นโยบายและแนวทางปฏิบัติ การรักษาความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Policy)

ศูนย์เทคโนโลยีสารสนเทศ กรมราชทัณฑ์

(ฉบับปรับปรุงปี พ.ศ. ๒๕๖๗)

นโยบายและแนวทางปฏิบัติ การรักษาความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Policy)

๑. หลักการและเหตุผล

สืบเนื่องจากประกาศกระทรวงยุติธรรม เรื่อง มาตราฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม พ.ศ. ๒๕๖๖ ลงวันที่ ๒๘ มีนาคม ๒๕๖๖ เพื่อให้การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมราชทัณฑ์เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมและกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยความมั่นคงปลอดภัยไซเบอร์โดยเร็วและเพื่อให้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของกรมราชทัณฑ์เกิดความชัดเจน เป็นไปในทิศทางเดียวกันและสอดคล้องกับมาตรฐานสากล

ศูนย์เทคโนโลยีสารสนเทศ ภายใต้กองยุทธศาสตร์และแผนงาน จึงได้จัดทำ “นโยบายและแนวทางปฏิบัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖-๒๕๗๐” ขึ้นเพื่อให้ภารกิจด้านระบบสารสนเทศและการสื่อสารของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถดำเนินงานได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัยป้องกันการถูกบุกรุกหรือถูกโจมตี ตลอดจนช่วยให้ระบบงานของหน่วยงานสามารถฟื้นฟูระบบอย่างรวดเร็วภายหลังจากภัยคุกคามได้สิ้นสุดลง

๒. วัตถุประสงค์

กรมราชทัณฑ์ ได้จัดทำ “นโยบายและแนวทางปฏิบัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ - ๒๕๗๐” โดยมีวัตถุประสงค์ดังนี้

๒.๑ เพื่อกำหนดนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามกฎระเบียบและแนวทางปฏิบัติที่ถูกต้อง

๒.๒ เพื่อสร้างความเชื่อมั่นด้านความมั่นคงปลอดภัยไซเบอร์ และดำเนินงานต่างๆ ภายในหน่วยงานเป็นไปอย่างมีประสิทธิภาพ ประสิทธิผลและเสถียรภาพ

๒.๓ เพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ผู้บริหาร ผู้ดูแลระบบ และผู้ใช้งานภายในหน่วยงาน รวมถึงการใช้งานจากบุคคลภายนอกในระบบที่เกี่ยวข้องตามที่ได้รับการอนุญาต ให้มีความรู้ ความเข้าใจ และมีความตระหนักถึงความสำคัญในนโยบายและแนวทางปฏิบัติพร้อมทั้งปฏิบัติตามนโยบายแนวทางปฏิบัตินี้อย่างเคร่งครัด

๓. องค์ประกอบและขอบเขตของนโยบาย

นโยบายและแนวทางปฏิบัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ - ๒๕๗๐ ของกรมราชทัณฑ์ จัดทำขึ้นเพื่อกำหนดแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยขอบเขตมีผลบังคับใช้นโยบายและแนวทางปฏิบัตินี้ครอบคลุมหน่วยงานและการให้บริการภายในทั้งหมดของกรมราชทัณฑ์ ตลอดจนรวมถึงหน่วยงานในเรือนจำ / ทัณฑสถานทั่วประเทศ

๔. คำนิยาม

ลำดับ	คำศัพท์	ความหมาย
๑	หน่วยงานหรือกรม	กรมราชทัณฑ์ รวมถึง เรือนจำ/ทัณฑสถานทั่วประเทศ
๒	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	หน่วยงานของกรมราชทัณฑ์ที่ประกาศ และมอบหมายหน้าที่ความรับผิดชอบให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมราชทัณฑ์
๓	ศท.	ศูนย์เทคโนโลยีสารสนเทศ ของกรมราชทัณฑ์
๔	ผู้ใช้งาน (User)	ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างตามสัญญาจ้างในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของกรมราชทัณฑ์
๕	สิทธิของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
๖	ผู้ดูแลระบบ (System Administrator)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบงาน
๗	สินทรัพย์	ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตน อันมีมูลค่า หรือคุณค่าสำหรับหน่วยงาน
๘	การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)	การอนุญาต การกำหนดสิทธิ หรือมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบสารสนเทศและระบบเครือข่าย
๙	ความมั่นคงปลอดภัยด้านสารสนเทศ	การธำรงไว้ซึ่งความลับ ความถูกต้อง ครบถ้วน และสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ
๑๐	เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)	กรณีระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์ อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
๑๑	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจ คาดคิดซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
๑๒	ระบบอินเทอร์เน็ต (Internet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล
๑๓	ระบบอินทราเน็ต (Intranet)	ระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และสารสนเทศภายในหน่วยงาน

ลำดับ	คำศัพท์	ความหมาย
๑๔	ระบบสารสนเทศ	ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่ หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น
๑๕	หน่วยงานภายนอก	องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึง และการใช้งานข้อมูล หรือทรัพย์สินต่างๆ ของหน่วยงานโดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล
๑๖	จดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-mail)	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงกันข้อมูลที่ส่ง จะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น
๑๗	สื่อบันทึกพกพา	สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Disk หรือ Floppy Disk เป็นต้น
๑๘	ชื่อผู้ใช้ (Username)	ชุดของตัวอักษร หรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์ และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้
๑๙	รหัสผ่าน (Password)	ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
๒๐	อุปกรณ์จัดเส้นทาง (Router)	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น
๒๑	การเข้ารหัส (Encryption)	การนาข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัส เพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
๒๒	การพิสูจน์ยืนยันตัวตน (Authentication)	ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการ พิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

ลำดับ	คำศัพท์	ความหมาย
๒๓	SSID (Service Set Identifier)	บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน
๒๔	WEP (Wired Equivalent Privacy)	ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้
๒๕	WPA (Wi-Fi Protected Access)	ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้ สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP
๒๖	MAC Address (Media Access Control Address)	หมายเลขเฉพาะที่ใช้อ้างอิงถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย โดยหมายเลขดังกล่าวมาพร้อมกับอีเทอร์เน็ตการ์ด ซึ่งแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกันตัวเลขจะอยู่ในรูปเลขฐาน ๑๖ มี ๖ คู่
๒๗	VPN (Virtual Private Network)	เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการ รับ-ส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่าย อินเทอร์เน็ตทาให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้น ไปจนถึงปลายทาง
๒๘	แผนผังระบบเครือข่าย (Network Diagram)	แผนผังซึ่งแสดงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน
๒๙	เครื่องแม่ข่าย (Server)	เครื่องหรือโปรแกรมคอมพิวเตอร์ซึ่งทำงานให้บริการในระบบเครือข่าย แก่ลูกข่าย
๓๐	อุปกรณ์กระจายสัญญาณข้อมูล (Switch)	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ - ส่งข้อมูล
๓๑	ไฟร์วอลล์(Firewall)	เทคโนโลยีป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์จากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย
๓๒	อุปกรณ์กระจายสัญญาณ แบบไร้สาย (Access Point)	อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย
๓๓	อัปเดต (Update)	ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ ทันสมัยอยู่เสมอ
๓๔	ไฟล์ที่สามารถประมวลผลได้ (Executable File)	ไฟล์โปรแกรมหรือชุดคำสั่งที่สามารถเรียกใช้งานได้ทันที เช่น ไฟล์ที่มี ชื่อสกุลเหล่านี้ .exe .com .bat .vbs .scr .pif .hta
๓๕	ช่องโหว่ (Vulnerability)	ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้ รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำ ให้มีการอาศัยข้อบกพร่องดังกล่าว เพื่อเข้าถึงข้อมูลโดยไม่ได้รับ อนุญาต

ลำดับ	คำศัพท์	ความหมาย
๓๖	ข้อมูลจราจรทาง คอมพิวเตอร์ (Log)	ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึง แหล่งกำหนด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลาและ ชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบ คอมพิวเตอร์
๓๗	IDS (Intrusion Detection System)	ระบบตรวจจับการบุกรุกเป็นเครื่องมือรักษาความปลอดภัยรองจาก ไฟร์วอลล์ใช้ในการตรวจจับความพยายามในการบุกรุกเครือข่าย และ เตือนภัยให้กับผู้ดูแลระบบได้รับทราบ
๓๘	IPS (Intrusion Prevention System)	ระบบตรวจจับการบุกรุกโดยจะทำงานคล้าย ๆ กับ IDS แต่จะมี คุณสมบัติพิเศษในการจู่โจมกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ ไม่จำเป็นต้องอาศัยโปรแกรมหรือ Hardware ตัวอื่น ๆ
๓๙	Configuration	การกำหนดคุณสมบัติของคอมพิวเตอร์ อุปกรณ์หรือโปรแกรมใด ๆ ที่จะนำมาใช้กับคอมพิวเตอร์เพื่อให้การทำงานมีประสิทธิภาพ เหมาะสมกับงานที่ต้องการ
๔๐	Wireless LAN Client	เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลนใช้คลื่นวิทยุในการ สื่อสารข้อมูลแทนการใช้สายสัญญาณ ซึ่งเครื่องคอมพิวเตอร์แต่ละ เครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ
๔๑	Recovery Time Objective (RTO)	ระยะเวลาในการกู้คืนระบบ
๔๒	Recovery Point Objective (RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
๔๓	Maximum Tolerance Period of Disruption (MTPD)	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่างๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
๔๔	Business Continuity Plan	แผนบริหารความต่อเนื่องทางธุรกิจ

๕. นโยบายอุปกรณ์แบบพกพา (Mobile device policy)

นโยบายและมาตรการสนับสนุนสำหรับการใช้งานอุปกรณ์แบบพกพาจะต้องมีการนำมาใช้งานเพื่อบริหารจัดการความเสี่ยงจากการใช้อุปกรณ์แบบพกพาโดยจะต้องดำเนินการ ดังนี้

๕.๑ อุปกรณ์สื่อสารประเภทพกพาจะต้องได้รับการอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศแล้วเท่านั้น จึงจะสามารถเข้าถึงข้อมูลสารสนเทศของกรมราชทัณฑ์ได้

๕.๒ อุปกรณ์สื่อสารประเภทพกพาจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตามแนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

๕.๓ ไม่ควรเก็บข้อมูลสำคัญของ กรมราชทัณฑ์ ไว้บนอุปกรณ์สื่อสารประเภทพกพาแต่ถ้ามีความจำเป็น ที่ต้องจัดเก็บบนอุปกรณ์สื่อสารประเภทพกพาจะต้องมีการเข้ารหัสข้อมูลตามแนวทางการ เข้ารหัสของกรมราชทัณฑ์

๕.๔ ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

๕.๕ ข้อมูลที่มีชั้นความลับซึ่งถูกจัดเก็บไว้บนอุปกรณ์สื่อสารประเภทพกพาหรือถูกส่งผ่านเครือข่าย ไร้สายที่ต้องส่งออกไปนอก กรมราชทัณฑ์ ต้องได้รับการอนุมัติจากเจ้าของข้อมูลและเข้ารหัสข้อมูล ก่อนเท่านั้น ไม่ควรเคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาต เป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและจะต้องกำหนดให้มีการทำลายเมื่อไม่มีการ ใช้งานแล้ว

๕.๖ ระบบคอมพิวเตอร์อื่นที่ต้องการเชื่อมต่อกับระบบของ กรมราชทัณฑ์ จะต้องได้รับการอนุมัติเป็น ลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศ

๕.๗ ต้องมีการรักษาความปลอดภัยทางกายภาพร่วมด้วย เช่น จะต้องปิดห้องทำงานเมื่อไม่มีบุคคล ที่ได้รับอนุญาตอยู่ประจำโต๊ะทำงานและชั้นเก็บเอกสารต่าง ๆ จะต้องล็อกอย่างดี

๕.๘ กรณีที่อุปกรณ์สื่อสารประเภทพกพาเป็นสมบัติของกรมราชทัณฑ์ การคืนเครื่องหรือส่งซ่อม ให้ผู้ใช้งานทำสำเนาข้อมูลจากอุปกรณ์สื่อสารประเภทพกพาเก็บไว้ทั้งหมดและลบข้อมูล ทั้งหมดที่มีอยู่บนอุปกรณ์สื่อสารประเภทพกพาก่อนส่งซ่อม

๕.๙ อุปกรณ์สื่อสารประเภทพกพา เช่น เครื่องคอมพิวเตอร์แบบพกพา (Notebook) หรือ Smart Device ควรมีกระบวนการเพื่ออัปเดตระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์ตามแนว ปฏิบัติการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ของกรมราชทัณฑ์

๕.๑๐ การเข้าถึงและใช้ข้อมูลสารสนเทศ ซึ่งรวมถึงชั้นความลับของผู้ใช้งานเป็นอันสิ้นสุดลงทันที เมื่อผู้ใช้งานพ้นสภาพตามสิทธิ์ของผู้ใช้งาน

๕.๑๑ กรมราชทัณฑ์ อาจดำเนินการทางวินัย แพ่ง หรืออาญา กับผู้ที่ล่วงละเมิดการเข้าถึงล่วงละเมิดใช้งาน หรือล่วงละเมิดเผยแพร่ข้อมูลสารสนเทศที่เป็นความลับโดยที่ผู้นั้นไม่มีสิทธิ์อันชอบ

๖. นโยบายการปฏิบัติงานจากระยะไกล (Teleworking Policy)

นโยบายและมาตรการสนับสนุนสำหรับการปฏิบัติงานจากภายนอกต้องมีการนำมาใช้งานเพื่อป้องกัน ข้อมูลที่มีการเข้าถึงการประมวลผลหรือการจัดเก็บจากกรมราชทัณฑ์ โดยจะต้องดำเนินการดังนี้

๖.๑ ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอกกรมราชทัณฑ์ หน่วยงานที่รับผิดชอบต้อง ปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยระบบสารสนเทศสำหรับ

หน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิ์ที่ได้รับและมีการตรวจสอบการใช้งาน อย่างสม่ำเสมอ

๖.๒ ไม่อนุญาตให้ใช้งาน Remote Access สำหรับการปฏิบัติงานภายใต้ขอบเขตการดำเนินงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เว้นแต่กรณีเกิดเหตุฉุกเฉินหรือเกิดเหตุการณ์ภัยพิบัติที่มีความจำเป็นต้องให้มีการปฏิบัติงานจากภายนอกเท่านั้น กรณีที่ต้องมี การเชื่อมต่อ Remote Access เพื่อปฏิบัติงานจากภายนอกต้องได้รับการอนุมัติการเชื่อมต่อ ผ่านระบบ Virtual Private Network (VPN) ของกรมราชทัณฑ์ เท่านั้น

๖.๓ การเข้าสู่ข้อมูลของกรมราชทัณฑ์ จากระยะไกลได้นั้นต้องได้รับการอนุมัติจากหน่วยงานที่ดูแล รับผิดชอบด้านเครือข่ายระบบสารสนเทศก่อนและผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติฯ ที่เกี่ยวข้องกับการเข้าสู่ระบบและข้อมูลของกรมราชทัณฑ์ จากระยะไกล นอกจากนี้เจ้าของข้อมูล มีหน้าที่ดูแลรักษาและเปลี่ยนแปลงรายชื่อของผู้ใช้งานที่สามารถเข้าสู่ระบบจากระยะไกลให้ ถูกต้องและเหมาะสมเพื่อให้หน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศ ตรวจสอบความถูกต้องได้

๖.๔ ต้องมีการกำหนดวิธีการพิสูจน์ตัวตน

๖.๕ ก่อนจะกำหนดสิทธิ์ของผู้ใช้งานในการเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐานระบุ เหตุผลหรือความจำเป็นอย่างเพียงพอ และต้องได้รับอนุมัติจากหน่วยงานที่เป็นเจ้าของข้อมูลอย่างเป็นทางการเท่านั้น

๖.๖ ต้องควบคุม Port ที่ใช้ในการเข้าสู่ระบบโดยการโทรเข้า / โทรออก (Dial-in / Dial-out) อย่างรัดกุม (ถ้ามี) ผู้ใช้งานที่มีความจำเป็นที่จะต้องใช้สาย Analog ในการเข้าสู่ระบบโดยวิธีการโทรเข้า / โทรออก ต้องได้รับการอนุมัติจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศ นอกจากนี้ สายที่ใช้ในการโทรออกต้องถูกตั้งค่าให้สามารถโทรออกได้เท่านั้น (ถ้าทำได้) การเข้าสู่ระบบโดยการโทรเข้านั้นต้องมีการดูแลและการจัดการโดยผู้ดูแลระบบ และวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๖.๗ ห้ามนำซอฟต์แวร์การควบคุมจากระยะไกล เช่น PC-Anywhere หรือ Carbon copy มาใช้กับคอมพิวเตอร์ของกรมราชทัณฑ์ การใช้ซอฟต์แวร์ที่ไม่เหมาะสมดังกล่าวสามารถเป็นช่องทางให้ผู้ที่ไม่ประสงค์ดีเข้ามายังเครือข่ายของกรมราชทัณฑ์

๗. นโยบายการควบคุมการเข้าถึง (Access control policy)

๗.๑ ความต้องการการให้บริการสำหรับการควบคุมการเข้าถึง

๗.๑.๑ นโยบายควบคุมการเข้าถึง (Access control policy) นโยบายควบคุมการเข้าถึงต้องมีการดำเนินการดังนี้

๑) กำหนดให้มีการควบคุมการเผยแพร่ข้อมูลและการให้สิทธิ์ เช่น หลักการความจำเป็นที่ต้องรู้ (Need to know), ระดับของความปลอดภัยและการจัดระดับชั้น การเข้าถึงข้อมูล

๒) ควบคุมการจัดการสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญทุกระบบ

๓) การแบ่งแยกการควบคุมการเข้าถึง เช่น การร้องขอเข้าถึงการให้สิทธิ์การเข้าถึง การบริหารการเข้าถึง

๔) ต้องมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้งทุกระบบสารสนเทศที่มีความสำคัญ

๕) ต้องถอดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศเมื่อบุคลากรพ้นสภาพ โยกย้าย เปลี่ยนผู้รับผิดชอบ หรือมีการปรับเปลี่ยนอย่างมีนัยสำคัญ

๖) ควบคุมการกำหนดหน้าที่ของผู้มีสิทธิ์เข้าถึงด้วยสิทธิพิเศษ และมีการตรวจสอบหรือทบทวนการใช้งานสิทธิ์พิเศษอย่างสม่ำเสมอหรืออย่างน้อยปีละ ๑ ครั้ง

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

๑) การกำหนดเครือข่าย และบริการเครือข่ายที่อนุญาตให้เข้าถึง

๒) ขั้นตอนให้สิทธิ์ที่อนุญาตให้เข้าถึงเครือข่าย และบริการเครือข่าย

๓) การควบคุมการจัดการ และขั้นตอนเพื่อป้องกันการเชื่อมต่อเครือข่าย และบริการ เครือข่าย

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

๕) ระบบเครือข่ายที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอก ต้องมีการใช้อุปกรณ์หรือซอฟต์แวร์ในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์ อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

๗.๒ การบริหารจัดการการเข้าถึงด้านระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

๗.๒.๑ การลงทะเบียนและถอดถอนผู้ใช้งาน (User registration and deregistration) ขั้นตอนการจัดการรหัสผู้ใช้งานจะต้องดำเนินการดังต่อไปนี้

๑) ต้องใช้รหัสผู้ใช้งานที่ไม่ซ้ำกันเพื่อให้ผู้ใช้งานรับผิดชอบสำหรับการดำเนินการของตน

๒) ยกเลิกการใช้งาน หรือถอดถอนรหัสผู้ใช้งานของคนที่ลาออก โยกย้าย หรือเปลี่ยนแปลงความรับผิดชอบอย่างทันท่วงทีในวันที่มีผลหรือก่อนวันที่มีผล หากไม่มีความจำเป็นต้องใช้งานแล้ว

๓) ควรกำหนดรอบในการยกเลิกการใช้งานหรือถอดถอนรหัสผู้ใช้งาน

๔) ควรมีการกำหนดให้มีการทบทวนรหัสผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๕) กำหนดให้มีการตรวจสอบ กรณีรหัสผู้ใช้งานแต่ไม่มีการใช้งานนานมากกว่า ๙๐ วันให้ดำเนินการระงับรหัสผู้ใช้งานชั่วคราวทันที จนกว่าผู้ใช้งานจะร้องขอ และหากหลังจากระงับรหัสผู้ใช้งานชั่วคราวแล้วจนครบ ๓๐ วัน ถ้ายังไม่มีการร้องขอจากผู้ใช้งานให้ดำเนินการอีกให้ลบชื่อ-รหัสผู้ใช้งานนั้นถาวรทันที และผู้ดูแลระบบสารสนเทศต้องทำการเก็บบันทึกข้อมูลผู้ใช้งานดังกล่าวไว้ด้วย เพื่อตรวจสอบระบบว่ามีผลกระทบเสียหายเกิดขึ้นหรือไม่

๗.๒.๒ การจัดเตรียมการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน (User access provisioning) ขั้นตอนการจัดเตรียมการเข้าถึงของผู้ใช้งานจะต้องดำเนินการดังนี้

๑) ได้รับสิทธิ์จากเจ้าของระบบเทคโนโลยีสารสนเทศ ก่อน จึงจะสามารถใช้งานในระบบได้

๒) ต้องตรวจสอบว่าระดับของการเข้าถึงที่ได้รับเหมาะสมกับนโยบายการเข้าถึงและสอดคล้องกับข้อกำหนดอื่น เช่น การแบ่งแยกหน้าที่ (Segregation of duties)

๓) ต้องมั่นใจว่าสิทธิ์การเข้าถึงไม่ได้ถูกเปิดใช้งานก่อนที่ขั้นตอนการให้สิทธิ์จะเสร็จสมบูรณ์

๔) การบันทึกที่ส่วนกลางของการให้สิทธิ์การเข้าถึงสำหรับรหัสผู้ใช้งานที่เข้าถึงระบบสารสนเทศและบริการ

๕) ปรับเปลี่ยนสิทธิ์การเข้าถึงของผู้ใช้งานที่เปลี่ยนหน้าที่ หรืองานที่รับผิดชอบ และถอดถอนสิทธิ์การเข้าถึงของผู้ใช้งานทันทีที่ลาออกหรือโยกย้าย

๖) มีการทบทวนสิทธิ์การเข้าถึงตามรอบกับเจ้าของระบบสารสนเทศหรือบริการหรืออย่างน้อยปีละ ๑ ครั้ง

๗.๒.๓ การบริหารจัดการสิทธิ์การเข้าถึงตามระดับพิเศษ (Management of Privileged Access Rights) ขั้นตอนการบริหารจัดการสิทธิ์การเข้าถึงตามระดับพิเศษ จะต้องดำเนินการดังนี้

๑) การกำหนดสิทธิ์การเข้าถึงระดับพิเศษของระบบปฏิบัติการ ระบบการจัดการฐานข้อมูล และแอปพลิเคชัน ต้องได้รับการควบคุมเป็นพิเศษ และระบุตัวตนของผู้ที่ใช้งานด้วย

๒) สิทธิ์การเข้าถึงระดับพิเศษควรจัดสรรให้กับผู้ใช้งานตามความจำเป็นในการใช้งาน

๓) การให้สิทธิ์และบันทึกของการแจกจ่ายสิทธิ์การเข้าถึงระดับพิเศษทั้งหมดต้องได้รับการควบคุมการใช้งาน

๔) กำหนดระยะเวลาในการใช้งานสิทธิ์การเข้าถึงระดับพิเศษ

๕) สิทธิ์การเข้าถึงระดับพิเศษควรถูกกำหนดให้กับผู้ใช้งานสำหรับงานที่เกี่ยวข้องกับระบบเท่านั้น และการทำงานทั่วไปควรดำเนินการด้วยรหัสผู้ใช้งานที่มีสิทธิ์ในระดับปกติ

๖) การใช้งานด้วยสิทธิ์การเข้าถึงระดับพิเศษควรทบทวนอย่างสม่ำเสมอเพื่อตรวจสอบว่าได้มีการใช้งานที่เหมาะสมตรงตามวัตถุประสงค์ของการใช้งาน

๗) กำหนดให้มีการทบทวนสิทธิ์พิเศษอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง

๗.๒.๔ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of Users) ขั้นตอนการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งานต้องดำเนินการดังนี้

๑) ผู้ใช้งานควรลงนามในรายงานเพื่อเก็บข้อมูลความลับสำหรับการพิสูจน์โดยการ ลงนามให้รวมข้อกำหนด และเงื่อนไขของของการจ้างงานด้วย

๒) เมื่อผู้ใช้งานต้องการจัดเก็บข้อมูลความลับสำหรับการพิสูจน์ตัวตนของตนเอง ผู้ใช้งานควรได้รับข้อมูลความลับสำหรับการพิสูจน์ตัวตนชั่วคราวที่ปลอดภัย ในขั้นต้น ซึ่งผู้ใช้งานจะถูกบังคับให้เปลี่ยนเมื่อใช้งานในครั้งแรก

๓) ควรมีการกำหนดขั้นตอนเพื่อตรวจสอบตัวตนของผู้ใช้งานก่อนที่จะให้ข้อมูล ความลับสำหรับการพิสูจน์ตัวตนที่ขอใหม่ ทดแทน หรือชั่วคราว

๔) ข้อมูลความลับสำหรับการพิสูจน์ตัวตนชั่วคราวควรมอบให้แก่ผู้ใช้งานในลักษณะที่ปลอดภัย ไม่อนุญาตให้ใช้บุคคลภายนอกส่ง หรือข้อความผ่านมือถือ หรืออีเมลที่ไม่มีการป้องกัน

๕) ข้อมูลความลับสำหรับการพิสูจน์ตัวตนชั่วคราวต้องเป็นข้อมูลเฉพาะบุคคล และรหัสผ่านต้องไม่คาดเดาได้ง่าย

๖) ข้อมูลความลับสำหรับการพิสูจน์ตัวตนของเจ้าของผลิตภัณฑ์ที่เป็นค่าเริ่มต้นต้องถูกปรับเปลี่ยนหลังจากการติดตั้งระบบหรือซอฟต์แวร์เรียบร้อยแล้วอย่างทันท่วงที

๗.๒.๕ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ขั้นตอนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานจะต้องดำเนินการ ดังนี้

๑) สิทธิ์การเข้าถึงของผู้ใช้งานต้องได้รับการทบทวนตามรอบที่ได้กำหนดไว้อย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง และหลังจากการเปลี่ยนแปลง เช่น การเลื่อนตำแหน่ง การลดตำแหน่ง การลาออก การโยกย้าย การเปลี่ยนความรับผิดชอบ

๒) สิทธิ์การเข้าถึงของผู้ใช้งานควรได้รับการทบทวนและปรับเปลี่ยนเมื่อมีการย้ายตำแหน่งภายในกรมราชทัณฑ์

๓) สิทธิ์การเข้าถึงระดับพิเศษควรได้รับการทบทวนตามรอบที่ได้กำหนดไว้อย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง และหลังจากการเปลี่ยนแปลง เช่น การเลื่อนตำแหน่ง การลดตำแหน่ง การลาออก การโยกย้าย การเปลี่ยน ความรับผิดชอบ

๔) การได้รับสิทธิ์ระดับพิเศษควรมีการตรวจสอบเป็นประจำเพื่อให้มั่นใจว่าไม่มีผู้ใช้งานที่ไม่ได้รับอนุญาตได้รับสิทธิ์ระดับพิเศษ

๕) การเปลี่ยนแปลงบัญชีผู้ในงานระดับพิเศษต้องได้รับการบันทึกและมีการทบทวนตามรอบการเปลี่ยนแปลง

๗.๒.๖ การถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงของผู้ใช้งาน (Removal or Adjustment of Access Right) ขั้นตอนการถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงของผู้ใช้งานจะต้องดำเนินการดังนี้

๑) เมื่อสิ้นสุดการจ้างงานต้องมีการถอน หรือระงับสิทธิ์การเข้าถึงของผู้ใช้งานที่ เกี่ยวข้องกับข้อมูลและทรัพย์สิน

๒) สิทธิ์การเข้าถึงต้องถูกถอนออก หรือ ปรับเปลี่ยนทั้งทางกายภาพ และลอจิคัล

๓) เอกสารใด ๆ ที่ระบุสิทธิ์การเข้าถึงของเจ้าหน้าที่และบุคคลภายนอกจะต้องถูกถอนออกหรือปรับเปลี่ยน ทันทีที่ลาออก หรือ หมดสัญญาจ้าง ในกรณีที่ผู้ใช้งานเป็นบุคคลภายนอกและทราบรหัสผ่านสำหรับบัญชีผู้ใช้งานที่ยังใช้งานอยู่ ต้องเปลี่ยนรหัสผ่านทันทีที่สิ้นสุดการจ้างงาน หรือหมดสัญญา

๗.๓ ความรับผิดชอบของผู้ใช้งาน

๗.๓.๑ การใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตน (Use of Secret Authentication Information) ขั้นตอนการใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตนจะต้องดำเนินการดังนี้

๑) ผู้ใช้งานต้องจัดเก็บข้อมูลความลับสำหรับการพิสูจน์ตัวตนไว้เป็นความลับ ต้องมั่นใจว่าไม่ได้เปิดเผยข้อมูลดังกล่าวต่อคนอื่น

๒) หลีกเลี่ยงการการเก็บบันทึกข้อมูลความลับสำหรับการพิสูจน์ตัวตน (เช่น กระดาษ ซอฟต์แวร์ หรือ อุปกรณ์มือถือ ยกเว้นจะสามารถจัดเก็บได้อย่างปลอดภัยและวิธีการจัดเก็บได้รับการอนุมัติแล้ว (เช่น ตู้ล็อกอย่างแน่นหนา ห้องนิรภัย)

๓) เปลี่ยนข้อมูลความลับสำหรับการพิสูจน์ตัวตน เมื่อมีข้อบ่งชี้ว่ามีภัยคุกคาม

๔) เมื่อรหัสผ่านถูกใช้เป็นข้อมูลความลับสำหรับการพิสูจน์ตัวตน ให้เลือกรหัสผ่านที่มีคุณภาพตามข้อ ๗.๔.๓

๕) ต้องมั่นใจว่ามีการป้องกันรหัสผ่านอย่างเหมาะสมเมื่อใช้รหัสผ่านเป็นข้อมูลความลับสำหรับการพิสูจน์ตัวตนในขั้นตอนการเข้าสู่ระบบแบบอัตโนมัติและในขั้นตอนการจัดเก็บ

๗.๔ การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน

๗.๔.๑ ข้อกำหนดการเข้าถึงสารสนเทศ (Information Access Restriction) ขั้นตอนสำหรับข้อกำหนดการเข้าถึงสารสนเทศจะต้องดำเนินการดังนี้

๑) ต้องมีการจัดเตรียมหน้าจอหรือเมนูสำหรับควบคุมการเข้าถึงระบบ

๒) ควบคุมสิทธิ์การเข้าถึงของผู้ใช้งาน เช่น อ่าน, เขียน และลบเป็นต้น

๓) ควบคุมสิทธิ์การเข้าถึงของแอปพลิเคชันไม่ควรมีใครได้สิทธิ์กระทำใดๆ ได้ทั้งหมดในระบบ

๔) จัดเตรียมสิทธิ์การเข้าถึงทางกายภาพ และลอจิคัลสำหรับระบบและแอปพลิเคชันที่สำคัญๆ

๗.๔.๒ ขั้นตอนในการเข้าสู่ระบบอย่างปลอดภัย (Secure log-on procedure) ขั้นตอนในการเข้าสู่ระบบอย่างปลอดภัยจะต้องดำเนินการ ดังนี้

๑) ไม่แสดงข้อมูล เช่น ชื่อ, รุ่น, ไอพีแอดเดรสของระบบ หรือแอปพลิเคชันจนกว่าจะมีการเข้าสู่ระบบจนกว่าจะเสร็จสิ้นสมบูรณ์

๒) ต้องไม่แสดงข้อความเพิ่มเติมระหว่างเข้าสู่ระบบซึ่งอาจช่วยให้ผู้ที่ไม่ได้รับอนุญาตเข้าสู่ระบบได้

๓) ตรวจสอบความถูกต้องของข้อมูลนำเข้าเฉพาะเมื่อการเข้าสู่ระบบเสร็จสิ้นสมบูรณ์แล้ว ถ้ามีความผิดพลาดระบบไม่ควรแสดงว่าข้อมูลนำเข้าส่วนไหนไม่ถูกต้อง

๔) จำกัดจำนวนครั้งของการพยายามเข้าสู่ระบบ เช่น ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง และหลังการเข้าสู่ระบบผิดพลาดให้บังคับระยะเวลาทิ้งช่วง เช่น ๑๕ นาที ก่อนที่จะยอมให้เข้าสู่ระบบอีกครั้งขึ้นอยู่กับระบบสารสนเทศที่มีความสำคัญต่อการให้บริการ

๕) ตัดการใช้งานของผู้ใช้งานที่ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่ง เช่น ๓๐ นาที โดยเฉพาะในพื้นที่ที่ความเสี่ยงสูง เช่น เครือข่ายสาธารณะหรือเครือข่ายภายนอกของกรมราชทัณฑ์ หรือบนอุปกรณ์เคลื่อนที่

๗.๔.๓ ระบบบริหารจัดการรหัสผ่าน (Password Management System) ขั้นตอนในการเข้าสู่ระบบอย่างปลอดภัยจะต้องดำเนินการดังนี้

๑) บังคับการใช้รหัสผู้ใช้งาน และรหัสผ่านให้ใช้งานสำหรับแต่ละบุคคลเท่านั้น

๒) บังคับใช้รหัสผ่านที่มีคุณภาพ โดยมีรายละเอียดดังนี้

๒.๑) ต้องมีความยาวมากกว่าหรือเท่ากับ ๘ ตัวอักษร เป็นอย่างน้อย

๒.๒) ต้องมีส่วนประกอบของอักษรตัวเล็ก ตัวใหญ่ อักขระพิเศษ และตัวเลข ประกอบกัน

๒.๓) บังคับผู้ใช้งานให้เปลี่ยนรหัสผ่านในการเข้าสู่ระบบครั้งแรก

๒.๔) บังคับให้เปลี่ยนรหัสผ่านตามรอบ เช่น ทุก ๖๐ วัน, ทุก ๙๐ วัน เป็นต้น

๒.๕) ไม่แสดงรหัสผ่านบนหน้าจอที่ผู้ใช้งานกำลังป้อนข้อมูล

๒.๗) จัดเก็บไฟล์รหัสผ่านแยกจากข้อมูลทั่วไปของแอปพลิเคชัน

๒.๘) รหัสผ่านต้องไม่ง่ายต่อการคาดเดา เช่น ไม่ตั้งรหัสผ่าน ๑๒๓๔ abcd

๒.๙) ต้องไม่บันทึกรหัสผ่านในระบบความจำของโปรแกรม

๗.๔.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs) ขั้นตอนในการใช้งานโปรแกรมอรรถประโยชน์จะต้องดำเนินการ ดังนี้

๑) ใช้โปรแกรมอรรถประโยชน์ต้องมีการระบุตัวตนพิสูจน์ตัวตนและการควบคุมสิทธิ์ของผู้ใช้งาน

๒) จำกัดการใช้งานของโปรแกรมอรรถประโยชน์ตามขั้นต่ำที่ต้องใช้งานสำหรับผู้ใช้งานที่ได้รับอนุญาตให้ใช้งาน

๓) การขอใช้งานโปรแกรมอรรถประโยชน์แบบเฉพาะกิจ (ad hoc) ต้องได้รับการอนุมัติจากศูนย์เทคโนโลยีสารสนเทศก่อนทุกครั้ง

๔) ต้องมีการจำกัดสิทธิ์ในการใช้งานโปรแกรมอรรถประโยชน์ตามความจำเป็นและเหมาะสม

๕) ต้องมีการบันทึกประวัติการใช้งานของโปรแกรมอรรถประโยชน์

๖) ต้องจัดทำเอกสารระดับการให้สิทธิ์ในการเข้าถึงโปรแกรมอรรถประโยชน์

๗) ต้องดำเนินการยกเลิกโปรแกรมอรรถประโยชน์ที่ไม่ได้ใช้งานหรือไม่จำเป็น

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

๑) ต้องไม่เก็บ Source Code Library ไว้บนระบบที่ใช้งานจริง (Production System)

๒) การเข้าถึง Source code ต้องจำกัดสิทธิ์ให้เฉพาะผู้ใช้งานที่จำเป็นเช่น โปรแกรมเมอร์ หรือผู้มีสิทธิ์เฉพาะหน้าที่ที่ได้รับมอบหมายเท่านั้น

๓) ระหว่างการทดสอบต้องไม่เก็บ Source code ที่ใช้ทดสอบร่วมกับที่ใช้งานจริง

๔) ต้องจัดเก็บ Source code ในสภาพแวดล้อมที่ปลอดภัย

๕) ต้องมีการบันทึกประวัติการเข้าถึง Source code

๖) การเปลี่ยนแปลงหรือแก้ไข Source code ต้องได้รับการอนุมัติจากศูนย์เทคโนโลยีสารสนเทศก่อนเสมอ

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

๘.๑ การใช้มาตรการเข้ารหัสข้อมูลจะต้องดำเนินการ ดังนี้

๘.๑.๑ กำหนดวิธีการเข้ารหัสข้อมูลตามมาตรฐานสากล

๘.๑.๒ อัลกอริทึมที่ใช้ในการเข้ารหัสต้องมีความปลอดภัย

๑) การเข้ารหัสแบบสมมาตรควรกำหนดให้ใช้อัลกอริทึมที่มีความปลอดภัย เช่น AES-๑๒๘, AES-๒๕๖

๒) การเข้ารหัสแบบอสมมาตรควรกำหนดให้ใช้อัลกอริทึมที่มีความปลอดภัย เช่น RSA๒๐๔๘

๓) ฟังก์ชันแฮช (hash function) ควรกำหนดให้ใช้อัลกอริทึมที่มีความปลอดภัย เช่น ECDSA-๒๕๖, SHA-๒๕๖, SHA-๓๘๔, SHA-๕๑๒

๘.๑.๓ โปรโตคอลที่ใช้สื่อสารต้องมีความปลอดภัย

๑) การใช้งานผ่านเว็บ HTTPS ควรใช้งานโปรโตคอล SSL/TLS ที่เป็น TLS ๑.๒, ๑.๓ ขึ้นไป หรือตามมาตรฐานสากล ณ ช่วงเวลานั้น

๒) การรับ-ส่งข้อมูลควรใช้งานโปรโตคอลที่ปลอดภัย เช่น SSH File Transfer Protocol (SFTP), File Transfer Protocol SSL/TLS (FTPS), Secure Shell (SSH), Remote Desktop Connection (RDP)

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

๔) การใช้งานข้อความหรือจดหมายอิเล็กทรอนิกส์ควรใช้งานโปรโตคอลที่ปลอดภัย เช่น Secure/Multipurpose Internet Mail Extensions (S/MIME), Pretty Good Privacy (PGP)

๕) ต้องมีการทบทวนมาตรฐานของการเข้ารหัสในทุกๆ ปีเพื่อให้สอดคล้องกับความปลอดภัย ตามมาตรฐานสากล ณ ช่วงเวลานั้น

๙. นโยบายการบริหารจัดการกุญแจ (Key Management Policy)

๙.๑ การบริหารจัดการกุญแจจะต้องดำเนินการดังนี้

๙.๑.๑ ข้อมูลที่ถูกเข้ารหัสต้องมีกระบวนการในการบริหารจัดการกุญแจอย่างมีประสิทธิภาพ โดยดำเนินการในขั้นตอนที่เกี่ยวข้องกับกุญแจทุกประเภท เช่น การสร้าง การจัดเก็บ การจัดส่ง การสำรอง การแจกจ่าย และการทำลาย ซึ่งต้องมีการควบคุมอย่างเหมาะสมและปลอดภัย

๙.๙.๒ กุญแจลับ หรือ กุญแจส่วนตัวที่ใช้สำหรับการเข้ารหัสจะต้องถูกจัดเก็บไว้เป็นความลับและมีความปลอดภัยเสมอ

๑๐. นโยบายการควบคุมการเข้าถึงทางกายภาพ (Physical Control Policy)

๑๐.๑ การกำหนดความปลอดภัยของพื้นที่

๑๐.๑.๑ พื้นที่ใช้งานระบบสารสนเทศ (Physical Security Perimeter)

๑) ต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศเพื่อการเฝ้าระวังควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๒) ต้องกำหนดการติดตั้งอุปกรณ์ในพื้นที่ใช้งานระบบสารสนเทศให้สอดคล้องกับความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

๓) หน่วยงานที่รับผิดชอบอุปกรณ์ที่สำคัญของระบบสารสนเทศ ต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย เช่น กล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถ ป้องกันภัยคุกคามจากผู้บุกรุก ในพื้นที่ใช้งานระบบ สารสนเทศ ได้แก่ ศูนย์ปฏิบัติการ SOC ห้อง Server/Data Center ห้อง Network Control หรือห้อง Network Center ห้องเก็บข้อมูลสำรองเพื่อให้ เป็นไปตามมาตรฐานสากลที่กำหนดไว้

๔) ไม่อนุญาตให้ถ่ายภาพบันทึกวิดีโอหรือเสียงภายในบริเวณที่ต้องมีความมั่นคงปลอดภัย ด้านสารสนเทศ (Secure Areas) เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

๑๐.๑.๒ การควบคุมการ เข้า-ออก (Physical entry controls)

๑) ระบุตัวตนผู้ใช้งานและช่วงเวลาที่มีสิทธิ์ผ่าน เข้า-ออก ในแต่ละพื้นที่อย่างชัดเจน

๒) ผู้ใช้งานจะได้รับสิทธิ์ให้เข้า-ออก สถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนด เท่านั้น

๓) หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งานขอเข้าพื้นที่ โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้าศูนย์เทคโนโลยีสารสนเทศต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้จะต้องแสดงบัตรประจำตัวหรือบัตรประจำตัวประชาชนหรือบัตรประจำตัวอื่นที่ราชการออกให้โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้า-ออก ไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่)

๔) ต้องขออนุญาตเข้ามาปฏิบัติงานในพื้นที่ให้ปฏิบัติตามขั้นตอนปฏิบัติการขอเข้าพื้นที่

๑๐.๑.๓ ความปลอดภัยของสำนักงานห้องทำงานและเครื่องมือต่างๆ (Securing Offices, Rooms and Facilities)

๑) พื้นที่สำนักงานห้องทำงานและเครื่องมือต่างๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออก ของบุคคลทั่วไป

๒) พื้นที่สำนักงานจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณดังกล่าว

๓) พื้นที่สำนักงานห้องทำงานและเครื่องมือต่างๆ ควรมีความปลอดภัยเช่น กั้นพื้นที่อย่างรอบด้าน ติดตั้งผนังติดตั้งเหล็กดัดล็อกประตูที่ใช้ดอกกุญแจหรือมีระบบ Access Control

๑๐.๑.๔ การป้องกันภัยคุกคามภายนอกและสิ่งแวดล้อม (Protecting Against External and Environmental Threats)

๑) พื้นที่สำนักงานที่มีระบบสำคัญจะต้องมีการควบคุมการเข้า-ออก อย่างเข้มงวดและตั้งอยู่ในพื้นที่ที่ปลอดภัยจากภัยทางธรรมชาติ เช่น แผ่นดินไหว หรือน้ำท่วม

๒) ต้องจะมีอุปกรณ์ดับเพลิงอย่างเพียงพอและเหมาะสม ทั้งนี้ในพื้นที่ที่ต้องมีการรักษาความปลอดภัยควรพิจารณาติดตั้งระบบดับเพลิงอัตโนมัติ

๓) ต้องดูแลเรื่องความสะอาดของพื้นที่โดยทั่วไปอย่างสม่ำเสมอเพื่อไม่ให้มีวัสดุที่เป็นเชื้อเพลิงอยู่ในพื้นที่ดังกล่าว

๑๐.๑.๕ การปฏิบัติงานในพื้นที่ควบคุม (Working in Control Areas)

๑) ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุมได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวิดีโอในบริเวณควบคุม เป็นต้น

๒) ต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวิดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

๑๐.๑.๖ การจัดเตรียมพื้นที่สำหรับส่งมอบ (Delivery and loading Areas)

๑) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอกเพื่อป้องกันการเข้าถึงทรัพย์สินโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ควรจัดเป็นบริเวณแยกออกมา

๒) ต้องจัดให้มีขั้นตอนการลงทะเบียนเพื่อบริหารจัดการทรัพย์สินที่ถูกส่งมอบ

๑๐.๒ การกำหนดความปลอดภัยของอุปกรณ์

๑๐.๒.๑ การจัดวางและป้องกันอุปกรณ์ (Equipment siting and protection)

๑) ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจจะเกิดขึ้นกับอุปกรณ์เหล่านั้น

๒) มีการจัดเตรียมพื้นที่จัดเก็บอุปกรณ์ที่ปลอดภัยและไม่สามารถเข้าถึงได้โดยง่ายเช่น ตู้หรือลิ้นชักที่มีกุญแจล็อก

๓) ห้ามมิให้มีการสูบบุหรี่รับประทานอาหารและน้ำดื่มในพื้นที่จัดวางอุปกรณ์ของศูนย์เทคโนโลยีสารสนเทศ

๔) ห้ามนำสารเคมีและเครื่องมือที่อาจก่อให้เกิดอันตรายกับอุปกรณ์เข้ามาในบริเวณพื้นที่ปฏิบัติงาน นอกจากได้รับการพิจารณาอนุญาตและตรวจสอบความเหมาะสมแล้วเท่านั้น

๕) ทำการติดตั้งระบบป้องกันฟ้าผ่ากับอาคารอย่างเหมาะสม

๑๐.๒.๒ ระบบสาธารณูปโภคพื้นฐาน (Supporting utilities)

๑) ต้องมีระบบไฟฟ้าสำรองอัตโนมัติเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่องและต้องมีการตรวจสอบระบบไฟฟ้าสำรองและบำรุงรักษาตามความเหมาะสม

๒) ต้องจัดให้มีระบบเตือนภัย/ป้องกันภัย เช่น ระบบดับเพลิง ระบบเตือนอัคคีภัย

๓) ต้องมีการวางแผนและซักซ้อมการปฏิบัติรับมือกับภัยพิบัติ เช่น อัคคีภัย อย่าง น้อยปีละ ๑ ครั้ง

๔) ระบบที่สำคัญจะต้องมีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจเพื่อลดความสูญเสียที่อาจเกิดขึ้นจากผลกระทบจากเหตุการณ์ภัยพิบัติหรือเหตุการณ์ไม่คาดคิด

๑๐.๒.๓ ความปลอดภัยของสายเคเบิล (Cabling security)

๑) ต้องคำนึงถึงการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน เช่น ผ่านเข้ามาทางใต้ดินผ่านช่องพิเศษที่จัดไว้ หรือเป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย

๒) ต้องจัดเก็บสายเคเบิลทั้งหมดที่ใช้ในการรับ-ส่งข้อมูลไว้ในรางหรืออุปกรณ์ป้องกัน เพื่อป้องกันการดักจับข้อมูลหรืออุบัติเหตุที่อาจทำให้สายขาดหรือชำรุดได้

๓) ต้องแยกสายไฟทั้งหมดออกจากสายเคเบิลในการรับ-ส่งข้อมูล เพื่อป้องกันสัญญาณรบกวน

๑๐.๒.๔ การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

๑) ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงปีละ ๑ ครั้งหรือระบบที่สำคัญมากอาจจะกำหนดให้มีการบำรุงรักษาทุก ๓ เดือน

๒) ทุกครั้งที่ต้องมีการซ่อมแซมอุปกรณ์ใดๆ จะต้องทำการบันทึกรายการซ่อมบำรุงรักษาอุปกรณ์ดังกล่าวทุกครั้ง

๓) ต้องบำรุงรักษาระบบควบคุมสภาพแวดล้อมและอุปกรณ์ต่างๆ ตามคำแนะนำที่ผู้ผลิตระบุไว้

๔) กำหนดให้บุคลากรที่ผ่านการฝึกอบรมและได้รับอนุญาตเท่านั้นที่จะสามารถทำการซ่อมบำรุงระบบและอุปกรณ์ต่างๆ

๑๐.๒.๕ การนำทรัพย์สินออกนอกสถานที่ (Removal of Assets)

๑) การเคลื่อนย้ายสินทรัพย์ต้องทำเป็นบันทึกและขออนุญาตอย่างถูกต้องในการเคลื่อนย้าย

๒) เมื่อมีการนำอุปกรณ์และสื่อที่เคลื่อนย้ายได้ออกไปใช้นอกสถานที่ผู้ที่รับผิดชอบต้องมีมาตรการการป้องกันการสูญหาย

๓) การเคลื่อนย้ายทรัพย์สินใดๆ จะต้องได้รับการอนุญาตลายลักษณ์อักษรและต้องมีการเก็บบันทึกการอนุญาตดังกล่าวไว้

๔) ต้องกำหนดระยะเวลาที่ต้องการยืมทรัพย์สินหรือเวลาที่จะทำการเคลื่อนย้ายทรัพย์สินและต้องบันทึกการเคลื่อนย้ายทรัพย์สินทุกครั้ง

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

๑) ปฏิบัติตามคำแนะนำในการใช้งานจากเจ้าของผลิตภัณฑ์ของอุปกรณ์และทรัพย์สินอย่างเคร่งครัด

๒) ไม่วางอุปกรณ์และทรัพย์สินไว้ในที่สาธารณะโดยขาด ต้องมีการดูแลหรือการเฝ้าระวัง

๓) ต้องกำหนดให้มีการป้องกันทรัพย์สินและอุปกรณ์ เช่น Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน

๑๐.๒.๗ การทำลายอย่างปลอดภัยหรือนำกลับมาใช้งานของอุปกรณ์ (Secure Disposal or Re-Use of Equipment)

๑) ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ทั้งนี้เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว

๒) การทำลายหรือการนำอุปกรณ์กลับมาใช้ใหม่จะต้องถูกกำหนดขั้นตอนการดำเนินงานในการทำลายหรือการนำอุปกรณ์อิเล็กทรอนิกส์กลับมาใช้ใหม่เพื่อให้แน่ใจได้ว่าข้อมูลใด ๆ ที่อยู่ในอุปกรณ์ ดังกล่าวได้ถูกลบทิ้งโดยที่ไม่สามารถกู้คืนกลับมาใช้ได้อีก

๑๐.๒.๘ อุปกรณ์ที่ไม่อยู่ระหว่างการใช้งาน (Unattended user equipment)

๑) ต้องใช้งานซอฟต์แวร์พักหน้าจอโดยตั้งเวลาให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

๒) ต้องทำการออกจากโปรแกรมหรือบริการระบบเครือข่ายเมื่อไม่ใช้งาน

๑๐.๒.๙ นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and Clear screen policy)

๑) ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศที่เป็นข้อมูลความลับหรือลับมากไว้ในที่สามารถพบเห็นได้ง่าย โดยจัดเก็บไว้ในที่ที่ปลอดภัย นอกจากนี้ตู้จ่ายเอกสารหรือจดหมายและเครื่องโทรสารจะต้องได้รับการดูแลให้ปลอดภัยด้วย

๒) เมื่อสั่งพิมพ์งานเอกสารที่มีข้อมูลสำคัญผู้สั่งพิมพ์ต้องทำการจัดเก็บเอกสารโดยทันที

๓) อุปกรณ์คอมพิวเตอร์แม่ข่ายต้องล็อกหรือป้องกันหน้าจอและคีย์บอร์ดที่มีกลไกป้องกันด้วยรหัสผ่านโทเคนหรือกลไกการพิสูจน์ตัวตนผู้ใช้งานเมื่อไม่ได้ใช้งาน

๔) สื่อที่มีข้อมูลอ่อนไหวหรือมีการระบุชั้นความลับไว้ต้องนำออกจากเครื่องถ่ายเอกสารอย่างทันที

๑๑. นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

- ต้องปฏิบัติตามนโยบาย**ข้อ ๑๐.๒.๙**

๑๒. นโยบายการสำรองข้อมูล (Backup Policy)

๑๒.๑ ต้องสำรองข้อมูลที่สำคัญเก็บไว้ตามระยะเวลาที่เหมาะสม

๑๒.๒ ต้องบันทึกรายละเอียดการสำรองข้อมูล โดยมีรายละเอียดเวลาเริ่มต้นและสิ้นสุดชื่อผู้ทำการสำรองข้อมูลและชนิดของข้อมูลที่บันทึก

๑๒.๓ กรณีที่เกิดการผิดพลาดในการสำรองข้อมูลผู้สำรองข้อมูลต้องบันทึกรายละเอียดของข้อผิดพลาดที่เกิดขึ้นพร้อมแนวทางแก้ไข

๑๒.๔ ต้องมีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมเพื่อให้สามารถกู้ข้อมูลกลับคืนได้ป้องกันระบบจากการถูกโจมตีหรือความเสียหายที่อาจเกิดขึ้น

๑๒.๕ ต้องควบคุมความปลอดภัยของข้อมูลที่สำรองตามชั้นความลับโดยใช้เทคโนโลยีที่เหมาะสมเพื่อป้องกันข้อมูลสำรองถูกเปิดเผย

๑๒.๖ ต้องจัดให้มีการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอและการทดสอบควรดำเนินการบนสื่อที่จัดเตรียมไว้แยกจากสื่อที่ใช้สำหรับสำรองข้อมูลตามปกติเพื่อป้องกันกรณีการทดสอบการกู้คืนข้อมูลไม่สำเร็จซึ่งอาจจะทำให้ข้อมูลที่สำรองไว้เสียหายและไม่สามารถนำกลับมาใช้งานได้

๑๓. นโยบายการถ่ายโอนสารสนเทศ (Information transfer policy)

๑๓.๑ ขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ

๑๓.๑.๑ ต้องออกแบบขั้นตอนเพื่อป้องกันการถ่ายโอนข้อมูลจากการถูกดักจับ คัดลอก แก้ไข ส่งผิดเส้นทาง

๑๓.๑.๒ ต้องมีขั้นตอนสำหรับการตรวจจับและป้องกันมัลแวร์ซึ่งอาจถูกส่งผ่านการสื่อสารทางอิเล็กทรอนิกส์

๑๓.๑.๓ ต้องมีการป้องกันการส่งข้อมูลที่สำคัญด้วยวิธีการแนบเอกสาร

๑๓.๑.๔ ผู้ใช้งานต้องรับผิดชอบในบทบาทหน้าที่ไม่ฝ่าฝืนนโยบายและแนวปฏิบัติเช่น การหมิ่นประมาทการข่มขู่หรือก่อกวนความสงบ การปลอมตัว การส่งต่อจดหมายลูกโซ่ การจัดซื้อจัดจ้างนอกเหนือการอนุมัติ

๑๓.๑.๕ ต้องมีเทคนิคการเข้ารหัสเพื่อปกป้องความลับ ความสมบูรณ์และความถูกต้องของข้อมูล

๑๓.๑.๖ ต้องมีแนวทางในการเก็บรักษาและทำลายสำหรับจดหมายธุรกิจต้องเป็นไปตามที่กฎหมายกำหนด

๑๓.๑.๗ ต้องไม่ทิ้งเอกสารสำคัญไว้ที่เครื่องถ่ายเอกสารเครื่องพิมพ์หรือเครื่องโทรสาร ซึ่งผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้

๑๓.๑.๘ ต้องควบคุมและยับยั้งการส่งต่อข้อมูลของอุปกรณ์สื่อสาร เช่น การส่งต่อเมลอัตโนมัติไปที่อยู่อีเมลนอกสำนักงาน

๑๓.๑.๙ ต้องแนะนำและอบรมให้ความรู้ต่อผู้ใช้งานให้ใช้มาตรการที่เหมาะสมเพื่อป้องกันข้อมูลรั่วไหล

๑๓.๑.๑๐ ต้องมีการควบคุมและตรวจสอบเครื่องโทรสารและเครื่องถ่ายเอกสารรุ่นใหม่ที่มีหน่วยความจำในการเก็บเอกสารบางหน้าหรือการส่งข้อมูลที่พิมพ์ผิดพลาด ซึ่งอาจจะถูกพิมพ์ออกมาเมื่อเครื่องทำงานได้ตามปกติ

๑๓.๒ ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ

๑๓.๒.๑ ต้องมีการบริหารจัดการในการควบคุมและแจ้งให้ทราบเกี่ยวกับการสื่อสารการส่งและการรับข้อมูล

๑๓.๒.๒ ต้องมีการแจ้งให้ผู้ส่งรับทราบเกี่ยวกับการสื่อสารการส่งและการรับข้อมูล

๑๓.๒.๓ ต้องมีกระบวนการที่สามารถติดตามและปฏิเสธความรับผิดชอบไม่ได้

๑๓.๒.๔ ต้องมีมาตรฐานทางเทคนิคขั้นต่ำในการสื่อสาร เช่น เอกสารมาตรฐานการเข้ารหัสแบบสมมาตรด้วย AES-๑๒๘, AES-๒๕๖ และการเข้ารหัสแบบอสมมาตรด้วย RSA๒๐๔๘

๑๓.๒.๕ ต้องมีสัญญาข้อตกลง เช่น สัญญาระหว่าง กรมราชทัณฑ์ และผู้ให้บริการภายนอกที่จะมีการสื่อสาร ผ่านเครือข่ายที่ปลอดภัยและมีการเข้ารหัส

๑๓.๒.๖ ต้องมีมาตรฐานในการระบุตัวผู้ส่งเอกสาร

๑๓.๒.๗ ต้องใช้ระบบป้ายชื่อตามข้อตกลงสำหรับข้อมูลที่มีความสำคัญ เพื่อเข้าใจได้ทันทีในความหมายของป้ายชื่อและข้อมูลได้รับการปกป้องข้อมูลอย่างเหมาะสม

๑๓.๒.๘ ต้องมีการควบคุมพิเศษที่จำเป็นในการปกป้องข้อมูลสำคัญ เช่น การเข้ารหัสแบบสมมาตรด้วย AES-๑๒๘, AES-๒๕๖ และการเข้ารหัสแบบอสมมาตรด้วย RSA๒๐๔๘

๑๓.๒.๙ ต้องมีการควบคุมการเข้าถึงในระดับที่ยอมรับได้และปลอดภัย

๑๓.๓ การส่งข้อความทางอิเล็กทรอนิกส์

๑๓.๓.๑ ต้องปกป้องข้อความจากผู้ที่ไม่ได้รับอนุญาตไม่ให้มีการแก้ไขข้อความหรือทำให้ระบบใช้งานไม่ได้

๑๓.๓.๒ ต้องมั่นใจว่าที่อยู่ปลายทางและการส่งข้อความถูกต้อง

๑๓.๓.๓ ต้องมีความน่าเชื่อถือและความสามารถในการให้บริการ

๑๓.๓.๔ ต้องปฏิบัติตามข้อกำหนดทางกฎหมาย เช่น การใช้ลายมืออิเล็กทรอนิกส์

๑๓.๓.๕ การใช้บริการแบบสาธารณะต้องระวังในการรับ–ส่งข้อมูลที่เป็นความลับ เช่น โปรแกรมแชท เครือข่ายสังคมออนไลน์ การแชร์ไฟล์

๑๓.๓.๖ ต้องมีการระบุตัวตนในการควบคุมการเข้าถึงจากระบบเครือข่ายสาธารณะต้องปฏิบัติตามมาตรการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างเข้มงวด

๑๓.๔ ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ

๑๓.๔.๑ ต้องจัดให้มีการลงนามในสัญญาการรักษาความลับหรือการไม่เปิดเผยความลับระหว่างผู้ใช้งานและ กรมราชทัณฑ์ว่าจะไม่เปิดเผยความลับของกรมราชทัณฑ์ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะทำงานและผูกพันอย่างต่อเนื่องเป็นเวลาไม่น้อยกว่า ๒ ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว พร้อมบทลงโทษ

๑๓.๔.๒ บุคลากรที่ต้องลงนามในสัญญาการรักษาความลับหรือการไม่เปิดเผยความลับประกอบไปด้วย ข้าราชการ พนักงาน ลูกจ้าง และบุคลากรจากหน่วยงานภายนอกรวมถึงนักศึกษาฝึกงานทุกคน ซึ่งเป็นส่วนหนึ่งของเงื่อนไขและข้อกำหนดในการจ้างงานหรือการฝึกงานและจะต้องจัดเก็บหลักฐานการลงนามไว้ด้วย

๑๔. นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

๑๔.๑ ระบบสารสนเทศต้องได้รับการพัฒนาในสภาพแวดล้อมที่มีความมั่นคงปลอดภัยทั้งทางกายภาพและลอจิคัล เช่น สถานที่ที่ใช้ในการพัฒนาระบบต้องไม่สามารถเข้าถึงโดยผู้ไม่เกี่ยวข้องได้โดยง่าย

๑๔.๒ การพัฒนาระบบสารสนเทศต้องคำนึงถึงความมั่นคงปลอดภัยตลอดวงจรชีวิตของการพัฒนาซอฟต์แวร์ โดยครอบคลุมตั้งแต่ขั้นตอนการรวบรวมความต้องการ การออกแบบ การพัฒนา การทดสอบ การใช้งาน ตลอดไปจนถึงการยกเลิกการใช้งานระบบ

๑๔.๓ ขั้นตอนการพัฒนาระบบสารสนเทศต้องมีการกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับ ระบบสารสนเทศ ดังต่อไปนี้

๑๔.๓.๑ การป้องกันข้อมูลจากการถูกเปิดเผยโดยไม่ได้รับอนุญาต

๑๔.๓.๒ การป้องกันข้อมูลจากการถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

๑๔.๓.๓ ความต้องการด้านความพร้อมใช้งานของข้อมูลและระบบสารสนเทศ

๑๔.๓.๔ การพิสูจน์ตัวตนของผู้ใช้งานและผู้ดูแลระบบ

๑๔.๓.๕ การจัดการสิทธิ์ในการใช้งานระบบ

๑๔.๓.๖ ความต้องการในการตรวจสอบและจัดเก็บประวัติการใช้งานประวัติการเข้าถึง

๑๔.๓.๗ การป้องกันการปฏิเสธการทำรายการ

๑๔.๓.๘ การบริหารจัดการค่าการปรับแต่ง, เซสชั่นและการจัดการกับข้อผิดพลาดที่เกิดขึ้น

๑๔.๓.๙ ความต้องการด้านสมรรถนะของระบบสารสนเทศ เช่น ความเร็วในการประมวลผลข้อมูล ความสามารถในการเก็บข้อมูล การประมวลผลในด้านภาพกราฟฟิก ขนาดหน่วยความจำ

๑๔.๓.๑๐ ความต้องการด้านความมั่นคงปลอดภัยอื่นๆ ที่สอดคล้องกับข้อกำหนดกฎหมายหรือกฎระเบียบที่องค์กรต้องปฏิบัติตาม

๑๔.๔ ต้องกำหนดจุดทบทวนด้านความมั่นคงปลอดภัยในแต่ละระยะการดำเนินงานของโครงการ เช่น มีการกำหนดให้มีการสอบทานด้านความมั่นคงปลอดภัยในขั้นตอน การออกแบบ การพัฒนา การ ทดสอบ และก่อนการใช้งานจริง

๑๔.๕ ต้องรักษาความปลอดภัยของพื้นที่ที่ใช้ในการจัดเก็บข้อมูลอย่างเหมาะสม เช่น มีการกำหนดและจำกัดสิทธิ์ในการเข้าถึงฐานข้อมูล

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

๑๕. ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationship)

๑๕.๑ ต้องมีการกำหนดมาตรการควบคุมการเข้าถึงสารสนเทศของกรมราชทัณฑ์ โดยผู้ให้บริการภายนอกอย่างเหมาะสมและปลอดภัย

๑๕.๒ ต้องมีการกำหนดประเภทของสารสนเทศที่ผู้ให้บริการภายนอกสามารถเข้าถึงได้ และกำหนดมาตรการเฝ้าระวังและสอบทานอย่างเหมาะสม

๑๕.๓ ต้องมีการให้ความรู้แก่ผู้ที่มีส่วนเกี่ยวข้องกับผู้ให้บริการภายนอก เพื่อช่วยในการเฝ้าระวังด้านความมั่นคงปลอดภัยสารสนเทศ

๑๖. นโยบายการจัดชั้นความลับ (Information Classification Policy)

๑๖.๑ การจัดชั้นความลับของสารสนเทศ

๑๖.๑.๑ เจ้าของสารสนเทศมีหน้าที่ในการกำหนดชั้นความลับของสารสนเทศตามกระบวนการจัดชั้นความลับของสารสนเทศภายใต้รับความผิดชอบของตน

๑๖.๑.๒ การป้องกันสารสนเทศต้องพิจารณาทั้ง ๓ ด้าน คือ การรักษาความลับ การรักษาความสมบูรณ์และความพร้อมใช้งาน

๑๖.๑.๓ ข้อมูลหรือสารสนเทศให้หน่วยงานระบุชนิดลักษณะของข้อมูลให้ชัดเจนว่าเกี่ยวกับเรื่องใด มีความสำคัญอย่างไร และต้องมีการจัดลำดับชั้นความลับเป็นอย่างใดอย่างหนึ่งต่อไปนี้ เช่น ชั้นเปิดเผย ชั้นใช้ภายใน ชั้นลับ ชั้นลับมาก ชั้นลับที่สุด

๑๖.๑.๔ ข้อมูลหรือสารสนเทศซึ่งมีการกำหนดชั้นความลับไว้ทั้งในกรณีทั้งหมดหรือบางส่วนให้ถือว่ามีชั้นความลับเดียวกันกับข้อมูลหรือสารสนเทศนั้นยกเว้นว่ามีการจัดลำดับชั้นความลับใหม่โดยหน่วยงานเจ้าของข้อมูลหรือสารสนเทศนั้น

๑๖.๑.๕ ต้องทำการจัดหมวดหมู่กำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสารเพื่อป้องกันสารสนเทศให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดยให้ปฏิบัติตามกระบวนการการจัดระดับชั้นความลับข้อมูลและสารสนเทศ

๑๖.๑.๖ ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษา ความปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การเก็บรักษาจนถึงการทำลายตามกระบวนการ การจัดระดับชั้นความลับข้อมูลและสารสนเทศ

๑๖.๒ การบ่งชี้สารสนเทศ

๑๖.๒.๑ เจ้าหน้าที่และผู้ปฏิบัติงานตามสัญญาจ้างทุกคนต้องปฏิบัติตามขั้นตอนในการจัดทำป้ายชื่อสารสนเทศ

๑๖.๒.๒ การจัดทำป้ายชื่อต้องสอดคล้องกับระดับชั้นความลับที่กำหนดไว้ในการจัดชั้นความลับสารสนเทศ

๑๖.๒.๓ การจัดทำป้ายชื่อสารสนเทศต้องครอบคลุมสารสนเทศทั้งในรูปแบบที่เป็นกายภาพและอิเล็กทรอนิกส์

๑๖.๒.๔ ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับสารสนเทศ โดยแยกตามหมวดหมู่ที่กำหนดไว้มีการส่งมอบและจัดเก็บตามขั้นตอนกระบวนการต่างๆ ซึ่งประกอบไปด้วยการถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสารและการทำลาย ให้ปฏิบัติตามแนวทางปฏิบัติของระเบียบปฏิบัติของทางราชการตามกฎหมายที่เกี่ยวข้อง

๑๖.๒.๕ หากมีความจำเป็นจะต้องกำหนดระดับชั้นความลับของข้อมูลในสื่อบันทึกดังกล่าวเป็นระดับอื่นจะต้องติดป้ายชื่อให้กับสื่อบันทึกดังกล่าวให้สอดคล้องกับข้อมูลดังกล่าว

๑๖.๒.๖ ข้อมูลทุกระดับชั้นจะต้องถูกส่งผ่านระบบอีเมลของกรมราชทัณฑ์เท่านั้น กรณีมีช่องทางอื่นๆ ที่มีความจำเป็นต้องใช้ส่งข้อมูลจะต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศเพื่อพิจารณาถึงความปลอดภัยอย่างเหมาะสม

๑๖.๓ การจัดการทรัพย์สิน

๑๖.๓.๑ กระบวนการปฏิบัติงานในการจัดการสินทรัพย์ต้องสอดคล้องและเป็นไปในทิศทางเดียวกับการจัดชั้นความลับสารสนเทศ

๑๖.๓.๒ ต้องมีการจัดเก็บสินทรัพย์ตามรายละเอียดการจัดเก็บจากผู้ผลิต หากสินทรัพย์นั้นต้องการ การจัดเก็บเป็นพิเศษ

๑๗. นโยบายการจัดการสื่อบันทึกข้อมูล (Media Handling policy)

๑๗.๑ การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้

๑๗.๑.๑ ข้อมูลที่มีชั้นความลับ ชั้นความลับมาก ชั้นความลับที่สุด ต้องกำหนดให้มีการทำลายสื่อบันทึกข้อมูลเมื่อไม่มีการใช้งานแล้ว

๑๗.๑.๒ ในกรณีที่สื่อบันทึกข้อมูลนั้นไม่ได้ถูกนำมาใช้งานแล้ว ก่อนที่จะนำออกไปจากกรมราชทัณฑ์ ต้องมั่นใจว่าข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก

๑๗.๑.๓ ในกรณีที่จำเป็นต้องนำสื่อบันทึกข้อมูลออกไป จะต้องได้รับการอนุมัติจากผู้ที่รับผิดชอบสื่อบันทึกข้อมูลดังกล่าว และต้องบันทึกการโยกย้าย เพื่อใช้ในการตรวจสอบภายหลัง

๑๗.๑.๔ สื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต เช่น อุณหภูมิสูงหรือต่ำเกินไป

๑๗.๑.๕ ในการจัดเก็บสื่อบันทึกข้อมูลที่สำคัญ ต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล เช่น มีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน กำหนดบุคลากรที่มีสิทธิ์ในการใช้งาน

๑๗.๑.๖ ถ้าข้อมูลที่ต้องการจัดเก็บมีอายุการจัดเก็บยาวนานกว่าอายุการใช้งานของสื่อบันทึกข้อมูล ควรจัดเก็บไว้ที่แหล่งอื่นเพื่อป้องกันการสูญหายของข้อมูล

๑๗.๑.๗ ต้องจัดทำทะเบียนบันทึกข้อมูลของสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้เพื่อลดโอกาสการสูญหายของข้อมูล

๑๗.๒ การทำลายสื่อบันทึกข้อมูล

๑๗.๒.๑ สื่อที่บันทึกข้อมูลที่มีความสำคัญมากจะต้องมีการทำลายด้วยวิธีการที่ปลอดภัย เช่น การเผาหรือแยกชิ้นส่วนเป็นชิ้นเล็กๆ หรือลบข้อมูลด้วยซอฟต์แวร์อื่นๆ ที่มีใช้ในกรมราชทัณฑ์

๑๗.๒.๒ กระบวนการต่างๆ ต้องระบุวิธีการกำจัดสื่อบันทึกข้อมูลอย่างชัดเจนเพื่อความปลอดภัยของข้อมูล

๑๗.๒.๓ เพื่อความสะดวกควรรวบรวมสื่อทั้งหมดที่ไม่ต้องการแล้วกำจัดพร้อมกันด้วยวิธีการที่ปลอดภัย

๑๗.๒.๔ ในกรณีที่เลือกใช้บริการกำจัดสื่อและเอกสารรวมทั้งอุปกรณ์ต่างๆ จากหน่วยงานภายนอก ควรระมัดระวังในการเลือกใช้บริการ ต้องเลือกหน่วยงานภายนอกที่มีการควบคุมที่ดีมีมาตรฐานและมีประสบการณ์

๑๗.๒.๕ ในการกำจัดสื่อบันทึกข้อมูลจะต้องมีการบันทึกเพื่อใช้ในการตรวจสอบ

๑๗.๓ การเคลื่อนย้ายสื่อบันทึกข้อมูล

๑๗.๓.๑ ใช้วิธีการขนส่งหรือพนักงานส่งของที่เชื่อถือได้

๑๗.๓.๒ รายชื่อของพนักงานส่งของหรือบริษัทส่งของควรได้รับการอนุมัติจากผู้มีอำนาจ

๑๗.๓.๓ กระบวนการตรวจสอบพนักงานส่งของต้องมีการปรับปรุงอย่างสม่ำเสมอ

๑๗.๓.๔ การบรรจุภัณฑ์ต้องป้องกันความเสียหายในระหว่างการขนส่งโดยเป็นไปตามข้อกำหนดของผู้ผลิต ตัวอย่างการป้องกันปัจจัยทางกายภาพที่จะมีผลต่อการกู้คืนข้อมูล เช่น ความร้อน, ความชื้น และสนามแม่เหล็ก

๑๗.๓.๕ การควบคุมที่จำเป็นในการปกป้องข้อมูลสำคัญจากการเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต

๑) ใช้ตู้ที่มีกุญแจล๊อค

๒) ส่งด้วยมือตนเองและลงบันทึกการรับเพื่อสามารถตรวจสอบได้

๓) บางกรณีอาจจะต้องใช้วิธีการแยกส่งออกหลายๆ ส่วนและหลายๆ เส้นทางเพื่อกระจายความเสี่ยง

๑๘. การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software)

๑๘.๑ การควบคุมการติดตั้งซอฟต์แวร์

๑๘.๑.๑ ต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ซอฟต์แวร์อุดช่องโหว่ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบ การใช้งานมาเป็นอย่างดี ว่าไม่ก่อให้เกิดปัญหาหรือผลกระทบต่อเครื่องที่ให้บริการอยู่

๑๘.๑.๒ มีการบริหารจัดการเวอร์ชันของซอฟต์แวร์และมีการจัดเก็บซอฟต์แวร์เวอร์ชันก่อนหน้าไว้ในกรณีที่มีความจำเป็นต้องทำการถอยกลับไปใช้เวอร์ชันก่อนหน้านี้

๑๙. การบริหารจัดการช่องโหว่ (Technical Vulnerability Management)

๑๙.๑ การบริหารจัดการช่องโหวในฮาร์ดแวร์และซอฟต์แวร์

๑๙.๑.๑ ต้องกำหนดหน้าที่ความรับผิดชอบที่ชัดเจน เช่น การเฝ้าระวังภัยคุกคามการประเมินความเสี่ยงของภัยคุกคาม การแพตช์ปิดช่องโหว่ในระบบ การตรวจสอบสินทรัพย์ที่ได้จัดส่วนหมวดหมู่ไว้

๑๙.๑.๒ ต้องร่วมกันวิเคราะห์ความเสี่ยงและประเมินสถานการณ์การบุกรุก ละเมิด ระบาดที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศอย่างสม่ำเสมอหรืออย่างน้อย ปีละ ๑ ครั้ง

๑๙.๑.๓ ในกรณีที่จะทำการอัพเดทแพตช์ของระบบสำคัญๆ ต้องมีการทดสอบและประเมินก่อนว่าจะไม่ก่อให้เกิดความเสียหายหรือมีผลกระทบต่อระบบ แต่ถ้าไม่สามารถอัปเดตแพตช์ได้ก็ให้พิจารณาดังต่อไปนี้

๑) ปิด Service หรือ การทำงานที่เกี่ยวข้องกับช่องโหว่

๒) ปรับปรุงหรือเพิ่มระดับความปลอดภัยในการเข้าถึงที่บริเวณรอบนอกเครือข่าย เช่น เพิ่มอุปกรณ์ไฟร์วอลล์หรือ IPS (Intrusion Prevention System)

๓) เพิ่มการเฝ้าระวังเพื่อตรวจจับหรือป้องกันการโจมตีเครือข่ายอย่างเข้มงวด

๔) ต้องมีการสร้างความตระหนักเกี่ยวกับช่องโหว่ที่เกิดขึ้น

๕) ต้องเก็บ Log ของเหตุการณ์ที่เกิดขึ้นทั้งหมดเพื่อใช้ในการตรวจสอบ

๖) ต้องมีกระบวนการบริหารจัดการช่องโหว่ที่มีการดำเนินการ เช่น การเฝ้าระวังต้องมั่นใจว่ามีประสิทธิภาพและประสิทธิผล

๗) ระบบที่มีความเสี่ยงสูงจะต้องมีการเตรียมการเป็นอันดับแรกตามลำดับความสำคัญและการประเมินความเสี่ยง

๑๙.๒ การจำกัดสิทธิ์ในการติดตั้งซอฟต์แวร์

๑๙.๒.๑ ต้องจัดทำรายการซอฟต์แวร์ที่จำเป็นสำหรับเครื่องผู้ใช้งาน เช่น เครื่องคอมพิวเตอร์, แล็ปท็อป

๑๙.๒.๒ ต้องทำการตรวจสอบและอนุมัติรายการซอฟต์แวร์ที่จำเป็นสำหรับเครื่องผู้ใช้งานเพื่อจัดทำเป็นรายการซอฟต์แวร์ที่อนุญาตให้ใช้งานในองค์กรสำหรับเครื่องผู้ใช้งานทั่วไป

๑๙.๒.๓ ห้ามผู้ใช้งานทำการติดตั้งซอฟต์แวร์ที่เป็นการละเมิดลิขสิทธิ์รวมถึงซอฟต์แวร์อื่นๆ ที่ไม่ได้รับอนุญาตให้ใช้งานในกรมราชทัณฑ์.

๑๙.๒.๔ หากผู้ใช้งานต้องการติดตั้งซอฟต์แวร์ที่อยู่นอกเหนือรายการซอฟต์แวร์ที่อนุญาตให้ใช้งานจะต้องทำการขออนุมัติศูนย์เทคโนโลยีสารสนเทศก่อนการติดตั้ง

๑๙.๒.๕ การติดตั้งซอฟต์แวร์บนเครื่องผู้ใช้งานจะต้องกระทำโดยผู้ดูแลระบบเท่านั้น โดยผู้ดูแลระบบต้องทำการจำกัดสิทธิ์ในการติดตั้งซอฟต์แวร์บนเครื่องของผู้ใช้งานอย่างเหมาะสม

๑๙.๒.๖ ต้องทำการตรวจสอบการใช้งานซอฟต์แวร์ที่ไม่ได้รับอนุญาตอย่างน้อยปีละ ๑ ครั้ง

๒๐. นโยบายการควบคุมการเปลี่ยนแปลงระบบ (System Change Control Policy)

๒๐.๑ ขั้นตอนปฏิบัติสำหรับการควบคุมการเปลี่ยนแปลงระบบอย่างเป็นทางการควรจัดทำเป็นเอกสาร และบังคับใช้เพื่อให้มั่นใจได้ว่าความถูกต้องของระบบแอปพลิเคชัน และผลิตภัณฑ์ตั้งแต่ขั้นตอนการออกแบบ จนถึงการบำรุงรักษาในปัจจุบัน

๒๐.๒ การปรับเปลี่ยนระบบใหม่หรือการเปลี่ยนแปลงครั้งใหญ่ที่มีผลกระทบกับระบบที่ทำงานอยู่ในปัจจุบัน ควรได้รับอนุญาตตามขั้นตอนตั้งแต่การทำจัดเอกสาร การจัดทำ, การระบุรายละเอียด, การทดสอบ, การควบคุมคุณภาพ และการจัดการสำหรับการติดตั้งระบบ

๒๐.๓ ขั้นตอนการควบคุมการเปลี่ยนแปลงต้องรวมการประเมินความเสี่ยง การวิเคราะห์ผลกระทบของการเปลี่ยนแปลง และรายละเอียดการควบคุมความปลอดภัยที่ต้องการ

๒๐.๔ ขั้นตอนการควบคุมการเปลี่ยนแปลงต้องมั่นใจได้ว่ามีการควบคุมความปลอดภัยอย่างเหมาะสม เช่น ผู้พัฒนาโปรแกรมควรได้รับสิทธิ์ในการเข้าถึงระบบเท่าที่จำเป็นสำหรับใช้ในการทำงาน และการเปลี่ยนแปลง ควรได้รับการอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๒๑. นโยบายการบริหารจัดการเพื่อสร้างความเนื่องทางธุรกิจ (Information security continuity policy)

๒๑.๑ ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

๒๑.๑.๑ ต้องมีการกำหนดแนวทางในการสร้างความต่อเนื่องด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในกรณีที่เกิดเหตุการณ์ไม่พึงประสงค์ เช่น เหตุฉุกเฉิน หรือ วิกฤต

๒๑.๑.๒ จัดให้ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ เป็นส่วนหนึ่งของกระบวนการในการบริหารจัดการความต่อเนื่องทางธุรกิจหรือกระบวนการในการกู้คืนระบบในภาวะวิกฤต

๒๑.๑.๓ พิจารณาด้านความมั่นคงปลอดภัยสารสนเทศ ระหว่างการวางแผนความต่อเนื่องทางธุรกิจ หรือการกู้คืนระบบในภาวะวิกฤต

๒๑.๒ การดำเนินการความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

๒๑.๒.๑ ต้องจัดตั้งคณะทำงานแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงานเจ้าของข้อมูล เจ้าของระบบงาน และหน่วยงานที่ดูแลระบบเครือข่าย เป็นต้น

๒๑.๒.๒ คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศที่เป็นลายลักษณ์อักษร

๒๑.๒.๓ กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศต้องประกอบด้วยหัวข้อหลัก ดังนี้

๑) การวิเคราะห์ผลกระทบทางธุรกิจ

๒) การประเมินความเสี่ยงและการควบคุม

๓) การวางกลยุทธ์สำหรับแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

๔) การพัฒนาแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

๕) การประชาสัมพันธ์และการฝึกอบรม

๖) การทดสอบปรับปรุงแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

๗) การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินภารกิจและการให้บริการ

๘) การตอบสนองต่อสถานการณ์ฉุกเฉินเพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุมการแก้ไขสถานการณ์ฉุกเฉิน

๙) การดำเนินการเพื่อให้สามารถดำเนินภารกิจได้อย่างต่อเนื่องเช่น การสำรอง ข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย

๑๐) ต้องมีการกลับคืนสู่การทำงานปกติเพื่อให้ภารกิจกลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ

๒๑.๒.๔ แนวทางปฏิบัติของการเก็บรักษาข้อมูลและสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศผู้ใช้งาน ควรปฏิบัติตามแนวปฏิบัติการสำรองข้อมูลการกู้คืนและรักษาความลับของข้อมูล

๑) เจ้าของข้อมูลเป็นผู้จัดเก็บรักษาข้อมูลเกี่ยวกับระบบ ซึ่งได้แก่ข้อมูลเกี่ยวกับระบบปฏิบัติการ, ซอฟต์แวร์ระบบงาน (ทั้ง Source Code และ Executable Files) โดยให้เป็นไปตามความต้องการที่เจ้าของข้อมูลในระบบนั้น กำหนดจำนวนครั้งและระยะเวลาในการเก็บรักษาข้อมูลดังกล่าว ต้องสอดคล้องกับการประเมินความเสี่ยงของข้อมูลนั้นๆ ด้วย

๒) ก่อนที่จะมีการปรับปรุงหรือเปลี่ยนแปลงระบบ หน่วยงานที่รับผิดชอบต้องทำการสำรองข้อมูลของระบบทุกครั้ง

๓) ถ้าการสำรองข้อมูลถูกดำเนินการที่เซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์หลักและเป็นข้อมูลของระบบงานที่สำคัญ จะต้องเพิ่มจำนวนครั้งในการสำรองข้อมูลของเซิร์ฟเวอร์นั้นด้วย

๔) ข้อมูลและสารสนเทศที่มีความสำคัญมาก จะต้องทำการสำรองข้อมูลไว้ทุกวันและข้อมูลสำรองดังกล่าว ต้องมีการจัดเก็บไว้นอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลักอย่างเหมาะสม โดยตรวจสอบให้แน่ใจว่าสถานที่นั้นมีความปลอดภัยด้วย

๕) ระบบข้อมูลที่สำคัญทั้งหมด ควรมีระบบการประมวลผลสำรองระบบเครือข่ายสำรองเพื่อป้องกันการพึ่งพาระบบหลักเพียงระบบเดียว ในกรณีที่ ระบบหนึ่งไม่สามารถทำงานได้สามารถใช้งานอีกระบบหนึ่งได้ทันทีเพื่อให้ภารกิจหลักดำเนินต่อไปได้

๖) ข้อมูลและสารสนเทศที่ถูกจัดประเภทเป็นข้อมูลธรรมดา ซึ่งไม่ส่งผลกระทบต่อการดำเนินกิจการ จำนวนครั้งในการสำรองข้อมูลนั้นขึ้นอยู่กับการพิจารณาของเจ้าของข้อมูลและข้อมูลดังกล่าวจะถูกนำไปจัดเก็บในสถานที่ ๆ มีความปลอดภัย

๒๑.๒.๕ แนวทางปฏิบัติของการเก็บข้อมูลสำรองนอกสถานที่

๑) ศูนย์คอมพิวเตอร์สำรองหรือสถานที่ที่ใช้ในการจัดเก็บข้อมูลสำรองควรตั้งอยู่ไกลจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะแน่ใจได้ว่าเหตุการณ์หรือภัยธรรมชาติชนิดเดียวกัน เช่น ไฟไหม้ หรือเหตุจลาจลต่างๆ จะไม่เกิดขึ้นกับศูนย์คอมพิวเตอร์ทั้งสองแห่งพร้อมกัน

๒) ศูนย์คอมพิวเตอร์สำรองหรือสถานที่ที่จัดเก็บข้อมูลสำรองนอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลัก ต้องมีการรักษาความปลอดภัยทั้งในด้านกายภาพ และสภาพแวดล้อมการควบคุมเช่นเดียวกันกับศูนย์คอมพิวเตอร์หลักหรือปรับเปลี่ยนตามความเหมาะสม

๒๑.๓ การตรวจสอบ สอบทาน และวัดผลความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

๒๑.๓.๑ คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศที่เป็นลายลักษณ์อักษรโดยต้องมีการสอบทานและปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละ ๑ ครั้ง

๒๒. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

๒๒.๑ การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Management of Information Security Incidents and Improvements) เพื่อให้มีวิธีการที่สอดคล้องและได้ผล สำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย

๒๒.๑.๑ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติต้องมีการกำหนดหน้าที่ความรับผิดชอบและกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและขั้นตอนดังกล่าวต้องมีความรวดเร็วได้ผล และมีความเป็นระบบระเบียบที่ดี

๒๒.๑.๒ การรายงานเหตุการณ์น่าสงสัย / จุดอ่อนด้านความมั่นคงปลอดภัย

๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการรายงานเหตุการณ์ทันทีที่สงสัยว่าเป็นเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล

๒) ถ้าหากพบเหตุการณ์ที่น่าสงสัยให้แจ้งต่อผู้รับผิดชอบทันทีเช่น เหตุการณ์ต่อไปนี้

(๒.๑) พบว่ารหัสผ่านส่วนบุคคลของตนถูกล็อกโดยไม่ทราบสาเหตุ

(๒.๒) เวลาการเข้าใช้งานระบบครั้งล่าสุดที่ผิดปกติ

(๒.๓) พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน เช่น มีไฟล์ที่ไม่รู้จักการเปลี่ยนแปลงของค่าต่างๆ

(๒.๔) มีการไม่ปฏิบัติตามขั้นตอนความมั่นคงปลอดภัย

(๒.๕) พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล

(๒.๖) พบหรือคาดว่าข้อมูลในระบบจะถูกทำลายแก้ไขหรือลบทิ้ง

(๒.๗) มีความพยายามที่จะเข้าใช้ระบบอย่างผิดวิธีไม่ว่าจะสำเร็จหรือไม่

(๒.๘) การให้บริการของระบบเกิดการชะงักหรือไม่สามารถให้บริการ

(๒.๙) เกิดการละเมิดสิทธิ์เข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล

(๒.๑๐) การแก้ไขค่าความปลอดภัยในระบบเช่น Hardware, Software หรือ Firmware โดยผู้ใช้งานไม่ทราบ

๒๒.๑.๓ การประเมินเหตุการณ์ด้านความมั่นคงปลอดภัย ผู้ดูแลระบบต้องประเมินขอบเขตและความรุนแรงของปัญหาหากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้างรุนแรง หรือมีผลต่อชื่อเสียงจะต้องรายงานให้ผู้บังคับบัญชาทราบโดยด่วนเพื่อหาแนวทางแก้ไขและป้องกันไม่ให้เกิดในครั้งต่อไป ควรมีการแบ่งประเภทของปัญหาอย่างเหมาะสม

๒๒.๑.๔ การตอบโต้ต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดและการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟต์แวร์ เพื่อลดความเสียหายจากเหตุการณ์ละเมิดความมั่นคงปลอดภัยและระบบทำงานบกพร่อง เช่น ไวรัสคอมพิวเตอร์แพร่กระจาย ระบบถูกบุกรุก และให้บุคลากรได้เรียนรู้จากประสบการณ์ความเสียหายดังกล่าว

๑) หากผู้ใช้งานพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัย และ/หรือจุดอ่อน ช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และ/หรือการทำงานที่บกพร่อง หรือการทำงานผิดปกติของซอฟต์แวร์ผู้ใช้งานต้องรายงานสิ่งที่เกิดขึ้นให้แก่ ผู้รับผิดชอบทราบโดยเร่งด่วน

๒) ในกรณีที่ไม่สามารถติดต่อผู้รับผิดชอบได้ ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้น

๓) ในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยให้ปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ดังนี้

(๓.๑) ภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง มีความเสี่ยงอย่างมีนัยสำคัญที่ทำให้ระบบคอมพิวเตอร์หรือการให้บริการของกรมราชทัณฑ์ ด้อยประสิทธิภาพลง

(๓.๒) ภัยคุกคามทางไซเบอร์ระดับร้ายแรง ถูกโจมตีอย่างมีนัยสำคัญ ทำให้เกิดความเสียหายกับระบบคอมพิวเตอร์หรือ การให้บริการของกรมราชทัณฑ์ จนไม่สามารถทำงานหรือให้บริการได้

(๓.๓) ภัยคุกคามทางไซเบอร์ระดับร้ายแรงวิกฤติถูกโจมตีในระดับสูง ส่งผลกระทบรุนแรงเป็นวงกว้างทำให้ระบบคอมพิวเตอร์ หรือการให้บริการที่กรมราชทัณฑ์ล้มเหลว มีความเสี่ยงที่จะลุกลามไปยังหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

๒๒.๑.๕ การเรียนรู้จากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๑) ต้องบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย จุดอ่อนช่องโหว่ ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้น และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

๒) ต้องจัดทำสรุปรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัยให้รับทราบพร้อมข้อเสนอแนะแนวทางการปรับปรุงแก้ไขและระยะเวลาในการดำเนินการอย่างน้อยเดือนละ ๑ ครั้ง

๒๒.๑.๖ การเก็บรวบรวมหลักฐาน

๑) ต้องกำหนดให้มีการรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์ สำหรับการเก็บหลักฐานอ้างอิงในการวิเคราะห์สืบสวนหรือเป็นหลักฐาน ในกระบวนการทางศาลที่เกี่ยวข้องเมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้น มีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

๒) ส่วนงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูล เพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบหรือข้อบังคับที่ได้กำหนดไว้โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล และกฎหมาย เช่น ๙๐ วัน หรือ ๑ ปี

๓) ต้องศึกษาถึงลักษณะของหลักฐานที่มีความสมบูรณ์และมีคุณภาพ เพื่อสามารถนำไปใช้ในกระบวนการของศาลได้