นโยบายและแนวทางปฏิบัติ การรักษาความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Policy)

ศูนย์เทคโนโลยีสารสนเทศ กรมราชทัณฑ์

(ฉบับปรับปรุงปี พ.ศ. ๒๕๖๙)

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 มีความมั่นคงปลอดภัยป้องกันการถูกบุกรุกหรือ ถูกโจมตี ตลอดจนช่วยให้ระบบงานของหน่วยงานสามารถฟื้นฟูระบบอย่างรวดเร็วภายหลังจากภัยคุกคามได้สิ้นสุดลง ทั้งนี้ เพื่อให้หน่วยงานในสังกัดสามารถนำไปใช้เป็นแนวทางในการปฏิบัติงาน การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ การเฝ้าระวัง ป้องกัน และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นระบบ ตลอดจนสนับสนุนการคุ้มครองข้อมูลสารสนเทศ ข้อมูลสำคัญของทางราชการ ข้อมูลส่วนบุคคลให้มีความถูกต้อง ครบถ้วน พร้อมใช้งาน สามารถรองรับการเปลี่ยนแปลงทางเทคโนโลยีภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้อย่างเหมาะสมและมีประสิทธิภาพต่อไป

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

๒.๔ เพื่อกำหนดกรอบการใช้งานและควบคุมเทคโนโลยีอุบัติใหม่ (Emerging Technologies) รวมถึงระบบปัญญาประดิษฐ์ (Artificial Intelligence: AI) และระบบการประมวลผลบนคลาวด์ (Cloud Computing) ภายในหน่วยงาน ให้เป็นไปอย่างปลอดภัย ไร้ความเสี่ยงต่อการรั่วไหลของข้อมูลชั้นความลับ ข้อมูลผู้ต้องขัง หรือข้อมูลส่วนบุคคล ตลอดจนป้องกันภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ที่ใช้เทคโนโลยีขั้นสูงในการโจมตีองค์กร

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

ลำดับ	คำศัพท์	ความหมาย
๑๐	เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)	กรณีระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์ อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
๑๑	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจ คาดคิดซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
๑๒	ระบบอินเทอร์เน็ต (Internet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล
๑๓	ระบบอินทราเน็ต (Intranet)	ระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และสารสนเทศภายในหน่วยงาน
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)	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงกันข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร 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

ลำดับ	คำศัพท์	ความหมาย
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)
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 - ส่ง ผ่านเครือข่าย อินเทอร์เน็ตทาให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้น ไปจนถึงปลายทาง
๒๘	แผนผังระบบเครือข่าย (Network Diagram)	แผนผังซึ่งแสดงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน
๒๙	เครื่องแม่ข่าย (Server)	เครื่องหรือโปรแกรมคอมพิวเตอร์ซึ่งทำงานให้บริการในระบบเครือข่าย แก่ลูกข่าย

ลำดับ	คำศัพท์	ความหมาย
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
๓๖	ข้อมูลจราจรทาง คอมพิวเตอร์ (Log)	ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึง แหล่งกำหนด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลาและ ชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบ คอมพิวเตอร์
๓๗	IDS (Intrusion Detection System)	ระบบตรวจจับการบุกรุกเป็นเครื่องมือรักษาความปลอดภัยรองจากไฟร์วอลล์ใช้ในการตรวจจับความพยายามในการบุกรุกเครือข่าย 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	เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลนใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ ซึ่งเครื่องคอมพิวเตอร์แต่ละ เครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ
๔๑	Recovery Time Objective (RTO)	ระยะเวลาในการกู้คืนระบบ

ลำดับ	คำศัพท์	ความหมาย
๔๒	Recovery Point Objective (RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
๔๓	Maximum Tolerance Period of Disruption (MTPD)	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่างๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
๔๔	Business Continuity Plan	แผนบริหารความต่อเนื่องทางธุรกิจ
๔๕	AI (Artificial Intelligence)	ภาษาไทยใช้คำว่า “ปัญญาประดิษฐ์” หมายถึง ระบบประมวลผลของคอมพิวเตอร์ หุ่นยนต์ เครื่องจักร หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ที่มีการวิเคราะห์เชิงลึกคล้ายความฉลาดของมนุษย์ และสามารถก่อให้เกิดผลลัพธ์ที่เป็นการกระทำได้
๔๖	Cloud Computing	การให้บริการทรัพยากรด้านคอมพิวเตอร์ เช่น ระบบประมวลผล พื้นที่จัดเก็บข้อมูล ระบบเครือข่าย และซอฟต์แวร์ ผ่านเครือข่ายอินเทอร์เน็ต โดยผู้ใช้สามารถเรียกใช้ทรัพยากรได้ตามความต้องการ และชำระค่าบริการตามการใช้งาน

๕. นโยบายอุปกรณ์แบบพกพา (Mobile device policy)

นโยบายและมาตรการสนับสนุนสำหรับการใช้งานอุปกรณ์แบบพกพาจะต้องมีการนำมาใช้งานเพื่อบริหารจัดการความเสี่ยงจากการใช้อุปกรณ์แบบพกพาโดยจะต้องดำเนินการ ดังนี้

๕.๑ อุปกรณ์สื่อสารประเภทพกพาจะต้องได้รับการอนุญาตจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศแล้วเท่านั้น จึงจะสามารถเข้าถึงข้อมูลสารสนเทศของกรมราชทัณฑ์ ได้

๕.๒ อุปกรณ์สื่อสารประเภทพกพาจะต้องมีวิธีในการตรวจสอบเพื่อพิสูจน์ตัวตนขั้นต่ำเป็นอย่างน้อย โดยการใส่รหัสผ่านตามแนวปฏิบัติการบริหารจัดการรหัสผ่าน (Password Management)

๕.๓ ไม่ควรเก็บข้อมูลสำคัญของ กรมราชทัณฑ์ ไว้บนอุปกรณ์สื่อสารประเภทพกพาแต่ถ้ามีความจำเป็น ที่ต้องจัดเก็บบนอุปกรณ์สื่อสารประเภทพกพาจะต้องมีการเข้ารหัสข้อมูลตามแนวทางการ เข้ารหัสของกรมราชทัณฑ์

๕.๔ ต้องป้องกันข้อมูลและสารสนเทศที่กำหนดชั้นความลับมิให้ถูกเปิดเผยไปสู่ผู้อื่น

๕.๕ ข้อมูลที่มีชั้นความลับซึ่งถูกจัดเก็บไว้บนอุปกรณ์สื่อสารประเภทพกพาหรือถูกส่งผ่านเครือข่ายไร้สายที่ต้องส่งออกไปนอก กรมราชทัณฑ์ ต้องได้รับการอนุมัติจากเจ้าของข้อมูลและเข้ารหัสข้อมูล ก่อนเท่านั้น ไม่ควรเคลื่อนย้ายโดยบุคคลที่ไม่ใช่เจ้าของข้อมูล เว้นเสียแต่จะได้รับการอนุญาต เป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและจะต้องกำหนดให้มีการทำลายเมื่อไม่มีการ ใช้งานแล้ว

๕.๖ ระบบคอมพิวเตอร์อื่นที่ต้องการเชื่อมต่อกับระบบของ กรมราชทัณฑ์ จะต้องได้รับการอนุมัติเป็น ลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านเครือข่ายระบบสารสนเทศ

๕.๗ ต้องมีการรักษาความปลอดภัยทางกายภาพร่วมด้วย เช่น จะต้องปิดห้องทำงานเมื่อไม่มีบุคคลที่ได้รับอนุญาตอยู่ประจำโต๊ะทำงานและชั้นเก็บเอกสารต่าง ๆ จะต้องล็อคอย่างดี

๕.๘ กรณีที่อุปกรณ์สื่อสารประเภทพกพาเป็นสมบัติของกรมราชทัณฑ์ การคืนเครื่องหรือส่งซ่อม ให้ผู้ใช้งานทำสำเนาข้อมูลจากอุปกรณ์สื่อสารประเภทพกพาเก็บไว้ทั้งหมดและลบข้อมูล ทั้งหมดที่มีอยู่บนอุปกรณ์สื่อสารประเภทพกพาก่อนส่งซ่อม

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

๕.๑๐ การเข้าถึงและใช้ข้อมูลสารสนเทศ ซึ่งรวมถึงชั้นความลับของผู้ใช้งานเป็นอันสิ้นสุดลงทันทีเมื่อผู้ใช้งานพ้นสภาพตามสิทธิ์ของผู้ใช้งาน

๕.๑๑ กรมราชทัณฑ์ อาจดำเนินการทางวินัย แพ่ง หรืออาญา กับผู้ที่ล่วงละเมิดการเข้าถึงล่วงละเมิดใช้งาน หรือล่วงละเมิดเผยแพร่ข้อมูลสารสนเทศที่เป็นความลับโดยที่ผู้นั้นไม่มีสิทธิ์อันชอบ

๖. นโยบายการปฏิบัติงานจากระยะไกล (Teleworking Policy)

นโยบายและมาตรการสนับสนุนสำหรับการปฏิบัติงานจากภายนอกต้องมีการนำมาใช้งานเพื่อป้องกัน ข้อมูลที่มีการเข้าถึงการประมวลผลหรือการจัดเก็บจากกรมราชทัณฑ์ โดยจะต้องดำเนินการดังนี้

๖.๑ ในกรณีที่มีการบริหารจัดการระบบสารสนเทศจากภายนอกกรมราชทัณฑ์ หน่วยงานที่รับผิดชอบต้อง ปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยระบบสารสนเทศสำหรับหน่วยงานภายนอก โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิ์ที่ได้รับและมีการตรวจสอบการใช้งาน อย่างสม่ำเสมอ

๖.๒ ไม่อนุญาตให้ใช้งาน Remote Access สำหรับการปฏิบัติงานภายใต้ขอบเขตการดำเนินงานของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ เว้นแต่กรณีเกิดเหตุฉุกเฉินหรือเกิด เหตุการณ์ภัยพิบัติที่มีความจำเป็นต้องให้มีการปฏิบัติงานจากภายนอกเท่านั้น 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

(๑) นโยบายควบคุมการเข้าถึง (Access control policy) นโยบายควบคุมการเข้าถึงต้องมีการดำเนินการดังนี้

(๑.๑) กำหนดให้มีการควบคุมการเผยแพร่ข้อมูลและการให้สิทธิ์ เช่น หลักการความจำเป็นที่ต้องรู้ (Need to know), ระดับของความปลอดภัยและการจัดระดับชั้นการเข้าถึงข้อมูล

(๑.๒) ควบคุมการจัดการสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญทุกระบบ

(๑.๓) การแบ่งแยกการควบคุมการเข้าถึง เช่น การร้องขอเข้าถึงการให้สิทธิ์การเข้าถึง การบริหารการเข้าถึง

(๑.๔) ต้องมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้งทุกระบบสารสนเทศที่มีความสำคัญ

(๑.๕) ต้องถอดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศเมื่อบุคลากรพ้นสภาพ โยกย้าย เปลี่ยนผู้รับผิดชอบ หรือมีการปรับเปลี่ยนอย่างมีนัยสำคัญ

(๑.๖) ควบคุมการกำหนดหน้าที่ของผู้มีสิทธิ์เข้าถึงด้วยสิทธิพิเศษ และมีการตรวจสอบหรือ ทบทวนการใช้งานสิทธิ์พิเศษอย่างสม่ำเสมอหรืออย่างน้อยปีละ ๑ ครั้ง

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

(๒.๑) การกำหนดเครือข่าย และบริการเครือข่ายที่อนุญาตให้เข้าถึง

(๒.๒) ขั้นตอนให้สิทธิ์ที่อนุญาตให้เข้าถึงเครือข่าย และบริการเครือข่าย

(๒.๓) การควบคุมการจัดการ และขั้นตอนเพื่อป้องกันการเชื่อมต่อเครือข่ายและบริการ เครือข่าย

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

(๒.๕) ระบบเครือข่ายที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอก ต้องมีการใช้อุปกรณ์ หรือซอฟต์แวร์ในการทำ Packet Filtering เช่น การใช้ Firewall หรือฮาร์ดแวร์ อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

๗.๒ การบริหารจัดการการเข้าถึงด้านระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

(๑) การลงทะเบียนและถอดถอนผู้ใช้งาน (User registration and deregistration) ขั้นตอนการจัดการรหัสผู้ใช้งานจะต้องดำเนินการดังต่อไปนี้

(๑.๑) ต้องใช้รหัสผู้ใช้งานที่ไม่ซ้ำกันเพื่อให้ผู้ใช้งานรับผิดชอบสำหรับการดำเนินการของตน

(๑.๒) ยกเลิกการใช้งาน หรือถอดถอนรหัสผู้ใช้งานของคนที่ลาออก โยกย้าย หรือเปลี่ยนแปลงความรับผิดชอบอย่างทันท่วงทีในวันที่มีผลหรือก่อนวันที่มีผลหากไม่มีความจำเป็นต้องใช้งานแล้ว

(๑.๓) ควรกำหนดรอบในการยกเลิกการใช้งานหรือถอดถอนรหัสผู้ใช้งาน

(๑.๔) ควรมีการกำหนดให้มีการทบทวนรหัสผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

(๑.๕) กำหนดให้มีการตรวจสอบ กรณีรหัสผู้ใช้งานแต่ไม่มีการใช้งานนานมากกว่า ๙๐ วัน ให้ดำเนินการระงับรหัสผู้ใช้งานชั่วคราวทันที จนกว่าผู้ใช้งานจะร้องขอ และหากหลังจากระงับรหัสผู้ใช้งานชั่วคราวแล้วจนครบ ๓๐ วัน ถ้ายังไม่มีการร้องขอจากผู้ใช้งานให้ดำเนินการอีกให้ลบชื่อ-รหัสผู้ใช้งานนั้นถาวรทันที และผู้ดูแลระบบสารสนเทศต้องทำการเก็บบันทึกข้อมูลผู้ใช้งานดังกล่าวไว้ด้วย เพื่อตรวจสอบระบบว่ามีผลกระทบเสียหายเกิดขึ้นหรือไม่

(๒) การจัดเตรียมการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน (User access provisioning) ขั้นตอนการจัดเตรียมการเข้าถึงของผู้ใช้งานจะต้องดำเนินการดังนี้

(๒.๑) ได้รับสิทธิ์จากเจ้าของระบบเทคโนโลยีสารสนเทศ ก่อน จึงจะสามารถใช้งานในระบบได้

(๒.๒) ต้องตรวจสอบว่าระดับของการเข้าถึงที่ได้รับเหมาะสมกับนโยบายการเข้าถึงและสอดคล้องกับข้อกำหนดอื่น เช่น การแบ่งแยกหน้าที่ (Segregation of duties)

(๒.๓) ต้องมั่นใจว่าสิทธิ์การเข้าถึงไม่ได้ถูกเปิดใช้งานก่อนที่ขั้นตอนการให้สิทธิ์จะเสร็จสมบูรณ์

(๒.๔) การบันทึกที่ส่วนกลางของการให้สิทธิ์การเข้าถึงสำหรับรหัสผู้ใช้งานที่เข้าถึงระบบสารสนเทศและบริการ

(๒.๕) ปรับเปลี่ยนสิทธิ์การเข้าถึงของผู้ใช้งานที่เปลี่ยนหน้าที่ หรืองานที่รับผิดชอบและถอดถอนสิทธิ์การเข้าถึงของผู้ใช้งานทันทีที่ลาออกหรือโยกย้าย

(๒.๖) มีการทบทวนสิทธิ์การเข้าถึงตามรอบกับเจ้าของระบบสารสนเทศหรือบริการหรืออย่างน้อยปีละ ๑ ครั้ง

(๓) การบริหารจัดการสิทธิ์การเข้าถึงตามระดับพิเศษ (Management of privileged access rights) ขั้นตอนการบริหารจัดการสิทธิ์การเข้าถึงตามระดับพิเศษ จะต้องดำเนินการดังนี้

(๓.๑) การกำหนดสิทธิ์การเข้าถึงระดับพิเศษของระบบปฏิบัติการ ระบบการจัดการฐานข้อมูล และแอปพลิเคชัน ต้องได้รับการควบคุมเป็นพิเศษ และระบุตัวตนของผู้ที่ใช้งานด้วย

(๓.๒) สิทธิ์การเข้าถึงระดับพิเศษควรจัดสรรให้กับผู้ใช้งานตามความจำเป็นในการใช้งาน

(๓.๓) การให้สิทธิ์และบันทึกของการแจกจ่ายสิทธิ์การเข้าถึงระดับพิเศษทั้งหมดต้องได้รับการควบคุมการใช้งาน

(๓.๔) กำหนดระยะเวลาในการใช้งานสิทธิ์การเข้าถึงระดับพิเศษ

(๓.๕) สิทธิ์การเข้าถึงระดับพิเศษควรถูกกำหนดให้กับผู้ใช้งานสำหรับงานที่เกี่ยวข้องกับ ระบบเท่านั้น และการทำงานทั่วไปควรดำเนินการด้วยรหัสผู้ใช้งานที่มีสิทธิ์ในระดับ ปกติ

(๓.๖) การใช้งานด้วยสิทธิ์การเข้าถึงระดับพิเศษควรทบทวนอย่างสม่ำเสมอเพื่อตรวจสอบว่า ได้มีการใช้งานที่เหมาะสมตรงตามวัตถุประสงค์ของการใช้งาน

(๓.๗) กำหนดให้มีการทบทวนสิทธิ์พิเศษอย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง

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

(๔.๑) ผู้ใช้งานควรลงนามในรายงานเพื่อเก็บข้อมูลความลับสำหรับการพิสูจน์ โดยการลงนามให้รวมข้อกำหนด และเงื่อนไขของของการจ้างงานด้วย

(๔.๒) เมื่อผู้ใช้งานต้องการจัดเก็บข้อมูลความลับสำหรับการพิสูจน์ตัวตนของตนเอง ผู้ใช้งานควรได้รับข้อมูลความลับสำหรับการพิสูจน์ตัวตนชั่วคราวที่ปลอดภัยในขั้นต้นซึ่งผู้ใช้งานจะถูกบังคับให้เปลี่ยนเมื่อใช้งานในครั้งแรก

(๔.๓) ควรมีการกำหนดขั้นตอนเพื่อตรวจสอบตัวตนของผู้ใช้งานก่อนที่จะให้ข้อมูลความลับสำหรับการพิสูจน์ตัวตนที่ขอใหม่ ทดแทน หรือชั่วคราว

(๔.๔) ข้อมูลความลับสำหรับการพิสูจน์ตัวตนชั่วคราวควรมอบให้แก่ผู้ใช้งานในลักษณะที่ ปลอดภัย ไม่อนุญาตให้ใช้บุคคลภายนอกส่ง หรือข้อความผ่านมือถือหรืออีเมล ที่ไม่มีการป้องกัน

(๔.๕) ข้อมูลความลับสำหรับการพิสูจน์ตัวตนชั่วคราวต้องเป็นข้อมูลเฉพาะบุคคลและรหัสผ่านต้องไม่คาดเดาได้ง่าย

(๔.๖) ข้อมูลความลับสำหรับการพิสูจน์ตัวตนของเจ้าของผลิตภัณฑ์ที่เป็นค่าเริ่มต้นต้องถูกปรับเปลี่ยนหลังจากการติดตั้งระบบหรือซอฟต์แวร์เรียบร้อยแล้วอย่างทันท่วงที

(๕) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights) ขั้นตอนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานจะต้องดำเนินการ ดังนี้

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

(๕.๒) สิทธิ์การเข้าถึงของผู้ใช้งานควรได้รับการทบทวนและปรับเปลี่ยนเมื่อมีการย้ายตำแหน่งภายในกรมราชทัณฑ์

(๕.๓) สิทธิ์การเข้าถึงระดับพิเศษควรได้รับการทบทวนตามรอบที่ได้กำหนดไว้อย่างสม่ำเสมอ หรืออย่างน้อยปีละ ๑ ครั้ง และหลังจากการเปลี่ยนแปลง เช่น การเลื่อนตำแหน่ง การลดตำแหน่ง การลาออก การโยกย้าย การเปลี่ยนความรับผิดชอบ

(๕.๔) การได้รับสิทธิ์ระดับพิเศษควรมีการตรวจสอบเป็นประจำเพื่อให้มั่นใจว่าไม่มีผู้ใช้งานที่ไม่ได้รับอนุญาตได้รับสิทธิ์ระดับพิเศษ

(๕.๕) การเปลี่ยนแปลงบัญชีผู้ในงานระดับพิเศษต้องได้รับการบันทึกและมีการทบทวนตามรอบการเปลี่ยนแปลง

(๖) การถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงของผู้ใช้งาน (Removal or adjustment of access right) ขั้นตอนการถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงของผู้ใช้งานจะต้องดำเนินการดังนี้

(๖.๑) เมื่อสิ้นสุดการจ้างงานต้องมีการถอน หรือระงับสิทธิ์การเข้าถึงของผู้ใช้งานที่เกี่ยวข้องกับข้อมูลและทรัพย์สิน

(๖.๒) สิทธิ์การเข้าถึงต้องถูกถอนออก หรือ ปรับเปลี่ยนทั้งทางกายภาพ และลอจิคัล

(๖.๓) เอกสารใด ๆ ที่ระบุสิทธิ์การเข้าถึงของเจ้าหน้าที่และบุคคลภายนอกจะต้องถูกถอนออก หรือปรับเปลี่ยน ทันทีที่ลาออก หรือ หมดสัญญาจ้าง ในกรณีที่ผู้ใช้งาน เป็นบุคคลภายนอกและทราบรหัสผ่านสำหรับบัญชีผู้ใช้งานที่ยังใช้งานอยู่ต้องเปลี่ยนรหัสผ่านทันทีที่สิ้นสุดการจ้างงาน หรือหมดสัญญา

๗.๓ ความรับผิดชอบของผู้ใช้งาน

(๑) การใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตน (Use of secret authentication information) ขั้นตอนการใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตนจะต้องดำเนินการดังนี้

(๑.๑) ผู้ใช้งานต้องจัดเก็บข้อมูลความลับสำหรับการพิสูจน์ตัวตนไว้เป็นความลับ ต้องมั่นใจว่าไม่ได้เปิดเผยข้อมูลดังกล่าวต่อคนอื่น

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

(๑.๓) เปลี่ยนข้อมูลความลับสำหรับการพิสูจน์ตัวตน เมื่อมีข้อบ่งชี้ว่ามีภัยคุกคาม

(๑.๔) เมื่อรหัสผ่านถูกใช้เป็นข้อมูลความลับสำหรับการพิสูจน์ตัวตน ให้เลือกรหัสผ่านที่มีคุณภาพตามข้อ ๗.๔ (๓)

(๑.๕) ต้องมั่นใจว่ามีการป้องกันรหัสผ่านอย่างเหมาะสมเมื่อใช้รหัสผ่านเป็นข้อมูลความลับ สำหรับการพิสูจน์ตัวตนในขั้นตอนการเข้าสู่ระบบแบบอัตโนมัติและในขั้นตอนการจัดเก็บ

๗.๔ การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน

(๑) ข้อกำหนดการเข้าถึงสารสนเทศ (Information Access Restriction) ขั้นตอนสำหรับข้อกำหนดการเข้าถึงสารสนเทศจะต้องดำเนินการดังนี้

(๑.๑) ต้องมีการจัดเตรียมหน้าจอหรือเมนูสำหรับควบคุมการเข้าถึงระบบ

(๑.๒) ควบคุมสิทธิ์การเข้าถึงของผู้ใช้งาน เช่น อ่าน, เขียน และลบเป็นต้น

(๑.๓) ควบคุมสิทธิ์การเข้าถึงของแอปพลิเคชันไม่ควรมีใครได้สิทธิ์กระทำใดๆ ได้ทั้งหมดในระบบ

(๑.๔) จัดเตรียมสิทธิ์การเข้าถึงทางกายภาพ และลอจิคัลสำหรับระบบและแอปพลิเคชันที่สำคัญๆ

(๒) ขั้นตอนในการเข้าสู่ระบบอย่างปลอดภัย (Secure log-on procedure) ขั้นตอนในการเข้าสู่ระบบอย่างปลอดภัยจะต้องดำเนินการ ดังนี้

(๒.๑) ไม่แสดงข้อมูล เช่น ชื่อ, รุ่น, ไอพีแอดเดรสของระบบ หรือแอปพลิเคชันจนกว่าจะมีการเข้าสู่ระบบจนกว่าจะเสร็จสิ้นสมบูรณ์

(๒.๒) ต้องไม่แสดงข้อความเพิ่มเติมระหว่างเข้าสู่ระบบซึ่งอาจช่วยให้ผู้ที่ไม่ได้รับอนุญาตเข้าสู่ระบบได้

(๒.๓) ตรวจสอบความถูกต้องของข้อมูลนำเข้าเฉพาะเมื่อการเข้าสู่ระบบเสร็จสิ้นสมบูรณ์แล้ว ถ้ามีความผิดพลาดระบบไม่ควรแสดงว่าข้อมูลนำเข้าส่วนไหนไม่ถูกต้อง

(๒.๔) จำกัดจำนวนครั้งของการพยายามเข้าสู่ระบบ เช่น ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง และหลังการเข้าสู่ระบบผิดพลาดให้บังคับระยะเวลาทิ้งช่วง เช่น ๑๕ นาที ก่อนที่จะยอมให้เข้าสู่ระบบอีกครั้งขึ้นอยู่กับระบบสารสนเทศที่มีความสำคัญต่อการให้บริการ

(๒.๕) ตัดการใช้งานของผู้ใช้งานที่ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่ง เช่น ๓๐ นาที โดยเฉพาะในพื้นที่ที่ความเสี่ยงสูง เช่น เครือข่ายสาธารณะหรือเครือข่ายภายนอกของกรมราชทัณฑ์ หรือบนอุปกรณ์เคลื่อนที่

(๓) ระบบบริหารจัดการรหัสผ่าน (Password Management System) ขั้นตอนในการเข้าสู่ระบบอย่างปลอดภัยจะต้องดำเนินการดังนี้

(๓.๑) บังคับการใช้รหัสผู้ใช้งาน และรหัสผ่านให้ใช้งานสำหรับแต่ละบุคคลเท่านั้น

(๓.๒) บังคับใช้รหัสผ่านที่มีคุณภาพ โดยมีรายละเอียดดังนี้

(๑) ต้องมีความยาวมากกว่าหรือเท่ากับ ๘ ตัวอักษร เป็นอย่างน้อย

(๒) ต้องมีส่วนประกอบของอักษรตัวเล็ก ตัวใหญ่ อักขระพิเศษ และตัวเลขประกอบกัน

(๓) บังคับผู้ใช้งานให้เปลี่ยนรหัสผ่านในการเข้าสู่ระบบครั้งแรก

(๔) บังคับให้เปลี่ยนรหัสผ่านตามรอบ เช่น ทุก ๖๐ วัน, ทุก ๙๐ วัน เป็นต้น

(๕) ไม่แสดงรหัสผ่านบนหน้าจอที่ผู้ใช้งานกำลังป้อนข้อมูล

(๗) จัดเก็บไฟล์รหัสผ่านแยกจากข้อมูลทั่วไปของแอปพลิเคชัน

(๘) รหัสผ่านต้องไม่ง่ายต่อการคาดเดา เช่น ไม่ตั้งรหัสผ่าน ๑๒๓๔ abcd

(๙) ต้องไม่บันทึกรหัสผ่านในระบบความจำของโปรแกรม

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs) ขั้นตอนในการใช้งานโปรแกรมอรรถประโยชน์จะต้องดำเนินการ ดังนี้

(๔.๑) ใช้โปรแกรมอรรถประโยชน์ต้องมีการระบุตัวตนพิสูจน์ตัวตนและการควบคุมสิทธิ์ของผู้ใช้งาน

(๔.๒) จำกัดการใช้งานของโปรแกรมอรรถประโยชน์ตามขั้นต่ำที่ต้องใช้งานสำหรับผู้ใช้งานที่ได้รับอนุญาตให้ใช้งาน

(๔.๓) การขอใช้งานโปรแกรมอรรถประโยชน์แบบเฉพาะกิจ (ad hoc) ต้องได้รับการอนุมัติจากศูนย์เทคโนโลยีสารสนเทศก่อนทุกครั้ง

(๔.๔) ต้องมีการจำกัดสิทธิ์ในการใช้งานโปรแกรมอรรถประโยชน์ตามความจำเป็นและเหมาะสม

(๔.๕) ต้องมีการบันทึกประวัติการใช้งานของโปรแกรมอรรถประโยชน์

(๔.๖) ต้องจัดทำเอกสารระดับการให้สิทธิ์ในการเข้าถึงโปรแกรมอรรถประโยชน์

(๔.๗) ต้องดำเนินการยกเลิกโปรแกรมอรรถประโยชน์ที่ไม่ได้ใช้งานหรือไม่จำเป็น

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

(๕.๑) ต้องไม่เก็บ Source Code Library ไว้บนระบบที่ใช้งานจริง (Production System)

(๕.๒) การเข้าถึง Source code ต้องจำกัดสิทธิ์ให้เฉพาะผู้ใช้งานที่จำเป็นเช่น โปรแกรมเมอร์หรือผู้มีสิทธิ์เฉพาะหน้าที่ที่ได้รับมอบหมายเท่านั้น

(๕.๓) ระหว่างการทดสอบต้องไม่เก็บ Source code ที่ใช้ทดสอบร่วมกับที่ใช้งานจริง

(๕.๔) ต้องจัดเก็บ Source code ในสภาพแวดล้อมที่ปลอดภัย

(๕.๕) ต้องมีการบันทึกประวัติการเข้าถึง Source code

(๕.๖) การเปลี่ยนแปลงหรือแก้ไข Source code ต้องได้รับการอนุมัติจากศูนย์เทคโนโลยีสารสนเทศก่อนเสมอ

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

๘.๑ การใช้มาตรการเข้ารหัสข้อมูลจะต้องดำเนินการ ดังนี้

(๑) กำหนดวิธีการเข้ารหัสข้อมูลตามมาตรฐานสากล

(๒) อัลกอริทึมที่ใช้ในการเข้ารหัสต้องมีความปลอดภัย

(๒.๑) การเข้ารหัสแบบสมมาตรควรกำหนดให้ใช้อัลกอริทึมที่มีความปลอดภัย เช่น AES-๑๒๘, AES-๒๕๖

(๒.๒) การเข้ารหัสแบบอสมมาตรควรกำหนดให้ใช้อัลกอริทึมที่มีความปลอดภัย เช่น RSA๒๐๔๘

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

(๓) โปรโตคอลที่ใช้สื่อสารต้องมีความปลอดภัย

(๓.๑) การใช้งานผ่านเว็บ HTTPS ควรใช้งานโปรโตคอล SSL/TLS ที่เป็น TLS ๑.๒, ๑.๓ ขึ้นไปหรือตามมาตรฐานสากล ณ ช่วงเวลานั้น

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

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

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

(๔) ต้องมีการทบทวนมาตรฐานของการเข้ารหัสในทุกๆ ปีเพื่อให้สอดคล้องกับความปลอดภัยตามมาตรฐานสากล ณ ช่วงเวลานั้น

๙. นโยบายการบริหารจัดการกุญแจ (Key Management Policy)

๙.๑ การบริหารจัดการกุญแจจะต้องดำเนินการดังนี้

(๑) ข้อมูลที่ถูกเข้ารหัสต้องมีกระบวนการในการบริหารจัดการกุญแจอย่างมีประสิทธิภาพ โดยดำเนินการในขั้นตอนที่เกี่ยวข้องกับกุญแจทุกประเภท เช่น การสร้าง การจัดเก็บ การจัดส่ง การสำรอง การแจกจ่าย และการทำลาย ซึ่งต้องมีการควบคุมอย่างเหมาะสมและปลอดภัย

(๒) กุญแจลับ หรือ กุญแจส่วนตัวที่ใช้สำหรับการเข้ารหัสจะต้องถูกจัดเก็บไว้เป็นความลับและมีความปลอดภัยเสมอ

๑๐. นโยบายการควบคุมการเข้าถึงทางกายภาพ (Physical Control Policy)

๑๐.๑ การกำหนดความปลอดภัยของพื้นที่

(๑) พื้นที่ใช้งานระบบสารสนเทศ (Physical Security Perimeter)

(๑.๑) ต้องมีการจำแนกและกำหนดบริเวณพื้นที่ใช้งานระบบสารสนเทศตามที่ได้นิยามไว้ รวมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ เพื่อการเฝ้าระวังควบคุมและรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

(๑.๒) ต้องกำหนดการติดตั้งอุปกรณ์ในพื้นที่ใช้งานระบบสารสนเทศให้สอดคล้องกับความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

(๑.๓) หน่วยงานที่รับผิดชอบอุปกรณ์ที่สำคัญของระบบสารสนเทศ ต้องดำเนินการติดตั้งอุปกรณ์ในการรักษาความปลอดภัย เช่น กล้องวงจรปิด ระบบ Access Control หรืออุปกรณ์ที่สามารถ ป้องกันภัยคุกคามจากผู้บุกรุก ในพื้นที่ใช้งานระบบ สารสนเทศ ได้แก่ ศูนย์ปฏิบัติการ SOC ห้อง Server/Data Center ห้อง Network Control หรือห้อง Network Center ห้องเก็บข้อมูลสำรองเพื่อให้เป็นไปตามมาตรฐานสากลที่กำหนดไว้

(๑.๔) ไม่อนุญาตให้ถ่ายภาพบันทึกวิดีโอหรือเสียงภายในบริเวณที่ต้องมีความมั่นคงปลอดภัย ด้านสารสนเทศ (Secure Areas) เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

(๒) การควบคุมการ เข้า - ออก (Physical entry controls)

(๒.๑) ระบุตัวตนผู้ใช้งานและช่วงเวลาที่มีสิทธิ์ผ่าน เข้า-ออก ในแต่ละพื้นที่อย่างชัดเจน

(๒.๒) ผู้ใช้งานจะได้รับสิทธิ์ให้เข้า-ออก สถานที่ทำงานได้เฉพาะบริเวณที่ถูกกำหนด เท่านั้น

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

(๒.๔) ต้องขออนุญาตเข้ามาปฏิบัติงานในพื้นที่ให้ปฏิบัติตามขั้นตอนปฏิบัติการขอเข้าพื้นที่

(๓) ความปลอดภัยของสำนักงานห้องทำงานและเครื่องมือต่างๆ (Securing Offices, Rooms and Facilities)

(๓.๑) พื้นที่สำนักงานห้องทำงานและเครื่องมือต่างๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออก ของบุคคลทั่วไป

(๓.๒) พื้นที่สำนักงานจะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญในบริเวณดังกล่าว

(๓.๓) พื้นที่สำนักงานห้องทำงานและเครื่องมือต่างๆ ควรมีความปลอดภัย เช่น กั้นพื้นที่ อย่างรอบด้าน ติดตั้งผนังติดตั้งเหล็กดัดล็อคประตูที่ใช้ดอกกุญแจหรือมีระบบ Access Control

(๔) การป้องกันภัยคุกคามภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)

(๔.๑) พื้นที่สำนักงานที่มีระบบสำคัญจะต้องมีการควบคุมการเข้า - ออก อย่างเข้มงวดและตั้งอยู่ในพื้นที่ที่ปลอดภัยจากภัยทางธรรมชาติ เช่น แผ่นดินไหว หรือน้ำท่วม

(๔.๒) ต้องจะมีอุปกรณ์ดับเพลิงอย่างเพียงพอและเหมาะสม ทั้งนี้ในพื้นที่ที่ต้องมีการรักษาความปลอดภัยควรพิจารณาติดตั้งระบบดับเพลิงอัตโนมัติ

(๔.๓) ต้องดูแลเรื่องความสะอาดของพื้นที่โดยทั่วไปอย่างสม่ำเสมอเพื่อไม่ให้มีวัสดุที่เป็นเชื้อเพลิงอยู่ในพื้นที่ดังกล่าว

(๕) การปฏิบัติงานในพื้นที่ควบคุม (Working in Control Areas)

(๕.๑) ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวิดีโอในบริเวณควบคุม เป็นต้น

(๕.๒) ต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวิดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

(๖) การจัดเตรียมพื้นที่สำหรับส่งมอบ (Delivery and loading Areas)

(๖.๑) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอกเพื่อป้องกันการเข้าถึงทรัพย์สินโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ควรจัดเป็นบริเวณแยกออกมา

(๖.๒) ต้องจัดให้มีขั้นตอนการลงทะเบียนเพื่อบริหารจัดการทรัพย์สินที่ถูกส่งมอบ

๑๐.๒ การกำหนดความปลอดภัยของอุปกรณ์

(๑) การจัดวางและป้องกันอุปกรณ์ (Equipment siting and protection)

(๑.๑) ผู้ใช้งานต้องจัดตั้งเครื่องมือไว้ในสถานที่ที่ปลอดภัยรวมทั้งมีการป้องกันภัยหรืออันตรายที่อาจจะเกิดขึ้นกับอุปกรณ์เหล่านั้น

(๑.๒) มีการจัดเตรียมพื้นที่จัดเก็บอุปกรณ์ที่ปลอดภัยและไม่สามารถเข้าถึงได้โดยง่าย เช่น ตู้หรือลิ้นชักที่มีกุญแจล็อค

(๑.๓) ห้ามมิให้มีการสูบบุหรี่รับประทานอาหารและน้ำดื่มในพื้นที่จัดวางอุปกรณ์ของศูนย์เทคโนโลยีสารสนเทศ

(๑.๔) ห้ามนำสารเคมีและเครื่องมือที่อาจก่อให้เกิดอันตรายกับอุปกรณ์เข้ามาในบริเวณ พื้นที่ปฏิบัติงาน นอกจากได้รับการพิจารณาอนุญาตและตรวจสอบความเหมาะสมแล้วเท่านั้น

(๑.๕) ทำการติดตั้งระบบป้องกันฟ้าผ่ากับอาคารอย่างเหมาะสม

(๒) ระบบสาธารณูปโภคพื้นฐาน (Supporting utilities)

(๒.๑) ต้องมีระบบไฟฟ้าสำรองอัตโนมัติเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่องและต้องมีการตรวจสอบระบบไฟฟ้าสำรองและบำรุงรักษาตามความเหมาะสม

(๒.๒) ต้องจัดให้มีระบบเตือนภัย/ป้องกันภัย เช่น ระบบดับเพลิง ระบบเตือนอัคคีภัย

(๒.๓) ต้องมีการวางแผนและซักซ้อมการปฏิบัติรับมือกับภัยพิบัติ เช่น อัคคีภัย อย่าง น้อยปีละ ๑ ครั้ง

(๒.๔) ระบบที่สำคัญจะต้องมีการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจเพื่อลดความสูญเสียที่อาจเกิดขึ้นจากผลกระทบจากเหตุการณ์ภัยพิบัติหรือเหตุการณ์ไม่คาดคิด

(๓) ความปลอดภัยของสายเคเบิล (Cabling security)

(๓.๑) ต้องคำนึงถึงการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน เช่น ผ่านเข้ามาทางใต้ดินผ่านช่องพิเศษที่จัดไว้ หรือเป็นบริเวณที่บุคคลทั่วไปไม่สามารถเข้าถึงได้ง่าย

(๓.๒) ต้องจัดเก็บสายเคเบิลทั้งหมดที่ใช้ในการรับ-ส่งข้อมูลไว้ในรางหรืออุปกรณ์ป้องกันเพื่อป้องกันการดักจับข้อมูลหรืออุบัติเหตุที่อาจทำให้สายขาดหรือชำรุดได้

(๓.๓) ต้องแยกสายไฟทั้งหมดออกจากสายเคเบิลในการรับ - ส่งข้อมูล เพื่อป้องกันสัญญาณรบกวน

(๔) การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

(๔.๑) ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงปีละ ๑ ครั้งหรือระบบที่สำคัญมากอาจจะกำหนดให้มีการบำรุงรักษาทุก ๓ เดือน

(๔.๒) ทุกครั้งที่ต้องมีการซ่อมแซมอุปกรณ์ใดๆ จะต้องทำการบันทึกรายการซ่อมบำรุงรักษา อุปกรณ์ดังกล่าวทุกครั้ง

(๔.๓) ต้องบำรุงรักษาระบบควบคุมสภาพแวดล้อมและอุปกรณ์ต่างๆ ตามคำแนะนำที่ผู้ผลิตระบุไว้

(๔.๔) กำหนดให้บุคลากรที่ผ่านการฝึกอบรมและได้รับอนุญาตเท่านั้นที่จะสามารถทำการซ่อมบำรุงระบบและอุปกรณ์ต่างๆ

(๕) การนำทรัพย์สินออกนอกสถานที่ (Removal of assets)

(๕.๑) การเคลื่อนย้ายสินทรัพย์ต้องทำเป็นบันทึกและขออนุญาตอย่างถูกต้องในการเคลื่อนย้าย

(๕.๒) เมื่อมีการนำอุปกรณ์และสื่อที่เคลื่อนย้ายได้ออกไปใช้นอกสถานที่ผู้ที่รับผิดชอบต้องมีมาตรการการป้องกันการสูญหาย

(๕.๓) การเคลื่อนย้ายทรัพย์สินใดๆ จะต้องได้รับการอนุญาตลายลักษณ์อักษรและต้องมีการเก็บบันทึกการอนุญาตดังกล่าวไว้

(๕.๔) ต้องกำหนดระยะเวลาที่ต้องการยืมทรัพย์สินหรือเวลาที่จะทำการเคลื่อนย้ายทรัพย์สินและต้องบันทึกการเคลื่อนย้ายทรัพย์สินทุกครั้ง

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

(๖.๑) ปฏิบัติตามคำแนะนำในการใช้งานจากเจ้าของผลิตภัณฑ์ของอุปกรณ์และทรัพย์สินอย่างเคร่งครัด

(๖.๒) ไม่วางอุปกรณ์และทรัพย์สินไว้ในที่สาธารณะโดยขาด ต้องมีการดูแลหรือการเฝ้าระวัง

(๖.๓) ต้องกำหนดให้มีการป้องกันทรัพย์สินและอุปกรณ์ เช่น Notebook, Mobile Phone เมื่อถูกนำไปใช้งานนอกสำนักงาน

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

(๗.๑) ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ทั้งนี้เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว

(๗.๒) การทำลายหรือการนำอุปกรณ์กลับมาใช้ใหม่จะต้องถูกกำหนดขั้นตอนการดำเนินงานในการทำลายหรือการนำอุปกรณ์อิเล็กทรอนิกส์กลับมาใช้ใหม่เพื่อให้แน่ใจได้ว่าข้อมูลใดๆ ที่อยู่ในอุปกรณ์ ดังกล่าวได้ถูกลบทิ้งโดยที่ไม่สามารถกู้คืนกลับมาใช้ได้อีก

(๘) อุปกรณ์ที่ไม่อยู่ระหว่างการใช้งาน (Unattended user equipment)

(๘.๑) ต้องใช้งานซอฟต์แวร์พักหน้าจอโดยตั้งเวลาให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

(๘.๒) ต้องทำการออกจากโปรแกรมหรือบริการระบบเครือข่ายเมื่อไม่ใช้งาน

(๙) นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and Clear screen policy)

(๙.๑) ต้องไม่ทิ้งเอกสารหรือสื่อบันทึกข้อมูลและสารสนเทศที่เป็นข้อมูลความลับหรือลับมากไว้ในที่สามารถพบเห็นได้ง่าย โดยจัดเก็บไว้ในที่ที่ปลอดภัย นอกจากนี้ตู้จ่ายเอกสารหรือจดหมายและเครื่องโทรสารจะต้องได้รับการดูแลให้ปลอดภัยด้วย

(๙.๒) เมื่อสั่งพิมพ์งานเอกสารที่มีข้อมูลสำคัญผู้สั่งพิมพ์ต้องทำการจัดเก็บเอกสารโดยทันที

(๙.๓) อุปกรณ์คอมพิวเตอร์แม่ข่ายต้องล็อคหรือป้องกันหน้าจอและคีย์บอร์ดที่มีกลไกป้องกันด้วยรหัสผ่านโทเคนหรือกลไกลการพิสูจน์ตัวตนผู้ใช้งานเมื่อไม่ได้ใช้งาน

(๙.๔) สื่อที่มีข้อมูลอ่อนไหวหรือมีการระบุชั้นความลับไว้ต้องนำออกจากเครื่องถ่ายเอกสารอย่างทันที

๑๑. นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)

- ต้องปฏิบัติตามนโยบายข้อ **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

(๑) ต้องออกแบบขั้นตอนเพื่อป้องกันการถ่ายโอนข้อมูลจากการถูกดักจับ คัดลอก แก้ไข ส่งผิดเส้นทาง

(๒) ต้องมีขั้นตอนสำหรับการตรวจจับและป้องกันมัลแวร์ซึ่งอาจถูกส่งผ่านการสื่อสารทางอิเล็กทรอนิกส์

(๓) ต้องมีการป้องกันการส่งข้อมูลที่สำคัญด้วยวิธีการแนบเอกสาร

(๔) ผู้ใช้งานต้องรับผิดชอบในบทบาทหน้าที่ไม่ฝ่าฝืนนโยบายและแนวปฏิบัติเช่น การหมิ่นประมาท การข่มขู่หรือก่อกวนความสงบ การปลอมตัว การส่งต่อจดหมายลูกโซ่ การจัดซื้อจัดจ้างนอกเหนือการอนุมัติ

(๕) ต้องมีเทคนิคการเข้ารหัสเพื่อปกป้องความลับ ความสมบูรณ์และความถูกต้องของข้อมูล

(๖) ต้องมีแนวทางในการเก็บรักษาและทำลายสำหรับจดหมายธุรกิจต้องเป็นไปตามที่กฎหมายกำหนด

(๗) ต้องไม่ทิ้งเอกสารสำคัญไว้ที่เครื่องถ่ายเอกสารเครื่องพิมพ์หรือเครื่องโทรสาร ซึ่งผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้

(๘) ต้องควบคุมและยับยั้งการส่งต่อข้อมูลของอุปกรณ์สื่อสาร เช่น การส่งต่อเมลอัตโนมัติไปที่อยู่อีเมลนอกสำนักงาน

(๙) ต้องแนะนำและอบรมให้ความรู้ต่อผู้ใช้งานให้ใช้มาตรการที่เหมาะสมเพื่อป้องกันข้อมูลรั่วไหล

(๑๐) ต้องมีการควบคุมและตรวจสอบเครื่องโทรสารและเครื่องถ่ายเอกสารรุ่นใหม่ที่มีหน่วยความจำในการเก็บเอกสารบางหน้าหรือการส่งข้อมูลที่พิมพ์ผิดพลาด ซึ่งอาจจะถูกพิมพ์ออกมาเมื่อเครื่องทำงานได้ตามปกติ

๑๓.๒ ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ

(๑) ต้องมีการบริหารจัดการในการควบคุมและแจ้งให้ทราบเกี่ยวกับการสื่อสารการส่งและการรับข้อมูล

(๒) ต้องมีการแจ้งให้ผู้ส่งรับทราบเกี่ยวกับการสื่อสารการส่งและการรับข้อมูล

(๓) ต้องมีกระบวนการที่สามารถติดตามและปฏิเสธความรับผิดชอบไม่ได้

(๔) ต้องมีมาตรฐานทางเทคนิคขั้นต่ำในการสื่อสาร เช่น เอกสารมาตรฐานการเข้ารหัสแบบสมมาตรด้วย AES-๑๒๘, AES-๒๕๖ และการเข้ารหัสแบบอสมมาตรด้วย RSA๒๐๔๘

(๕) ต้องมีสัญญาข้อตกลง เช่น สัญญาระหว่าง กรมราชทัณฑ์ และผู้ให้บริการภายนอกที่จะมีการสื่อสาร ผ่านเครือข่ายที่ปลอดภัยและมีการเข้ารหัส

(๖) ต้องมีมาตรฐานในการระบุตัวผู้ส่งเอกสาร

(๗) ต้องใช้ระบบป้ายชื่อตามข้อตกลงสำหรับข้อมูลที่มีความสำคัญ เพื่อเข้าใจได้ทันทีในความหมายของป้ายชื่อและข้อมูลได้รับการปกป้องข้อมูลอย่างเหมาะสม

(๘) ต้องมีการควบคุมพิเศษที่จำเป็นในการปกป้องข้อมูลสำคัญ เช่น การเข้ารหัสแบบสมมาตรด้วย AES-๑๒๘, AES-๒๕๖ และการเข้ารหัสแบบอสมมาตรด้วย RSA๒๐๔๘

(๙) ต้องมีการควบคุมการเข้าถึงในระดับที่ยอมรับได้และปลอดภัย

๑๓.๓ การส่งข้อความทางอิเล็กทรอนิกส์

(๑) ต้องปกป้องข้อความจากผู้ที่ไม่ได้รับอนุญาตไม่ให้มีการแก้ไขข้อความหรือทำให้ระบบใช้งานไม่ได้

(๒) ต้องมั่นใจว่าที่อยู่ปลายทางและการส่งข้อความถูกต้อง

(๓) ต้องมีความน่าเชื่อถือและความสามารถในการให้บริการ

(๔) ต้องปฏิบัติตามข้อกำหนดทางกฎหมาย เช่น การใช้ลายมืออิเล็กทรอนิกส์

(๕) การใช้บริการแบบสาธารณะต้องระวังในการรับ–ส่งข้อมูลที่เป็นความลับ เช่น โปรแกรมแชท เครือข่ายสังคมออนไลน์ การแชร์ไฟล์

(๖) ต้องมีการระบุตัวตนในการควบคุมการเข้าถึงจากระบบเครือข่ายสาธารณะต้องปฏิบัติตามมาตรการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างเข้มงวด

๑๓.๔ ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ

(๑) ต้องจัดให้มีการลงนามในสัญญาการรักษาความลับหรือการไม่เปิดเผยความลับระหว่างผู้ใช้งาน และกรมราชทัณฑ์ว่าจะไม่เปิดเผยความลับของกรมราชทัณฑ์ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะทำงานและผูกพันอย่างต่อเนื่องเป็นเวลาไม่น้อยกว่า ๒ ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว พร้อมบทลงโทษ

(๒) บุคลากรที่ต้องลงนามในสัญญาการรักษาความลับหรือการไม่เปิดเผยความลับประกอบไปด้วย ข้าราชการ พนักงาน ลูกจ้าง และบุคลากรจากหน่วยงานภายนอกรวมถึงนักศึกษาฝึกงานทุกคน ซึ่งเป็นส่วนหนึ่งของเงื่อนไขและข้อกำหนดในการจ้างงานหรือการฝึกงานและจะต้องจัดเก็บหลักฐานการลงนามไว้ด้วย

๑๔. นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

๑๔.๑ ระบบสารสนเทศต้องได้รับการพัฒนาในสภาพแวดล้อมที่มีความมั่นคงปลอดภัยทั้งทางกายภาพและลอจิคัล เช่น สถานที่ที่ใช้ในการพัฒนาระบบต้องไม่สามารถเข้าถึงโดยผู้ไม่เกี่ยวข้องได้โดยง่าย

๑๔.๒ การพัฒนาระบบสารสนเทศต้องคำนึงถึงความมั่นคงปลอดภัยตลอดวงจรชีวิตของการพัฒนาซอฟต์แวร์ โดยครอบคลุมตั้งแต่ขั้นตอนการรวบรวมความต้องการ การออกแบบ การพัฒนา การทดสอบ การใช้งานตลอดไปจนถึงการยกเลิกการใช้งานระบบ

๑๔.๓ ขั้นตอนการพัฒนาระบบสารสนเทศต้องมีการกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ ดังต่อไปนี้

(๑) การป้องกันข้อมูลจากการถูกเปิดเผยโดยไม่ได้รับอนุญาต

(๒) การป้องกันข้อมูลจากการถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(๓) ความต้องการด้านความพร้อมใช้งานของข้อมูลและระบบสารสนเทศ

(๔) การพิสูจน์ตัวตนของผู้ใช้งานและผู้ดูแลระบบ

(๕) การจัดการสิทธิ์ในการใช้งานระบบ

(๖) ความต้องการในการตรวจสอบและจัดเก็บประวัติการใช้งานประวัติการเข้าถึง

(๗) การป้องกันการปฏิเสธการทำรายการ

(๘) การบริหารจัดการค่าการปรับแต่ง, เซสชั่นและการจัดการกับข้อผิดพลาดที่เกิดขึ้น

(๙) ความต้องการด้านสมรรถนะของระบบสารสนเทศ เช่น ความเร็วในการประมวลผลข้อมูล ความสามารถในการเก็บข้อมูล การประมวลผลในด้านภาพกราฟิก ขนาดหน่วยความจำ

(๑๐) ความต้องการด้านความมั่นคงปลอดภัยอื่นๆ ที่สอดคล้องกับข้อกำหนดกฎหมายหรือกฎระเบียบที่องค์กรต้องปฏิบัติตาม

๑๔.๔ ต้องกำหนดจุดทบทวนด้านความมั่นคงปลอดภัยในแต่ละระยะการดำเนินงานของโครงการ เช่น มีการกำหนดให้มีการสอบทานด้านความมั่นคงปลอดภัยในขั้นตอน การออกแบบ การพัฒนา การทดสอบ 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

(๑) เจ้าของสารสนเทศมีหน้าที่ในการกำหนดชั้นความลับของสารสนเทศตามกระบวนการจัดชั้นความลับของสารสนเทศภายใต้รับความผิดชอบของตน

(๒) การป้องกันสารสนเทศต้องพิจารณาทั้ง ๓ ด้าน คือ การรักษาความลับ การรักษา ความสมบูรณ์และความพร้อมใช้งาน

(๓) ข้อมูลหรือสารสนเทศให้หน่วยงานระบุชนิดลักษณะของข้อมูลให้ชัดเจนว่าเกี่ยวกับเรื่องใด มีความสำคัญอย่างไร และต้องมีการจัดลำดับชั้นความลับเป็นอย่างใดอย่างหนึ่งต่อไปนี้ เช่น ชั้นเปิดเผย ชั้นใช้ภายใน ชั้นลับ ชั้นลับมาก ชั้นลับที่สุด

(๔) ข้อมูลหรือสารสนเทศซึ่งมีการกำหนดชั้นความลับไว้ทั้งในกรณีทั้งหมดหรือบางส่วนให้ถือว่ามีชั้นความลับเดียวกันกับข้อมูลหรือสารสนเทศนั้นยกเว้นว่ามีการจัดลำดับชั้นความลับใหม่ โดยหน่วยงานเจ้าของข้อมูลหรือสารสนเทศนั้น

(๕) ต้องทำการจัดหมวดหมู่กำหนดชั้นความลับ และกำหนดระดับความสำคัญของเอกสารเพื่อป้องกันสารสนเทศให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดยให้ปฏิบัติตามกระบวนการการจัดระดับชั้นความลับข้อมูลและสารสนเทศ

(๖) ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การเก็บรักษาจนถึงการทำลายตามกระบวนการ การจัดระดับชั้นความลับข้อมูลและสารสนเทศ

๑๖.๒ การบ่งชี้สารสนเทศ

(๑) เจ้าหน้าที่และผู้ปฏิบัติงานตามสัญญาจ้างทุกคนต้องปฏิบัติตามขั้นตอนในการจัดทำป้ายชื่อสารสนเทศ

(๒) การจัดทำป้ายชื่อต้องสอดคล้องกับระดับชั้นความลับที่กำหนดไว้ในการจัดชั้นความลับสารสนเทศ

(๓) การจัดทำป้ายชื่อสารสนเทศต้องครอบคลุมสารสนเทศทั้งในรูปแบบที่เป็นกายภาพและอิเล็กทรอนิกส์

(๔) ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับสารสนเทศ โดยแยกตามหมวดหมู่ที่กำหนดไว้ มีการส่งมอบและจัดเก็บตามขั้นตอนกระบวนการต่างๆ ซึ่งประกอบไปด้วยการถ่ายเอกสาร การจัดเก็บ การส่งต่อ การสื่อสารและการทำลาย ให้ปฏิบัติตามแนวทางปฏิบัติของระเบียบปฏิบัติของทางราชการตามกฎหมายที่เกี่ยวข้อง

(๕) หากมีความจำเป็นจะต้องกำหนดระดับชั้นความลับของข้อมูลในสื่อบันทึกดังกล่าวเป็นระดับอื่นจะต้องติดป้ายชื่อให้กับสื่อบันทึกดังกล่าวให้สอดคล้องกับข้อมูลดังกล่าว

(๖) ข้อมูลทุกระดับชั้นจะต้องถูกส่งผ่านระบบอีเมลของกรมราชทัณฑ์เท่านั้น กรณีมีช่องทางอื่นๆ ที่มีความจำเป็นต้องใช้ส่งข้อมูลจะต้องได้รับอนุญาตจากศูนย์เทคโนโลนีสารสนเทศเพื่อพิจารณาถึงความปลอดภัยอย่างเหมาะสม

๑๖.๓ การจัดการทรัพย์สิน

(๑) กระบวนการปฏิบัติงานในการจัดการสินทรัพย์ต้องสอดคล้องและเป็นไปในทิศทางเดียวกับการจัดชั้นความลับสารสนเทศ

(๒) ต้องมีการจัดเก็บสินทรัพย์ตามรายละเอียดการจัดเก็บจากผู้ผลิต หากสินทรัพย์นั้นต้องการการจัดเก็บเป็นพิเศษ

๑๗. นโยบายการจัดการสื่อบันทึกข้อมูล (Media Handling policy)

๑๗.๑ การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้

(๑) ข้อมูลที่มีชั้นความลับ ชั้นความลับมาก ชั้นความลับที่สุด ต้องกำหนดให้มีการทำลายสื่อบันทึกข้อมูลเมื่อไม่มีการใช้งานแล้ว

(๒) ในกรณีที่สื่อบันทึกข้อมูลนั้นไม่ได้ถูกนำมาใช้งานแล้ว ก่อนที่จะนำออกไปจากกรมราชทัณฑ์ต้องมั่นใจว่าข้อมูลที่อยู่ในสื่อดังกล่าวไม่สามารถกู้คืนกลับมาใช้งานได้อีก

(๓) ในกรณีที่จำเป็นต้องนำสื่อบันทึกข้อมูลออกไป จะต้องได้รับการอนุมัติจากผู้ที่รับผิดชอบสื่อบันทึกข้อมูลดังกล่าว และต้องบันทึกการโยกย้าย เพื่อใช้ในการตรวจสอบภายหลัง

(๔) สื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูลตามข้อกำหนดของผู้ผลิต เช่น อุณหภูมิสูงหรือต่ำเกินไป

(๕) ในการจัดเก็บสื่อบันทึกข้อมูลที่สำคัญ ต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล เช่น มีการติดป้ายชื่อไว้ที่สื่อบันทึกอย่างชัดเจน กำหนดบุคลากรที่มีสิทธิ์ในการใช้งาน

(๖) ถ้าข้อมูลที่ต้องการจัดเก็บมีอายุการจัดเก็บยาวนานกว่าอายุการใช้งานของสื่อบันทึกข้อมูลควรจัดเก็บไว้ที่แหล่งอื่นเพื่อป้องกันการสูญหายของข้อมูล

(๗) ต้องจัดทำทะเบียนบันทึกข้อมูลของสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้เพื่อลดโอกาสการสูญหายของข้อมูล

๑๗.๒ การทำลายสื่อบันทึกข้อมูล

(๑) สื่อที่บันทึกข้อมูลที่มีความสำคัญมากจะต้องมีการทำลายด้วยวิธีการที่ปลอดภัย เช่น การเผาหรือแยกชิ้นส่วนเป็นชิ้นเล็กๆ หรือลบข้อมูลด้วยซอฟต์แวร์อื่นๆ ที่มีใช้ในกรมราชทัณฑ์

(๒) กระบวนการต่างๆ ต้องระบุวิธีการกำจัดสื่อบันทึกข้อมูลอย่างชัดเจนเพื่อความปลอดภัยของข้อมูล

(๓) เพื่อความสะดวกควรรวบรวมสื่อทั้งหมดที่ไม่ต้องการแล้วกำจัดพร้อมกันด้วยวิธีการที่ปลอดภัย

(๔) ในกรณีที่เลือกใช้บริการกำจัดสื่อและเอกสารรวมทั้งอุปกรณ์ต่างๆ จากหน่วยงานภายนอก ควรระมัดระวังในการเลือกใช้บริการ ต้องเลือกหน่วยงานภายนอกที่มีการควบคุมที่ดีมีมาตรฐานและมีประสบการณ์

(๕) ในการกำจัดสื่อบันทึกข้อมูลจะต้องมีการบันทึกเพื่อใช้ในการตรวจสอบ

๑๗.๓ การเคลื่อนย้ายสื่อบันทึกข้อมูล

(๑) ใช้วิธีการขนส่งหรือพนักงานส่งของที่เชื่อถือได้

(๒) รายชื่อของพนักงานส่งของหรือบริษัทส่งของควรได้รับการอนุมัติจากผู้มีอำนาจ

(๓) กระบวนการตรวจสอบพนักงานส่งของต้องมีการปรับปรุงอย่างสม่ำเสมอ

(๔) การบรรจุภัณฑ์ต้องป้องกันความเสียหายในระหว่างการขนส่งโดยเป็นไปตามข้อกำหนดของผู้ผลิต ตัวอย่างการป้องกันปัจจัยทางกายภาพที่จะมีผลต่อการกู้คืนข้อมูล เช่น ความร้อน, ความชื้น และสนามแม่เหล็ก

(๕) การควบคุมที่จำเป็นในการปกป้องข้อมูลสำคัญจากการเปิดเผยหรือแก้ไขโดยไม่ได้รับอนุญาต

(๕.๑) ใช้ตู้ที่มีกุญแจล็อค

(๕.๒) ส่งด้วยมือตนเองและลงบันทึกการรับเพื่อสามารถตรวจสอบได้

(๕.๓) บางกรณีอาจจะต้องใช้วิธีการแยกส่งออกหลายๆ ส่วนและหลายๆ เส้นทางเพื่อกระจายความเสี่ยง

๑๘. การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software)

๑๘.๑ การควบคุมการติดตั้งซอฟต์แวร์

(๑) ต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ซอฟต์แวร์อุดช่องโหว่ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดีว่าไม่ก่อให้เกิดปัญหาหรือผลกระทบต่อเครื่องที่ให้บริการอยู่

(๒) มีการบริหารจัดการเวอร์ชันของซอฟต์แวร์และมีการจัดเก็บซอฟต์แวร์เวอร์ชันก่อนหน้าไว้ในกรณีที่มีความจำเป็นต้องทำการถอยกลับไปใช้เวอร์ชันก่อนหน้านี้

๑๙. การบริหารจัดการช่องโหว่ (Technical Vulnerability Management)

๑๙.๑ การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์

(๑) ต้องกำหนดหน้าที่ความรับผิดชอบที่ชัดเจน เช่น การเฝ้าระวังภัยคุกคามการประเมินความเสี่ยงของภัยคุกคาม การแพตช์ปิดช่องโหว่ในระบบ การตรวจสอบสินทรัพย์ที่ได้จัดส่วนหมวดหมู่ไว้

(๒) ต้องร่วมกันวิเคราะห์ความเสี่ยงและประเมินสถานการณ์การบุกรุก ละเมิด ระบาดที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศอย่างสม่ำเสมอหรืออย่างน้อย ปีละ ๑ ครั้ง

(๓) ในกรณีที่จะทำการอัปเดทแพตช์ของระบบสำคัญๆ ต้องมีการทดสอบและประเมินก่อนว่าจะไม่ก่อให้เกิดความเสียหายหรือมีผลกระทบต่อระบบ แต่ถ้าไม่สามารถอัปเดตแพตช์ได้ก็ให้พิจารณาดังต่อไปนี้

(๓.๑) ปิด Service หรือ การทำงานที่เกี่ยวข้องกับช่องโหว่

(๓.๒) ปรับปรุงหรือเพิ่มระดับความปลอดภัยในการเข้าถึงที่บริเวณรอบนอกเครือข่าย เช่น เพิ่มอุปกรณ์ไฟร์วอลล์หรือ IPS (Intrusion Prevention System)

(๓.๓) เพิ่มการเฝ้าระวังเพื่อตรวจจับหรือป้องกันการโจมตีเครือข่ายอย่างเข้มงวด

(๓.๔) ต้องมีการสร้างความตระหนักเกี่ยวกับช่องโหว่ที่เกิดขึ้น

(๓.๕) ต้องเก็บ Log ของเหตุการณ์ที่เกิดขึ้นทั้งหมดเพื่อใช้ในการตรวจสอบ

(๓.๖) ต้องมีกระบวนการบริหารจัดการช่องโหว่ที่มีการดำเนินการ เช่น การเฝ้าระวังต้องมั่นใจว่ามีประสิทธิภาพและประสิทธิผล

(๓.๗) ระบบที่มีความเสี่ยงสูงจะต้องมีการเตรียมการเป็นอันดับแรกตามลำดับความสำคัญและการประเมินความเสี่ยง

๑๙.๒ การจำกัดสิทธิ์ในการติดตั้งซอฟต์แวร์

(๑) ต้องจัดทำรายการซอฟต์แวร์ที่จำเป็นสำหรับเครื่องผู้ใช้งาน เช่น เครื่องคอมพิวเตอร์, แล็ปท็อป

(๒) ต้องทำการตรวจสอบและอนุมัติรายการซอฟต์แวร์ที่จำเป็นสำหรับเครื่องผู้ใช้งานเพื่อจัดทำเป็นรายการซอฟต์แวร์ที่อนุญาตให้ใช้งานในองค์กรสำหรับเครื่องผู้ใช้งานทั่วไป

(๓) ห้ามผู้ใช้งานทำการติดตั้งซอฟต์แวร์ที่เป็นการละเมิดลิขสิทธิ์รวมถึงซอฟต์แวร์อื่นๆ ที่ไม่ได้รับอนุญาตให้ใช้งานในกรมราชทัณฑ์

(๔) หากผู้ใช้งานต้องการติดตั้งซอฟต์แวร์ที่อยู่นอกเหนือรายการซอฟต์แวร์ที่อนุญาตให้ใช้งานจะต้องทำการขออนุมัติศูนย์เทคโนโลยีสารสนเทศก่อนการติดตั้ง

(๕) การติดตั้งซอฟต์แวร์บนเครื่องผู้ใช้งานจะต้องกระทำโดยผู้ดูแลระบบเท่านั้น โดยผู้ดูแลระบบต้องทำการจำกัดสิทธิ์ในการติดตั้งซอฟต์แวร์บนเครื่องของผู้ใช้งานอย่างเหมาะสม

(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 ผู้พัฒนาโปรแกรมควรได้รับสิทธิ์ในการเข้าถึงระบบเท่าที่จำเป็นสำหรับใช้ในการทำงานและการเปลี่ยนแปลง ควรได้รับการอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๒๑. นโยบายการบริหารจัดการเพื่อสร้างความเนื่องทางธุรกิจ (Information security continuity policy)

๒๑.๑ ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

(๑) ต้องมีการกำหนดแนวทางในการสร้างความต่อเนื่องด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในกรณีที่เกิดเหตุการณ์ไม่พึงประสงค์ เช่น เหตุฉุกเฉิน หรือ วิกฤต

(๒) จัดให้ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ เป็นส่วนหนึ่งของกระบวนการในการบริหารจัดการความต่อเนื่องทางธุรกิจหรือกระบวนการในการกู้คืนระบบในภาวะวิกฤต

(๓) พิจารณาด้านความมั่นคงปลอดภัยสารสนเทศ ระหว่างการวางแผนความต่อเนื่องทางธุรกิจหรือการกู้คืนระบบในภาวะวิกฤต

๒๑.๒ การดำเนินการความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

(๑) ต้องจัดตั้งคณะทำงานแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ ซึ่งประกอบไปด้วยตัวแทนจากหน่วยงานเจ้าของข้อมูล เจ้าของระบบงาน และหน่วยงานที่ดูแลระบบเครือข่าย เป็นต้น

(๒) คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศที่เป็นลายลักษณ์อักษร

(๓) กระบวนการหลักในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศต้องประกอบด้วยหัวข้อหลัก ดังนี้

(๓.๑) การวิเคราะห์ผลกระทบทางธุรกิจ

(๓.๒) การประเมินความเสี่ยงและการควบคุม

(๓.๓) การวางกลยุทธ์สำหรับแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

(๓.๔) การพัฒนาแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

(๓.๕) การประชาสัมพันธ์และการฝึกอบรม

(๓.๖) การทดสอบปรับปรุงแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ แนวทางปฏิบัติในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศ

(๓.๗) การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินภารกิจและการให้บริการ

(๓.๘) การตอบสนองต่อสถานการณ์ฉุกเฉินเพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุมการแก้ไขสถานการณ์ฉุกเฉิน

(๓.๙) การดำเนินการเพื่อให้สามารถดำเนินภารกิจได้อย่างต่อเนื่องเช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย

(๓.๑๐) ต้องมีการกลับคืนสู่การทำงานปกติเพื่อให้ภารกิจกลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงาน ตามปกติ

(๔) แนวทางปฏิบัติของการเก็บรักษาข้อมูลและสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและสารสนเทศผู้ใช้งาน ควรปฏิบัติตามแนวปฏิบัติการสำรองข้อมูลการกู้คืนและรักษาความลับของข้อมูล

(๔.๑) เจ้าของข้อมูลเป็นผู้จัดเก็บรักษาข้อมูลเกี่ยวกับระบบ ซึ่งได้แก่ข้อมูลเกี่ยวกับระบบปฏิบัติการ, ซอฟต์แวร์ระบบงาน (ทั้ง Source Code และ Executable Files) โดยให้เป็นไปตามความต้องการที่เจ้าของข้อมูลในระบบนั้น กำหนด จำนวนครั้งและระยะเวลาในการเก็บรักษาข้อมูลดังกล่าว ต้องสอดคล้องกับการประเมินความเสี่ยงของข้อมูลนั้นๆ ด้วย

(๔.๒) ก่อนที่จะมีการปรับปรุงหรือเปลี่ยนแปลงระบบ หน่วยงานที่รับผิดชอบต้องทำการสำรองข้อมูลของระบบทุกครั้ง

(๔.๓) ถ้าการสำรองข้อมูลถูกดำเนินการที่เซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์หลักและเป็นข้อมูลของระบบงานที่สำคัญ จะต้องเพิ่มจำนวนครั้งในการสำรองข้อมูลของเซิร์ฟเวอร์นั้นด้วย

(๔.๔) ข้อมูลและสารสนเทศที่มีความสำคัญมาก จะต้องทำการสำรองข้อมูลไว้ทุกวันและข้อมูลสำรองดังกล่าว ต้องมีการจัดเก็บไว้นอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลักอย่างเหมาะสม โดยตรวจสอบให้แน่ใจว่าสถานที่นั้นมีความปลอดภัยด้วย

(๔.๕) ระบบข้อมูลที่สำคัญทั้งหมด ควรมีระบบการประมวลผลสำรองระบบเครือข่ายสำรองเพื่อป้องกันการพึ่งพาระบบหลักเพียงระบบเดียว ในกรณีที่ระบบหนึ่งไม่สามารถทำงานได้สามารถใช้งานอีกระบบหนึ่งได้ทันทีเพื่อให้ภารกิจหลักดำเนินต่อไปได้

(๔.๖) ข้อมูลและสารสนเทศที่ถูกจัดประเภทเป็นข้อมูลธรรมดา ซึ่งไม่ส่งผลกระทบต่อการดำเนินกิจการ จำนวนครั้งในการสำรองข้อมูลนั้นขึ้นอยู่กับการพิจารณาของเจ้าของข้อมูลและข้อมูลดังกล่าวจะถูกนำไปจัดเก็บในสถานที่ๆ มีความปลอดภัย

(๕) แนวทางปฏิบัติของการเก็บข้อมูลสำรองนอกสถานที่

(๕.๑) ศูนย์คอมพิวเตอร์สำรองหรือสถานที่ที่ใช้ในการจัดเก็บข้อมูลสำรองควรตั้งอยู่ไกลจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะแน่ใจได้ว่าเหตุการณ์หรือภัยธรรมชาติชนิดเดียวกัน เช่น ไฟไหม้ หรือเหตุจลาจลต่างๆ จะไม่เกิดขึ้นกับศูนย์คอมพิวเตอร์ทั้งสองแห่งพร้อมกัน

(๕.๒) ศูนย์คอมพิวเตอร์สำรองหรือสถานที่ที่จัดเก็บข้อมูลสำรองนอกอาคารที่ตั้งศูนย์คอมพิวเตอร์หลัก ต้องมีการรักษาความปลอดภัยทั้งในด้านกายภาพและสภาพแวดล้อมการควบคุมเช่นเดียวกันกับศูนย์คอมพิวเตอร์หลักหรือปรับเปลี่ยนตามความเหมาะสม

๒๑.๓ การตรวจสอบ สอบทาน และวัดผลความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

(๑) คณะทำงานจะต้องจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบสารสนเทศที่เป็นลายลักษณ์อักษรโดยต้องมีการสอบทานและปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละ ๑ ครั้ง

๒๒. การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

๒๒.๑ การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Management of Information Security Incidents and Improvements) เพื่อให้มีวิธีการที่สอดคล้องและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย

(๑) กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติต้องมีการกำหนดหน้าที่ความรับผิดชอบและกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและขั้นตอนดังกล่าวต้องมีความรวดเร็วได้ผล และมีความเป็นระบบระเบียบที่ดี

(๒) การรายงานเหตุการณ์น่าสงสัย / จุดอ่อนด้านความมั่นคงปลอดภัย

(๒.๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการรายงานเหตุการณ์ทันทีที่สงสัยว่าเป็นเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล

(๒.๒) ถ้าหากพบเหตุการณ์ที่น่าสงสัยให้แจ้งต่อผู้รับผิดชอบทันทีเช่น เหตุการณ์ต่อไปนี้

(๑) พบว่ารหัสผ่านส่วนบุคคลของตนถูกล็อคโดยไม่ทราบสาเหตุ

(๒) เวลาการเข้าใช้งานระบบครั้งล่าสุดที่ผิดปกติ

(๓) พบหลักฐานหรือสิ่งผิดสังเกตในเครื่องคอมพิวเตอร์ของตน เช่น มีไฟล์ที่ไม่รู้จักการเปลี่ยนแปลงของค่าต่างๆ

(๔) มีการไม่ปฏิบัติตามขั้นตอนความมั่นคงปลอดภัย

(๕) พบหรือคาดว่าระบบงานจะมีปัญหาด้านความปลอดภัยของข้อมูล

(๖) พบหรือคาดว่าข้อมูลในระบบจะถูกทำลายแก้ไขหรือลบทิ้ง

(๗) มีความพยายามที่จะเข้าใช้ระบบอย่างผิดวิธีไม่ว่าจะสำเร็จหรือไม่

(๘) การให้บริการของระบบเกิดการชะงักหรือไม่สามารถให้บริการ

(๙) เกิดการละเมิดสิทธิ์เข้าไปใช้งานระบบเพื่อประมวลผลหรือจัดเก็บข้อมูล

(๑๐) การแก้ไขค่าความปลอดภัยในระบบเช่น Hardware, Software หรือ Firmware โดยผู้ใช้งานไม่ทราบ

(๓) การประเมินเหตุการณ์ด้านความมั่นคงปลอดภัย ผู้ดูแลระบบต้องประเมินขอบเขตและความรุนแรงของปัญหาหากพบว่าเป็นปัญหาที่จะมีผลกระทบในวงกว้างรุนแรงหรือมีผลต่อชื่อเสียงจะต้องรายงานให้ผู้บังคับบัญชาทราบโดยด่วนเพื่อหาแนวทางแก้ไขและป้องกันไม่ให้เกิดในครั้งต่อไป ควรมีการแบ่งประเภทของปัญหาอย่างเหมาะสม

(๔) การตอบโต้ต่อสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดและการทำงานที่บกพร่องของระบบสารสนเทศหรือซอฟต์แวร์ เพื่อลดความเสียหายจากเหตุการณ์ละเมิดความมั่นคงปลอดภัยและระบบทำงานบกพร่อง เช่น ไวรัสคอมพิวเตอร์แพร่กระจาย ระบบถูกบุกรุก และให้บุคลากรได้เรียนรู้จากประสบการณ์ความเสียหายดังกล่าว

(๔.๑) หากผู้ใช้งานพบเห็นเหตุการณ์ด้านความมั่นคงปลอดภัย และ/หรือจุดอ่อน ช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และ/หรือการทำงานที่บกพร่อง หรือการทำงานผิดปกติของซอฟต์แวร์ผู้ใช้งานต้องรายงานสิ่งที่เกิดขึ้นให้แก่ผู้รับผิดชอบทราบโดยเร่งด่วน

(๔.๒) ในกรณีที่ไม่สามารถติดต่อผู้รับผิดชอบได้ ให้รายงานกับผู้บังคับบัญชาตามลำดับขั้น

(๔.๓) ในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยให้ปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ดังนี้

(๑) ภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง มีความเสี่ยงอย่างมีนัยสำคัญที่ทำให้ระบบคอมพิวเตอร์หรือการให้บริการของกรมราชทัณฑ์ด้อยประสิทธิภาพลง

(๒) ภัยคุกคามทางไซเบอร์ระดับร้ายแรง ถูกโจมตีอย่างมีนัยสำคัญ ทำให้เกิดความเสียหายกับระบบคอมพิวเตอร์หรือ การให้บริการของกรมราชทัณฑ์จนไม่สามารถทำงานหรือให้บริการได้

(๓) ภัยคุกคามทางไซเบอร์ระดับร้ายแรงวิกฤติถูกโจมตีในระดับสูง ส่งผลกระทบรุนแรงเป็นวงกว้างทำให้ระบบคอมพิวเตอร์ หรือการให้บริการที่กรมราชทัณฑ์ ล้มเหลว มีความเสี่ยงที่จะลุกลามไปยังหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

(๕) การเรียนรู้จากสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

(๕.๑) ต้องบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย จุดอ่อนช่องโหว่ ภัยคุกคาม หรือการทำงานบกพร่องของระบบสารสนเทศ รวมทั้งวิธีการแก้ไข เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้น และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

(๕.๒) ระบบต้องจัดทำสรุปรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัยให้รับทราบ อย่างน้อยเดือนละ ๑ ครั้ง

(๖) การเก็บรวบรวมหลักฐาน

(๖.๑) ต้องกำหนดให้มีการรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในการวิเคราะห์สืบสวนหรือเป็นหลักฐานในกระบวนการทางศาลที่เกี่ยวข้องเมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

(๖.๒) ส่วนงานที่มีระบบงานสารสนเทศที่สำคัญต้องจัดเก็บข้อมูล เพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎระเบียบหรือข้อบังคับที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล และกฎหมาย เช่น ๙๐ วัน หรือ ๑ ปี

(๖.๓) ต้องศึกษาถึงลักษณะของหลักฐานที่มีความสมบูรณ์และมีคุณภาพ เพื่อสามารถนำไปใช้ในกระบวนการของศาลได้

๒๓.นโยบายการควบคุมการเปลี่ยนแปลงระบบ (System Change Control Policy)

๒๓.๑ ขั้นตอนปฏิบัติสำหรับการควบคุมการเปลี่ยนแปลงระบบอย่างเป็นทางการ ต้องจัดทำเป็นลายลักษณ์อักษรและบังคับใช้ เพื่อให้มั่นใจในความถูกต้องและรักษาความมั่นคงปลอดภัยของระบบ แอปพลิเคชัน และผลิตภัณฑ์เทคโนโลยีสารสนเทศ ตั้งแต่ขั้นตอนการออกแบบจนถึงสิ้นสุดวงจรการบำรุงรักษา

๒๓.๒ การปรับเปลี่ยนระบบงานใหม่ หรือการเปลี่ยนแปลงโครงสร้างระบบครั้งใหญ่ที่มีผลกระทบต่อระบบที่ให้บริการอยู่ในปัจจุบัน ต้องได้รับการอนุมัติอย่างเป็นทางการ โดยมีขั้นตอนครอบคลุมตั้งแต่การจัดทำเอกสารข้อกำหนด การระบุรายละเอียดเชิงเทคนิค การทดสอบระบบ (Testing) การควบคุมคุณภาพ (Quality Assurance) และแผนการติดตั้งระบบอย่างปลอดภัย

๒๓.๓ ขั้นตอนการควบคุมการเปลี่ยนแปลง ต้องรวมถึงกระบวนการประเมินความเสี่ยง (Risk Assessment) การวิเคราะห์ผลกระทบที่จะเกิดขึ้นต่อระบบและผู้ใช้งาน (Impact Analysis) และการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยที่จำเป็น

๒๓.๔ ขั้นตอนการควบคุมการเปลี่ยนแปลง ต้องมั่นใจได้ว่ามีการควบคุมสิทธิ์การเข้าถึงอย่างเหมาะสมตามหลักความจำเป็นขั้นต่ำ (Least Privilege) โดยผู้พัฒนาซอฟต์แวร์ต้องได้รับสิทธิ์ในการเข้าถึงระบบเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น และการนำข้อมูลหรือซอร์สโค้ดที่เปลี่ยนแปลงขึ้นสู่ระบบใช้งานจริง (Production System) ต้องได้รับการอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๒๔.นโยบายการใช้เทคโนโลยี Generative AI ที่ยอมรับได้ (Acceptable Use Policy: Generative AI)

๒๔.๑ การใช้เทคโนโลยี Generative AI ที่ยอมรับได้ สำหรับการดำเนินงานตามภารกิจ ของสำนักงาน

๒๔.๑.๑ ผู้ใช้งานต้องทำการศึกษาข่อมูลเทคโนโลยี Generative AI แต่ละประเภท เพื่อสร้างความเข้าใจเกี่ยวกับข้อมูลพื้นฐาน ศักยภาพ ประโยชน ความเสี่ยง และข้อจำกัด เพื่อให้ผู้ใช้งาน สามารถประยุกต์ใช้เทคโนโลยี Generative AI ได้อย่างเหมาะสม มีประสิทธิภาพและสอดคล้องกับเป้าหมาย ของงานแต่ละประเภทที่ได้รับมอบหมาย

๒๔.๑.๒ ผู้ใช้งานต้องประยุกต์ใช้เทคโนโลยี Generative AI เพื่อช่วยสนับสนุน ในการดำเนินงานในบริบทที่กำหนด ดังต่อไป

(๑) การวิเคราะห์ข้อมูลและสร้างรายงาน

(๒) การเขียนชุดคำสั่งหรือโปรแกรม

(๓) การจัดทำร่างหนังสือหรือเอกสารต่าง ๆ เช่น บันทึกขอความ นโยบาย หรือ คำแนะนำเป็นต้น

(๔) การให้คำแนะนำหรือแนวทางเบื้องต้นในการแก้ปัญหาด้านต่าง ๆ

(๕) การสร้างเนื้อหาสำหรับการสื่อสารภายในองค์กร

(๖) การสร้างสื่อประชาสัมพันธ์

(๗) ดำเนินงานอื่น ๆ ที่ได้รับมอบหมายจากผู้บังคับบัญชา

ทั้งนี้ การประยุกต์ใช้เทคโนโลยี Generative AI ต้องเป็นไปตามภารกิจ และเพื่อประโยชน์ของสำนักงาน เท่านั้น

๒๔.๑.๓ ผู้ใช้งานต้องใช้เทคโนโลยี Generative AI อย่างมีธรรมาภิบาล เหมาะสม มีความมั่นคงปลอดภัย และสอดคล้องกับกฎหมาย ข้อบังคับ ระเบียบ ประกาศ หรือคำสั่งของสำนักงาน หรืออื่น ๆ ที่เกี่ยวข้อง

๒๔.๒ ข้อห้ามในการใช้เทคโนโลยี Generative AI

แม้ว่าเทคโนโลยี Generative AI จะเป็นเครื่องมือที่ช่วยสนับสนุนและเพิ่มประสิทธิภาพ ในการดำเนินงานให้แก่ผู้ใช้งานอยู่หลายประการ แต่อย่างไรก็ตาม การใช้เทคโนโลยี Generative AI จำต้องอยู่ในขอบเขตที่เหมาะสมและไม่ก่อให้เกิดความเสียหายใด ๆ ต่อบุคคล สำนักงาน สังคม หรือประเทศชาติ ในการนี้ สำนักงานจึงกำหนดข้อห้ามสำหรับผู้ใช้งานเทคโนโลยี Generative AI ไว้ดังนี้

(๑) ห้ามใช้แทนการตัดสินใจของผู้ใช้งานในกรณีที่มีความเสี่ยงสูง เช่น การตัดสินใจทางกฎหมาย ทางการแพทย์ ทางการเงิน หรือการตัดสินใจที่อาจส่งผลกระทบต่อชีวิต ทรัพย์สินและสิทธิของบุคคล

(๒) ห้ามใช้เพื่อสร้างข้อมูลอันเป็นเท็จ หรือสร้างเนื้อหาที่อาจก่อให้เกิดความเสียหายต่อบุคคล สำนักงาน หรือสังคม อันอาจนำไปสู่ความเข้าใจผิด หรือสร้างความขัดแย้งในสังคม

(๓) ห้ามใช้หรือเปิดเผยข้อมูลที่เป็นความลับของสำนักงาน รวมถึงข้อมูลภายในเอกสารสำคัญ หรือข้อมูลที่อาจส่งผลกระทบต่อการดำเนินงานของสำนักงาน

(๔) ห้ามใช้ข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือใช้ข้อมูลที่อาจเป็นความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือกฎหมายอื่นที่เกี่ยวข้อง

(๕) ห้ามใช้ในทางที่ขัดต่อหลักธรรมาภิบาล คุณธรรม จริยธรรม ศีลธรรม หรือมีเจตนาแอบแฝงโดยไม่สุจริต

(๖) ห้ามใช้เพื่อสร้างเนื้อหาที่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา รวมถึงการทำซ้ำ คัดลอก หรือ ดัดแปลงซึ่งเนื้อหาที่เป็นของบุคคลหรือหน่วยงานอื่นโดยไม่ได้รับอนุญาต

(๗) ห้ามใช้เพื่อสร้างเนื้อหาที่ส่งเสริมการเหยียดเชื้อชาติ ศาสนา เพศ วัย ความพิการ หรือ สถานะทางสังคม ซึ่งอาจขัดต่อกฎหมายและหลักสิทธิมนุษยชน

(๘) ห้ามใช้ในการดำเนินการใด ๆ ที่อาจเป็นการกระทำความผิดตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ประกาศ คำสั่ง หลักเกณฑ์ หรืออื่น ๆ ที่เกี่ยวข้อง

๒๔.๓ การรักษาความลับและคุ้มครองข้อมูลส่วนบุคคล

การใช้งานเทคโนโลยี Generative AI โดยเฉพาะอย่างยิ่งที่มีการให้บริการแบบไม่มีค่าใช้จ่าย อาจมีความเสี่ยงที่ข้อมูลที่ผู้ใช้งานระบุหรือโต้ตอบกับระบบ จะถูกเข้าถึงหรือบันทึกและนำไปใช้ในการฝึกสอนโมเดล Generative AI เพื่อปรับปรุงและพัฒนาประสิทธิภาพการทำงานของระบบ ดังนั้น เพื่อเป็นการป้องกันมิให้เกิดการรั่วไหลของข้อมูล การละเมิดสิทธิของบุคคล หรือก่อให้เกิดความเสียหาย ต่อสำนักงาน หน่วยงานภายนอก หรือบุคคลที่เกี่ยวข้อง ผู้ใช้งานจึงต้องมีความระมัดระวังและต้องปฏิบัติ ดังนี้

(๑) ห้ามนำข้อมูลภายในสำนักงาน และข้อมูลที่มีชั้นความลับ (เช่น รหัสผ่าน เอกสาร สัญญา เอกสารหรือหนังสือที่ประทับข้อความลับ เอกสารหรือข้อมูลเกี่ยวกับโครงการภายในสำนักงาน เป็นต้น) ไปใช้งานร่วมกับเทคโนโลยี Generative AI

(๒) ในกรณีที่ต้องใช้เทคโนโลยี Generative AI ร่วมกับข้อมูลภายในองค์กร ข้อมูลที่มีชั้นความลับ ข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลที่อ่อนไหว ผู้ใช้งานจะต้องใช้เทคโนโลยี Generative AI ที่สำนักงานประกาศกำหนดเท่านั้น และผู้ใช้งานต้องได้รับอนุมัติก่อนนำมาใช้งานทุกกรณี

(๓) ในกรณีที่มีข้อสงสัยเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลหรือข้อกำหนดตามกฎหมาย ผู้ใช้งานต้องปรึกษาหารือกับผู้บังคับบัญชาหรือเจ้าหน้าที่ที่เกี่ยวข้องก่อนดำเนินการใด ๆ

๒๔.๔ การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีนำเทคโนโลยี Generative AI มาใช้งาน

(๑) ห้ามนำข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (เช่น รหัสผ่าน ข้อมูล API Key รายละเอียดการตั้งค่าของระบบ เป็นต้น) ไปใช้งานร่วมกับเทคโนโลยี Generative AI

(๒) ต้องตรวจสอบซอร์สโค้ดที่สร้างโดยเทคโนโลยี Generative AI ก่อนนำมาใช้งาน โดยพิจารณาถึงความถูกต้อง และการตรวจสอบช่องโหว่อย่างถี่ถ้วน

(๓) หากพบเหตุการณ์ละเมิดความมั่นคงปลอดภัยที่เกิดจากการประยุกต์ใช้เทคโนโลยี Generative AI ผู้ใช้งานต้องแจ้งให้ผู้บังคับบัญชาตามลำดับชั้นทราบ และต้องปฏิบัติตามขั้นตอนการปฏิบัติงาน (Work Procedure) เกี่ยวกับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยโดยทันที

(๔) การใช้งานเทคโนโลยี Generative AI ผู้ใช้งานต้องดำเนินการให้มีความมั่นคงปลอดภัยไซเบอร์ ความมั่นคงปลอดภัยของระบบสารสนเทศ ความมั่นคงปลอดภัยของข้อมูล และความมั่นคงปลอดภัยในด้านอื่น ๆ ที่เกี่ยวข้อง

(๕) สำนักงานจะมีการตรวจสอบการใช้เทคโนโลยีสารสนเทศ Generative AI ของผู้ใช้งานอย่างต่อเนื่องเพื่อเป็นการรักษาความมั่นคงปลอดภัยของสำนักงาน

๒๔.๕ การลดหรือหลีกเลี่ยงการเกิดอคติ (Bias) และการเลือกปฏิบัติ (Discrimination) ต่อบุคคลหรือกลุ่มบุคคล

ด้วยผลลัพธ์จากการประยุกต์ใช้เทคโนโลยี Generative AI มีโอกาสที่จะสร้างเนื้อหาที่มีความคิดเชิงลบ อคติ หรือแบ่งแยก อันอาจถูกเผยแพร่เป็นวงกว้างและไม่สามารถควบคุมการแพร่กระจายได้โดยง่าย อาจก่อให้เกิดความเสียหายแก่ชื่อเสียง จิตใจของบุคคล เกิดอคติ หรือการเลือกปฏิบัติต่อบุคคลหรือกลุ่มบุคคล ดังนั้น ผู้ใช้งานจึงต้องมีความระมัดระวังและปฏิบัติ ดังนี้

(๑) ต้องตรวจสอบเนื้อหาที่สร้างโดยเทคโนโลยี Generative AI ก่อนนำไปใช้งาน หรือเผยแพร่ต่อสาธารณะ เพื่อลดหรือหลีกเลี่ยงการเกิดอคติหรือการเลือกปฏิบัติอย่างไม่เป็นธรรม

(๒) ในกรณีที่ต้องใช้เทคโนโลยี Generative AI ร่วมกับข้อมูลภายในองค์กร ข้อมูลที่มีชั้นความลับ ข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลที่อ่อนไหว ผู้ใช้งานจะต้องใช้เทคโนโลยี Generative AI ที่สำนักงานประกาศกำหนดเท่านั้น และผู้ใช้งานต้องได้รับอนุมัติก่อนนำมาใช้งานทุกกรณี

(๓) ระมัดระวังการใช้งานเทคโนโลยี Generative AI ในการดำเนินงานที่อาจกระทบต่อสิทธิของบุคคลหรือกลุ่มบุคคล หรือมีผลกระทบต่อหลักความเสมอภาคและมาตรฐานด้านสิทธิมนุษยชน

๒๔.๖ หน้าที่และความรับผิดชอบ

การนำเนื้อหาที่สร้างโดยเทคโนโลยี Generative AI มาใช้งาน อาจส่งผลกระทบเชิงลบต่อบุคคล หน่วยงาน สังคม และประเทศชาติ ทั้งโดยเจตนาหรือไม่เจตนา ซึ่งสำนักงานและผู้ใช้งานไม่อาจปฏิเสธความรับผิดชอบต่อผลที่เกิดขึ้นจากการกระทำดังกล่าวได้ ดังนั้น ผู้ใช้งานและบุคคลที่เกี่ยวข้องกับการประยุกต์ใช้เทคโนโลยี Generative AI จึงมีหน้าที่และความรับผิดชอบ ดังนี้

(๑) ผู้ใช้งานต้องแจ้งผู้บังคับบัญชาเกี่ยวกับวัตถุประสงค์ ขอบเขตและลักษณะของการทำงานร่วมกันระหว่างผู้ใช้งานกับเทคโนโลยี Generative AI (AI-Human Involvement) และเมื่อมีการใช้เทคโนโลยี Generative AI ในการปฏิบัติงาน

(๒) ผู้ใช้งานต้องปฏิบัติตามหลักเกณฑ์และวิธีการใช้งานเทคโนโลยี Generative AI ตามที่กำหนดในนโยบายนี้ และตรวจสอบเนื้อหาที่สร้างโดยเทคโนโลยี Generative AI ก่อนนำไปใช้งานหรือเผยแพร่ และต้องมีการตรวจสอบอย่างเคร่งครัด โดยเฉพาะเนื้อหาที่เกี่ยวข้องกับกฎหมาย ข้อมูลด้านการเงิน ข้อมูลอ่อนไหว ซึ่งผู้ใช้งานจำเป็นต้องพิจารณาในประเด็นดังต่อไปนี้ประกอบด้วย

- ความถูกต้องของเนื้อหา
- ผลการใช้งานหรือเผยแพร่เนื้อหาที่นำไปสู่การกระทำผิดทางกฎหมาย รวมถึงการละเมิดลิขสิทธิ์ เครื่องหมายการค้า หรือทรัพย์สินทางปัญญาอื่น ๆ
- ความเท่าเทียมและการไม่เลือกปฏิบัติต่อบุคคลหรือกลุ่มบุคคล
- การรักษาความลับและการคุ้มครองข้อมูลส่วนบุคคล
- ผลกระทบต่อความมั่นคงปลอดภัยและความเสี่ยงที่อาจเกิดขึ้นจากการใช้งาน
- ผลกระทบเชิงลบอื่น ๆ ที่อาจเกิดขึ้นต่อบุคคล สำนักงาน สังคม และประเทศชาติ

(๓) ผู้ใช้งานต้องรายงานให้ผู้บังคับบัญชารับทราบโดยทันที ในกรณีที่การประยุกต์ใช้ Generative AI เกิดความผิดพลาดหรือพบประเด็นปัญหา ทั้งกรณีการนำเข้าข้อมูลและแสดงผลลัพธ์ ที่อาจส่งผลกระทบเชิงลบต่อบุคคล สำนักงาน สังคม และประเทศชาติ เพื่อให้สามารถดำเนินมาตรการแก้ไขได้โดยเร็ว

(๔) ผู้บังคับบัญชาและผู้ใช้งานต้องมีการติดตาม ทบทวน และประเมินประสิทธิภาพ ประสิทธิผลของการใช้งานเทคโนโลยี Generative AI อย่างต่อเนื่อง เพื่อปรับปรุงวิธีการทำงานและการเลือกใช้เทคโนโลยี Generative AI ที่เหมาะสมกับการปฏิบัติงาน

(๕) การนำเนื้อหาที่สร้างจากเทคโนโลยี Generative AI มาใช้งาน ต้องมีการระบุว่า “เนื้อหานี้ได้รับความช่วยเหลือจากเทคโนโลยี Generative AI” ตามความเหมาะสม เพื่อให้เกิดความโปร่งใส และป้องกันความเข้าใจผิดของผู้รับข้อมูล

(๖) (หน่วยงานที่รับผิดชอบทางด้านเทคโนโลยี) มีหน้าที่ในการพิจารณาตรวจสอบและนำเสนอ (ผู้บริหารระดับสูงของหน่วยงาน เช่น CEO/CIO/CISO) รายการแอปพลิเคชัน หรือบริการ Generative AI ที่ใช้งานภายในสำนักงาน ตามความเหมาะสมของระดับการใช้งาน

๒๕.นโยบายการใช้งานคลาวด์ (Cloud Computing Policy)

นโยบายการใช้งานระบบคลาวด์ (Cloud Computing Policy) คือ แนวทางปฏิบัติและมาตรการบังคับในการควบคุมการใช้งานระบบคอมพิวเตอร์ประมวลผลบนคลาวด์ของหน่วยงาน เพื่อให้การจัดเก็บ การประมวลผล และการรับส่งข้อมูลผ่านโครงสร้างพื้นฐานเสมือนและเครือข่ายอินเทอร์เน็ต เป็นไปอย่างมั่นคงปลอดภัย มีประสิทธิภาพสูงสุด และสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยคลาวด์ภาครัฐแห่งชาติ

๒๕.๑ นโยบายการกำกับดูแลและความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Governance & Security Policy)

๒๕.๑.๑ การเข้ารหัสและการแยกแยะข้อมูลบนระบบแบ่งปันทรัพยากร (Multi-tenancy Encryption) ข้อมูลของหน่วยงานภาครัฐต้องได้รับการเข้ารหัสข้อมูลทั้งในขณะจัดเก็บ (Data at Rest) และในระหว่างการรับ-ส่งข้อมูล (Data in Transit) บนระบบคลาวด์ และต้องมีมาตรการแยกส่วนระบบจัดเก็บข้อมูลและระบบประมวลผลเสมือน (Logical Separation) ออกจากหน่วยงานอื่นอย่างเด็ดขาด เพื่อป้องกันการเข้าถึงข้อมูลข้ามเขตระบบ (Cross-Tenant Access)

๒๕.๑.๒ การพิสูจน์ตัวตนและการควบคุมสิทธิ์ระดับสถาปัตยกรรมคลาวด์ (Identity and Cloud Access Control) การเข้าถึงหน้าจอระบบบริหารจัดการคลาวด์ (Cloud Management Console/Portal) ต้องบังคับใช้ระบบการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) และจำกัดสิทธิ์ผู้ดูแลระบบ (Cloud Administrator) ตามหลักความจำเป็นขั้นต่ำ (Least Privilege) เพื่อป้องกันการปรับเปลี่ยนโครงสร้างระบบคลาวด์โดยไม่ได้รับอนุญาต

๒๕.๑.๓ ความปลอดภัยของระบบทรัพยากรเสมือน (Virtualization & Hypervisor Security) การติดตั้งและใช้งานแอปพลิเคชันบนระบบคลาวด์ ต้องผ่านการตรวจสอบความปลอดภัยของภาพระบบเสมือน (Virtual Machine Image / Container Image) และมีมาตรการป้องกันช่องโหว่ระดับโครงสร้างสถาปัตยกรรม (Hypervisor Vulnerability Protection) เพื่อไม่ให้กระทบต่อเสถียรภาพของระบบโดยรวม

๒๕.๒ นโยบายการจัดการและธรรมาภิบาลข้อมูลบนคลาวด์ (Cloud Data Governance)

๒๕.๒.๑ การจำแนกประเภทข้อมูลและอธิปไตยของข้อมูล (Data Classification & Sovereignty) ข้อมูลของทางราชการ ข้อมูลความลับของทางราชการ หรือข้อมูลส่วนบุคคล (PDPA) ต้องได้รับการคัดแยกความลับอย่างชัดเจน และต้องจัดเก็บอยู่ภายในระบบคลาวด์ที่ตั้งอยู่ในราชอาณาจักรไทยเท่านั้น (Data Sovereignty) เพื่อให้สอดคล้องกับข้อกำหนดทางกฎหมายและความมั่นคงปลอดภัยแห่งชาติ

๒๕.๒.๒ การสำรองข้อมูลและการกู้คืนระบบบนคลาวด์ (Cloud Backup & Disaster Recovery) ต้องจัดทำแผนและกำหนดวิธีการสำรองข้อมูลข้ามเขตระบบ (Cross-Region Backup) หรือสำรองข้อมูลจากระบบคลาวด์กลับมายังศูนย์ข้อมูลภายในหน่วยงาน (Cloud-to-On-Premise Backup) เพื่อรองรับสถานการณ์ฉุกเฉินกรณีผู้ให้บริการคลาวด์เกิดระบบล้มเหลว (Cloud Outage) ให้สามารถกู้คืนระบบได้อย่างต่อเนื่อง

๒๕.๓ นโยบายสำหรับผู้ใช้งานและข้อตกลงระดับการให้บริการ (Acceptable Use & SLA Policy)

๒๕.๓.๑ การเชื่อมต่อเครือข่ายและการใช้อุปกรณ์เข้าถึงระบบคลาวด์ (Secure Connection & BYOD) การเข้าถึงระบบคลาวด์ของหน่วยงานผ่านอุปกรณ์ส่วนตัว (BYOD) หรือเครื่องคอมพิวเตอร์พกพา ต้องกระทำผ่านช่องทางเครือข่ายเสมือนส่วนตัวที่มีการเข้ารหัสปลอดภัย (Secure VPN) หรือระบบเครือข่ายภาครัฐ (GIN) เท่านั้น เพื่อป้องกันการดักรับข้อมูลระหว่าง

๒๕.๓.๒ การสำรองข้อมูลและการกู้คืนระบบบนคลาวด์ (Cloud Backup & Disaster Recovery) ต้องจัดทำแผนและกำหนดวิธีการสำรองข้อมูลข้ามเขตระบบ (Cross-Region Backup) หรือสำรองข้อมูลจากระบบคลาวด์กลับมายังศูนย์ข้อมูลภายในหน่วยงาน (Cloud-to-On-Premise Backup) เพื่อรองรับสถานการณ์ฉุกเฉินกรณีผู้ให้บริการคลาวด์เกิดระบบล่มเหลว (Cloud Outage) ให้สามารถกู้คืนระบบได้อย่างต่อเนื่อง

๒๕.๓.๓ การใช้งานและการควบคุมระดับการให้บริการที่เหมาะสม (Cloud SLA Enforcement) ห้ามผู้ใช้งานนำบัญชีหรือทรัพยากรระบบคลาวด์ขององค์กร ไปใช้ในวัตถุประสงค์ส่วนตัวหรือจัดเก็บข้อมูลที่ผิดกฎหมาย และศูนย์เทคโนโลยีสารสนเทศต้องมีการตรวจสอบประสิทธิภาพและการปฏิบัติตามข้อตกลงระดับการให้บริการ (SLA) ของผู้ให้บริการคลาวด์ภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจในความพร้อมใช้งานของระบบราชการ

๒๖. นโยบายการเตรียมความพร้อมสู่ยุคควอนตัม (Quantum Computing Readiness Policy)

แนวปฏิบัติและกฎเกณฑ์การเตรียมความพร้อมเพื่อยกระดับระบบรักษาความปลอดภัยเชิงรหัสลับขององค์กร เพื่อให้การจัดเก็บ ประมวลผล และรับส่งข้อมูลผ่านเครือข่ายสารสนเทศ เป็นไปอย่างปลอดภัย มีประสิทธิภาพ และสอดคล้องกับมาตรฐานการเข้ารหัสลับที่ทนทานต่อคอมพิวเตอร์ควอนตัมในระดับสากล

๒๖.๑ นโยบายความมั่นคงปลอดภัย (Security Policy)

๒๖.๑.๑ การเข้ารหัสลับที่ทนทานต่อควอนตัม (Post-Quantum Cryptography): ข้อมูลสำคัญและระบบสารสนเทศหลักขององค์กร ต้องได้รับการวางแผนและปรับเปลี่ยนมาใช้แอลกอริทึมเข้ารหัสลับที่ทนทานต่อการโจมตีด้วยคอมพิวเตอร์ควอนตัม ทั้งในขณะจัดเก็บ (At rest) และในขณะรับ-ส่งข้อมูล (In transit) ตามมาตรฐานสากลล่าสุด (เช่น มาตรฐาน NIST PQC)

๒๔.๑.๒ สถาปัตยกรรมรหัสลับแบบยืดหยุ่น (Cryptographic Agility): ต้องกำหนดให้การออกแบบระบบงานและการจัดซื้อจัดจ้างระบบไอทีใหม่ รองรับโครงสร้างสถาปัตยกรรมแบบยืดหยุ่นที่สามารถอัปเดตหรือปรับเปลี่ยนกลไกการเข้ารหัสลับใหม่ ๆ ได้ทันทีโดยไม่ต้องรื้อถอนระบบเดิม เพื่อรองรับภัยคุกคามควอนตัมที่เปลี่ยนแปลงอย่างรวดเร็ว

๒๔.๑.๓ การควบคุมสิทธิ์การเข้าถึงและการตรวจสอบระบบเชิงรุก: การเข้าถึงสิทธิ์ระดับผู้ดูแลระบบที่ควบคุมโครงสร้างพื้นฐานด้านรหัสลับ ต้องยึดหลักการให้สิทธิ์เท่าที่จำเป็น (Least Privilege) และต้องมีการบันทึกประวัติการเข้าใช้งาน (Log) อย่างเข้มงวดเพื่อป้องกันการแอบคัดลอกข้อมูลไปรอถอดรหัสในอนาคต

๒๖.๒ นโยบายการจัดการข้อมูล (Data Governance)

๒๖.๒.๑ การจำแนกประเภทข้อมูลและประเมินความเสี่ยงควอนตัม: ต้องจัดทำบัญชีสินทรัพย์รหัสลับ (Cryptographic Asset Inventory) เพื่อคัดแยกความลับของข้อมูล เช่น ข้อมูลสาธารณะ ข้อมูลส่วนบุคคล (PDPA) หรือข้อมูลความลับทางราชการ และประเมินความเสี่ยงต่อการถูกดักรับข้อมูลในปัจจุบันเพื่อนำไปถอดรหัสในยุคควอนตัม (Harvest Now, Decrypt Later)

๒๖.๒.๒ การสำรองและกู้คืนกุญแจรหัสลับ (Key Management & Recovery): ต้องกำหนดระยะเวลา วงรอบ และวิธีการบริหารจัดการ รวมถึงการสำรองกุญแจรหัสลับยุคหลังควอนตัม (PQC Keys) ให้มีความปลอดภัยขั้นสูงสุด เพื่อป้องกันเหตุฉุกเฉินและพร้อมกู้คืนระบบรักษาความปลอดภัยให้ทำงานได้อย่างต่อเนื่อง

๒๖.๓ นโยบายสำหรับผู้ใช้งานและคู่สัญญา (Acceptable Use & Third-Party Policy)

๒๖.๓.๑ ข้อกำหนดสำหรับผู้พัฒนาและผู้ให้บริการภายนอก (Vendor Readiness): กำหนดมาตรการควบคุมความปลอดภัยเชิงบังคับ โดยคู่สัญญาหรือผู้ให้บริการระบบคลาวด์ภายนอกที่ร่วมงานกับหน่วยงาน ต้องแสดงแผนความพร้อมและการรองรับเทคโนโลยีความปลอดภัยยุคควอนตัมในระบบที่นำมาให้บริการแก่ทางราชการ

๒๖.๓.๒ การใช้งานและการพัฒนาองค์ความรู้อย่างเหมาะสม: ห้ามผู้ใช้งานปรับเปลี่ยน ปิดกั้น หรือแก้ไขค่าคอนฟิกด้านการเข้ารหัสลับความปลอดภัยของระบบคอมพิวเตอร์องค์กรโดยพลการ และบุคลากรที่เกี่ยวข้องต้องเข้ารับการศึกษาอบรมสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามและนโยบายความมั่นคงปลอดภัยยุคควอนตัมอย่างต่อเนื่อง เพื่อการปฏิบัติงานที่ถูกต้องและเท่าทันเทคโนโลยี