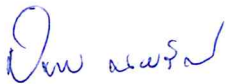


เรียน ผอ.สำนัก/กอง

เพื่อโปรดทราบประกาศ วศ. จำนวน ๑ ฉบับ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคง
ปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ
พ.ศ. ๒๕๖๕ และถือปฏิบัติตามนโยบายและแนว
ปฏิบัติฯ ดังกล่าว ทั้งนี้สามารถเปิดอ่านได้ทาง URL
<https://bit.ly/3OiSwWo> หรือ สแกน QR Code ที่
ปรากฏด้านล่างนี้



(นางสาวปัทมา นพรัตน์)

ผสท.

๑๖ เม.ย. ๖๕



ประกาศ เรื่องนโยบายฯ



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 โปรแกรมอรรถประโยชน์ 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 เพื่อให้เกิดความตระหนักรู้ 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) สม่ำเสมอ มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนด

๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ 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. ๒๕๔๔

๕) การควบคุมการเข้าถึงเครือข่าย (Network access control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องมีแนวทางอย่างน้อย ดังนี้

๕.๑ การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่ เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๕.๒ การยืนยันตัวตนบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (User authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกหน่วยงาน 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) ต้องควบคุมการ จัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือ 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 การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities) ได้จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๖.๕ เมื่อมีการวางเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (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 ทั้งนี้เพื่อให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

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 และเป็นไปตามที่กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๑๐) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) โดยคอมพิวเตอร์ส่วนบุคคลที่หน่วยงานอนุญาตผู้ใช้ระบบสารสนเทศใช้งาน เป็นทรัพย์สินของหน่วยงาน ที่ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยผู้ดูแลระบบเป็นผู้ดำเนินการ ซึ่งผู้ใช้งานมีหน้าที่ดูแลและใช้งานอย่างปลอดภัย

๑๑) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Notebook) โดยเครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงาน เพื่อใช้ในงานราชการ ควบคุมด้วยหมายเลขครุภัณฑ์ อยู่ในความรับผิดชอบของผู้ถือครองที่ต้องดูแลให้ปลอดภัย และอยู่ในสภาพพร้อมใช้งาน และใช้งานอย่างปลอดภัย

๑๒) การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server) ผู้ดูแลระบบ จะต้องควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server) และควบคุมการเปลี่ยนแปลงต่าง ๆ ที่อาจส่งผลกระทบต่อระบบสารสนเทศของหน่วยงาน รวมถึงความมั่นคงปลอดภัยของข้อมูล

๑๓) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) โดยจัดแบ่งพื้นที่ในการควบคุมตามระดับความสำคัญทางสารสนเทศ ควบคุมการเข้าถึงพื้นที่อย่างปลอดภัย รวมถึงการจัดให้มีการบำรุงรักษาอุปกรณ์สารสนเทศ ให้พร้อมใช้เสมอ

๑๔) การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-mail) การลงทะเบียนผู้ใช้งาน และการใช้งานจดหมายอิเล็กทรอนิกส์อย่างปลอดภัย

๑๕) การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) อย่างปลอดภัยไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยในระบบสารสนเทศขององค์กร

หมวดที่ ๒ นโยบายการรักษาความปลอดภัยและระบบสำรองข้อมูล ประกอบด้วยแนวปฏิบัติที่สำคัญดังนี้

๑) การสำรองระบบและสำรองข้อมูล

๑.๑ การจัดลำดับความสำคัญของระบบ เพื่อวางแผนในการจัดทำระบบสำรอง

๑.๒ กำหนดประเภทของข้อมูลที่ต้องการสำรอง

๑.๓ การจัดเก็บระบบ และข้อมูลสำรองไว้อย่างปลอดภัย และทดสอบการกู้คืนข้อมูล (Restore) อย่างสม่ำเสมอ

๒) การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน และเตรียมความพร้อมโดยการทดสอบแผนสม่ำเสมอ เพื่อให้มั่นใจได้ว่าเมื่อเกิดเหตุฉุกเฉินสามารถกู้คืน (Recover) กลับมาได้ตามเป้าหมาย

หมวด ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

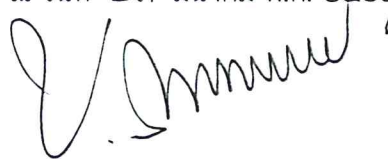
๑) จัดให้มีการประเมินความเสี่ยงด้านสารสนเทศสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง โดยประเมินเพื่อจัดระดับความสำคัญของความเสี่ยงแต่ละรายการ และวางแผนการจัดการความเสี่ยงอย่างเหมาะสม

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