



ประกาศกรมวิทยาศาสตร์บริการ

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ เพื่อให้การดำเนินการต่าง ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงาน โดยอาศัยอำนาจตามความใน มาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชบัญญัติกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

เพื่อให้การปฏิบัติงานและการบริหารราชการมีความมั่นคงปลอดภัย เชื่อถือได้ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ และสามารถดำเนินงานได้อย่างต่อเนื่อง กรมวิทยาศาสตร์บริการจึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมวิทยาศาสตร์บริการ พ.ศ. ๒๕๖๔ เพื่อเป็นเครื่องมือให้กับผู้ให้บริการ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการ

จึงประกาศให้ทราบ และถือปฏิบัติโดยทั่วกัน

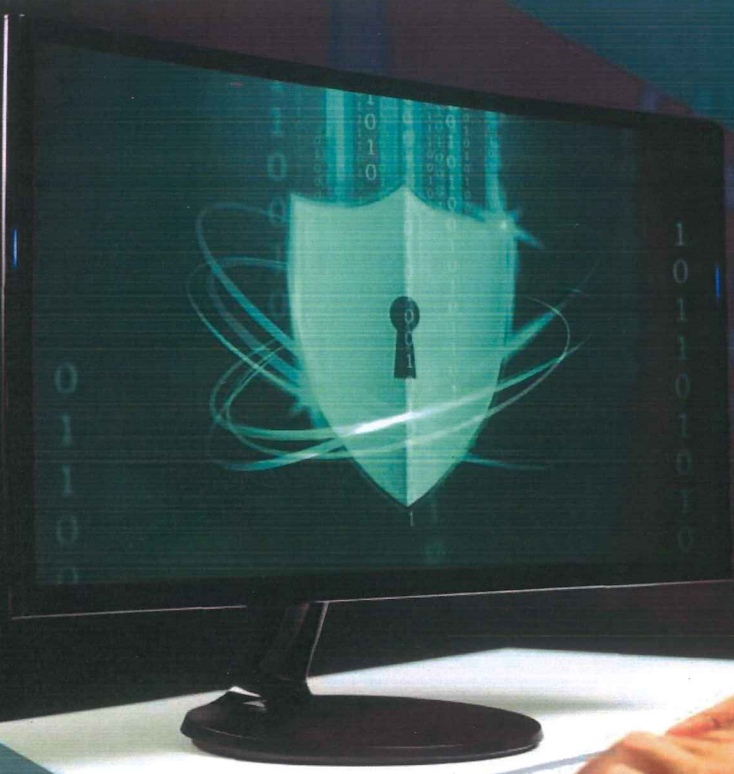
ประกาศ ณ วันที่ ๑๕ พฤษภาคม พ.ศ. ๒๕๖๔

(นายปฐม สุวรรณปัญญาเลิศ)

อธิบดีกรมวิทยาศาสตร์บริการ

๑๓๑ ปี

กรมวิทยาศาสตร์บริการ



นโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมวิทยาศาสตร์บริการ

พ.ศ. ๒๕๖๔

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กรมวิทยาศาสตร์บริการ พ.ศ. ๒๕๖๔

สารบัญ

เนื้อหา	หน้า
ความเป็นมา	
๑. หลักการและเหตุผล	๑
๒. วัตถุประสงค์	๑
๓. เป้าหมาย	๑
๔. องค์ประกอบของนโยบาย	๒
ส่วนที่ ๑	
นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ	
๑.๑ การควบคุมการเข้าถึงข้อมูลและสารสนเทศ	๓
๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน	๔
๑.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน	๖
๑.๔ การควบคุมการเข้าถึงระบบเครือข่าย	๘
๑.๕ การใช้งานอินเทอร์เน็ต	๙
๑.๖ การใช้งานเครือข่ายสังคมออนไลน์	๙
๑.๗ การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์	๙
๑.๘ การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ใช้งานร่วมกัน	๙
๑.๙ การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ	๑๐
๑.๑๐ การควบคุมการเข้าถึงระบบปฏิบัติการ	๑๑
๑.๑๑ การบริหารจัดการคอมพิวเตอร์แม่ข่าย	๑๑
๑.๑๒ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย	๑๒
๑.๑๓ การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์	๑๒
๑.๑๔ หน้าที่และความรับผิดชอบของผู้ดูแลระบบ	๑๒
๑.๑๕ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม	๑๓
ส่วนที่ ๒	
นโยบายการจัดทำระบบสำรองสารสนเทศ	
๒.๑ ระบบสำรอง	๑๕
๒.๒ การสำรองข้อมูล	๑๕
๒.๓ การกู้คืนข้อมูล	๑๖
ส่วนที่ ๓	
นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ	๑๗
ส่วนที่ ๔	
นโยบายการสร้างตระหนักรู้ในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	๑๘

ความเป็นมา

๑. หลักการและเหตุผล

ตามที่ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ กรมวิทยาศาสตร์บริการ ได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมวิทยาศาสตร์บริการเป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันภัยคุกคามต่างๆ และการปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาดังกล่าวได้อย่างถูกต้องและเหมาะสม รวมถึงยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่นๆ ที่เกี่ยวข้อง และการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจน จากภัยคุกคามต่างๆ

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมวิทยาศาสตร์บริการ ให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๒ เพื่อให้เกิดความเชื่อมั่นด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมวิทยาศาสตร์บริการ และทำให้ดำเนินงานต่างๆ เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

๒.๓ เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหารเจ้าหน้าที่ทุกระดับ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร มีความรู้ ความเข้าใจและตระหนักถึงความสำคัญ และถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔ เพื่อให้มีระบบสำหรับตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี

๓. เป้าหมาย

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของกรมวิทยาศาสตร์บริการ

๓.๒ กำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๓ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้กับบุคลากรและผู้เกี่ยวข้องทุกระดับของกรมวิทยาศาสตร์บริการ

๓.๔ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๔. องค์ประกอบของนโยบาย

ส่วนที่ ๑ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

- ๑.๑ การควบคุมการเข้าถึงข้อมูลและสารสนเทศ
- ๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน
- ๑.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
- ๑.๔ การควบคุมการเข้าถึงระบบเครือข่าย
- ๑.๕ การใช้งานอินเทอร์เน็ต
- ๑.๖ การใช้งานเครือข่ายสังคมออนไลน์
- ๑.๗ การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์
- ๑.๘ การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ใช้งานร่วมกัน
- ๑.๙ การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ
- ๑.๑๐ การควบคุมการเข้าถึงระบบปฏิบัติการ
- ๑.๑๑ การบริหารจัดการคอมพิวเตอร์แม่ข่าย
- ๑.๑๒ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
- ๑.๑๓ การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์
- ๑.๑๔ หน้าที่และความรับผิดชอบของผู้ดูแลระบบ
- ๑.๑๕ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๒ นโยบายการจัดทำระบบสำรองสารสนเทศ

- ๒.๑ ระบบสำรอง
- ๒.๒ การสำรองข้อมูล
- ๒.๓ การกู้คืนข้อมูล

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๔ นโยบายการสร้างตระหนักรู้ในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑

นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของกรมวิทยาศาสตร์บริการ
๒. เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้ เข้าใจขั้นตอนและปฏิบัติตามแนวทางการบริหารจัดการบัญชีผู้ใช้งานสารสนเทศของกรมวิทยาศาสตร์บริการ โดยเคร่งครัด

ผู้รับผิดชอบ

๑. กลุ่มเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑.๑ การควบคุมการเข้าถึงข้อมูลและสารสนเทศ

กรมวิทยาศาสตร์บริการได้กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ การจัดแบ่งระดับการเข้าถึงข้อมูล เวลา และช่องทางการเข้าถึงข้อมูล ดังนี้

๑.๑.๑ การจัดแบ่งประเภทสิทธิของผู้เข้าถึงข้อมูลแต่ละกลุ่มที่เกี่ยวข้อง

- (๑) อ่านอย่างเดียว
- (๒) สร้างข้อมูล
- (๓) แก้ไข
- (๔) ลบ
- (๕) อนุมัติ

๑.๑.๒ การแบ่งระดับการเข้าถึงข้อมูลและสารสนเทศ

- (๑) ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น
- (๒) ผู้ปฏิบัติงาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย
- (๓) ผู้ดูแลระบบ มีสิทธิในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่

หน้าที่

(๔) ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น

(๕) การกำหนดสิทธิพิเศษสามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูลเท่านั้น

- (๖) การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิเท่านั้น
- ๑.๑.๓ การกำหนดเวลาที่สามารถเข้าถึงได้ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

๑.๑.๔ ทบทวนและตรวจสอบสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ

(๑) ทบทวนและตรวจสอบสิทธิการเข้าถึงและใช้งานระบบสารสนเทศ ปีละ ๑ ครั้ง โดยผู้ดูแลระบบ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามสำนัก/กอง แล้วจัดส่งรายชื่อดังกล่าวให้กับสำนัก/กอง ดำเนินการ ทบทวนว่า มีรายชื่อที่ เกษียณ โอนย้าย ลาออกหรือไม่ หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้แก้ไขสิทธิการเข้าถึงให้ ถูกต้องหรือไม่

(๒) สำนัก/กอง แจ้งกลับผู้ดูแลระบบเพื่อดำเนินการแก้ไขให้ถูกต้อง

(๓) สำนัก/กอง ที่เป็นเจ้าของระบบสารสนเทศต้องตรวจสอบคุณสมบัติและสิทธิของผู้ใช้อย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องดำเนินการเปลี่ยนแปลงสิทธิให้สอดคล้องกับระดับชั้นการเข้าถึงและการ ใช้งานระบบทันที

๑.๑.๕ ช่องทางการเข้าถึงข้อมูลและระบบสารสนเทศมีดังนี้

- (๑) เครือข่ายภายในกรมวิทยาศาสตร์บริการ
- (๒) เครือข่ายภายนอกกรมวิทยาศาสตร์บริการ
- (๓) เข้าถึงโดยผ่านเครือข่ายส่วนตัวเสมือน (VPN) ที่จัดไว้ให้

๑.๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน

๑.๒.๑ การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานโดย

(๑) กำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้าน สารสนเทศ

(๒) อบรมผู้ใช้งาน เพื่อให้สามารถใช้งานข้อมูลสารสนเทศ และระบบสารสนเทศได้อย่างถูกต้อง รวมถึงให้ตระหนักและเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานข้อมูลสารสนเทศ และระบบสารสนเทศโดย ไม่ระมัดระวัง

(๓) ประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่ สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๑.๒.๒ การลงทะเบียนผู้ใช้งานมีแนวทางดังนี้

- (๑) จัดทำแบบสั่งซ่อม/ทำสิ่งของ (F-CDO-071) สำหรับขอใช้ระบบสารสนเทศ
- (๒) จัดทำคู่มือการใช้งานระบบสารสนเทศให้ผู้ใช้งานสามารถเข้าใจการทำงานของระบบสารสนเทศ

ทราบ

(๓) ให้ผู้ใช้งานกรอกข้อมูลการขอใช้ระบบสารสนเทศลงในแบบ F-CDO-071 และดำเนินการตาม ขั้นตอนการลงทะเบียนผู้ใช้งานระบบ

(๔) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย กำหนดระดับการเข้าใช้งานสารสนเทศเท่าที่จำเป็นในแต่ละ ระบบงาน และทำการบันทึกจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศทุกครั้ง

(๕) ระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล และไม่ซ้ำซ้อนกัน

(๖) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษ หากซ้ำ ให้เพิ่มอักษรตัวแรกของนามสกุลไว้ด้านหลังชื่อ หรือจนกว่าจะไม่ซ้ำ กับชื่อผู้ใช้งานคนอื่น

(๗) กำหนดบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และกำหนดสิทธิการใช้งานระบบเท่าที่จำเป็นในแต่ละระบบงาน

(๘) ต้องตรวจสอบและมอบหมายสิทธิที่เหมาะสมต่อหน้าที่ความรับผิดชอบ หรือ ความต้องการของกรมวิทยาศาสตร์บริการ ให้ผู้มีส่วนเกี่ยวข้องกับระบบงาน

(๙) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

(๑๐) ผู้ดูแลระบบจัดทำการบันทึกการเปลี่ยนแปลงบัญชีผู้ใช้งานแต่ละรายในระบบเมื่อได้รับรายงานบัญชีรายชื่อผู้ใช้งานได้ถูกเพิกถอนสิทธิ หรือลาออก หรือเปลี่ยนแปลงตำแหน่ง หรือย้ายหน่วยงาน

๑.๒.๓ การบริหารจัดการสิทธิของผู้ใช้งานโดย

(๑) ผู้ดูแลระบบจัดทำขั้นตอนการปฏิบัติสำหรับวิธีการมอบหมาย หรือการกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒) ผู้ดูแลระบบบันทึกการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศ ตามที่ได้รับอนุมัติ หรือตามอำนาจหน้าที่ความรับผิดชอบ หรือตามความจำเป็น ในการใช้งานระบบเท่านั้น

(๓) ผู้ดูแลระบบ สามารถมอบหมายสิทธิการบริหารจัดการบัญชีผู้ใช้งาน ให้ผู้อื่นที่มีส่วนเกี่ยวข้องกับระบบงานดำเนินการแทนได้ โดยต้องได้รับการอนุมัติจากผู้บังคับบัญชา

(๔) บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งานระบบ

(๕) บันทึกและจัดเก็บข้อมูลการเปลี่ยนแปลงบัญชีผู้ใช้งาน การมอบหมายอำนาจ หน้าที่ หรือสิทธิการควบคุมการใช้งานทุกครั้ง

(๖) ทำการทบทวนระดับและสิทธิของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๑.๒.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานโดย

(๑) ผู้ดูแลระบบจัดทำขั้นตอนการปฏิบัติสำหรับการตั้งหรือการเปลี่ยนรหัสผ่านให้ผู้ใช้งานทราบ

(๒) กำหนดรหัสผ่านควรมีความยาวมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการ ผสมผสาน ตัวอักษรระหว่างตัวอักษรตัวปกติตัวพิมพ์ใหญ่ ตัวเลข และ สัญลักษณ์เข้าด้วยกัน)

(๓) ไม่กำหนดรหัสผ่านจากสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย เช่น ชื่อ สกุล เบอร์โทรศัพท์ของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือ จากคำศัพท์ที่ใช้ในพจนานุกรม

(๔) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(๕) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(๖) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันทีหลังจากได้รับรหัสผ่าน

(๗) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยน ให้รหัสผ่านยากต่อการเดา

(๘) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๙) ในกรณีระบบงานได้อนุญาตให้เปลี่ยนรหัสผ่าน ควรเปลี่ยนรหัสผ่านใหม่ทันที สำหรับการเข้าใช้งานครั้งแรก

(๑๐) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งาน และรหัสผ่านปัจจุบันให้ ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๑๑) ถ้ารหัสผ่านถูกเปิดเผยบนระบบต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

(๑๒) ไม่อนุญาตให้เจ้าหน้าที่หรือผู้ใช้งานระบบใช้รหัสผ่านร่วมกัน

๑.๒.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งานโดย

(๑) การทบทวนสิทธิการเข้าใช้งาน ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและ ระเบียบการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(๒) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการ ลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๑.๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

๑.๓.๑ การใช้งานบัญชีผู้ใช้และรหัสผ่าน

(๑) ผู้ใช้งานต้องทำการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมี บัญชีชื่อผู้ใช้ของตนเอง และห้ามทำการเผยแพร่แจกจ่ายหรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

(๒) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๑.๓.๒ การใช้งานรหัสผ่าน

(๑) ไม่กำหนดรหัสผ่านที่มีส่วนหนึ่งมาจากสิ่งที่เกี่ยวข้องตัวผู้ใช้งาน เช่น ชื่อ นามสกุล ชื่อเล่น ชื่อบิดา ชื่อมารดา ชื่อหน่วยงาน หรือคำศัพท์ที่มีใช้ในพจนานุกรม เป็นต้น ต้องประกอบด้วย ตัวอักษรไม่น้อยกว่า ๘ ตัว โดยต้องผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และตัวอักขระพิเศษเข้าด้วยกัน

(๒) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

(๓) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๔) เก็บบัญชีและรหัสผ่านของตนเองไว้เป็นความลับ

๑.๓.๓ การป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งาน

(๑) ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อก หน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

(๒) ผู้ใช้งานต้องล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแล

(๓) ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกันที่กำหนดไว้

๑.๓.๔ การจัดวางและการป้องกันอุปกรณ์

(๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการสูญหายหรือใช้งานโดยไม่ได้รับอนุญาต

(๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

(๓) ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่

๑.๓.๕ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์โดย

(๑) จัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ต้องควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยผู้เป็นเจ้าของ หรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น

(๓) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญ ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญได้

(๔) สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๕) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

(๖) โปรแกรมต่างๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของกรมวิทยาศาสตร์บริการ เป็นโปรแกรมที่กรมวิทยาศาสตร์บริการได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมและนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานเพราะเป็นการกระทำที่ผิดกฎหมาย

(๗) ไม่เก็บข้อมูลสำคัญของกรมวิทยาศาสตร์บริการไว้บนเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลที่เป็นสมบัติส่วนบุคคล

(๘) ต้องลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำการเปลี่ยน หรือทดแทนอุปกรณ์

(๙) ต้องลบหรือฟอร์แมต (Format) ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำลาย หรือเปลี่ยนทดแทน หรือจำหน่ายอุปกรณ์

๑.๓.๖ การป้องกันโปรแกรมไม่ประสงค์ดี

(๑) ผู้ดูแลระบบดำเนินการติดตั้งโปรแกรมคอมพิวเตอร์สำหรับป้องกัน และกำจัดโปรแกรมไม่ประสงค์ดี รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

(๒) ต้องทำการปรับปรุงระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

(๓) ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ ผ่านทางระบบเครือข่าย และผ่านทางสื่อบันทึกข้อมูลทุกชนิด ผู้ใช้งานต้องทำการตรวจสอบ โปรแกรมไม่ประสงค์ดีก่อนการรับส่งทุกครั้ง

๑.๔. การควบคุมการเข้าถึงระบบเครือข่าย

๑.๔.๑ การเข้าใช้งานระบบเครือข่ายของกรมวิทยาศาสตร์บริการ

(๑) การเข้าใช้งานระบบเครือข่าย จะต้องพิสูจน์ตัวตนผู้ใช้งานด้วยบัญชีผู้ใช้ที่กลุ่มเทคโนโลยีสารสนเทศออกให้

(๒) ผู้ใช้งานที่ได้รับอนุญาตให้เข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบเครือข่ายตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

(๓) การเข้าใช้เครือข่ายของบุคคลที่ไม่มีบัญชีผู้ใช้ของกรมวิทยาศาสตร์บริการ ต้องขออนุญาตใช้บัญชีชั่วคราวจากกลุ่มเทคโนโลยีสารสนเทศ ซึ่งจะเข้าถึงได้ตามสิทธิ์ที่ได้รับอนุญาตและจะต้องพิสูจน์ตัวตนด้วยบัญชีชั่วคราวนั้น

(๔) ต้องลงทะเบียนอุปกรณ์กระจายสัญญาณ (access point) ทุกตัวที่นำมาใช้ในระบบเครือข่ายไว้สาย

(๕) ต้องเปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถคาดเดาหรือเจาะรหัสผ่านได้โดยง่าย

(๖) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่าย อย่างสม่ำเสมอ เพื่อยกยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่าย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบโดยทันที

๑.๔.๒ การควบคุมการเชื่อมต่อทางเครือข่าย

(๑) ผู้ดูแลระบบต้องควบคุม พอร์ตและหมายเลขไอพีแอดเดรส รหัสผ่าน ของอุปกรณ์ระบบเครือข่ายสำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่าย ให้กับผู้ที่ได้รับอนุญาตเท่านั้น

(๒) ผู้ดูแลระบบต้องกำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

(๓) ไม่อนุญาตให้เชื่อมต่อกับอุปกรณ์เครือข่ายโดยตรง จากเครือข่ายภายนอกกรมวิทยาศาสตร์บริการ ให้เชื่อมต่อผ่านช่องทางที่ปลอดภัยที่กรมวิทยาศาสตร์บริการกำหนด เช่น VPN เป็นต้น

(๔) ต้องปิดพอร์ต หรือปิดบริการ บนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๕) ผู้ดูแลระบบต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งาน ทุก ๓ เดือน

๑.๕. การใช้งานอินเทอร์เน็ต

๑.๕.๑ ห้ามใช้อินเทอร์เน็ตของกรมวิทยาศาสตร์บริการเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล

๑.๕.๒ ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลนี้อาจก่อความเสียหายให้กับกรมวิทยาศาสตร์บริการ เป็นต้น

๑.๕.๓ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๑.๕.๔ ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน

๑.๖. การใช้งานเครือข่ายสังคมออนไลน์

๑.๖.๑ การใช้งานหรือใช้บริการเว็บไซต์เครือข่ายสังคมออนไลน์ ต้องใช้งานเพื่อประโยชน์ของทางราชการเป็นสำคัญ

๑.๖.๒ การใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความยั่ว ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรมวิทยาศาสตร์บริการ

๑.๖.๓ หากผู้ใช้งานทราบว่าการใช้งานเครือข่ายสังคมออนไลน์ของท่านอาจมีผลกระทบกับกรมวิทยาศาสตร์บริการ ผู้ใช้งานต้องแจ้งกลุ่มเทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑.๗. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์

๑.๗.๑ ผู้ใช้งานต้องไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่านหรือรับ-ส่งข้อความ

๑.๗.๒ ผู้ใช้งานมีหน้าที่จะต้องรักษาบัญชีผู้ใช้ และรหัสผ่านเป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้องเพื่อป้องกันการใช้งานโดยผู้ไม่ประสงค์ดี

๑.๗.๓ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ของตน

๑.๗.๔ ก่อนส่งต่อ เปิดไฟล์ หรือคลิกลิงก์ที่แนบมา ต้องตรวจสอบให้แน่ใจก่อนว่าไม่ใช่จดหมายหลอกลวง

๑.๗.๕ ต้องไม่ส่งข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัสผ่าน บัญชีผู้ใช้ หมายเลขบัตรประชาชน หมายเลขบัตรเครดิต ฯลฯ ผ่านจดหมายอิเล็กทรอนิกส์

๑.๘. การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ใช้งานร่วมกัน

๑.๘.๑ ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตนเอง

๑.๘.๒ ต้องตั้งค่าระบบให้สามารถยุติการยืนยันตัวตนเมื่อพบว่ามีคามพยายามคาดเดารหัสผ่าน

๑.๘.๓ ระบบจะต้องจำกัดสิทธิผู้ใช้งานในการติดตั้ง เปลี่ยนแปลง ลบโปรแกรมหรือข้อมูลบนเครื่องคอมพิวเตอร์

๑.๙. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ

๑.๙.๑ การจำกัดการเข้าถึงสารสนเทศ

(๑) การจำกัดการเข้าถึงของผู้ใช้งาน

(ก) เข้าได้ตามสิทธิที่ได้รับอนุญาตเท่านั้น

(ข) กำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคล

(ค) ต้องออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

(๒) แบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศของกรมวิทยาศาสตร์บริการ ออกเป็น ๓ กลุ่ม คือ ผู้ดูแลระบบ ผู้พัฒนาระบบงาน และผู้ใช้งานระบบ โดยกำหนดหน้าที่รับผิดชอบอย่างชัดเจนเป็นลายลักษณ์อักษร

๑.๙.๒ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๑) แนวปฏิบัติสำหรับการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ทั้งของส่วนตัวและอุปกรณ์ของทางราชการ

(ก) ต้องล็อกหรือยึดเครื่องให้อยู่กับที่กรณีที่น่าเครื่องไปใช้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(ข) ต้องเปิดใช้ระบบล็อกหน้าจออัตโนมัติหรือปิดเครื่องอัตโนมัติเมื่อไม่ได้ใช้งาน และในกรณีที่ไม่ได้ใช้งานเป็นการชั่วคราวต้องล็อกหน้าจอทุกครั้ง

(ค) ผู้ใช้ต้องตั้งรหัสผ่านเพื่อเข้าใช้งานคอมพิวเตอร์แบบพกพา

(ง) ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนการใช้งานสื่อบันทึกข้อมูลพกพาต่าง ๆ

(จ) ต้องจัดการกับโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น ติดตั้งโปรแกรมป้องกันมัลแวร์ ปรับปรุงระบบปฏิบัติการให้ทันสมัย ไม่ติดตั้งซอฟต์แวร์ผิดกฎหมาย ไม่ติดตั้งซอฟต์แวร์ที่ไม่รู้จัก ฯลฯ

(๒) การสำรองข้อมูลและการกู้คืน

ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูล (backup media) เช่น ดีวีดี ฮาร์ดดิสก์ภายนอก (External hard disks) เป็นต้น

๑.๙.๓ การปฏิบัติงานจากภายนอกกรมวิทยาศาสตร์บริการ

(๑) ผู้ใช้งานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

(๒) ผู้ใช้งานต้องตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศ ของกรมวิทยาศาสตร์บริการ จากระยะไกลมีระบบป้องกันไวรัสและการใช้งานไฟร์วอลล์อย่างเหมาะสม

๑.๙.๔ การใช้งานโปรแกรมอรรถประโยชน์

(๑) โปรแกรมที่ติดตั้ง ต้องเป็นโปรแกรมที่กรมวิทยาศาสตร์บริการได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย หรือเป็นโปรแกรมที่ผู้พัฒนาแจกจ่ายให้ฟรี

(๒) ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ แล้วนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๑.๙.๕ การหมดเวลาใช้งานระบบสารสนเทศ

(๑) ให้ยุติการใช้งานระบบสารสนเทศโดยอัตโนมัติเมื่อไม่มีการใช้งานเป็นเวลานาน ๓๐ นาที หรือตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๑.๑๐. การควบคุมการเข้าถึงระบบปฏิบัติการ

๑.๑๐.๑ ผู้ดูแลระบบ

(๑) ต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของกรมวิทยาศาสตร์บริการ

๑.๑๐.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน

(๑) ผู้ใช้งานต้องมีบัญชีผู้ใช้ และรหัสผ่าน สำหรับเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของกรมวิทยาศาสตร์บริการ

๑.๑๐.๓ การบริหารจัดการรหัสผ่าน

(๑) จำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้ง ที่กำหนดระบบจะทำการล็อกสิทธิการเข้าถึงของผู้ใช้งาน

(๒) ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

๑.๑๑. การบริหารจัดการคอมพิวเตอร์แม่ข่าย

๑.๑๑.๑ กำหนดผู้ดูแลระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องอย่างเป็นลายลักษณ์อักษร

๑.๑๑.๒ มีขั้นตอน/กระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าที่ผิดปกติ จะต้องดำเนินการแก้ไขและบันทึกรายงานการแก้ไขโดยทันที

๑.๑๑.๓ ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงมาตรฐาน ที่กรมวิทยาศาสตร์บริการใช้อ้างอิง

๑.๑๑.๔ ต้องปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่ออุดช่องโหว่ต่างๆ

๑.๑๑.๕ การติดตั้งและการเชื่อมต่อนระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบของกรมวิทยาศาสตร์บริการ

๑.๑๒. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๑.๑๒.๑ ต้องแต่งตั้งผู้มีสิทธิ และกำหนดจำนวนผู้มีสิทธิในการเข้าถึงระบบปฏิบัติการ

๑.๑๒.๒ ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตัวเอง

๑.๑๒.๓ ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีภัยคุกคามเดา รหัสผ่านจากเครื่องปลายทาง

๑.๑๒.๔ ผู้ดูแลระบบต้องยุติการให้บริการทันที ในกรณีตรวจพบว่ามีใช้งานที่ผิดปกติ หรือไม่ปลอดภัย

๑.๑๒.๕ ภายหลังการใช้งานเครื่องแม่ข่ายเสร็จสิ้น จะต้องทำการ log off ทุกครั้ง

๑.๑๒.๖ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องที่ต้องการให้เข้าถึงได้จากอินเทอร์เน็ตจะต้องลงทะเบียนกับ กลุ่มเทคโนโลยีสารสนเทศ

๑.๑๓. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์

๑.๑๓.๑ จัดให้มี Centralized Log server สำหรับรวบรวมข้อมูลจราจรคอมพิวเตอร์ของกรมวิทยาศาสตร์ บริการ

๑.๑๓.๒ กำหนดวิธีการในการนำส่งข้อมูลจราจรคอมพิวเตอร์จากอุปกรณ์ ในระบบเครือข่าย ไปเก็บไว้ใน Centralized Log Server เพื่อประโยชน์ในการใช้ตรวจสอบและเก็บบันทึกดังกล่าวไว้ตามที่กำหนดใน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๑.๑๓.๓ ตรวจสอบการบันทึกข้อมูลจราจรคอมพิวเตอร์อย่างน้อยสัปดาห์ละ ๑ ครั้ง

๑.๑๓.๔ กำหนดวิธีการป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลาย ข้อมูลจราจรคอมพิวเตอร์ต่างๆ และ จำกัดสิทธิการเข้าถึงข้อมูลจราจรคอมพิวเตอร์เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑.๑๔. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ

๑.๑๔.๑ ผู้ดูแลระบบ แบ่งออกเป็น ๓ กลุ่ม

(๑) ผู้ดูแลระบบเครือข่าย

(๒) ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย

(๓) ผู้ดูแลระบบสารสนเทศ

๑.๑๔.๒ ผู้ดูแลระบบเครือข่าย มีหน้าที่และความรับผิดชอบดังนี้

(๑) ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่าย และช่องทางการสื่อสารของระบบเครือข่ายและปิด ช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งาน

(๒) เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งานนับตั้งแต่ เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นระยะเวลาตามที่กฎหมายกำหนดนับตั้งแต่การให้บริการสิ้นสุดลง และการ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(ก) มีระบบรักษาความปลอดภัย ครอบคลุม ถูกต้อง และความน่าเชื่อถือของข้อมูล โดยไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ได้

(ข) ข้อมูลจราจรทางคอมพิวเตอร์ต้องระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

(ค) ข้อมูลจราจรทางคอมพิวเตอร์ต้องบันทึกอ้างอิงเวลากับ ntp.dss.local

๑.๑๔.๓ ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่และความรับผิดชอบดังนี้

(๑) ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของกรมวิทยาศาสตร์บริการ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงาน ให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานทันที

(๒) ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่ายให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

(๓) ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

(๔) ติดตั้งซอฟต์แวร์เพื่อป้องกันไวรัสบนเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง

(๕) ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๑.๑๔.๔ ผู้ดูแลระบบสารสนเทศ มีหน้าที่และความรับผิดชอบดังนี้

(๑) ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

(๒) ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้นให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

๑.๑๔.๕ หลักธรรมาภิบาลของผู้ดูแลระบบ

(๑) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งาน ยกเว้นเป็นการปฏิบัติหน้าที่ตามกฎหมายหรือระเบียบของทางราชการ

(๒) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ ยกเว้นเป็นการปฏิบัติหน้าที่ตามกฎหมายหรือระเบียบของทางราชการ

(๓) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ ยกเว้นเป็นการปฏิบัติหน้าที่ตามกฎหมายหรือระเบียบของทางราชการ

๑.๑๕. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑.๑๕.๑ การจัดการบริเวณแวดล้อมทางกายภาพ

(๑) กำหนดพื้นที่ควบคุมในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย

(๒) กำหนดระบบป้องกันการบุกรุกสำหรับพื้นที่ควบคุมในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย

(๓) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพอย่างสม่ำเสมอ เพื่อตรวจสอบว่า ยังใช้งานได้ตามปกติ

๑.๑๕.๒ การควบคุมการเข้า-ออกพื้นที่ทางกายภาพ

(๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่ควบคุม

(๒) มีกลไกการอนุญาตการเข้าถึงพื้นที่ควบคุม สำหรับบุคคลภายนอก/บุคคลภายใน ที่ไม่ใช่เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศ

(๓) ต้องบันทึกวันและเวลาเข้า-ออก พื้นที่ควบคุม

(๔) ต้องบันทึกรายการอุปกรณ์ที่นำเข้า-ออก พื้นที่ควบคุม

(๕) ต้องดูแลและควบคุมการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่ควบคุม จนกว่าจะแล้วเสร็จ

๑.๑๕.๓ การนำทรัพย์สินของกรมวิทยาศาสตร์บริการออกนอกสำนักงาน

(๑) ผู้ประสงค์นำทรัพย์สินออก ต้องขออนุญาตผู้มีอำนาจตามระเบียบของทางราชการ ก่อนนำทรัพย์สินออกนอก กรมวิทยาศาสตร์บริการ

(๒) เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ บันทึกข้อมูลการนำทรัพย์สินออกนอกกรมวิทยาศาสตร์บริการ เพื่อใช้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำทรัพย์สินส่งคืน

๑.๑๕.๔ ระบบและอุปกรณ์สนับสนุนการทำงาน

(๑) ต้องสนับสนุนการทำงานของระบบสารสนเทศและการสื่อสารของกรมวิทยาศาสตร์บริการที่เพียงพอต่อความต้องการใช้งาน โดยให้มี

(ก) ระบบสำรองกระแสไฟฟ้า

(ข) ระบบระบายอากาศ

(ค) ระบบปรับอากาศและควบคุมความชื้น

(ง) ระบบป้องกันอัคคีภัย

(๒) ต้องตรวจสอบหรือทดสอบระบบสนับสนุนดังกล่าวเป็นประจำทุกวันทำการ เพื่อให้มั่นใจได้ว่าระบบทำงานปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

ส่วนที่ ๒

นโยบายการจัดทำระบบสำรองสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของกรมวิทยาศาสตร์บริการมีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง
๒. เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่าย ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและผู้ดูแลระบบสารสนเทศหน่วยงานถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหา ต้องสำรองข้อมูลและสามารถกู้คืนข้อมูลได้ในกรณีที่จำเป็น

ผู้รับผิดชอบ

๑. กลุ่มเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

๒.๑. ระบบสำรอง

- ๒.๑.๑ จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรอง และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง
- ๒.๑.๒ ระบบสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม ดังนี้
 - (๑) มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง
 - (๒) มีระบบไฟฟ้าสำรอง
 - (๓) มีระบบปรับอากาศและความชื้น
 - (๔) มีระบบป้องกันอัคคีภัย
 - (๕) มีระบบส่องสว่าง
 - (๖) มีระบบสื่อสารหรือระบบเครือข่ายสำรอง
- ๒.๑.๓ มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

๒.๒. การสำรองข้อมูล

- ๒.๒.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการสำรองข้อมูล และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง
- ๒.๒.๒ กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ ตามคู่มือปฏิบัติงานการสำรองข้อมูลเครื่องแม่ข่าย (M-CD0-007)

๒.๒.๓ กำหนดความถี่ในการสำรองข้อมูลของระบบที่มีการเปลี่ยนแปลงบ่อยอย่างน้อย ๓ ครั้งต่อวัน

๒.๒.๔ เก็บข้อมูลที่สำรองไว้ไม่น้อยกว่า ๙๐ วัน

๒.๒.๕ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานะการทำงานสำเร็จ/ไม่สำเร็จ ตาม M-CD0-007

๒.๒.๖ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆ เป็นต้น

๒.๒.๗ มีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

(๑) ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๒.๓. การกู้คืนข้อมูล

๒.๓.๑ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล

๒.๓.๒ ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างน้อยเดือนละ ๑ ครั้ง

๒.๓.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

๒.๓.๔ ทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓

นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายได้รับทราบถึงหน้าที่ ความรับผิดชอบ และความจำเป็นในการประเมินความเสี่ยงสารสนเทศ เพื่อหาแนวทางป้องกันภัยคุกคามและการโจมตีต่างๆ ซึ่งทำให้ระบบสารสนเทศของกรมวิทยาศาสตร์บริการหรือของหน่วยงานมีความปลอดภัยและมีความพร้อมใช้งานอยู่เสมอ

ผู้รับผิดชอบ

๑. กลุ่มเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. หน่วยตรวจสอบภายใน

แนวปฏิบัติ

๓.๑. กลุ่มเทคโนโลยีสารสนเทศต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศของกรมวิทยาศาสตร์บริการ อย่างน้อยปีละ ๑ ครั้ง

๓.๒. ระบุความเสี่ยงและผลกระทบของความเสี่ยง เพื่อการประเมินความเสี่ยง ดังต่อไปนี้

๓.๒.๑ ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบเครือข่าย

๓.๒.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่าย โดยไม่ได้รับอนุญาต

๓.๒.๓ ความเสี่ยงที่เกิดจากระบบสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๓.๒.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้าระบบสารสนเทศของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด

๓.๒.๕ ความเสี่ยงที่เกิดจากการลักลอบใช้บัญชีผู้ใช้และรหัสผ่านของผู้อื่นโดยไม่ได้รับอนุญาต

๓.๒.๖ ความเสี่ยงที่เกิดจากความเสียหายทางกายภาพ เช่น ไฟไหม้ น้ำท่วม อุปกรณ์สูญหาย เป็นต้น

๓.๓. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๓.๔. การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

๓.๔.๑ ระดับความน่าจะเป็นที่จะเกิดความเสี่ยงที่ระบุ

๓.๔.๒ ระดับความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๓.๔.๓ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ

๓.๕. ต้องแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบ และประเมินผลงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๔

นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและผู้เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ผู้รับผิดชอบ

๑. กลุ่มเทคโนโลยีสารสนเทศ
๒. เจ้าหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

- ๔.๑. กลุ่มเทคโนโลยีสารสนเทศต้องกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เข้ากับแผนการพัฒนามูลฐานของกรมวิทยาศาสตร์บริการ
- ๔.๒. ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจาก การใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์
- ๔.๓. จัดฝึกอบรมการใช้งานระบบสารสนเทศของกรมวิทยาศาสตร์บริการ ทุกครั้งที่มีการปรับปรุงหรือเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ
- ๔.๔. จัดทำคู่มือการใช้งานระบบสารสนเทศ และเผยแพร่ทางเว็บไซต์ของกรมวิทยาศาสตร์บริการ
- ๔.๕. ให้ความรู้เกี่ยวกับแนวปฏิบัติ หรือข้อควรระวังที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่าย เช่น การติดประกาศ ประชาสัมพันธ์ เผยแพร่ผ่านเว็บไซต์ อีเมล ฯลฯ