แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ ประจำปี พ.ศ. ๒๕๖๙

จัดทำโดย
กรมวิทยาศาสตร์บริการ
กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้น ในการให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจ ในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชน รวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบาย และการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย หลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้อง ความสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมั่นคงปลอดภัยในระบบสารสนเทศ ที่มีรูปแบบหลากหลาย ส่งผลทวีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องมาจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศการขาดนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

โดยคณะอนุกรรมการความมั่นคงปลอดภัยภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั้นคงปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานภาครัฐ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

กรมวิทยาศาสตร์บริการ จึงได้จัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ ประจำปี ๒๕๖๙ ขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงาน และบุคลากรทุกคนในกรมวิทยาศาสตร์บริการ มีความรู้ เข้าใจในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ

กรมวิทยาศาสตร์บริการ

สารบัญ

หน้า

หมวดที่ ๑ การควบคุมการเข้าถึงและการบริหารจัดการการเข้าใช้งานระบบสารสนเทศ ๔

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) ๕

ส่วนที่ ๒ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for access control) ๑๒

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ๑๒

ส่วนที่ ๔ การควบคุมการเข้าถึงระบบของผู้ดูแลระบบและผู้ใช้สิทธิพิเศษ (Privileged Access Right) ๑๕

ส่วนที่ ๕ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility) ๑๖

ส่วนที่ ๖ การบริหารจัดการทรัพย์สิน (Asset Management) ๒๐

ส่วนที่ ๗ การควบคุมการเข้าถึงเครือข่าย (Network Access Control) ๒๒

ส่วนที่ ๘ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) ๒๖

ส่วนที่ ๙ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) ๒๘

ส่วนที่ ๑๐ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malware) ๓๑

ส่วนที่ ๑๑ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) ๓๓

ส่วนที่ ๑๒ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control) ๓๔

ส่วนที่ ๑๓ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : อีเมล) ๓๕

ส่วนที่ ๑๔ การควบคุมการใช้อินเทอร์เน็ต (Internet) ๓๖

ส่วนที่ ๑๕ การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ๓๗

ส่วนที่ ๑๖ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server) ๓๘

ส่วนที่ ๑๗ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) ๔๑

ส่วนที่ ๑๘ การใช้งานอุปกรณ์และเครื่องคอมพิวเตอร์แบบพกพา (Notebook) ๔๒

ส่วนที่ ๑๙ การตรวจจับ/ป้องกันการบุกรุก (Intrusion Detection System/Intrusion Prevention System Policy: IDS/IPS) ๔๓

ส่วนที่ ๒๐ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration) ๔๕

ส่วนที่ ๒๑ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์และการเฝ้าระวัง (Logging and Monitoring) ๔๗

ส่วนที่ ๒๒ การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information Security) ๔๗

ส่วนที่ ๒๓ การรักษาความมั่นคงปลอดภัยของฐานข้อมูล (Database Security) ๔๘

ส่วนที่ ๒๔ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) ๔๘

ส่วนที่ ๒๕ การป้องกันข้อมูลรั่วไหล (Data Leakage Prevention) ๕๑

สารบัญ

หน้า

ส่วนที่ ๒๖ ปฏิบัติให้สอดคล้องกับกฎหมาย กฎระเบียบ ข้อบังคับ (Legal and Regulatory Compliance) ๕๑

หมวดที่ ๒ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ๕๒

ส่วนที่ ๑ การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware) ๕๒

ส่วนที่ ๒ การสำรองข้อมูลและกู้คืน (Backup and Recovery) ๕๒

ส่วนที่ ๓ การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software) ๕๕

ส่วนที่ ๔ การบริหารจัดการข่าวกรองภัยคุกคาม และช่องโหว่ทางเทคนิค (Threat Intelligence and Technical Vulnerability Management) ๕๕

หมวดที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ๕๗

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ๕๗

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบสารสนเทศ ๕๘

หมวดที่ ๔ การปฏิบัติเพื่อตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ ๖๐

หมวดที่ ๕ การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ๖๕

หมวดที่ ๖ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information Systems Acquisition, Development, and Maintenance) ๖๗

หมวดที่ ๗ การบริหารจัดการผู้ให้บริการภายนอก ๖๘

หมวดที่ ๘ การรักษาความมั่นคงปลอดภัยของข้อมูลสำหรับทรัพยากรบุคคล ๗๕

หมวดที่ ๙ หน้าที่และความรับผิดชอบด้านสารสนเทศ ๗๖

ส่วนที่ ๑ ระดับนโยบาย ๗๗

ส่วนที่ ๒ ระดับปฏิบัติงาน ๗๗

หมวดที่ ๑๐ การพัฒนาระบบสารสนเทศ ๗๘

๑. บทนำ

๑.๑ หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กรซึ่งจะได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัย เช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีสำคัญอย่างยิ่งต่อองค์กร ที่จะต้องมีการวางแผนและมีกระบวนการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมาย และมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้องนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

๑.๒ วัตถุประสงค์

๑) เพื่อให้กรมวิทยาศาสตร์บริการ (วศ.) มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นกรอบและแนวทางมาตรฐานในการป้องกัน รับมือ และแก้ไขเหตุการณ์ภัยคุกคาม สอดคล้องกับกฎหมายด้านความมั่นคงปลอดภัยสารสนเทศ มาตรฐานสากล ISO/IEC 27001 รวมถึงรองรับการปฏิบัติงานของสำนักบริหารและรับรองห้องปฏิบัติการตามมาตรฐาน ISO/IEC 17011 และ ISO/IEC 17024 และการดำเนินการของห้องปฏิบัติการตามมาตรฐาน ISO/IEC 17025

๒) เพื่อปกป้องระบบสารสนเทศ ระบบบริหารจัดการห้องปฏิบัติการ ข้อมูลผลการทดสอบ และข้อมูลที่เกี่ยวข้องให้มีความถูกต้อง ครบถ้วน เป็นความลับและพร้อมใช้งานอยู่เสมอ

๓) เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอ้างอิงตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ มาตรฐานที่กรมวิทยาศาสตร์บริการ (วศ.) ปรับใช้ และนโยบายอื่น ๆ ที่เกี่ยวข้อง

๔) เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร พนักงาน ลูกจ้าง ผู้ดูแลระบบและบุคลากรภายนอกที่ปฏิบัติงานให้กรมวิทยาศาสตร์บริการ (วศ.) ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและปฏิบัติตามอย่างเคร่งครัด

๑.๓ องค์ประกอบของแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมวิทยาศาสตร์บริการ ฉบับนี้ อ้างอิงตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรฐานสากล ISO/IEC 27001 และ NIST Cybersecurity Framework โดยแนวทางปฏิบัตินี้ ประกอบด้วยวัตถุประสงค์ ผู้เกี่ยวข้อง และรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการ

๑.๔ บทบังคับใช้

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของกรมวิทยาศาสตร์บริการ บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุนและติดตามการประยุกต์ใช้ โดยอธิบดีกรมวิทยาศาสตร์บริการ

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรือเกิดอันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูง (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๑.๕ การเผยแพร่และทบทวน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมวิทยาศาสตร์บริการ ฉบับนี้ จัดทำขึ้น และมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง โดยแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) และเผยแพร่ในเว็บไซต์หลักของกรมวิทยาศาสตร์บริการ (https://www.dss.go.th) เพื่อให้บุคลากรของกรมวิทยาศาสตร์บริการ และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒. คำนิยาม

๑. คำเรียกแทนหน่วยงานในเอกสารฉบับนี้ เช่น กรม หมายความว่า กรมวิทยาศาสตร์บริการ

๒. ผู้บริหารระดับสูง หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารราชการของ กรมวิทยาศาสตร์บริการ

๓. การรักษาความมั่นคงปลอดภัย หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับด้านสารสนเทศของกรมวิทยาศาสตร์บริการ

๔. ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับผิดชอบ ผู้ใช้งานทั่วไป อันได้แก่

๔.๑ ผู้บริหารสูงสุด หมายความว่า อธิบดีกรมวิทยาศาสตร์บริการ

๔.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer :DCIO) หมายความว่า รองอธิบดีกรมวิทยาศาสตร์บริการ ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๔.๓ ผู้ดูแลระบบ/ผู้ดูแลห้องเครื่อง หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์

๔.๔ ผู้พัฒนาระบบ หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนาระบบแอปพลิเคชัน

๔.๕ เจ้าหน้าที่ หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ พนักงานจ้างเหมาบริการ และเจ้าหน้าที่ประจำโครงการของกรมวิทยาศาสตร์บริการ

๔.๖ บุคคลภายนอก หมายความว่า บุคคลที่กรมวิทยาศาสตร์บริการอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการได้ชั่วคราว เพื่อประโยชน์ในการดำเนินงานของกรมวิทยาศาสตร์บริการ เช่น พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับกรมวิทยาศาสตร์บริการ หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง หรือนิสิตนักศึกษาฝึกงาน

๕. สิทธิ์ของผู้ใช้งาน หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๖. สินทรัพย์ (Asset) หรือ ทรัพย์สินสารสนเทศ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่

๖.๑ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๖.๒ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

๖.๓ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๗. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๘. ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ (Information Security) หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) ห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไขทำสูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

๙. เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันนำไปสู่ปัญหาด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๑๐. สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

หมวดที่ ๑ การควบคุมการเข้าถึงและการบริหารจัดการการเข้าใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑) เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

๒) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกรมวิทยาศาสตร์บริการ ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑) สถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

แนวทางปฏิบัติ

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

เพื่อให้การเข้าถึงและการควบคุมการใช้งานสารสนเทศมีความมั่นคงปลอดภัย กำหนดให้ผู้ดูแลระบบมีแนวปฏิบัติดังนี้

๑. การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลข้อมูล

๑.๑ ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ หรือผู้มีอำนาจตัดสินใจ โดยการเข้าถึงระบบสารสนเทศต้องพิจารณาตามความจำเป็นต่อการใช้งานเท่านั้น และต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญถูกจำกัดไว้ที่

(๑) บุคลากร และกิจกรรมที่ได้รับอนุญาต

(๒) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

๑.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

๑.๒.๑ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

๑.๒.๑.๑ กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

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

๑.๒.๑.๒ กำหนดเกณฑ์การระงับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๒.๑.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๒.๑.๔ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อ ผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

กรมวิทยาศาสตร์บริการใช้แนวทางการจัดลำดับชั้นข้อมูลตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔, พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และมาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๒.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น

๒.๑.๑ ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

๒.๑.๒ ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ บริการรับรองระบบงานห้องปฏิบัติการบริการกิจกรรมทดสอบความชำนาญ บริการสารสนเทศวิทยาศาสตร์และเทคโนโลยี บริการฝึกอบรมบุคลากรด้านวิทยาศาสตร์และเทคโนโลยี บริการรับรองความสามารถบุคลากรด้านวิทยาศาสตร์และเทคโนโลยี บริการทดสอบ สอบเทียบ และบริการรับรองผลิตภัณฑ์ เป็นต้น

๒.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ ดังนี้

ระดับที่ ๑ ข้อมูลที่มีระดับความสำคัญมากที่สุด

ระดับที่ ๒ ข้อมูลที่มีระดับความสำคัญปานกลาง

ระดับที่ ๓ ข้อมูลที่มีระดับความสำคัญน้อย

๒.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล ดังนี้

ตารางกำหนดลำดับชั้นข้อมูล	
ลำดับชั้นข้อมูล	**ความหมาย**
ข้อมูลเปิดเผยได้ (Public)	๑) ข้อมูลข่าวสารที่สามารถเปิดเผยต่อสาธารณะได้ โดยได้แก่ข้อมูลที่ถูกจัดหมวดหมู่เป็นข้อมูลสาธารณะ และข้อมูลข่าวสารส่วนบุคคลที่ไม่ขัดต่อ พ.ร.บ. ข้อมูลข่าวสารฯ และเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ข้อมูลความมั่นคง และข้อมูลความลับทางราชการ สามารถเปิดเผยชื่อบัญชีได้ตามสิทธิ์ หรือเฉพาะ

ตารางกำหนดลำดับชั้นข้อมูล	
ลำดับชั้นข้อมูล	**ความหมาย**
	ผู้ที่ถูกกำหนดสิทธิ์เท่านั้นจึงจะสามารถดูรายการบัญชีข้อมูลความมั่นคง และ บัญชีข้อมูลความลับทางราชการได้ ๒) ข้อมูลที่บุคคลภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น ซึ่งเป็นข้อมูลที่ไม่มีผลต่อการปฏิบัติงานของกรมฯ ผู้ปฏิบัติงาน พนักงานและลูกจ้าง สามารถนำเสนอต่อสาธารณชน และเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย ๓) หากมีการเปิดเผยข้อมูลประเภทนี้ทั้งหมดหรือบางส่วน จะไม่เกิดผลเสียหายต่อกรมฯ ตัวอย่าง รายงานประจำปี ข่าวสารต่าง ๆ สำหรับบุคคลทั่วไป ข้อมูลบนเว็บไซต์ของกรมฯ (ในส่วนที่เป็นข้อมูลที่สามารถอ่านได้โดยไม่ต้องมีการใส่รหัสผ่าน) เป็นต้น <u>ตัวอย่าง</u> รายงานประจำปี ข่าวสารต่าง ๆ สำหรับบุคคลทั่วไป ข้อมูลบนเว็บไซต์ของกรมฯ (ในส่วนที่เป็นข้อมูลที่สามารถอ่านได้โดยไม่ต้องมีการใส่รหัสผ่าน) ข้อมูลอัตราการให้บริการ เป็นต้น
ใช้ภายในเท่านั้น (Private)	๑) ข้อมูลที่ไม่สามารถเปิดเผยต่อสาธารณะได้ แต่สามารถใช้หรือเปิดเผยเพื่อการดำเนินงานภายในหน่วยงานเท่านั้น หรือข้อมูลที่องค์กรไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปจะเกี่ยวข้องกับข้อมูลบุคคลหรือกรมฯ และแม้ว่าการสูญเสียหรือการเปิดเผยข้อมูลอาจไม่ส่งผลให้เกิดผลกระทบที่สำคัญ แต่ก็ไม่พึงประสงค์ที่ให้เปิดเผยโดยไม่ได้รับอนุญาต ๒) เป็นข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้ผู้ปฏิบัติงาน พนักงานและลูกจ้างทุกคนภายในกรมฯ รับทราบได้ แต่ไม่สมควรเปิดเผยต่อบุคคลภายนอกกรมฯ เนื่องจากอาจสร้างความเสียหายให้กับกรมฯ ได้ หากมีการร้องขอจากบุคคลภายนอก เจ้าของข้อมูลต้องใช้ดุลยพินิจในการเปิดเผย โดยยึดหลักความจำเป็นในการใช้และความเสมอภาค ๓) หากมีการเปิดเผยข้อมูลประเภทนี้ทั้งหมดหรือบางส่วนให้กับบุคคลภายนอกให้ใช้ดุลยพินิจทุกครั้ง และมีการระบุสิทธิของกรมฯในข้อมูลนั้นๆ พร้อมกับหน้าที่ของบุคคลภายนอกให้ชัดเจน <u>ตัวอย่าง</u> นโยบายหรือระเบียบคำสั่งภายในกรมฯ คู่มือการปฏิบัติงานระบบต่าง ๆ บันทึก หนังสือเวียนภายในต่าง ๆ และผังเบอร์โทรศัพท์ภายในกรมฯ เป็นต้น

ตารางกำหนดลำดับชั้นข้อมูล	
ลำดับชั้นข้อมูล	**ความหมาย**
ข้อมูลลับ (Confidential)	๑) ข้อมูลที่เมื่อเปิดเผยทั้งหมดหรือบางส่วนแล้วก่อให้เกิดผลเสียหายแก่กรมฯ และส่งผลให้เกิดความอับอายอย่างมากต่อบุคคล หรือกรมฯ และอาจเป็นผลทางกฎหมาย ๒) ข้อมูลภายในกรมฯ ที่เจ้าของข้อมูลพิจารณาแล้วว่าไม่สามารถเปิดเผยให้ผู้ปฏิบัติงาน พนักงาน และลูกจ้างทุกคนทราบ ข้อมูลประเภทนี้จะถูกกำหนดให้ผู้ที่เกี่ยวข้องและจำเป็นต้องใช้ในการปฏิบัติงานได้ทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่พึงทราบ เพื่อให้เพียงพอต่อการปฏิบัติงานโดยทั่วไปข้อมูลชั้นนี้มีความสำคัญต่อการดำเนินการของกรมฯ เป็นข้อมูลภายในและไม่สามารถเปิดเผยต่อบุคคลภายนอกกรมฯ ที่ไม่เกี่ยวข้องตามกฎหมาย เนื่องจากข้อมูลนี้จะเป็นประโยชน์ในการดำเนินการตามหน้าที่ความรับผิดชอบของกรมฯ หรือเป็นข้อมูลสร้างความเสียหายให้กับกรมฯ ได้ ๓) การใช้งานข้อมูลชั้นนี้จะต้องได้รับการอนุมัติจากผู้บริหารระดับหัวหน้ากลุ่ม/ศูนย์ที่เป็นเจ้าของข้อมูลขึ้นไปเป็นลายลักษณ์อักษร โดยต้องมีการลงนามในเอกสารข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่ กฎหมายให้การรับรอง ๔) ข้อมูลในชั้นนี้ร่วมถึงข้อมูลส่วนบุคคล ข้อมูลประชาชนผู้ใช้บริการ และข้อมูลผู้ปฏิบัติงาน พนักงาน หรือลูกจ้าง ซึ่งการเปิดเผยข้อมูลต่อบุคคลภายนอกกรมฯ จะต้องเป็นไปตามฐานการประมวลผลข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือได้รับการยินยอมจากเจ้าของข้อมูลหรือประชาชนผู้รับบริการ แล้วแต่กรณีก่อนเปิดเผยให้กับผู้ปฏิบัติงาน พนักงานหรือลูกจ้างที่มีส่วนเกี่ยวข้อง หากพนักงานและลูกจ้างที่ไม่เกี่ยวข้องร้องขอ เจ้าของข้อมูล หรือผู้ควบคุมข้อมูลต้องใช้ดุลยพินิจและหากมีการเปิดเผยต้องจัดทำทะเบียนเพื่อควบคุม หากมีการเปิดเผยข้อมูลประเภทนี้ทั้งหมดหรือบางส่วนแล้วจะเกิดความเสียหายต่อวัตถุประสงค์ที่ข้อมูลถูกจัดสร้างขึ้นมา ไม่ว่าจะเป็นผลเสียหายด้านสถานะทางการเงินของกรมฯ หรือผลเสียหายด้านการละเมิดกฎ ระเบียบต่าง ๆ หรือการทำลายชื่อเสียง และภาพลักษณ์ของกรมฯ และจะกระทบกับความสามารถในการปฏิบัติงานประจำวันของกรมฯ ด้วย

ตารางกำหนดลำดับชั้นข้อมูล	
ลำดับชั้นข้อมูล	**ความหมาย**
	หากบุคคลภายนอกร้องขอ กรมฯ จะต้องใช้ดุลยพินิจ ในการพิจารณาอนุมัติเป็นกรณีไป โดยยึดหลักความเสียหายต่อกรมฯ ตัวอย่าง ข้อมูลส่วนบุคคล ข้อมูลประชาชนผู้รับบริการ ข้อมูลผู้ปฏิบัติงาน พนักงาน หรือลูกจ้าง รายงานของหน่วยงานตรวจสอบ และสัญญาหรือข้อตกลงกับประชาชนผู้รับบริการ เป็นต้น
ข้อมูลลับมาก (Secret)	๑) เป็นข้อมูลภายในกรมฯ แต่เป็นข้อมูลลับซึ่งใช้งานโดยผู้ใช้บางกลุ่มของกรมฯ โดยส่วนใหญ่จะเป็นผู้บริหารของกรมฯ เท่านั้น และไม่สามารถเปิดเผยต่อบุคคลภายนอกกรมฯ ได้ เนื่องจากข้อมูลประเภทนี้มีความจำเป็นต่อการปฏิบัติงานของกรมฯ ซึ่งทำให้เกิดผลเสียหายร้ายแรงต่อกรมฯ ๒) การใช้งานข้อมูลชั้นนี้จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษร โดยผู้บริหารระดับผู้ช่วยผู้อำนวยการ กอง/ สำนัก/สถาบันที่เป็นเจ้าของข้อมูลขึ้นไป โดยต้องมีการลงนามในเอกสาร ข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) เว้นแต่การ เผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง ๓) นอกเหนือจากเป็นข้อมูลภายในของกรมฯ แล้ว ชั้นข้อมูลลับมากยังรวมถึงข้อมูลส่วนบุคคลบางประเภทที่ไม่สามารถเปิดเผยให้บุคคลอื่นได้ทราบด้วย เช่น รหัสผ่านสำหรับเข้าใช้ระบบงานต่าง ๆ ของผู้ปฏิบัติงาน พนักงานและลูกจ้าง หรือรหัสผ่านสำหรับจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นต้น ๔) หากมีการเปิดเผยข้อมูลประเภทนี้ทั้งหมดหรือบางส่วนแล้ว จะเกิดผลเสียหายอย่างร้ายแรงต่อการดำเนินงานของกรมฯ ไม่ว่าจะเป็นผลเสียหายทางการเงินของกรมฯ ผลเสียหายจากการละเมิดกฎระเบียบ การล่วงละเมิดสิทธิส่วนบุคคลหรือของประชาชนผู้รับบริการ หรือผลเสียหายซึ่งจะทำลายชื่อเสียงและภาพลักษณ์ของกรมฯ อย่างมาก รวมทั้งเกิดความเสียหายต่อการดำเนินงานของกรมฯ ๕) หากบุคคลภายนอกร้องขอ กรมฯ จะต้องใช้ดุลพินิจอย่างเข้มงวดในการพิจารณาอนุมัติเป็นกรณีไป โดยยึดหลักความเสียหายต่อกรมฯ กรณีข้อมูลที่ร้องขอเป็นข้อมูลส่วนบุคคล ข้อมูลลูกค้าการเปิดเผยข้อมูลต่อบุคคลภายนอก ให้เป็นไปตามฐานการประมวลผลข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ตารางกำหนดลำดับชั้นข้อมูล	
ลำดับชั้นข้อมูล	**ความหมาย**
	ตัวอย่าง ข้อมูลประชาชนผู้รับบริการ รายงานที่เกี่ยวข้องกับระบบการรักษาความมั่นคงปลอดภัยของกรมฯ เป็นต้น
ข้อมูลลับที่สุด (Top Secret)	๑) ข้อมูลภายในกรมฯ แต่เป็นข้อมูลลับซึ่งใช้งานโดยผู้บริหารระดับสูงของกรมฯ เท่านั้นที่เป็นผู้ใช้ และเป็นการใช้เพื่อการวินิจฉัยและตัดสินใจที่สำคัญของกรมฯ ไม่สามารถเปิดเผยต่อบุคคลภายนอกกรมฯ ได้เลย เนื่องจากข้อมูลประเภทนี้มีความจำเป็นต่อการปฏิบัติงานของกรมฯ และมีผลกระทบต่อประเทศชาติ ทำให้เกิดผลเสียหายร้ายแรงต่อกรมฯ การนำข้อมูลชั้นนี้ไปเปิดเผยต่อบุคคลภายนอกกรมฯ ไม่สามารถทำได้ เว้นแต่การบังคับตามกฎหมาย ชั้นข้อมูลนี้ยังร่วมถึงข้อมูลส่วนบุคคลบางประเภทที่ไม่สามารถเปิดเผยให้บุคคลอื่นได้ทราบด้วย ๒) การใช้งานข้อมูลชั้นนี้จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษร โดยผู้บริหารระดับรองอธิบดีที่เป็นเจ้าของข้อมูลขึ้นไป และต้องมีการลงนามในเอกสาร ข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง ๓) หากมีการเปิดเผยข้อมูลประเภทนี้โดยเปิดเผยทั้งหมดหรือบางส่วนแล้ว จะเกิดผลเสียหายอย่างร้ายแรงที่สุดต่อกรมฯ และความมั่นคงปลอดภัยของประเทศชาติ ไม่ว่าจะเป็นผลเสียหายทางการเงินของกรมฯ ผลเสียหายจากการละเมิดกฎ ระเบียบ การล่วงละเมิดสิทธิส่วนบุคคลหรือสิทธิของประชาชนผู้รับบริการ หรือผลเสียหายซึ่งจะทำลายชื่อเสียงและภาพลักษณ์ของกรมฯ อย่างมาก รวมทั้งเกิดความเสียหายต่อการดำเนินงานของกรมฯ และเกิดความเสียหายต่อความมั่นคงปลอดภัยต่อประเทศชาติ ๔) หากบุคคลภายนอกร้องขอ จะต้องใช้ดุลยพินิจอย่างเข้มงวดในการวินิจฉัยเป็นกรณี ๆ ไป โดยยึดหลักความเสียหายต่อกรมฯ และต้องผ่านการอนุมัติโดยผู้บริหารระดับสูงที่มีอำนาจของกรมฯ กรณีข้อมูลที่ร้องขอเป็นข้อมูลส่วนบุคคล ข้อมูลประชาชนผู้รับบริการ การเปิดเผยข้อมูลต่อบุคคลภายนอก ให้เป็นไปตามฐานการประมวลผลข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตัวอย่าง ข้อมูลส่วนบุคคลที่มีความอ่อนไหว พยากรณ์สถานะการเงินของกรมฯ เป็นต้น

๒.๔ การจัดแบ่งระดับชั้นการเข้าถึง

ระดับที่ ๑ ระดับชั้นสำหรับผู้บริหาร

ระดับที่ ๒ ระดับชั้นสำหรับผู้ใช้งานทั่วไป

ระดับที่ ๓ ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๒.๕ การกำหนดเวลาในการเข้าถึงข้อมูล

การเข้าถึงข้อมูลของกรมวิทยาศาสตร์บริการ กำหนดไว้เป็นช่วงเวลาเข้าถึงได้ดังนี้

ลำดับ	เวลาที่เข้าถึงได้	ข้อมูล/ ช่องทางการเข้าถึงข้อมูล
๑	ทุกวัน ตั้งแต่เวลา ๐๕.๐๐ – ๒๒.๐๐ น	- ระบบลงเวลาปฏิบัติราชการ
๒	ทุกวัน ตลอด ๒๔ ชั่วโมง	- เว็บไซต์ - ระบบสารบรรณอิเล็กทรอนิกส์ - ระบบลาออนไลน์ - ระบบรับเรื่องร้องเรียนออนไลน์ - ระบบถ่ายทอดเทคโนโลยี - ระบบประกาศการจัดซื้อจัดจ้าง - ระบบผลงานวิจัยที่นำไปใช้ในเชิงพาณิชย์ - ระบบรายงานผลการดำเนินงาน ตามตัวชี้วัด - ระบบประชุมแบบอิเล็กทรอนิกส์ - ระบบจดหมายอิเล็กทรอนิกส์ - ระบบ Back Office - ระบบบริการทดสอบ สอบเทียบ - ระบบฐานข้อมูล OTOP - ระบบ e-Learning - ระบบบริการทดสอบความชำนาญ - ระบบห้องสมุดอิเล็กทรอนิกส์ - ระบบยื่นขอรับรองออนไลน์ - ระบบลงทะเบียนฝึกอบรมออนไลน์

ส่วนที่ ๒ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ

(Business Requirement for access control)

เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศของกรม รวมทั้งการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ ข้อกำหนดด้านความมั่นคงปลอดภัย และการใช้งานตามภารกิจ โดยมีแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ ดังนี้

๒.๑ การควบคุมการเข้าถึงสารสนเทศ

๒.๑.๑ ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๒.๑.๒ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

๒.๒ จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ์ และภารกิจดังนี้

๒.๒.๑ Executive คือ กลุ่มผู้บริหาร อธิบดี ผู้ทรงคุณวุฒิ รองอธิบดี ผู้อำนวยการกองหรือเทียบเท่า

๒.๒.๒ Administrator คือ กลุ่มของผู้ดูแลระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการ

๒.๒.๓ Officer กลุ่มผู้ใช้งานทั่วไปเป็นบุคลากรของกรมวิทยาศาสตร์บริการ

๒.๒.๔ Consultant คือ กลุ่มที่ปรึกษาหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับกรมวิทยาศาสตร์บริการ

๒.๒.๕ Guest คือ ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อบริหารจัดการการเข้าถึงระบบสารสนเทศของกรมวิทยาศาสตร์บริการ และมั่นใจได้ว่ามีเฉพาะผู้ที่ได้รับสิทธิ์การเข้าถึงระบบสารสนเทศตามที่กำหนดเท่านั้นที่สามารถเข้าใช้งานระบบสารสนเทศได้ โดยมีแนวปฏิบัติในการบริหารจัดการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน ดังนี้

๓.๑ สร้างความรู้ ความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้งาน

๓.๑.๑ กรมวิทยาศาสตร์บริการ จัดให้มีการอบรมเพื่อสร้างความรู้ และความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ และรู้เท่าทันต่อภัยคุกคาม และผลกระทบที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศอย่างไม่ระมัดระวัง โดยจัดให้มีการอบรมผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๓.๑.๒ กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิ์เพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เมื่อได้รับสิทธิ์การเข้าใช้งานระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

๓.๒ การลงทะเบียนผู้ใช้งาน (User Registration)

๓.๒.๑ ผู้ดูแลระบบ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการ

๓.๒.๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๓.๒.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามรายละเอียดสิทธิ์ในแต่ละภารกิจในส่วนที่ ๒

๓.๒.๔ ผู้ดูแลระบบต้องชี้แจง และแจ้งผู้ใช้งาน เป็นลายลักษณ์อักษร เพื่อให้ผู้ใช้งานทราบถึงสิทธิ์หน้าที่รับผิดชอบ และมาตรการด้านความมั่นคงปลอดภัย ในการเข้าถึงระบบสารสนเทศ

๓.๒.๕ กำหนดให้มีการยกเลิก เพิกถอนการอนุญาตเข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนผู้ใช้งาน เมื่อได้รับแจ้งจากต้นสังกัด หรือเมื่อมีการลาออก เปลี่ยนแปลงตำแหน่ง โยกย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๓.๓ การบริหารจัดการสิทธิ์ผู้ใช้งาน (User Management)

๓.๓.๑ กำหนดระดับสิทธิ์การเข้าถึงระบบสารสนเทศตามหน้าที่รับผิดชอบ ความจำเป็นในการใช้งาน และทบทวนสิทธิ์สม่ำเสมอ

๓.๓.๒ ผู้ดูแลระบบต้องปรับปรุงสิทธิ์การเข้าถึงข้อมูล และระบบสารสนเทศตามหน้าที่รับผิดชอบ และจัดเก็บข้อมูลการมอบสิทธิ์ให้แก่ผู้ใช้งานไว้เป็นฐานข้อมูล

๓.๓.๓ ในกรณีที่ต้องให้สิทธิ์พิเศษนอกเหนือจากภาระงานที่กำหนด จะต้องได้รับการอนุมัติเห็นชอบจากต้นสังกัด และผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ จัดทำขอเป็นลายลักษณ์อักษร โดยการให้สิทธิ์พิเศษดังกล่าวจะต้องกำหนดช่วงเวลาที่ชัดเจน และเมื่อพ้นกำหนดการให้สิทธิ์พิเศษ จะต้องระงับการใช้งานทันที

๓.๓.๔ ให้ยกเลิกบัญชีผู้ใช้งาน (Disable User Account) เมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง

๓.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๓.๔.๑ ผู้ดูแลระบบกำหนดรหัสผ่านให้แก่ผู้ใช้งาน จากนั้นส่งมอบให้ผู้ใช้งานเป็นเอกสารปิดผนึกที่เป็นความลับ

๓.๔.๒ กำหนดให้ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่านไว้ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึงโดยบุคคลอื่นนอกจากตนเอง

๓.๔.๓ รหัสผ่านประกอบไปด้วยตัวอักษรเล็ก ตัวอักษรใหญ่ สัญลักษณ์พิเศษ ไม่น้อยกว่า ๘ ตัวอักษร

๓.๔.๔ ผู้ใช้งานไม่สามารถเปลี่ยนรหัสผ่านได้ กรณีลืมรหัสผ่านจะต้องแจ้งไปยังฝ่าย IT เพื่อขอรับรหัสใหม่

๓.๔.๕ รหัสผ่าน ๑ บัญชี สามารถใช้กับระบบงานภายในได้ทุกระบบ (Single Sign On)

๓.๕ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access right)

ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิ์การใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น การปรับเปลี่ยนตำแหน่งงาน การโยกย้าย ปรับย้าย รวมถึงการสิ้นสภาพการเป็นพนักงาน เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตจากผู้ที่ไม่มีสิทธิ์การเข้าถึง โดยมีแนวปฏิบัติ ดังนี้

๓.๕.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน พร้อมรายละเอียดสิทธิ์ที่ได้รับของแต่ละบุคคล

๓.๕.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

๓.๕.๓ ดำเนินการแก้ไขข้อมูล สิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับ

๓.๕.๔ ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๗ วัน หรือ เมื่อเปลี่ยนตำแหน่งงานภายใน ต้องดำเนินการภายใน ๑๕ วัน หรือ เมื่อถูกให้ออก จากราชการภายใน ๑ วัน หลังจากที่ได้รับแจ้งจากหน่วยงาน กรณีการยกเลิกสัญญาของ ลูกจ้างเหมา ให้หน่วยงานแจ้งว่าการยกเลิกสัญญานั้น เข้าข่ายเป็นการลาออก หรือให้ออก

๓.๖ ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศรวมถึงวิธีการทำลายข้อมูล แต่ละประเภทตามชั้นความลับ ดังต่อไปนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทตามชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ

(๒) กำหนดกลุ่มผู้ใช้งานให้กับชื่อผู้ใช้งาน เพื่อการตรวจสอบตัวตนจริงของผู้ใช้งานในแต่ละลำดับชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) รอบความถี่ในการทำลายข้อมูล

(๕) ระบุผู้ที่มีหน้าที่ในการทำลายข้อมูล

(๖) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL หรือ VPN หรือ XML Encryption เป็นต้น

(๗) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๘) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน ได้แก่ บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรอง และ ลบข้อมูลที่เก็บอยู่ใน สื่อบันทึกก่อน เป็นต้น

(๙) เจ้าของข้อมูลต้องตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความจำเป็นในการปฏิบัติงาน

๓.๗ การเชื่อมโยงแลกเปลี่ยนข้อมูล ให้ผู้บริหารระดับสูง พิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัยและจุดอ่อนต่าง ๆ ก่อนตัดสินใจเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างกันในระบบสารสนเทศ ได้แก่ ระหว่างกรมวิทยาศาสตร์บริการกับหน่วยงานภายนอก ดังนี้

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการเชื่อมโยงแลกเปลี่ยน ข้อมูลระหว่างกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลลับ

(๓) พิจารณากำหนดผู้ใช้งานใดที่มีสิทธิหรือได้รับอนุญาตให้เข้าถึง

(๔) พิจารณาการลงทะเบียนผู้ใช้งาน

(๕) ต้องไม่อนุญาตการใช้งานข้อมูลสำคัญหรือข้อมูลลับ ในกรณีที่ระบบไม่มีมาตรการ ป้องกันเพียงพอ

ส่วนที่ ๔ การควบคุมการเข้าถึงระบบของผู้ดูแลระบบและผู้ใช้สิทธิพิเศษ (Privileged Access Right)

เพื่อป้องกันการเข้าถึงระบบของผู้ดูแลระบบและผู้ใช้สิทธิพิเศษ ของกรมวิทยาศาสตร์บริการ โดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบ ดังนี้

๔.๑ บัญชีผู้ใช้งานในระดับสูงหรือระดับพิเศษ เช่น ระดับ System (ตัวอย่างเช่น ระดับ root หรือ administrator เป็นต้น) หรือ Power User เป็นต้น ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นเท่านั้น ทั้งนี้ สำหรับบัญชีผู้ใช้งานในระดับ System ผู้ใช้งานต้องใช้บัญชีดังกล่าว เพื่อทำงานที่เกี่ยวข้องกับการดูแลระบบเท่านั้น ส่วนการทำงานทั่วไปอื่น ๆ ให้ใช้บัญชีผู้ใช้งานที่มีสิทธิในระดับปกติ

๔.๒ ในกรณีที่มีความจำเป็นต้องใช้งานบัญชีผู้ใช้งานในระดับ System และสิทธิการเข้าถึงในระดับพิเศษสำหรับการตรวจประเมินภายใน การตรวจประเมินโดยหน่วยงานภายนอก การพัฒนาซอฟต์แวร์ การติดตั้งซอฟต์แวร์ หรือกิจกรรมอื่นใด ที่นอกเหนือไปจากการปฏิบัติงานตามปกติ ต้องดำเนินการดังต่อไปนี้

(๑) กำหนดสิทธิการเข้าถึงในระดับพิเศษ สำหรับ User ID ที่ต่างไปจาก User ID ที่ใช้ในการปฏิบัติงานตามปกติ

(๒) กำหนดระยะเวลาใช้งานของบัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงในระดับพิเศษ

(๓) เพิกถอนบัญชีผู้ใช้งานดังกล่าวทันทีที่ใช้งานเสร็จสิ้นสมบูรณ์

(๔) จัดเก็บและปรับปรุงรายชื่อผู้ใช้งานสิทธิการเข้าถึงในระดับพิเศษทั้งหมด

๔.๓ ให้มีการทบทวนบัญชีผู้ใช้งานที่มีสิทธิระดับสูงหรือระดับพิเศษ อย่างสม่ำเสมออย่างน้อย ปีละ๑ ครั้ง

๔.๔ กำหนดนโยบายหรือมาตรการยืนยันตัวตนของบัญชีผู้ใช้งานที่มีสิทธิระดับสูงหรือระดับพิเศษที่เข้มงวดกว่าบัญชีผู้ใช้งานทั่วไป

๔.๕ การสร้าง การเปลี่ยนแปลง และการเพิกถอน User ID ทั้งหมดที่ได้รับการดำเนินการโดยผู้ดูแลระบบและบุคคลอื่นใดที่มีสิทธิในระดับพิเศษ ต้องได้รับการบันทึก Log เก็บไว้เสมอ รวมถึง ทำการสอบทาน Log ของบัญชีผู้ใช้งานที่มีสิทธิระดับสูงหรือระดับพิเศษ หลังเสร็จสิ้นการใช้งาน หรือสอบทานอย่างสม่ำเสมอ ตามรอบระยะเวลาที่เหมาะสมกับความเสี่ยง หรืออย่างน้อยปีละ ๑ ครั้ง

๔.๖ กรณีที่มีการเปลี่ยนตัวผู้ดูแลระบบ ให้มีการเปลี่ยนรหัสผ่านบัญชีผู้ใช้งานในระดับ System หรือยกเลิกบัญชีผู้ใช้งานเดิม (Disable User Account) และสร้างใหม่ตามความเหมาะสมทันที และเก็บบันทึกข้อมูลผู้ทำหน้าที่ผู้ดูแลระบบอย่างเหมาะสม

๔.๗ การเข้าถึงโปรแกรมอรรถประโยชน์ปฏิบัติการด้วยสิทธิพิเศษในระดับสูง ซึ่งทำให้สามารถเลี่ยงผ่านกลไกการควบคุมระบบงานของกรมวิทยาศาสตร์บริการได้นั้น ต้องถูกจำกัดให้เฉพาะผู้ใช้งาน หรือผู้ดูแลระบบที่มีความจำเป็นต้องใช้งานเป็นประจำเท่านั้น สำหรับการใช้งานและการเข้าถึง System Utilities เหล่านั้นโดยบุคคลอื่น ให้พิจารณาอนุมัติเป็นกรณี ๆ ไป โดยกำหนดระยะเวลาที่อนุญาตให้เข้าถึงได้

๔.๘ โปรแกรมอรรถประโยชน์ในข้อ ๔.๗ ต้องถูกแยกออกจากแอปพลิเคชัน และซอฟต์แวร์อื่น ๆ เพื่อประโยชน์ในการจำกัดการเข้าถึงให้แก่ผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

ส่วนที่ ๕ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

๕.๑ การใช้งานรหัสผ่าน (Password Use)

๕.๑.๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) ของตนเอง

๕.๑.๒ การกำหนดรหัสผ่าน (Password) ที่เดาสุ่มได้ยาก ซึ่งประกอบด้วย

- กำหนดให้ความยาวไม่น้อยกว่า ๘ ตัวอักษร
- ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น "abcdef", "aaaaa" เป็นต้น
- การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับของเดิมครั้งสุดท้าย
- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องผู้ใช้งาน เช่น ชื่อ, นามสกุล หรือวันเกิด เป็นต้น
- ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม
- ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

๕.๑.๓ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

๕.๑.๔ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๕.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

การป้องกันอุปกรณ์เมื่อไม่มีผู้ใช้งาน มีแนวปฏิบัติเพื่อป้องกันผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์ขณะที่ไม่มีผู้ดูแลอุปกรณ์ ดังนี้

๕.๒.๑ มีการกำหนดมาตรการป้องกันทรัพย์สินขององค์กรและควบคุมไม่ให้มีการทิ้ง หรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัยให้ครอบคลุมเรื่องต่าง ๆ คือ การจัดการบริเวณล้อมรอบ การควบคุมการเข้าออก การจัดบริเวณการเข้าถึงกรณีมีการส่งผลิตภัณฑ์โดยบุคคลภายนอก การจัดวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการทำงานในสถานที่ที่มีความปลอดภัย

๕.๒.๒ การนำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัสที่เป็นมาตรฐานสากล รวมถึงมีการวิเคราะห์และคัดเลือกวิธีการเข้ารหัสที่เหมาะสมสำหรับข้อมูลแต่ละประเภทตามมาตรการเข้ารหัสของข้อมูลแต่ละระดับชั้น เช่น

- เว็บไซต์: การใช้โปรโตคอล TLS ในการเข้ารหัสมีความปลอดภัยมากกว่าโปรโตคอล SSL
- การส่งข้อมูลผ่านเครือข่าย: การใช้โปรโตคอล CFI, SCP, SFTP, หรือ FTPS ในการส่งข้อมูลมีความปลอดภัยมากกว่าโปรโตคอล FTP
- การเชื่อมต่อโดย Remote Command: การใช้โปรโตคอล SSH มีความปลอดภัยมากกว่าโปรโตคอล telnet
- การเชื่อมต่อเพื่อบริหารจัดการระบบจากระยะไกล: การเชื่อมต่อผ่านช่องทางที่ปลอดภัย อย่าง SSL VPN, IPSec VPN หรือเครื่องมือที่มีการใช้ช่องทางที่ปลอดภัย

๕.๓ ให้มีการทบทวนมาตรฐานวิธีเข้ารหัสข้อมูล เพื่อให้มั่นใจว่าวิธีการเข้ารหัสที่ใช้งานยังคง มีความปลอดภัย โดยทบทวนอย่างน้อยปีละ ๑ ครั้ง

๕.๔ ให้มีการจัดเก็บบันทึกหลักฐานทั้งการเข้าถึง (Access log) และการดำเนินงาน (Activity log/Audit log) ที่เกี่ยวกับการบริหารจัดการกุญแจเข้ารหัส ได้แก่ การสร้างกุญแจ การสำรองกุญแจ และการเพิกถอนกุญแจ เพื่อการสอบทานในอนาคต รวมถึงมีการสอบทานบันทึกเหตุการณ์เกี่ยวกับการใช้กุญแจเข้ารหัสอย่างสม่ำเสมอตามมาตรการบริหารจัดการบันทึกเหตุการณ์ของระบบสารสนเทศ

๕.๕ ให้มีการกำหนดมาตรการการควบคุมกุญแจเข้ารหัสที่ให้บริการโดยผู้ให้บริการภายนอก โดยกำหนดไว้ในสัญญาว่าจ้างหรือเอกสารแนบท้ายอันเป็นส่วนหนึ่งของสัญญาว่าจ้าง ซึ่งครอบคลุมเนื้อหาขั้นต่ำ ดังต่อไปนี้

(๑) ประเภทของกุญแจเข้ารหัสที่ให้บริการ

(๒) รายละเอียดของระบบหรือเครื่องมือเข้ารหัส รวมถึงกระบวนการควบคุมการเข้ารหัสในแต่ละขั้นตอน ตลอดวงจรการบริหารจัดการกุญแจเข้ารหัส

(๓) ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล

๕.๖ มีการกำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส โดยครอบคลุมเนื้อหา เช่น

- ข้อมูลการติดต่อหน่วยงานและผู้ที่เกี่ยวข้องกับชุดข้อมูลที่ใช้กุญแจเข้ารหัส
- การตรวจสอบชุดข้อมูลที่มีความเสี่ยงในการรั่วไหล การเปลี่ยนหรือเพิกถอนกุญแจการเข้ารหัสข้อมูล

๕.๗ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีผู้ใช้งาน ที่มีกฎหมายกำหนดให้เป็นความผิด ผู้ใช้งานมีหน้าที่รักษารหัสผ่านไว้เป็นความลับ หากเกิดความเสียหายจากการที่ผู้ใช้งานจงใจหรือประมาทเลินเล่ออย่างร้ายแรงในการรักษารหัสผ่าน ผู้ใช้งานต้องรับผิดตามกฎหมาย

๕.๘ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) กรมวิทยาศาสตร์บริการได้กำหนดแนวปฏิบัติเพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ รวมถึงกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน โดยมีแนวปฏิบัติดังนี้

๕.๘.๑ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๕.๘.๒ ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าขณะที่ไม่ได้ใช้งาน เช่น ภายใน ๑๕ นาที ให้เครื่องล็อคหน้าจอ และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๕.๘.๓ ผู้ใช้งานต้องล็อคใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๕.๘.๔ กรณีข้อมูลสำคัญที่บันทึกไว้ใน กระดาษ สื่อบันทึกข้อมูลแฟลชไดรฟ์ หรือ ฮาร์ดดิสก์เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

๕.๘.๕ ผู้ ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

๕.๙ การใช้งานระบบสารสนเทศอย่างปลอดภัย

เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัย และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งาน ดังนี้

๕.๙.๑ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ผู้ใช้งานมีหน้าที่รักษารหัสผ่านไว้เป็นความลับ หากเกิดความเสียหายจากการที่ผู้ใช้งานจงใจหรือประมาทเลินเล่ออย่างร้ายแรงในการรักษารหัสผ่าน ผู้ใช้งานต้องรับผิดตามกฎหมาย

๕.๙.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงานและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อคก็ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๕.๙.๓ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของกรมวิทยาศาสตร์บริการ หรือเป็นบุคคลภายนอก

๕.๙.๔ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของ กรมวิทยาศาสตร์บริการ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารสูงสุด

๕.๙.๕ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่กรมวิทยาศาสตร์บริการต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับกรมวิทยาศาสตร์บริการ ซึ่งกรมวิทยาศาสตร์บริการอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๕.๙.๖ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกันหมายความว่าแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (BitTorrent), อีเมล (Email) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บริหารสูงสุด

๕.๙.๗ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น

๕.๙.๘ ห้ามใช้สินทรัพย์ของ กรมวิทยาศาสตร์บริการที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูลข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของกรมวิทยาศาสตร์บริการ

๕.๙.๙ ห้ามใช้ระบบสารสนเทศของกรมวิทยาศาสตร์บริการ เพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกรมวิทยาศาสตร์บริการ

๕.๙.๑๐ ห้ามใช้ระบบสารสนเทศของ กรมวิทยาศาสตร์บริการเพื่อประโยชน์ทางการค้า

๕.๙.๑๑ ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ในเครือข่ายของกรมวิทยาศาสตร์บริการโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ส่วนที่ ๖ การบริหารจัดการทรัพย์สิน (Asset Management)

๖.๑ ผู้ใช้งานต้องไม่เข้าไปในห้องระบบคอมพิวเตอร์ (หมายถึง สถานที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และ/หรือ อุปกรณ์จัดการเครือข่าย) ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่จะได้รับอนุญาตจาก ผู้บริหารระดับสูง หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

๖.๒ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใด ออกจากห้องระบบคอมพิวเตอร์ เว้นแต่จะได้รับ อนุญาตจากผู้ดูแลระบบ

๖.๓ ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใด เชื่อมต่อเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนตัว

๖.๔ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลของผู้อื่น ก่อนได้รับอนุญาตจากเจ้าของแฟ้มข้อมูล และผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

๖.๕ ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัด อุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญนั้นได้ และ พิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ลำดับ	ประเภทสื่อบันทึกข้อมูล	แนวทางการทำลาย
๑	แฟลชไดรฟ์ (Flash Drive) ฮาร์ดดิสก์ (Hard disk) เอ็กเทอนอลฮาร์ดดิสก์ (External Hard disk)	- ทำลายข้อมูลตามแนวทางของ DOD 5220.22- M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับ ข้อมูลเดิมหลายๆ รอบ - ทุบทำลาย หรือบดให้อุปกรณ์เสียหายไม่สามารถนำไปใช้งานได้
๒	แผ่นซีดี / ดีวีดี (CD/DVD)	- ใช้วิธีการตัด เผา ทำให้สิ้นสภาพการใช้งาน
๓	เทป	- ใช้วิธีทุบ ทำลายให้เสียหายสิ้นสภาพการใช้งาน
๔	กระดาษ	- ตัดด้วยเครื่องทำลายเอกสาร

๖.๖ ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ที่กรมวิทยาศาสตร์บริการ มอบไว้ให้ใช้งาน เสมือนหนึ่งเป็นสินทรัพย์ของ ผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset Lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์ จะต้องได้รับการบันทึกและตรวจสอบทุกครั้ง โดยเจ้าหน้าที่ที่กรมวิทยาศาสตร์บริการ มอบหมายให้รับผิดชอบการดูแลสินทรัพย์

๖.๗ กรณีที่ผู้ใช้งานนำสินทรัพย์ออกนอกกรมวิทยาศาสตร์บริการ ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของกรมวิทยาศาสตร์บริการ ที่ได้รับไว้ใช้งาน

๖.๘ ผู้ใช้งานต้องชดใช้ค่าเสียหาย ไม่ว่าสินทรัพย์นั้นจะชำรุด หรือสูญหายตามมูลค่าของสินทรัพย์ หากความเสียหายนั้นเกิดจากความประมาทเลินเล่ออย่างร้ายแรงของผู้ใช้งาน

๖.๙ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมสินทรัพย์ ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้น ได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

๖.๑๐ ผู้ใช้งานมีสิทธิใช้สินทรัพย์หรือระบบสารสนเทศที่กรมวิทยาศาสตร์บริการ จัดเตรียมไว้ให้ใช้งานตาม วัตถุประสงค์ในการทำงานของกรมวิทยาศาสตร์บริการ ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศไปใช้ในกิจกรรมที่กรมวิทยาศาสตร์บริการ ไม่ได้กำหนด หรือในกิจกรรมที่ก่อให้เกิดความเสียหายต่อกรมวิทยาศาสตร์บริการ

๖.๑๑ ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๖.๑๐ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๖.๑๒ เจ้าของระบบจะต้องจัดทำทะเบียนทรัพย์สินสารสนเทศ (Inventory) ที่ระบุทรัพย์สินของบริการ ที่สำคัญของกรมวิทยาศาสตร์บริการ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

(๑) ลำดับ (No.)
(๒) หมายเลขทรัพย์สิน (Asset Number)
(๓) รายการทรัพย์สิน (Asset)
(๔) รายละเอียดทรัพย์สิน (Detail)
(๕) ประเภททรัพย์สิน (Asset Type)
(๖) เจ้าของอุปกรณ์ (Vendor)
(๗) หน่วยงานที่เป็นผู้รับผิดชอบทรัพย์สิน (Asset Owner)
(๘) สถานที่ตั้งทรัพย์สิน (Location)
(๙) หมายเลขซีเรียล/ เลขไอพี (Serial No./IP Address)
(๑๐) รุ่น (Model Name)
(๑๑) ประกัน (Warranty)

๖.๑๓ ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของกรมวิทยาศาสตร์บริการ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๖.๑๔ ต้องมีการทบทวนและตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของกรมวิทยาศาสตร์บริการ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าว

๖.๑๕ ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของกรมวิทยาศาสตร์บริการ ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ อย่างน้อยปีละ ๑ ครั้ง

๖.๑๖ ให้มีการกำกับและติดตามให้มีการคืนทรัพย์สิน (Return of Assets) ของเจ้าหน้าที่ คู่สัญญา หรือผู้ให้บริการภายนอก อาทิ เครื่องคอมพิวเตอร์พกพา เอกสาร กุญแจ บัตรเจ้าหน้าที่ ที่เป็นทรัพย์สินของกรมวิทยาศาสตร์บริการ ให้กับหน่วยงานที่เกี่ยวข้อง เมื่อเกิดกรณีต่อไปนี้

(๑) เมื่อสิ้นสุดการจ้างงาน ต้องคืนทรัพย์สินของกรมวิทยาศาสตร์บริการ ที่ได้รับไปเพื่อการปฏิบัติงาน

(๒) เมื่อได้รับการเลื่อนตำแหน่งหรือมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ ต้องดำเนินการคืนทรัพย์สินที่ใช้เพื่อปฏิบัติงานตามตำแหน่งงานเดิม และรับมอบทรัพย์สินของตำแหน่งงานใหม่ทดแทน (ถ้ามี)

(๓) เมื่อการว่าจ้างใกล้จะสิ้นสุดลง ให้มีการถ่ายโอนข้อมูลที่เกี่ยวข้องกับการทำงานทั้งหมด และข้อมูลที่ถือว่าเป็นทรัพย์สิน รวมถึงใบอนุญาตใช้งานซอฟต์แวร์ของกรมวิทยาศาสตร์บริการ คืนให้กับกรมวิทยาศาสตร์บริการ อย่างครบถ้วน

(๔) กรณีที่มีการใช้อุปกรณ์ที่ไม่ใช่ทรัพย์สินของกรมวิทยาศาสตร์บริการ ในการปฏิบัติงาน ต้องดำเนินการทำลายข้อมูลของกรมวิทยาศาสตร์บริการ ที่อยู่ในอุปกรณ์เหล่านั้นเมื่อการจ้างงานสิ้นสุดลง หรือเมื่อไม่จำเป็นต้องใช้งาน

๖.๑๗ ให้มีการบำรุงรักษาทรัพย์สินสารสนเทศให้มีสภาพพร้อมใช้งานและรองรับการดำเนินธุรกิจอย่างต่อเนื่อง พร้อมทั้งวางแผนรองรับทรัพย์สินสารสนเทศที่ใกล้จะสิ้นสุดอายุการใช้งาน (End of Life) หรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต (End of Support) ได้อย่างเหมาะสมทันการณ์ พร้อมทั้ง มีมาตรการควบคุมความเสี่ยง ในกรณีที่มีความจำเป็นต้องใช้ทรัพย์สินที่สิ้นสุดอายุการใช้งานหรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต

ส่วนที่ ๗ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการเครือข่ายโดยไม่ได้รับอนุญาต จึงได้กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบดังนี้

๗.๑ การใช้งานบริการเครือข่าย

๗.๑.๑ กำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

๗.๑.๒ กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๗.๑.๓ กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๗.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกกรมวิทยาศาสตร์บริการ (User authentication for external connections)

๗.๒.๑ เมื่อผู้ใช้งานที่อยู่ภายนอกกรมวิทยาศาสตร์บริการ เมื่อต้องเข้าใช้งานระบบสารสนเทศต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

๗.๒.๒ มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงด้วยการใช้รหัสผ่าน (Password)

๗.๒.๓ การเข้าสู่ระบบสารสนเทศของกรมวิทยาศาสตร์บริการ จากเครือข่ายอินเทอร์เน็ตต้องได้รับอนุญาต จากผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ และต้องมีการเข้ารหัสที่เป็นมาตรฐานสากลเพื่อความมั่นคงปลอดภัยด้วย VPN

๗.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment identification in network)

๗.๓.๑ กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย IP Address และ MAC Address

๗.๓.๒ จัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่ใช้เชื่อมกับระบบเครือข่ายของกรมวิทยาศาสตร์บริการ โดยมีรายละเอียดของอุปกรณ์ประกอบด้วย เครื่องคอมพิวเตอร์ IP Address MAC Address สถานที่ติดตั้ง ผู้ใช้งาน เป็นต้น

๗.๓.๓ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับอนุญาตเท่านั้น

๗.๓.๔ ต้องใช้ไฟร์วอลล์ (Firewall) ที่สามารถกำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายของกรมวิทยาศาสตร์บริการได้

๗.๓.๕ จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

๗.๓.๖ แผนผังเครือข่าย เป็นเอกสารในระดับลับมากจะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่ และทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

๗.๔ การป้องกันพอร์ตที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

๗.๔.๑ การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่ายต้องมีการตั้งรหัสผ่านและให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๗.๔.๒ มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย และเปิดใช้เฉพาะอุปกรณ์และเวลาที่จำเป็นเท่านั้น

๗.๔.๓ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น

๗.๔.๔ ติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

๗.๕ การแบ่งแยกเครือข่าย (Segregation in network)

กำหนดให้มีการแบ่งแยกเครือข่ายตามประเภทการใช้งานเพื่อความปลอดภัย ดังนี้

๗.๕.๑ Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

๗.๕.๒ Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

๗.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

เพื่อควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้มีความมั่นคงปลอดภัย ได้กำหนดแนวปฏิบัติดังนี้

๗.๖.๑ จำกัดสิทธิ์ของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

๗.๖.๒ ระบบเครือข่ายต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall, IDS/IPS)

๗.๖.๓ การเข้าสู่ระบบเครือข่ายของกรมวิทยาศาสตร์บริการ ต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยที่กำหนดไว้เท่านั้น

๗.๖.๔ ต้องระบุอุปกรณ์และเครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๗.๖.๕ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบ เครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๗.๖.๖ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนี้

(๑) จำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่าย ที่ได้รับอนุญาตเท่านั้น

(๒) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของกรมวิทยาศาสตร์บริการ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกกรมวิทยาศาสตร์บริการต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกรมวิทยาศาสตร์บริการ ในลักษณะที่ผิดปกติ

(๖) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง หากมีการแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๗) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของกรมวิทยาศาสตร์บริการ ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๘) IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

(๙) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๗.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

การจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือ สารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจซึ่งมีแนวปฏิบัติ ในการจัดเส้นทางบนเครือข่าย ดังนี้

๗.๗.๑ ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๗.๗.๒ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๗.๗.๓ กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก

๗.๗.๔ ต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

๗.๘ การควบคุมการเข้า - ออกห้องระบบคอมพิวเตอร์

(๑) ผู้ติดต่อจากหน่วยงานภายนอก ต้องแลกบัตรที่ใช้ระบุตัวตน ได้แก่ บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor) แล้วลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

(๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์มาใช้ในการปฏิบัติงานที่ห้องระบบคอมพิวเตอร์ ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์ม ขออนุญาตเข้าออก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน

(๓) ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มขออนุญาตเข้าออก กับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

๗.๙ ผู้ดูแลระบบ ต้องบริหารจัดการคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในกำหนด แก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software) ของคอมพิวเตอร์แม่ข่าย

๗.๑๐ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องขออนุมัติจากผู้ดูแลระบบก่อนติดตั้ง

๗.๑๑ กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบรารี่ (Source code Library) และเอกสารสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๗.๑๒ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ถูกต้อง เพื่อใช้ระบุตัวบุคคลผู้เข้าใช้งานระบบคอมพิวเตอร์ และระบบเครือข่ายได้ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมาย ที่เกี่ยวข้อง

ส่วนที่ ๘ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการของกรมวิทยาศาสตร์บริการ โดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบ ดังนี้

๘.๑ ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

๘.๑.๑ กำหนดให้ระบบไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๘.๑.๒ กำหนดให้ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๘.๑.๓ จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน โดยผู้ใช้งานจะต้องป้อนรหัสผ่านภายในเวลา ๑๕ นาที เพื่อเข้าใช้งานระบบ

๘.๑.๔ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๘.๑.๕ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมพักหน้าจอ (Screen sever) เพื่อล็อคหน้าจอภาพเมื่อไม่ได้ใช้งาน ซึ่งผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งานต่อ

๘.๑.๖ ผู้ใช้งานต้องบันทึกเข้าใช้งาน (Login) ทุกครั้งก่อนเข้าใช้ระบบปฏิบัติการ และต้องลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๘.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๘.๒.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

๘.๒.๒ หากต้องการใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นทางด้านเทคนิค หรือสอดคล้องกับการปฏิบัติงาน โดยจะต้องได้รับการอนุมัติจาก ผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ และกำหนดกรอบเวลาการใช้งานที่ชัดเจน และยุติการใช้งานทันทีเมื่อพบความผิดปกติหรือหมดช่วงเวลาที่ขออนุมัติไว้

๘.๓ การบริหารจัดการรหัสผ่าน (Password Management System)

กำหนดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

๘.๓.๑ มีระบบการตรวจสอบการกำหนดรหัสผ่าน ซึ่งประกอบด้วยตัวอักขระ ตัวเลข และตัวอักขระพิเศษ หรือเทคนิคอื่นใดในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) และมีคุณภาพ ผู้ใช้งานทั้งหมดที่ถูกกำหนดไว้เริ่มต้นซึ่งมาพร้อมกับการติดตั้งระบบโดยทันที

๘.๓.๒ เมื่อดำเนินการติดตั้งระบบแล้วให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของรายชื่อผู้ใช้งานทั้งหมดที่ถูกกำหนดไว้เริ่มต้นซึ่งมาพร้อมกับการติดตั้งระบบโดยทันที

๘.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

กำหนดให้มีการจำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่กำหนด โดยมีแนวปฏิบัติ ดังนี้

๘.๔.๑ การใช้งานโปรแกรมอรรถประโยชน์ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

๘.๔.๒ โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

๘.๔.๓ จัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน และเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๘.๔.๔ จำกัดสิทธิ์การใช้งาน เฉพาะผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์เท่านั้น

๘.๔.๕ กำหนดให้ผู้ดูแลระบบมีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

๘.๕ การกำหนดระยะเวลายุติการใช้งานระบบสารสนเทศ (Session Time - Out)

๘.๕.๑ กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมการใช้งานภายในช่วงระยะเวลา ๓๐ นาที

๘.๕.๒ ระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบ เมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นระยะเวลาไม่เกิน ๓๐ นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๘.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection)

เพื่อป้องกันการเข้าถึงระบบสารสนเทศ และโปรแกรมที่มีความเสี่ยงสูง หรือมีความสำคัญสูงกำหนดแนวปฏิบัติในการจำกัดระยะเวลาในการเชื่อมต่อเพื่อความมั่นคงปลอดภัย ดังนี้

๘.๖.๑ กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ภายใน ๑๐ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง

๘.๖.๒ กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะหรือพื้นที่ภายนอกกรม) มีการจำกัดระยะเวลาการเชื่อมต่อไม่เกิน ๑๐ ชั่วโมงต่อครั้ง

ส่วนที่ ๙ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

(Application and Information Access Control)

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศโดยไม่ได้รับอนุญาตกำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบต้องดำเนินการ ดังนี้

๙.๑ จำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน โดยการเข้าใช้งาน การเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ได้กำหนดหลักเกณฑ์การจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศ ดังนี้

๙.๑.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของกรมวิทยาศาสตร์บริการตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิ์ของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิ์การเข้าถึงระบบสารสนเทศและข้อมูล

๙.๑.๒ จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด โดยยกเลิกการเชื่อมต่อระบบเมื่อครบกำหนดเวลา

๙.๑.๓ ผู้ให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน และต้องลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของกรมวิทยาศาสตร์บริการ

๙.๑.๔ ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

๙.๑.๕ ผู้ดูแลระบบต้องควบคุม การเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิ์เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource)

๙.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อ กรมวิทยาศาสตร์บริการต้องแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ กำหนดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ (Mobile Computing and Teleworking) โดยกำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัยไว้ ดังนี้

๙.๒.๑ แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น และแสดงให้เห็น ถึงผลกระทบและระดับความสำคัญต่อกรมวิทยาศาสตร์บริการ

๙.๒.๒ ควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ดังนี้

(๑) ระบบซึ่งไวต่อการรบกวน จะต้องควบคุมการเข้าถึงอุปกรณ์ และระบบ โดยติดตั้งไว้ในในพื้นที่ปลอดภัย

(๒) ติดตามเฝ้าระวังการใช้งานระบบซึ่งไวต่อการรบกวน และระงับการใช้งานทันทีเมื่อพบเหตุการณ์ผิดปกติ

๙.๒.๓ ควบคุมอุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว ดังนี้

(๑) อุปกรณ์ที่ใช้ในการสื่อสาร หรือปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ ต้องนำมาขึ้นทะเบียนกับผู้ดูแลระบบ

(๒) การเข้าถึงระบบโดยการปฏิบัติงานจากภายนอกต้องขออนุมัติการใช้งานจาผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ เพื่อเปิดสิทธิ์ให้ปฏิบัติงานจากผู้ปฏิบัติงานจากภายนอกได้

(๓) ผู้ปฏิบัติงานจากภายนอก ต้องปฏิบัติงานในที่ปลอดภัย และงดการใช้เครือข่าสาธารณะเพื่อเข้าถึงระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

๙.๒.๔ ควบคุมการเข้าใช้งานจากเครือข่ายภายใน และเครือข่ายภายนอกตามข้อกำหนด

๙.๒.๕ วางแผนการสำรอง และทดสอบการกู้คืนระบบ ตามคู่มือการสำรองระบบสารสนเทศ

๙.๓ การควบคุมอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่

กำหนดแนวปฏิบัติและมาตรการเพื่อปกป้องระบบสารสนเทศ ซึ่งจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ โดยผู้ใช้งานอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ต้องปฏิบัติ ดังนี้

๙.๓.๑ การป้องกันอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ครอบคลุมการใช้งานอุปกรณ์สื่อสารประเภทพกพา ได้แก่ Smart Phone, Notebook, Laptop, Tablet หรืออุปกรณ์อื่นใดในลักษณะเดียวกันนี้ โดยกำหนดให้มีการป้องกัน การเชื่อมต่อของอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่เข้ากับเครือข่ายของกรมวิทยาศาสตร์บริการ โดยไม่ได้รับอนุญาต

๙.๓.๒ กำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ ซึ่งจะต้องแสดงตัวตนเมื่อเข้าใช้งาน

๙.๓.๓ ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ของตนเอง

๙.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

เพื่อปกป้องระบบสารสนเทศจากการปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ กำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัย ดังนี้

๙.๔.๑ การปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการและระบบงานต่างๆ ภายในกรมวิทยาศาสตร์บริการ

๙.๔.๒ การเข้าถึงระบบสารสนเทศของกรมวิทยาศาสตร์บริการ จากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัว ต้องได้รับอนุญาตจากผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๙.๔.๓ การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการได้ ต้องมีหนังสือเป็นลายลักษณ์อักษร และมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ โดยระบุรายละเอียดการขอเปิดใช้งานระบบสารสนเทศจากภายนอกกรมวิทยาศาสตร์บริการ โดยมีรายละเอียด ดังนี้

(๑) เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ

(๒) รายละเอียดและลักษณะของระบบงาน

(๓) ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ

(๔) รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน

(๕) ช่วงเวลาและระยะเวลาในการปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ

๙.๔.๔ ไม่อนุญาตให้ปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ สำหรับระบบงานที่มีความลับในระดับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

๙.๔.๕ การเข้าสู่ระบบสารสนเทศของกรมวิทยาศาสตร์บริการ จากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๙.๔.๖ ผู้ได้รับอนุญาตให้สามารถเข้าถึงระบบสารสนเทศและข้อมูลของกรมวิทยาศาสตร์บริการต้องไม่ให้สมาชิกภายในครอบครัว หรือบุคคลอื่นใดสามารถเข้าถึงระบบได้ด้วยสิทธิ์ของตนเอง

๙.๔.๗ ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

๙.๔.๘ ผู้ดูแลระบบจะทำการยกเลิกสิทธิ์การเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกกรมวิทยาศาสตร์บริการของผู้ใช้งานทันที เมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๙.๔.๙ ผู้ดูแลระบบต้องทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกกรมวิทยาศาสตร์บริการ อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๐ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี

(Software Licensing and intellectual property and Preventing Malware)

เพื่อบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และป้องกันการโปรแกรมไม่ประสงค์ดี กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบต้องดำเนินการ ดังนี้

๑๐.๑ ซอฟต์แวร์ที่กรมวิทยาศาสตร์บริการ อนุญาตให้ใช้งาน หรือที่ กรมวิทยาศาสตร์บริการ มีลิขสิทธิ์

ผู้ใช้งานสามารถขอใช้งานได้ตาม หน้าที่และความจำเป็น โดยห้ามผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่า เป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

๑๐.๒ ซอฟต์แวร์ที่กรมวิทยาศาสตร์บริการ จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามผู้ใช้งานติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ยกเว้นได้รับการอนุญาตจากผู้บริหารระดับสูง หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ หรือผู้ที่มีสิทธิในลิขสิทธิ์

๑๐.๓ คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่กรมวิทยาศาสตร์บริการ ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องที่ใช้เพื่อการศึกษาหรือทดสอบที่ได้รับอนุญาตจาก ผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

๑๐.๔ ต้องตรวจสอบข้อมูล แฟ้มข้อมูล ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่น เพื่อตรวจจับไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดี ก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๑๐.๕ ผู้ใช้งานต้องปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น

๑๐.๖ ผู้ใช้งานต้องระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานจะต้องแจ้งเหตุแก่ผู้ดูแลระบบผ่านเบอร์โทรติดต่อ

๑๐.๗ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

๑๐.๘ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของกรมวิทยาศาสตร์บริการ หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติ หน้าที่ หากพบว่ามีการฝ่าฝืน จะมีการพิจารณาบทลงโทษตาม พ.ร.บ.ระเบียบข้าราชการพลเรือน พ.ศ. ๒๕๕๑ ประกอบกฎ ก.พ. ว่าด้วยการดำเนินการทางวินัย พ.ศ. ๒๕๕๖ สำหรับข้าราชการ และระเบียบสำนักนายกรัฐมนตรีว่าด้วยพนักงานราชการ พ.ศ. ๒๕๔๗

๑๐.๙ ห้ามเผยแพร่ไวรัสคอมพิวเตอร์ โปรแกรมไม่ประสงค์ดี หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายต่อสินทรัพย์ของกรมวิทยาศาสตร์บริการ แต่การพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ อาจกระทำได้โดยห้ามดำเนินการ ดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสารสนเทศ รวมทั้งการกระทำในลักษณะที่เป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลของบุคคลอื่น หรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใด ๆ ที่จะทำซ้ำตัวโปรแกรม หรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะได้แก่เดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

(๕) สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ที่นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์

แสดงข้อความรูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย

๑๐.๑๐ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีกระบวนการควบคุมโครงการพัฒนาซอฟต์แวร์ที่จัดจ้างผู้รับจ้างพัฒนาภายนอก

(๒) กรมวิทยาศาสตร์บริการ ถือสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดของซอฟต์แวร์ที่ได้รับการพัฒนา โดยผู้รับจ้างพัฒนาภายนอก

(๓) กำหนดการสงวนสิทธิที่จะตรวจสอบคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะพัฒนา โดยให้ระบุไว้ในสัญญาจ้างที่จะทำกับผู้รับจ้างพัฒนาภายนอกนั้น

(๔) ให้ตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะติดตั้งก่อนติดตั้งทุกครั้ง

(๕) หลังจากติดตั้งระบบเพื่อใช้งาน ต้องยกเลิกบัญชีผู้ใช้งาน หรือเปลี่ยนรหัสผ่านของผู้ใช้งานทุกรายที่ถูกกำหนดเอาไว้เป็นค่าเริ่มต้นที่มาพร้อมกับระบบในทันที

ส่วนที่ ๑๑ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

เพื่อให้การเข้าถึงระบบเครือข่ายไร้สายในกรมวิทยาศาสตร์บริการมีความมั่นคงปลอดภัยกำหนดแนวทางปฏิบัติ เพื่อควบคุมการเข้าถึงระบบเครือข่ายไร้สายไว้ ดังนี้

๑๑.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรมวิทยาศาสตร์บริการ จะต้องลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑๑.๒ ผู้ดูแลระบบต้องดำเนินการลงทะเบียนผู้ใช้งาน ดังนี้

๑๑.๒.๑ ลงทะเบียน และกำหนดสิทธิ์ผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๑๑.๒.๒ ต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๑๑.๒.๓ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๑๑.๒.๔ ดำเนินการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน และกำหนดให้ซ่อน SSID (Service Set Identifier) เพื่อความปลอดภัย

๑๑.๒.๕ เปลี่ยนค่าชื่อผู้ใช้งานและรหัสผ่านในการเข้าสู่ระบบ สำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและเลือกใช้ชื่อผู้ใช้งานและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถคาดเดาหรือเจาะรหัสได้โดยง่าย

๑๑.๒.๖ กำหนดค่าใช้ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจาย (Access Point) เพื่อให้ยากต่อการดักจับ และเพิ่มความปลอดภัยให้กับระบบเครือข่ายไร้สาย

๑๑.๒.๗ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้สามารถเข้าใช้ระบบเครือข่ายไร้สายได้

๑๑.๒.๘ ควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สาย กับเครือข่ายภายในกรมวิทยาศาสตร์บริการ

๑๑.๒.๙ ใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการทันที

ส่วนที่ ๑๒ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

๑๒.๑ ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของอุปกรณ์ป้องกันเครือข่ายทั้งหมด

๑๒.๒ ต้องกำหนดค่าเริ่มต้นของอุปกรณ์ป้องกันเครือข่าย (Firewall) ให้เป็นปฏิเสธทั้งหมด (Deny)

๑๒.๓ บริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายและแนวปฏิบัติของกรมวิทยาศาสตร์บริการ จะต้องถูกบล็อค (Block) โดย Firewall

๑๒.๔ ผู้ใช้งานอินเทอร์เน็ตจะต้องพิสูจน์ตัวตน (Authentication) ก่อนการใช้งานทุกครั้ง

๑๒.๕ จะต้องบันทึกการเปลี่ยนแปลงค่าบริการและการเชื่อมต่อที่อนุญาต ทุกครั้งที่เปลี่ยนแปลงค่าต่าง ๆ ของอุปกรณ์ป้องกันเครือข่าย ได้แก่ ค่า Parameter เป็นต้น

๑๒.๖ ให้เฉพาะผู้ได้รับมอบหมายให้ดูแลจัดการเท่านั้น ที่สามารถเข้าถึงตัวอุปกรณ์ป้องกันเครือข่าย

๑๒.๗ จะต้องส่งข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ป้องกันเครือข่าย ไปจัดเก็บที่ อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๑๒.๘ การให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ตการเชื่อมต่อพื้นฐานของ

โปรแกรมทั่วไปที่อนุญาตให้ใช้งาน หากผู้ใช้งานมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อที่นอกเหนือไปจากที่กำหนด จะต้องได้รับอนุญาตจากผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

๑๒.๙ จะต้องกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อกำหนดตามนโยบายการป้องกันเครือข่าย (Policy) จะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องที่ให้บริการจริง

๑๒.๑๐ จะต้องสำรองข้อมูลค่าต่าง ๆ ที่กำหนดของอุปกรณ์ป้องกันเครือข่าย เป็นประจำทุกสัปดาห์และทุกครั้งก่อนที่จะเปลี่ยนแปลง

๑๒.๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศของกรมวิทยาศาสตร์บริการ ที่มีลักษณะที่เป็นอินทราเน็ตจะไม่อนุญาตให้เชื่อมต่อเพื่อใช้งานผ่านอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

๑๒.๑๒ กรมวิทยาศาสตร์บริการ มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรม การใช้งานที่ผิดนโยบายการป้องกันเครือข่าย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

๑๒.๑๓ จะต้องบันทึกรายการของการเชื่อมต่อในลักษณะของการควบคุมระยะไกล (Remote Login) จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน ตามแบบการขออนุญาตดำเนินการ เกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และต้องได้รับอนุญาตก่อนจากผู้บริหารระดับสูงหรือ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่

๑๒.๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของอุปกรณ์ป้องกันเครือข่าย จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ส่วนที่ ๑๓ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : อีเมล)

๑๓.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมวิทยาศาสตร์บริการ ให้เหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๑๓.๒ ผู้ดูแลระบบรับเรื่องการขอใช้งานจดหมายอิเล็กทรอนิกส์ของกรมวิทยาศาสตร์บริการ โดยกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานอีเมล รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งาน

๑๓.๓ กำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านใหม่ทันที เมื่อได้รับรหัสผ่านครั้งแรก (Default Password) และต้องเปลี่ยนรหัสผ่านใหม่ทุก ๑๘๐ วัน หรือเมื่อได้รับแจ้งให้เปลี่ยนรหัสผ่าน

๑๓.๔ ผู้ดูแลระบบต้องกำหนดให้การเข้ารหัสผ่านจดหมายอิเล็กทรอนิกส์ เมื่อใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘x’ หรือ ‘*’ ในการพิมพ์แต่ละตัวอักษร

๑๓.๕ กำหนดให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

๑๓.๖ ระบบจดหมายอิเล็กทรอนิกส์จะออกจากระบบ (Log out) เพื่อตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาภายใน ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

๑๓.๗ ผู้ใช้งานควรหลีกเลี่ยงค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๑๓.๘ ผู้ใช้งานต้องระมัดระวังในการใช้อีเมล เพื่อไม่ให้เกิดความเสียหายต่อกรมวิทยาศาสตร์บริการ ได้แก่ การละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์รวมทั้งไม่อนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้อีเมล ผ่านระบบเครือข่ายของกรมวิทยาศาสตร์บริการ

๑๓.๙ ผู้ใช้งานต้องไม่ใช้ที่อยู่อีเมล (E-mail Address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของอีเมล

๑๓.๑๐ หลังจากการใช้งานอีเมลเสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานอีเมล โดยไม่ได้รับอนุญาต

๑๓.๑๑ ผู้ใช้งานควรตรวจสอบเอกสารแนบจากอีเมล ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันไวรัสโดยเฉพาะการเปิดไฟล์ที่เป็น Executable File เช่น .exe หรือ .com เป็นต้น

๑๓.๑๒ ผู้ใช้งานไม่เปิดหรือส่งต่ออีเมล หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๓.๑๓ ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับ-ส่งอีเมล ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียง หรือข้อมูลทำให้เกิดความแตกแยกผ่านทางอีเมล

๑๓.๑๔ ผู้ใช้งานควรตรวจสอบตู้เก็บอีเมล (Inbox) ของตนเองทุกวัน และควรลบอีเมลที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่บนอีเมล

ส่วนที่ ๑๔ การควบคุมการใช้อินเทอร์เน็ต (Internet)

กำหนดแนวปฏิบัติเพื่อควบคุมการใช้งานอินเทอร์เน็ตอย่างปลอดภัย ดังนี้

๑๔.๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่กรมวิทยาศาสตร์บริการจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Mobile Hotspot Wi-Fi,

Pocket Wi-Fi หรืออุปกรณ์ที่มีลักษณะการทำงานคล้ายกัน ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการเป็นลายลักษณ์อักษร

๑๔.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

๑๔.๓ การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๑๔.๔ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของกรมวิทยาศาสตร์บริการ เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับกรมวิทยาศาสตร์บริการ

๑๔.๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมวิทยาศาสตร์บริการที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๑๔.๖ ระมัดระวังการดาวน์โหลดโปรแกรมจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

๑๔.๗ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์จะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของกรมวิทยาศาสตร์บริการ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรมวิทยาศาสตร์บริการ การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๑๔.๘ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๑๔.๙ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ (Web Browser) และออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๑๔.๑๐ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

ส่วนที่ ๑๕ การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๕.๑ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักในเรื่องความมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือข้อมูลความลับของกรมวิทยาศาสตร์บริการ

๑๕.๒ ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรมวิทยาศาสตร์บริการ

๑๕.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อกรมวิทยาศาสตร์บริการ ผู้ใช้งานต้องแจ้งต่อกลุ่มเทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

ส่วนที่ ๑๖ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๑๖.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ โดยผู้ดูแลระบบ ดังนี้

๑๖.๑.๑ ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

๑๖.๑.๒ ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

๑๖.๑.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติจากผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ ก่อนดำเนินการ

๑๖.๑.๔ ไม่ติดตั้งซอร์สโค้ดคอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๑๖.๑.๕ กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

๑๖.๑.๖ กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบสารสนเทศ เป็นต้น

๑๖.๑.๗ วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

๑๖.๑.๘ จัดเก็บซอฟต์แวร์เวอร์ชั่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ที่ไม่ได้ใช้งานไว้อย่างปลอดภัยเพื่ออ้างอิง

๑๖.๒ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ

๑๖.๒.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๑๖.๒.๒ วางแผนเฝ้าระวังและทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

๑๖.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๑๖.๓.๑ กำหนดให้มีการควบคุมการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

๑๖.๓.๒ ระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๑๖.๓.๓ กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๑๖.๓.๔ กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ก่อนมีการติดตั้ง

๑๖.๓.๕ การทดสอบซอฟต์แวร์ห้ามทดสอบบนระบบ และฐานข้อมูลที่ใช้งาน เลือกสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

๑๖.๔ มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

๑๖.๔.๑ ผู้ให้บริการที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของกรมวิทยาศาสตร์บริการจะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจาก ผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๑๖.๔.๒ ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

๑๖.๔.๓ กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๑๖.๔.๔ การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็นช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการก่อนทุกครั้ง

๑๖.๕ มาตรการควบคุมช่องโหว่ทางเทคนิค

๑๖.๕.๑ กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน และบริหารจัดการช่องโหว่ของระบบเหล่านั้น โดยมีการบันทึกข้อมูลอย่างน้อย ดังนี้

(๑) ชื่อซอฟต์แวร์และเวอร์ชั่นที่ใช้งาน

(๒) สถานที่ที่ติดตั้ง

(๓) เครื่องแม่ข่ายที่ติดตั้ง

(๔) ผู้ผลิตซอฟต์แวร์

(๕) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

๑๖.๕.๒ กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

๑๖.๕.๓ กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบ ดำเนินการดังนี้

(๑) มีการเฝ้าระวังและติดตามประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

(๒) กำหนดแหล่งข้อมูลข่าวสาร สำหรับใช้ในการติดตามช่องโหว่ระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

(๓) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

๑๖.๕.๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๑๖.๕.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ข้อมูลชื่อบัญชีผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลการล็อกอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลการเปลี่ยนคอนฟิกกูเรชั่น (Configuration) ของระบบ

(๘) ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)

(๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

(๑๐) ข้อมูลไอพีแอดเดรส (IP Address) ที่เข้าถึง

(๑๑) ข้อมูลโพรโทคอล (Protocol) เครือข่ายที่ใช้

(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จครื่องคอมพิวเตอร์แม่ข่าย (Server)

ส่วนที่ ๑๗ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)

เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลให้มีความปลอดภัย กำหนดแนวปฏิบัติ ดังนี้

๑๗.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลที่กรมวิทยาศาสตร์บริการอนุญาตให้ผู้ใช้ระบบสารสนเทศใช้งานเป็นทรัพย์สินของกรมวิทยาศาสตร์บริการ ที่ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

๑๗.๒ โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของกรมวิทยาศาสตร์บริการ ต้องเป็นโปรแกรมที่กรมวิทยาศาสตร์บริการได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคลหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย และห้ามผู้ใช้งานติดตั้ง แก้ไขโปรแกรมด้วยตนเอง ผู้ดูแลระบบมีหน้าที่จัดหาและติดตั้งโปรแกรมในเครื่องของกรมวิทยาศาสตร์บริการเท่านั้น

๑๗.๓ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของกรมวิทยาศาสตร์บริการ หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับกรมวิทยาศาสตร์บริการเท่านั้น การนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกนอกกรมวิทยาศาสตร์บริการเพื่อการใดก็ตาม ต้องขออนุมัติผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการเป็นลายลักษณ์อักษรเท่านั้น

๑๗.๔ การใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบสื่อ เพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลก่อนทุกครั้ง

๑๗.๕ ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ดังนี้

๑๗.๕.๑ กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เพื่อเปิดใช้เครื่องและเก็บรักษารหัสผ่านอย่างปลอดภัย

๑๗.๕.๒ เมื่อไม่ได้ใช้งานเกิน ๑๕ นาที ควรตั้งโปรแกรมรักษาจอภาพ (Screen Saver) และต้องใช้รหัสผ่านเพื่อเข้าใช้งานอีกครั้ง และเมื่อเลิกใช้งานควรล็อคเอาท์ (Log Out) ออกจากเครื่อง

๑๗.๕.๓ ต้องอัพเดต (Update) ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ ส่วนบุคคลของกรมวิทยาศาสตร์บริการ

๑๗.๕.๔ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่มิได้ขึ้นทะเบียนอุปกรณ์กับผู้ดูแลระบบ มาใช้งานและเชื่อมต่อกับระบบเครือข่ายของกรมวิทยาศาสตร์บริการ ยกเว้นจะได้รับอนุญาตเป็นลายลักษณ์อักษรและนำมาขึ้นทะเบียนกับผู้ดูแลระบบของกรมวิทยาศาสตร์บริการก่อนการใช้งาน

๑๗.๕.๕ ต้องไม่ถอดถอนการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ในเครื่องคอมพิวเตอร์

ส่วนที่ ๑๘ การใช้งานอุปกรณ์และเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

๑๘.๑ เครื่องคอมพิวเตอร์แบบพกพาทีหน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของกรมวิทยาศาสตร์บริการ เพื่อใช้ในงานราชการ ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพร้อมใช้งาน

๑๘.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของกรมวิทยาศาสตร์บริการต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑๘.๓ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เพื่อเปิดเข้าใช้งานเครื่องทุกครั้ง และควรกำหนดรหัสผ่านให้ยากต่อการคาดเดา และเก็บรักษาไว้เป็นความลับ

๑๘.๔ ตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) เมื่อไม่ได้ใช้งานเกิน ๑๕ นาที เพื่อล็อกหน้าจอเมื่อไม่มีการใช้งาน และต้องใส่รหัสผ่านอีกครั้งเมื่อกลับมาใช้งาน

๑๘.๕ ต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งาน

๑๘.๖ ต้องสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา ลงบนสื่อจัดเก็บที่ปลอดภัย เพื่อป้องกันการสูญหายของข้อมูล และจัดเก็บอย่างปลอดภัย หรือกำหนดรหัสการเข้าสื่อบันทึกข้อมูล รวมถึงการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๘.๗ การเคลื่อนย้ายคอมพิวเตอร์แบบพกพา ต้องดำเนินการด้วยความระมัดระวัง เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือพลัดหลุดมือ เป็นต้น หลีกเลี่ยงการใส่เครื่องคอมพิวเตอร์พกพาไว้ในกระเป๋าเดินทาง เพราะอาจถูกกดทับเกิดความเสียหายได้

๑๘.๘ หลีกเลี่ยงการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดอยู่ กรณีต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์ภายในเครื่อง

๑๘.๙ ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

(๓) หลีกเลี่ยงการวางเครื่องคอมพิวเตอร์พกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ และวางไว้หรือใช้งานในที่ที่มีแรงสั่นสะเทือนมาก

(๔) ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(๕) หลีกเลี่ยงการใช้วัสดุ หรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน ไม่วางของทับบนหน้าจอและแป้นพิมพ์ หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๖) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดด้วยความระมัดระวัง ควรเช็ดไปในแนวทางเดียวกัน ไม่ควรเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๗) ดูแลบำรุงรักษาเครื่องคอมพิวเตอร์แบบพกพาให้อยู่ในสภาพพร้อมใช้งาน พักเครื่องเมื่อต้องใช้เป็นระยะเวลานานเกินไป หรือในสภาพที่มีอากาศร้อนจัด

ส่วนที่ ๑๙ การตรวจจับ/ป้องกันการบุกรุก (Intrusion Detection System/Intrusion Prevention System Policy: IDS/IPS)

๑๙.๑ นโยบายตรวจจับ/ป้องกันการบุกรุก (IDS/IPS Policy) เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันสินทรัพย์ ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในของกรมวิทยาศาสตร์บริการ ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

๑๙.๒ นโยบายตรวจจับ/ป้องกันการบุกรุกครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของกรมวิทยาศาสตร์บริการ และระบบเครือข่ายทั้งหมด รวมถึงเส้นทางที่ไม่อยู่ในเครือข่ายอินเทอร์เน็ตที่ข้อมูลอาจเดินทางทุกเส้นทาง

๑๙.๓ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะ จะต้องผ่านการ ตรวจสอบจากระบบตรวจจับ/ป้องกันการบุกรุก

๑๙.๔ ระบบทั้งหมดที่ใน DMZ (Demilitarized Zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

๑๙.๕ ต้องบันทึกผลการตรวจสอบโฮสต์ (Host) และระบบเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่านระบบตรวจจับ/ป้องกันการบุกรุก

๑๙.๖ ต้องตรวจสอบและ Update Patch/Signature ของระบบตรวจจับ/ป้องกันการบุกรุกเป็นประจำ

๑๙.๗ ผู้ดูแลระบบต้องตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวัน

๑๙.๘ ระบบตรวจจับ/ป้องกันการบุกรุกจะทำงานภายใต้กฎควบคุมพื้นฐานของอุปกรณ์ป้องกันเครือข่าย ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

๑๙.๙ ต้องตรวจสอบข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งระบบตรวจจับ/ป้องกันการบุกรุก (IDS/IPS) เป็นประจำทุก ๆ วัน

๑๙.๑๐ จะต้องรายงาน จัดประเภท และวิเคราะห์พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือพยายามเข้าระบบทั้งที่ประสบความสำคัญและไม่ประสบความสำเร็จ ให้ผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ทราบทันทีที่ตรวจพบ

๑๙.๑๑ จะต้องรายงานพฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติให้ผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ ทราบภายใน ๑ ชั่วโมงหลังจากตรวจพบ

๑๙.๑๒ ต้องเก็บบันทึกข้อมูลการตรวจสอบการบุกรุกทั้งหมดไว้ไม่น้อยกว่า ๙๐ วัน

๑๙.๑๓ ระบบตรวจจับ/ป้องกันการบุกรุกต้องตอบสนองต่อเหตุการณ์ที่เกิดขึ้นในรูปแบบต่าง ๆ ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่าง ๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์ไม่ประสงค์ดีที่ตรวจพบป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย

๑๙.๑๔ กรมวิทยาศาสตร์บริการ มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องแจ้งแก่ผู้ใช้งานทราบล่วงหน้า

๑๙.๑๕ ผู้ที่ถูกตรวจสอบว่า พยายามละเมิดนโยบายด้านความมั่นคงปลอดภัยของกรมวิทยาศาสตร์บริการ พยายามเข้าถึงระบบโดยมิชอบ โจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศจะถูกระงับการ ใช้เครือข่ายทันที และหากการกระทำดังกล่าว เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และสินทรัพย์ของกรมวิทยาศาสตร์บริการ จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

๑๙.๑๖ ต้องมีการทบทวนกลไกขั้นตอน และกระบวนการตรวจสอบและฝ้าระวังภัยคุกคามทาง

ไซเบอร์ หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่กำหนดในส่วนที่ ๑๙ นี้อย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

ส่วนที่ ๒๐ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

๒๐.๑ ปรับปรุงระบบปฏิบัติการ (Operating System Update) ดังนี้

(๑) ตรวจสอบเครื่องแม่ข่าย และอุปกรณ์ระบบ

(๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

(๓) กำหนดชื่อและรหัสผ่านผู้ดูแลระบบและชื่อผู้ใช้งาน (User)

(๔) กำหนดค่าติดตั้งชื่อเครื่อง (Computer Name)/IP Address

(๕) ปรับปรุง/กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี Service Patch Update)

(๖) ติดตั้งโปรแกรม Antivirus/ปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการตรวจจับและปรับปรุงโปรแกรม

๒๐.๒ บริหารบัญชีผู้ใช้งาน/สิทธิการเข้าถึงและการใช้งานระบบ (User Management) ดังนี้

(๑) กำหนดบัญชีผู้ดูแลระบบ (System Administrator Account)

(๒) กำหนดบัญชีผู้ใช้งาน (User Account)

(๓) บันทึกบัญชีผู้ใช้งานและสิทธิการเข้าใช้ระบบ

๒๐.๓ ปรับปรุงการรักษาความปลอดภัย/Anti-Virus (System Security & Antivirus Update)

(๑) ติดตาม เฝ้าระวัง การทำงานของคอมพิวเตอร์และการเข้าใช้ระบบปฏิบัติการ

(๒) ตรวจสอบการทำงาน (Performance) ของระบบปฏิบัติการ หรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

(๓) ปรับปรุง/กำหนดค่าระบบความปลอดภัยให้เหมาะสมกับสภาพการใช้งาน

(๔) ปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

(๕) ตรวจจับไวรัสคอมพิวเตอร์ (Scan) เป็นประจำ

๒๐.๔ ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อมูล (Database Management Operation) ดังนี้

(๑) ติดตั้งระบบจัดการฐานข้อมูล ตามความต้องการของระบบสารสนเทศ

(๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูลให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพ ตามข้อกำหนดของระบบฐานข้อมูล

(๓) สร้างและกำหนดรายชื่อผู้บริหารระบบฐานข้อมูล (Database Admin) ชื่อผู้ใช้งานอื่น และสิทธิการใช้งาน

(๔) ปรับปรุง/กำหนดค่าระบบให้เหมาะสม หรือป้องกันการเกิดปัญหาเป็นประจำ

๒๐.๕ ติดตั้งฐานข้อมูลโปรแกรมระบบสารสนเทศหรือกำหนดค่าระบบของโปรแกรมรวมทั้ง กำหนดบัญชีผู้ใช้และสิทธิการเข้าใช้งานหรือเข้าถึงฐานข้อมูล

(๑) ติดตั้งโปรแกรมระบบสารสนเทศตามความต้องการหรือรุ่นการพัฒนา

(๒) กำหนดค่าโปรแกรมหรือบริการ (Services) ให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพ

(๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบสารสนเทศ และทดสอบการใช้งานตามที่กำหนด

(๔) แจ้งผู้ใช้งานให้ใช้งาน โดยแจ้งชื่อบัญชีผู้ใช้และสิทธิการเข้าใช้ระบบสารสนเทศตาม ที่กำหนดไว้

(๕) กำหนดเกณฑ์การสำรอง/สำเนา/ทดสอบกู้คืน (Restore Test)

(๖) บันทึกข้อกำหนด ค่าติดตั้ง และบัญชีผู้ใช้งานแต่ละระดับของระบบสารสนเทศทุกครั้งที่สร้างหรือปรับปรุง

๒๐.๖ การสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงานหรือแอปพลิเคชัน และอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่ายทั้งหมดของบริการที่สำคัญของกรมวิทยาศาสตร์บริการให้สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของ กรมวิทยาศาสตร์บริการ โดยต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังนี้

(๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

(๒) การแบ่งแยกหน้าที่ (Separation of Duties)

(๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

(๔) การลบบัญชีที่ไม่ได้ใช้

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

(๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(๗) การป้องกันมัลแวร์ (Malware)

(๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์ และเหมาะสม

(๙) การแสดงข้อความแจ้งเตือนต้องไม่เกินความจำเป็น หรือบ่งชี้อย่างเจาะจงว่าข้อมูลส่วนใดส่วนหนึ่งผิดพลาด เช่น ใช้ถ้อยคำว่า "ชื่อผู้ใช้งานหรือรหัสผ่านไม่ถูกต้อง" แทนการแจ้งเตือนว่า "รหัสผ่านไม่ถูกต้อง" เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีคาดเดาได้ รวมทั้งต้องไม่แสดงข้อมูลภายในของระบบ เช่น เวอร์ชัน และ ยี่ห้อ ของระบบงาน IP Address และ Path เป็นต้น

๒๐.๗ ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของ กรมวิทยาศาสตร์บริการ รวมทั้งต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของกรมวิทยาศาสตร์บริการ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒๐.๘ ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของ กรมวิทยาศาสตร์บริการ

ส่วนที่ ๒๑ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์และการเฝ้าระวัง (Logging and Monitoring)

๒๑.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ โดยให้กำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว และต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน

๒๑.๒ ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

๒๑.๓ กำหนดให้บันทึกการทำงานของระบบบันทึกการเข้าใช้งานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้า - ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๒๑.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น ให้เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น

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

ส่วนที่ ๒๒ การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Data and Information Security)

๒๒.๑ ผู้ใช้งานระบบจะต้องพึงระวังให้ข้อมูลข่าวสารที่เป็นทรัพย์สินของ กรมวิทยาศาสตร์บริการว่าอยู่ในสภาพปลอดภัยจากการเข้าถึงโดยไม่ได้รับอนุญาต โดยการระวังและติดตามบุคคลภายนอกที่เข้ามาหาในกรมวิทยาศาสตร์บริการ ให้อยู่ในการควบคุมดูแล กำหนดเอกสารที่มีความสุมเสี่ยงหรือเป็นเอกสารที่ไม่เปิดเผยและทำลายเอกสารทิ้งเมื่อไม่มีความจำเป็นต้องใช้งานแล้ว

๒๒.๒ ผู้ใช้งานระบบต้องทำการจัดหมวดหมู่ของทรัพย์สินสารสนเทศและทรัพย์สินอื่น ๆ ที่เกี่ยวข้อง

ให้เป็นไปตามกระบวนการจัดระดับชั้นความลับสารสนเทศที่ กรมวิทยาศาสตร์บริการ กำหนด และทำการเก็บรักษาและทำลายข้อมูลให้เหมาะสมกับชั้นความลับ และมีการบริหารจัดการการเข้ารหัสข้อมูล (Cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากล เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล

๒๒.๓ ผู้ดูแลระบบจะจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล ทั้งในการรับส่งข้อมูลผ่านเครือข่ายสื่อสารและการจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง

ส่วนที่ ๒๓ การรักษาความมั่นคงปลอดภัยของฐานข้อมูล (Database Security)

๒๓.๑ การใช้ฐานข้อมูลร่วมหรือแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก หรือหน่วยงานภายนอกขอใช้ข้อมูล ให้จัดทำบันทึกข้อตกลงการใช้ หรือแลกเปลี่ยนข้อมูลสารสนเทศระหว่าง กรมวิทยาศาสตร์บริการกับหน่วยงานภายนอก ดังต่อไปนี้

(๑) กำหนดนโยบายขั้นตอนปฏิบัติและมาตรฐาน เพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะจัดส่งระหว่างกัน

(๒) กำหนดหน้าที่ความรับผิดชอบของผู้เกี่ยวข้อง และขั้นตอนปฏิบัติในการแลกเปลี่ยน หรือใช้ข้อมูลร่วมกัน ได้แก่ วิธีการรับ-ส่ง เป็นต้น

(๓) กำหนดหน้าที่และความรับผิดชอบของแต่ละฝ่ายในการป้องกันข้อมูลรั่วไหล หรือสูญหาย ตลอดจนระบุผู้รับผิดชอบในกรณีที่ข้อมูลสูญหายหรือเสียหาย

(๔) กำหนดขั้นตอนในการตรวจสอบผู้ส่งข้อมูลและผู้รับข้อมูล เพื่อป้องกันการปฏิเสธความรับผิดชอบ

(๕) กำหนดสิทธิในการเข้าถึงข้อมูลของแต่ละฝ่าย

(๖) กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

(๗) กำหนดมาตรการพิเศษสำหรับป้องกันเอกสารข้อมูลซอฟต์แวร์หรืออื่น ๆ ที่มีความสำคัญ ได้แก่ กุญแจที่ใช้ในการเข้ารหัส เป็นต้น

ส่วนที่ ๒๔ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environmental Security)

๒๔.๑ ห้องควบคุมเครื่องแม่ข่ายและระบบเครือข่ายคอมพิวเตอร์ของกรมวิทยาศาสตร์บริการ

๒๔.๑.๑ กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร โดยกำหนดพื้นที่ปฏิบัติงานพื้นที่ควบคุมเฉพาะให้ชัดเจน เพื่อกำหนดสิทธิ์การเข้าถึงพื้นที่ โดยผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒๔.๑.๒ กำหนดมาตรการควบคุมการเข้า - ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร ดังนี้

(๑) ผู้เข้าใช้งานต้องเป็นผู้ที่ได้รับสิทธิ์การเข้าใช้งานพื้นที่เท่านั้น

(๒) ควบคุมการเข้าใช้งานในพื้นที่ควบคุมเฉพาะโดยแบบพิมพ์นิ้วมือ (Finger Scan)

(๓) ติดตั้งกล้องวงจรปิดเพื่อติดตาม และเฝ้าระวัง การเข้าพื้นที่ห้องควบคุมเครื่องแม่ข่ายและระบบเครือข่ายคอมพิวเตอร์

๒๔.๑.๓ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในกรมวิทยาศาสตร์บริการ จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องได้รับอนุญาตจากผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒๔.๑.๔ จัดให้มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งาน และมีความพร้อมในการใช้งาน ดังนี้

(๑) ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง

(๒) ติดตั้งระบบดับเพลิง และแจ้งเตือนอัคคีภัย

(๓) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น

(๔) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องควบคุม

(๕) เครื่องแม่ข่ายและระบบเครือข่ายคอมพิวเตอร์ทำงานผิดปกติหรือหยุดการทำงาน

(๖) วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนอย่างสม่ำเสมอให้มั่นใจได้ว่าระบบต่างๆ สามารถทำงานได้ตามปกติ

๒๔.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ

๒๔.๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของกรมวิทยาศาสตร์บริการในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงติดตั้งระบบป้องกันที่ปลอดภัย

๒๔.๒.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๒๔.๒.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๒๔.๒.๔ ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

๒๔.๒.๕ จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๒๔.๒.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ต้องล็อคกุญแจตลอดเวลา เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๒๔.๒.๗ พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

๒๔.๒.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๒๔.๓ การบำรุงรักษาอุปกรณ์

๒๔.๓.๑ วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา

๒๔.๓.๒ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๒๔.๓.๓ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๒๔.๓.๔ ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในกรมวิทยาศาสตร์บริการ ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุม ผู้ดูแลระบบจะต้องอยู่ในพื้นที่ด้วยทุกครั้ง

๒๔.๓.๕ จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๒๔.๔ การนำทรัพย์สินของกรมวิทยาศาสตร์บริการออกนอกกรมวิทยาศาสตร์บริการ

๒๔.๔.๑ ต้องขออนุญาตจากผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ ก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอก หรือ นำไปซ่อมบำรุงภายนอก

๒๔.๔.๒ ผู้ดูแลระบบจะต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าวกลับมาตามช่วงเวลาที่กำหนดและตรวจสอบอยู่ในสภาพดี

๒๔.๔.๓ บันทึกข้อมูลการนำอุปกรณ์ของกรมวิทยาศาสตร์บริการออกไปใช้งานนอกกรมวิทยาศาสตร์บริการ และบันทึกส่งคืน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย

๒๔.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกกรมวิทยาศาสตร์บริการ

๒๔.๕.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ หรือทรัพย์สินของกรมวิทยาศาสตร์บริการออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๒๔.๕.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของกรมวิทยาศาสตร์บริการไว้โดยลำพังในที่สาธารณะหรือสถานที่เสี่ยงต่อการสูญหาย

๒๔.๕.๓ เจ้าหน้าที่ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๒๔.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

๒๔.๖.๑ ผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ เป็นผู้อนุมัติในการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมามาใช้ โดยผู้ที่ต้องการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ต้องยื่นเรื่องขออนุมัติเป็นลายลักษณ์อักษร

๒๔.๖.๒ ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

ส่วนที่ ๒๕ การป้องกันข้อมูลรั่วไหล (Data Leakage Prevention)

๒๕.๑ ต้องเฝ้าระวังช่องทางที่อาจจะทำให้เกิดเหตุการณ์ข้อมูลรั่วไหล เช่น การรับส่งข้อมูลทางอิเล็กทรอนิกส์ รวมถึงเหตุการณ์การรักษาความมั่นคงปลอดภัยสารสนเทศ

๒๕.๒ เมื่อพบเหตุการณ์ข้อมูลรั่วไหลต้องปฏิบัติตามกระบวนการตอบสนองต่อเหตุการณ์ ความมั่นคงปลอดภัยสารสนเทศ และต้องมีการแจ้งต่อหน่วยงานที่เกี่ยวข้อง

๒๕.๓ พิจารณาใช้เครื่องมือ เทคโนโลยีในการป้องกันข้อมูลรั่วไหลตามความเหมาะสม

๒๕.๔ ต้องสร้างความตระหนักรู้ให้แก่พนักงาน ผู้ให้บริการภายนอกในการป้องกันข้อมูลรั่วไหลและปกป้องข้อมูลให้เหมาะสมกับระดับชั้นความลับ

ส่วนที่ ๒๖ ปฏิบัติให้สอดคล้องกับกฎหมาย กฎระเบียบ ข้อบังคับ (Legal and Regulatory Compliance)

ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศอันเนื่องมาจากกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้างที่กรมวิทยาศาสตร์บริการ ต้องปฏิบัติตามและวิธีการของกรมวิทยาศาสตร์บริการ ที่จะต้องปฏิบัติเพื่อให้สอดคล้องกับความต้องการเหล่านั้น ต้องมีการกำหนด บันทึกไว้เป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบัน

ทั้งนี้ ต้องมีการพิจารณา กฎหมาย กฎระเบียบที่เกี่ยวข้องในการดำเนินงาน ที่มีการประกาศโดยหน่วยงานกำกับดูแล เพื่อนำมาปฏิบัติ และต้องมีการตรวจสอบการดำเนินการเพื่อให้สามารถมั่นใจได้ว่าการปฏิบัติงานของกรมวิทยาศาสตร์บริการ มีความสอดคล้องกับกฎหมาย กฎระเบียบ ข้อบังคับ ที่กรมวิทยาศาสตร์บริการต้องดำเนินการ

หมวดที่ ๒ การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑) เพื่อให้ระบบสารสนเทศของกรมวิทยาศาสตร์บริการ สามารถให้บริการได้อย่างต่อเนื่อง

๒) เพื่อกำหนดมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับกรมวิทยาศาสตร์บริการ อย่างเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๓) เพื่อให้ผู้ใช้งานรับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ผู้รับผิดชอบ

๑) สถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

แนวทางปฏิบัติ

ส่วนที่ ๑ การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

ส่วนที่ ๒ การสำรองข้อมูลและกู้คืน (Backup and Recovery)

คัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตามแนวทางต่อไปนี้

๒.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานพร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๒.๒ กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

๒.๓ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และวางแผน โดยการกำหนดความถี่ในการสำรองข้อมูล โดยพิจารณาจากความสำคัญของข้อมูล ความถี่ในการเปลี่ยนแปลงข้อมูล โดยมีรายละเอียดการสำรองข้อมูล ดังนี้

๒.๓.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ ดังนี้

(๑) ข้อมูลคอนฟิกกูเรชัน (Configuration) สำหรับระบบ

(๒) ฐานข้อมูล (Database) ในระบบสารสนเทศ

(๓) ซอฟต์แวร์ (Software) ต่าง ๆ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ ระบบงานหรือซอฟต์แวร์อื่น ๆ ที่สำคัญ

๒.๓.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสม โดยแบ่งเป็น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๒.๓.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมสำหรับการกู้คืนระบบ

๒.๓.๔ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อ ข้อมูลที่สำรอง สถานการณ์สำรองข้อมูล เป็นต้น

๒.๓.๕ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และหากพบว่าผิดปกติต้องจัดทำบันทึกและดำเนินการแก้ไขโดยทันที

๒.๓.๖ ในกรณีที่จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล ต้องชี้บ่งสื่อบันทึกข้อมูลไว้อย่างชัดเจน โดยมีรายละเอียดของชื่อ วัน/เวลาสำรองข้อมูล ผู้รับผิดชอบ สถานะการสำรองข้อมูล (สำเร็จ/ไม่สำเร็จ) ขนาดของข้อมูล เป็นต้น โดยสื่อสำรองข้อมูลจะต้องจัดเก็บไว้อย่างปลอดภัย และข้อมูลที่สำรองต้องเข้ารหัสเพื่อความปลอดภัย

๒.๓.๗ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับกรมวิทยาศาสตร์บริการควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติ

๒.๓.๘ จัดระบบป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่ที่ใช้จัดเก็บข้อมูลสำรอง

๒.๓.๙ วางแผนทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ (restore) โดยการทดสอบต้องจัดทำบันทึกการทดสอบไว้เป็นหลักฐาน

๒.๓.๑๐ จัดทำขั้นตอนการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่สำรองไว้ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสม โดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

๒.๓.๑๑ กำหนดให้ใช้การเข้ารหัสข้อมูลกับข้อมูลลับที่สำรองไว้

๒.๔ จัดทำแผนการฝึกอบรมและแผนบริหารความต่อเนื่องทางธุรกิจ (Business continuity Plan) เพื่อให้แน่ใจว่าบริการที่สำคัญของกรมวิทยาศาสตร์บริการ สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึง

สอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของกรมวิทยาศาสตร์บริการ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่เกี่ยวข้อง ดังนี้

๒.๔.๑ กำหนดหน้าที่และความรับผิดชอบของผู้เกี่ยวข้องทั้งหมดในการรับผิดชอบระบบสารสนเทศระบบสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินโดยมีเบอร์โทรศัพท์ที่สะดวกติดต่อ

๒.๔.๒ ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญและกำหนดมาตรการ เพื่อลดความเสี่ยง ได้แก่ ไฟดับเป็นระยะเวลานานไฟไหม้แผ่นดินไหวเกิดเหตุจลาจลที่มีผลให้ไม่สามารถเข้าใช้งานระบบสารสนเทศได้ เป็นต้น

๒.๔.๓ กำหนดขั้นตอนในการกู้คืนระบบสารสนเทศ

๒.๔.๔ กำหนดขั้นตอนในการสำรองข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้

๒.๔.๕ กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการเครือข่ายฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น

๒.๔.๖ สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุฉุกเฉิน

๒.๕ ต้องจัดเตรียมอุปกรณ์ประมวลผลสำรองไว้ให้เพียงพอ เพื่อให้เป็นไปตามความต้องการในการใช้งานเมื่อเกิดเหตุฉุกเฉิน

๒.๖ ทบทวนระบบสารสเทศ ระบบสำรองข้อมูล และแผนบริหารความต่อเนื่องทางธุรกิจดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ ให้เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๒.๗ ต้องกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ผู้ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองข้อมูล และการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ ในกรณีที่ไม่สามารถดำเนินการด้วย วิธีการทางอิเล็กทรอนิกส์

๒.๘ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศระบบสำรองข้อมูล และแผนบริหารความต่อเนื่องทางธุรกิจ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสม โดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอและเพื่อประเมิน ประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๓ การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software)

๓.๑ ซอฟต์แวร์ต้นฉบับ ทั้งโปรแกรมเครื่องมือ ระบบปฏิบัติการ และ License key รวมถึงเอกสารที่เกี่ยวข้อง ต้องได้รับการจัดเก็บในสถานที่มั่นคงปลอดภัย และมีระบบหรือกระบวนการบริหารจัดการที่ดี เพื่อป้องกันความเสียหาย สูญหาย หรือการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

๓.๒ การติดตั้งซอฟต์แวร์ลงบนระบบให้บริการต้องได้รับอนุญาตก่อนดำเนินการ และต้องผ่านกระบวนการบริหารการเปลี่ยนแปลงที่กรมวิทยาศาสตร์บริการกำหนด

ส่วนที่ ๔ การบริหารจัดการข่าวกรองภัยคุกคาม และช่องโหว่ทางเทคนิค (Threat Intelligence and Technical Vulnerability Management)

๔.๑ ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญของกรมวิทยาศาสตร์บริการ อ้างอิงตามหลักการบริหารความเสี่ยงของกรมวิทยาศาสตร์บริการ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญของกรมวิทยาศาสตร์บริการ อย่างน้อยปีละ ๑ ครั้ง โดยต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย

(๑) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

(๒) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

(๓) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๔.๒ ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของกรมวิทยาศาสตร์บริการ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบสำคัญใด ๆ กับบริการที่สำคัญของกรมวิทยาศาสตร์บริการ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๔.๓ ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของกรมวิทยาศาสตร์บริการ โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๔.๔ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญของกรมวิทยาศาสตร์บริการ โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ต (Internet Facing)

๔.๕ ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยสารสนเทศของบริการที่สำคัญของกรมวิทยาศาสตร์บริการ ก่อนทำการ

ทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๔.๖ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลหรือตามที่กฎหมายที่เกี่ยวข้องกำหนด

๔.๗ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของกรมวิทยาศาสตร์บริการ

๔.๘ ต้องสร้างกระบวนการเพื่อติดตามและจัดการช่องโหว่ที่ระบุในผลประเมินช่องโหว่ และในผลการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

๔.๙ หากได้รับการร้องขอจาก กกม. หรือ สกมช. ทางกรมวิทยาศาสตร์บริการ ต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของกรมวิทยาศาสตร์บริการ ไปยัง สกมช. ภายใน ๓๐ วัน นับแต่วันที่ได้รับหนังสือ ทั้งนี้ รูปแบบรายงานสรุปผลการทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่ สกมช. ประกาศกำหนด

๔.๑๐ หากการตรวจสอบช่องโหว่และการทดสอบเจาะระบบนั้น ดำเนินการโดยผู้ให้บริการภายนอก ให้กรมวิทยาศาสตร์บริการดำเนินการควบคุม ดังนี้

(๑) จัดทำสัญญารักษาความลับ (Non-Disclosure Agreement: NDA) และกำหนดข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมในสัญญาว่าจ้างหรือเอกสารแนบท้ายสัญญาว่าจ้างอันเป็นส่วนหนึ่งของสัญญาดังกล่าว

(๒) ต้องได้รับความเห็นชอบจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรมก่อนดำเนินการเสมอ และมีการวางแผนก่อนดำเนินการ ซึ่งครอบคลุมถึงการดำเนินการนอกเวลางาน

(๓) หากมีการสำเนาข้อมูล ต้องทำลายสำเนาข้อมูลทั้งหมดทันทีที่การดำเนินงานเสร็จสิ้นลงแต่ไม่รวมไปถึงรายงานการดำเนินการ

(๔) ในกรณีเจ้าหน้าที่ของกรมวิทยาศาสตร์บริการ ทำการตรวจสอบระบบเอง โดยใช้ซอฟต์แวร์หรือเครื่องมือเข้าช่วย ต้องทำการเก็บรักษาซอฟต์แวร์หรือเครื่องมือนั้นไว้ในที่มั่นคงปลอดภัย เช่น เก็บไว้ในเครื่องคอมพิวเตอร์ที่มีรหัสผ่านปกป้อง เป็นต้น เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิสามารถนำเอาซอฟต์แวร์หรือเครื่องมือดังกล่าวไปใช้งานโดยไม่ได้รับอนุญาตเมื่อดำเนินการเสร็จสิ้น หากมีบัญชีผู้ใช้งานและรหัสผ่านที่กำหนดให้ผู้เชี่ยวชาญจากภายนอกใช้ในการดำเนินการ ต้องถูกลบหรือยกเลิก

(๕) จัดเก็บรายงานผลการดำเนินการไว้เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถตรวจสอบย้อนหลังได้อย่างน้อย ๕ ปี

๔.๑๑ ต้องจัดให้มีการติดตามข้อมูลข่าวสารจากแหล่งข้อมูลต่าง ๆ ที่เชื่อถือได้ เช่น เว็บไซต์ของเจ้าของผลิตภัณฑ์หรือผู้ให้บริการ เป็นต้น เกี่ยวกับโปรแกรมแก้ไขข้อบกพร่องของซอฟต์แวร์และระบบปฏิบัติการ (Patch) ตลอดจนอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง และดำเนินการติดตั้งโปรแกรมดังกล่าวตามขั้นตอนปฏิบัติงานที่กรมวิทยาศาสตร์บริการกำหนด ซึ่งรวมไปถึงกระบวนการบริหารการเปลี่ยนแปลง (Change Management)

๔.๑๒ ต้องจัดให้มีการจัดทำเอกสารรายชื่อ และข้อมูลการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ ในเรื่องเดียวกัน เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) เป็นต้น และผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และต้องทบทวนรายชื่อและข้อมูลการติดต่อดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

๔.๑๓ จัดให้มีการรวบรวม และวิเคราะห์ข้อมูลข่าวกรองภัยคุกคามด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ

หมวดที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้

๒) เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓) เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

ผู้รับผิดชอบ

๑) สถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้ตรวจสอบภายใน

แนวทางปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ตรวจสอบและประเมินความเสี่ยงดำเนินการโดยผู้ตรวจสอบภายในของกรมวิทยาศาสตร์บริการ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้กรมวิทยาศาสตร์บริการได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ มีการตรวจสอบและประเมินความเสี่ยงและจัดทำรายงานพร้อมข้อเสนอแนะ

๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

๒.๔.๑ กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่าง

๒.๔.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งานรวมทั้งการทำลายหรือลบข้อมูลโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างเหมาะสม

๒.๔.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๔.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อค (Log) แสดงการเข้าถึง วันและเวลาที่เข้าถึงระบบ

๒.๔.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบสารสนเทศ

ภัยด้านความมั่นคงปลอดภัยของระบบสารสนเทศแยกได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยจากเจ้าหน้าที่ของกรมวิทยาศาสตร์บริการ (Human Error) ได้แก่ เจ้าหน้าที่ขาดความรู้ความเข้าใจ ในการใช้งานอุปกรณ์คอมพิวเตอร์ ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ ซึ่งอาจทำให้ระบบสารสนเทศเสียหายใช้งาน ไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน ซึ่งส่งผลให้ไม่สามารถใช้งานระบบสารสนเทศได้อย่างเต็มประสิทธิภาพ โดยกำหนดแนวทางการดำเนินการเบื้องต้น เพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศไว้ ดังนี้

(๑) จัดอบรมเจ้าหน้าที่ของกรมวิทยาศาสตร์บริการให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์

และซอฟต์แวร์ เบื้องต้น เพื่อลดความเสี่ยงให้เกิดน้อยที่สุด

(๒) จัดทำหนังสือแจ้งเวียนหน่วยงานเรื่องการใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยจากซอฟต์แวร์ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) ข่าวลวง (Hoax) เป็นต้น ซึ่งซอฟต์แวร์เหล่านี้อาจรบกวนการทำงานและก่อให้เกิด ความเสียหายให้แก่ระบบสารสนเทศถึงขั้นทำให้ระบบเครือข่ายใช้งานไม่ได้ โดยกำหนดแนวทางปฏิบัติ เพื่อเตรียมรับสถานการณ์ภัยจากซอฟต์แวร์ ดังนี้

(๑) ติดตั้งอุปกรณ์ป้องกันเครือข่ายที่ระบบเครือข่าย เพื่อให้ทำหน้าที่กำหนดสิทธิในการเข้าใช้งานระบบเครือข่าย และป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งโปรแกรมป้องกันไวรัส เพื่อดักจับไวรัสที่เข้ามาในระบบเครือข่ายที่สามารถตรวจสอบชนิดของไวรัสชนิดที่ทำความเสียหายกับระบบเครือข่าย

ประเภทที่ ๓ ภัยจากไฟไหม้หรือระบบไฟฟ้าจัดเป็นภัยที่สร้างความเสียหายให้แก่ระบบสารสนเทศอย่างร้ายแรง โดยกำหนดแนวทางปฏิบัติ เพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบคอมพิวเตอร์แม่ข่าย (Server) ในกรณีกระแสไฟฟ้าขัดข้องระบบคอมพิวเตอร์แม่ข่าย จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บ และสำรองข้อมูลไว้ อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควันสำหรับเหตุการณ์กระแสไฟฟ้าขัดข้อง หรือมีควันไฟเกิดขึ้นภายในห้องระบบคอมพิวเตอร์อุปกรณ์ดังกล่าว ต้องส่งสัญญาณแจ้งเตือนให้หน่วยรักษาความปลอดภัยทราบและรีบเข้ามาระงับเหตุฉุกเฉินในทันที โดยให้ตรวจสอบ ความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องระบบคอมพิวเตอร์ เพื่อใช้ในกรณีเหตุไฟไหม้ โดยให้ตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วมจัดเป็นภัยที่สร้างความเสียหายให้แก่ระบบสารสนเทศอย่างร้ายแรง โดยกำหนดแนวทางปฏิบัติ เพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) เฝ้าระวังอุทกภัยโดยติดตามพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(๒) ถอดเทปสำรองข้อมูลทั้งหมดไปเก็บในที่ปลอดภัย

(๓) ตัดระบบไฟฟ้าในห้องระบบคอมพิวเตอร์ โดยปิดเบรกเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหายและป้องกันภัยจากไฟฟ้า

(๔) ย้ายเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายไปไว้บนที่สูง

(๕) เมื่อน้ำลดลงแล้วให้ช่างไฟฟ้าตรวจสอบการทำงานระบบไฟฟ้าในห้องระบบคอมพิวเตอร์และเตรียมความพร้อมของห้องระบบคอมพิวเตอร์ เพื่อติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย

(๖) ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายพร้อมทั้งทดสอบการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่อง ตรวจสอบการเชื่อมต่อของระบบเครือข่ายกับ เครื่องคอมพิวเตอร์ลูกข่าย แจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อเข้าใช้งานตามปกติ

หมวดที่ ๔ การปฏิบัติเพื่อตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี และการรับมือเมื่อเกิดเหตุการณ์ละเมิดความมั่นคงปลอดภัยของระบบสารสนเทศ

ผู้รับผิดชอบ

๑) สถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

แนวทางปฏิบัติ

๑. การจัดการระบบป้องกันผู้บุกรุกโดยตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก โดยให้ตรวจสอบในประเด็น ดังต่อไปนี้

(๑) ความถี่ในการโจมตีและประเภทของการโจมตี

(๒) ลักษณะของการโจมตีว่าสามารถคาดการณ์ได้หรือไม่

(๓) ระดับความรุนแรง

(๔) หมายเลขไอพีของเครือข่ายของผู้โจมตี

๒. การจัดการระบบไฟร์วอลล์ โดยดำเนินการ ดังนี้

(๑) ตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

(๒) ตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ โดยให้ตรวจสอบรายการดังต่อไปนี้

(ก) Packet ที่ไฟร์วอลล์ได้ปิดกั้น (block)

(ข) ลักษณะของ Packet ที่ถูกปิดกั้น

(ค) Packet ของหมายเลขไอพีของเครือข่ายที่ถูกปิดกั้นตามจำนวนมากไปหาน้อย

(๓) เมื่อตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศ ให้แจ้งผู้บริหารระดับสูง หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เพื่อขอการตัดสินใจ ในการแก้ไขปัญหา

๓. การจัดการระบบป้องกันภัยคุกคามทางอินเทอร์เน็ตหรือโปรแกรมไม่ประสงค์ดี (Malware) ซึ่งครอบคลุมถึงไวรัสหนอนอินเทอร์เน็ตโปรแกรมโทรจันรวมถึงสปายแวร์ (Spyware) ให้ดำเนินการ ดังนี้

(๑) ตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต โดยให้ตรวจสอบรายการ ดังต่อไปนี้

(ก) ประเภทของโปรแกรมไม่ประสงค์ดีที่ถูกพบเรียงลำดับจากมากไปหาน้อย

(ข) เครือข่ายที่ส่งโปรแกรมไม่ประสงค์ดีและปลายทางของการส่ง

(ค) โปรแกรมไม่ประสงค์ดีถูกส่งออกจากหรือผ่านเครือข่ายภายในกรมวิทยาศาสตร์บริการ หรือไม่

(๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดโปรแกรมไม่ประสงค์ดี โดยเฉพาะประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของ กรมวิทยาศาสตร์บริการ

(๓) ให้ระงับการเชื่อมต่อของเครื่องคอมพิวเตอร์ที่ติดโปรแกรมไม่ประสงค์ดีกับระบบเครือข่าย แล้วแก้ไขเครื่องคอมพิวเตอร์นั้นทันทีที่ตรวจสอบพบว่า เครื่องคอมพิวเตอร์ ภายในเครือข่ายติดโปรแกรมไม่ประสงค์ดี หรือเป็นเครื่องที่ส่งโปรแกรมไม่ประสงค์ดี ออกไปสู่เครือข่ายภายนอก

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

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

(๒) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่า กรมวิทยาศาสตร์บริการจะปฏิบัติตามภาระหน้าที่ในการรายงานใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองที่ตราขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมายนั้น ๆ และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับการปกป้องคุ้มครองโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และบริการที่สำคัญของกรมวิทยาศาสตร์บริการ

(๓) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ IRT

(๔) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคง

ปลอดภัยไซเบอร์

(๕) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๖) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๗) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๘) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

(๙) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๕. ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของ กรมวิทยาศาสตร์บริการ

๖. ต้องทบทวนแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย อย่างน้อยปีละ ๑ ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางสารสนเทศของบริการที่สำคัญของ กรมวิทยาศาสตร์บริการ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งแก้ไขปรับปรุงแผนดังกล่าวหากเห็นสมควรว่า การแก้ไขปรับปรุงดังกล่าวทำให้การรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยมีประสิทธิภาพและประสิทธิผล

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

(๑) สถานการณ์ความเสี่ยง (Risk Scenario) รูปแบบการทดสอบ วัน เวลา สถานที่ ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้องที่ใช้ในการทดสอบ

(๒) สรุปผลการทดสอบ ผลการประเมิน และ ผลการทบทวนขั้นตอนการบริหารจัดการเหตุการณ์

๘. ต้องมีการวิเคราะห์หาสาเหตุที่แท้จริง (Root Cause) ของเหตุการณ์ด้านความมั่นคงปลอดภัยและนำองค์ความรู้ที่ได้มาใช้ในการวางแผนและเตรียมการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจจะเกิดขึ้นในอนาคต

๙. ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัย ซึ่งอย่างน้อยต้องระบุเนื้อหาดังต่อไปนี้

(๑) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

(๒) ระบุสถานการณ์จำลองเหตุการณ์ด้านความมั่นคงปลอดภัยที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

(๓) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ด้านความมั่นคงปลอดภัยแต่ละประเภท

(๔) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนของ กรมวิทยาศาสตร์บริการเมื่อกล่าวแถลงกับสื่อมวลชน

(๕) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๑๐. ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๑๑. ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ด้านความมั่นคงปลอดภัย

๑๒. ต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ (Cybersecurity Exercise) เมื่อได้รับคำสั่งเป็นลายลักษณ์อักษรจาก กมช. การฝึกซ้อมดังกล่าวอาจดำเนินการได้ทั้งในระดับชาติหรือระดับภาคส่วน โดย กรมวิทยาศาสตร์บริการ ต้องตรวจสอบให้แน่ใจว่า บุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยมีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

๑๓. ต้องปฏิบัติตามคำขอใด ๆ ของ กมช. กกม. และ สกมช. เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ และ กรมวิทยาศาสตร์บริการ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่ กมช. กกม. และ สกมช. อาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยและแผนการสื่อสารในภาวะวิกฤต ขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของ กรมวิทยาศาสตร์บริการ

๑๔. ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และบริการที่สำคัญของ กรมวิทยาศาสตร์บริการ รวมทั้งมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจได้รับผลกระทบ เช่น ผู้ใช้งาน ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญของ กรมวิทยาศาสตร์บริการ เป็นต้น เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้ โดยรายละเอียด แนวทาง และรูปแบบใดการแบ่งปันข้อมูล ให้เป็นไปตามหลักเกณฑ์และวิธีการ สกมช. ประกาศกำหนด

๑๕. ต้องแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแล หากมีการเปลี่ยนแปลงข้อมูล ให้แจ้งข้อมูลที่เปลี่ยนแปลงไปยัง สกมช. โดยเร็ว

๑๖. ต้องแจ้งรายชื่อหน่วยงานภายในหรือบุคคลที่เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์และผู้ดูแลระบบคอมพิวเตอร์ พร้อมด้วยข้อมูลการติดต่อสำหรับที่สามารถติดต่อได้ในกรณีมีเหตุฉุกเฉินภายในไปยัง สกมช. หน่วยงานควบคุมหรือกำกับดูแล และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หากมีการเปลี่ยนแปลงข้อมูลให้แจ้งข้อมูลที่เปลี่ยนแปลงไปยังหน่วยงานดังกล่าวเหล่านี้

๑๗. ในกรณีที่มีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของ กรมวิทยาศาสตร์บริการ ให้แจ้งเหตุและส่งรายงานภัยคุกคามทางไซเบอร์ต่อ สกมช. ภายในระยะเวลา ๒๔ ชั่วโมงหลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์ พร้อมจัดส่งรายงานดังกล่าวไปยังหน่วยงานควบคุมหรือกำกับดูแลภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด โดยแบบรายงานภัยคุกคามทางไซเบอร์ให้เป็นไปตามที่ กกม. ประกาศกำหนด ให้ กรมวิทยาศาสตร์บริการ พิจารณาส่งข้อมูลสำคัญที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายหรือแนวปฏิบัติว่าด้วยการรักษาความลับของกรมวิทยาศาสตร์บริการด้วย และต้องปรับปรุงข้อมูลในรายงานเหตุภัยคุกคามทางไซเบอร์และสถานะการตอบสนองภัยคุกคามทางไซเบอร์ให้สอดคล้องกับข้อมูลอันเป็นปัจจุบัน ที่กรมวิทยาศาสตร์บริการได้สืบทราบเพิ่มมากขึ้นในระหว่างการดำเนินการรับมือเหตุภัยคุกคาม รวมทั้งจัดส่งรายงานปิดเหตุการณ์ภัยคุกคามดังกล่าวด้วย

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

๑๙. จัดทำรายงานประจำปี ส่งรายงานดังกล่าวให้ สกมช. และหน่วยงานควบคุมหรือกำกับดูแลภายในวันที่ ๓๑ มกราคมของปีถัดไป โดยรายงานต้องมีรายละเอียด ดังนี้

(๑) ระบุจำนวนและลักษณะของเหตุการณ์ภัยคุกคามทางไซเบอร์ ตามแบบรายงานสรุปที่ กกม. กำหนด

(๒) วิเคราะห์สาเหตุหรือผลกระทบที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๓) ปัญหาและอุปสรรคในการดำเนินงาน

(๔) ข้อเสนอแนะต่าง ๆ ซึ่งรวมถึงข้อเสนอแนะเชิงนโยบาย

๒๐. ให้ความร่วมมือหรือสนับสนุนแก่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบ

คอมพิวเตอร์แห่งชาติ (ThaiCERT) ในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะการติดตามการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และผลการตอบสนองและรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

หมวดที่ ๕ การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

วัตถุประสงค์

๑) เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของกรมวิทยาศาสตร์บริการ

๒) เพื่อให้การเกิดความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์

๓) เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่ตั้งใจ

ผู้รับผิดชอบ

๑) สถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

แนวทางปฏิบัติ

๑. จัดให้มีการทบทวนเพื่อปรับปรุงหรือแก้ไขเพิ่มเติมแนวปฏิบัติฉบับนี้ให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อการปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมวิทยาศาสตร์บริการ

๒. เมื่อมีความเสี่ยงที่เกิดขึ้นอย่างเด่นชัด เช่น การนำระบบสารสนเทศใหม่เข้ามาใช้งาน กฎหมาย หรือข้อบังคับใหม่ ฯลฯ ที่มีผลกับการดำเนินการของกรมวิทยาศาสตร์บริการ หากแนวปฏิบัติปัจจุบัน ยังไม่ตอบสนองต่อภารกิจและความเสี่ยงเหล่านี้ได้อย่างเหมาะสม กรมวิทยาศาสตร์บริการ จะต้องมีทบทวนปรับปรุง ข้อปฏิบัติภายใน ๓๐ วันหลังจากรับทราบ เพื่อปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย และรับมือกับความเสี่ยงเหล่านี้ได้อย่างเหมาะสมและทันการณ์

๓. จัดฝึกอบรมแนวปฏิบัติอย่างสม่ำเสมอ โดยผสานความรู้ความเข้าใจในนโยบายและวิธีปฏิบัติตามแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศไว้ในหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

๔. ประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถ

เข้าใจและนำไปปฏิบัติได้ง่าย ได้แก่ ติดประกาศ ฯลฯ โดยปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๕. กระตุ้นการมีส่วนร่วมโดยผ่านการกำกับติดตามประเมินผลและสำรวจความต้องการของผู้ใช้งาน

๖. ให้ความรู้ความเข้าใจเกี่ยวกับโปรแกรมไม่ประสงค์ดีแก่ผู้ใช้งาน เพื่อให้ตระหนักในปัญหาและสามารถป้องกันตนได้และให้ทราบขั้นตอนปฏิบัติเมื่อพบตรวจพบโปรแกรมไม่ประสงค์ดี

๗. ให้ความรู้ความเข้าใจเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่ได้คาดการณ์แก่ผู้ใช้งาน เพื่อให้สามารถปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของกรมวิทยาศาสตร์บริการ ได้อย่างถูกต้อง

๘. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบของกรมวิทยาศาสตร์บริการ และข้อตกลงระหว่างประเทศอย่างเคร่งครัด โดยให้ถือว่าการละเลยเพิกเฉยเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นด้วยตนเอง

๙. ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Security Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือระบบการทำงานของบริการที่สำคัญของกรมวิทยาศาสตร์บริการได้ ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(๑) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ดังนี้

(ก) พนักงานใหม่ (New Employees)

(ข) ผู้ใช้และระดับบริหาร (Users and Management)

(ค) ผู้ขาย ผู้รับเหมา และผู้ให้บริการภายนอก (Vendors, Contractors and Service Providers)

(๒) การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศของบริการที่สำคัญของกรมวิทยาศาสตร์บริการ

(๓) การตระหนักรู้กฎหมายความมั่นคงปลอดภัยสารสนเทศ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งานและการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบควบคุมบริการที่สำคัญของกรมวิทยาศาสตร์บริการ

(๔) การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ

๑๐. ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเสศอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

หมวดที่ ๖ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

(Information Systems Acquisition, Development, and Maintenance)

วัตถุประสงค์

เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะ

ผู้รับผิดชอบ

๑) สถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

แนวทางปฏิบัติ

๑. ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in Development and Support Processes)

๑.๑ กฎเกณฑ์ในการพัฒนาซอฟต์แวร์และระบบ ต้องมีการกำหนดขั้นตอนการปฏิบัติงานเพื่อเป็นแนวปฏิบัติสำหรับการพัฒนาระบบของกรมวิทยาศาสต์บริการ

๑.๒ การเปลี่ยนแปลงระบบหรือการพัฒนาระบบ ต้องมีการควบคุมโดยปฏิบัติตามนโยบายการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management) และขั้นตอนการปฏิบัติงานการบริหารจัดการการเปลี่ยนแปลง

๑.๓ เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบที่สำคัญต้องมีการทบทวนและทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงาน หรือต่อความมั่นคงปลอดภัยของกรมวิทยาศาสต์บริการ

๑.๔ ต้องพิจารณาสภาพแวดล้อมที่เหมาะสมต่อการพัฒนาระบบที่มีความมั่นคงปลอดภัย ได้แก่ พื้นที่ปฏิบัติงานไม่อยู่พื้นที่พลุกพล่าน หรือเข้าถึงได้ง่าย

๑.๕ ต้องจัดให้มีการแยกระบบที่ให้บริการจริงออกจากระบบสำหรับการพัฒนาและการทดสอบเพื่อป้องกันปัญหาที่อาจมีผลกระทบกับข้อมูล หรือการประมวลผลของระบบที่ให้บริการจริง

๑.๖ การจ้างพัฒนาระบบจากผู้ให้บริการภายนอก ต้องมีการควบคุม เฝ้าระวัง ติดตามการดำเนินงานอย่างใกล้ชิดเพื่อให้เป็นไปตามขอบเขตการดำเนินงาน และสอดคล้องกับนโยบาย ขั้นตอนปฏิบัติของ กรมวิทยาศาสต์บริการที่กำหนดไว้

๑.๗ ผู้พัฒนาระบบควรมีการจัดทำคู่มือหรือขั้นตอนการทดสอบระบบ และจะต้องมีการปรับปรุงคู่มือในการใช้งาน หรือคู่มือในการอบรมผู้ใช้งาน เมื่อการขอเปลี่ยนแปลงนั้น ๆ มีผลต่อคู่มือฉบับเดิม

๑.๘ ควรมีการทดสอบการใช้งานระบบ เพื่อเป็นการสอบทานคู่มือหรือขั้นตอนการทดสอบระบบ รวมถึงการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชั่นใหม่

๑.๙ ควรมีการยืนยันผลการทดสอบจากผู้ที่เกี่ยวข้อง และมีการอนุมัติจากผู้มีอำนาจก่อนการโอนย้ายระบบงานที่ได้จัดทำเรียบร้อยแล้วจากระบบทดสอบเข้าสู่ระบบงานจริงอย่างเป็นลายลักษณ์อักษร

๑.๑๐ ต้องมีการควบคุม กำหนดสิทธิการเข้าถึง Source Code อย่างเหมาะสมให้สอดคล้องตามบทบาทหน้าที่ความรับผิดชอบที่ได้รับมอบหมาย

๑.๑๑ ในกระบวนการพัฒนาระบบเทคโนโลยีสารสนเทศ จะต้องมีการตรวจทานความถูกต้องของข้อมูลที่ดีเพื่อลดความเสี่ยงที่อาจเกิดจากความผิดพลาดในการนำเข้าข้อมูล และความผิดพลาดของข้อมูลที่เกิดจากประมวลผลข้อมูล

๑.๑๒ ควรมีการควบคุมและตรวจสอบการทำงานของแอปพลิเคชัน เพื่อป้องกันความเสี่ยงที่อาจเกิดจากการทำงานหรือการประมวลผลข้อมูลที่ผิดพลาดอันจะส่งผลเสียต่อระบบโดยรวม

๑.๑๓ ควรจัดทำข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอปพลิเคชัน รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

๒. การควบคุมข้อมูลในการทดสอบ (Test Data)

หน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง และต้องมีการควบคุมข้อมูลในระบบทดสอบให้เป็นไปตามชั้นความลับและการคุ้มครองข้อมูลส่วนบุคคล

หมวดที่ ๗ การบริหารจัดการผู้ให้บริการภายนอก

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการ เมื่อต้องมีการดำเนินงานร่วมหรือใช้บริการจากผู้ให้บริการภายนอก และเพื่อควบคุมให้บริการที่ได้รับจากผู้ให้บริการภายนอก เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และตรงตามสัญญา/ข้อตกลง

ผู้รับผิดชอบ

๑) สถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

แนวทางปฏิบัติ

๑. ต้องทำการคัดเลือก ตรวจสอบคุณสมบัติ และประเมินความสามารถของผู้ให้บริการภายนอกที่จะคัดเลือกเข้าทำงานร่วมกับกรมวิทยาศาสตร์บริการอย่างเหมาะสม ตามลักษณะของงานที่ทำการจ้าง และระดับความสำคัญของข้อมูลและระบบเทคโนโลยีสารสนเทศที่ผู้ให้บริการภายนอกนั้น ๆ ต้องเข้าถึงหรือใช้งาน ทั้งนี้ วิธีการดำเนินการตรวจสอบคุณสมบัติต้องไม่ขัดต่อกฎหมาย กฎระเบียบ และจริยธรรม และต้องแจ้งต่อผู้ให้บริการภายนอกที่ถูกตรวจสอบอย่างเหมาะสมทุกครั้งก่อนดำเนินการ โดยการตัดสินใจในการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกที่มีความเสี่ยงหรือมีนัยสำคัญ ควรได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

๒. ต้องมีการกำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกผู้ให้บริการภายนอก โดยคำนึงถึงเรื่องดังนี้

(๑) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการในช่วงที่ผ่านมา และระบบการบริหารงานภายใน

(๒) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน

(๓) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ ต่าง ๆ

(๔) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง

(๕) การปฏิบัติตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ ซึ่งรวมไปถึงการรักษาความมั่นคงปลอดภัยสารสนเทศ

(๖) การใช้เทคโนโลยีสารสนเทศแบบเปิด (open technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยีสารสนเทศ ผู้ให้บริการหรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง

(๗) การที่ผู้ให้บริการภายนอกมอบหมายการปฏิบัติงานที่สำคัญให้กับบุคคลอื่นต่อ (sub-contracting to another supplier)

๓. ต้องมีการประเมินด้านคุณภาพและความน่าเชื่อถือของบุคคลภายนอก โดยพิจารณาจากประสบการณ์ คุณภาพของบริการและผลงานที่ส่งมอบ ตลอดจนมาตรฐานด้านความปลอดภัยสารสนเทศ ที่เกี่ยวข้องกับสินค้าและบริการ และจัดทำเป็นรายชื่อบุคคลภายนอกที่เชื่อถือได้ (trusted third-party/trusted vendor) เพื่อใช้เป็นส่วนหนึ่งของเกณฑ์การคัดเลือกผู้ให้บริการในอนาคต

๔. ต้องจัดให้ผู้ให้บริการภายนอกทุกรายลงนามในเอกสารต่อไปนี้ ตามความเหมาะสมก่อนเริ่มปฏิบัติงาน

(๑) สัญญาการปฏิบัติงาน (Contract) และ/หรือ สัญญาบริการ (Service Level Agreement)

(๒) สัญญารักษาความลับ (Non-Disclosure Agreement: NDA)

(๓) วิธีการปฏิบัติงานมาตรฐานจรรยาบรรณสำหรับผู้ให้บริการภายนอก (Third-Party Code of Conduct)

๕. มีการกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ให้บริการภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร โดยควรพิจารณาการกำหนดรายละเอียด ดังนี้

(๑) ขอบเขตการให้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก

(๒) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของกรมวิทยาศาสตร์บริการ ตามความต้องการทางธุรกิจของกรมวิทยาศาสตร์บริการ และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) บทบาท หน้าที่ และความรับผิดชอบในการปกป้องบริการที่สำคัญของกรมวิทยาศาสตร์บริการ จากเหตุการณ์ด้านความมั่นคงปลอดภัย

(๔) มาตรฐานขั้นต่ำในการปฏิบัติงานของผู้ให้บริการภายนอก

(๕) ข้อตกลงระดับการให้บริการ (Service Level Agreement)

(๖) การติดตามและรายงานผลการปฏิบัติงานของผู้ให้บริการภายนอก

(๗) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

(๘) รายชื่อ และช่องทางการติดต่อในกรณีเกิดปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

(๙) การทำลายข้อมูลเมื่อสิ้นสุดสัญญาหรือข้อตกลง

(๑๐) เงื่อนไขหรือสิทธิของกรมวิทยาศาสตร์บริการ ในการเปลี่ยนแปลง ยุติ หรือยกเลิกสัญญาหรือข้อตกลง กับผู้ให้บริการภายนอก

(๑๑) การจัดให้มีแผนฉุกเฉินด้านความมั่นคงปลอดภัยสารสนเทศ

(๑๒) สิทธิ์ของกรมวิทยาศาสตร์บริการ ในการเข้าตรวจสอบการปฏิบัติงาน และการปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่กรมวิทยาศาสตร์บริการ กำหนด

(๑๓) ความรับผิดชอบต่อความเสียหายที่เกิดจากผู้ให้บริการภายนอก

(๑๔) เงื่อนไขเกี่ยวกับการจ้างช่วง

(๑๕) การรายงานการเปลี่ยนแปลงที่สำคัญของผู้ให้บริการภายนอก ที่อาจมีผลกระทบต่อความสามารถในการปฏิบัติตามสัญญา เช่น การเปลี่ยนแปลงการบริการของผู้ให้บริการภายนอก เป็นต้น

(๑๖) การแจ้งล่วงหน้าต่อกรมวิทยาศาสตร์บริการ เป็นลายลักษณ์อักษรกรณีที่ผู้ให้บริการภายนอกมีการดำเนินการเปลี่ยนแปลงใด ๆ ที่อาจส่งผลกระทบต่อการให้บริการตามสัญญาจ้างหรือข้อตกลงอื่น ๆ เพื่อให้กรมวิทยาศาสตร์บริการ ทำการพิจารณาอนุมัติ วิเคราะห์ผลกระทบ และหาวิธีในการแก้ไขควบคุมความ

เสี่ยงได้อย่างเหมาะสม

โดยมีการประเมินความเสี่ยงและแนวทางควบคุมความเสี่ยง พร้อมทั้งขออนุมัติยกเว้นจากผู้มีอำนาจหากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญา

ข้อตกลงหรือสัญญาการให้บริการระหว่างกรมวิทยาศาสตร์บริการ และผู้ให้บริการภายนอกที่เป็นผู้ให้บริการงานด้านเทคโนโลยีสารสนเทศรายที่มีนัยสำคัญ มีการระบุสิทธิให้กรมวิทยาศาสตร์บริการ และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากกรมวิทยาศาสตร์บริการ สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของผู้ให้บริการภายนอกดังกล่าวได้

กรณีที่ไม่สามารถระบุสิทธิข้างต้น การเลือกใช้ผู้ให้บริการภายนอกจะมีการพิจารณาอย่างรัดกุม และเหมาะสมกับความเสี่ยง เช่น พิจารณาจากผลการตรวจสอบด้านเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอกที่ดำเนินการโดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล

๖. ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

๗. ต้องควบคุมให้บุคลากร ลูกจ้าง หรือตัวแทนของผู้ให้บริการภายนอกปฏิบัติตามกฎระเบียบนโยบาย ขั้นตอนการปฏิบัติงาน และวิธีการปฏิบัติงานต่าง ๆ ของกรมวิทยาศาสตร์บริการ อย่างเคร่งครัด

๘. ต้องควบคุมให้ผู้ให้บริการภายนอกเก็บรักษาข้อมูลทุกประเภทที่ได้รับหรือรับทราบจากกรมวิทยาศาสตร์บริการไว้เป็นความลับ โดยอนุญาตให้ใช้ข้อมูลเพื่อการปฏิบัติงานให้แก่กรมวิทยาศาสตร์บริการเท่านั้น

๙. ต้องจัดให้มีการบันทึกรายการของอุปกรณ์และซอฟต์แวร์ทั้งหมด รวมถึงบันทึกการเข้าถึงอุปกรณ์และการเชื่อมต่อกับระบบเครือข่ายของกรมวิทยาศาสตร์บริการ ในกรณีที่กรมวิทยาศาสตร์บริการ มีการตั้งอุปกรณ์และซอฟต์แวร์ของกรมวิทยาศาสตร์บริการ ไว้ในสถานที่ของผู้ให้บริการภายนอก

๑๐. ต้องกำหนดให้ผู้ให้บริการภายนอกแจ้งรายชื่อของเจ้าหน้าที่ที่จะเข้าปฏิบัติงานต่อกรมวิทยาศาสตร์บริการก่อนเริ่มปฏิบัติงาน และทุกครั้งที่มีการเปลี่ยนแปลงบุคคลที่เข้าปฏิบัติงาน

๑๑. ต้องควบคุมให้ผู้ให้บริการภายนอก เข้าถึงและใช้งานข้อมูล และระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการ ตามวิธีปฏิบัติตามที่กรมวิทยาศาสตร์บริการ กำหนดไว้

๑๒. ต้องมีการกำหนดระยะเวลาของสิทธิของผู้ให้บริการภายนอกในการเข้าใช้งานระบบสารสนเทศของกรมวิทยาศาสตร์บริการ อย่างชัดเจน โดยกรมวิทยาศาสตร์บริการ ต้องกำหนดให้ผู้ให้บริการภายนอกได้รับสิทธิในการเข้าถึงเฉพาะระบบสารสนเทศที่ได้รับอนุญาตเท่านั้น

๑๓. ต้องจัดให้มีการบันทึกและตรวจสอบสิทธิในการเข้าถึงระบบต่าง ๆ ของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

๑๔. ต้องกำหนดให้ผู้ให้บริการภายนอก รายงานสิ่งผิดปกติหรือเหตุละเมิดความมั่นคงปลอดภัย (Security Incident) ต่อกรมวิทยาศาสตร์บริการ ทันทีที่พบเหตุ

๑๕. ผู้ดูแลระบบและพนักงานผู้ติดต่อประสานงานกับผู้ให้บริการภายนอก มีหน้าที่ดูแล ควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอก ที่เกี่ยวข้องให้เป็นไปตามเอกสารสัญญา ข้อตกลง รวมถึงกฎระเบียบ นโยบาย ขั้นตอนการปฏิบัติงานและวิธีการปฏิบัติงานต่าง ๆ ของกรมวิทยาศาสตร์บริการ อย่างเคร่งครัด

๑๖. ต้องมีการควบคุมการจ้างช่วงของผู้ให้บริการภายนอกให้เป็นไปตามระเบียบของกรมวิทยาศาสตร์บริการ

๑๗. มีการประเมินผลการปฏิบัติงานหรือผลการให้บริการของผู้ให้บริการภายนอก ทั้งในด้านประสิทธิภาพของบริการการรักษาความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามกฎหมายที่เกี่ยวข้องเมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่กรมวิทยาศาสตร์บริการ กำหนด รวมถึง มีการทบทวนคุณสมบัติผู้ให้บริการภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกยังคงมีคุณสมบัติที่เหมาะสม

๑๘. ต้องมีการเตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย และปัญหาด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง

๑๙. เมื่อสิ้นสุดสัญญาการปฏิบัติงาน มีการเปลี่ยนแปลงสัญญา ยกเลิกสัญญา หรือ มีการเปลี่ยนแปลงบุคคลที่เข้าปฏิบัติงานของผู้ให้บริการภายนอก พนักงานผู้ติดต่อประสานงาน ผู้ดูแลระบบที่เกี่ยวข้อง หรือพนักงานที่ได้รับมอบหมาย ต้องทำการควบคุมดูแลให้มีการส่งคืนทรัพย์สินต่าง ๆ ของกรมวิทยาศาสตร์บริการ และ เพิกถอนสิทธิในการเข้าระบบต่าง ๆ อย่างเหมาะสม

๒๐. การใช้บริการคลาวด์ (Cloud) เพื่อให้เกิดการควบคุมการใช้บริการคลาวด์จากผู้ให้บริการภายนอก ควรพิจารณาการกำหนดรายละเอียด ดังนี้

(๑) ต้องได้รับอนุญาตให้ใช้บริการคลาวด์จากผู้บริหารหรือรับผิดชอบอย่างเหมาะสม (เช่น เจ้าของข้อมูล หน่วยงานด้านเทคโนโลยีสารสนเทศ หน่วยงานทางกฎหมาย และผู้มีส่วนเกี่ยวข้องที่เกี่ยวข้องอื่น ๆ)

(๒) หน่วยงาน หรือผู้รับผิดชอบต้องตรวจสอบความน่าเชื่อถือและชื่อเสียงของผู้ให้บริการ ว่าสอดคล้องกับรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รวมถึงความต้องการของกฎระเบียบที่บังคับในการดูแลข้อมูล ทั้งนี้ ผู้ให้บริการคลาวด์ต้องได้รับการรับรองและปฏิบัติตามมาตรฐานสากล เช่น ISO/IEC 27001 CSA STAR

(๓) ต้องรับรองการปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องทั้งหมด เช่น

กฎหมายที่เกี่ยวกับความปลอดภัยของระบบสารสนเทศ การบริหารจัดการความเสี่ยง กฎหมายความเป็นส่วนตัว และนโยบายที่เกี่ยวข้องอื่น ๆ ที่เกี่ยวข้อง

(๔) ต้องมีการกำหนดข้อตกลงที่กำหนดความรับผิดชอบของผู้ให้บริการคลาวด์ในการรักษาความเป็นส่วนตัว

(๕) หน่วยงานหรือผู้รับผิดชอบต้องมีการประเมินสถานที่ที่ให้บริการคลาวด์อย่างละเอียด รวมถึงสถานที่สำรองข้อมูลหรือสถานที่สำรองเพื่อให้มั่นใจว่ามีความสอดคล้องต่อแนวทางการรักษาความต่อเนื่องและผลกระทบต่อธุรกิจของกรมวิทยาศาสตร์บริการ

(๖) หน่วยงานหรือผู้รับผิดชอบต้องมีการประเมินความเสี่ยงในการใช้บริการคลาวด์ ตามกระบวนการประเมินความเสี่ยงที่กรมวิทยาศาสตร์บริการ กำหนดไว้

(๗) ไม่อนุญาตให้มีการใช้บัญชีคลาวด์ส่วนตัวสำหรับการเก็บรักษา ประมวลผล หรือการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับกรมวิทยาศาสตร์บริการ

(๘) สัญญาการให้บริการ ควรครอบคลุมถึงขอบเขต ประเภท เงื่อนไขของการให้บริการ มีการกำหนดของสัญญาการรับประกันการบริการ (SLAs) ที่เกี่ยวข้อง

(๙) มีการกำหนดในสัญญาด้านเงื่อนไขการรับผิดชอบกรณีที่ผู้ให้บริการคลาวด์ไม่สามารถให้บริการตามที่กำหนดในข้อตกลงการให้บริการ

(๑๐) กำหนดให้ผู้ให้บริการคลาวด์ปฏิบัติตามข้อกำหนดความปลอดภัยของกรมวิทยาศาสตร์บริการ และใช้ควบคุมความปลอดภัยที่เหมาะสมตามกฎระเบียบและข้อกำหนดที่เกี่ยวข้องทั้งหมด (เช่น มาตรฐานมาตรฐานความปลอดภัยอุตสาหกรรมบัตรชำระเงิน (Payment Card Industry Data Security Standard: PCI DSS) ระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไป ของสหภาพยุโรป (General Data Protection Regulation: GDPR) พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒)

(๑๑) กำหนดการสำรองข้อมูลและการกู้คืนข้อมูลของผู้ให้บริการคลาวด์ที่สอดคล้องกับแผนความต่อเนื่องทางธุรกิจของกรมวิทยาศาสตร์บริการ เช่น ระยะเวลากู้คืนระบบให้บริการ ระยะเวลากู้คืนข้อมูล (RTO) ชุดข้อมูลล่าสุดที่กู้คืนได้ (RPO)

(๑๒) กำหนดหน้าที่ความรับผิดชอบที่ชัดเจน ระหว่างผู้ให้บริการและผู้ใช้บริการในการบริหารจัดการและใช้งานคลาวด์

(๑๓) กำหนดเงื่อนไขและความรับผิดชอบกรณีที่ต้องเปลี่ยนผู้ให้บริการคลาวด์ หรือมีการโอนสิทธิจากผู้ให้บริการคลาวด์ไปยังผู้ให้บริการรายอื่น

(๑๔) กำหนดหน้าที่ในการตรวจสอบเกี่ยวกับบริการคลาวด์

(๑๕) ดำเนินการตรวจสอบความถูกต้องของระดับบริการที่ให้บริการ

(๑๖) ดำเนินการประเมินความเสี่ยงสำหรับบริการคลาวด์

(๑๗) ตรวจสอบการปฏิบัติตามความปลอดภัยโดยผู้ให้บริการคลาวด์

(๑๘) บริการที่ทำงานในคลาวด์ต้องปฏิบัติตามหลักการของสิทธิ์ที่น้อยที่สุด

(๑๙) ต้องมีการแยกกันระหว่างโซนความปลอดภัยต่าง ๆ โดยใช้ชั้นของไฟร์วอลล์ภายในระบบคลาวด์

(๒๐) การใช้งานไฟร์วอลล์ในระบบคลาวด์ต้องปฏิบัติตามมาตรฐานการแยกโซนโดยอ้างอิงตามการจัดประเภทข้อมูลหรือความลับของข้อมูล

(๒๑) ข้อมูลที่เป็นความลับที่เก็บในบริการคลาวด์ต้องเข้ารหัสโดยเทคนิคการเข้ารหัสที่เหมาะสม โดยกุญแจการเข้ารหัสควรถูกเก็บรักษาโดยองค์กร

(๒๒) การปิดบังข้อมูลและการเข้ารหัสต้องนำเข้าไปใช้ตามความลับของข้อมูลที่จัดตามนโยบายการจัดการและการจัดการข้อมูลของ กรมวิทยาศาสตร์บริการ

(๒๓) แอปพลิเคชันต้องใช้การเข้ารหัสระดับการส่งข้อมูลที่สิ้นสุด (เช่น TLS หรือ IPSEC) เพื่อรักษาความปลอดภัยของข้อมูลที่ถูกส่งผ่านระหว่างแอปพลิเคชันที่ติดตั้งในคลาวด์และเครือข่ายของ

(๒๔) กรมวิทยาศาสตร์บริการ

(๒๕) หากใช้การเข้าสู่ระบบครั้งเดียว (Single Sign-On: SSO) จะต้องรองรับโปรโตคอลที่ได้มาตรฐาน (เช่น SAML 2.0)

(๒๖) การให้สิทธิพิเศษในการเข้าถึงหรือใช้บริการคลาวด์ ต้องมีการประเมินและอนุมัติจากผู้ที่รับผิดชอบ

(๒๗) ต้องมีการบันทึก Log สำหรับการเข้าถึงข้อมูลภายในระบบคลาวด์

(๒๘) ทำการตรวจสอบความปลอดภัยในคลาวด์อย่างเหมาะสม

(๒๙) ควรพิจารณาทำการสำรองข้อมูลของข้อมูลทั้งหมดที่เก็บในบริการคลาวด์ การสำรองข้อมูลนี้อาจจะทำโดยกรมวิทยาศาสตร์บริการ โดยตรงหรือโดยผู้ให้บริการคลาวด์

(๓๐) ข้อมูลทั้งหมดของกรมวิทยาศาสตร์บริการ ต้องถูกนำออกจากบริการคลาวด์เมื่อสิ้นสุดสัญญาโดยอันใดอันหนึ่ง ข้อมูลไม่ควรถูกเก็บในคลาวด์นานเกินความจำเป็นในการดำเนินกระบวนการธุรกิจ

หมวดที่ ๘ การรักษาความมั่นคงปลอดภัยของข้อมูลสำหรับทรัพยากรบุคคล

วัตถุประสงค์

เพื่อให้บุคลากร และบุคลากรของผู้ให้บริกรภายนอกของกรมวิทยาศาสตร์บริการ ได้เข้าใจบทบาทและหน้าที่ความรับผิดชอบของตน เพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง รวมทั้งการใช้สารสนเทศรวมถึงระบบเทคโนโลยีสารสนเทศอย่างไม่ถูกต้อง หรือผิดวัตถุประสงค์

ผู้รับผิดชอบ

๑) สถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

แนวทางปฏิบัติ

๑. ต้องมีการจัดทำกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่โดยคำนึงถึงความรู้ ความสามารถและความเพียงพอในการปฏิบัติงาน รวมถึง มีการพิจารณารับพนักงานเข้าทำงานหรือการว่าจ้างหน่วยงานให้มีการตรวจสอบประวัติและคุณสมบัติเพื่อให้เพียงพอและสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ

๒. ต้องกำกับให้มีการลงนามในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของเจ้าหน้าที่หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ซึ่งได้มีการระบุหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ ไว้ในสัญญาหรือข้อตกลงการปฏิบัติงาน ซึ่งผู้ใช้งานต้องรับทราบและยอมรับระเบียบปฏิบัติของกรมวิทยาศาสตร์บริการ โดยจะต้องอ่านทำความเข้าใจและปฏิบัติตามนโยบาย กฎ ระเบียบที่กรมวิทยาศาสตร์บริการ ได้กำหนดไว้

๓. ต้องมีการจัดทำข้อตกลงการไม่เปิดเผยความลับ (Non-disclosure Agreement) โดยครอบคลุมเนื้อหาขั้นต่ำ ดังนี้

(๑) ความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และการป้องกันการรั่วไหลของข้อมูล

(๒) ความรับผิดชอบในการเก็บรักษาความลับ และไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

(๓) การแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

(๔) การดำเนินการกรณีละเมิดหรือยกเลิกข้อตกลง รวมทั้งข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลง

๔. ต้องจัดให้มีการอบรมที่เกี่ยวข้องกับการปฏิบัติงานทั่วไป โดยหน่วยงานผู้รับผิดชอบ เพื่อให้ผู้รับจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้น เช่น วิธีการใช้ระบบงาน วิธีการใช้งานซอฟต์แวร์สำเร็จรูปการแก้ปัญหา

การใช้คอมพิวเตอร์เบื้องต้น การปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง เป็นต้น ตลอดจนการสร้างความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอให้แก่บุคลากร ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของกรมวิทยาศาสตร์บริการ โดยมีเนื้อหาครอบคลุม ดังนี้

(๑) การรักษาความมั่นคงปลอดภัยสารสนเทศ

(๒) ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และภัยคุกคามทางไซเบอร์

(๓) หลักเกณฑ์และกฎหมายที่เกี่ยวข้อง

๕. ต้องมีการกำหนดกระบวนการทางวินัยในกรณีที่เกิดการละเมิดการรักษาความมั่นคงปลอดภัยสารสนเทศของกรมวิทยาศาสตร์บริการ ให้สอดคล้องกับกฎหมาย กฎระเบียบ ข้อบังคับ สัญญาที่เกี่ยวข้อง และต้องสื่อสารให้ผู้ที่เกี่ยวข้องได้รับทราบ

๖. ข้อตกลงที่เกี่ยวข้องกับการรักษาความลับซึ่งระบุไว้ในสัญญาจ้างที่เจ้าหน้าที่ได้ทำไว้กับกรมวิทยาศาสตร์บริการ มีผลผูกพันนับตั้งแต่เริ่มจ้างจนกระทั่งภายหลังจากพ้นสภาพการเป็นเจ้าหน้าที่ตามระยะเวลาที่ระบุไว้ในข้อตกลง

๗. ต้องมีการกำหนดข้อตกลง หรือสัญญาในการรักษาความลับกับบุคลากร หรือผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร

๘. ต้องจัดให้มีกลไก ช่องทางในการรายงานเหตุละเมิดการรักษาความมั่นคงปลอดภัยสารสนเทศแก่บุคลากร หรือผู้ให้บริการภายนอกอย่างเหมาะสม

๙. ต้องจัดให้มีผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม หรือผู้บริหารที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยต้องมีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Development) สอดคล้องตามหลักการถ่วงดุล (Check and Balance) และเป็นผู้ที่มีความรู้ความสามารถหรือมีประสบการณ์สารสนเทศ และด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๑๐. ต้องมีกระบวนการจัดการเกี่ยวกับการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน และมอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน เช่น การคืนทรัพย์สินของกรมวิทยาศาสตร์บริการ การปรับปรุงสิทธิให้เป็นปัจจุบันและยกเลิกสิทธิเมื่อสิ้นสุดการจ้างงาน รวมทั้งมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิหน้าที่ และความรับผิดชอบ

หมวดที่ ๙ หน้าที่และความรับผิดชอบด้านสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดหน้าที่และความรับผิดชอบของผู้บริหารระดับสูงสุด (CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ และผู้ใช้งาน

แนวทางปฏิบัติ

ส่วนที่ ๑ ระดับนโยบาย

๑.๑ ผู้บริหารระดับสูง ของกรมวิทยาศาสตร์บริการ มีหน้าที่กำกับดูแลให้มีการปฏิบัติตามแนวปฏิบัตินี้ ทั้งนี้ ความรับผิดทางแพ่ง อาญา และวินัย ของผู้เกี่ยวข้อง ให้เป็นไปตามที่กฎหมายว่าด้วยการนั้นกำหนด

๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) กรมวิทยาศาสตร์บริการ เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ คณะกรรมการบริหารการเปลี่ยนแปลงสู่องค์กรดิจิทัลของกรมวิทยาศาสตร์บริการ เป็นผู้รับผิดชอบกำหนดนโยบาย ยุทธศาสตร์ แผนการดำเนินงาน แนวทางปฏิบัติ และโครงการเพื่อขับเคลื่อนการพัฒนาเทคโนโลยีดิจิทัลและสารสนเทศของกรมวิทยาศาสตร์บริการ

๑.๔ คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เป็นผู้รับผิดชอบกำกับดูแล พิจารณานโยบาย กระบวนการบริหารความเสี่ยงและบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศในส่วนงานที่เกี่ยวข้องให้เป็นไปตามขอบเขต และกรอบการดำเนินงานการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001:2022

๑.๕ ผู้อำนวยการสถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ ของกรมวิทยาศาสตร์บริการ เป็นผู้รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูล และเทคโนโลยีสารสนเทศ

๑.๖ หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ เป็นผู้รับผิดชอบ ดังนี้

๑.๖.๑ ควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

๑.๖.๒ วางแผน จัดทำทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ส่วนที่ ๒ ระดับปฏิบัติงาน

ระดับผู้ปฏิบัติงานประกอบด้วย ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน เป็นผู้รับผิดชอบตามภารกิจ ดังนี้

๒.๑ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ เป็นผู้รับผิดชอบ ดังนี้

๒.๑.๑ ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๒.๑.๓ ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศ ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๒.๑.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๒.๑.๕ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๑.๖ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ

๒.๒ ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศตามสิทธิ์ที่ได้รับอนุญาต โดยให้ปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด

หมวดที่ ๑๐ การพัฒนาระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดขั้นตอนและข้อกำหนดต่าง ๆ ในการจัดทำโครงการพัฒนาระบบสารสนเทศของกรมวิทยาศาสตร์บริการ ให้สอดคล้องกับสถาปัตยกรรมระบบ (Enterprise Architecture: EA) นโยบายด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ของกรมวิทยาศาสตร์บริการ

ผู้รับผิดชอบ

๑) สถาบันเทคโนโลยีดิจิทัลวิทยาศาสตร์บริการ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้ใช้งาน

แนวทางปฏิบัติ

๑. การพัฒนาระบบสารสนเทศต้องกำหนดขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง การใช้งาน โดยระบบต้องมีคุณสมบัติ ดังนี้

(๑) สอดคล้องกับสถาปัตยกรรมระบบของกรมวิทยาศาสตร์บริการ (Enterprise Architecture: EA)

(๒) สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

(๓) สามารถทำงานร่วมกันกับระบบเดิมที่ยังใช้งานอยู่ได้อย่างราบรื่น

(๔) ต้องแยกสภาวะแวดล้อมในการพัฒนาระบบสารสนเทศออกเป็น ๓ ส่วน คือ ส่วนแรก สำหรับการพัฒนาระบบ (Development) ส่วนที่สองสำหรับการทดสอบ (Testing) ส่วนที่สาม สำหรับการใช้งานจริง (Production) และต้องใช้ข้อมูลที่สร้างขึ้นสำหรับการทดสอบระบบ (Mockup Data) เท่านั้น ในกรณีที่นำข้อมูลจริงมาใช้ในการทดสอบ เช่น ข้อมูลส่วนบุคคล ต้องทำการปกปิดข้อมูล (Data Masking) เพื่อไม่ให้สามารถระบุตัวผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้ รวมทั้งกำหนดสิทธิการเข้าถึงแต่ละสภาพแวดล้อมตามหลักการแบ่งแยกหน้าที่

(๕) การพัฒนาหรือแก้ไขระบบให้ทำในส่วนสำหรับการพัฒนาระบบ (Development) เท่านั้น

(๖) หลังจากทดสอบฟังก์ชันและการทำงานในส่วนสำหรับการพัฒนาระบบแล้ว เมื่อต้องการให้ผู้ใช้งานทดสอบความถูกต้อง และความสามารถในการทำงานของระบบสารสนเทศ ให้นำระบบขึ้นไปไว้ยังส่วนสำหรับการทดสอบ (Testing)

(๗) โดยสภาวะแวดล้อมของส่วนสำหรับการทดสอบ (Testing) นั้น ควรมีสภาวะแวดล้อมใกล้เคียงมากที่สุดกับสภาวะแวดล้อมในการใช้งานจริง (Production) ได้แก่ ใช้ระบบปฏิบัติการรุ่นเดียวกัน ระบบจัดการฐานข้อมูลตัวเดียวกัน หรือหากเป็นไปได้ใช้ ฮาร์ดแวร์และซอฟต์แวร์แบบเดียวกัน ความสามารถเท่ากัน และต้องได้รับความ เห็นชอบเป็นลายลักษณ์อักษรจากผู้มีอำนาจหรือผู้ที่ได้รับมอบหมายจากผู้มีอำนาจ

(๘) เมื่อผ่านการทดสอบและยอมรับจากผู้ใช้งานแล้ว ผู้ใช้งานจะต้องลงนามเป็นลายลักษณ์อักษร

(๙) การนำระบบที่ผ่านการทดสอบแล้วไปไว้ยังส่วนสำหรับการใช้งานจริง (Production) ต้องกระทำโดยผู้ดูแลระบบที่ไม่มีสิทธิในการพัฒนาหรือแก้ไขระบบสารสนเทศนั้น

(๑๐) ห้ามมีการพัฒนาหรือแก้ไขระบบสารสนเทศใด ๆ ในส่วนสำหรับการใช้งานจริง (Production)

(๑๑) หากมีความจำเป็นต้องพัฒนาหรือแก้ไขระบบสารสนเทศใด ๆ ในส่วนสำหรับการใช้งานจริง (Production) ต้องทำเรื่องขออนุมัติ พร้อมทั้งนำเสนอความเสี่ยงและผลกระทบ ที่อาจจะเกิดขึ้น และวิธีการลดความเสี่ยงจากการกระทำนี้ ผู้มีอำนาจอาจพิจารณา อนุมัติเป็นครั้งคราวไป โดยต้องกำหนดระยะเวลาที่สามารถกระทำการนี้ไว้อย่างชัดเจน

(๑๒) การจัดหาครุภัณฑ์คอมพิวเตอร์ที่ใช้สำหรับโครงการ ให้พิจารณาจัดหา โดยการใช้บริการของรัฐบาลอิเล็กทรอนิกส์ หรือวิธีการเช่า หากมีความจำเป็นที่จะต้องจัดซื้อครุภัณฑ์คอมพิวเตอร์ดังกล่าว ให้ผู้รับผิดชอบโครงการจัดทำข้อเสนอต่อคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของกรมวิทยาศาสตร์บริการ เพื่อชี้แจงเหตุผลและความจำเป็นตลอดจนความคุ้มค่า เมื่อเทียบกับการเช่าหรือเช่าซื้อตามวงเงินที่จะใช้จัดซื้อ โดยให้ยึดเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ฉบับล่าสุดของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นเกณฑ์ในการกำหนดคุณลักษณะพื้นฐานขั้นต่ำและเพดานราคาของครุภัณฑ์คอมพิวเตอร์

๒. ในการเสนอโครงการพัฒนาระบบสารสนเทศต้องดำเนินการตามขั้นตอนการพิจารณาทบทวนเพื่ออนุมัติการสร้างการติดตั้งการใช้งาน ดังนี้

(๑) ทบทวนสถานการณ์การทำงานและสำรวจความต้องการ

(๒) จัดทำข้อเสนอโครงการพัฒนาระบบสารสนเทศ โดยมีผู้แทนฝ่ายเทคโนโลยีสารสนเทศร่วมในการจัดทำ

(๓) เสนอคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของกรมวิทยาศาสตร์บริการ พิจารณาข้อเสนอโครงการพัฒนาระบบสารสนเทศ

(๔) จัดทำร่างข้อกำหนดของโครงการพัฒนาระบบสารสนเทศ โดยมีผู้แทนฝ่ายข้อมูลและสารสนเทศร่วมในการจัดทำ

(๕) เสนอคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของกรมวิทยาศาสตร์บริการ พิจารณาร่างข้อกำหนดของโครงการพัฒนาระบบสารสนเทศ

(๖) เสนอขออนุมัติโครงการจากคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของกรมวิทยาศาสตร์บริการ

(๗) เสนอขออนุมัติงบประมาณจากสำนักงบประมาณ

(๘) ดำเนินการตามระเบียบพัสดุฯ ต่อไป

๓. การพัฒนาระบบสารสนเทศหลังจากทำสัญญาจ้างพัฒนาแล้วให้จัดการควบคุมการพัฒนา ระบบสารสนเทศที่จัดจ้างผู้รับจ้างพัฒนาภายนอก ดังนี้

(๑) ชี้แจงแนวความคิดของระบบและข้อกำหนดมาตรฐานพร้อมด้วยกระบวนการทำงานให้ผู้รับจ้างพัฒนาภายนอกทราบ

(๒) กำหนดหน้าที่และความรับผิดชอบของผู้เกี่ยวข้องในการพัฒนาระบบสารสนเทศ

(๓) กำหนดตารางเวลาในการพัฒนาแบบละเอียด โดยให้ผู้รับจ้างพัฒนาภายนอกนำเสนอความคืบหน้าของการพัฒนาระบบสารสนเทศ ได้แก่ สัปดาห์ละครั้ง หรือสองสัปดาห์ต่อครั้ง เป็นต้น

(๔) ตรวจสอบและติดตามการพัฒนาระบบสารสนเทศตามตารางเวลาในการพัฒนาอย่างละเอียด

(๕) ในการดำเนินการแก้ไข ปรับปรุงส่วนหนึ่งส่วนใดของระบบระบบสารสนเทศ ผู้รับจ้างต้องจัดทำเอกสารประกอบการดำเนินการให้ครบถ้วน ถูกต้อง และผ่านความเห็นชอบเป็นลายลักษณ์อักษรจากผู้มีอำนาจหรือผู้ที่ได้รับมอบหมายจากผู้มีอำนาจ

๔. การตรวจรับระบบสารสนเทศที่ผู้รับจ้างพัฒนาภายนอกส่งมอบให้ดำเนินการตามระเบียบพัสดุฯ โดยมีข้อกำหนดการบริการผู้รับจ้างพัฒนาภายนอกหลังตรวจรับระบบสารสนเทศในระยะเวลารับประกัน ดังนี้

(๑) ให้ผู้รับจ้างพัฒนาภายนอกแก้ไขปัญหาให้แล้วเสร็จภายใน ๒๔ ชั่วโมง นับตั้งแต่ได้รับแจ้ง หากไม่สามารถแก้ไขได้ภายในเวลาดังกล่าว ให้ผู้รับจ้างพัฒนาภายนอกแจ้งให้ผู้ดูแลระบบทราบถึงสภาพปัญหาและแนวทางการแก้ไข ภายในเวลา ๒ ชั่วโมง นับตั้งแต่ได้รับแจ้ง ทั้งนี้ ต้องใช้เวลาแก้ไขไม่เกิน ๗๒ ชั่วโมง

(๒) ผู้รับจ้างพัฒนาภายนอกต้องจัดให้มีผู้ให้บริการตามข้อกำหนดในสัญญาจ้าง โดยประกอบด้วย ผู้จัดการโครงการ นักวิเคราะห์ระบบ นักเขียนโปรแกรม เป็นต้น ประจำที่กรมวิทยาศาสตร์บริการตลอดเวลาทำการตามที่กรมวิทยาศาสตร์บริการกำหนด