แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒

๑. ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๒. ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๓. ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๔. ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๕. ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

หมวด ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

วัตถุประสงค์

เพื่อให้บุคลากรกรมสนับสนุนบริการสุขภาพ และบุคคลภายนอก ให้มีความรู้ ความเข้าใจและสามารถปฏิบัติตามแนวทางปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) พร้อมทั้งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ

นโยบาย

บุคลากรกรมสนับสนุนบริการสุขภาพ และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้

๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งาน ตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) ต้องสอดคล้อง และเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ

๑.๒ กลุ่มเทคโนโลยีสารสนเทศมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน (User) สำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๓ เจ้าของระบบ (System Owner) มีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน (User)

๑.๔ ผู้ดูแลระบบ (Administrator) มีหน้าที่กำหนดสิทธิให้แก่ผู้ใช้งาน (User) ตามที่เจ้าของระบบ (System Owner) อนุมัติ

๑.๕ ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

๑.๖ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ และอุปกรณ์ในการประมวลผลข้อมูล (Process Device) ทั้งทางกายภาพ (Physical Access) และจากระยะไกล (Remote Access) บุคคลภายนอกดังกล่าว ต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจ จากกลุ่มเทคโนโลยีสารสนเทศ และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

๑.๗ การเข้าถึงห้องศูนย์ข้อมูล (Data Center) เพื่อปฏิบัติงานที่เกี่ยวข้องกับอุปกรณ์ ในการประมวลผลข้อมูล (Process Device) ให้ดำเนินการ ดังนี้

๑.๗.๑ กลุ่มเทคโนโลยีสารสนเทศต้องกำหนดหลักเกณฑ์สำหรับการปฏิบัติงาน ในห้องศูนย์ข้อมูล (Data Center)

๑.๗.๒ การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศก่อนเริ่มดำเนินการทุกครั้ง

๑.๗.๓ ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับอนุญาตจากกลุ่มเทคโนโลยีสารสนเทศ

๑.๗.๔ ผู้ใช้งาน (User) หรือบุคคลภายนอก ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน โดยมีผู้ดูแลระบบ (Administrator) ควบคุมการปฏิบัติงานของผู้ใช้งาน (User) หรือบุคคลภายนอก ตลอดเวลา และต้องไม่นำอาหาร หรือเครื่องดื่มเข้าไปในห้องศูนย์ข้อมูล (Data Center) และห้ามสูบบุหรี่ ในห้องศูนย์ข้อมูล (Data Center)

๒. การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนด ดังนี้

๒.๑ สิทธิของผู้ใช้งาน (User) ประกอบด้วย

๒.๑.๑ อ่านอย่างเดียว

๒.๒.๒ สร้างข้อมูล

๒.๒.๓ แก้ไขข้อมูล

๒.๒.๔ ลบข้อมูล

๒.๒ สิทธิผู้ดูแลระบบ (Administrator) กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การกำหนดประเภทของข้อมูล ลำดับความสำคัญ ลำดับชั้นความลับ รวมถึงระดับชั้น การเข้าถึง เวลาที่เข้าถึง และช่องทางการเข้าถึง ดังนี้

๓.๑ ประเภทของข้อมูล แบ่งเป็น ๓ ประเภท ดังนี้

๓.๑.๑ ข้อมูลสารสนเทศสำหรับการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร และข้อมูลงบประมาณรายจ่าย (SMART)

๓.๑.๒ ข้อมูลสารสนเทศสำหรับการสนับสนุนการปฏิบัติงาน ได้แก่ ข้อมูลระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ (GFMIS)

๓.๑.๓ ข้อมูลสารสนเทศสำหรับการเผยแพร่แก่ประชาชนทั่วไปและผู้ที่สนใจ ได้แก่ ข้อมูลในเว็บไซต์ของกรมสนับสนุนบริการสุขภาพ

๓.๒ ลำดับความสำคัญของข้อมูล แบ่งเป็น ๓ ระดับ ดังนี้

๓.๒.๑ สำคัญมากที่สุด

๓.๒.๒ สำคัญมาก

๓.๓.๓ ปกติ

๓.๓ ลำดับชั้นความลับของข้อมูล แบ่งเป็น ๔ ระดับ ดังนี้

๓.๓.๑ ลับที่สุด - ความลับที่มีความสำคัญที่สุด เกี่ยวกับข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหากความลับดังกล่าวทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือเป็นภยันตรายต่อความมั่นคง ความปลอดภัย หรือความสงบเรียบร้อยของประเทศชาติหรือพันธมิตร หรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้องอย่างร้ายแรงที่สุด

๓.๓.๒ ลับมาก - ความลับที่มีความสำคัญมาก เกี่ยวกับข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหากความลับดังกล่าวทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคลที่ไม่มีหน้าที่ได้ทราบ จะทำให้เกิดความเสียหาย หรือเป็นภยันตรายต่อความมั่นคง ความปลอดภัยของประเทศชาติหรือพันธมิตร หรือความสงบเรียบร้อยภายในราชอาณาจักร หรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้องได้อย่างร้ายแรง

๓.๓.๓ ลับ - ความลับที่มีความสำคัญเกี่ยวกับ ข่าวสาร วัตถุ หรือบุคคล ซึ่งถ้าหากความลับดังกล่าวทั้งหมด หรือเพียงบางส่วนรั่วไหลไปถึงบุคคลผู้ไมมีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายต่อราชการ หรือการดำเนินงานขององค์กร หรือหน่วยงานที่เกี่ยวข้องได้

๓.๓.๔ ปกปิด – ความลับซึ่งไม่พึงเปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบ โดยสงวนไว้ให้ทราบเฉพาะบุคคลที่มีหน้าที่ต้องทราบเพื่อประโยชน์ในการปฏิบัติภารกิจองค์กรเท่านั้น

๓.๔ ระดับชั้นการเข้าถึง แบ่งเป็น ๓ ระดับ ดังนี้

๓.๔.๑ กลุ่มผู้บริหาร

๓.๔.๒ กลุ่มผู้ปฏิบัติงาน

๓.๔.๓ กลุ่มประชาชนทั่วไปและผู้ที่สนใจ

๓.๕ เวลาที่เข้าถึง

ระบบคอมพิวเตอร์และระบบสารสนเทศสามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง ๗ วัน

๓.๖ ช่องทางการเข้าถึง

ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศได้ ๒ ช่องทาง ดังนี้

๓.๖.๑ ระบบเครือข่ายภายใน (Intranet)

๓.๖.๒ ระบบเครือข่ายภายนอก (Internet)

๔. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) แบ่งเป็น ๒ ส่วน ดังนี้

๔.๑ การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้สอดคล้องตามภารกิจ

๔.๑.๑ เจ้าของระบบ (System Owner) อนุมัติสิทธิให้ผู้ใช้งาน (User) ตามภารกิจ เพื่อให้สามารถเข้าถึงข้อมูลในระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะในส่วนที่ได้รับมอบหมาย ตามความจำเป็นในการใช้งาน

๔.๑.๒ ผู้ดูแลระบบ (Administrator) กำหนดสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน (User) ตามที่เจ้าของระบบ (System Owner) อนุมัติ

๔.๒ การปรับปรุงการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศให้สอดคล้อง ตามภารกิจและการรักษาความมั่นคงปลอดภัย ผู้ดูแลระบบ (Administrator) ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุด การจ้างเพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัย ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

หมวด ๒
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งาน (User) ที่ได้รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศ และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนบุคลากรใหม่ (User Registration) เพื่อรับสิทธิ การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

๒. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อบุคลากรไม่ได้ปฏิบัติงานที่กรมสนับสนุนบริการสุขภาพ แล้ว

๓. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการ ควบคุม จำกัด และเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ ที่ได้รับมอบหมาย ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๔. กำหนดให้มีการบริหารจัดการรหัสผ่าน (User Password Management) อย่างรัดกุม โดยเริ่มตั้งแต่กระบวนการสร้างรหัสผ่านชั่วคราว (Temporary Password) ตามสิทธิที่ได้รับของผู้ใช้งาน (User) การส่งมอบรหัสผ่านชั่วคราว (Temporary Password) การเปลี่ยนรหัสผ่าน เงื่อนไขการเปลี่ยน รหัสผ่าน และการกำหนดรหัสผ่านใหม่ในกรณีลืมรหัสผ่าน หรือใช้เทคโนโลยีอื่นใด ในการบริหารจัดการรหัสผ่าน เช่น e-KYC

๕. กำหนดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง

๖. กำหนดให้มีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User) เพื่อให้เกิดความตระหนักและความเข้าใจเรื่องภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

๗. กำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

แนวปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน (User Registration) ให้ดำเนินการ ดังนี้

๑.๑ ให้กลุ่มเทคโนโลยีสารสนเทศกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศสำหรับบุคลากร กรมสนับสนุนบริการสุขภาพ และบุคคลภายนอกอย่างน้อยประกอบด้วยชื่อ นามสกุล ตำแหน่ง สังกัด หมายเลขโทรศัพท์ และจดหมายอิเล็กทรอนิกส์ (E - Mail) ที่ใช้งานในปัจจุบันเพื่อเป็นการยืนยันตัวตนผ่านจดหมายอิเล็กทรอนิกส์ รวมทั้งจดหมายอิเล็กทรอนิกส์สำรองของผู้ขอใช้งาน

๑.๒ การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

๑.๒.๑ กรณีบุคลากรกรมสนับสนุนบริการสุขภาพ

(๑) ให้บุคลากรใหม่กรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคลากรของ กรมสนับสนุนบริการสุขภาพ ในวันรายงานตัว

(๒) ให้หน่วยงานส่งแบบฟอร์มการขออนุญาตเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคลากรของ กรมสนับสนุนบริการสุขภาพ ให้กลุ่มเทคโนโลยีสารสนเทศ เพื่อสร้างบัญชี ผู้ใช้งาน (Username) และกำหนดรหัสผ่านชั่วคราว (Temporary Password)

(๓) ให้เจ้าของระบบ (System Owner) อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้บุคลากรใหม่

(๔) ให้ผู้ดูแลระบบ (Administrator) กำหนดสิทธิให้บุคลากรใหม่ ตามที่ เจ้าของระบบ (System Owner) อนุมัติ พร้อมทั้งแจ้งให้บุคลากรใหม่ได้รับทราบ

๑.๒.๒ กรณีบุคคลภายนอก

(๑) ให้สำนัก/กอง/ศูนย์/กลุ่ม/กลุ่มงาน แจ้งความประสงค์พร้อมเหตุผลในการให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาต เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคคลภายนอก

(๒) ให้กลุ่มเทคโนโลยีสารสนเทศพิจารณาเหตุผลดังกล่าวก่อนดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านชั่วคราว (Temporary Password)

(๓) ให้เจ้าของระบบ (System Owner) อนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้บุคคลภายนอก

(๔) ให้ผู้ดูแลระบบ (Administrator) กำหนดสิทธิให้ผู้ใช้งาน (User) ตามที่เจ้าของระบบ (System Owner) อนุมัติ พร้อมทั้งแจ้งให้บุคคลภายนอกได้รับทราบ

๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และการกำหนดรหัสผ่าน (Password) ให้ดำเนินการ ตามหลักเกณฑ์ ดังนี้

๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้ใช้ชื่อภาษาอังกฤษตามบัตรประจำตัวประชาชน ตามด้วยเครื่องหมาย “_” หรือ “.” ตามด้วยอักษรนามสกุลตัวแรก หรืออักษรอื่นใดที่มีการตกลงร่วมกัน

๑.๓.๒ การกำหนดรหัสผ่าน (Password) ชุดของตัวอักษร ตัวเลข และอักขระพิเศษ อย่างน้อย ๘ ตัวขึ้นไป และยากต่อการคาดเดา โดยใช้ร่วมกับบัญชีผู้ใช้งาน (Username) เพื่อใช้เป็นเครื่องมือ ในการตรวจสอบยืนยันตัวตน (Authentication) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ หรือนำระบบยืนยันตัวตนอิเล็กทรอนิกส์ (e-KYC) หรือการยืนยันตัวตนหลายขั้นตอน เช่น 2FA (Two Factor Authentication) or MFA (Multifactor Authentication) มาปรับใช้ในระบบงานขึ้นกับระดับความสำคัญในการเข้าถึงสิทธินั้นๆ[๑]

๑.๓.๓ ให้ผู้ดูแลระบบ (Administrator) แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน ชั่วคราว (Temporary Password) ให้ผู้ใช้งาน (User) ทราบโดยตรง

๑.๓.๔ เมื่อบุคลากรกรมสนับสนุนบริการสุขภาพ มีการเปลี่ยนชื่อหรือนามสกุลให้แจ้งกลุ่มเทคโนโลยีสารสนเทศ เพื่อเปลี่ยนบัญชีผู้ใช้งาน (Username)

๑.๔ บัญชีผู้ใช้งาน (Username) สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ได้จนกว่าบุคลากรหรือบุคคลภายนอกสิ้นสุดการปฏิบัติหน้าที่ใน กรมสนับสนุนบริการสุขภาพ และกลุ่มเทคโนโลยีสารสนเทศดำเนินการยกเลิกสิทธิการใช้งาน

๒. การยกเลิกสิทธิการใช้งานของบุคลากรหรือบุคคลภายนอกให้ดำเนินการ ดังนี้

๒.๑ กรณีบุคลากรกรมสนับสนุนบริการสุขภาพ

๒.๑.๑ ให้หน่วยงานแจ้งกลุ่มเทคโนโลยีสารสนเทศ เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก ให้โอน หรือสิ้นสุด การจ้าง

๒.๑.๒ กลุ่มเทคโนโลยีสารสนเทศจะปิดบัญชีผู้ใช้งาน (Username) ชั่วคราว เป็นเวลา ๙๐ วัน หากบุคลากรที่มีความประสงค์จะใช้ข้อมูลในบัญชีผู้ใช้งาน (Username) ดังกล่าว ให้แจ้ง ความประสงค์พร้อมเหตุผลต่อกลุ่มเทคโนโลยีสารสนเทศ เพื่อขอเปิดใช้งานบัญชีผู้ใช้งาน (Username) ดังกล่าวชั่วคราว พร้อมทั้งกำหนดรหัสผ่านชั่วคราว (Temporary Password) ทั้งนี้ เมื่อครบกำหนด ๙๐ วัน นับจากมีคำสั่งเป็นลายลักษณ์อักษร กลุ่มเทคโนโลยีสารสนเทศจะยกเลิกสิทธิการเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ และลบข้อมูลสารสนเทศของบัญชีผู้ใช้งาน (Username) ดังกล่าว เป็นการถาวร

---

[๑] พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

๒.๒ กรณีบุคคลภายนอก

๒.๒.๑ ให้สำนัก/กอง/ศูนย์/กลุ่ม/กลุ่มงาน แจ้งความประสงค์ยกเลิกสิทธิในการเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศต่อกลุ่มเทคโนโลยีสารสนเทศทันทีที่หมดความจำเป็น

๒.๒.๒ กลุ่มเทคโนโลยีสารสนเทศจะยกเลิกสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ และลบข้อมูลสารสนเทศเป็นการถาวร

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศของผู้ใช้งาน (User) ให้ดำเนินการ ดังนี้

๓.๑ ผู้ดูแลระบบ (Administrator) ตรวจสอบสิทธิการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศตามแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ สำหรับบุคลากร กรมสนับสนุนบริการสุขภาพ หรือบุคคลภายนอกให้สอดคล้องกับคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่ง มอบอำนาจ หรือเหตุผลความจำเป็นของสำนัก/กอง/ศูนย์/กลุ่ม/กลุ่มงาน ที่ได้แจ้งความประสงค์ในการให้บุคคลภายนอก เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ แล้วแต่กรณี

๓.๒ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้หน่วยงานแจ้งกลุ่มเทคโนโลยีสารสนเทศ เพื่อเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว

๓.๓ ในกรณีที่ผู้ใช้งาน (User) ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สูงกว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อกลุ่มเทคโนโลยีสารสนเทศ ทั้งนี้ ต้องมีการกำหนดระยะเวลาการใช้งาน และยกเลิกสิทธิการใช้งานทันทีที่หมดความจำเป็น

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการ ตามหลักเกณฑ์ ดังนี้

๔.๑ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่านชั่วคราว (Temporary Password) ทันทีที่เข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศในครั้งแรก

๔.๒ การเปลี่ยนรหัสผ่านใหม่ (Password) ให้ดำเนินการผ่านระบบบริหารจัดการรหัสผ่าน (Password Management System) โดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เดิม

๔.๓ ในกรณีที่ผู้ใช้งาน (User) ลืมรหัสผ่าน (Password) ให้ขอรับรหัสผ่านใหม่ ผ่านระบบบริหารจัดการรหัสผ่าน (Password Management System) โดยเลือกใช้วิธีการตอบคำถาม หรือเลือกรับ Link / URL สำหรับการตั้งรหัสผ่านใหม่ผ่านระบบจดหมายอิเล็กทรอนิกส์ (E - Mail) สำรองของผู้ใช้งาน (User)

๔.๔ กรณีผู้ใช้งาน (User) ไม่สามารถเปลี่ยนรหัสผ่านใหม่ได้ ให้แจ้งกลุ่มเทคโนโลยีสารสนเทศ เพื่อขอรับรหัสผ่านชั่วคราว (Temporary Password)

๔.๕ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๖ เดือน และรหัสผ่าน (Password) ใหม่ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

๕. ผู้ดูแลระบบ (Administrator) ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง

๖. ให้กลุ่มเทคโนโลยีสารสนเทศจัดฝึกอบรมให้แก่ผู้ใช้งาน (User) เพื่อให้มีความรู้ ความเข้าใจ และเกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ อย่างน้อยปีละ ๑ ครั้ง หรือจัดให้ผู้ใช้งาน (User) เข้าร่วมการฝึกอบรม ที่หน่วยงานอื่นจัดขึ้น

๗. ให้กลุ่มเทคโนโลยีสารสนเทศกำหนดมาตรการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศ ตามความเหมาะสม ได้แก่ การไม่เปิดจดหมายอิเล็กทรอนิกส์ (E - Mail) ที่ไม่ระบุที่มาหรือชื่อผู้ส่งที่น่าสงสัย โดยให้ลบจดหมายอิเล็กทรอนิกส์ทันที หรือการแจ้งเตือนผู้ใช้งาน (User) เมื่อมีไวรัสแพร่ระบาด

หมวด ๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนา ข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

๑. กำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)

๒. กำหนดแนวปฏิบัติในการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) ดูแล

๓. กำหนดแนวปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ได้แก่ เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศ เพื่อไม่ให้สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งาน (User) ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔. กำหนดให้ผู้ใช้งาน (User) อาจนำการเข้ารหัสข้อมูล (Encryption) มาใช้กับการรับส่งข้อมูล ที่สำคัญหรือข้อมูลที่เป็นความลับของ กรมสนับสนุนบริการสุขภาพ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

แนวปฏิบัติ

๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้

๑.๑ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่านชั่วคราว (Temporary Password) ทันทีที่เข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศในครั้งแรก

๑.๒ ผู้ใช้งาน (User) ต้องกำหนดรหัสผ่าน (Password) ตามหมวด ๒ ข้อ ๑.๓ (๒)

๑.๓ ผู้ใช้งาน (User) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๖ เดือน และรหัสผ่าน (Password) ใหม่ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

๑.๔ ผู้ใช้งาน (User) ต้องไม่ใช้รหัสผ่าน (Password) ร่วมกับบุคคลอื่น และไม่ควรให้ระบบคอมพิวเตอร์หรือระบบสารสนเทศจำรหัสผ่าน (Password) ในการเข้าใช้งานโดยอัตโนมัติ

๑.๕ ผู้ใช้งาน (User) ต้องไม่เปิดเผยรหัสผ่าน (Password) สำหรับการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเก็บเป็นความลับเสมือนเป็นสมบัติส่วนตัว ห้ามจดหรือเขียน รหัสผ่าน (Password) ที่ใช้งานไว้ในที่เปิดเผย

๑.๖ หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็น ในการเข้าถึง หลังจากดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

๑.๗ หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของ บัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดในเอกสารฉบับนี้แล้ว

๑.๘ ผู้ดูแลระบบ (Administrator) ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๓ เดือน และรหัสผ่าน (Password) ใหม่ ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

๒. การป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) ผู้ใช้งาน (User) ต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๓.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ในการประมวลผลข้อมูล (Process Device) มีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานของ กรมสนับสนุนบริการสุขภาพ เท่านั้น

๓.๒ ระบบคอมพิวเตอร์และระบบสารสนเทศ เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์ประมวลผลข้อมูล ต้องถูกติดตั้งด้วยซอฟต์แวร์ที่มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมายเท่านั้น

๓.๓ ระบบคอมพิวเตอร์และระบบสารสนเทศ ต้องได้รับการป้องกันด้วยรหัสผ่าน ของระบบพิสูจน์ตัวตนจากส่วนกลาง (Active Directory : AD) ทุกครั้งเมื่อเข้าใช้งาน และออกจาก ระบบ (Log out) ทันทีทุกครั้งเมื่อเลิกใช้งาน

๓.๔ ผู้ใช้งาน (User) ต้องรับผิดชอบต่อสินทรัพย์ (Asset) ของ กรมสนับสนุนบริการสุขภาพ และให้ใช้งาน ด้วยความระมัดระวังเสมือนเป็นทรัพย์สินของตน

๓.๕ ผู้ใช้งาน (User) ต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ ใดๆ ที่เครื่องคอมพิวเตอร์ลูกข่ายหรือเครื่องคอมพิวเตอร์พกพา หรือระบบคอมพิวเตอร์หรือระบบสารสนเทศ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลต่อกลุ่มเทคโนโลยีสารสนเทศ

๓.๖ ผู้ใช้งาน (User) ต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึก ข้อมูลแบบพกพา หรือการ์ดความจำในโทรศัพท์มือถือ เพื่อป้องกันการรั่วไหลของข้อมูล

๓.๗ บุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานระบบคอมพิวเตอร์และระบบสารสนเทศ ต้องขออนุมัติกลุ่มเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร ก่อนเข้าปฏิบัติงาน และต้องได้รับการอนุมัติ จากกลุ่มเทคโนโลยีสารสนเทศก่อนเริ่มปฏิบัติงาน

๓.๘ การทำลายอุปกรณ์บันทึกข้อมูลหรือการนำอุปกรณ์บันทึกข้อมูลกลับมาใช้งานใหม่ ให้ดำเนินการ ดังนี้

๓.๘.๑ การทำลายอุปกรณ์บันทึกข้อมูล เช่น Flash Drive CD/DVD ฮาร์ดดิสก์ เทป เป็นต้น ให้ใช้วิธีการทุบ หรือบดให้เสียหาย หรือเผาทำลายด้วยวิธีการทำลายตามมาตรฐานสากล หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

๓.๘.๒ การนำอุปกรณ์บันทึกข้อมูลไปใช้งานใหม่ ให้ฟอร์แมต (Format) อุปกรณ์บันทึก ข้อมูลนั้นโดยใช้วิธีการฟอร์แมต (Format) ตามมาตรฐานสากล หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

๔. ผู้ใช้งาน (User) อาจนำการเข้ารหัสข้อมูล (Encryption) ที่ได้รับรองมาตรฐานสากลหรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด ได้แก่ HTTPS, SSL, LDAPS, VPN, XML, ebXML หรือเทคโนโลยีอื่นใดที่ดีกว่า มาใช้ในกรณีมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับของ กรมสนับสนุนบริการสุขภาพ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

หมวด ๔
การควบคุมการเข้าถึงเครือข่าย
(Network Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึง

๒. กำหนดแนวปฏิบัติในการยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาต ให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่าย ระบบคอมพิวเตอร์และระบบสารสนเทศของ กรมสนับสนุนบริการสุขภาพ ได้

๓. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดยต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่าย เป็นการยืนยัน

๔. กำหนดแนวปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) โดยต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕. กำหนดแนวปฏิบัติในการแบ่งแยกเครือข่าย (Segregation in Networks) โดยต้องแบ่งแยกเครือข่ายตามกลุ่มของการให้บริการสารสนเทศ กลุ่มการใช้งาน กลุ่มของอุปกรณ์สารสนเทศ และกลุ่มประเภท ของเครือข่าย

๖. กำหนดแนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

๗. กำหนดแนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศและการส่งข้อมูล สารสนเทศสอดคล้องกับแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

๑. การเข้าถึงเครือข่ายของผู้ใช้งาน (User)

๑.๑ การใช้งานระบบเครือข่ายภายนอก (Internet) ให้ดำเนินการ ดังนี้

๑.๑.๑ กำหนดให้ใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าใช้งานระบบเครือข่ายภายนอก (Internet)

๑.๑.๒ ห้ามใช้งานระบบเครือข่ายภายนอก (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) สูงที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ ได้แก่ Youtube หนังออนไลน์ หรือรายการ บันเทิงต่างๆ ในเวลาราชการ

๑.๑.๓ ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดต่อศีลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์ เสื่อมเสีย

๑.๑.๔ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของ กรมสนับสนุนบริการสุขภาพ ผ่านระบบเครือข่าย ภายนอก (Internet) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๕ ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. ๒๕๔๔ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเคร่งครัด ได้แก่ ห้ามเปิดเผยข้อมูลของทางราชการโดยไม่ได้รับอนุญาติ ห้ามแพร่ภาพหรือข้อมูลใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความ

ผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือที่มีลักษณะลามกอนาจาร และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าว ผ่านระบบเครือข่ายภายนอก (Internet) ห้ามเผยแพร่ภาพของผู้อื่นที่เกิดจากการสร้างขึ้น ตัดต่อ ต่อเติม หรือดัดแปลงด้วยวิธีการ ทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่จะทำให้ผู้นั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑.๑.๖ ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่างๆ จากระบบเครือข่าย ภายนอก (Internet) เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๑.๗ หลังจากใช้งานระบบเครือข่ายภายนอก (Internet) แล้วให้ปิดเว็บบราวเซอร์ (Web Browser) เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

๑.๒ การใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ให้ดำเนินการ ดังนี้

๑.๒.๑ ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม โดยเคร่งครัด และห้ามใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ในทางที่ ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศีลธรรม

๑.๒.๒ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ ด้วยการใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ที่ส่งโดยโดเมนเนม (Domain Name) ของกรมสนับสนุนบริการสุขภาพ (@hss.mail.go.th)

๑.๒.๓ ต้องตรวจสอบชื่อผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender) ก่อนเปิดจดหมายอิเล็กทรอนิกส์ (E - Mail) เพื่อป้องกันการเปิดไฟล์อันตรายที่อาจมีไวรัสคอมพิวเตอร์ โดยเฉพาะ Executable File ได้แก่ ไฟล์ที่มีนามสกุล .exe, .com, .bat และ .inf ที่อาจนำเข้าสู่ระบบเครือข่ายกรมสนับสนุนบริการสุขภาพ

๑.๒.๔ หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ต้องออกจากระบบ (Log Out) ทันที เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

๑.๓ การใช้งานเครือข่ายไร้สาย (WiFi) ให้ดำเนินการ ดังนี้

๑.๓.๑ ผู้ดูแลระบบ (Administrator) ต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดเป็นค่ามาตรฐานมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Acess Point) มาติดตั้งเพื่อใช้งาน

๑.๓.๒ ผู้ใช้งาน (User) ต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (WiFi)

๑.๓.๓ ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายไร้สาย (WiFi) ผู้ใช้งาน (User) จะสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะที่ได้รับอนุญาตตามสิทธิ ของเครือข่ายไร้สาย (Wifi) เท่านั้น

๑.๓.๔ ผู้ใช้งาน (User) ต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็นทรัพย์สินของ กรมสนับสนุนบริการสุขภาพ ไปใช้งานเครือข่ายไร้สาย (WiFi) ที่ไม่น่าเชื่อถือ

๑.๓.๕ ผู้ใช้งาน (User) ไม่ควรทำธุรกรรมการเงินทางอิเล็กทรอนิกส์ระหว่างการใช้งาน เครือข่ายไร้สาย (WiFi) เนื่องจากอาจเกิดความไม่ปลอดภัยและอาจขาดการเชื่อมต่อของสัญญาณ

๑.๓.๖ ห้ามผู้ใช้งาน (User) ติดตั้งและเปิดการทำงานโปรแกรมประเภทดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายของกรมสนับสนุนบริการสุขภาพ และมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๔ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

๑.๔.๑ การประชาสัมพันธ์ผ่านเครือข่ายสังคมออนไลน์ (Social Network) ในนามของกรมสนับสนุนบริการสุขภาพ ผู้รับผิดชอบต้องแสดงตำแหน่ง หน้าที่ สังกัด ให้ชัดเจน เพื่อความน่าเชื่อถือ โดยอาจใช้รูปสัญลักษณ์ หรือเครื่องหมายแสดงสังกัดได้

๑.๔.๒ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ควรนำเสนอเกี่ยวกับภารกิจงานของ กรมสนับสนุนบริการสุขภาพ ได้แก่ วิสัยทัศน์ พันธกิจ ผลการดำเนินงาน และข่าวสาร ที่เป็นประโยชน์ มีความถูก

ต้อง ใช้ภาษาที่สุภาพ และมีรูปแบบที่น่าสนใจ โดยเนื้อหาต้องผ่านความเห็นชอบจากผู้ที่ได้รับมอบหมายหรือผู้บังคับบัญชาก่อนทุกครั้ง

๑.๔.๓ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของ กรมสนับสนุนบริการสุขภาพ ผ่านเครือข่ายสังคม ออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๔.๔ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงในเรื่องที่เกี่ยวข้องต่อไป

๑.๔.๕ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจาก กรมสนับสนุนบริการสุขภาพ และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑.๔.๖ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน (User) ต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที

๒. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections)

การระบุและยืนยันตัวตนของผู้ใช้งานอยู่ภายนอกองค์กร (User Authentication for External Connections) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง เพื่อตรวจสอบความถูกต้องในการพิสูจน์ยืนยันตัวตน (Authentication) ก่อนเข้าถึงเครือข่าย ระบบคอมพิวเตอร์ และระบบสารสนเทศ

๓. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ให้ดำเนินการ ดังนี้

๓.๑ กลุ่มเทคโนโลยีสารสนเทศต้องจัดทำผังระบบเครือข่าย (Network Diagram) พร้อมรายละเอียดอุปกรณ์บนเครือข่ายที่เห็นว่าจำเป็นต่อการใช้งาน ได้แก่ กลุ่มอุปกรณ์ เลขที่อยู่ไอพี (IP Address) และหมายเลขเฉพาะอุปกรณ์ (MAC Address) โดยให้ปรับปรุงทุก ๒ ปี หรือตามความเหมาะสม

๓.๒ การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ มาใช้งานบนเครือข่ายต้องได้รับอนุญาตจากกลุ่มเทคโนโลยีสารสนเทศ

๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ให้ดำเนินการ ดังนี้

๔.๑ กลุ่มเทคโนโลยีสารสนเทศต้องจัดทำแนวทางหรือคู่มือในการป้องกันพอร์ตที่ใช้สำหรับ ตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

๔.๒ กลุ่มเทคโนโลยีสารสนเทศต้องเปิดใช้งานเฉพาะพอร์ตที่จำเป็นสำหรับการใช้งานเท่านั้น และต้องตรวจสอบพอร์ตที่เปิดให้บริการสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

๕. การแบ่งแยกเครือข่าย (Segregation in Networks) แบ่งเป็น ๔ กลุ่ม ดังนี้

๕.๑ กลุ่มของการให้บริการสารสนเทศ ได้แก่ ระบบสารสนเทศเพื่อการสนับสนุนภารกิจหลักและระบบสารสนเทศเพื่อการสนับสนุนการปฏิบัติงาน

๕.๒ กลุ่มการใช้งาน ได้แก่ เจ้าของระบบ (System Owner) ผู้ดูแลระบบ (Administrator) และผู้ใช้งาน (User)

๕.๓ กลุ่มของอุปกรณ์สารสนเทศ ได้แก่ อุปกรณ์รักษาความมั่นคงปลอดภัยสารสนเทศ และอุปกรณ์บริหารจัดการเครือข่าย

๕.๔ กลุ่มประเภทของเครือข่ายคอมพิวเตอร์ ได้แก่ ระบบเครือข่ายภายใน (Intranet) ระบบเครือข่ายภายนอก (Internet) และระบบเครือข่ายโซนพิเศษ (Demilitarized Zone : DMZ)

๖. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้ดำเนินการ ดังนี้

๖.๑ กลุ่มเทคโนโลยีสารสนเทศต้องติดตั้งระบบป้องกันการบุกรุกโจมตีทางเครือข่าย (Firewall) เพื่อใช้เป็นจุดควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๖.๒ ผู้ดูแลระบบ (Administrator) ต้องไม่เปิดเผยข้อมูลการเชื่อมต่อทางเครือข่าย ก่อนได้รับอนุญาตจากกลุ่มเทคโนโลยีสารสนเทศ

๖.๓ ผู้ดูแลระบบ (Administrator) มีหน้าที่ในการควบคุมการเชื่อมต่อสัญญาณหรือยกเลิก การเชื่อมต่อสัญญาณตามที่ได้รับอนุญาตจากกลุ่มเทคโนโลยีสารสนเทศ ทั้งนี้ หากพบข้อผิดพลาดหรือเห็นว่า หมดความจำเป็นในการเชื่อมต่อสัญญาณให้รายงานกลุ่มเทคโนโลยีสารสนเทศทันที

๖.๔ การเชื่อมต่อเครือข่ายสารสนเทศระหว่างกรมสนับสนุนบริการสุขภาพ กับหน่วยงานภายนอก ต้องได้รับอนุญาตจากอธิบดีและเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ของผู้ให้บริการที่มีความน่าเชื่อถือ

๗. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ให้ดำเนินการ ดังนี้

๗.๑ ผู้ดูแลระบบ (Administrator) ต้องควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ และการรับ - ส่งหรือการไหลเวียนของข้อมูลหรือสารสนเทศเป็นไปอย่างรวดเร็ว

๗.๒ ผู้ดูแลระบบ (Administrator) ต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ใช้งาน (User) เป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

หมวด ๕
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกัน การเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) โดยต้องมีการควบคุมการเข้าถึงด้วยวิธีการยืนยันตัวตนที่ปลอดภัย

๒. กำหนดแนวปฏิบัติในการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยต้องกำหนดให้ผู้ใช้งาน (User) มีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน (User) ได้ และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการยืนยันว่าเป็นผู้ใช้งาน (User) ที่ได้รับอนุญาต

๓. กำหนดแนวปฏิบัติในการบริหารจัดการรหัสผ่าน (Password Management System) โดยต้องจัดทำระบบบริหารจัดการรหัสผ่าน (Password) ที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่าน (Password) ที่มีคุณภาพ

๔. กำหนดแนวปฏิบัติในการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการ ความมั่นคงปลอดภัยที่ได้กำหนดไว้

๕. กำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน (Session Time - Out)

๖. กำหนดระยะเวลาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time)

แนวปฏิบัติ

๑. ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ ผู้ใช้งาน (User) ต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง เพื่อตรวจสอบ ความถูกต้องในการพิสูจน์ยืนยันตัวตน (Authentication) ก่อนเข้าถึงระบบปฏิบัติการ (Operating System)

๓. กลุ่มเทคโนโลยีสารสนเทศต้องจัดให้มีระบบการบริหารจัดการรหัสผ่าน (Password Management System) ที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการเปลี่ยนรหัสผ่าน (Password) ที่มีคุณภาพ โดยผู้ใช้งาน (User) สามารถเปลี่ยนรหัสผ่าน (Password) ใหม่ หรือขอรหัสผ่าน (Password) ใหม่ได้ด้วยตนเองผ่านระบบบริหารจัดการรหัสผ่าน (Password Management System) กำหนด ดังนี้

๓.๑ กรณีปกติ

การใช้รหัสผ่าน (Password) เดิม เพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวตน (Authentication) และตั้งรหัสผ่าน (Password) ใหม่ ไปในคราวเดียวกัน

๓.๒ กรณีลืมรหัสผ่าน (Password)

๓.๒.๑ การเลือกใช้วิธีการตอบคำถาม หรือ

๓.๒.๒ การเลือกรับ Link/URL สำหรับการตั้งรหัสผ่าน (Password) ใหม่ผ่าน ระบบจดหมายอิเล็กทรอนิกส์ (E - Mail) สำรองของผู้ใช้งาน (User)

๔. การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) กำหนด ดังนี้

๔.๑ ผู้ใช้งาน (User) ต้องไม่ดัดแปลงหรือติดตั้งโปรแกรมอรรถประโยชน์ใดๆ บนระบบปฏิบัติการ ทั้งนี้ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์ต่อกลุ่มเทคโนโลยีสารสนเทศ

๔.๒ การใช้งานโปรแกรมอรรถประโยชน์อื่นๆ นอกเหนือจากที่ติดตั้งมากับระบบปฏิบัติการ ได้แก่ โปรแกรมประเภทดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรม Formatter กำหนดให้ผู้ดูแลระบบ (Administrator) เท่านั้นที่มีสิทธิใช้งาน

๕. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลายุติการใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ เมื่อเว้นว่างจากการใช้งาน (Session Time - Out) เมื่อครบ ๑๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๖. ผู้ดูแลระบบ (Administrator) ต้องกำหนดระยะเวลาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง (Limitation of Connection Time) โดยให้ใช้งานได้ เป็นเวลา ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง และในกรณีที่เชื่อมต่อจากภายนอก กำหนดให้ใช้งานได้ภายใน วันและเวลาราชการ เว้นแต่กรณีที่มีเหตุผลความจำเป็นให้ขออนุญาตผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ

หมวด ๖
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
(Application and Information Access Control)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติในการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ของผู้ใช้งาน (User) และฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น (Application and Information Access Control) ตามสิทธิที่กำหนดไว้

๒. กำหนดแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพ โดยต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking)

๓. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศจากความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๔. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) โดยต้องกำหนด ข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกสำนักงาน

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการ ดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User) การกำหนดสิทธิ ตามตำแหน่งและหน้าที่ที่ได้รับมอบหมาย และการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง ซึ่งรวมถึงบุคคลภายนอกหรือผู้รับจ้าง (Outsource) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศด้วย

๑.๒ ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งาน (User) ที่เข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศผ่านเครือข่ายภายนอก ให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) โดยมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL)

๑.๓ การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) รายละเอียดปรากฏตามภาคผนวก

๒. ระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพให้ดำเนินการ ดังนี้

๒.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อองค์กร ดังนี้

๒.๑.๑ ระบบการบริหารจัดการความมั่นคงปลอดภัยและเครือข่าย ได้แก่ ระบบ Antivirus, ระบบ Active Directory, ระบบ Backup Systems, ระบบ Domain Name Server, ระบบ Dynamic Host Configuration Protocol, ระบบ Network Management, ระบบ Network Monitoring และระบบจัดเก็บข้อมูลกลาง

๒.๑.๒ ระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ (GFMIS)

๒.๒ ระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพ ต้องได้รับการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกออกจากระบบอื่นๆ

๒.๓ ผู้ดูแลระบบ (Administrator) ต้องแบ่งพื้นที่สำหรับการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายตามระดับความสำคัญและความปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพ เพื่อควบคุมสภาพแวดล้อมโดยเฉพาะ

๒.๔ การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking) เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการ รบกวนมีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องเข้าถึงในสถานที่ที่มีความปลอดภัยและต้องได้รับอนุญาตจากกลุ่มเทคโนโลยีสารสนเทศ

๓. การควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ให้ดำเนินการ ดังนี้

๓.๑ ผู้ดูแลระบบ (Administrator) ต้องตรวจสอบเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ของผู้ใช้งาน (User) หรือบุคคลภายนอก ก่อนนำมาเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศ

๓.๑.๑ เครื่องคอมพิวเตอร์ต้องตรวจสอบ ดังนี้

(๑) ระบบปฏิบัติการต้องได้รับการติดตั้ง Service Pack เวอร์ชั่นล่าสุด

(๒) โปรแกรมตรวจสอบและป้องกันไวรัสคอมพิวเตอร์ต้องได้รับการอัพเดทฐานข้อมูลไวรัสคอมพิวเตอร์ที่เป็นปัจจุบัน

(๓) ไม่ติดตั้งโปรแกรมประเภทดักจับข้อมูล (Network Sniffer) และโปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer)

๓.๑.๒ อุปกรณ์สื่อสารเคลื่อนที่ ได้แก่ Smart Phone และ Taplet ต้องได้รับการยืนยัน ตัวตนโดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของผู้ใช้งาน (User) สำหรับเข้าใช้งาน

๔. การปฏิบัติงานจากภายนอก กรมสนับสนุนบริการสุขภาพ (Teleworking) กำหนด ดังนี้

๔.๑ ผู้ใช้งาน (User) ต้องปฏิบัติตามหมวด ๔ แนวปฏิบัติ ข้อ ๒ การยืนยันตัวบุคคล สำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections)

๔.๒ บุคคลภายนอกต้องปฏิบัติตามหมวด ๒ แนวปฏิบัติ ข้อ ๑.๒ การขออนุญาตเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศ (๒) กรณีบุคคลภายนอก และหากต้องปฏิบัติงานด้านเทคนิค จากภายนอกกรมสนับสนุนบริการสุขภาพ (Teleworking) ให้ดำเนินการตามที่กลุ่มเทคโนโลยีสารสนเทศกำหนดเป็นการเฉพาะคราว

๔.๓ เมื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศแล้ว ผู้ใช้งาน (User) ต้องระมัดระวัง ไม่ให้ผู้ไม่มีส่วนเกี่ยวข้องเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ สื่อสารเคลื่อนที่ได้ และต้องออกจากระบบ (Log Out) ทันทีเมื่อปฏิบัติเลิกใช้งาน

หมวด ๗
การจัดทำระบบสำรองของระบบสารสนเทศ
(Disaster Recovery Site)

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูล สารสนเทศ และการกู้คืนข้อมูลสารสนเทศ และการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของกรมสนับสนุนบริการสุขภาพ ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉิน และการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่องแม้ในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม และสามารถใช้งานสารสนเทศ ได้อย่างต่อเนื่อง

นโยบาย

๑. พิจารณาคัดเลือกระบบสารสนเทศที่เหมาะสมในการจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน

๒. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ กรมสนับสนุนบริการสุขภาพ เพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ

๓. กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบตามแผนบริหารความต่อเนื่อง ของกรมสนับสนุนบริการสุขภาพด้านสารสนเทศ

๔. ทดสอบสภาพพร้อมใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ และระบบสำรองตามแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ กรมสนับสนุนบริการสุขภาพ อย่างน้อยปีละ ๑ ครั้ง

๕. กำหนดความถี่ของการปฏิบัติในแต่ละข้อ โดยต้องมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของหน่วยงาน

แนวปฏิบัติ

๑. กลุ่มเทคโนโลยีสารสนเทศต้องจัดทำระบบสารสนเทศและระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน โดยมีขั้นตอน ดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) จัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูล และการกู้คืนข้อมูลสารสนเทศ

๑.๒ ผู้ดูแลระบบ (Administrator) กำหนดรูปแบบการสำรองข้อมูลของระบบการสำรองข้อมูล (Backup System) ดังนี้

๑.๒.๑ รายชื่อระบบคอมพิวเตอร์และระบบสารสนเทศที่ได้รับการพิจารณาคัดเลือก ดังนี้

(๑) ระบบคอมพิวเตอร์เครื่องลูกข่ายเสมือน (Virtual Desktop Infrastructure : VDI)

(๒) ระบบติดตามการดำเนินการของโครงการ (Tracking System)

(๓) ระบบจดหมายอิเล็กทรอนิกส์ (E - Mail)

(๔) ระบบสำนักงานอัตโนมัติ (E - Office)

(๕) ระบบสารบรรณอิเล็กทรอนิกส์ (E - Sarabun)

(๖) ระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ (GFMIS)

๑.๒.๒ กำหนดรูปแบบการสำรองข้อมูลเฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) หรือเฉพาะส่วนที่มีการเปลี่ยนแปลง (Differential Backup) ทุกวัน

๑.๒.๓ กำหนดรูปแบบการสำรองข้อมูลแบบสมบูรณ์ (Full Backup) ทุกสัปดาห์และทุกเดือน ทั้งนี้เนื่องจากกลุ่มเทคโนโลยีสารสนเทศได้ดำเนินการสำรองข้อมูลระบบคอมพิวเตอร์ และระบบสารสนเทศแบบสมบูรณ์ (Full Backup) ทุกระบบงานจึงได้รับการสำรองข้อมูลด้วย

๑.๓ ผู้ดูแลระบบ (Administrator) ต้องพิมพ์รายละเอียดไว้บนตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใดที่ใช้สำหรับการสำรองข้อมูล ได้แก่ รูปแบบการสำรองข้อมูลแบบรายวันหรือรายสัปดาห์หรือรายเดือน วันและเวลา และผู้รับผิดชอบ พร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการสำรองข้อมูล

๑.๔ ผู้ดูแลระบบ (Administrator) ต้องกำหนดรูปแบบการกู้คืนข้อมูลของระบบการสำรองข้อมูล[๒] (Backup System) โดยมีความถี่และรูปแบบ ดังนี้

๑.๔.๑ การกู้คืนข้อมูลรายวันจากตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใดที่ใช้สำหรับการสำรองข้อมูล ที่สำรองข้อมูลเฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) หรือที่สำรองข้อมูลเฉพาะส่วนที่มีการเปลี่ยนแปลง (Differential Backup)

๑.๔.๒ การกู้คืนข้อมูลรายสัปดาห์หรือรายเดือนจากตลับเทปแม่เหล็ก (Magnetic Tape Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใดที่ใช้สำหรับการสำรองข้อมูลที่สำรองข้อมูลแบบสมบูรณ์ (Full Backup)

๒. กลุ่มเทคโนโลยีสารสนเทศดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ดังนี้

๒.๑ กำหนดผู้มีหน้าที่รับผิดชอบระบบสารสนเทศ

๒.๒ กำหนดผู้มีหน้าที่รับผิดชอบระบบสำรองข้อมูลสารสนเทศ

๒.๓ กำหนดผู้มีหน้าที่รับผิดชอบการจัดทำแผนดังกล่าว

๒.๔ กำหนดให้ปรับปรุงแผนดังกล่าวทุก ๑ ปี

๓. กลุ่มเทคโนโลยีสารสนเทศต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้อย่างน้อย ปีละ ๑ ครั้ง

ทั้งนี้ แผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และแผนการสำรองข้อมูล กรมสนับสนุนบริการสุขภาพ รวมถึงการทดสอบสภาพความพร้อมใช้งานได้นำข้อมูลไปรวมไว้ในแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ กรมสนับสนุนบริการสุขภาพ รายละเอียดปรากฏตามเอกสารภาคผนวก

---

[๒] หรือเลือกใช้วิธีการอื่นใด ที่ดีกว่าตามความก้าวหน้าด้านเทคโนโลยีสารสนเทศและเครือข่าย

หมวด ๘
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Ris Assessment and Risk Management)

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ทำให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนด มีความมั่นคงปลอดภัยและหน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

นโยบาย

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒. การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

แนวปฏิบัติ

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒. กำหนดให้มีผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๒.๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศประจำปีงบประมาณ ให้ดำเนินการโดยกลุ่มตรวจสอบภายใน (Internal Auditor)

๒.๒ หากมีความประสงค์ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศเชิงเทคนิค ให้ดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๓. กำหนดแนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๓.๑ ผู้ตรวจสอบต้องจัดทำรายงานพร้อมข้อเสนอแนะในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๒ กลุ่มเทคโนโลยีสารสนเทศต้องอำนวยความสะดวกแก่ผู้ตรวจสอบในการตรวจสอบข้อมูลที่สำคัญ

๓.๓ ในกรณีที่ผู้ตรวจสอบจำเป็นต้องเข้าถึงข้อมูลสำคัญให้กลุ่มเทคโนโลยีสารสนเทศ สร้างสำเนาสำหรับข้อมูลนั้น โดยให้ผู้ตรวจสอบใช้งานและทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือหากประสงค์จัดเก็บข้อมูลนั้นเป็นหลักฐานให้แจ้งกลุ่มเทคโนโลยีสารสนเทศทราบ

๓.๔ กลุ่มเทคโนโลยีสารสนเทศต้องจัดสรรอุปกรณ์ที่จำเป็นต้องใช้ในการตรวจสอบเชิงเทคนิค

๓.๕ ในกรณีมีการติดตั้งเครื่องมือที่ใช้ในการตรวจประเมินความเสี่ยงระบบคอมพิวเตอร์ และระบบสารสนเทศสารสนเทศ ให้แยกการติดตั้งเครื่องมือออกจากระบบที่ให้บริการจริง หรือระบบที่ใช้ในการพัฒนาและกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว (Read Only)

๓.๖ ผู้ตรวจสอบต้องแจ้งความเสี่ยงและระบุความรุนแรงของเครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยง

๓.๗ ผู้ดูแลระบบ (Administrator) ต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ตรวจสอบเป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

ภาคผนวก