ประกาศสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. 2562

โดยที่มาตรา 5 มาตรา 7 และมาตรา 8 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ซึ่งออกโดยอาศัยอำนาจตามความในมาตรา 35 วรรคหนึ่งแห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

อาศัยอำนาจและหน้าที่ตามความในมาตรา 28 และมาตรา 29 แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน) พ.ศ. 2543 จึงกำหนดประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ดังนั้น สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน) จึงออกประกาศดังนี้

ข้อ 1 ประกาศนี้เรียกว่า "ประกาศสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน) เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2562"

ข้อ 2 ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ 3 ในประกาศนี้

(1) "ผู้ใช้งาน" หมายความว่า เจ้าหน้าที่ หรือลูกจ้างของสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ ผู้รับจ้างทำของและพนักงานหรือลูกจ้างที่รับทำการงานให้กับสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ และผู้ใช้บริการที่ใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ

(2) "สิทธิผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์

(3) "บัญชีผู้ใช้งาน" หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ

(4) "สินทรัพย์" หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับหน่วยงาน

(5) "ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษาหรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(6) "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาตการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้ง การอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(7) "ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วนและสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิดและความน่าเชื่อถือ

(8) “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า การเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(9) “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

(10) “นโยบาย” หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(11) “ผู้บริหาร” หมายความว่า ผู้อำนวยการ รองผู้อำนวยการ ผู้ช่วยผู้อำนวยการ ผู้อำนวยการสำนักหรือผู้ที่ผู้อำนวยการ สทอภ. ได้มอบหมาย

(12) “ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” หมายความว่า เจ้าหน้าที่ที่ผู้อำนวยการมอบหมายให้ดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

(13) “ผู้อำนวยการ" หมายความว่า ผู้อำนวยการสำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ

(14) “สำนักงาน” หมายความว่า สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน)

หมวด 1

นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อ 4 นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

4.1 ส่วนที่ว่าด้วยการบริหารจัดการนโยบาย

(1) คณะทำงานสนับสนุนผู้บริหารเทคโนโลยีสารสนเทศระดับสูงและเจ้าหน้าที่ของสำนักงานที่ปฏิบัติการด้านคอมพิวเตอร์ ร่วมกันในการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้มีหน้าที่ในการทบทวน ปรับปรุง แนวนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ โดยในการดำเนินการให้รับฟังความคิดเห็นของผู้ใช้งานประกอบด้วย ทั้งนี้ เมื่อดำเนินการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เสนอผู้อำนวยการ เพื่อพิจารณาอนุมัติและบังคับใช้ประกาศต่อไป

(2) นโยบายให้จัดทำเป็นลายลักษณ์อักษรและประกาศให้บุคลากรและผู้เกี่ยวข้องทั้งหมดทราบให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามแนวนโยบายและแนวปฏิบัติได้

(3) กำหนดผู้รับผิดชอบตามแนวนโยบายและแนวปฏิบัติอย่างชัดเจน

(4) ทบทวนและปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่าสม่ำเสมออย่างน้อยทุก 2 ปี

4.2 ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(1) การเข้าถึงและควบคุมการใช้งานสารสนเทศสำนักงานมีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ประชาชนสามารถเข้าถึงและใช้งานเทคโนโลยีสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งให้ความคุ้มครองข้อมูลของประชาชนที่ไม่พึงเปิดเผย ทั้งนี้ ภายใต้บทบัญญัติของกฎหมายและครอบคลุม 4 ด้าน ดังนี้

(1.1) การเข้าถึงระบบสารสนเทศ เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เฉพาะผู้ที่รับอนุญาตและป้องกันการเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผล

(1.2) การเข้าถึงระบบเครือข่าย เพื่อป้องกันการเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต

(1.3) การเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

(1.4) การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศโดยต้องมีการควบคุมและการจำกัดการเข้าถึงของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนเข้าใช้งานฟังชั่นต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น

(2) การรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ สำนักงานมีนโยบายที่จะรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยมีระบบการควบคุมเทคโนโลยีในการจัดทำเอกสารอิเล็กทรอนิกส์ โครงสร้างพื้นฐานกุญแจสาธารณะและหน่วยงานบริการพื้นฐานต่างๆ ระบบเทคโนโลยีสารสนเทศ การบริหารจัดการข้อมูลและเอกสารอิเล็กทรอนิกส์และการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ที่มีมาตรฐานในการรักษาความมั่นคงปลอดภัยเป็นที่ยอมรับ

(3) การจัดระบบเทคโนโลยีสารสนเทศ ระบบสำรองเทคโนโลยีสารสนเทศ และระบบคอมพิวเตอร์รวมทั้งแผนใช้งานเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ในกรณีฉุกเฉิน สำนักงานมีนโยบายในการบริหารจัดการเทคโนโลยีสารสนเทศที่ได้มาตรฐาน โดยมีระบบการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งต้องมีแผนฉุกเฉินในการใช้งานเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์เพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(4) การตรวจสอบ การประเมินความเสี่ยงและมาตรการในการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานมีนโยบายให้มีการตรวจสอบประเมินความเสี่ยงและกำหนดมาตรการในการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบอิสระหรือสำนักตรวจสอบภายในอย่างน้อยปีละ 1 ครั้ง

(5) การสร้างความรู้ความเข้าใจในการใช้งานระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งาน สำนักงานมีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรมและเผยแพร่การใช้งานระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

หมวด 2

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ข้อ 5 ในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้ดำเนินการตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

5.1 การควบคุมการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

5.1.1 การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ของเจ้าหน้าของสำนักงานที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งาน เพื่อให้เกิดความชัดเจนในการปฏิบัติงานของบุคลากรภายในและเป็นการยืนยันตัวบุคคล ซึ่งเป็นการลดความเสี่ยงในการเข้าถึงและใช้งานระบบสารสนเทศ

(1) การแบ่งแยกอำนาจหน้าที่ของบุคลากรในส่วนของงานคอมพิวเตอร์

(1.1) แบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนของการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารระบบ (System Administrator) ที่ปฏิบัติงานอยู่ในส่วนคอมพิวเตอร์

(1.2) กำหนดหน้าที่รับผิดชอบของงานในแต่ละหน้าที่ที่ปฏิบัติงานอยู่ในส่วนคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร

(1.3) กำหนดบุคลากรสำรองในงานที่สำคัญเพื่อทำงานทดแทนในกรณีจำเป็น

(2) การกำหนดคุณสมบัติ สิทธิในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ

(2.1) กำหนดระดับชั้น ประเภทของข้อมูล ลำดับความสำคัญ เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงการใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน

(2.2) กำหนดหน่วยงานควบคุมการให้สิทธิการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ ให้สอดคล้องกับอำนาจหน้าที่และความจำเป็นของผู้ใช้งานอย่างเคร่งครัด

(2.3) ตรวจสอบคุณสมบัติและอำนาจหน้าที่ของผู้ใช้งานอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องยกเลิกหรือเปลี่ยนแปลงสิทธิให้สอดคล้องกับระดับชั้นการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศทันที

5.1.2 การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์และการเข้าออกศูนย์คอมพิวเตอร์ เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงล่วงรู้ (AccessRisk) แก้ไขเปลี่ยนแปลง (Integrity Risk) หรือก่อให้เกิดความเสียหาย (Availability Risk) ต่อระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์และป้องกันความเสียหายจากสภาพแวดล้อมหรือภัยพิบัติต่างๆ รวมทั้งเพื่อให้การใช้งานระบบคอมพิวเตอร์เป็นไปอย่างถูกต้องและมีประสิทธิภาพ

(1) การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์

(1.1) ควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ โดยกำหนดขั้นตอนและวิธีปฏิบัติในการปฏิบัติงานด้านต่างๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้เจ้าหน้าที่ใช้ปฏิบัติงาน กำหนดขั้นตอนการเปิด - ปิดระบบ การประมวลผล การตรวจสอบประสิทธิภาพ การทำงานของระบบและตารางเวลาของการปฏิบัติงาน กำหนดให้ปฏิบัติงานผ่านเมนูและจำกัดการปฏิบัติงานโดยใช้ Command Line เท่าที่จำเป็น กำหนดให้มีการบันทึก (Log Book) รายละเอียดเกี่ยวกับผู้ปฏิบัติงาน เวลาปฏิบัติงาน ปัญหาที่เกิดขึ้นและการแก้ไขสถานะของระบบ และผู้ตรวจทานการปฏิบัติงาน

(1.2) ติดตามการทำงานของระบบคอมพิวเตอร์ (Monitoring) โดยตรวจสอบและติดตามประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ที่สำคัญให้ทำงานได้อย่างต่อเนื่อง และมีประสิทธิภาพการรับส่งข้อมูล การเชื่อมต่อระหว่างสำนักงานต่างจังหวัด การใช้งาน Hard Disk และการใช้งานหน่วยประมวลผล (CPU)

(1.3) มีการจัดการปัญหาและการจัดทำรายงาน โดยกำหนดให้มีผู้รับผิดชอบในการแก้ไขปัญหา มีระบบบันทึกรวบรวมปัญหาและเหตุการณ์ผิดปกติเพื่อศึกษาหาแนวทางป้องกันและแก้ไขมีการจัดทำทะเบียนควบคุมการพิมพ์ การแก้ไขและการจัดส่งรายงาน

(2) การควบคุมการเข้าออกศูนย์คอมพิวเตอร์

(2.1) จัดศูนย์คอมพิวเตอร์ให้เป็นสัดส่วน โดยแบ่งเป็นส่วนระบบเครือข่าย (Network Zone) และส่วนเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง (Server Zone) เพื่อสะดวกในการปฏิบัติงานและควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์

(2.2) จัดเก็บสินทรัพย์ที่สำคัญไว้ในพื้นที่หวงห้ามของศูนย์คอมพิวเตอร์และกำหนดสิทธิให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเข้าออกศูนย์คอมพิวเตอร์

(2.3) ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ จะต้องมีเจ้าหน้าที่ศูนย์คอมพิวเตอร์ควบคุมดูแลการทำงานของบุคคลดังกล่าวตลอดเวลา

(2.4) บันทึกการเข้าออกศูนย์คอมพิวเตอร์ โดยมีรายละเอียดเกี่ยวกับตัวบุคคล และเวลาที่ผ่านเข้าออก

5.1.3 ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) แบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ

(1) การควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(2) การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

5.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เฉพาะผู้ที่ได้รับอนุญาตแล้ว โดยสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

(1) มีการลงทะเบียนผู้ใช้งาน (User Registration) ด้วยการจัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบเทคโนโลยีสารสนเทศ โดยต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อนและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(2) ต้องทำการตรวจสอบรายชื่อผู้ใช้งานของระบบงานที่สำคัญอย่างสม่ำเสมอ และดำเนินการระงับการใช้งานโดยทันทีเมื่อตรวจพบว่าผู้ใช้งานไม่มีสิทธิเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศหรือไม่มีการใช้ระบบงานเป็นระยะเวลาหกเดือน

(3) การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (User Privilege) โดยกำหนดระดับชั้นของสิทธิที่จะให้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ ควบคุมการให้สิทธิแก่ผู้ใช้งานทั้งภายในและภายนอก โดยการให้สิทธิผู้ใช้งานภายในที่สามารถเข้าถึง เปลี่ยนแปลง แก้ไขเทคโนโลยีสารสนเทศต้องควบคุมอย่างเคร่งครัดและได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร ให้มีการตรวจสอบทบทวนอำนาจหน้าที่ของผู้ใช้งานภายในอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องยกเลิกหรือเปลี่ยนแปลงสิทธิให้สอดคล้องกับอำนาจหน้าที่ของผู้ใช้งานนั้นทันที

(4) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุมและสามารถทำงานเชิงโต้ตอบ (Interactive) หรือทำงานในลักษณะอัตโนมัติเพื่อเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพโดยผู้ดูแลระบบ (Admin) เป็นผู้กำหนดรหัสผ่านเริ่มแรกสำหรับผู้ใช้งาน (Password) ที่ใช้สำหรับเข้าสู่ระบบ รหัสผ่านที่ถูกกำหนดต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษรมีการผสมกันระหว่างตัวอักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่และตัวเลขเข้าด้วยกันผู้ใช้งานเปลี่ยนรหัสผ่าน (Password) ทุก 6 เดือน ผู้ดูแลระบบ (Admin) จะแจ้งให้ผู้ใช้งานที่ได้รับอนุญาตทราบและต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

(5) ทบทวนสิทธิการเข้าถึงของผู้ใช้งานทุกๆ 1 ปี หรือเมื่อเกิดการเปลี่ยนแปลงสิทธิของผู้ใช้งาน การลาออก การโยกย้ายหน่วย อีกทั้งการทบทวนสิทธิ ต้องพิจารณาถึงพฤติกรรมการทำงานของผู้ใช้งาน รวมทั้งถ้ามีการเปลี่ยนแปลงระบบงานใหม่ จะต้องมีการทบทวนสิทธิการใช้งานทุกครั้งอีกด้วย

5.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

(1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้ง ห้ามทำการเผยแพร่

แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน กำหนดรหัสผ่านที่มีคุณภาพให้ยากแก่การคาดเดา โดยต้องเปลี่ยนรหัสผ่านไม่เกิน 6 เดือนหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

(2) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของสำนักงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

(3) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and Clear screen policy) ต้องควบคุมป้องกันสินทรัพย์คอมพิวเตอร์ ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ คอมพิวเตอร์ หรือสารสนเทศไม่ให้อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ กำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน และผู้ใช้งานต้องป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิเข้าถึง อุปกรณ์ต้องทำการล็อกหน้าจอและออกจากระบบโปรแกรมประยุกต์ทุกครั้ง รวมทั้งเครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย 30 นาที รวมทั้งต้องทำลายข้อมูลและสื่อบันทึกข้อมูลเพื่อป้องกันการนำกลับมาใช้ใหม่

(4) การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

5.4 การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(1) การใช้งานบริการเครือข่าย ต้องจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(2) การเข้าสู่ระบบเครือข่ายภายในสำนักงาน โดยผ่านทางระบบอินเตอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งานและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

(3) การระบุอุปกรณ์บนเครือข่าย โดยใช้ MAC Address เพื่อทำการยืนยันการติดต่อสื่อสารผ่านระบบเครือข่ายของสำนักงานจากสถานที่ที่กำหนดโดยเฉพาะ ซึ่ง MAC Address ที่กำหนดเท่านั้น จะสามารถเข้าถึงระบบเครือข่ายของสำนักงานได้

(4) ไม่อนุญาตในการตรวจสอบและปรับแต่งอุปกรณ์ในระบบเครือข่ายจากระยะไกลภายนอกสถานที่ของสำนักงาน โดยพอร์ตหรือเซอร์วิสที่ไม่ถูกใช้งานจะต้องถูกปิดเพื่อให้ระบบเครือข่ายมีความปลอดภัย

(5) การบริหารจัดการระบบเครือข่าย (Network) โดยแบ่งแยกระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศ จัดทำระบบป้องกันการบุกรุกระหว่างเครือข่าย ระบบตรวจสอบ การบุกรุกและการใช้งานที่ผิดปกติผ่านระบบเครือข่าย จัดทำแผนผัง (Network Diagram) และขอบเขตของระบบเครือข่าย การเชื่อมต่อเครือข่ายต้องได้รับอนุมัติจากผู้บังคับบัญชา และตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนการเชื่อมต่อ มีผู้รับผิดชอบในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ของระบบเครือข่ายและอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายและทบทวนการกำหนดค่า Parameter อย่างน้อยปีละ 1 ครั้ง ให้มีการติดตั้ง Software ที่ถูกต้องตามลิขสิทธิ์ที่จำเป็นต่อการใช้งาน ติดตั้ง Software ป้องกันไวรัส และควบคุมไม่ให้ผู้ใช้งานระงับการใช้ Software ป้องกันไวรัสที่ติดตั้งไว้

(6) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ในการควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ต้องเชื่อมต่อผ่าน Firewall หรือ Hardware อื่น ที่มีคุณสมบัติป้องกันการบุกรุกหรือป้องกันการทำ Packet Filtering โดยผ่านระบบเครือข่ายสายเช่าระบบเครือข่ายเสมือนส่วนตัว (VPN) มีความปลอดภัยสูง

(7) การติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสำนักงานในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายของการใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(8) การจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน ผู้ดูแลระบบเครือข่ายต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network routingtable) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณข้อมูล (Switch layer3) เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

5.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(1) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ผู้ใช้งานต้องระบุรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

(2) การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นทางเทคนิคที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(3) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้ง ห้ามทำการเผยแพร่แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

(4) กำหนดรหัสผ่านให้ยากแก่การคาดเดา โดยการกำหนดรหัสผ่านต้องมีการแจ้งเตือนผู้ใช้ที่กำหนดรหัสผ่านที่ง่ายต่อการคาดเดาโดยต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร มีการผสมกันระหว่างตัวอักษรตัวพิมพ์เล็กตัวพิมพ์ใหญ่ และตัวเลขเข้าด้วยกัน (กรณีระบบรองรับ) เพื่อให้ผู้ใช้สามารถกำหนดรหัสผ่านที่มีคุณภาพได้อย่างถูกต้อง

(5) ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (System Utilities) เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยและห้ามมิให้ละเมิดลิขสิทธิ์โปรแกรม

(6) เมื่อว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out) ต้องจำกัดระยะเวลาเชื่อมต่อระบบสารสนเทศ ไม่เกิน 15 นาทีหลังจากที่ไม่มีกิจกรรมการใช้งาน โดยทำการล้างหน้าจอเพื่อให้มิให้ผู้อื่นใช้งานหรือเห็นข้อมูลสำคัญของระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

(7) ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง มีระยะเวลาสิ้นสุดการเชื่อมต่อไม่เกิน 180 นาที

5.6 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

(1) จำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้และกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(2) กำหนดมาตรการควบคุม Outsource กรณีมีการจ้างเหมาดำเนินการพัฒนาบำรุงรักษาระบบสารสนเทศและระบบเครือข่าย เพื่อจำกัดสิทธิใช้งานโปรแกรมประยุกต์และสารสนเทศต่างๆ ตามความจำเป็นและหน้าที่ที่รับผิดชอบเท่านั้น

(3) ระบบสารสนเทศซึ่งมีผลกระทบและความสำคัญสูงต่อสำนักงาน ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอก (Mobile computing and Teleworking)

(4) ไม่อนุญาตให้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่เชื่อมต่อเพื่อเข้าถึงโปรแกรมประยุกต์และสารสนเทศที่มีความสำคัญสูง ภายในเครือข่ายคอมพิวเตอร์ของสำนักงานหรือจากภายนอกโดยเด็ดขาด

(5) การปฏิบัติงานจากภายนอกสำนักงาน ต้องเชื่อมต่อผ่านเครือข่ายของสำนักงานหรือผ่านเครือข่ายเสมือนส่วนตัว (Virtual Private Network) เท่านั้น โดยผู้มีสิทธิเข้าถึงโปรแกรมประยุกต์และสารสนเทศจากภายนอกสำนักงาน ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรเท่านั้น

5.7 การควบคุมโปรแกรมประสงค์ร้าย (Controls against malicious code)

(1) ให้ผู้ใช้งานคอมพิวเตอร์ตรวจสอบหาไวรัสจากสื่อต่างๆก่อนนำมาใช้งาน เช่น Flash drive และ Data storage เป็นต้น

(2) ไฟล์ที่ผ่านการดาวน์โหลดได้แก่ ไฟล์แนบมากับจดหมายอิเล็กทรอนิกส์ (E-mail) แฟ้มที่ได้รับ (Download) มาจากอินเตอร์เน็ต สำเนาจากแผ่นดิสก์หรือไฟล์แชร์ต่างๆ ต้องผ่านการสแกนไวรัสก่อนเปิดใช้งาน

(3) ห้ามขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

(4) ให้ผู้ใช้งานตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นๆมีความเสียหาย ถูกทำลาย แก้ไข เปลี่ยนแปลงหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ และรีบแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันที

5.8 การควบคุมโปรแกรมชนิดเคลื่อนไหวได้ (Controls against mobile code)

เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่ (Mobile device) ของผู้ใช้ที่สามารถเข้าถึงระบบเครือข่ายและระบบสารสนเทศของสำนักงาน ต้องได้รับการปรับค่าโครงแบบ (Configuration) อย่างเหมาะสมเพื่อป้องกัน Active Code ต่างๆ (เช่น Java, Active X) จากแหล่งที่ไม่น่าเชื่อถือในอินเตอร์เน็ต

5.9 แนวปฏิบัติการใช้งานคุกกี้

กำหนดให้คุกกี้ใช้สำหรับการบันทึกประวัติการเข้าชมของเว็บไซต์ของผู้ใช้งานเท่านั้น โดยไม่มีการระบุถึงข้อมูลส่วนบุคคลของผู้ใช้งานด้วยคุกกี้ ผู้ใช้งานสามารถเปลี่ยนการตั้งค่าคุกกี้ด้วยตัวเองและสามารถบล็อกคุกกี้ได้ ทั้งนี้ขึ้นอยู่กับการใช้สภาพแวดล้อมในการใช้งานของผู้ใช้

5.10 แนวทางการตั้งเวลาเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

กำหนดให้เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายต้องตั้งเทียบเวลามาตรฐาน (NTP) ตรงกับเวลาอ้างอิงสากล (Stratum o) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที เช่น กรมอุทกศาสตร์ (กองทัพเรือ) ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC)

5.11 แนวทางการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

กำหนดให้ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า 90 วัน นับแต่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ไม่อนุญาตให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ผู้มีหน้าที่เกี่ยวข้องที่ผู้บริหารสำนักงานกำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของสำนักงานหรือบุคคลที่สำนักงานมอบหมาย

หมวด 3

ข้อปฏิบัติในการจัดระบบเทคโนโลยีสารสนเทศ

ข้อ 6 ให้เจ้าหน้าที่ของสำนักงานที่ปฏิบัติการด้านคอมพิวเตอร์ดำเนินการตามข้อปฏิบัติในการจัดระบบเทคโนโลยีสารสนเทศ ระบบสำรองเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ รวมทั้งการจัดทำแผนใช้งานเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ เพื่อให้ในกรณีฉุกเฉินมีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่องตลอดเวลา ดังนี้

6.1 การจัดระบบเทคโนโลยีสารสนเทศ

6.1.1 การแบ่งประเภทข้อมูล โดยแบ่งเป็นข้อมูลทั่วไป ข้อมูลที่ไม่เปิดเผย ข้อมูลส่วนบุคคลและข้อมูลลับ

6.1.2 ต้องมีระบบการจัดเก็บข้อมูล โดยจัดเก็บตามประเภทของข้อมูลและมีการบันทึกรายละเอียดของข้อมูลในแต่ละประเภทที่จัดเก็บ

6.1.3 กำหนดผู้รับผิดชอบตรวจสอบความมีอยู่อย่างถูกต้องครบถ้วนของข้อมูลอย่างน้อยปีละ 1 ครั้ง และมีการบันทึกรายละเอียดการตรวจสอบ ในกรณีตรวจพบข้อมูลสูญหายไม่ถูกต้องครบถ้วน ผู้รับผิดชอบในการจัดเก็บดำเนินการปรับปรุงแก้ไขข้อมูลให้มีความสมบูรณ์ครบถ้วนในทันที

6.2 การจัดระบบสำรองเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์

6.2.1 พิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

6.2.2 จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง และเก็บในสถานที่ปลอดภัย

6.2.3 ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแล รับผิดชอบระบบสารสนเทศระบบสำรองและการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

6.2.4 ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศและระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

6.2.5 สื่อสารแผนฉุกเฉินให้บุคคลที่เกี่ยวข้องทราบ

หมวด 4

ข้อปฏิบัติในการตรวจสอบ

ข้อ 7 ในการตรวจสอบให้ดำเนินการตามข้อปฏิบัติในการตรวจสอบ การประเมินความเสี่ยงและมาตรการในการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อความมั่นคงปลอดภัยในการให้บริการเทคโนโลยีสารสนเทศและระบบงานคอมพิวเตอร์ ดังนี้

7.1 ตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง

7.2 ตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบอิสระ หรือสำนักตรวจสอบภายในซึ่งขึ้นตรงต่อคณะกรรมการบริหาร

7.3 รายงานการตรวจสอบและประเมินความเสี่ยงเสนอผู้รับผิดชอบและหน่วยงานที่รับผิดชอบจะดำเนินการปรับปรุงตามคำแนะนำโดยทันที

7.4 กำหนดความรับผิดชอบของผู้ใช้งานและผู้บริหาร ให้ผู้ใช้งานและผู้บริหารรับผิดชอบในกรณีเกิดความเสียหายหรืออันตรายอันเนื่องมาจากผู้ใช้งานหรือผู้บริหารบกพร่องหรือไม่ปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แล้วแต่กรณี

หมวด 5

ข้อปฏิบัติในการสร้างความรู้ความเข้าใจการใช้งานระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์

ข้อ 8 ให้คณะทำงานสนับสนุนผู้บริหารเทคโนโลยีสารสนเทศระดับสูงและเจ้าหน้าที่ของสำนักงานที่ปฏิบัติการด้านคอมพิวเตอร์ ดำเนินการตามข้อปฏิบัติในการสร้างความรู้ความเข้าใจการใช้งานระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักและความเข้าใจถึงภัยหรือผลกระทบที่เกิดจากการใช้เทคโนโลยีสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ ดังนี้

8.1 จัดทำคู่มือแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

8.2 ฝึกอบรมให้ผู้ใช้งานตระหนักและเข้าใจในเรื่องภัยและผลกระทบที่เกิดจากการใช้งานเทคโนโลยีสารสนเทศโดยไม่ถูกต้องหรือไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมทั้งมาตรการป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

8.3 เผยแพร่แนวนโยบายและแนวปฏิบัติดังกล่าว ทางเว็บไซต์สำนักงานให้แก่ผู้ใช้งานและบุคคลทั่วไป

ข้อ 9 ต้องทบทวนและปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีความทันสมัย เป็นปัจจุบันและเป็นมาตรฐานที่ยอมรับได้อย่างสม่ำเสมออย่างน้อยทุก 2 ปี

หมวด 6

ผู้กำกับ ดูแล

ข้อ 10 กำหนดให้เจ้าหน้าที่ที่ได้รับมอบหมาย หรือดำรงตำแหน่งเป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ประจำสำนักงาน เป็นผู้รับผิดชอบต่อนโยบายในฐานะผู้กำกับดูแล ติดตามทบทวน แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน

ประกาศ ณ วันที่ 5 เมษายน พ.ศ. 2562

(นายพีร์ ชูศรี)
รองผู้อำนวยการ
รักษาการแทนผู้อำนวยการ
สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ