

หมวดที่ ๑

การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control)

วัตถุประสงค์

เพื่อให้บุคลากรของกลุ่มแผนงานมีความรู้ ความเข้าใจและสามารถปฏิบัติตามแนวทางปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control) พร้อมทั้งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูล ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้

๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ ต้องสอดคล้อง และเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ

๑.๒ เจ้าของระบบมีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน

๑.๓ ผู้ดูแลระบบมีหน้าที่กำหนดสิทธิให้แก่ผู้ใช้งานตามที่เจ้าของระบบอนุมัติ

๑.๔ ผู้ดูแลระบบมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน สำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๕ ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

๑.๖ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ ต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากเจ้าของระบบ และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

๒. การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนด ดังนี้

๒.๑ สิทธิของผู้ใช้งาน (User) ได้ตามสิทธิการเข้าถึงข้อมูล

๒.๒ สิทธิผู้ดูแลระบบ (Administrator) กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การกำหนดประเภทของข้อมูล ลำดับความสำคัญ ลำดับชั้นความลับ รวมถึงระดับชั้น การเข้าถึงเวลาที่เข้าถึง และช่องทางการเข้าถึง ดังนี้

๓.๑ ลำดับความสำคัญของข้อมูล แบ่งเป็น ๓ ระดับ ดังนี้

๓.๑.๑ สำคัญมากที่สุด

๓.๑.๒ สำคัญมาก

๓.๑.๓ ปกติ

๓.๒ ระดับชั้นการเข้าถึง แบ่งเป็น ๓ ระดับ ดังนี้

๓.๒.๑ กลุ่มผู้บริหาร

๓.๒.๒ กลุ่มผู้ปฏิบัติงาน

๓.๒.๓ กลุ่มประชาชนทั่วไปและผู้ที่เกี่ยวข้อง

๓.๓ ช่องทางการเข้าถึงสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ได้ ๒ ช่องทาง ดังนี้

๓.๓.๑ ระบบเครือข่ายภายใน (Intranet)

๓.๓.๒ ระบบเครือข่ายภายนอก (Internet)

๔. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Business Requirements For Access Control) ดังนี้

๔.๑ เจ้าของระบบอนุมัติสิทธิให้ผู้ใช้งาน ตามภารกิจเพื่อให้สามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ เฉพาะในส่วนที่ได้รับมอบหมาย ตามความเป็นจำเป็นในการทำงาน

๔.๒ ผู้ดูแลระบบกำหนดสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน ตามที่เจ้าของระบบอนุมัติ

หมวดที่ ๒

การบริหารจัดการเข้าถึงของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งานที่ได้รับอนุญาตแล้วและสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

แนวปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้

๑.๑ ผู้รับผิดชอบงานด้านสารสนเทศของหน่วยงานต้องกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ อย่างน้อยประกอบด้วยชื่อ นามสกุล ตำแหน่ง สังกัด และหมายเลขโทรศัพท์

๑.๒ การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

๑.๒.๑ กรณีบุคลากรกลุ่มแผนงาน

(๑) ให้บุคลากรกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๒) ให้หน่วยงานส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้เจ้าของระบบที่ขอใช้งาน

(๓) ให้เจ้าของระบบอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิ ตามที่เจ้าของระบบอนุมัติ พร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๒.๒ กรณีบุคคลภายนอก

(๑) ให้บุคคลภายนอกกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมระบุเหตุผลในการเข้าใช้งาน หรือหนังสือขอเข้าใช้งานจากบริษัท/หน่วยงานต้นสังกัด

(๒) ให้หน่วยงานพิจารณาเหตุผล และดำเนินการส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้เจ้าของระบบที่ขอใช้งาน

(๓) ให้เจ้าของระบบอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิตามที่เจ้าของระบบ อนุมัติพร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้เจ้าของระบบ กำหนด เช่น ชื่อภาษาอังกฤษ หรือบัตรประจำตัวประชาชนตามด้วยเครื่องหมาย “_” หรือ “.” ตามด้วยอักษรนามสกุลตัวแรก หรือลักษณะอื่นใดตามที่เจ้าของระบบ ที่มีการตกลงร่วมกัน

๑.๓.๒ การกำหนดรหัสผ่าน (Password) ต้องมีตัวอักษรภาษาอังกฤษ ตัวเลข และอักขระพิเศษ อย่างน้อย ๘ ตัวขึ้นไป เพื่อยากต่อการคาดเดา

๑.๓.๓ ให้ผู้ดูแลระบบ แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ผู้ใช้งาน ทราบโดยตรง

๑.๓.๔ เมื่อผู้ใช้งาน มีการเปลี่ยนข้อมูลให้แจ้งเจ้าของระบบ เพื่อปรับปรุงข้อมูลผู้ใช้งาน

๑.๓.๕ ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่าน(Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒. การยกเลิกสิทธิการใช้งานของบุคลากร หรือบุคคลภายนอกให้ดำเนินการ ดังนี้

๒.๑ ผู้รับผิดชอบงานด้านสารสนเทศต้องแจ้งเจ้าของระบบ หรือดำเนินการยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก ให้โอน หรือสิ้นสุด การจ้าง

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้ใช้งาน ให้ดำเนินการ ดังนี้

๓.๑ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้ดำเนินการแจ้งผู้รับผิดชอบงานด้านสารสนเทศ เพื่อให้ผู้รับผิดชอบงานด้านสารสนเทศเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๓.๓ ในกรณีที่ผู้ใช้งาน ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สูงกว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อเจ้าของระบบ เพื่อให้ผู้รับผิดชอบงานด้านสารสนเทศเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการ ตามหลักเกณฑ์ ดังนี้

๔.๑ ในกรณีที่ผู้ใช้งาน สิ้นรหัสผ่าน (Password) ให้ขอรับรหัสผ่านใหม่ วิธีการของเจ้าของระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนด เช่น โทรศัพท์ หรือ ออนไลน์

๔.๒ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๑ ปี และรหัสผ่าน (Password) ใหม่ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

๕. ผู้รับผิดชอบงานด้านสารสนเทศ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดสิ้นการจ้าง เพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษาความมั่นคงปลอดภัย ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

หมวดที่ ๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยไม่ได้รับอนุญาต การเปิดเผย การลวงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

แนวปฏิบัติ

๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้

๑.๑ ผู้ใช้งานต้องไม่ใช้รหัสผ่าน (Password) ร่วมกับบุคคลอื่น และไม่ควรให้ระบบคอมพิวเตอร์หรือระบบสารสนเทศจำรหัสผ่าน (Password) ในการเข้าใช้งานโดยอัตโนมัติ

๑.๒ ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่าน (Password) สำหรับการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเก็บเป็นความลับเสมือนเป็นสมบัติส่วนตัว ห้ามจดหรือเขียนรหัสผ่าน (Password) ที่ใช้งานไว้ในที่เปิดเผย

๑.๓ หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็น ในการเข้าถึงหลังจากดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

๑.๔ หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของบัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดแล้ว

๒. ผู้ใช้งานต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ

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

๓.๑ ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ (Asset) ของกลุ่มแผนงาน และให้ใช้งานด้วยความระมัดระวังเสมือนเป็นทรัพย์สินส่วนตน

๓.๒ ผู้ใช้งานต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใด ๆ ที่เครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์พกพา หรือระบบคอมพิวเตอร์และระบบสารสนเทศ ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลต่อผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัด

๓.๓ ผู้ใช้งานต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา หรือการจดความจำในโทรศัพท์มือถือ เพื่อป้องกันการรั่วไหลของข้อมูล

๓.๔ บุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานด้านสารสนเทศ ต้องขออนุมัติเป็นลายลักษณ์อักษรก่อนเข้าปฏิบัติงาน

๓.๕ การทำลายอุปกรณ์บันทึกข้อมูลหรือการนำอุปกรณ์บันทึกข้อมูลกลับมาใช้งานใหม่ให้ดำเนินการ ดังนี้

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

๓.๕.๒ การนำอุปกรณ์บันทึกข้อมูลไปใช้งานใหม่ ให้ฟอร์แมต (Format) อุปกรณ์บันทึกข้อมูลนั้นโดยใช้วิธีการฟอร์แมต (Format) ตามมาตรฐานสากล หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

หมวดที่ ๔

การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายให้มีความมั่นคงปลอดภัย

แนวปฏิบัติ

๑ การเข้าถึงเครือข่ายของผู้ใช้งาน

๑.๑ การใช้งานระบบเครือข่ายภายนอก (Internet) ให้ดำเนินการ ดังนี้

๑.๑.๑ ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดศีลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์เสื่อมเสีย

๑.๑.๒ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของกลุ่มแผนงาน เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๓ ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเคร่งครัด

๑.๑.๔ ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่างๆ เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ โดยแจ้งให้ผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัดทราบก่อนติดตั้งใช้งาน

๑.๒ การใช้งานจดหมายอิเล็กทรอนิกส์ (E – Mail) โดเมนเนม (Domain Name)

๑.๒.๑ ห้ามใช้งานจดหมายอิเล็กทรอนิกส์ (E – Mail) ในทางที่ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศีลธรรม

๑.๒.๒ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจด้วยการใช้งานจดหมายอิเล็กทรอนิกส์ (E – Mail) ที่ส่งโดยโดเมนเนม (Domain Name)

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

๑.๒.๔ หลีกเลี่ยงการใช้งานจดหมายอิเล็กทรอนิกส์ (E – Mail) ต้องออกจากระบบ (Log Out) ทันที

๑.๓ การใช้งานเครือข่ายไร้สาย (WiFi) ให้ดำเนินการ ดังนี้

๑.๓.๑ ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็นของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อใช้งานเครือข่ายไร้สาย (WiFi)

๑.๓.๒ ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็นทรัพย์สินของกลุ่มแผนงานไปใช้งานเครือข่ายไร้สาย (WiFi) ที่ไม่น่าเชื่อถือ

๑.๓.๓ ผู้ใช้งานไม่ควรทำธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ระหว่างการใช้งานเครือข่ายไร้สาย (WiFi) เนื่องจากอาจเกิดความไม่ปลอดภัยและอาจขาดการเชื่อมต่อของสัญญาณ

๑.๓.๔ ห้ามผู้ใช้งานติดตั้งและเปิดการทำงานโปรแกรมดักจับข้อมูล (Network Sniffer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายของกลุ่มแผนงาน และมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๔ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

๑.๔.๑ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของกลุ่มแผนงาน ผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๔.๒ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงต่อไป

๑.๔.๓ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากกลุ่มแผนงาน และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑.๔.๔ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน ต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที

หมวดที่ ๕
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกัน การเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

แนวปฏิบัติ

๑. ผู้ใช้งานต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าถึงระบบปฏิบัติการ
๒. ผู้ใช้งานไม่มีสิทธิ์เปลี่ยนแปลงแก้ไขค่าต่าง ๆ ของระบบปฏิบัติการ เช่น
 - ๒.๑ Product Key หรือ License ของระบบปฏิบัติการ
 - ๒.๒ ค่าคอนฟิกูเรชัน (Configuration) ต่าง ๆ เช่น Computer Name, IP Address เป็นต้น
๓. การจำกัดและควบคุมการใช้งานโปรแกรมมอรรถประโยชน์ (Use of System Utilities) กำหนด ดังนี้
 - ๓.๑ ผู้ใช้งานต้องไม่ดัดแปลงหรือติดตั้งโปรแกรมมอรรถประโยชน์ใด ๆ บนระบบปฏิบัติการ ทั้งนี้ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์ต่อผู้รับผิดชอบด้านสารสนเทศของหน่วยงาน
 - ๓.๒ การใช้งานโปรแกรมมอรรถประโยชน์อื่น ๆ นอกเหนือจากที่ติดตั้งมากับระบบปฏิบัติการ เช่น โปรแกรมดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และโปรแกรม Formatter กำหนดให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่มีสิทธิใช้งาน

หมวดที่ ๖

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control) โดยไม่ได้รับอนุญาต

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งานที่เข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศผ่านเครือข่ายภายนอก ให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN)

๑.๒ การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) รายละเอียดปรากฏตามภาคผนวก

๑.๓ การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking) เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องเข้าถึงในสถานที่ที่มีความปลอดภัยและต้องได้รับอนุญาตจากกลุ่มเทคโนโลยีสารสนเทศ

๓. การควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ให้ดำเนินการ ดังนี้

๓.๑. อุปกรณ์สื่อสารเคลื่อนที่ ได้แก่ Smart Phone และ Tablet ต้องได้รับการยืนยันตัวตนโดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของผู้ใช้งานสำหรับการเข้าใช้งาน

๔.การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) กำหนด ดังนี้

๔.๑ ผู้ใช้งานต้องปฏิบัติตามหมวด ๖ แนวปฏิบัติ ข้อ ๑ การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

๔.๒ เมื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศแล้ว ผู้ใช้งานต้องระมัดระวังไม่ให้ผู้ไม่มีส่วนเกี่ยวข้องเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ สื่อสารเคลื่อนที่ได้ และต้องออกจากระบบ (Log Out) ทันทีเมื่อปฏิบัติเลิกใช้งาน

หมวดที่ ๗
การจัดทำระบบสำรองของระบบสารสนเทศ
(Disaster Recovery Site)

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศและจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกลุ่มแผนงาน ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมฉุกเฉิน และการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่องแม้ในสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่างๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสมและสามารถใช้งานสารสนเทศได้อย่างต่อเนื่อง

แนวปฏิบัติ

๑. ผู้ดูแลระบบจะต้องจัดทำสำรองของระบบสารสนเทศโดยมีขั้นตอน ดังนี้
 - ๑.๑ ผู้ดูแลระบบต้องจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูล และการกู้คืนข้อมูลสารสนเทศ
 - ๑.๒ กำหนดรูปแบบการสำรองข้อมูลระบบสารสนเทศ ดังนี้
 - ๑.๒.๑ คัดเลือกระบบสารสนเทศในการสำรองข้อมูล
 - ๑.๒.๒ กำหนดรูปแบบการสำรองข้อมูล เช่น เฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) แบบสมบูรณ์ (Full Backup)
 - ๑.๒.๓ กำหนดความถี่ในการสำรองข้อมูลตามความเหมาะสมของระบบสารสนเทศ
 - ๑.๓ ผู้ดูแลระบบดำเนินการสำรองของระบบสารสนเทศ ตามข้อที่ ๑.๒
๒. ผู้ดูแลระบบต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศที่สำรองไว้ อย่างน้อย ๑ ระบบ โดยอย่างน้อยปีละ ๑ ครั้ง
๓. ผู้รับผิดชอบงานด้านเทคโนโลยีสารสนเทศต้องดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกลุ่มแผนงาน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่องโดยกำหนดให้ปรับปรุงแผนดังกล่าวทุก ๑ ปี
๔. มีการทบทวนระบบสารสนเทศในการระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๘
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Risk Assessment and Risk Management)

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ทำให้มั่นใจว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนด มีความมั่นคงปลอดภัยและหน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

แนวปฏิบัติ

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

๒. กำหนดแนวทางเพื่อรองรับการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๒.๑ กลุ่มแผนงานต้องอำนวยความสะดวกแก่ผู้ตรวจสอบในการตรวจสอบข้อมูลที่สำคัญ

๒.๒ ในกรณีที่ผู้ตรวจสอบจำเป็นต้องเข้าถึงข้อมูลสำคัญให้กลุ่มแผนงาน สร้างสำเนาสำหรับข้อมูลนั้น โดยให้ผู้ตรวจสอบใช้งานและทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือหากประสงค์จัดเก็บข้อมูลนั้นเป็นหลักฐานให้แจ้งกลุ่มแผนงานเป็นลายลักษณ์อักษร

๒.๓ ในกรณีต้องการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบประเมินความเสี่ยงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้แยกการติดตั้งเครื่องมือออกจากระบบที่ให้บริการจริง หรือระบบที่ใช้ในการพัฒนาและกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่ต้องตรวจสอบได้แบบอ่านได้อย่างเดียว (Read Only)

หมวดที่ ๙

การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพในช่วงระยะเวลาที่เหมาะสม

แนวทางปฏิบัติ

๑. จัดให้มีขั้นตอนหรือกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศที่สำคัญ รวมทั้งกำหนดผู้ที่มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถ และประสบการณ์ โดยมีการกำหนดขั้นตอนและกระบวนการดังต่อไปนี้

๑.๑ การกำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร

๑.๒ การประเมินเหตุการณ์หรือจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

๑.๓ จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ และรายงานเหตุการณ์ ผู้ที่เกี่ยวข้องให้ทราบและดำเนินการต่อไป

๑.๔ การดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อให้เหตุการณ์คลี่คลายหรือกลับสู่ภาวะปกติ

๑.๕ วิเคราะห์ รวบรวมและรายงานเหตุการณ์ต่อผู้บังคับบัญชาทราบ ทั้งนี้ เพื่อระบุถึงสาเหตุการณ์ และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต

๒. ต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ ผ่านบุคคล หรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) โดยให้ดำเนินการดังนี้

๒.๑ แจ้งผู้บังคับบัญชา โดยช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ เช่น Social Network, E-mail เป็นต้น ทั้งนี้ เนื้อหาขั้นต่ำ ต้องประกอบด้วย วันเวลา เหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น

๒.๒ รายงานผู้บังคับบัญชาเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น

- การบุกรุกด้านกายภาพ
- การปฏิบัติงานที่ไม่เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
- การเปลี่ยนแปลง การเข้าถึงโดยไม่ได้รับอนุญาต
- การทำงานผิดของโปรแกรมและอุปกรณ์คอมพิวเตอร์ หรือการปฏิบัติงาน

จัดให้มีบุคคลหรือหน่วยงานงาน (point of contact) เพื่อทำหน้าที่รายงานเหตุการณ์ที่เกิดขึ้นต่อผู้บังคับบัญชา โดยให้รายงานดังต่อไปนี้

รายงานทันทีเมื่อเกิดเหตุ	ระหว่างดำเนินการแก้ไข	แก้ไขปัญหาได้ และเหตุยุติ
1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น 4. ชื่อผู้ติดต่อ/ประสานงานของบริษัทเพื่อให้ข้อมูล	1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น 4. ดำเนินการแก้ไขปัญหาและระยะเวลาในการแก้ไข 5. ความคืบหน้าในการแก้ไขปัญหา	1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น โดยประเมินมูลค่าความเสียหายที่อาจเกิดขึ้น 4. ดำเนินการแก้ไขปัญหา 5. ผลการแก้ไขปัญหา และระยะเวลาในการแก้ไข 6. แนวทางป้องกันในอนาคตและการเก็บรวบรวมหลักฐาน เพื่อระบุสาเหตุและแนวทางแก้ไขต่อไป

รายงานทันทีเมื่อเกิดเหตุ	ระหว่างดำเนินการแก้ไข	แก้ไขปัญหาได้ และเหตุยุติ
รายงานโดยไม่ชักช้า อาจแจ้งด้วยวาจาหรือช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ เมื่อทราบเหตุการณ์และตรวจสอบในเบื้องต้นแล้ว	รายงานโดยไม่ชักช้า อาจแจ้งด้วยวาจาหรือช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ เมื่อทราบเหตุการณ์และตรวจสอบในเบื้องต้นแล้ว	รายงานเป็นลายลักษณ์อักษรโดยมีเนื้อหาจากข้อมูลข้างต้น

ภาคผนวก

การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้รับจ้าง (Outsource)

เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศ ศูนย์ข้อมูลและสารสนเทศ และพื้นที่ปฏิบัติงานทั่วไป ซึ่งเป็นทรัพย์สินที่มีค่าของกลุ่มแผนงาน มีความปลอดภัยต่อการถูกบุกรุกโจมตีและลดความเสี่ยงต่อลักลอบเปิดเผยข้อมูลสารสนเทศ จึงกำหนดแนวปฏิบัติการควบคุมการเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศของผู้รับจ้าง (Outsource) ดังนี้

๑. ก่อนปฏิบัติงาน

๑.๑ ผู้รับจ้าง (Outsource) ต้องขออนุญาตหัวหน้าส่วนราชการนั้น ๆ เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคคลภายนอก ตามหมวดที่ ๒ ข้อปฏิบัติที่ ๑

๑.๒ หัวหน้าส่วนราชการหรือผู้ที่ได้รับมอบหมายพิจารณาเหตุผลการขออนุญาตดังกล่าวและต้องอนุมัติเป็นลายลักษณ์อักษร

๒. ระหว่างปฏิบัติงาน

๒.๑ ผู้รับจ้าง (Outsource) ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน

๒.๒ ผู้รับผิดชอบด้านสารสนเทศหรือผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนราชการต้องกำกับดูแลการปฏิบัติงานของผู้รับจ้าง โดยเฉพาะการติดตั้ง ซ่อมแซม หรือการเปลี่ยนอุปกรณ์ประมวลผลข้อมูล ภายในห้องศูนย์ข้อมูล (Data Center) ต้องกำกับดูแลโดยเคร่งครัด

๒.๓ ผู้รับจ้างต้องปฏิบัติตามหน้าที่ที่ได้รับมอบหมายเท่านั้นและต้องคำนึงถึงการรักษาความลับข้อมูลของทางราชการเป็นสำคัญ หากเกิดปัญหาระหว่างการปฏิบัติงานให้แจ้งผู้รับผิดชอบด้านสารสนเทศหรือผู้ที่ได้รับมอบหมายที่กำกับดูแลการปฏิบัติงานทันที

๓. หลังปฏิบัติงาน

๓.๑ ให้ผู้รับจ้างแจ้งความประสงค์ต่อผู้รับผิดชอบด้านสารสนเทศเพื่อยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศทันทีเมื่อปฏิบัติงานแล้วเสร็จ

๓.๒ ผู้ดูแลระบบ จะยกเลิกสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ และลบข้อมูลสารสนเทศของผู้รับจ้างเป็นการถาวรทันทีเมื่อสิ้นสุดการจ้างงานหรือข้อตกลงร่วมกัน

๔. การรักษาความลับ

ผู้รับจ้างต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงดังกล่าว ต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ