



ประกาศกรมวิทยาศาสตร์บริการ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของ กรมวิทยาศาสตร์บริการ พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับ

กรมวิทยาศาสตร์บริการจึงได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ เป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางสำหรับผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศ และปฏิบัติตามมาตรการความปลอดภัยที่กำหนด มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในหน่วยงาน โดยมีผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) เป็นผู้รับผิดชอบต่อนโยบายในฐานะเป็นผู้กำกับ ติดตามและทบทวนนโยบาย

อธิบดีกรมวิทยาศาสตร์บริการโดยความเห็นชอบของคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยด้านสารสนเทศ จึงออกประกาศ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศ กรมวิทยาศาสตร์บริการ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กรมวิทยาศาสตร์บริการ พ.ศ. ๒๕๖๕ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๒ นิยาม

๒.๑ “องค์กร”	หมายถึง กรมวิทยาศาสตร์บริการ
๒.๒ “คณะกรรมการ”	หมายถึง คณะกรรมการกำกับดูแลความมั่นคงปลอดภัยด้านสารสนเทศ
๒.๓ “CEO”	หมายถึง อธิบดีกรมวิทยาศาสตร์บริการ
๒.๔ “DCIO”	หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม

- ๒.๕ “การเข้าถึงการควบคุมการใช้งานสารสนเทศ” หมายถึง การควบคุมการเข้าถึง หรือจำกัดการเข้าถึงข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเครือข่ายระบบปฏิบัติการ โปรแกรมสำเร็จรูป โปรแกรมประยุกต์ โปรแกรมมัลแวร์ประโยชน์ เพื่อความมั่นคงปลอดภัยด้านสารสนเทศ
- ๒.๖ “ข้อมูลสารสนเทศ” หมายถึง ข้อมูลที่ถูกประมวลผลโดยระบบสารสนเทศ และสามารถนำไปใช้งานหรือประมวลผลต่อไปได้
- ๒.๗ “ระบบเครือข่าย” หมายถึง ระบบเครือข่ายคอมพิวเตอร์ภายใต้การกำกับดูแลขององค์กรเพื่อใช้ในการติดต่อสื่อสาร หรือ รับ-ส่งข้อมูลสารสนเทศระหว่างระบบสารสนเทศต่าง ๆ ของกรมวิทยาศาสตร์บริการ
- ๒.๘ “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด (Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด ซึ่งอาจทำให้ความมั่นคงของระบบสารสนเทศถูกบุกรุก คุกคาม และโจมตี

ข้อ ๓ วัตถุประสงค์

๓.๑ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ ที่สอดคล้องกับบริบทองค์กร และกฎหมายที่เกี่ยวข้อง

๓.๒ จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศ เทคโนโลยี และการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

๓.๓ เพื่อให้มั่นใจได้ว่าข้อมูลและระบบสารสนเทศของ กรมวิทยาศาสตร์บริการ มีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจเกิดขึ้นในระบบสารสนเทศ กรมวิทยาศาสตร์บริการ และใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการ

๓.๔ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเครือข่ายของกรมวิทยาศาสตร์บริการมีความมั่นคงปลอดภัยจากสถานการณ์ไม่พึงประสงค์หรือไม่คาดคิดในระบบสารสนเทศ

๓.๕ เพื่อให้มั่นใจได้ว่าการปฏิบัติงานของกรมวิทยาศาสตร์บริการสามารถดำเนินได้อย่างต่อเนื่อง และเมื่อเกิดผลกระทบจากเหตุการณ์ไม่พึงประสงค์สามารถกู้คืนระบบสารสนเทศได้อย่างรวดเร็วและลดความเสียหายที่อาจเกิดขึ้น

๓.๖ เพื่อเป็นแนวทางปฏิบัติในการใช้งานระบบสารสนเทศอย่างปลอดภัย สำหรับผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ และบุคคลภายนอก

ข้อ ๔ ขอบเขต

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ กำหนดขึ้นเพื่อสร้างมาตรฐานและแนวทางในการรักษาความมั่นคงปลอดภัยในระบบสารสนเทศของกรมวิทยาศาสตร์บริการ ให้ปลอดภัยจากความเสี่ยงด้านความมั่นคงปลอดภัยด้านสารสนเทศ ที่อาจส่งผลกระทบต่อข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเครือข่าย ของกรมวิทยาศาสตร์บริการ โดยข้าราชการ พนักงานราชการ ลูกจ้างประจำ พนักงานจ้างเหมาบริการ และผู้เกี่ยวข้องกับระบบสารสนเทศของหน่วยงานทั้งหมดต้องถือปฏิบัติอย่างเคร่งครัด

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีสาระสำคัญประกอบด้วย

(๑) การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ

(๒) การมีระบบสารสนเทศและระบบสำรองสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและมีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้อย่างปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ องค์กรได้กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัย โดยมีเนื้อหาสาระสำคัญประกอบด้วย

หมวดที่ ๑ นโยบายการเข้าถึง และการควบคุมการใช้งานสารสนเทศ ประกอบด้วยแนวปฏิบัติดังนี้

๑) การเข้าถึงหรือการควบคุมการใช้งานระบบสารสนเทศ (Access control)

๑.๑ มีการควบคุมการเข้าถึงข้อมูลอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย โดยกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตการเข้าถึงระบบสารสนเทศ ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจของหน่วยงาน

๑.๒ กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงไว้อย่างชัดเจน

๑.๓ ต้องจัดทำข้อปฏิบัติการควบคุมการเข้าถึงสารสนเทศและปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความปลอดภัย

๒) การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business requirement for access control)

๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างตระหนักรู้เรื่องความมั่นคงปลอดภัยด้านสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ได้กำหนดแนวทาง ดังนี้

๓.๑ สร้างความรู้ ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงข้อกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๓.๒ การลงทะเบียนผู้ใช้งาน (User registration) กำหนดไว้เป็นขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๓.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User management) มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๓.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) กำหนดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม และใช้งานอย่างปลอดภัย

๓.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) สม่าเสมอ มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนด

๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่อลวง หรือการลักลอบทำสำเนา ข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ต้องมีแนวทางอย่างน้อย ดังนี้

๔.๑ การใช้งานรหัสผ่าน (Password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการ กำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๔.๒ มีการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๔.๓ กำหนดให้การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔.๔ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่า ด้วย การรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔

๕) การควบคุมการเข้าถึงเครือข่าย (Network access control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องมีแนวทางอย่างน้อย ดังนี้

๕.๑ การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่ เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (User authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกหน่วยงาน สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks) ต้องมีวิธีการ ที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้ง การเข้าถึงทางกายภาพและทางเครือข่าย

๕.๕ การแบ่งแยกเครือข่าย (Segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตาม กลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ต้องควบคุม การเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการ ควบคุมการเข้าถึง

๕.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ต้องควบคุมการจัด เส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือ สารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๖) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ได้กำหนดแนวทางปฏิบัติดังนี้

๖.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการ จะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๖.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และกำหนดขั้นตอนทางเทคนิคการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างของผู้ใช้งานที่ระบุถึง

๖.๓ การบริหารจัดการรหัสผ่าน (Password management system) จัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๖.๔ การใช้งานโปรแกรมมรรถประโยชน์ (Use of system utilities) ได้จำกัดและควบคุมการใช้งานโปรแกรมมรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๖.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง

๗) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and information access control)

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือการใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๗.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and Teleworking)

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๗.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) โดยกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

๘) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN access control) โดยผู้ใช้งานจะต้องลงทะเบียนใช้งานกับผู้ดูแลระบบ และนำอุปกรณ์มาขึ้นทะเบียนเพื่อให้สามารถเข้าใช้งานกับเครือข่ายที่ลงทะเบียนได้

๙) การควบคุมการใช้อินเทอร์เน็ต (Internet)

กำหนดแนวปฏิบัติเพื่อควบคุมการใช้งานอินเทอร์เน็ตอย่างปลอดภัย

๙.๑ กำหนดการใช้เส้นทางเชื่อมต่อระบบอินเทอร์เน็ตที่ปลอดภัย ที่องค์กรจัดไว้ให้เท่านั้น ได้แก่ Proxy, Firewall, IPS-IDS ห้ามมิให้ผู้ใช้งานเชื่อมต่อผ่าน Dial-up Modem

๙.๒ การรับส่งข้อมูลผ่านอินเทอร์เน็ต ต้องมีการทดสอบไวรัส (Virus Scanning) ก่อนรับส่งข้อมูล

๙.๓ การดาวน์โหลดข้อมูล หรือโปรแกรมใด ๆ จากอินเทอร์เน็ต ต้องไม่เป็นการละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

๙.๔ ต้องใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นไปตามที่กฎหมายว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๑๐) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) โดยคอมพิวเตอร์ส่วนบุคคลที่หน่วยงานอนุญาตผู้ใช้ระบบสารสนเทศใช้งาน เป็นทรัพย์สินของหน่วยงาน ที่ขึ้นทะเบียนและควบคุม ด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

๑๑) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook) โดยเครื่องคอมพิวเตอร์แบบพกพา ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ในงานราชการ ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพพร้อมใช้งาน และใช้งานอย่าง ปลอดภัย

๑๒) การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server) ผู้ดูแลระบบ จะต้องควบคุมการเข้าถึง เครื่องคอมพิวเตอร์แม่ข่าย (Server) และควบคุมการเปลี่ยนแปลงต่าง ๆ ที่อาจส่งผลกระทบต่อระบบ สารสนเทศของหน่วยงาน รวมถึงความมั่นคงปลอดภัยของข้อมูล

๑๓) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) โดยจัดแบ่งพื้นที่ในการควบคุมตามระดับความสำคัญทางสารสนเทศ ควบคุม การเข้าถึงพื้นที่อย่างปลอดภัย รวมถึงการจัดให้มีการบำรุงรักษาอุปกรณ์สารสนเทศ ให้พร้อมใช้เสมอ

๑๔) การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-mail) การลงทะเบียน ผู้ใช้งาน และการใช้งานจดหมายอิเล็กทรอนิกส์อย่างปลอดภัย

๑๕) การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) อย่างปลอดภัยไม่ส่งผล กระทบต่อความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

หมวดที่ ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล ประกอบด้วยแนวปฏิบัติที่สำคัญดังนี้

๑) การสำรองระบบและสำรองข้อมูล

๑.๑ การจัดลำดับความสำคัญของระบบ เพื่อวางแผนในการจัดทำระบบสำรอง

๑.๒ กำหนดประเภทของข้อมูลที่ต้องการสำรอง

๑.๓ การจัดเก็บระบบ และข้อมูลสำรองไว้อย่างปลอดภัย และทดสอบการกู้คืนข้อมูล (Restore) อย่างสม่ำเสมอ

๒) การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน และเตรียมความพร้อมโดยการทดสอบแผน สำเสมอ เพื่อให้มั่นใจได้ว่าเมื่อเกิดเหตุฉุกเฉินสามารถกู้คืน (Recover) กลับมาได้ตามเป้าหมาย

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑) จัดให้มีการประเมินความเสี่ยงด้านสารสนเทศสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง โดยประเมิน เพื่อจัดระดับความสำคัญของความเสี่ยงแต่ละรายการ และวางแผนการจัดการความเสี่ยงอย่างเหมาะสม

๒) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงาน (Internal auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) โดยดำเนินการตามความเหมาะสมอย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

หมวด ๔ หน้าที่และความรับผิดชอบด้านสารสนเทศ

ข้อ ๖ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) มีหน้าที่รับผิดชอบต่อความเสียหายที่เกิดขึ้นโดยตรง

ประกาศ ณ วันที่ ๒๓ มีนาคม พ.ศ. ๒๕๖๕



(นายปฐม สวรรค์ปัญญาเลิศ)
อธิบดีกรมวิทยาศาสตร์บริการ

นโยบายและแนวปฏิบัติในการรักษา
ความมั่นคงปลอดภัยด้านสารสนเทศ
กรมวิทยาศาสตร์บริการ
ประจำปี พ.ศ. ๒๕๖๕

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นในการให้ข้อมูลที่ข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจในการดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชน รวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบาย และการพัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย หลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้อง ความสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมั่นคงปลอดภัยในระบบสารสนเทศ ที่มีรูปแบบหลากหลาย ส่งผลให้ความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องมาจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศ การขาดนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

โดยคณะอนุกรรมการความมั่นคงปลอดภัยภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานภาครัฐ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

กรมวิทยาศาสตร์บริการ จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ ประจำปี ๒๕๖๕ ขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงาน และบุคลากรทุกคนในกรมวิทยาศาสตร์บริการ มีความรู้ เข้าใจในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ

กรมวิทยาศาสตร์บริการ

สารบัญ

บทที่ ๑ บทนำ

๑.๑. หลักการ	๑
๑.๒. วัตถุประสงค์	๑
๑.๓. องค์ประกอบของนโยบาย	๒
๑.๔. บทบังคับใช้	๒
๑.๕. การเผยแพร่และทบทวน	๒

บทที่ ๒ คำนิยาม

๓

บทที่ ๓ นโยบายการรักษาความมั่นคงปลอดภัย

หมวด ๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๘

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)	๘
ส่วนที่ ๒ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for access control)	๑๐
ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)	๑๑
ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)	๑๒
ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)	๑๕
ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	๑๘
ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)	๑๙
ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)	๒๒
ส่วนที่ ๙ การควบคุมการใช้อินเทอร์เน็ต (Internet)	๒๓
ส่วนที่ ๑๐ การใช้งานคอมพิวเตอร์ส่วนบุคคล (Personal Computer)	๒๔
ส่วนที่ ๑๑ การใช้งานคอมพิวเตอร์แบบพกพา (Notebook)	๒๔
ส่วนที่ ๑๒ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)	๒๖
ส่วนที่ ๑๓ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)	๒๘
ส่วนที่ ๑๔ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-mail)	๓๐
ส่วนที่ ๑๕ การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)	๓๑

หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล

ส่วนที่ ๑ การสำรองข้อมูล (Back Up)	๓๒
ส่วนที่ ๒ การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน	๓๓

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓๕

หมวด ๔ หน้าที่และความรับผิดชอบด้านสารสนเทศ

ส่วนที่ ๑ ระดับนโยบาย	๓๕
ส่วนที่ ๒ ระดับปฏิบัติงาน	๓๕

๑. บทนำ

๑.๑ หลักการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ข้อมูลถือเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการ และเป็นสิ่งที่มีค่าอย่างยิ่งสำหรับองค์กร ซึ่งจะได้รับการป้องกันรักษาให้มีความมั่นคงปลอดภัย เช่นเดียวกับสินทรัพย์อื่น ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปแบบสิ่งพิมพ์ สื่ออิเล็กทรอนิกส์ และในระบบสารสนเทศที่มีความสะดวกรวดเร็ว ง่ายต่อการเข้าถึง แต่ก็คงมีความเสี่ยงของภัยคุกคามที่อยู่ในวงกว้าง และอาจก่อให้เกิดความเสียหายต่อข้อมูล หรือมีการลักลอบนำข้อมูลไปใช้ในทางมิชอบ สร้างความเสียหายต่อองค์กรได้

ความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศจึงมีสำคัญอย่างยิ่งต่อองค์กร ที่จะต้องมีการวางแผนและมีกระบวนการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงจากภัยคุกคามที่เข้ามาในระบบสารสนเทศ องค์กรจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับกฎหมาย และมาตรฐานสากล เพื่อเป็นแนวปฏิบัติด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้แก่บุคลากรในองค์กร และบุคลากรอื่นที่เกี่ยวข้องนำไปปฏิบัติอย่างเคร่งครัด เพื่อให้บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรต่อไป

๑.๒ วัตถุประสงค์

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมวิทยาศาสตร์บริการ ฉบับนี้มีวัตถุประสงค์เพื่อ

๑) กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ ที่สอดคล้องกับบริบทองค์กร และกฎหมายที่เกี่ยวข้อง

๒) จัดทำเป็นบรรทัดฐานด้านความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศ เทคโนโลยี และการสื่อสารของบุคลากรในองค์กร และบุคลากรอื่นที่มีส่วนเกี่ยวข้องกับกิจกรรมอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศขององค์กร

๓) เพื่อให้มั่นใจได้ว่าข้อมูลและระบบสารสนเทศของ กรมวิทยาศาสตร์บริการ มีมาตรการในการรักษาความมั่นคงปลอดภัย ลดผลกระทบ ลดความเสียหายที่อาจเกิดขึ้นในระบบสารสนเทศ กรมวิทยาศาสตร์บริการ และใช้เป็นแนวทางเพื่อการพัฒนาและปรับปรุงคุณภาพการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการ

๔) เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเครือข่ายของกรม วิทยาศาสตร์บริการมีความมั่นคงปลอดภัยจากสถานการณ์ไม่พึงประสงค์หรือไม่คาดคิดในระบบสารสนเทศ

๕) เพื่อให้มั่นใจได้ว่าการปฏิบัติงานของกรมวิทยาศาสตร์บริการสามารถดำเนินได้อย่างต่อเนื่อง และเมื่อเกิดผลกระทบจากเหตุการณ์ไม่พึงประสงค์สามารถกู้คืนระบบสารสนเทศได้อย่างรวดเร็วและลดความเสียหายที่อาจจะเกิดขึ้น

๖) เพื่อเป็นแนวทางปฏิบัติในการใช้งานระบบสารสนเทศอย่างปลอดภัย สำหรับผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ และบุคคลภายนอก

๑.๓ องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของ กรมวิทยาศาสตร์บริการ ฉบับนี้ อ้างอิงตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรฐานสากล ISO/IEC 27001 และ NIST Cybersecurity Framework โดยแนวทางปฏิบัตินี้ ประกอบด้วย วัตถุประสงค์ ผู้เกี่ยวข้อง และรายละเอียด หรือขั้นตอนแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบ เทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการ

๑.๔ บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ ครอบคลุมข้อมูลและระบบสารสนเทศของกรมวิทยาศาสตร์บริการ บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตาม นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุน และติดตามการประยุกต์ใช้ โดยอธิบดีกรมวิทยาศาสตร์บริการ

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรือเกิดอันตรายใด ๆ แก่องค์กรหรือผู้หนึ่ง ผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูง (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อ ความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๑.๕ การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมวิทยาศาสตร์ บริการ ฉบับนี้ จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่ โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายใน (Intranet) และเผยแพร่ในเว็บไซต์หลักของกรม วิทยาศาสตร์บริการ (<https://www.dss.go.th>) เพื่อให้บุคลากรของกรมวิทยาศาสตร์บริการ และ บุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒. คำนิยาม

๑. คำเรียกแทนหน่วยงานในเอกสารฉบับนี้ เช่น กรม หมายความว่า กรมวิทยาศาสตร์บริการ
๒. ผู้บริหารระดับสูง หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารราชการของ กรมวิทยาศาสตร์บริการ
๓. การรักษาความมั่นคงปลอดภัย หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับด้านสารสนเทศ ของ กรมวิทยาศาสตร์บริการ
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 ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ และการสื่อสาร
 - 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. สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
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 การกำหนด สิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้อย่างก็ได้

๘. **ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ (Information Security)** หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) ห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ
๙. **เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันนำไปสู่ปัญหาด้านความมั่นคงปลอดภัยด้านสารสนเทศ
๑๐. **สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

หมวดที่ ๑ นโยบายการเข้าถึง และการควบคุมการใช้งานสารสนเทศ

วัตถุประสงค์

- ๑) เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของกรมวิทยาศาสตร์บริการ
- ๒) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับกรมวิทยาศาสตร์บริการ ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

- ๑) กองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี
- ๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๓) ผู้ใช้งาน

แนวปฏิบัติ

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

เพื่อให้การเข้าถึงและควบคุมการใช้งานสารสนเทศมีความมั่นคงปลอดภัย กำหนดให้ผู้ดูแลระบบมีแนวปฏิบัติดังนี้

๑. การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ประมวลผลข้อมูล
 - ๑.๑ ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน เท่านั้น
 - ๑.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้
 - ๑.๒.๑ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ 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 ผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

กรมวิทยาศาสตร์บริการใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๒.๑ จัดแบ่งประเภทของข้อมูล ออกเป็น

๒.๑.๑ ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

๒.๑.๒ ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ บริการรับรองระบบงานห้องปฏิบัติการ บริการกิจกรรมทดสอบความชำนาญ 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 จัดแบ่งลำดับชั้นความลับของข้อมูลดังนี้

“ข้อมูลลับที่สุด” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

“ข้อมูลลับมาก” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

“ข้อมูลลับ” หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

“ข้อมูลทั่วไป” หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๒.๔ การจัดแบ่งระดับชั้นการเข้าถึง

ระดับที่ ๑ ระดับชั้นสำหรับผู้บริหาร

ระดับที่ ๒ ระดับชั้นสำหรับผู้ใช้งานทั่วไป

ระดับที่ ๓ ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๒.๕ การกำหนดเวลาในการเข้าถึงข้อมูล

การเข้าถึงข้อมูลของกรมวิทยาศาสตร์บริการ กำหนดไว้เป็นช่วงเวลาเข้าถึงได้ดังนี้

ลำดับ	เวลาที่เข้าถึงได้	ข้อมูล / ช่องทางการเข้าถึงข้อมูล
๑	ทุกวัน ตั้งแต่เวลา ๐๕.๓๐ – ๒๒.๐๐ น.	- ระบบลงเวลาปฏิบัติราชการ
๒	ทุกวัน ตลอด ๒๔ ชั่วโมง	- เว็บไซต์ - ระบบสารบรรณอิเล็กทรอนิกส์ - ระบบลาออนไลน์ - ระบบรับเรื่องร้องเรียนออนไลน์ - ระบบถ่ายทอดเทคโนโลยี - ระบบประกาศการจัดซื้อจัดจ้าง - ระบบผลงานวิจัยที่นำไปใช้ในเชิงพาณิชย์ - ระบบรายงานผลการดำเนินงานตามตัวชี้วัด - ระบบประชุมแบบอิเล็กทรอนิกส์ - ระบบจดหมายอิเล็กทรอนิกส์ - ระบบ Back Office - ระบบบริการทดสอบ สอบเทียบ - ระบบฐานข้อมูล OTOP - ระบบ e-Learning - ระบบบริการทดสอบความชำนาญ - ระบบห้องสมุดอิเล็กทรอนิกส์ - ระบบยื่นขอรับรองออนไลน์ - ระบบลงทะเบียนฝึกอบบรมออนไลน์

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 คือ 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 ความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้งาน

๓.๑.๑ กรมวิทยาศาสตร์บริการ จัดให้มีการอบรมเพื่อสร้างความรู้ และความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ และรู้เท่าทันต่อภัยคุกคาม และผลกระทบที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศอย่างไม่มีระยะวัง 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 เพื่อให้ผู้ใช้งานทราบถึงสิทธิ์ หน้าที่รับผิดชอบ และมาตรการด้านความมั่นคงปลอดภัย ในการเข้าถึงระบบสารสนเทศ

๓.๒.๕ กำหนดให้มีการยกเลิก เพิกถอนการอนุญาตเข้าถึงระบบสารสนเทศ การตัดออกจากการลงทะเบียนผู้ใช้งาน 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 และผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี จัดทำขอเป็นลายลักษณ์อักษร โดยการให้สิทธิ์พิเศษดังกล่าวจะต้องกำหนดช่วงเวลาชัดเจน และเมื่อพ้นกำหนดการให้สิทธิ์พิเศษ จะต้องระงับการใช้งานทันที

๓.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๓.๔.๑ ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราวในครั้งแรกให้แก่ผู้ใช้งาน จากนั้นส่งมอบให้ผู้ใช้งาน เป็นเอกสารปิดผนึกที่เป็นความลับ เมื่อผู้ใช้งานได้รับจะต้องเปลี่ยนรหัสผ่านใหม่ทันที ภายใน ๗ วัน

๓.๔.๒ การตั้งรหัสผ่านใหม่จะต้องตั้งรหัสให้มีความยากในการคาดเดา โดยรหัสผ่านต้อง ประกอบด้วย ตัวอักษรเล็ก ตัวอักษรใหญ่ สัญลักษณ์พิเศษ ๘ หลัก (digits)

๓.๔.๓ กำหนดให้การเข้ารหัสผิดได้ ไม่เกิน ๓ ครั้ง กรณีบัญชีผู้ใช้งานไม่สามารถเข้าใช้งานได้ เนื่องจากเข้ารหัสผิดเกินจำนวนครั้งที่กำหนด ให้ติดต่อผู้ดูแลระบบ และแจ้งความจำนงค์ขอตั้งรหัสผ่านใหม่

๓.๔.๔ กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ทุก ๆ ๑๘๐ วัน

๓.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access right)

ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งาน สิทธิการใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตจากผู้ที่ไม่มียสิทธิการเข้าถึง โดยมีแนวปฏิบัติ ดังนี้

๓.๕.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน พร้อมรายละเอียดสิทธิที่ได้รับของแต่ละบุคคล

๓.๕.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและ สิทธิการใช้งานว่าถูกต้องหรือไม่

๓.๕.๓ ดำเนินการแก้ไขข้อมูล สิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับ

๓.๕.๔ ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๗ วัน หรือ เมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน ๑๕ วัน

ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibility)

๔.๑ การใช้งานรหัสผ่าน (Password Use)

๔.๑.๑ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับ ผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) ของตนเอง

๔.๑.๒ การกำหนดรหัสผ่าน (Password) ที่เดาสุ่มได้ยาก ซึ่งประกอบด้วย

- กำหนดให้ความยาวไม่น้อยกว่า ๘ ตัวอักษร
- ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef”, “aaaaa” เป็นต้น
- การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับของเดิมครั้งสุดท้าย
- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ, นามสกุล หรือวันเกิด เป็นต้น
- ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม
- ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

๔.๑.๓ ไม่ใช่โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

๔.๑.๔ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๔.๑.๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๑๘๐ วันหรือทุกครั้งที่มีการแจ้งเตือน ให้เปลี่ยนรหัสผ่าน

๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

การป้องกันอุปกรณ์เมื่อไม่มีผู้ใช้งาน มีแนวปฏิบัติเพื่อป้องกันผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์ขณะที่ไม่มีผู้ดูแลอุปกรณ์ ดังนี้

๔.๒.๑ มีการกำหนดมาตรการป้องกันทรัพย์สินขององค์กรและควบคุมไม่ให้มีการทิ้ง หรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัยให้ครอบคลุมเรื่องต่าง ๆ คือ การจัดการบริเวณล้อมรอบ การควบคุมการเข้าออก การจัดบริเวณการเข้าถึงกรณีมีการส่งผลิตภัณฑ์โดยบุคคลภายนอก การจัดวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการทำงานในสถานที่ที่มีความปลอดภัย

๔.๒.๒ การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ เจ้าของข้อมูลต้องปฏิบัติตาม แนวทางการทำลาย ดังนี้

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

๔.๒.๓ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ โดยการรับ-ส่งข้อมูลสำคัญ หรือ ข้อมูลซึ่งเป็นความลับให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล SSL หรือ VPN

๔.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

กรมวิทยาศาสตร์บริการได้กำหนดแนวปฏิบัติเพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ รวมถึงกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน โดยมีแนวปฏิบัติดังนี้

๔.๓.๑ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๔.๓.๒ ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าขณะที่ไม่ได้ใช้งาน เช่น ภายใน ๑๕ นาที ให้เครื่องล็อกหน้าจอ และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๔.๓.๓ ผู้ใช้งานต้องล็อกใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๔.๓.๔ กรณีข้อมูลสำคัญที่บันทึกไว้ใน กระดาษ สื่อบันทึกข้อมูลแฟลชไดรฟ์ หรือ ฮาร์ดดิสก์ เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล

๔.๓.๕ ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

๔.๔ การใช้งานระบบสารสนเทศอย่างปลอดภัย

เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัย และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งาน ดังนี้

๔.๔.๑ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าจะเป็นการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๔.๔.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงานและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเป็นเกิดจากการรหัสผ่านลืตกี้ดี หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

๔.๔.๓ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าจะเป็นข้อมูลนั้นจะเป็นของกรมวิทยาศาสตร์บริการ หรือเป็นบุคคลภายนอก

๔.๔.๔ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของ กรมวิทยาศาสตร์บริการ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารสูงสุด

๔.๔.๕ ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่กรมวิทยาศาสตร์บริการต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับกรมวิทยาศาสตร์บริการ ซึ่งกรมวิทยาศาสตร์บริการอาจแต่งตั้งให้ผู้ที่ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๔.๔.๖ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (BitTorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจาก ผู้บริหารสูงสุด

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

๔.๔.๘ ห้ามใช้สินทรัพย์ของ กรมวิทยาศาสตร์บริการที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของกรมวิทยาศาสตร์บริการ

๔.๔.๙ ห้ามใช้ระบบสารสนเทศของกรมวิทยาศาสตร์บริการ เพื่อรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกรมวิทยาศาสตร์บริการ

๔.๔.๑๐ ห้ามใช้ระบบสารสนเทศของ กรมวิทยาศาสตร์บริการเพื่อประโยชน์ทางการค้า

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

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการเครือข่ายโดยไม่ได้รับอนุญาต จึงได้กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบ ดังนี้

๕.๑ การใช้งานบริการเครือข่าย

๕.๑.๑ กำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

๕.๑.๒ กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

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

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกกรมวิทยาศาสตร์บริการ (User authentication for external connections)

๕.๒.๑ เมื่อผู้ใช้งานที่อยู่ภายนอกกรมวิทยาศาสตร์บริการ เมื่อต้องเข้าใช้งานระบบสารสนเทศ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

๕.๒.๒ มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงด้วยการใช้รหัสผ่าน (Password)

๕.๒.๓ การเข้าสู่ระบบสารสนเทศของกรมวิทยาศาสตร์บริการ จากเครือข่ายอินเทอร์เน็ตต้องได้รับอนุญาตจาก ผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี และต้องมีการเข้ารหัสที่เป็นมาตรฐานสากลเพื่อความปลอดภัยด้วย VPN

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment identification in network)

๕.๓.๑ กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย IP Address และ MAC Address

๕.๓.๒ จัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่ใช้เชื่อมกับระบบเครือข่ายของกรมวิทยาศาสตร์บริการ โดยมีรายละเอียดของอุปกรณ์ประกอบด้วย เครื่องคอมพิวเตอร์ IP Address MAC Address สถานที่ติดตั้ง ผู้ใช้งาน เป็นต้น

๕.๓.๓ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับอนุญาตเท่านั้น

๕.๓.๔ ต้องใช้ไฟร์วอลล์ (Firewall) ที่สามารถกำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายของกรมวิทยาศาสตร์บริการได้

๕.๓.๕ จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวข้องกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

๕.๓.๖ แผนผังเครือข่าย เป็นเอกสารในระดับลับมากจะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่ และทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

๕.๔.๑ การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่ายต้องมีการตั้งรหัสผ่านและให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๕.๔.๒ มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย และเปิดใช้เฉพาะอุปกรณ์และเวลาที่จำเป็นเท่านั้น

๕.๔.๓ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น

๕.๔.๔ ติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

๕.๕ การแบ่งแยกเครือข่าย (Segregation in network)

กำหนดให้มีการแบ่งแยกเครือข่ายตามประเภทการใช้งานเพื่อความปลอดภัย ดังนี้

๕.๕.๑ Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

๕.๕.๒ Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

เพื่อควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้มีความมั่นคงปลอดภัย ได้กำหนดแนวปฏิบัติดังนี้

๕.๖.๑ จำกัดสิทธิ์ของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

๕.๖.๒ ระบบเครือข่ายต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall, IDS/IPS)

๕.๖.๓ การเข้าสู่ระบบเครือข่ายของกรมวิทยาศาสตร์บริการ ต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยที่กำหนดไว้เท่านั้น

๕.๖.๔ ต้องระบุอุปกรณ์และเครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

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

๕.๖.๖ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังนี้

(๑) จำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่าย ที่ได้รับอนุญาตเท่านั้น

(๒) จำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

(๓) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์
แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

(๔) ระบบเครือข่ายทั้งหมดของกรมวิทยาศาสตร์บริการ ที่มีการเชื่อมต่อไปยังระบบ
เครือข่ายอื่น ๆ ภายนอกกรมวิทยาศาสตร์บริการต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องม
ีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

(๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention
System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของ
กรมวิทยาศาสตร์บริการ ในลักษณะที่ผิดปกติ

(๖) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่าง
ชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง หากมีการ
แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๗) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของ
บุคคลที่เข้าใช้งานระบบเครือข่ายของกรมวิทยาศาสตร์บริการ ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุ
กรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่
ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๘) IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงาน
ภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับ
โครงสร้างของระบบเครือข่ายได้โดยง่าย

(๙) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการ
อนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

การจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียน
ของข้อมูลหรือ สารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ
ซึ่งมีแนวปฏิบัติในการจัดเส้นทางบนเครือข่าย ดังนี้

๕.๗.๑ ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน
หรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งาน
ตามภารกิจ

๕.๗.๒ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๕.๗.๓ กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อย เครือข่าย
ภายในและภายนอก

๕.๗.๔ ต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง
(Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการของกรมวิทยาศาสตร์บริการ โดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบ ดังนี้

๖.๑ ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

๖.๑.๑ กำหนดให้ระบบไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๖.๑.๒ กำหนดให้ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่าการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๖.๑.๓ จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน โดยผู้ใช้งานจะต้องป้อนรหัสผ่านภายในเวลา ๑๕ นาที เพื่อเข้าใช้งานระบบ

๖.๑.๔ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๖.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๖.๒.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

๖.๒.๒ หากต้องการใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกันต้องขึ้นอยู่กับความจำเป็นทางด้านเทคนิค หรือสอดคล้องกับการปฏิบัติงาน โดยจะต้องได้รับการอนุมัติจาก ผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี และกำหนดกรอบเวลาการใช้งานที่ชัดเจน และยุติการใช้งานทันที เมื่อพบความผิดปกติหรือหมดเวลาที่ขออนุมัติไว้

๖.๓ การบริหารจัดการรหัสผ่าน (Password Management System)

กำหนดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ ดังนี้

๖.๓.๑ มีระบบการตรวจสอบการกำหนดรหัสผ่าน ซึ่งประกอบด้วยตัวอักษร ตัวเลข และตัวอักษรพิเศษ หรือเทคนิคอื่นใดในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) และมีคุณภาพ

๖.๓.๒ เมื่อดำเนินการติดตั้งระบบแล้วให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของรายชื่อผู้ใช้งานทั้งหมดที่ถูกกำหนดไว้เริ่มต้นซึ่งมาพร้อมกับการติดตั้งระบบโดยทันที

๖.๔ การใช้โปรแกรมอรรถประโยชน์ (Use of System Utilities)

กำหนดให้มีการจำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่กำหนด โดยมีแนวปฏิบัติ ดังนี้

๖.๔.๑ การใช้โปรแกรมอรรถประโยชน์ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการพิสูจน์ ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

๖.๔.๒ โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

๖.๔.๓ จัดเก็บโปรแกรมมัลแวร์ประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน และเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๖.๔.๔ จำกัดสิทธิ์การใช้งาน เฉพาะผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมมัลแวร์ประโยชน์เท่านั้น

๖.๔.๕ กำหนดให้ผู้ดูแลระบบมีการถอดถอนโปรแกรมมัลแวร์ประโยชน์ที่ไม่จำเป็นออกจากระบบ รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมมัลแวร์ประโยชน์ได้

๖.๕ การกำหนดระยะเวลาการใช้งานระบบสารสนเทศ (Session Time - Out)

๖.๕.๑ กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานภายในช่วงระยะเวลา ๑๕ นาที

๖.๕.๒ ระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลาการใช้งานระบบ เมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นระยะเวลาไม่เกิน ๑๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

เพื่อป้องกันการเข้าถึงระบบสารสนเทศ และโปรแกรมที่มีความเสี่ยงสูง หรือมีความสำคัญสูง กำหนดแนวปฏิบัติในการจำกัดระยะเวลาในการเชื่อมต่อเพื่อความมั่นคงปลอดภัย ดังนี้

๖.๖.๑ กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศสำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ให้ใช้งานได้ภายใน ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาราชการ วันจันทร์ ถึง วันศุกร์ เวลา ๐๘.๓๐ – ๑๖.๓๐ น. เท่านั้น

๖.๖.๒ กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกกรม) มีการจำกัดระยะเวลาการเชื่อมต่อไม่เกิน ๓ ชั่วโมงต่อครั้ง

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

(Application and Information Access Control)

เพื่อป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศโดยไม่ได้รับอนุญาต กำหนดแนวปฏิบัติสำหรับผู้ดูแลระบบต้องดำเนินการ ดังนี้

๗.๑ จำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ควบคุมการเข้าถึงหรือการใช้งานของผู้ใช้งาน โดยการเข้าใช้งาน การเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ได้กำหนดหลักเกณฑ์การจำกัดหรือควบคุมการเข้าถึงหรือการใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศ ดังนี้

๗.๑.๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของกรมวิทยาศาสตร์บริการตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิ์ของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิ์การเข้าถึงระบบสารสนเทศและข้อมูล

๗.๑.๒ จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด โดยยกเลิกการเชื่อมต่อระบบเมื่อครบกำหนดเวลา

๗.๑.๓ ผู้ให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน และต้องลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของกรมวิทยาศาสตร์บริการ

๗.๑.๔ ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

๗.๑.๕ ผู้ดูแลระบบต้องควบคุม การเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิ์เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource)

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

๗.๒.๑ แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น และแสดงให้เห็น ถึงผลกระทบและระดับความสำคัญต่อกรมวิทยาศาสตร์บริการ

๗.๒.๒ ควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ ดังนี้

(๑) ระบบซึ่งไวต่อการรบกวน จะต้องควบคุมการเข้าถึงอุปกรณ์ และระบบ โดยติดตั้งไว้ในพื้นที่ปลอดภัย

(๒) ติดตามเฝ้าระวังการใช้งานระบบซึ่งไวต่อการรบกวน และระงับการใช้งานทันทีเมื่อพบเหตุการณ์ผิดปกติ

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

(๑) อุปกรณ์ที่ใช้ในการสื่อสาร หรือปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ ต้องนำมาขึ้นทะเบียนกับผู้ดูแลระบบ

(๒) การเข้าถึงระบบโดยการปฏิบัติงานจากภายนอกต้องขออนุมัติการใช้งานจากผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี เพื่อเปิดสิทธิ์ให้ปฏิบัติงานจากภายนอกได้

(๓) ผู้ปฏิบัติงานจากภายนอก ต้องปฏิบัติงานในที่ปลอดภัย และงดการใช้เครือข่ายสาธารณะเพื่อเข้าถึงระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

๗.๒.๔ ควบคุมการเข้าใช้งานจากเครือข่ายภายใน และเครือข่ายภายนอกตามข้อกำหนด

๗.๒.๕ วางแผนการสำรอง และทดสอบการกู้คืนระบบ ตามคู่มือการสำรองระบบสารสนเทศ

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่

กำหนดแนวปฏิบัติและมาตรการเพื่อปกป้องระบบสารสนเทศ ซึ่งจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ โดยผู้ใช้งานอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ที่ต้องปฏิบัติ ดังนี้

๗.๓.๑ การป้องกันอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ครอบคลุมการใช้งาน อุปกรณ์สื่อสารประเภทพกพา ได้แก่ Smart Phone, Notebook, Laptop, Tablet หรืออุปกรณ์อื่นใดใน ลักษณะเดียวกันนี้ โดยกำหนดให้มีการป้องกัน การเชื่อมต่อของอุปกรณ์คอมพิวเตอร์ และอุปกรณ์สื่อสาร เคลื่อนที่เข้ากับเครือข่ายของกรมวิทยาศาสตร์บริการ โดยไม่ได้รับอนุญาต

๗.๓.๒ กำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์ และ อุปกรณ์สื่อสารเคลื่อนที่ ซึ่งจะต้องแสดงตัวตนเมื่อใช้งาน

๗.๓.๓ ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์ คอมพิวเตอร์ และอุปกรณ์สื่อสารเคลื่อนที่ของตนเอง

๗.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking)

เพื่อปกป้องระบบสารสนเทศจากการปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ กำหนด แนวปฏิบัติเพื่อความมั่นคงปลอดภัย ดังนี้

๗.๔.๑ การปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการ สื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ และระบบงานต่าง ๆ ภายในกรมวิทยาศาสตร์บริการ

๗.๔.๒ การเข้าถึงระบบสารสนเทศของกรมวิทยาศาสตร์บริการ จากระยะไกลด้วยอุปกรณ์ที่เป็น ของส่วนตัว ต้องได้รับอนุญาตจาก ผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี

๗.๔.๓ การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์ บริการได้ ต้องมีหนังสือเป็นลายลักษณ์อักษร และมีความเห็นของผู้บังคับบัญชาตามลำดับชั้น และได้รับความ เห็นชอบจาก ผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี โดยระบุรายละเอียด การขอเปิดใช้งานระบบสารสนเทศจากภายนอกกรมวิทยาศาสตร์บริการ โดยมีรายละเอียด ดังนี้

(๑) เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ

(๒) รายละเอียดและลักษณะของระบบงาน

(๓) ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ

(๔) รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน

(๕) ช่วงเวลาและระยะเวลาในการปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ

๗.๔.๔ ไม่อนุญาตให้ปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ สำหรับระบบงานที่มี ความลับในระดับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

๗.๔.๕ การเข้าสู่ระบบสารสนเทศของกรมวิทยาศาสตร์บริการ จากระยะไกลต้องมีการลงบันทึก เข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วย การใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๗.๔.๖ ผู้ได้รับอนุญาตให้สามารถเข้าถึงระบบสารสนเทศและข้อมูลของกรมวิทยาศาสตร์บริการ ต้องไม่ให้สมาชิกภายในครอบครัว หรือบุคคลอื่นใดสามารถเข้าถึงระบบได้ด้วยสิทธิของตนเอง

๗.๔.๗ ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้า ระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

๗.๔.๘ ผู้ดูแลระบบจะทำการยกเลิกสิทธิ์การเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอก
กรมวิทยาศาสตร์บริการของผู้ใช้งานทันที เมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์
อักษรเพื่อขอยกเลิกต่อผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี

๗.๔.๙ ผู้ดูแลระบบต้องทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกกรม
วิทยาศาสตร์บริการ อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

เพื่อให้การเข้าถึงระบบเครือข่ายไร้สายในกรมวิทยาศาสตร์บริการมีความมั่นคงปลอดภัยกำหนด
แนวทางปฏิบัติ เพื่อควบคุมการเข้าถึงระบบเครือข่ายไร้สายไว้ ดังนี้

๘.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของกรมวิทยาศาสตร์บริการ จะต้องลงทะเบียนกับ
ผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการกอง
หอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๘.๒ ผู้ดูแลระบบต้องดำเนินการลงทะเบียนผู้ใช้งาน ดังนี้

๘.๒.๑ ลงทะเบียน และกำหนดสิทธิ์ผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับ
หน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิ์การเข้าถึง
อย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานจะได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๘.๒.๒ ต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนระบบเครือข่ายไร้สาย

๘.๒.๓ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้
สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่ง
สัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

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

๘.๒.๕ เปลี่ยนค่าชื่อผู้ใช้งานและรหัสผ่านในการเข้าสู่ระบบ สำหรับการตั้งค่าการทำงานของ
อุปกรณ์ไร้สายและเลือกใช้ชื่อผู้ใช้งานและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่
สามารถคาดเดาหรือเจาะรหัสได้โดยง่าย

๘.๒.๖ กำหนดค่าใช้ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless
LAN Client และอุปกรณ์กระจาย (Access Point) เพื่อให้ยากต่อการดักจับ และเพิ่มความปลอดภัยให้กับ
ระบบเครือข่ายไร้สาย

๘.๒.๗ เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) ชื่อผู้ใช้
(Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะ
อนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้
เท่านั้นให้สามารถเข้าใช้ระบบเครือข่ายไร้สายได้

๘.๒.๘ ควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สาย กับ
เครือข่ายภายในกรมวิทยาศาสตร์บริการ

๘.๒.๙ ใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย
สม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบ
พบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศ
วิทยาศาสตร์และเทคโนโลยีทันที

ส่วนที่ ๙ การควบคุมการใช้อินเทอร์เน็ต (Internet)

กำหนดแนวปฏิบัติเพื่อควบคุมการใช้งานอินเทอร์เน็ตอย่างปลอดภัย ดังนี้

๙.๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการใช้งานอินเทอร์เน็ต
ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่กรมวิทยาศาสตร์บริการจัดสรรไว้เท่านั้น เช่น Proxy, Firewall,
IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Mobile Hotspot Wi-Fi,
Pocket Wi-Fi หรืออุปกรณ์ที่มีลักษณะการทำงานคล้ายกัน ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการ
ขออนุญาตจากผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยีเป็นลายลักษณ์อักษร

๙.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ต
ผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของ
ระบบปฏิบัติการ

๙.๓ การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning)
โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๙.๔ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของกรมวิทยาศาสตร์บริการ เพื่อหาประโยชน์ในเชิงพาณิชย์
เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอัน
อาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อ
สังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลนี้อาจก่อให้เกิดความเสียหายให้กับกรมวิทยาศาสตร์บริการ

๙.๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมวิทยาศาสตร์บริการที่ยังไม่ได้
ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

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

๙.๗ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์จะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ
กรมวิทยาศาสตร์บริการ ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อ
ชื่อเสียงของกรมวิทยาศาสตร์บริการ การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๙.๘ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความ
มั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการ
เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

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

๙.๑๐ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่าง
เคร่งครัด

ส่วนที่ ๑๐ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)

เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลให้มีความปลอดภัย กำหนดแนวปฏิบัติ ดังนี้

๑๐.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลที่กรมวิทยาศาสตร์บริการอนุญาตให้ผู้ใช้งานระบบสารสนเทศใช้งาน เป็นทรัพย์สินของกรมวิทยาศาสตร์บริการ ที่ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบ เป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

๑๐.๒ โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของกรมวิทยาศาสตร์บริการ ต้องเป็นโปรแกรมที่ กรมวิทยาศาสตร์บริการได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคลหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย และห้าม ผู้ใช้งานติดตั้ง แก้ไขโปรแกรมด้วยตนเอง ผู้ดูแลระบบมีหน้าที่จัดหาและติดตั้งโปรแกรมในเครื่องของกรม วิทยาศาสตร์บริการเท่านั้น

๑๐.๓ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการโดยเจ้าหน้าที่ ของกรมวิทยาศาสตร์บริการ หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับกรม วิทยาศาสตร์บริการเท่านั้น การนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกนอกกรมวิทยาศาสตร์บริการ เพื่อการใดก็ตาม ต้องขออนุมัติผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยีเป็น ลายลักษณ์อักษรเท่านั้น

๑๐.๔ การใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบสื่อก่อนเพื่อหาไวรัสโดยโปรแกรมป้องกัน ไวรัสที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลก่อนทุกครั้ง

๑๐.๕ ผู้ใช้งาน มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ดังนี้

๑๐.๕.๑ กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เพื่อเปิดใช้เครื่อง และ เก็บรักษารหัสผ่านอย่างปลอดภัย

๑๐.๕.๒ เมื่อไม่ได้ใช้งานเกิน ๑๕ นาที ควรตั้งโปรแกรมรักษาจอภาพ (Screen Saver) และ ต้องใช้รหัสผ่านเพื่อเข้าใช้งานอีกครั้ง และเมื่อเลิกใช้งานควรล็อกเอาท์ (Log Out) ออกจากเครื่อง

๑๐.๕.๓ ต้องอัปเดต (Update) ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัย คุกคามต่าง ๆ

๑๐.๕.๔ ต้องไม่ถอดถอนการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ในเครื่องคอมพิวเตอร์ ส่วนบุคคลของกรมวิทยาศาสตร์บริการ

๑๐.๕.๕ ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่มีได้ขึ้นทะเบียนอุปกรณ์กับผู้ดูแลระบบ มาใช้ งานและเชื่อมต่อกับระบบเครือข่ายของกรมวิทยาศาสตร์บริการ ยกเว้นจะได้รับอนุญาตเป็นลายลักษณ์อักษร และนำมาขึ้นทะเบียนกับผู้ดูแลระบบของกรมวิทยาศาสตร์บริการก่อนการใช้งาน

ส่วนที่ ๑๑ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

๑๑.๑ เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของกรม วิทยาศาสตร์บริการ เพื่อใช้ในงานราชการ ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครอง ที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพพร้อมใช้งาน

๑๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของกรมวิทยาศาสตร์บริการ ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

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

๑๑.๔ ตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) เมื่อไม่ได้ใช้งานเกิน ๑๕ นาที เพื่อล็อกหน้าจอเมื่อไม่มีการใช้งาน และต้องใส่รหัสผ่านอีกครั้งเมื่อกลับมาใช้งาน

๑๑.๕ ต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งาน

๑๑.๖ ต้องสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา ลงบนสื่อจัดเก็บที่ปลอดภัย เพื่อป้องกันการสูญหายของข้อมูล และจัดเก็บอย่างปลอดภัย หรือกำหนดรหัสการเข้าสู่ระบบที่ข้อมูล รวมถึงการทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๑.๗ การเคลื่อนย้ายคอมพิวเตอร์แบบพกพา ต้องดำเนินการด้วยความระมัดระวัง เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือพลัดหลุดมือ เป็นต้น หลีกเลี่ยงการใส่เครื่องคอมพิวเตอร์พกพาไว้ในกระเป๋าเดินทาง เพราะอาจถูกกดทับเกิดความเสียหายได้

๑๑.๘ หลีกเลี่ยงการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดอยู่ กรณีต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์ภายในเครื่อง

๑๑.๙ ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

(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 ๑๒ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๑๒.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ โดยผู้ดูแลระบบ ดังนี้

๑๒.๑.๑ ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

๑๒.๑.๒ ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

๑๒.๑.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติจากผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี ก่อนดำเนินการ

๑๒.๑.๔ ไม่ติดตั้งซอร์สโค้ดคอมไพเลอร์ (Compiler) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๑๒.๑.๕ กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

๑๒.๑.๖ กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบสารสนเทศ เป็นต้น

๑๒.๑.๗ วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

๑๒.๑.๘ จัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ที่ไม่ได้ใช้งานไว้อย่างปลอดภัยเพื่ออ้างอิง

๑๒.๒ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ

๑๒.๒.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๑๒.๒.๒ วางแผนเผื่อระวังและทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลง ระบบปฏิบัติการ

๑๒.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๑๒.๓.๑ กำหนดให้มีการควบคุมการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

๑๒.๓.๒ ระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๑๒.๓.๓ กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๑๒.๓.๔ กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ก่อนมีการติดตั้ง

๑๒.๓.๕ การทดสอบซอฟต์แวร์ห้ามทดสอบบนระบบ และฐานข้อมูลที่ใช้งาน เลือกสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นได้กับระบบที่ใช้งาน

๑๒.๔ มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

๑๒.๔.๑ ผู้ให้บริการที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของกรมวิทยาศาสตร์บริการ จะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจาก ผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี

๑๒.๔.๒ ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

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

๑๒.๔.๔ การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจาก ผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยีก่อนทุกครั้ง

๑๒.๕ มาตรการควบคุมช่องโหว่ทางเทคนิค

๑๒.๕.๑ กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน และบริหารจัดการช่องโหว่ของระบบเหล่านั้น โดยมีการบันทึกข้อมูลอย่างน้อย ดังนี้

- (๑) ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- (๒) สถานที่ที่ติดตั้ง
- (๓) เครื่องแม่ข่ายที่ติดตั้ง
- (๔) ผู้ผลิตซอฟต์แวร์
- (๕) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

๑๒.๕.๒ กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

๑๒.๕.๓ กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบ ดำเนินการ ดังนี้

(๑) มีการเฝ้าระวังและติดตามประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

(๒) กำหนดแหล่งข้อมูลข่าวสาร สำหรับใช้ในการติดตามช่องโหว่ระบบสารสนเทศของกรมวิทยาศาสตร์บริการ

(๓) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

๑๒.๕.๔ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

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

- (๑) ข้อมูลชื่อบัญชีผู้ใช้งาน
- (๒) ข้อมูลวันเวลาที่เข้าถึงระบบ
- (๓) ข้อมูลวันเวลาที่ออกจากระบบ
- (๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
- (๕) ข้อมูลการล็อกอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ
- (๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
- (๗) ข้อมูลการเปลี่ยนคอนฟิกูเรชัน (Configuration) ของระบบ
- (๘) ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)
- (๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น
- (๑๐) ข้อมูลไอพีแอดเดรส (IP Address) ที่เข้าถึง
- (๑๑) ข้อมูลโปรโตคอล (Protocol) เครือข่ายที่ใช้
- (๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
- (๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

ส่วนที่ ๑๓ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๑๓.๑ ห้องควบคุมเครื่องแม่ข่ายและระบบเครือข่ายคอมพิวเตอร์ของกรมวิทยาศาสตร์บริการ

๑๓.๑.๑ กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร โดยกำหนดพื้นที่ปฏิบัติงาน พื้นที่ควบคุมเฉพาะให้ชัดเจน เพื่อกำหนดสิทธิ์การเข้าถึงพื้นที่ โดยผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศ วิทยาศาสตร์และเทคโนโลยี

๑๓.๑.๒ กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร ดังนี้

- (๑) ผู้เข้าใช้งานต้องเป็นผู้ที่ได้รับสิทธิ์การเข้าใช้งานพื้นที่เท่านั้น
- (๒) ควบคุมการเข้าใช้งานในพื้นที่ควบคุมเฉพาะโดยแบบพิมพ์นิ้วมือ (Finger Scan)
- (๓) ติดตั้งกล้องวงจรปิดเพื่อติดตาม และเฝ้าระวัง การเข้าพื้นที่ห้องควบคุมเครื่องแม่

ข่ายและระบบเครือข่ายคอมพิวเตอร์

๑๓.๑.๓ หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบ เครือข่ายภายในกรมวิทยาศาสตร์บริการ จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่อง คอมพิวเตอร์หรืออุปกรณ์ และต้องได้รับอนุญาตจากผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศ วิทยาศาสตร์และเทคโนโลยี

๑๓.๑.๔ จัดให้มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอ ต่อ ความต้องการใช้งาน และมีความพร้อมในการใช้งาน ดังนี้

- (๑) ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง
- (๒) ติดตั้งระบบดับเพลิง และแจ้งเตือนอัคคีภัย
- (๓) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น

(๔) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีจากระบบสนับสนุนการทำงานภายในห้องควบคุมเครื่องแม่ข่ายและระบบเครือข่ายคอมพิวเตอร์ทำงานผิดปกติหรือหยุดการทำงาน

(๕) วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนอย่างสม่ำเสมอให้มั่นใจได้ว่าระบบต่าง ๆ สามารถทำงานได้ตามปกติ

๑๓.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ

๑๓.๒.๑ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของกรมวิทยาศาสตร์บริการในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงติดตั้งระบบป้องกันที่ปลอดภัย

๑๓.๒.๒ ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๑๓.๒.๓ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๑๓.๒.๔ ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

๑๓.๒.๕ จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๑๓.๒.๖ ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ต้องล็อกกุญแจตลอดเวลา เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๑๓.๒.๗ พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

๑๓.๒.๘ ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๑๓.๓ การบำรุงรักษาอุปกรณ์

๑๓.๓.๑ วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา

๑๓.๓.๒ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๑๓.๓.๓ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๑๓.๓.๔ ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในกรมวิทยาศาสตร์บริการ ในกรณีที่ต้องเข้าไปปฏิบัติงานในพื้นที่ควบคุม ผู้ดูแลระบบจะต้องอยู่ในพื้นที่ด้วยทุกครั้ง

๑๓.๓.๕ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑๓.๔ การนำทรัพย์สินของกรมวิทยาศาสตร์บริการออกนอกกรมวิทยาศาสตร์บริการ

๑๓.๔.๑ ต้องขออนุญาตจากผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี ก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอก หรือ นำไปซ่อมบำรุงภายนอก

๑๓.๔.๒ ผู้ดูแลระบบจะต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าวกลับมาตามช่วงเวลาที่กำหนด และตรวจสอบอยู่ในสภาพดี

๑๓.๔.๓ บันทึกข้อมูลการนำอุปกรณ์ของกรมวิทยาศาสตร์บริการออกไปใช้งานนอกกรม วิทยาศาสตร์บริการ และบันทึกส่งคืน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย

๑๓.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกกรมวิทยาศาสตร์บริการ

๑๓.๕.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ หรือทรัพย์สินของกรมวิทยาศาสตร์บริการออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๑๓.๕.๒ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของกรมวิทยาศาสตร์บริการไว้โดยลำพังในที่สาธารณะ หรือสถานที่เสี่ยงต่อการสูญหาย

๑๓.๕.๓ เจ้าหน้าที่ผู้ใช้งานรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๑๓.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

๑๓.๖.๑ ผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี เป็นผู้อนุมัติในการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ต้องยื่นเรื่องขออนุมัติเป็นลายลักษณ์อักษร

๑๓.๖.๒ ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยต้องมั่นใจว่า ข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

ส่วนที่ ๑๔ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : อีเมล)

๑๔.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมวิทยาศาสตร์ บริการ ให้เหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่าง สม่าเสมออย่างน้อยปีละ ๑ ครั้ง

๑๔.๒ ผู้ดูแลระบบรับเรื่องการขอใช้งานจดหมายอิเล็กทรอนิกส์ของกรมวิทยาศาสตร์บริการ โดย กำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานอีเมล รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบ ตัวตนจริงของผู้ใช้งาน

๑๔.๓ กำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านใหม่ทันที เมื่อได้รับรหัสผ่านครั้งแรก (Default Password) และต้องเปลี่ยนรหัสผ่านใหม่ทุก ๑๘๐ วัน หรือเมื่อได้รับแจ้งให้เปลี่ยนรหัสผ่าน

๑๔.๔ ผู้ดูแลระบบต้องกำหนดให้การเข้ารหัสผ่านจดหมายอิเล็กทรอนิกส์ เมื่อใส่รหัสผ่านต้องไม่ ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘x’ หรือ ‘*’ ในการพิมพ์แต่ละตัวอักษร

๑๔.๕ กำหนดให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

๑๔.๗ ระบบจดหมายอิเล็กทรอนิกส์จะออกจากระบบ (Log out) เพื่อตัดการใช้งาน เมื่อผู้ใช้งาน ไม่ได้ใช้งานระบบเป็นระยะเวลาภายใน ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีก ครั้ง

๑๔.๘ ผู้ใช้งานควรหลีกเลี่ยงค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๑๔.๙ ผู้ใช้งานต้องระมัดระวังในการใช้อีเมล เพื่อไม่ให้เกิดความเสียหายต่อกรมวิทยาศาสตร์บริการ ได้แก่ การละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์รวมทั้ง

ไม่อนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้อีเมล ผ่านระบบเครือข่ายของกรมวิทยาศาสตร์บริการ

๑๔.๑๐ ผู้ใช้งานต้องไม่ใช่ที่อยู่อีเมล (E-mail Address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของอีเมล

๑๔.๑๑ หลังจากการใช้งานอีเมลเสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานอีเมล โดยไม่ได้รับอนุญาต

๑๔.๑๒ ผู้ใช้งานควรตรวจสอบเอกสารแนบจากอีเมล ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันไวรัส โดยเฉพาะการเปิดไฟล์ที่เป็น Executable File เช่น .exe หรือ .com เป็นต้น

๑๔.๑๓ ผู้ใช้งานไม่เปิดหรือส่งต่ออีเมล หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๔.๑๔ ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับ-ส่งอีเมล ที่ไม่เหมาะสม หรือข้อมูลอันอาจทำให้เสียชื่อเสียง หรือข้อมูลทำให้เกิดความแตกแยกผ่านทางอีเมล

๑๔.๑๕ ผู้ใช้งานควรตรวจสอบตู้เก็บอีเมล (Inbox) ของตนเองทุกวัน และควรลบอีเมลที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่บนอีเมล

ส่วนที่ ๑๕ การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๕.๑ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความระมัดระวังในเรื่องความมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือข้อมูลความลับของกรมวิทยาศาสตร์บริการ

๑๕.๒ ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรมวิทยาศาสตร์บริการ

๑๕.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อกรมวิทยาศาสตร์บริการ ผู้ใช้งานต้องแจ้งต่อกลุ่มเทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

หมวด ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล

วัตถุประสงค์

- ๑) เพื่อให้ระบบสารสนเทศของกรมวิทยาศาสตร์บริการ สามารถให้บริการได้อย่างต่อเนื่อง
- ๒) เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับกรมวิทยาศาสตร์บริการ อย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย
- ๓) เพื่อให้ผู้ใช้งานได้รับรู้ เข้าใจ สามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

- ๑) กองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี
- ๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

ส่วนที่ ๑ การสำรองข้อมูล (Back Up)

คัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๑.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานพร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และวางแผน โดยการกำหนดความถี่ในการสำรองข้อมูล โดยพิจารณาจากความสำคัญของข้อมูล ความถี่ในการเปลี่ยนแปลงข้อมูล โดยมีรายละเอียดการสำรองข้อมูล ดังนี้

๑.๒.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ ดังนี้

(๑) ข้อมูลคอนฟิกูเรชัน (Configuration) สำหรับระบบ

(๒) ฐานข้อมูล (Database) ในระบบสารสนเทศ

(๓) ซอฟต์แวร์ (Software) ต่าง ๆ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ ระบบงาน หรือซอฟต์แวร์อื่น ๆ ที่สำคัญ

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

๑.๒.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมสำหรับการกู้คืนระบบ

๑.๒.๔ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานการณ์สำรองข้อมูล เป็นต้น

๑.๒.๕ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และหากพบว่าผิดปกติต้องจัดทำบันทึกและดำเนินการแก้ไขโดยทันที

๑.๒.๖ ในกรณีที่จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล ต้องขี้งบสื่อบันทึกข้อมูลไว้อย่างชัดเจน โดยมีรายละเอียดของชื่อ วัน/เวลาสำรองข้อมูล ผู้รับผิดชอบ โดยสื่อสำรองข้อมูลจะต้องจัดเก็บไว้อย่างปลอดภัย และข้อมูลที่สำรองต้องเข้ารหัสเพื่อความปลอดภัย

๑.๒.๗ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับ กรมวิทยาศาสตร์บริการควรห่างกันเพียงพอ เพื่อไม่ให้เกิดผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานในสถานที่ทำงานได้ เป็นต้น ทั้งนี้สอดคล้องตามแผนฉุกเฉินด้านสารสนเทศที่กำหนดไว้

๑.๒.๘ วางแผนทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ (restore) โดยการทดสอบต้องจัดทำบันทึกการทดสอบไว้เป็นหลักฐาน

ส่วนที่ ๒ การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการ ทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๒.๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการ ทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

๒.๑.๑ กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๑.๒ ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้นรวมทั้งมาตรการลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานในสถานที่ทำงานได้ เป็นต้น ทำให้ไม่สามารถเข้ามาใช้งานระบบสารสนเทศได้

๒.๑.๓ กำหนดขั้นตอนปฏิบัติในการกู้คืน (Recover) ระบบสารสนเทศ และระยะเวลาการกู้คืนระบบที่สอดคล้องตามเป้าหมายที่หน่วยงานกำหนดไว้

๒.๑.๔ กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบ และการทดสอบแผนฉุกเฉิน

๒.๑.๕ กำหนดช่องทางในการติดต่อเมื่อเกิดกรณีฉุกเฉิน ทั้งผู้รับผิดชอบภายใน กรมวิทยาศาสตร์บริการ และผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อผู้ให้บริการ

๒.๑.๖ สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๕ ทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

- ๑) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
- ๒) เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นได้กับระบบสารสนเทศ
- ๓) เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

ผู้รับผิดชอบ

- ๑) กองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี
- ๒) ผู้ดูแลระบบที่ได้รับมอบหมาย
- ๓) ผู้ตรวจสอบภายใน

แนวทางปฏิบัติ

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 กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่ต้องตรวจสอบแบบอ่านได้อย่างเดียว
 - ๒.๔.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งการทำลายหรือลบข้อมูลโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างเหมาะสม
 - ๒.๔.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
 - ๒.๔.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อก (Log) แสดงการเข้าถึง วันและเวลาที่เข้าถึงระบบ
 - ๒.๔.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือจากการเข้าถึงโดยไม่ได้รับอนุญาต

หมวด ๔ หน้าที่และความรับผิดชอบด้านสารสนเทศ

วัตถุประสงค์

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

แนวปฏิบัติ

ส่วนที่ ๑ ระดับนโยบาย

๑.๑ ผู้บริหารระดับสูงสุด (Chief Executive Officer: CEO) ของกรมวิทยาศาสตร์บริการ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer: DCIO) กรมวิทยาศาสตร์บริการ เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓ ผู้อำนวยการกองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี ของกรมวิทยาศาสตร์บริการ เป็นผู้รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูล และเทคโนโลยีสารสนเทศ

๑.๔ หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ กองหอสมุดและศูนย์สารสนเทศวิทยาศาสตร์และเทคโนโลยี เป็นผู้รับผิดชอบ ดังนี้

๑.๔.๑ ควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

๑.๔.๒ 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 และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

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 โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด