Availability) รวมทั้งควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมที่จะส่งผลต่อข้อมูลสำคัญ (Sensitive Information) อย่างไร เช่น ข้อมูลถูกทำลาย หรือสูญหาย หรือรั่วไหล หรือการแก้ไขโดยไม่ได้รับอนุญาต เป็นต้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึง โดยที่ไม่ได้รับอนุญาต
- Privacy Breach ข้อมูลที่ใช้ระบุตัวบุคคล (Personal Identifiable Information; PII) รั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
- Proprietary Breach ข้อมูลความลับที่ใช้ในการดำเนินธุรกิจ รั่วไหล หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
- Integrity Loss ข้อมูลที่เป็น Privacy และ Propriety ถูกเปลี่ยนแปลง หรือทำลายโดยไม่ได้รับอนุญาต

๓. ความสามารถในการฟื้นฟูระบบ (Recoverability) ความสามารถในการฟื้นฟูระบบควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของ

เหตุภัยคุกคามและประเภทของทรัพย์สินสารสนเทศ เช่น ระบบ และข้อมูล เป็นต้น ที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณาความสามารถ หรือความยากง่ายในการฟื้นฟูระบบ รวมทั้งทรัพยากรที่จำเป็นต้องใช้โดยระดับของ Recoverability Effort มีดังนี้

- Regular เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
- Supplemented เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
- Extended เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก
- Not Recoverable การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

๑๓.๒.๗ การฝึกฝนและการทดสอบผู้ทำหน้าที่รับมือและตอบสนองต่อ incident ควรได้รับการอบรมฝึกฝนและทดสอบการรับมือและตอบสนองต่อ incident เพื่อให้ทุกคนตระหนักและเข้าใจถึงหน้าที่ความรับผิดชอบและเป้าหมายตามแผนที่กำหนด รวมทั้งเพื่อเป็นการพัฒนาทักษะเพื่อให้สามารถดำเนินงานตามแผนได้อย่างมีประสิทธิภาพ และควรจัดให้มีการทดสอบแผนเป็นประจำ เพื่อประเมินและทราบถึงประเด็นหรือช่องโหว่ (Gap) ที่ควรพัฒนาและเพิ่มความชำนาญให้กับบุคลากรของทีมรับมือและตอบสนองฯ โดยการทดสอบแผนควรดำเนินการทดสอบอย่างสม่ำเสมอ

<u>๑๓.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication and recovery)</u>

ขร. จะต้องดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ประกอบด้วยการดำเนินการหลัก ดังนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึก การยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

โดยมีรายละเอียดในการดำเนินการ ดังนี้

๑. วิธีการควบคุมความเสียหาย คือ การตัดสินใจเลือกใช้วิธีการที่เหมาะสม ดังนี้

- ปิดระบบ (Shut Down)
- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

๒. การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัลวัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือ เพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อยที่สุด (Minimizing impact to the business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการ ตามขั้นตอนทางกฎหมาย ดังนี้ การดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณา ตามหลักการดังต่อไปนี้

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ ได้ในชั้นศาล
- หลักฐานมีบันทึกการเข้าถึงและการกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม
- การเปลี่ยนตัวผู้ดูแลจำเป็นต้องมีการจัดทำบันทึกห่วงโซ่หลักฐาน (Chain of Custody) (ภาคผนวก) รายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

๑) ข้อมูลเฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) และ Address เป็นต้น

๒) ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident

๓) สถานที่จัดเก็บหลักฐาน

๓. การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ เมื่อมีการควบคุมความเสียหายและมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้วข้อมูลทั้งหมด จะต้องนำกลับมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “ขั้นตอนที่ ๒ เรื่องการตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามา ในระบบทั้งหมดได้เรียบร้อย ซึ่งการกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบ ได้แก่

- การปิดช่องโหว่ของระบบ
- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน
- การลบโปรแกรมประเภท Backdoor ออกจากระบบ
- การใช้ข้อมูล Indicator of Compromise (IoC) ในการสแกนหา Malware หรือร่องรอยอื่นๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด

หลังจากดำเนินการควบคุมความเสียหาย กำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติ โดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่งและควรเตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย
- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

นอกจากนี้ ขร. พิจารณาดำเนินการตามเอกสารแนบท้าย ตารางที่ ๒.๓ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

<u>๑๓.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)</u>

ขร. กำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้ ขร. สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้ ขร. ต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง

ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) การทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

(๒) ดำเนินการตามเอกสารแนบท้าย ตารางที่ ๒.๔ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

โดยการเก็บข้อมูลบางประเภทนั้น อาจจำเป็นต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลาย โดยผู้โจมตีเมื่อมีการเก็บรวบรวมข้อมูล และหลักฐานที่จำเป็นแล้ว ให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญมี ๕ ข้อ ดังนี้

๑. การประเมิน (Assessment) เพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ incident ที่กำลังรับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น

๒. การดำเนินการจัดเก็บหลักฐาน (Acquisition) ด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้

๑) ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker

๒) ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของ หลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น

๓) ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด

๔) ต้องทำการบันทึกหลักฐาน (Chain of Custody)

๓. การตรวจสอบความถูกต้อง (Authentication) ของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับ ด้วยวิธี Cryptographic Hash เช่น MD๕, SHA๑, SHA๒๕๖

๔. การวิเคราะห์หาข้อมูลจากชุดหลักฐาน (Analysis & Report) ที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อค้นหาสาเหตุของการเกิด Incident

๕. การจัดเก็บหลักฐาน (Archive) ไว้ในที่เหมาะสม ปลอดภัย และบันทึกห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of custody form) ซึ่งเป็นเอกสารแสดงลำดับการเกิดเหตุการณ์ หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในยืนยันได้ในชั้นศาล หลักฐานเหล่านี้ จึงจะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำขึ้นมา ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย

๑๓.๕ การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

ขร. จะต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่ ขร. เกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดย ขร. สามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก ๕)

๑๔. การสื่อสารและรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์

๑๔.๑ รายงานเหตุการณ์ภัยคุกคามทางไซเบอร์

ขร. ต้องดำเนินการรายงานเหตุไปยัง สกมช. ในกรณีดังต่อไปนี้

๑๔.๑.๑ กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามข้อ ๔ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๑ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔)

๑๔.๑.๒ กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามข้อ ๕ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๒ รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔)

๑๔.๑.๓ จัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปีภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔)

นอกจากนี้ ขร.พิจารณาดำเนินการตามเอกสารแนบท้าย ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๔.๒ การสื่อสารไปยังกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียในภาวะวิกฤตทางไซเบอร์

เมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ ผู้รับหน้าที่ด้านสื่อสารองค์กรควรทำงานร่วมกับบุคลากรที่เกี่ยวข้อง เพื่อดำเนินการกำหนดกลยุทธ์และวิธีการสื่อสารอย่างเหมาะสม โดยควรพิจารณาแนวทางในการสื่อสาร ดังต่อไปนี้

หัวข้อ	แนวทางปฏิบัติในการสื่อสาร
แผนการสื่อสารในภาวะวิกฤต	จัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้องที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง
การระบุผู้มีส่วนได้ส่วนเสีย และช่องทางการสื่อสาร	กำหนดผู้มีส่วนได้ส่วนเสียหลัก เช่น ผู้ปฏิบัติงาน ขร. หน่วยงานรัฐบาล ประชาชนผู้รับบริการและสื่อมวลชน และกำหนดแพลตฟอร์ม หรือช่องทางการเผยแพร่ที่เหมาะสม และเผยแพร่ข้อมูลที่เหมาะสมกับแต่ละกลุ่ม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย)
การจัดตั้งทีมการสื่อสารฉุกเฉิน	ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน หรือต่อสาธารณะ
การกำหนดข้อความและโทนการสื่อสาร	พัฒนาข้อความที่ชัดเจนและสอดคล้องกับนโยบายและมาตรฐานขององค์กร โดยมีโทนการสื่อสารที่เป็นมืออาชีพและมุ่งเน้นการให้ข้อมูล

หัวข้อ	แนวทางปฏิบัติในการสื่อสาร
	สำหรับการสื่อสารไปยังบุคคลภายนอกซึ่งที่อาจส่งผลกระทบต่อ ขร. ภาพลักษณ์และชื่อเสียงของ ขร. ผู้รับหน้าที่ด้านสื่อสารองค์กรพิจารณาขออนุมัติจากผู้บริหารขององค์กรก่อนดำเนินการ
การตอบสนองต่อการสอบถามจากภายนอก	ตอบสนองต่อการสอบถามจากภายนอกอย่างรวดเร็วและมีข้อมูลที่ถูกต้อง พร้อมทั้งให้ข้อมูลอัปเดตอย่างสม่ำเสมอ
รักษาความลับและการปฏิบัติตามกฎหมาย	ตรวจสอบให้แน่ใจว่าการสื่อสารทุกครั้งปฏิบัติตามข้อกำหนดด้านกฎหมายและนโยบายความเป็นส่วนตัวขององค์กร โดยอาจพิจารณาให้ผู้เชี่ยวชาญด้านทางกฎหมาย ทบทวนเนื้อหาก่อนดำเนินการสื่อสาร
วิเคราะห์และปรับปรุงแผนแผนการสื่อสาร	หลังจากการสื่อสารเสร็จสิ้นในภาวะวิกฤตทางไซเบอร์ ควรทำการวิเคราะห์ผลลัพธ์และปรับปรุงแผนการสื่อสารเพื่อเพิ่มประสิทธิภาพในอนาคต

๑๕. การฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์

ดำเนินการฝึกซ้อมแผนการรับมือภัยคุกคามไซเบอร์ที่กำหนดขึ้น และการทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง นับแต่วันที่แผนได้รับการอนุมัติ โดยเริ่มทบทวนตั้งแต่การจัดทำแผนฯ เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล หรือดำเนินการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงกลยุทธ์และข้อกำหนดของ ขร. ระเบียบข้อบังคับ และกฎหมายที่เกี่ยวข้อง ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และภูมิทัศน์ ภัยคุกคามทางไซเบอร์และสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของการให้บริการที่สำคัญของ ขร. และควรดำเนินการทบทวนเพิ่มเติมเมื่อมีเหตุการณ์ ดังนี้

(ก) บทเรียนจากการปฏิบัติการตอบสนองต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นจริงในแต่ละวัน

(ข) สิ่งที่ได้จากการฝึกหัด/การอบรม

(ค) ผลที่ได้จากการฝึกซ้อมและข้อเสนอแนะหลังจากการฝึกซ้อมตามแผนการรับมือภัยคุกคามทางไซเบอร์ดังกล่าว

(ง) กลยุทธ์และข้อกำหนดของหน่วยงานที่อาจมีการเปลี่ยนแปลง

(จ) สภาพแวดล้อมของการปฏิบัติการทางไซเบอร์ของการให้บริการในหน่วยงานที่สำคัญที่อาจมีการเปลี่ยนแปลง

(ฉ) ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และภูมิทัศน์ภัยคุกคามทางไซเบอร์ (Threat Landscape) ที่มีการเปลี่ยนแปลง

(ช) ระเบียบ ข้อบังคับ และกฎหมายใหม่

(ซ) เทคโนโลยีใหม่

(ฌ) การเปลี่ยนแปลงยุทธศาสตร์ระดับชาติที่เกี่ยวข้องกับลำดับความสำคัญของระบบสารสนเทศหรือของการดำเนินงานตามภารกิจของหน่วยงาน

(ญ) ข้อมูลที่ได้จากระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence: CTI)

เอกสาร และข้อมูลประกอบ

ตารางที่ ๒.๑ การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	(๑) จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคล หรือองค์กรต่าง ๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใดที่ช่วยสนับสนุนการรายงานเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น (๒) จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคาม ทางไซเบอร์ (๓) ดำเนินการให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับแนวทางของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ตลอดจนสภาพพร้อมใช้งาน (availability) ของข้อมูลและระบบสารสนเทศดังกล่าว (๔) จัดเตรียมข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น รายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย(Network diagrams) เป็นต้น (๕) พิจารณาซ่อนบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (discovery protocol) เป็นต้น (๖) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan) (๗) กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ รวมถึงการทำหน้าที่ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง (๘) จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทำการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ใด ๆ เช่น การเข้ารหัสข้อมูลและการบริหารจัดการคีย์สำหรับการเข้าถึงระบบต่าง ๆ (cryptography / key managements) เป็นต้น (๙) ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยมีการคัดกรองนักพัฒนา (developer screening) ที่ได้รับมอบหมายให้ดำเนินการใด ๆ กับเครือข่าย แอปพลิเคชัน หรือระบบงานต่าง ๆ (๑๐) ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (incident respond capability testing) (๑๑) รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (threat Intelligence) (๑๒) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ เพื่อดำเนินการทดสอบการเจาะระบบเป็นประจำและสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อพบช่องโหว่หรือ จุดอ่อนต่าง ๆ (ถ้าหน่วยงานมีความพร้อม) (๑๓) กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ (๑๔) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลง ค่าของอุปกรณ์ (configuration management plan) โดยจะต้องจัดให้มีกลไกที่สามารถบันทึกประวัติการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ที่เป็นลายลักษณ์อักษร การแจ้งเตือนเมื่อมีการเปลี่ยนแปลงค่าของอุปกรณ์ที่ตั้งไว้ และให้พิจารณาจัดให้มีกลไกที่สามารถป้องกันการเปลี่ยนแปลงค่าของอุปกรณ์ต่าง ๆ โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๑๕) จัดให้มีการฝึกอบรมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น (simulated events) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและความรับผิดชอบของตนเมื่อต้องรับมือกับสถานการณ์ดังกล่าว (๑๖) สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์

ตารางที่ ๒.๒ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	(๑) จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น (๒) จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ (๓) จัดให้มีข้อพึงปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัย ด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (critical systems) โดยจะต้องจัดให้มีข้อพึงปฏิบัติที่สูงขึ้นสำหรับทุกระบบงานที่มีความสำคัญมากขึ้น (๔) วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่าย และ ระบบงาน (profile networks and systems) เป็นต้น เพื่อทำความเข้าใจพฤติกรรมการใช้งานในช่วงเวลาปกติ (normal behaviors) ทำการศึกษาวิจัยและค้นหา ความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (event correlation) (๕) ทันทีที่พบว่ามีหรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหา และ รวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์, ช่องโหว่ที่อาจถูกใช้ในการ โจมตี, สถานการณ์ของการโจมตี (อาทิ กำลังเกิดเหตุหรือสถานการณ์ได้สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการที่ได้รับผลกระทบ, โฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับผลกระทบ ข้อมูลผู้ใช้ เวลา ประทับข้อมูล payload ข้อมูลแจ้งเตือนจาก IDS (ถ้ามี) และข้อมูลจราจรทางคอมพิวเตอร์ (log) เป็นต้น โดยหน่วยงานจะต้องเก็บรักษาข้อมูลดังกล่าว (safeguard incident data) ให้มีความปลอดภัย เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำาเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ (๖) ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้น และติดตามเพื่อระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่าสถานการณ์ดังกล่าว จะสิ้นสุด โดยอาจพิจารณาจากข้อมูลตามที่ระบุในข้อ ๒ ของภาคผนวกแนบท้ายนี้ (๗) จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น (๘) ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทางไซเบอร์ รวมถึงจุดอ่อนของระบบที่ถูกโจมตี (๙) ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัย โดยคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูล เพื่อให้บุคคลดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (๑๐) รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญให้ผู้ที่เกี่ยวข้องทราบภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายนี้ แล้วแต่กรณี

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤต	ขร. ดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) จัดให้มีกลไกที่สามารถแจ้งเตือนได้ทันที (real-time alerts) เมื่อพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น (๒) จัดให้มีกลไกหรือระบบงานที่สามารถติดตามเหตุการณ์ และสามารถจัดเก็บและ วิเคราะห์ข้อมูลต่าง ๆ เพื่อตรวจจับการเกิดภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ (ถ้า ขร. มีความพร้อม) (๓) จัดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน เช่น แจ้งเตือนเมื่อหน่วยความจำที่ใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เหลือน้อย (storage capacity warning) เมื่อมีการใช้หน่วยประมวลผลกลาง (CPU) หรือมีการใช้หน่วยความจำหลัก (RAM) ของอุปกรณ์เครือข่ายหรือระบบงานหลักที่สูงผิดปกติ หรือ เมื่อมีการส่งข้อมูลออกนอกเครือข่ายมากผิดปกติ เป็นต้น (๔) วิเคราะห์ข้อมูลและค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่าง ๆ (information correlation) โดยอาจรับข้อมูลจากแหล่งข้อมูลอื่น ๆ นอกเหนือจากข้อมูลในระบบเพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ตารางที่ ๒.๓ การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง	(๑) ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้แนวทางดังกล่าวรวมถึง (๑.๑) การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่าย ภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในกระบวนการทาง นิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดีแล้ว เป็นต้น (๑.๒) การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและภายนอกหน่วยงาน เป็นต้น (๑.๓) การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด (๒) ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้ เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี (๓) ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุ หมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้ การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น (๔) ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้องตลอดจนผู้ที่อาจได้รับผลกระทบอย่างทันท่วงที โดยอาจขอความช่วยเหลือไปยังบุคคลหรือ หน่วยงานต่าง ๆ โดยเฉพาะการเกิดภัยคุกคามทางไซเบอร์ที่จัดอยู่ในหมวดหมู่ที่ ๑, ๒, ๔, ๕ และ ๗ ตามที่ระบุในข้อ ๑ ของภาคผนวกแนบท้ายนี้ทั้งนี้ ในการแจ้งหรือรายงานสถานการณ์นั้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	หน่วยงานควรเลือกใช้ช่องทางที่มีความเหมาะสมและปลอดภัย และดำเนินการแจ้งหรือรายงานเหตุภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับ ดูแลกำหนด หรืออาจเทียบเคียงจากตามที่ระบุในข้อ ๓ ของภาคผนวก แนบท้ายนี้ แล้วแต่กรณี (๕) ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่น การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ ไฟร์วอลล์) การติดตั้งลายเซ็นของ Anti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพในโครงสร้างพื้นฐานและดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ เป็นต้น (๖) ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติ ภายในกรอบระยะเวลาที่กำหนด (restore within time period) เช่น การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) การสร้างระบบงานขึ้นใหม่ (rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์ (install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) เป็นต้น (๗) สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการเฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	ให้หน่วยงานดำเนินการตามข้อ ๑ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) หากมีความจำเป็นให้หน่วยงานดำเนินการใช้ระบบงานสำรองสำหรับการประมวลผล (alternate processing) การจัดเก็บข้อมูล (storage site) และกู้คืนข้อมูลที่เกี่ยวข้องกับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (transaction recovery) (๒) ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือไปยังหน่วยงานที่เกี่ยวข้อง (supply chain coordination) รวมถึงแจ้งไปยัง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (๓) ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายใน หน่วยงาน ซึ่งครอบคลุมถึงรูปแบบ ระดับความลับ และเนื้อหาที่ต้องรายงาน ลำดับชั้นการรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือ ที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ(ถ้าหน่วยงานมีความพร้อม) (๔) ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติหน่วยงานควบคุมหรือกำกับดูแล พนักงาน เจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติหน้าที่ ตามกฎหมาย (๕) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติในการรับมือหรือสนับสนุนการรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (automated incident handling processes) (ถ้าหน่วยงานมีความพร้อม)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถ ให้บริการได้ภายในกรอบระยะเวลาที่กำหนด (restore within time period) โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและเครือข่ายของหน่วยงานทำได้อย่างรวดเร็ว

ตาราง ที่ ๒.๔ การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ	ภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ให้หน่วยงานพิจารณาดำเนินการดังนี้ (๑) นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้างพื้นฐานของบริการ นโยบายและกระบวนการ การฝึกบุคลากร การระบุผู้มีอำนาจดำเนินงานและเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง (๒) รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของภัยคุกคามทางไซเบอร์ ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และ วัตถุประสงค์ของการโจมตี เป็นต้น เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายใน หน่วยงาน (๓) ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสมและเป็นปัจจุบัน (๔) เก็บรักษาข้อมูลและหลักฐานที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือ ใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดีตามแนวทางและระยะเวลาการเก็บรักษา หลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่หน่วยงานได้กำหนด

ตารางที่ ๑ ลักษณะภัยคุกคามทางไซเบอร์แต่ละระดับและแนวทางการพิจารณาผลกระทบ

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๑.ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ดังนี้ (๑) ระบบคอมพิวเตอร์ของหน่วยงาน ขร. หรือ (๒) อุปกรณ์หรือระบบงานอื่นที่ใช้สำหรับการให้บริการของรัฐ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว ทำให้ระบบคอมพิวเตอร์ของ ขร. หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ถูกใช้สำหรับให้บริการหลัก ดังนี้ (๑) ระบบคอมพิวเตอร์ (๒) โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าว แสดงให้เห็นได้ว่าผู้โจมตีมีความมุ่งหมายที่จะทำให้โครงสร้างพื้นฐานสำคัญของประเทศเสียหายจนไม่สามารถทำงานหรือให้บริการได้	การประทุษร้ายต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่รุนแรงในลักษณะที่เป็นวงกว้างต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ทั้งนี้ ผลกระทบที่เกิดกับอุปกรณ์หรือระบบงานดังกล่าวทำให้ (๑) การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชน ล้มเหลวทั้งระบบจนรัฐไม่สามารถ ควบคุมการทำงานส่วนกลางของำระบบคอมพิวเตอร์ของรัฐได้ หรือ (๒) การใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคาม ไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ หรือระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	ไม่เจาะจงอุปกรณ์หรือระบบงานที่ได้รับผลกระทบ แต่เมื่อพิจารณาจากพฤติกรรมของผู้โจมตีหรือพฤติการณ์แวดล้อมแล้วมีเหตุอันควรเชื่อได้ว่าการก่อภัยคุกคามทางไซเบอร์นั้นกระทบ หรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๒. ลักษณะ ผลกระทบต่อข้อมูลในระบบ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้าย ต่อข้อมูล ซึ่งส่งผลกระทบทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลที่ใช้สำหรับระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศ ซึ่งส่งผลให้บริการหลักไม่สามารถทำงานหรือให้บริการได้	มีเหตุอันควรเชื่อได้ว่าผู้โจมตี มีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลอันมีลักษณะดังนี้ (๑) เป็นข้อมูลที่เกี่ยวข้องกับการทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชน หรือ (๒) เป็นข้อมูลที่เกี่ยวข้องกับชีวิตของ บุคคลจำนวนมาก หรือเป็นข้อมูลคอมพิวเตอร์จำนวนมากในระดับประเทศ	มีเหตุอันควรเชื่อได้ว่าผู้โจมตีมีความมุ่งหมายให้เกิดการประทุษร้ายต่อข้อมูลใด ๆ อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้าย ตามประมวลกฎหมายอาญา การรบ หรือการสงคราม
๓. แนวโน้มในการกู้คืนระบบ	สามารถกู้คืนระบบคอมพิวเตอร์ หรือ ทำให้บริการของรัฐกลับมาได้บางส่วน โดยสามารถดำเนินการได้ตามแผนการกู้คืน	ไม่สามารถกู้คืนระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศ ที่ใช้สำหรับให้บริการหลักได้ตามแผนการกู้คืน	ไม่สามารถกู้คืนการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของประเทศได้ตามแผนการกู้คืนทำให้ (๑) รัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ (๒) มีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของ ประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ	ไม่สามารถกู้คืนอุปกรณ์หรือระบบงานที่ได้รับผลกระทบได้ และจำเป็นต้องมีมาตรการเร่งด่วนในการกู้คืนอุปกรณ์หรือระบบงานที่เกี่ยวข้อง

ปัจจัยที่ใช้ในการประเมิน	ลักษณะภัยคุกคามทางไซเบอร์			
	ระดับไม่ร้ายแรง	ระดับร้ายแรง	ระดับวิกฤติ	
			กรณี (ก)	กรณี (ข)
๔. ลักษณะผลกระทบต่อลูกค้าหรือผู้ใช้บริการ	ส่งผลหรืออาจส่งผลกระทบต่อผู้ใช้บริการในวงจำกัด	อาจส่งผลกระทบต่อผู้ใช้บริการทั้งหมด	ส่งผลกระทบต่อผู้ใช้บริการทั้งหมด หรืออาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต	ส่งผลหรืออาจส่งผลกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม

ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

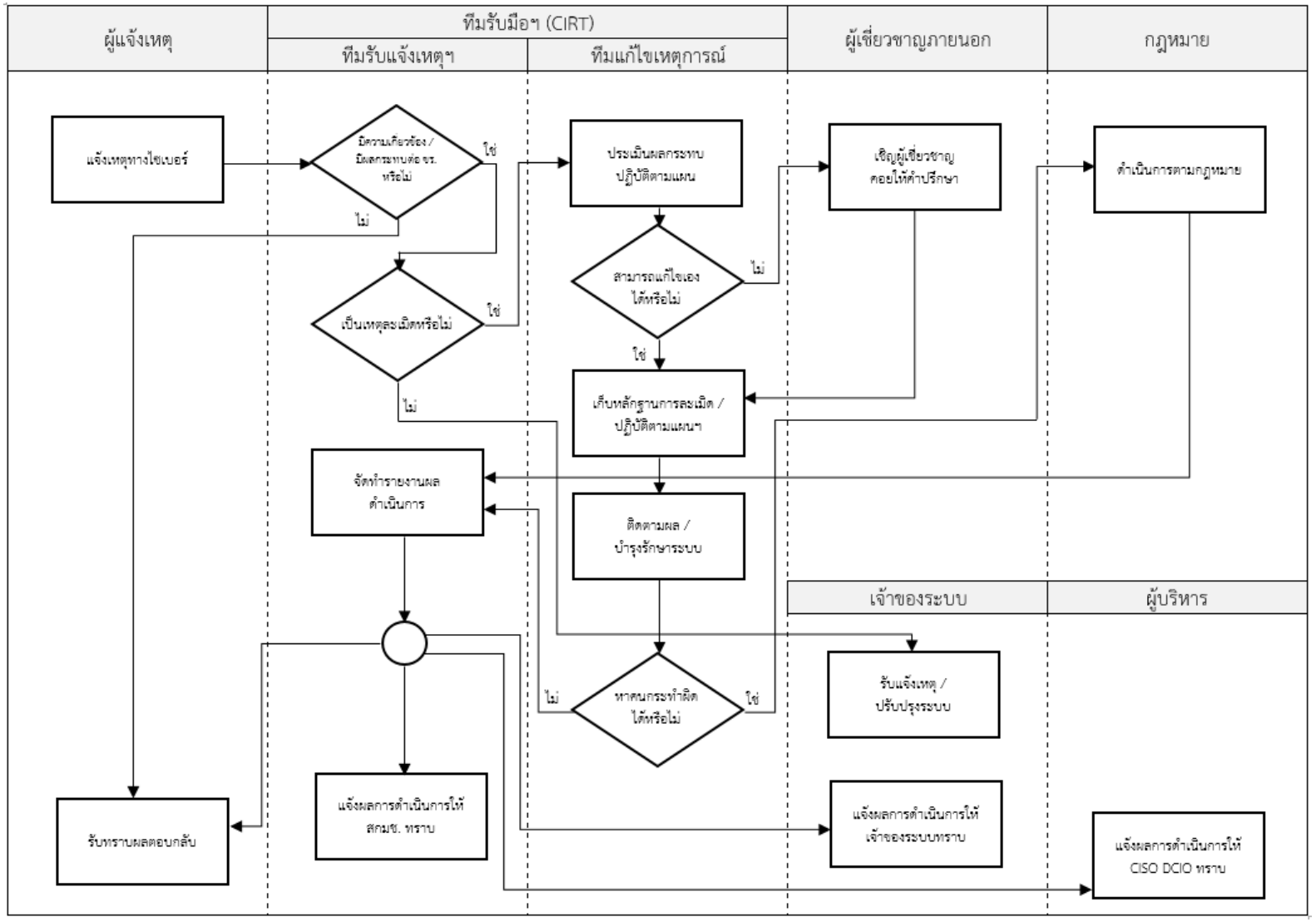
ข้อ ๒ ลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

หมวดหมู่ภัยคุกคาม							
ประเภทอุปกรณ์เครือข่าย	๑	๒	๓	๔	๕	๖	๗
Backbone	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เราเตอร์	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายสำหรับการจัดการเครือข่าย หรือ ดูแลความปลอดภัย	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง
เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง
เครื่องเวิร์กสเตชั่น	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง

ข้อ ๓ กำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	ทุกเหตุการณ์	๓๐ นาที	๔ ชั่วโมง
๒	ทุกเหตุการณ์	ตาม ขร. กำหนด	ตาม ขร. กำหนด
๓	ทุกเหตุการณ์	๓๐ นาที	๘ ชั่วโมง
๔	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๒ ชั่วโมง
	ไม่ร้ายแรง	ตาม ขร. กำหนด	ตาม ขร. กำหนด
๕	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๔ ชั่วโมง
๖	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๔ ชั่วโมง
๗	วิกฤต	๑๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๑๐ นาที	๑ ชั่วโมง
	ไม่ร้ายแรง	ตาม ขร. กำหนด	ตาม ขร. กำหนด
๘	-	๒๐ นาที	๔ ชั่วโมง
๙	-	-	๑๒ ชั่วโมง

แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)



เอกสารประกอบ

ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนองต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงานความคืบหน้าครั้งถัดไป :		

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง สถานการณ์ที่เกิดขึ้น การตัดสินใจ ผลกระทบ)
ตัวอย่าง ๑๒/๑/๖๖ – ๐๙.๐๐ น.	*ทีมรับมือฯ ตรวจสอบพบภัยคุกคามลักษณะ Phishing ทำให้เกิด Ransomware เข้าสู่ระบบเครือข่ายภายในหน่วยงาน*

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

๑. ข้อมูลการประสานงาน

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม

วันที่และเวลาที่แจ้ง

๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม

๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล ตำแหน่งงาน

ชื่อหน่วยงาน อีเมล

โทรศัพท์ (ที่ทำงาน / มือถือ)

๔. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

๕. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ในระดับใด (มาตรา ๖๐)

☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)

☐ ยังไม่สามารถระบุได้

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ **หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี):** โปรดระบุ **วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ
ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ
ก๓. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก๔. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม

ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ

☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม

☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว

☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ

ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว

☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว

☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว

☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ

ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

ส่วนที่ ๒

หมวด ง : รายละเอียดภัยคุกคาม

ง๑. ข้อมูลการตรวจจับและการวิเคราะห์

ง๑.๑ <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)

วันที่: เลือกวันที่ เวลา: โปรดระบุ ไม่ทราบ: ☐

ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร):

โปรดระบุ

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

๑๑.๔ <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:

โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ

☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ

☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ

☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)

☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ

☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ

☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย

☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง

☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก

☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย

☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ

☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ

☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)

☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ

☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น

☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ

☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)

☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

๑๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)

โปรดระบุ

๑๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

๑๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

๑๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

๑๒.๒ การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

๑๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

๑๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

๑๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

๑๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย	จำนวน
๐	เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)	
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

ทรัพย์สินที่ได้รับผลกระทบ	จำนวน
เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	
เครื่องเวิร์กสเตชัน (Workstation)	
สวิตซ์ (Switch) /เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์

ระดับภัยคุกคาม	จำนวน
ไม่ร้ายแรง	
ร้ายแรง	
วิกฤต (ก)	
วิกฤต (ข)	

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
๑	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
๑.๑	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
๑.๒	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
๑.๓	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
๑.๔	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
๒	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
๓	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
๕	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
๖	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
๗	ทำการกำจัดสาเหตุ (Eradicate the incident)	
๗.๑	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
๗.๒	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่น ๆ	
๗.๓	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
๘	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
๘.๑	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
๘.๒	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
๘.๓	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๙	จัดทำรายงานการติดตามผล	
๑๐	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	