นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2567

สำนักเทคโนโลยีสารสนเทศ

สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของ
สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

เมษายน ๒๕๖๗

ประวัติเอกสาร

เวอร์ชั่น	วันที่	ผู้แก้ไข	สิ่งที่แก้ไข/ดำเนินการ
๑.๐	๒๖ ธันวาคม ๒๕๕๕	นายบุญเกียรติ สวัสดิ์โชติชวลิต	ได้รับความเห็นชอบจาก คณะกรรมการธุรกรรมอิเล็กทรอนิกส์
๑.๑	๒๑ พฤษภาคม ๒๕๕๗	นายบุญเกียรติ สวัสดิ์โชติชวลิต	ทบทวนครั้งที่ ๑ ประจำปี ๒๕๕๗
๒.๐	กันยายน ๒๕๖๒	นายเฟาซี เจ๊ะเต๊ะ	ทบทวนครั้งที่ ๒ ประจำปี ๒๕๖๒
๒.๑	สิงหาคม ๒๕๖๓	นายเฟาซี เจ๊ะเต๊ะ	ทบทวนครั้งที่ ๓ ประจำปี ๒๕๖๓
๒.๒	พฤษภาคม ๒๕๖๖	นายเฟาซี เจ๊ะเต๊ะ	ทบทวนครั้งที่ ๔ ประจำปี ๒๕๖๖
๒.๓	เมษายน ๒๕๖๗	นายเฟาซี เจ๊ะเต๊ะ	ทบทวนครั้งที่ ๕ ประจำปี ๒๕๖๗

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

๑. หลักการและเหตุผล

สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) เล็งเห็นถึงความสำคัญของระบบข้อมูลสารสนเทศและเทคโนโลยีดิจิทัลซึ่งเป็นเครื่องมือสนับสนุนการปฏิบัติงานและการบริหารงานได้อย่างมีประสิทธิภาพ และโดยที่มีการประกาศบังคับใช้กฎหมายที่เกี่ยวกับการพัฒนารัฐบาลดิจิทัลของรัฐบาลได้แก่ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐ พ.ศ.๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันจึงได้จัดทำนโยบายและแนวปฏิบัติฉบับนี้ขึ้น เพื่อใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศลของสถาบันให้มีความมั่นคงปลอดภัยและเชื่อถือได้ สอดคล้องกับกฎหมายที่เกี่ยวข้อง

๒. ความหมายและขอบเขตของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายและแนวปฏิบัติของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จัดทำขึ้นเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศซึ่งครอบคลุมการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลที่อยู่ในความรับผิดชอบของสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) ในขอบเขตดังต่อไปนี้

๒.๑ การรักษาความมั่นคงปลอดภัยของการเข้าถึงข้อมูลและระบบข้อมูล ตลอดจนควบคุมการใช้งานระบบสารสนเทศ ซึ่งครอบคลุมการเข้าถึง ๔ ด้าน ได้แก่

๒.๑.๑ การเข้าถึงระบบเทคโนโลยีสารสนเทศ (Information Access Control)

๒.๑.๒ การเข้าถึงระบบเครือข่าย (Network Access control)

๒.๑.๓ การเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๒.๑.๔ การเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application Access Control)

๒.๒ การจัดให้มีการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๒.๓ การตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละครั้ง

๒.๔ การคุ้มครองข้อมูลส่วนบุคคล

๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๑ การพิจารณาถึงความสำคัญของข้อมูลและระบบข้อมูลต่อพันธกิจและนโยบายของหน่วยงาน และสนับสนุนการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลที่สำคัญ และครอบคลุมขอบเขตที่กฎหมายกำหนด

๓.๒ การเผยแพร่ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้อง

๓.๓ การบริหารจัดการความต่อเนื่องของภารกิจที่หน่วยงานรับผิดชอบ

๓.๔ การมีแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสม กรณีมีการละเมิดหรือฝ่าฝืนนโยบายความมั่นคงปลอดภัย

๓.๕ การนิยามและกำหนดความรับผิดชอบของบุคลากรที่เกี่ยวข้อง ซึ่งประกอบด้วย

๓.๕.๑ ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย แนวทางและมาตรการด้านต่าง ๆ ที่เกี่ยวกับการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร ตลอดจนมาตรการเกี่ยวกับการรักษาความปลอดภัยของข้อมูล ได้แก่ ผู้อำนวยการ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของสถาบันพัฒนาองค์กรชุมชน คณะทำงานพัฒนาระบบข้อมูลสารสนเทศและเทคโนโลยีดิจิทัลและหัวหน้าสำนักเทคโนโลยีสารสนเทศ

๓.๕.๒ ระดับปฏิบัติ รับผิดชอบในการปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และปฏิบัติหน้าที่อื่น ๆ ตามที่ได้รับมอบหมาย ได้แก่ ผู้ดูแลระบบ และ ผู้ปฏิบัติงาน

๓.๖ การจัดทำหรือปรับปรุงนโยบายและแนวทางปฏิบัติ ควรมีการระบุความเสี่ยง มีการประเมินและกำหนดแนวทางจัดการความเสี่ยงนั้น ๆ โดยการประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๓.๖.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๓.๖.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๓.๖.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๓.๗ การปรับปรุงนโยบายและแนวปฏิบัติ ให้มีการทบทวนปรับปรุงอย่างน้อยปีละครั้ง

๓.๘ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายอันตรายใด ๆ แก่สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้ผู้บริหารระดับสูงสุดเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๔. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำหรับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นการจัดทำเอกสารเพื่อกำหนดแนวทางวิธีการในการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องเป็นไปตามนโยบายที่กำหนดไว้ และสามารถนำไปอ้างอิงปฏิบัติได้ โดยแบ่งแนวปฏิบัติออกเป็นส่วน ๆ ดังนี้

ส่วนที่ ๑ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ส่วนที่ ๒ แนวปฏิบัติการควบคุมการเข้าออกห้องสำนักเทคโนโลยีสารสนเทศ

ส่วนที่ ๓ แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๔ แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๕ แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ส่วนที่ ๖ แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ส่วนที่ ๗ แนวปฏิบัติการใช้งานอินเทอร์เน็ต

ส่วนที่ ๘ แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

ส่วนที่ ๙ แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ส่วนที่ ๑๐ แนวปฏิบัติการสำรองข้อมูล

ส่วนที่ ๑๑ แนวปฏิบัติในการสร้างความต่อเนื่องให้กับธุรกิจ

ส่วนที่ ๑๒ แนวปฏิบัติในการประเมินความเสี่ยงเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

ส่วนที่ ๑๓ แนวปฏิบัติการกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๑๔ แนวปฏิบัติการบริหารจัดการรหัสผ่าน

ส่วนที่ ๑๕ แนวปฏิบัติการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๑๖ แนวปฏิบัติการบริหารจัดการครุภัณฑ์คอมพิวเตอร์และเครือข่าย

ส่วนที่ ๑๗ แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑๘ แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย

ส่วนที่ ๑๙ แนวทางปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๒๐ แนวปฏิบัติการควบคุมแอพพลิเคชั่น

ส่วนที่ ๒๑ แนวปฏิบัติเข้ารหัสข้อมูล

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

๑. สถาบัน หมายความว่า สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

๒. ผู้อำนวยการ หมายความว่า ผู้อำนวยการสถาบันพัฒนาองค์กรชุมชน

๓. ผู้บังคับบัญชา หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสถาบัน

๔. สำนักเทคโนโลยีสารสนเทศ หมายความว่า ส่วนงานที่มีหน้าที่ดูแลระบบสารสนเทศของสถาบันตามโครงสร้างของสถาบัน

๕. ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หมายความว่า ผู้ที่ผู้อำนวยการแต่งตั้งให้ดำรงตำแหน่งหรือรักษาการ

๖. ผู้ใช้งาน หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของสถาบันโดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งสถาบันกำหนดไว้ ได้แก่ ผู้บริหาร ผู้ดูแลระบบ ผู้ปฏิบัติงาน องค์กรชุมชน เครือข่ายองค์กรชุมชน และหน่วยงานภายนอก

๗. ผู้บริหาร หมายความว่า ผู้มีอำนาจบริหารในระดับสูงของสถาบัน

๙. ผู้ดูแลระบบ (System Administrator) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

๑๐. ผู้ปฏิบัติงาน หมายความว่า ผู้ปฏิบัติงานตามความในมาตรา ๓๒ แห่งพระราชกฤษฎีกาจัดตั้งสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) พ.ศ. ๒๕๔๓

๑๑. องค์กรชุมชน หมายความว่า กลุ่มคนที่มีระบบการจัดการที่สมาชิกของชุมชนจัดตั้งขึ้นเพื่อดำเนินการร่วมกัน โดยมีวัตถุประสงค์เพื่อประโยชน์ในการประกอบอาชีพ พัฒนาอาชีพ เพิ่มรายได้ พัฒนาที่อยู่อาศัยและสิ่งแวดล้อมหรือพัฒนาชีวิตความเป็นอยู่ของสมาชิกในกลุ่ม

๑๒. เครือข่ายองค์กรชุมชน หมายความว่า กลุ่มองค์กรชุมชนที่มีการรวมตัวกันโดยมีวัตถุประสงค์ที่จะกระทำกิจการอย่างหนึ่งอย่างใด เพื่อประโยชน์ขององค์กรชุมชนในกลุ่มนั้น

๑๓. หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานภายนอกที่สถาบัน อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของสถาบัน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๔. สิทธิของผู้ใช้งาน หมายความว่า สิทธิของผู้ใช้ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและ

การสื่อสาร โดยมีการอนุญาตให้เฉพาะผู้ที่เกี่ยวข้องและมีความจำเป็น

๑๕. ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๖. สารสนเทศ (Information) หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๑๗. ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑๘. ระบบเครือข่าย (Network System) หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสถาบันได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

๑๘.๑ ระบบแลน (LAN) และ ระบบอินทราเน็ต (Intranet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

๑๘.๒ ระบบอินเทอร์เน็ต (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๑๘.๓ ระบบเครือข่ายไร้สาย (Wireless Lan) หมายความว่า ระบบการสื่อสารข้อมูลที่มีรูปแบบในการสื่อสารแบบไม่ใช้สาย โดยใช้การส่งคลื่นความถี่วิทยุ ในการรับและส่งข้อมูลระหว่างคอมพิวเตอร์แต่ละเครื่อง

๑๙. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

๒๐. พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

๒๐.๑ พื้นที่ทำงานทั่วไป (General working area) หมายความว่า พื้นที่ติดตั้งเครื่อง

คอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

๒๐.๒ พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)

๒๐.๓ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)

๒๐.๔ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

๒๐.๕ พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

๒๑. เจ้าของข้อมูล หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๒๒. สินทรัพย์ หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๒๓. จดหมายอิเล็กทรอนิกส์ (e-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

๒๔. รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๒๕. ชุดคำสั่งไม่พึงประสงค์ (Malware) หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เช่น ไวรัส (virus), เวิร์ม (Worm) หรือหนอนคอมพิวเตอร์, มาโทรจัน (Trojan), สปายแวร์ (Spyware) เป็นต้น

๒๖. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การควบคุมบุคคลที่ไม่ได้รับอนุญาตในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก

๒๗. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน ให้เป็นไปตามหลักของการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้าม

ปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

๒๘. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน ทำให้ระบบข้อมูลไม่มีความมั่นคงปลอดภัย หรือสร้างความเสียหายให้แก่สถาบันได้ในลักษณะใดลักษณะหนึ่ง ดังนี้

๒๘.๑ เกิดการหยุดชะงักต่อกระบวนการสำคัญทางธุรกิจ

๒๘.๒ ละเมิดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสถาบัน

๒๘.๓ ละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่าง ๆ ที่สถาบันกำหนดไว้

๒๘.๔ ทำให้สถาบันสูญเสียชื่อเสียง

๒๙. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของสถาบันถูกบุกรุกโจมตี และคุกคามความมั่นคงปลอดภัย

๓๐. การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

๓๑. ภัยคุกคามทางไซเบอร์ (cyber threats) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๓๒. ไซเบอร์ (Cyber) หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

๓๓. หน่วยงานของรัฐ หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

๓๔. ประมวลแนวทางปฏิบัติ หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กาหนด

๓๕. เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

๓๖. มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

๓๗. โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

๓๘. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓๙. หน่วยงานควบคุมหรือกำกับดูแล หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกาหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๔๐. ดิจิทัล หมายความว่า เทคโนโลยีที่ใช้วิธีการนำสัญลักษณ์ศูนย์และหนึ่ง หรือสัญลักษณ์อื่นมาแทนค่าสิ่งทั้งปวง เพื่อใช้สร้างหรือก่อให้เกิดระบบต่าง ๆ เพื่อให้มนุษย์ใช้ประโยชน์

๔๑. รัฐบาลดิจิทัล หมายความว่า การนำเทคโนโลยีดิจิทัลมาใช้เป็นเครื่องมือในการบริหารงานภาครัฐและการบริการสาธารณะ โดยปรับปรุงการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล เพื่อเพิ่มประสิทธิภาพ และอำนวยความสะดวกในการให้บริการประชาชน ในการเปิดเผยข้อมูลภาครัฐต่อสาธารณชน และสร้างการมีส่วนร่วมของทุกภาคส่วน

๔๒. ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

๔๓. ผู้ควบคุมข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๔๔. ผู้ประมวลผลข้อมูลส่วนบุคคล หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

๔๕. บุคคล หมายความว่า บุคคลธรรมดา

๔๖. คณะกรรมการ หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๔๗. พนักงานเจ้าหน้าที่ หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

๔๘. คอมไพเลอร์ หมายความว่า โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น

๔๙. แพตช์ หมายความว่า โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update

๕๐. Recovery Time Objective (RTO) หมายความว่า ระยะเวลาในการกู้คืนระบบ

๕๑. Recovery Point Objective (RPO) หมายความว่า ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

๕๒. Maximum Tolerance Period of Disruption (MTPD) หมายความว่า ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่นภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) ต่อไปนี้เรียกว่า พอช. ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัย ไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

๑.๑ กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

๑.๒ บริการที่สำคัญตามผลการวิเคราะห์ในข้อ ๑.๑

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ พอช. กำหนดให้ต้องมีการประเมินอย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นการเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น รวมถึงให้มีแนวทางในการดำเนินงาน การกำกับดูแลในช่วงสถานการณ์ที่เกิดขึ้นและให้สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที โดยต้องประกอบไปด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑ การประเมินความเสี่ยง (Risk Assessment)

๒.๑.๑ การระบุความเสี่ยง (Risk Identification)

ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

๒.๑.๒ การวิเคราะห์ความเสี่ยง (Risk Analysis)

ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๒.๑.๓ การประเมินค่าความเสี่ยง (Risk Evaluation)

ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงาน รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ยอมรับได้ (Risk Appetite)

๒.๒ การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๒.๓ การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

การติดตามและทบทวนความเสี่ยง ควรมีการดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการ ภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นรวมถึงการแก้ไขปัญหาที่ถูกต้อง และมีประสิทธิภาพ

๒.๔ การรายงานความเสี่ยง (Risk Reporting)

ให้มีการรายงานเหตุการณ์ความเสี่ยง ระดับความเสี่ยง และผลการบริหารความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ พอช.ทุกครั้ง ทั้งนี้ต้องทบทวนระเบียบวิธีปฏิบัติ และกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๓. แผนการรับมือภัยคุกคามทางไซเบอร์

๓.๑ สำนักเทคโนโลยีสารสนเทศ ต้องจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan: CIRP) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๓.๒ ให้มีการตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของ พอช.

๓.๓ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

๓.๔ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของ พอช.

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๑ การจัดการสินทรัพย์ (Asset Management)

๑.๑.๑ จัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของของบริการที่สำคัญ และดูและรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน

๑.๑.๒ ระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๓ มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หรือหากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าว

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๑.๒.๑ ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) และจัดทำทะเบียนประเมินความเสี่ยง

๑.๒.๒ กำหนดปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการประเมินความเสี่ยงที่เกิดขึ้นจากปัจจัยภายนอก เช่น สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๑.๒.๓ ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลักการประเมินความเสี่ยง โดยมีรายละเอียดอย่างน้อย ดังนี้

๑.๒.๔ กำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ ระบุโอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง การระบุผลกระทบของเหตุการณ์ความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้

๑.๒.๕ วิเคราะห์และประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงทรัพย์สินของระบบสารสนเทศที่สำคัญ โดยมีการบริหารจัดการความเสี่ยง ดังนี้

๑.๒.๕.๑ จัดทำแผนการลดความเสี่ยง โดยพิจารณาถึงลำดับความสำคัญในการดำเนินการ ค่าใช้จ่าย ความคุ้มค่า หรือประโยชน์ที่ได้รับ และผู้รับผิดชอบในการดำเนินการ

๑.๒.๕.๒ นำเสนอแผนการลดความเสี่ยงต่อผู้บังคับบัญชาเพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

๑.๒.๕.๓ ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผน และรายงานผลการดำเนินการให้ได้รับทราบเป็นระยะ ๆ จนกระทั่งเสร็จสิ้น

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๑.๓.๑ ติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่าง ๆ ที่มีการใช้งานบนระบบสารสนเทศ หรือจากแหล่งข้อมูลของศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติ หรือจากแหล่งอื่นที่น่าเชื่อถือ

๑.๓.๒ ประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยงของพอช. เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญ

๑.๓.๓ การตรวจสอบขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

๑.๓.๓.๑ การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

๑.๓.๓.๒ การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

๑.๓.๓.๓ ตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๑.๓.๔ การประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใดๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใดๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๑.๓.๕ การทดสอบเจาะระบบ (Penetration Testing) สำหรับบริการที่สำคัญโดยเฉพาะอย่างยิ่งระบบสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง (Internet Facing) เพื่อให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย.

๑.๓.๖ ตรวจสอบขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ

๑.๓.๗ ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง หรือตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบการรักษาความปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๑.๓.๘ ผู้ให้บริการทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ ต้องมีการรับรอง และได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบหรือเป็นไปตามที่กฎหมายกำหนด

๑.๓.๙ การทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบจะต้องดำเนินการภายใต้

การควบคุมดูแลของ พอช.

๑.๓.๑๐ ติดตาม ปรับปรุง และแก้ไข ตามข้อเสนอแนะจากผลการทดสอบเจาะระบบ และจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ พร้อมทั้งตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอแล้ว โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤติ และระดับสูง

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

๑.๔.๑ แจ้งผู้ให้บริการภายนอกได้รับทราบถึงความรับผิดชอบ (Responsible) และภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ว่าผู้ให้บริการภายนอกจะดำเนินการใดๆ ก็ตามในส่วนของบริการที่สำคัญของ พอช.

๑.๔.๒ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

๑.๔.๒.๑ ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญตามความต้องการทางธุรกิจของ พอช. และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๔.๒.๒ ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญ

๑.๔.๒.๓ ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

๑.๔.๒.๔ สิทธิของ พอช. ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก (Right to Audit)

๑.๔.๓ สร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ตามเงื่อนไขที่ระบุในสัญญา เช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

๑.๔.๔ ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับที่เกี่ยวข้อง

๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

๒.๑.๑ การเข้าถึงบริการที่สำคัญของ พอช. ถูกจำกัดไว้ที่

๒.๑.๑.๑ บุคลากร/เจ้าหน้าที่ ที่ปฏิบัติงานให้ พอช.

๒.๑.๑.๒ อุปกรณ์ และอินเทอร์เฟซ (Interface) ของบุคลากร/เจ้าหน้าที่ ที่ปฏิบัติงานให้พอช.

๒.๑.๒ ให้แต่ละบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญของ พอช. ต้องจัดให้มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับ โปรไฟล์ความเสี่ยงด้านการรักษาความ

มั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับ แต่ละโหลดการเข้าถึงบริการที่สำคัญ

๒.๑.๓ เก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๒.๑.๔ ตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางสารสนเทศเท่านั้น และทำภายใต้ การดูและของ พอช.

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๑ สร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญ

๒.๒.๒ มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) มีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

๒.๒.๒.๑ สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒.๒.๒.๒ การแบ่งแยกหน้าที่ (Separation of Duties)

๒.๒.๒.๓ การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๒.๒.๒.๔ การลบบัญชีที่ไม่ได้ใช้

๒.๒.๒.๕ การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Complier) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๒.๒.๒.๖ การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๒.๒.๒.๗ การป้องกันมัลแวร์ (Malware)

๒.๒.๒.๘ การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันต่อเหตุการณ์และเหมาะสม

๒.๒.๓ มีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนจะมีทรัพย์สินใดๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ

๒.๒.๔ ตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อการรับมือกับภัยคุกคามทางไซเบอร์

๒.๒.๕ จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๒.๓.๑ ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ ได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ ต้องปฏิบัติตามแนวทางปฏิบัติ ดังต่อไปนี้

๒.๓.๒.๑ เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็น

๒.๓.๒.๒ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง

๒.๓.๒.๓ ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

๒.๓.๒.๔ ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร.

๒.๓.๒.๕ จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๔.๑ กำหนดมาตรฐานควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์ยคอมพิวเตอร์แบบพกพำ เช่น แล็ปท็อป กับบริการที่สำคัญ โดยปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด เช่น พอร์ต USB ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพำ และเปิดใช้งานเมื่อจำเป็นเท่านั้น กรณีที่ต้องการใช้งานให้แจ้งขึ้นทะเบียนและบันทึกข้อมูล และขออนุมัติการเชื่อมต่อเป็นรำยกรณี พร้อมทั้งมีการตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์พกพำทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ

๒.๔.๒ เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) บทบาทหน้าที่ความรับผิดชอบ กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การประชาสัมพันธ์และสื่อสารผ่านช่องทางต่าง ๆ ที่ พอช.กำหนด ให้กับบุคลากรในหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

ต้องมีการกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล รายละเอียด แนวทางและรูปแบบในการแบ่งปันข้อมูล

๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

มีกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ จัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และวิเคราะห์ภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของ พอช. โดยต้องมีการทบทวนกลไกและกระบวนการ อย่างน้อย ปีละ ๑ ครั้ง

๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ การสื่อสาร การฝึกซ้อม การทบทวน และปรับปรุงตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้การรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง

๔.๓ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

มีการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๕.๑.๑ จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของ พอช. สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อให้พิจารณาความสอดคล้องกับแผนของ พอช. เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลา ที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๕.๑.๒ การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และกำหนด

บริการสำคัญที่ส่งผลกระทบต่อความต่อเนื่องทางธุรกิจ (Business Impact Analysis: BIA)

๕.๑.๓ บริหารแผนความต่อเนื่องทางธุรกิจ (BIA)

๕.๑.๔ ฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องทางธุรกิจ (BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๒. แนวปฏิบัติทั่วไป

๒.๑ ภายในสถาบัน มีการจำแนก และกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม ซึ่งกำหนดอยู่ใน *“แนวปฏิบัติการกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ”* (ส่วนที่ ๑๓) เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๒.๒ ผู้บริหาร ควรกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

๒.๓ ผู้บริหาร ควรกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถมีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน การกำหนดสิทธิประกอบด้วย

๒.๓.๑ การจัดทำ *“แบบฟอร์มทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่”* เพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๓.๒ การบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว

๒.๓.๓ การจัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ และให้มีการปรับปรุงรายการผู้มีสิทธิเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๓. แนวปฏิบัติการควบคุมการเข้า-ออกอาคารสถานที่

๓.๑ ผู้ใช้งาน จะได้รับสิทธิให้เข้า-ออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๓.๒ หากมีบุคคลอื่นใดที่ไม่ใช่ ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการ

ล่วงหน้า หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่ทางราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกรายชื่อบุคคล และการขอเข้าออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

๔. แนวปฏิบัติการควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย

๔.๑ ข้อมูลที่สำคัญมาก เช่น ข้อมูลในกระดาษ ข้อมูลในสื่อหน่วยความจำสำรอง ควรได้รับการปกป้อง (เช่น ในตู้เซฟ หรือในตู้ และอื่น ๆ) เมื่อไม่จำเป็นต้องใช้และเมื่อมีการยกเลิกหรือพ้นจากตำแหน่ง

๔.๒ จุดรับเข้าและส่งออกจดหมาย และเครื่องโทรสารที่ไม่ได้ใช้งานควรได้รับการป้องกัน

๔.๓ เครื่องถ่ายเอกสารและอุปกรณ์ผลิตซ้ำแบบอื่น (เช่น เครื่องสแกนเนอร์ กล้องดิจิตอล) ควรได้รับการปกป้องจากการใช้งานที่ไม่ได้รับอนุญาต

๔.๔ เอกสารที่มีข้อมูลสำคัญควรนำออกจากเครื่องพิมพ์ทันที

ส่วนที่ ๒
แนวปฏิบัติการควบคุมการเข้าออกห้องสำนักเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของสถาบัน โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องสำนักเทคโนโลยีสารสนเทศ

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๒.๑.๑ อนุมัติสิทธิเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๑.๒ อนุมัติกระบวนการควบคุมการเข้า-ออกสำนักเทคโนโลยีสารสนเทศ

๒.๒ ผู้ดูแลระบบ

๒.๒.๑ ตรวจสอบบุคคลที่ขออนุญาตเข้ามาภายในสำนักเทคโนโลยีสารสนเทศให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของสำนักเทคโนโลยีสารสนเทศ อย่างเคร่งครัด

๒.๒.๒ ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกสำนักเทคโนโลยีสารสนเทศ ต้องติด *“บัตรผู้ติดต่อ”* หรือมีการยืนยันตัวตนว่าเป็นผู้ปฏิบัติงานของสถาบัน เท่านั้น

๓. แนวปฏิบัติ

๓.๑ ผู้ดูแลระบบ และผู้ปฏิบัติงานสถาบัน มีแนวปฏิบัติดังนี้

๓.๑.๑ ผู้ดูแลระบบ ควรจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนของงานระบบฐานข้อมูล ส่วนของงานระบบเทคโนโลยี เป็นต้น โดยจัดทำเป็น *“แนวปฏิบัติการกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ”* (ส่วนที่ ๑๓) เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

๓.๑.๒ กรณีผู้ปฏิบัติงานที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้า-ออกสำนักเทคโนโลยีสารสนเทศ ก็ต้องมีการควบคุมอย่างรัดกุม

๓.๑.๓ การเข้าถึงสำนักเทคโนโลยีสารสนเทศ และห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ต้องมีการลงบันทึกการเข้า-ออกไว้เป็นหลักฐาน

๓.๒ ผู้ติดต่อจากหน่วยงานภายนอก มีแนวปฏิบัติดังนี้

๓.๒.๑ ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือ ใบอนุญาตขับขี่กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับ *“บัตรผู้ติดต่อ”*

๓.๒.๒ ผู้ติดต่อจากหน่วยงานภายนอกต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจน

ตลอดเวลาที่อยู่ในสำนักเทคโนโลยีสารสนเทศ

๓.๒.๓ ผู้ติดต่อจากหน่วยงานภายนอกสามารถเข้า-ออกสำนักเทคโนโลยีสารสนเทศ ได้ด้วย *“บัตรผู้ติดต่อ”* โดยสิทธิจะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าปฏิบัติงานภายในสำนักเทคโนโลยีสารสนเทศ

ส่วนที่ ๓
แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตในการเข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบัน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของสถาบันได้อย่างถูกต้อง

๒. หลักการในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๒.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๒.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๓ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

๒.๔ ผู้ดูแลระบบ ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของสถาบัน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ

๒.๕ ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๓. แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓.๑ ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐานตามที่ระบุใน *“แนวปฏิบัติการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ”* (ส่วนที่ ๑๕)

๓.๒ เจ้าของข้อมูลและเจ้าของระบบ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓.๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๔. แนวปฏิบัติการบริหารจัดการการเข้าถึงข้อมูลของผู้ใช้

๔.๑ การลงทะเบียนผู้มีสิทธิหรือยกเลิกสิทธิการใช้ระบบสารสนเทศของสถาบัน กรณีผู้ปฏิบัติงานต้องได้รับการจดแจ้งหรือรับรองเป็นลายลักษณ์อักษร จากหน่วยงานซึ่งมีหน้าที่ดูแลการจ้างงานของสถาบัน

๔.๒ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบ รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ โดยเป็นไปตามที่ระบุใน *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน”* (ส่วนที่ ๑๔)

๔.๓ การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน

๔.๓.๑ ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

๔.๓.๒ การกำหนด การเปลี่ยนแปลง และการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน”* (ส่วนที่ ๑๔)

๔.๓.๓ ต้องกำหนดให้ผู้ใช้เก็บรักษาเอกสารยอมรับที่จะเก็บรักษารหัสผ่านให้เป็นความลับเฉพาะตนและเก็บรหัสผ่านของกลุ่มไว้เฉพาะสมาชิกในกลุ่มเท่านั้น

๔.๓.๔ การส่งรหัสผ่านชั่วคราวให้กับผู้ใช้ให้ใช้วิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลที่สามหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๔.๓.๖ ต้องกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๔.๓.๗ การกำหนดชื่อผู้ใช้หรือรหัส ID ต้องไม่ซ้ำกัน

๔.๓.๘ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยต้องปฏิบัติตาม *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน”* (ส่วนที่ ๑๔)

๔.๓.๘.๑ ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานที่ต้องการ

๔.๓.๘.๒ ต้องควบคุมการใช้งานอย่างเข้มงวดโดยจัดสรรบนพื้นฐานของความจำเป็นเป็นครั้งๆ ไป เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๔.๓.๘.๓ ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๔.๓.๘.๔ ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานให้ทำการเปลี่ยนรหัสผ่านทุก ๓ เดือน หรือกำหนดรหัสผ่านที่มั่นคง รัดกุม และปลอดภัย สอดคล้องตาม“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ ๑๔)

๔.๓.๘.๕ ต้องมีการกำหนดให้ชัดเจนถึงสิทธิพิเศษที่ได้รับว่าการเข้าถึงแต่ละผลิตภัณฑ์ เช่น ซอฟต์แวร์ประเภทระบบปฏิบัติการ ระบบจัดการฐานข้อมูล และโปรแกรมประยุกต์แต่ละตัวสามารถเข้าถึงผลิตภัณฑ์ใดบ้าง

๔.๓.๘.๖ กระบวนการกำหนดสิทธิและการบันทึกการให้สิทธิพิเศษทั้งหมดต้องได้รับการดูแลพิเศษ โดยไม่จัดสรรให้จนกว่ากระบวนการขอสิทธิจะเสร็จสิ้นสมบูรณ์

๔.๓.๘.๗ สิทธิพิเศษของการเข้าถึงนั้นจะจำเป็นเฉพาะในกรณีพิเศษ เช่น เกิดความผิดพลาดในกระบวนการปฏิบัติงาน เป็นต้น

๔.๓.๘.๘ ส่งเสริมให้มีการพัฒนาและใช้โปรแกรมที่ไม่ใช้สิทธิพิเศษในการทำงาน

๔.๓.๘.๙ สิทธิพิเศษต้องได้รับการมอบหมายให้กับรหัสผู้ใช้งานที่ต่างจากรหัสผู้ใช้งานที่ใช้งานตามปกติ

๔.๔ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๔.๔.๑ ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔.๔.๒ กำหนดรายชื่อผู้ใช้และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๔.๕ ผู้ดูแลระบบ จะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ทุกครั้งที่มีการเปลี่ยนแปลงสิทธิและความรับผิดชอบ เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔.๖ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption หรือวิธีอื่นใดที่เหมาะสม

๔.๗ กำหนดให้มีการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ตามที่ระบุไว้ใน *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน”* (ส่วนที่ ๑๔)

๔.๘ กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของสถาบัน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ผู้ใช้งานต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

๕. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ

๕.๑ ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) และโซนสำหรับเครื่องแม่ข่าย (DMZ zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๕.๒ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๓ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน รวมทั้งตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๕.๔ ผู้ดูแลระบบ ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

๕.๕ ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ ตามความจำเป็น

๕.๖ ระบบเครือข่ายทั้งหมดของสถาบันที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสถาบันจะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๕.๗ ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสถาบันในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๕.๘ การเข้าสู่ระบบเครือข่ายและระบบสารสนเทศภายในสถาบัน โดยผ่านทางอินเทอร์เน็ต จำเป็นต้องมีการ login เพื่อการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง และติดตามการเข้าใช้งาน และกระบวนการกำหนดสิทธิ์การเข้าถึงหรือการใช้งานของผู้ใช้งาน (Authorization) โดยระบบจะตรวจสอบสิทธิ์ของผู้ใช้งานและกำหนดการเข้าถึงหรือการใช้งานที่เหมาะสมตามสิทธิ์ที่กำหนดไว้ให้

๕.๙ กำหนดประเภทของข้อมูล ช่องทางและเวลาในการเข้าถึง ดังต่อไปนี้

๕.๙.๑ ข้อมูลที่ผู้ปฏิบัติงานสถาบัน สามารถเข้าถึงได้ตามสิทธิการใช้งานที่ได้รับอนุญาต สามารถใช้งานได้ผ่านระบบแลน (LAN) เครือข่ายไร้สาย (Wi-Fi) อินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet) คือข้อมูลที่อนุญาตให้เจ้าหน้าที่ของสถาบันสามารถเข้าถึงได้ ตลอด ๒๔ ชั่วโมง หรือในเวลาปฏิบัติงาน คือข้อมูลที่ที่เกี่ยวกับการปฏิบัติงาน

๕.๙.๒ ข้อมูลที่ผู้ใช้งานที่ไม่ได้เป็นผู้ปฏิบัติงานของสถาบัน สามารถเข้าถึงข้อมูลที่เกี่ยวข้องกับการดำเนินงานของผู้ใช้งานตามสิทธิการใช้งานที่ได้รับอนุญาต โดยสามารถใช้งานได้ผ่านระบบอินเทอร์เน็ต (Internet) ได้ตลอด ๒๔ ชั่วโมง ภายใต้โดเมน codi.or.th

๕.๑๐ IP address ภายในของระบบงานเครือข่ายภายในของสถาบัน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของสำนักเทคโนโลยีสารสนเทศได้โดยง่าย ซึ่งผู้ดูแลระบบเท่านั้นที่จะเป็นผู้กำหนด IP address ให้กับอุปกรณ์ต่าง ๆ (Fixed IP address)

๕.๑๑ เพื่อให้สามารถระบุอุปกรณ์บนเครือข่ายได้ จะต้องจัดทำแผนผังระบบเครือข่าย (Network

Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ โดยใช้ IP address ในการระบุอุปกรณ์บนเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๑๒ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบและปรับแต่งระบบเครือข่าย จะต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานและช่องทางหรือพอร์ตเฉพาะที่จำเป็นเท่านั้น เช่น Telnet ftp หรือ ping เป็นต้น

๕.๑๓ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ เท่านั้น

๖. แนวปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๖.๑ กำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๖.๒ ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

๖.๓ ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

๖.๔ ดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

๖.๕ ดำเนินการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๖.๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศเท่านั้น

๖.๗ การสำรองค่า config (Configuration Backup) เป็นกระบวนการที่เกี่ยวข้องกับการบันทึกข้อมูลการกำหนดค่า (configuration) ของระบบหรือแอปพลิเคชัน เพื่อใช้ในการเก็บไว้เป็นสำรองหากเกิดปัญหาหรือสูญเสียข้อมูลในการกำหนดค่าหลัก เพื่อให้สามารถกู้คืนการตั้งค่าได้ง่ายและรวดเร็วในกรณีที่เกิดความผิดพลาดหรือภัยคุกคามต่างๆ อีกทั้งยังช่วยให้สามารถเรียกคืนสถานะที่สมบูรณ์ของระบบหรือแอปพลิเคชันในกรณีที่เกิดข้อผิดพลาดร้ายแรงและต้องนำสถานะกลับมาใช้งานก่อนหน้าได้

๗. แนวปฏิบัติการบริหารจัดการการบันทึกและตรวจสอบ

๗.๑ กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall Log เป็นต้น เพื่อประโยชน์การใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๗.๒ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น

ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๘. แนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอกสถาบัน

สำนักเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในสถาบันเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกสถาบัน โดยมีแนวทางปฏิบัติดังนี้

๘.๑ การเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องเชื่อมต่อเครือข่ายผ่าน VPN เท่านั้น เนื่องเป็นการป้องกันระบบเครือข่ายคอมพิวเตอร์ของสถาบันที่อาจก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของสถาบัน การควบคุมบุคคลที่เข้าสู่ระบบของสถาบันจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๘.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๘.๓ ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสถาบันอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๘.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ไม่เปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องถูกตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๘.๖ ผู้ดูแลระบบควรทบทวนสิทธิ์ในการเข้าใช้เครือข่ายภายใน Virtual Private Network (VPN) อย่างน้อย 3 เดือนครั้ง เพื่อให้มั่นใจว่าการเข้าถึงและการใช้งานเครือข่าย VPN ยังคงมีความปลอดภัยและไม่มีการละเมิดสิทธิ์ของผู้ใช้งาน

๙. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกสถาบัน

การเข้าสู่ระบบจากระยะไกล (Remote Access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

๑๐. ข้อกำหนดเกี่ยวกับประเภทของข้อมูล และลำดับชั้นความลับของข้อมูล

๑๐.๑ ประเภทของข้อมูลหรือรูปแบบของเอกสารอิเล็กทรอนิกส์ กำหนดตามมาตรฐานทั่วไปได้ดังนี้

๑๐.๑.๑ รูปแบบเอกสารข้อความ (Text format) ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น

๑๐.๑.๑.๑ TEXT format เป็นไฟล์ที่เก็บเฉพาะตัวอักษร ไม่เก็บลักษณะที่ใช้

๑๐.๑.๑.๒ Document format เป็นไฟล์ที่ผลิตจาก เวิร์ด โปรเซสเซอร์ เช่น ไมโครซอฟท์เวิร์ด ซึ่งไฟล์ประเภทนี้จะเก็บคุณลักษณะของการแสดงผลของเอกสารไว้พร้อมกับตัวอักษร

๑๐.๑.๑.๓ PDF format (Portable Document Format) เป็นไฟล์เอกสารที่ถูกออกแบบให้สามารถเปิดใช้งานกับระบบคอมพิวเตอร์ต่างระบบกันได้ โดยต้องใช้โปรแกรมในการเปิดและการสร้างเอกสารในรูปแบบ PDF

๑๐.๑.๑.๔ XML (Extensible Markup Language) เป็นภาษาที่ใช้สำหรับการ

เขียน Markup document โดยมีการใช้ Metadata เพื่อบอกหน้าที่และประเภทของข้อมูลของส่วนต่าง ๆ ในเอกสารนั้น

๑๐.๑.๒ รูปแบบเอกสารภาพ (Image) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟท์แวร์ มีรูปแบบที่ใช้งาน เช่น

๑๐.๑.๒.๑ JPEG format เป็นรูปแบบที่ออกแบบมาเพื่อเก็บภาพได้หลายสี มีการบีบอัดข้อมูล

๑๐.๑.๒.๒ PNG หรือ GIF formats เป็นรูปแบบที่ออกแบบมาเพื่อเก็บภาพ มีการบีบอัดข้อมูลแบบไม่มีการสูญเสียของคุณภาพ

๑๐.๑.๒.๓ Bitmapping formats เป็นรูปแบบที่ออกแบบมาเพื่อเก็บภาพในรูปแบบอื่น ๆ เป็นจุดของภาพ

๑๐.๒ การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

๑๐.๒.๑ การกำหนดชั้นความลับตามความสำคัญของข้อมูล กำหนดไว้ ๔ ชั้น ได้แก่ ลับที่สุด ลับมาก ลับ และ ปกปิด และมีการกำหนดความรับผิดชอบให้แก่ผู้มีอำนาจกำหนดชั้นความลับเป็นผู้พิจารณากำหนะระดับชั้นความลับของเอกสาร และการยกเลิก หรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

๑๐.๒.๒ การควบคุมเอกสาร กำหนดให้มีมาตรการควบคุมต่าง ๆ คือ การลงทะเบียน การดำเนินการ การส่ง การเก็บรักษา การแจกจ่ายเอกสาร ระดับชั้นการเข้าถึง และการทำลายให้เป็นไปโดยถูกต้อง กรณีที่เป็นหนังสือลับ กำหนดให้ สำนักผู้อำนวยการ เป็นผู้รับผิดชอบในการดำเนินการเกี่ยวกับหนังสือลับเท่านั้น

๑๐.๒.๓ การเข้ารหัส หรือการถอดรหัสข้อมูลข่าวสารลับ ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๑๐.๓ การทำลายสื่อบันทึกข้อมูล หรือการทำลายข้อมูลในสื่อชนิดต่าง ๆ ให้ปฏิบัติตามแนวทางดังต่อไปนี้

๑๐.๓.๑ สื่อบันทึกข้อมูลประเภทกระดาษ ให้ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร

๑๐.๓.๒ สื่อบันทึกข้อมูลประเภท Flash Drive ให้ใช้วิธีการทุบหรือบดให้เสียเสียหาย

๑๐.๓.๓ สื่อบันทึกข้อมูลประเภทแผ่น CD/DVD ให้ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร

๑๐.๓.๔ สื่อบันทึกข้อมูลประเภทฮาร์ดดิสก์ ให้พิจารณาเลือกใช้วิธีการทำลายข้อมูลบนฮาร์ดดิสก์ตามความสำคัญของข้อมูลที่บันทึกหรือจัดเก็บ ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ที่ได้รับการยอมรับ ได้แก่ Fill Sectors With Zero/One, DOD 5220.22 M หรือ NSA เป็นต้น

ส่วนที่ ๔
แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกหรือบุคลากรฝ่ายสนับสนุนอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสถาบัน ให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบ การใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

๒. แนวปฏิบัติ

๒.๑ หัวหน้าสำนักเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้

๒.๒ ในการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือบุคลากรฝ่ายสนับสนุนต้องปฏิบัติตามแนวทางดังต่อไปนี้

๒.๒.๑ บุคคลจากหน่วยงานภายนอกหรือบุคลากรฝ่ายสนับสนุนที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสถาบันจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากหัวหน้าสำนักเทคโนโลยีสารสนเทศ

๒.๒.๒ ผู้ขอใช้ระบบต้องกรอกข้อมูลลงใน *“แบบฟอร์มการขออนุญาตเข้าใช้งานระบบสารสนเทศ สำหรับหน่วยงานภายนอก”* ซึ่งต้องมีรายละเอียดอย่างน้อยดังนี้

๒.๒.๒.๑ เหตุผลในการขอใช้

๒.๒.๒.๒ ระยะเวลาในการใช้

๒.๒.๒.๓ การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๒.๒.๒.๔ การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

๒.๒.๒.๕ การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูลแล้วจึงยื่นคำขอให้กับเจ้าหน้าที่ผู้รับผิดชอบดำเนินการพิจารณาตามขั้นตอน

๒.๒.๓ หน่วยงานภายนอกที่ทำงานให้กับสถาบันทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในสถาบันหรือนอกสถานที่จำเป็นต้องลงนามใน *“สัญญาการไม่เปิดเผยข้อมูลของสถาบัน”* โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๒.๒.๔ หลังจากที่ผู้ขอใช้งานระบบจากหน่วยงานภายนอกผ่านการอนุมัติสิทธิเข้าใช้งานระบบแล้ว เจ้าหน้าที่ผู้กำหนดสิทธิการใช้งานระบบจะเป็นผู้กำหนดบัญชีรายชื่อ และรหัสผ่านชั่วคราว โดยระบุลงใน *“แบบฟอร์มกำหนดสิทธิการเข้าใช้ระบบสารสนเทศ”* แล้วแจ้งให้ผู้ขอใช้งานระบบจากหน่วยงาน

ภายนอกมารับเอกสารดังกล่าว โดยลงลายมือชื่อรับเอกสาร โดยผู้ขอใช้ต้องเก็บเอกสารดังกล่าวเป็นความลับ และทำการเปลี่ยนแปลงรหัสผ่านเมื่อเข้าใช้งานระบบในครั้งแรก ซึ่งรหัสผ่านที่ผู้ขอใช้งานระบบกำหนดขึ้นมาใหม่ต้องเป็นไปตามแนวปฏิบัติของเอกสาร *“การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”*

๒.๒.๕ สถาบันจะต้องเข้าไปประเมินความเสี่ยงหน่วยงานภายนอก ทั้งนี้ ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศที่เข้าไปปฏิบัติงาน โดยใช้แนวนโยบายตาม *“แนวปฏิบัติในการประเมินความเสี่ยงเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” (ส่วนที่ ๑๒)*

๒.๒.๖ เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามใน *“สัญญาการไม่เปิดเผยข้อมูลของสถาบัน”*

๒.๒.๗ สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของสถาบัน ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๒.๒.๘ สถาบันมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจได้ว่าสถาบันสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๒.๒.๙ ผู้ให้บริการจากหน่วยงานภายนอกจะต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ ๕
แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๑. วัตถุประสงค์

นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล ผู้ใช้งานจะต้องทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของสถาบันให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

๒. แนวปฏิบัติทั่วไป

๒.๑ เครื่องคอมพิวเตอร์ที่สถาบันอนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินของสถาบัน ดังนั้นผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์ของสถาบันอย่างมีประสิทธิภาพเพื่องานของสถาบัน

๒.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของสถาบัน ต้องเป็นโปรแกรมที่สถาบันได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมใด ๆ ในเครื่องคอมพิวเตอร์ส่วนบุคคลของสถาบัน เว้นแต่ได้รับอนุญาตจากเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศเป็นที่เรียบร้อย

๒.๔ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคลของสถาบันจะต้องกำหนดโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ เท่านั้น

๒.๕ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลของสถาบันตรวจซ่อมจะต้องได้รับความเห็นและตรวจสอบเบื้องต้นโดยเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศหรือเจ้าหน้าที่พัสดุก่อนเท่านั้น ทั้งนี้ผู้ใช้งาน จะต้องดำเนินการสำรองข้อมูล และลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อนทุกครั้ง

๒.๖ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๒.๗ ไม่เก็บข้อมูลสำคัญของสถาบันไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่ เว้นแต่จัดเก็บไว้บนระบบคลาวด์ Microsoft OneDrive ที่เป็นลิขสิทธิ์ของสถาบัน

๒.๘ เพื่อรักษาความปลอดภัยของคอมพิวเตอร์จากการใช้งานที่ไม่ถูกต้อง ผู้ใช้งานอาจจะต้องล็อกเครื่องคอมพิวเตอร์ หรือการควบคุมแบบอื่น ๆ เช่น ให้ใส่รหัสผ่าน เมื่อไม่ได้ใช้งาน

๒.๙ ไม่นำ อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ อยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๒.๑๐ ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์ส่วนบุคคล

๓. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๓.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ

เข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ให้แจ้งผู้ดูแลระบบทำการแก้ไขทันที

๓.๓ ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

๓.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๓.๕ ผู้ใช้งานต้องปิดระบบหรือเซสชั่นที่ใช้งานเสร็จแล้ว ไม่เช่นนั้นก็ต้องใช้กลไกป้องกันการเข้าถึงระบบของระบบปฏิบัติการเป็นตัวล็อค เพื่อไม่ให้ผู้ที่ไม่มีสิทธิใช้งานซึ่งไม่ทราบชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เข้าใช้งานเครื่องคอมพิวเตอร์

๓.๖ ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้งานต้อง logout ออกจากเครื่องคอมพิวเตอร์ หรือล็อคหน้าจอ หรือได้รับการป้องกันจากการใช้หน้าจอและคีย์บอร์ด หรือการตรวจสอบและยืนยันตัวตนแบบอื่น ที่ไม่ใช่แต่เพียงปิดหน้าจอเท่านั้น

๔. แนวปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน *“แนวปฏิบัติการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ” (ส่วนที่ ๑๕)* และ *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ ๑๔)*

๕. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๕.๑ ผู้ใช้งานต้องทำการอัพเดท (update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ รวมทั้งโปรแกรมป้องกันไวรัส (Antivirus) อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๕.๒ ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์

๕.๓ ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกพกพาต่าง ๆ เช่น ฮาร์ดดิสก์แบบติดตั้งภายนอก (External Hard Disk) ธัมบ์ไดรฟ์ (Thumb Drive) ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๕.๔ ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๕.๕ ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๖. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

๖.๑ ผู้ใช้งาน ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น ฮาร์ดดิสก์แบบติดตั้งภายนอก หรือบันทึกไว้บน Microsoft OneDrive เพื่อป้องกันการสูญหายของข้อมูล

๖.๒ ผู้ใช้งาน ต้องเก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อ

การรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๖.๓ ผู้ใช้งาน ต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บนฮาร์ดดิสก์ประจำเครื่อง ต้องไม่เป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหากฮาร์ดดิสก์เสียไปก็ไม่กระทบต่อการดำเนินการของสถาบัน

๖.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

ส่วนที่ ๖
แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกสถาบัน รวมทั้งเป็นมาตรการป้องกันข้อมูลและอุปกรณ์ของสถาบันให้เกิดความปลอดภัย ผู้ใช้งานจะต้องรับทราบถึงข้อกำหนดและแนวปฏิบัติในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยง เพื่อให้ผู้ใช้งานสามารถใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

๒. แนวปฏิบัติทั่วไป

๒.๑ เครื่องคอมพิวเตอร์แบบพกพาที่สถาบันอนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินของสถาบัน ดังนั้น ผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาของสถาบันอย่างมีประสิทธิภาพเพื่องานของสถาบัน

๒.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของสถาบัน ต้องเป็นโปรแกรมที่สถาบันได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมใด ๆ ในเครื่องคอมพิวเตอร์แบบพกพาของสถาบัน

๒.๔ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพาของสถาบันจะต้องกำหนดโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ เท่านั้น

๒.๕ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาของสถาบันตรวจซ่อมจะต้องได้รับความเห็นและตรวจสอบเบื้องต้นโดยเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศก่อน เท่านั้น ทั้งนี้ผู้ใช้งาน จะต้องดำเนินการสำรองข้อมูล และลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อนทุกครั้ง

๒.๖ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๒.๗ ไม่เก็บข้อมูลสำคัญของสถาบันไว้บนเครื่องคอมพิวเตอร์แบบพกพาที่ท่านใช้งานอยู่ เว้นแต่จัดเก็บบนระบบคลาวด์ Microsoft OneDrive ที่เป็นลิขสิทธิ์ของสถาบัน

๒.๘ เพื่อรักษาความปลอดภัยของคอมพิวเตอร์จากการใช้งานที่ไม่ถูกต้อง ผู้ใช้งานอาจจะใช้กุญแจล็อกหรือการควบคุมแบบอื่น ๆ เช่น ให้ใส่รหัสผ่าน เมื่อไม่ได้ใช้งาน

๒.๙ ผู้ใช้งาน ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๒.๑๐ ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๒.๑๑ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

๒.๑๒ ไม่ใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

๒.๑๓ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๒.๑๔ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๒.๑๕ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๒.๑๖ ไม่เคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน

๒.๑๗ ไม่ใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

๒.๑๘ ไม่ใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๒.๑๙ ไม่ติดตั้ง หรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

๓. แนวปฏิบัติด้านความปลอดภัยทางกายภาพ

๓.๑ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๓.๒ ผู้ใช้งานต้องไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๓.๓ ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่

๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๔.๑ ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๔.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ให้แจ้งผู้ดูแลระบบทำการแก้ไขทันที

๔.๓ ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ ๑๕ นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

๔.๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๔.๕ ผู้ใช้งานต้องปิดระบบหรือเซสชั่นที่ใช้งานเสร็จแล้ว ไม่เช่นนั้นก็ต้องใช้กลไกป้องกันการเข้าถึง

ระบบของระบบปฏิบัติการเป็นตัวล็อค เพื่อไม่ให้ผู้ที่ไม่มีสิทธิใช้งานซึ่งไม่ทราบชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) เข้าใช้งานเครื่องคอมพิวเตอร์

๔.๖ ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้งานต้อง logout ออกจากเครื่องคอมพิวเตอร์ หรือล็อคหน้าจอด้วยโปรแกรม Screen saver หรือได้รับการป้องกันจากการใช้หน้าจอและคีย์บอร์ด หรือการป้องกันโดยใช้รหัสผ่านอุปกรณ์ Token หรือการตรวจสอบและยืนยันตัวตนแบบอื่น ที่ไม่ใช่แต่เพียงปิดหน้าจอเท่านั้น

๕. แนวปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้งานปฏิบัติตาม แนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน *“แนวปฏิบัติการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ” (ส่วนที่ ๑๕)* และ *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ ๑๔)*

๖. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๖.๑ ผู้ใช้งานต้องทำการอัพเดท (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ รวมทั้งโปรแกรมป้องกันไวรัส (Antivirus) อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๖.๒ ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์

๖.๓ ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกพกพาต่าง ๆ เช่น ฮาร์ดดิสก์แบบติดตั้งภายนอก (External Hard disk) ธัมบ์ไดรฟ์ (Thumb drive) ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๖.๔ ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๖.๕ ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๖.๖ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

๗. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

๗.๑ ผู้ใช้งาน ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาไว้บนสื่อบันทึกอื่น ๆ เช่น ระบบคลาวด์ Microsoft OneDrive หรือ ฮาร์ดดิสก์แบบติดตั้งภายนอก เพื่อป้องกันการสูญหายของข้อมูล

๗.๒ ผู้ใช้งาน ต้องเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๗.๓ ผู้ใช้งาน ต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บนฮาร์ดดิสก์ประจำเครื่อง ต้องไม่เป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหากฮาร์ดดิสก์เสียไปก็ไม่กระทบต่อการดำเนินการของสถาบัน

๗.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

ส่วนที่ ๗
แนวปฏิบัติการใช้งานอินเทอร์เน็ต

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของสถาบันถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

๒.๑ ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สถาบันจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เครือข่ายอินเทอร์เน็ตไร้สายของสถาบัน เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Wireless Router ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรแล้ว

๒.๒ ก่อนที่จะนำเครื่องคอมพิวเตอร์ส่วนบุคคลเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ เว็บเบราเซอร์

๒.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต ผู้ใช้งานต้องทำการทดสอบไวรัส (Virus scanning) โดยใช้โปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง และควรหมั่นตรวจสอบการ Update ระบบปฏิบัติการและการตั้งค่าเบราว์เซอร์อุปกรณ์ต่างให้ทันสมัยอยู่เสมอ

๒.๔ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของสถาบันเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่มีความเสี่ยงที่จะก่อให้เกิดปัญหาทางความมั่นคงปลอดภัยแก่ผู้ใช้งาน เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๒.๕ ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของสถาบัน

๒.๖ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสถาบัน

๒.๗ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสถาบันที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๒.๘ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๒.๙ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๒.๑๐ ผู้ใช้งานต้องมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๒.๑๑ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๒.๑๒ ในการใช้งานโซเชียลมีเดีย (Social Media) ของสถาบัน ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสถาบัน

๒.๑๓ ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสถาบัน การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

๒.๑๔ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ส่วนที่ ๘
แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของสถาบัน ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวปฏิบัติ

๒.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

๒.๒ สำนักทรัพยากรบุคคล จะจัดส่งรายชื่อเจ้าหน้าที่ใหม่ให้กับสำนักเทคโนโลยีสารสนเทศเพื่อดำเนินการกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน

๒.๓ ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน

๒.๔ ผู้ใช้งานต้องกำหนดรหัสผ่านที่ดี (Good Password) ตามแนวปฏิบัติที่ระบุไว้ใน *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ ๑๔)*

๒.๕ ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน ๓ ครั้ง

๒.๖ ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการ logout ออกจากหน้าจอตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

๒.๗ ผู้ใช้งานไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) ของระบบจดหมายอิเล็กทรอนิกส์

๒.๘ ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๖ เดือน เป็นตามความสมัครใจไม่บังคับเปลี่ยน โดยขอให้ผู้ใช้งานกำหนดรหัสผ่านที่มั่นคง รัดกุม และปลอดภัย สอดคล้องตาม *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ ๑๔)*

๒.๙ ผู้ใช้งานควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อสถาบัน หรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

ของสถาบัน

๒.๑๐ ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่น เพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๒.๑๑ ผู้ใช้งานควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของสถาบัน เพื่อการทำงานของสถาบันเท่านั้น การให้บริการจดหมายอิเล็กทรอนิกส์ของสถาบัน สงวนสิทธิให้ผู้ใช้งาน ใช้เพื่อติดต่อสื่อสารทั่วไป ห้ามนำไปใช้ในเชิงการค้าเพื่อประโยชน์ส่วนบุคคล

๒.๑๒ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานควรทำการ logout ออกจากระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๒.๑๓ ผู้ใช้งานควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

๒.๑๔ ผู้ใช้งานไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๒.๑๕ ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของสถาบัน ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

๒.๑๖ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒.๑๗ ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๒.๑๘ ผู้ใช้งานควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๒.๑๙ ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้น ไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในกล่องจดหมายอิเล็กทรอนิกส์

๒.๒๐ ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ ควรให้ความรู้เกี่ยวกับการรักษาความปลอดภัยในจดหมายอิเล็กทรอนิกส์แก่ผู้ใช้งานจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ การให้ความรู้ถือเป็นการป้องกันเบื้องต้นเพื่อมิให้ผู้ใช้งานตกเป็นเหยื่อของผู้ไม่หวังดี และเป็นการป้องกันไม่ให้เกิดปัญหาในกรณีที่ทำผิดพลาดแม้เพียงครั้งเดียว อาจส่งผลกระทบทำให้ระบบไม่สามารถทำงานได้

๒.๒๑ ในการใช้จดหมายอิเล็กทรอนิกส์ในการติดต่อสื่อสารนั้น ผู้ใช้งานควรให้เกียรติกับผู้รับปลายทางเหมือนการสนทนาด้วยวาจา ควรตรวจสอบตัวสะกดไวยากรณ์ อ่านทวนเนื้อหาก่อนส่ง ใช้ข้อความที่กระชับเข้าถึงประเด็นอย่างรวดเร็ว แต่ข้อความต้องไม่สั้นเกินจนดูแล้วห้วน และให้ตระหนักอยู่เสมอว่าข้อความใด ๆ ที่ส่งผ่านเครือข่ายอินเทอร์เน็ตนั้นเป็นข้อความที่สามารถมองเห็น และอ่านได้โดยผู้อื่น ดังนั้น

การส่งข้อความที่เป็นความลับจะต้องใช้ซอฟท์แวร์หรือฮาร์ดแวร์เพื่อเข้ารหัสข้อมูลนั้นก่อนส่งออกไป

๒.๒๒ ผู้ใช้งานต้องไม่ทำการเปลี่ยนแปลง หรือแก้ไขข้อความจดหมายอิเล็กทรอนิกส์ต้นฉบับที่ได้รับมาและต้องการส่งต่อไป หากจดหมายอิเล็กทรอนิกส์นั้นถูกส่งถึงผู้รับเป็นการส่วนตัว ต้องขออนุญาตผู้ส่งก่อนที่จะส่งต่อจดหมายอิเล็กทรอนิกส์นั้นไปจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคล ควรได้รับการเข้ารหัสอย่างปลอดภัย (Encryption)

๒.๒๓ ผู้ใช้งานควรใส่ชื่อหัวข้อเรื่องใน Subject ของจดหมายอิเล็กทรอนิกส์ เพื่อแสดงถึงเรื่องของจดหมายอิเล็กทรอนิกส์ที่ต้องการหารือหรือแจ้งให้ทราบ และควรส่งจดหมายอิเล็กทรอนิกส์ตอบกลับสั้น ๆ หากไม่มีเวลาพอเพื่อให้ผู้ส่งได้รับทราบว่าผู้รับได้รับจดหมายอิเล็กทรอนิกส์นั้นแล้ว และจะตอบกลับอย่างสมบูรณ์ในภายหลัง

๒.๒๔ ผู้ใช้งานต้องไม่ส่งต่อจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่ไม่สมควรทำบนเครือข่ายอินเทอร์เน็ต จดหมายชี้ชวน หรือ อื่น ๆ อันเป็นการกระทำที่เข้าข่าย spam หรือ unsolicited electronic mail อย่างเด็ดขาด หากได้รับจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ และมีข้อความขอให้ส่งต่อจดหมายอิเล็กทรอนิกส์นั้นให้ติดต่อหรือแจ้งผู้ดูแลระบบโดยทันที

๒.๒๕ ผู้ใช้งานไม่ควรส่งจดหมายอิเล็กทรอนิกส์ที่เกี่ยวกับการล่วงละเมิดหรือข่มขู่ หรือมีเนื้อหาข้อความที่ขัดต่อกฎหมายและศีลธรรม และใช้จดหมายอิเล็กทรอนิกส์เป็นเครื่องมือในการกระจายข่าวสาร เว้นแต่เป็นการประกาศที่เหมาะสม

๒.๒๖ ผู้ใช้งานควรพิจารณาใช้ “BCC” (Blind Carbon Copy – สำเนาโดยที่ผู้รับไม่ทราบ) ในการส่งจดหมายอิเล็กทรอนิกส์ถึงผู้รับเป็นจำนวนมาก เพื่อไม่ให้รายชื่อผู้รับทั้งหมดปรากฏในลักษณะที่ยาวมากเกินไป

๒.๒๗ ผู้ใช้งานควรทำตามนโยบายอย่างเคร่งครัด และแจ้งผู้ดูแลระบบเมื่อพบการใช้จดหมายอิเล็กทรอนิกส์ที่ไม่ถูกต้อง

๒.๒๘ ผู้ใช้งานต้องกรอกข้อมูลในช่องข้อมูลส่วนตัว (Identity) โดยจะต้องใช้ชื่อผู้ส่ง (Sender) ที่เป็นจริง ตามที่มีบัญชีรายชื่ออยู่จริง เพื่อให้สามารถอ้างอิงในกรณีที่มีปัญหาเกิดขึ้น

๒.๒๙ ผู้ใช้งานต้องไม่ตั้งชื่อผู้ส่ง (Sender) หรือข้อมูลอื่น ในลักษณะที่ส่อว่าเป็นผู้ดูแลระบบ (Administrator) เช่น webmaster, host master, administrator, admin, postmaster เป็นต้น โดยไม่ได้รับอนุญาต

๒.๓๐ ผู้ใช้บริการมีหน้าที่จะต้องรักษาชื่อผู้ใช้งาน และรหัสผ่านเป็นความลับ ไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๒.๓๑ จดหมายของผู้ใช้บริการ ถือเป็นข้อมูลส่วนบุคคล ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ไม่สามารถจะทำการเก็บ กู้ หรือดึงข้อมูลส่วนตัวขึ้นมาได้ ดังนั้นผู้ใช้บริการจะต้องดูแลรักษาข้อมูลดังกล่าวอย่างระมัดระวัง โดยเฉพาะการลบจดหมายที่ไม่ต้องการ รวมทั้งจะต้องดูแลรักษาไม่ให้ขนาดของจดหมายที่จัดเก็บเกินกว่าจำนวนพื้นที่ที่ได้รับอนุญาต

๒.๓๒ ผู้ใช้งานต้องมีความรับผิดชอบ และระมัดระวังในการใช้บริการตามสมควร ไม่ให้ล่วงละเมิด

บุคคลอื่น รวมถึงศีลธรรม หรือกฎหมายใด ๆ อันเป็นผลให้เกิดความไม่สงบเรียบร้อยในสถาบันและสังคม

๒.๓๓ ในกรณีที่ทางสำนักเทคโนโลยีสารสนเทศ ตรวจพบว่า ผู้ใช้งานได้ละเมิดข้อกำหนดการใช้งานระบบจดหมายอิเล็กทรอนิกส์ จะทำการระงับการให้บริการและทำการตรวจสอบทันที เพื่อเป็นการรักษาผลประโยชน์ของผู้ใช้บริการโดยส่วนรวม และของสถาบัน อีกทั้งในกรณีที่การละเมิดดังกล่าว เป็นการกระทำอันขัดต่อกฎหมายจะต้องได้รับโทษตามที่ระบุไว้ ทั้งนี้ การใช้งานระบบจดหมายอิเล็กทรอนิกส์ของทางสำนักเทคโนโลยีสารสนเทศ จะถือว่าผู้ที่ใช้ ได้รับทราบ ทำความเข้าใจ และได้ยอมรับข้อกำหนดตามที่ระบุในฉบับนี้แล้ว

๒.๓๔ กรณีเจ้าหน้าที่ลาออก ให้สำนักทรัพยากรบุคคลแจ้งให้สำนักเทคโนโลยีสารสนเทศทราบและผู้ดูแลระบบต้องทำการลบบัญชีผู้ใช้งาน ภายใน ๓ วัน

ส่วนที่ ๙
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของสถาบัน โดยการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. แนวปฏิบัติ

๒.๑ บทบาทหน้าที่ของผู้ดูแลระบบ

๒.๑.๑ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๑.๒ ผู้ดูแลระบบจะต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๒.๑.๓ ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

๒.๑.๔ ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (default) มาจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

๒.๑.๕ ผู้ดูแลระบบควรเปลี่ยนค่าชื่อ login และรหัสผ่าน สำหรับการตั้งค่าการทำงานของอุปกรณ์ ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๒.๑.๖ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ Access Point เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

๒.๑.๗ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ (User name) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address และชื่อผู้ใช้รหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

๒.๑.๘ ผู้ดูแลระบบควรจะมีการติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในสถาบัน

๒.๑.๙ ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับช่องสัญญาณ SSID (Service Set Identifier) ที่กำหนดไว้เท่านั้น เพื่อช่วยป้องกันการโจมตี

๒.๑.๑๐ ผู้ดูแลระบบควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

๒.๑.๑๑ ผู้ดูแลระบบควรทบทวนชื่อบัญชีผู้ใช้งานในระบบเพื่อป้องกันการใช้งานเครือข่ายไร้สายที่ไม่ได้รับอนุญาติ

๒.๒ ผู้ใช้งานทั้งที่เป็นผู้ปฏิบัติงานสถาบันและไม่ใช่ผู้ปฏิบัติงาน ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของสถาบัน ต้องมีการยืนยันตัวตนตามระบบที่สถาบันกำหนด

ส่วนที่ ๑๐
แนวปฏิบัติในการสำรองข้อมูล

๑. วัตถุประสงค์

เพื่อให้ระบบสารสนเทศของสถาบันสามารถดำเนินการได้อย่างต่อเนื่อง ข้อมูลไม่สูญหาย ในกรณีที่เกิดความเสียหายต่ออุปกรณ์คอมพิวเตอร์ และเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งเป็นที่จัดเก็บข้อมูลงานสำคัญและระบบฐานข้อมูล

๒. ระบบสารสนเทศที่มีความจำเป็นในการสำรองข้อมูล

ระบบสารสนเทศทุกระบบ จะต้องมีการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้องครบถ้วน ทั้ง ระบบซอฟท์แวร์ และข้อมูลในทุกระบบข้อมูล แยกตามระบบสารสนเทศแต่ละระบบ ซึ่งมีขั้นตอนปฏิบัติดังต่อไปนี้

๒.๑ ระบบซอฟท์แวร์ จะทำการสำรองข้อมูลทุกครั้งที่มีการแก้ไขหรือปรับปรุงระบบ หรืออย่างน้อยเดือนละ ๑ ครั้ง

๒.๒ ระบบข้อมูล จะทำการสำรองข้อมูลทุกวัน โดยเลือกช่วงเวลาที่มีการใช้งานน้อยที่สุดหรือไม่มีการใช้งานเพื่อไม่ให้กระทบต่อการทำงานของผู้ใช้งาน

๒.๓ การสำรองข้อมูล จะทำการสำรองแบบ Full Backup และไม่ควรจัดเก็บไว้ในที่เดียวกับระบบข้อมูล

๒.๔ การสำรองข้อมูลทุกครั้งจะต้องทำการตรวจสอบความถูกต้องของข้อมูลที่ทำการสำรอง

๒.๕ ระบบซอฟท์แวร์และข้อมูลที่ทำการสำรอง จะถูกรวบรวมเพื่อนำไปเก็บรักษาไว้ที่ *“สถานที่เก็บข้อมูลสำรอง”* เป็นประจำทุกเดือน

๓. รูปแบบข้อมูลที่สำรอง

ข้อมูลที่สำรองในแต่ละระบบตามขั้นตอนที่กำหนดไว้ข้างต้นแล้ว แปลงให้อยู่ในรูปแบบบีบอัดข้อมูลเป็นแฟ้มข้อมูลเดียวของแต่ละระบบโดยใช้มาตรฐานการบีบอัดข้อมูลแบบ ZIP และอาจจะมีการตรวจสอบความถูกต้องของข้อมูลเพื่อสร้างความเชื่อมั่นในความถูกต้องของข้อมูล ซึ่งอาจจะมีการสร้างลายมือชื่ออิเล็กทรอนิกส์โดยใช้มาตรฐาน XML Signature และเพื่อรักษาความลับของข้อมูลนั้นให้มีการเข้ารหัสโดยใช้รูปแบบข้อมูล XML Encryption

๔. สถานที่เก็บข้อมูลสำรอง

การเก็บข้อมูลที่สำรองนั้นต้องถูกจัดเก็บในสื่อเก็บข้อมูลแบบฮาร์ดดิสพกพา (External HDD) ระบบคลาวด์ (Cloud) Microsoft OneDrive โดยมีการกำหนดชื่อโฟลเดอร์อย่างชัดเจน สามารถแสดงถึงระบบซอฟท์แวร์ และวันที่เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลได้อย่างชัดเจนเพื่อให้รู้ได้ว่าเป็นข้อมูลสำรองของระบบสารสนเทศใดและทำสำรองเมื่อใด โดยใคร ข้อมูลสำรองควรจัดเก็บไว้ที่หน่วยงานอื่น หรือระบบคลาวด์ (Cloud)

๕. การทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

มีการทดสอบสื่อเก็บข้อมูล ฮาร์ดดิสพกพา (External HDD), ระบบคลาวด์ (Cloud), Microsoft OneDrive อย่างสม่ำเสมอทุกระบบ อย่างน้อยเดือนละ ๑ ครั้ง

ส่วนที่ ๑๑
แนวปฏิบัติในการสร้างความต่อเนื่องให้กับธุรกิจ

๑. คำนำ

กระบวนการสร้างความต่อเนื่องให้กับธุรกิจในที่นี้ หมายถึง การบริหารจัดการเพื่อให้สถาบันดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารได้อย่างต่อเนื่อง แม้ในช่วงสภาวะที่เกิดปัญหาหรือเหตุการณ์ผิดปกติ อันเนื่องมาจากความล้มเหลวของระบบเครือข่าย ระบบฐานข้อมูล ภัยพิบัติทางธรรมชาติ อุบัติเหตุ ความบกพร่องของเครื่องมืออุปกรณ์ รวมทั้งการกระทำผิดส่วนบุคคลในกรณีประมาทเลินเล่อหรือกระทำอย่างตั้งใจก็ตาม ทั้งนี้เพื่อลดผลกระทบที่มีต่อสถาบันไม่ให้ภารกิจต้องหยุดชะงักเป็นเวลานาน เปลี่ยนเป็นชะลอการทำงานในระดับที่ยอมรับได้

นอกจากนี้ยังจะต้องสร้างความเชื่อมั่นให้แก่ทุกฝ่ายในการกู้คืนทรัพยากรของระบบสารสนเทศ ให้สามารถนำกลับมาใช้งานได้ตามปกติ หรือใกล้เคียงสภาพปกติได้มากที่สุดในระดับที่ทุกฝ่ายยอมรับได้ ด้วยการดูแลการปฏิบัติของเจ้าหน้าที่ เครื่องมืออุปกรณ์ ระบบซอฟท์แวร์ และทรัพยากรที่เกี่ยวข้อง ให้มีความพร้อมรองรับการใช้งานได้อย่างต่อเนื่อง โดยผ่านการดำเนินงานตามแนวปฏิบัติในแผนงานและการประเมินความเสี่ยงที่มีผลต่อการหยุดชะงักของการปฏิบัติภารกิจ ดังนี้

๒. แนวปฏิบัติในกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ

๒.๑ จัดประชุมชี้แจงเพื่อสร้างความเข้าในประเด็นความเสี่ยงที่สถาบันอาจต้องประสบ โดยประกอบด้วย

๒.๑.๑ ระบุความเสี่ยง และจัดลำดับความสำคัญของภารกิจที่เกี่ยวข้อง

๒.๑.๒ ระบุทรัพยากรสารสนเทศ ทั้งเครื่องมืออุปกรณ์และฐานข้อมูล ในกระบวนการที่เป็นภารกิจสำคัญ

๒.๑.๓ ผลกระทบที่มีต่อการปฏิบัติภารกิจในภาวะความเสี่ยงและแนวทางจัดการ โดยกำหนดวัตถุประสงค์ของการจัดการความเสี่ยงดังกล่าว

๒.๒ จัดสรรงบประมาณสำหรับดำเนินการในส่วนที่เกี่ยวข้องกับทรัพยากร โครงสร้างการบริหารงานด้านเทคโนโลยี และสิ่งแวดล้อม รวมทั้งเริ่มดำเนินการทันทีเพื่อป้องกันหรือผ่อนคลายผลกระทบจากความเสี่ยงดังกล่าว

๒.๓ จัดทำเอกสารแผนการทำงานในภาวะฉุกเฉินหรือเกิดเหตุการณ์ผิดปกติ เพื่อสร้างความต่อเนื่องของการดำเนินงานตามภารกิจของแต่ละฝ่าย

๒.๔ จัดให้มีการทดสอบและปรับปรุงกระบวนการสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ

๒.๕ จัดให้มีโครงสร้างการบริหารและบุคลากรผู้รับผิดชอบต่อกระบวนการสร้างความต่อเนื่องให้กับธุรกิจในแต่ละขั้นตอน

๓. แนวปฏิบัติในการประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ

๓.๑ ระบุเหตุการณ์ซึ่งเป็นต้นเหตุของการหยุดชะงักในการปฏิบัติภารภิจ ความน่าจะเป็นหรือโอกาสที่จะเกิดเหตุการณ์ดังกล่าว รวมทั้งผลกระทบที่เกิดขึ้นทันทีและที่จะเกิดตามมาในภายหลัง

๓.๒ ระบุสาเหตุที่อาจทำให้เกิดความล้มเหลวของเครื่องมืออุปกรณ์ ความผิดพลาดของบุคลากร การโจรกรรมข้อมูล และการก่ออาชญากรรมทางคอมพิวเตอร์

๓.๓ จัดให้มีการประเมินความเสี่ยง เพื่อที่จะกำหนดความน่าจะเป็นและความรุนแรงของผลกระทบที่เกิดขึ้น อย่างน้อยปีละ ๑ ครั้ง

๓.๔ พิจารณาภารกิจให้ครอบคลุมทุกกระบวนการ ไม่จำกัดเฉพาะระบบข้อมูล เพื่อที่จะได้มองเห็นผลกระทบที่เกิดขึ้นในภาพรวมทั้งหมดของสถาบัน

๓.๕ การประเมินความเสี่ยง ให้จัดลำดับความสำคัญของความเสี่ยงเป็นตัวเลข โดยคำนึงถึงความร้ายแรงและผลกระทบต่อภารกิจ ซึ่งครอบคลุมถึงทรัพยากรสารสนเทศ ผลกระทบต่อการหยุดชะงักของการปฏิบัติภารกิจ ระยะเวลาหยุดชะงักที่ยอมรับได้ และการกู้คืนข้อมูลตามลำดับความสำคัญ

๓.๖ กำหนดให้มีแนวทาง วิธีการ หรือกลยุทธ์ในการดำเนินการ เพื่อรักษาความต่อเนื่องบนพื้นฐานจากผลของการประเมินความเสี่ยง

๓.๗ เผยแพร่ให้มีการรับรู้และอนุญาตให้ดำเนินการอย่างเป็นทางการ ตามข้อกำหนดแนวทาง วิธีการหรือกลยุทธ์ที่กำหนดไว้

๔. แนวปฏิบัติในการจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ

๔.๑ จัดให้มีการทำแผนและดำเนินการตามแผน โดยคำนึงถึงภารกิจของหน่วยงานเป็นสำคัญ เพื่อรักษาความต่อเนื่องของการปฏิบัติงาน และสร้างความเชื่อมั่นในความพร้อมใช้งานได้อย่างต่อเนื่องของระบบข้อมูลในระดับที่ยอมรับได้

๔.๒ กำหนดหน้าที่ความรับผิดชอบและการยินยอมดำเนินการตามขั้นตอนในการรักษาความต่อเนื่องของการปฏิบัติภารกิจที่กำหนดขึ้น

๔.๓ ระบุการยอมรับความสูญเสียของข้อมูลและบริการ ที่อาจเกิดขึ้นจากเหตุการณ์ที่ก่อให้เกิดการหยุดชะงักของการปฏิบัติภารกิจ

๔.๔ ดำเนินการตามขั้นตอนที่กำหนด เพื่อรักษาความต่อเนื่องของการปฏิบัติภารกิจ โดยให้ความสำคัญกับผลกระทบที่ต่อเนื่องกับหน่วยภารกิจอื่น ทั้งภายในและภายนอกที่เกิดจากเหตุการณ์

๔.๕ กำหนดขั้นตอนปฏิบัติงานสำหรับการกู้คืนงานที่ยังอยู่ระหว่างการดำเนินการ ก่อนที่ระบบข้อมูลจะหยุดชะงักไป

๔.๖ จัดให้มีการจัดทำกระบวนการและขั้นตอนปฏิบัติเป็นเอกสาร รวมทั้งจัดฝึกอบรมบุคลากรที่เกี่ยวข้องในกระบวนการและขั้นตอนปฏิบัติที่ได้รับการอนุมัติแล้ว

๔.๗ ระบุทรัพยากรและสิ่งที่จำเป็นในการดำเนินการให้ชัดเจน รวมทั้งด้านทรัพยากรบุคคล และทรัพยากรที่ไม่ใช่สารสนเทศ

๔.๘ ในบางขั้นตอนกระบวนการอาจมีหน่วยงานอื่นเข้าร่วมเป็นส่วนหนึ่งด้วยก็ได้ ไม่จำเป็นต้องเป็นหน่วยงานเดียวกันทั้งหมด

๔.๙ ให้มีการจัดทำสำเนาแผน และเก็บรักษาไว้ในสถานที่อื่นซึ่งห่างไกลเพียงพอที่จะไม่ได้รับผลกระทบจากความเสียหายที่เกิดจากเหตุการณ์ที่ระบุไว้

๔.๑๐ สิ่งอื่นๆ นอกจากแผนแล้ว ถ้าสิ่งนั้นจำเป็นต้องใช้ในการปฏิบัติตามแผน ให้จัดเก็บไว้ในสถานที่นั้นเช่นกัน

๔.๑๑ กรณีที่มีการใช้สถานที่อื่นที่เป็นสถานที่ทำการชั่วคราว การจัดทำแผนและการดำเนินงานต้องอยู่ในระดับเดียวกันกับสถานที่ทำการหลัก

๔.๑๒ จัดให้มีการทดสอบและปรับปรุงแผนอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าแผนรักษาความต่อเนื่องนั้นถูกต้อง เป็นปัจจุบัน

๕. แนวปฏิบัติในการกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ

๕.๑ กรอบแนวปฏิบัติเพื่อการรักษาความต่อเนื่องของภารกิจจะต้องได้รับการดูแลบำรุงรักษาและสร้างความเชื่อมั่นได้ว่าแผนดำเนินการต่าง ๆ มีความสอดคล้องกับความต้องการของหน่วยงานเพื่อที่จะสามารถจัดลำดับความสำคัญในการฝึกซ้อมหรือดูแลรักษาได้

๕.๒ แผนการรักษาความต่อเนื่องทุกแผน จะต้องอธิบายหลักการและวิธีการที่นำมาประยุกต์ใช้

๕.๓ แต่ละแผนให้มีการกำหนดแผนเพิ่มเติมหรือแผนสำรอง รวมทั้งเงื่อนไขในการเลือกใช้แผน พร้อมทั้งระบุผู้รับผิดชอบดำเนินการในแต่ละส่วน

๕.๔ เมื่อมีการระบุความต้องการใหม่หรือความจำเป็นใหม่เพิ่มเติมขึ้นมา ขั้นตอนปฏิบัติยามฉุกเฉินเดิมต้องได้รับการแก้ไขอย่างเหมาะสมด้วย

๕.๕ ขั้นตอนปฏิบัติเหล่านี้ให้บรรจุไว้เป็นส่วนหนึ่งของการบริหารการเปลี่ยนแปลงของสถาบันด้วย เพื่อที่จะสร้างความเชื่อมั่นได้ว่าการรักษาความต่อเนื่องนี้จะได้รับการปฏิบัติ

๕.๖ ให้มีการกำหนดเจ้าของแผนหรือผู้รับผิดชอบโดยเฉพาะของแต่ละแผนด้วย

๕.๗ ขั้นตอนปฏิบัติกรณีฉุกเฉิน แผนการกู้คืน ให้อยู่ภายใต้ความรับผิดชอบของบุคลากรผู้ที่เป็นเจ้าของทรัพยากรสารสนเทศที่เกี่ยวข้องนั้น

๕.๘ การกู้คืนโดยใช้ผู้ให้บริการรายอื่น (ที่ไม่ใช่รายเดิม) เช่น ระบบประมวลผลข้อมูล หรือระบบเครือข่ายคอมพิวเตอร์ เป็นต้น ให้ถือเป็นความรับผิดชอบของผู้ให้บริการปัจจุบัน

๕.๙ กำหนดเงื่อนไขสำหรับการตัดสินใจใช้แผนปฏิบัติการก่อนที่จะอนุมัติแผนนั้น

๕.๑๐ ขั้นตอนกรณีฉุกเฉิน จะต้องอธิบายถึงกิจกรรมที่ต้องดำเนินการสำหรับแต่ละเหตุการณ์

๕.๑๑ ขั้นตอนปฏิบัติในการกู้คืน จะต้องอธิบายกิจกรรมที่จำเป็นในการเคลื่อนย้ายไปยังสถานที่ชั่วคราว และการเคลื่อนย้ายกลับคืนมาได้ภายในระยะเวลาที่ยอมรับได้

๕.๑๒ ขั้นตอนปฏิบัติชั่วคราวสำหรับการสานต่องานที่ยังคั่งค้างอยู่

๕.๑๓ ขั้นตอนปฏิบัติสำหรับการกู้คืนสู่สภาพเดิม ซึ่งอธิบายกิจกรรมที่ต้องดำเนินการ

๕.๑๔ กำหนดการสำหรับการทดสอบหรือฝึกซ้อมการดำเนินการตามแผน

๕.๑๕ จัดให้มีกิจกรรมในการสร้างความตระหนัก และฝึกอบรม ให้บุคลากรมีความเข้าใจในกระบวนการรักษาความต่อเนื่องของภารกิจ เพื่อให้มั่นใจได้ว่าจะสามารถดำเนินการได้เมื่อมีเหตุการณ์เกิดขึ้นจริง

๕.๑๖ กำหนดบทบาทหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับกิจกรรมในแผน

๕.๑๗ กำหนดหรือระบุเครื่องมืออุปกรณ์และทรัพยากรที่จำเป็นต้องใช้ในการปฏิบัติตามแผน

๖. แนวปฏิบัติในการทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ

๖.๑ แผนการรักษาความต่อเนื่องในการปฏิบัติงาน จะต้องได้รับการทดสอบ ซักซ้อม ทบทวน และปรับปรุงอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสามารถใช้งานได้จริง และบุคลากรที่เกี่ยวข้องสามารถที่จะเข้าใจแผนและบทบาทของแต่ละหน่วยงานได้เป็นอย่างดี

๖.๒ การซ้อมสามารถทำได้บนพื้นฐานของเหตุการณ์สมมติ

๖.๓ การซ้อมสามารถทำได้โดยใช้วิธีการจำลองสถานการณ์ขึ้น

๖.๔ จัดให้มีการทดสอบการซ้อมกู้ข้อมูลคืนจริง

๖.๕ จัดให้มีการทดสอบซ้อมกู้ข้อมูลคืน ณ สถานที่ชั่วคราวที่เตรียมไว้สำรอง

๖.๖ จัดให้มีการทดสอบร่วมกับหน่วยงานอื่นที่เกี่ยวข้อง

๖.๗ จัดให้มีการซ้อมแบบสมบูรณ์เต็มรูปแบบด้วย

๖.๘ เทคนิควิธีการในการทดสอบและซ้อมดำเนินการเหล่านี้สามารถนำไปใช้ได้ขึ้นอยู่กับความจำเป็นและความต้องการ

๖.๙ ผลการทดสอบหรือซ้อม จะต้องได้รับการบันทึกอย่างเป็นระบบเพื่อการปรับปรุงแก้ไขในอนาคต

๖.๑๐ จัดให้มีผู้รับผิดชอบในการทบทวนแผนการรักษาความต่อเนื่องในการปฏิบัติงาน และจะต้องดำเนินการอย่างน้อยปีละ ๑ ครั้ง

๖.๑๑ การเปลี่ยนแปลงที่เกิดขึ้นกับกระบวนการปฏิบัติงานปกติ จะได้รับการสะท้อนในการปรับปรุงแผนการรักษาความต่อเนื่องด้วย

๖.๑๒ การเปลี่ยนแปลงต่างๆ ที่เกิดขึ้น จะได้รับการควบคุมอย่างเป็นระบบและอย่างเป็นทางการเพื่อให้เชื่อมั่นได้ว่าแผนล่าสุดที่ถูกต้องจะถึงมือผู้เกี่ยวข้อง

๖.๑๓ การเปลี่ยนแปลงที่จะต้องพิจารณาเพื่อการควบคุมอย่างเป็นระบบและเป็นทางการประกอบด้วย

๖.๑๓.๑ การเปลี่ยนแปลงบุคลากร

๖.๑๓.๒ การเปลี่ยนแปลงที่อยู่และหมายเลขโทรศัพท์

๖.๑๓.๓ การเปลี่ยนแปลงวิธีการปฏิบัติงาน

๖.๑๓.๔ การเปลี่ยนแปลงสถานที่ อุปกรณ์ และทรัพยากรอื่นๆ

๖.๑๓.๕ การเปลี่ยนแปลงด้านกฎหมาย

๖.๑๓.๖ การเปลี่ยนแปลงผู้ให้บริการ ผู้รับบริการ และองค์กรภายนอกอื่นๆ

๖.๑๓.๗ การเปลี่ยนแปลงกระบวนการใหม่

๖.๑๓.๘ การเปลี่ยนแปลงความเสี่ยง

๗. การกำหนดผู้รับผิดชอบ

กำหนดให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนฉุกเฉินด้าน ICT เป็นผู้มีหน้าที่ดังต่อไปนี้

๗.๑ ตรวจสอบ บำรุง รักษา แก้ไขข้อบกพร่องต่างๆ ของระบบเครือข่ายและระบบบสารสนเทศของสถาบัน

๗.๒ จัดให้มีการทำแผนและดำเนินการตามแผนฉุกเฉินด้าน ICT ของสถาบันเพื่อสร้างความต่อเนื่องของการปฏิบัติงาน

ส่วนที่ ๑๒
แนวปฏิบัติในการประเมินความเสี่ยงเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. คำนำ

สถาบัน ตระหนักถึงความสำคัญของการพัฒนาองค์กรตามแนวทางการบริหารจัดการที่ดี มีธรรมาภิบาล ซึ่งรวมถึงการมีนโยบายและพัฒนาระบบการบริหารความเสี่ยงของสถาบัน เพื่อให้มั่นใจว่าการบริหารความเสี่ยงของสถาบันจะดำเนินการอย่างเป็นระบบ มีความต่อเนื่อง ส่งผลให้การบริหารงานในความรับผิดชอบมีประสิทธิภาพ เกิดประสิทธิผล อำนวยประโยชน์ให้กับชุมชนท้องถิ่นและสังคมตามวัตถุประสงค์และวิสัยทัศน์ขององค์กร ดังที่ได้กำหนดนโยบายบริหารความเสี่ยงไว้แล้ว

สถาบันได้กำหนดกระบวนการบริหารความเสี่ยงและการจัดทำแผนบริหารความเสี่ยงตามกรอบการบริหารความเสี่ยงตามแนวทางของ COSO – ERM (Enterprise Risk Management)

สำหรับกระบวนการบริหารความเสี่ยงทั่วทั้งองค์กรของสถาบัน ซึ่งประกอบด้วยการบริหารความเสี่ยงระดับองค์กรและระดับส่วนงานนั้น มุ่งเน้นให้เกิดผลสำเร็จตามแผนยุทธศาสตร์การดำเนินงาน ดังนั้น โครงการหรือกิจกรรมที่ต้องดำเนินการวิเคราะห์ ประเมิน และบริหารจัดการความเสี่ยง จึงเป็นโครงการหรือกิจกรรมที่ส่วนงานได้จัดทำขึ้นตามแผนปฏิบัติการและแผนงบประมาณ

หลักการสำคัญประการหนึ่งในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศคือการประเมินความเสี่ยงที่อาจเกิดขึ้นและมีผลกระทบทำให้ข้อมูลและระบบข้อมูลมีความไม่มั่นคงปลอดภัยได้ เพื่อให้การประเมินความเสี่ยงสามารถทำได้อย่างมีประสิทธิภาพจำเป็นต้องมีการระบุความเสี่ยงและกำหนดวิธีการประเมินอย่างชัดเจนเป็นระบบ อย่างไรก็ตาม ความเสี่ยงที่อาจเกิดขึ้นได้มีได้หลายประเภท แต่ละประเภทความเสี่ยงก็อาจมีวิธีในการประเมินแตกต่างกันออกไป ดังนั้นอาจจำเป็นต้องระบุและประเมินความเสี่ยงเป็นเรื่อง ๆ ไป

ในการประมวลผลค่าความเสี่ยงอาจจะมีได้หลายวิธีการขึ้นอยู่กับสถานการณ์สภาพแวดล้อมและปัจจัยที่เกี่ยวข้อง ตัวอย่างเช่น การใช้ดุลพินิจพิจารณาจากองค์ประกอบต่าง ๆ เช่น มูลค่าของสินทรัพย์ (Asset Value) ความรุนแรงของผลกระทบที่เกิดขึ้น ภาวะคุกคาม (Threat) และจุดอ่อน (Vulnerability) เป็นต้น หรือโดยวิธีประเมินระดับความเสี่ยงเป็นระดับสูง (H) ระดับปานกลาง (M) และระดับต่ำ (L) นอกจากนี้ยังสามารถประเมินโดยกำหนดเป็นคะแนนให้กับองค์ประกอบที่เกี่ยวข้อง

สำหรับการประเมินผลค่าความเสี่ยงที่ใช้ของสถาบัน ใช้วิธีการประเมินความเสี่ยงโดยคำนึงถึงผลกระทบด้านความสำเร็จ โดยกำหนดเป็นร้อยละของระดับความรุนแรงต่อความสำเร็จของโครงการ

โดยทั่วไปในการให้คะแนนในแต่ละด้าน อาจประเมินโดยใช้วิธีการต่าง ๆ กัน เช่น ประเมินจากดุลพินิจของผู้ที่เกี่ยวข้อง ประเมินโดยผู้เชี่ยวชาญทางด้านนั้น ๆ หรือประเมินโดยการสำรวจข้อมูล เป็นต้น

๒. แนวปฏิบัติในการประเมินความเสี่ยงด้านสารสนเทศ

๒.๑ กำหนดเกณฑ์การประเมินมาตรฐาน โดยพิจารณาเงื่อนไขในการกำหนดเกณฑ์การประเมินความเสี่ยง ๒ มิติ คือ โอกาสที่จะเกิดความเสี่ยง (Likelihood) และ ระดับความรุนแรงของผลกระทบ (Impact) เพื่อกำหนดระดับความเสี่ยง (Degree of Risks) ของความเสี่ยงแต่ละเหตุการณ์ต่อไป

๒.๒ ประเมินโอกาสและผลกระทบของความเสี่ยง โดยควรให้ความสำคัญต่อความเสี่ยงที่มีผลกระทบสูง และมีโอกาสเกิดความเสี่ยงสูง เพื่อจัดการความเสี่ยงดังกล่าวก่อน

๒.๓ จัดลำดับความเสี่ยง เพื่อให้สามารถจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของหน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดยพิจารณาจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยง

๒.๔ ดำเนินการตามระเบียบ ข้อกำหนด รวมทั้งคำแนะนำตามแผนปฏิบัติการหรือแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ได้มีการจัดทำขึ้น เพื่อลดความเสี่ยงและผลกระทบที่มีต่อความเสียหายด้านข้อมูลสารสนเทศอย่างเคร่งครัด

๓. การประเมินความเสี่ยง

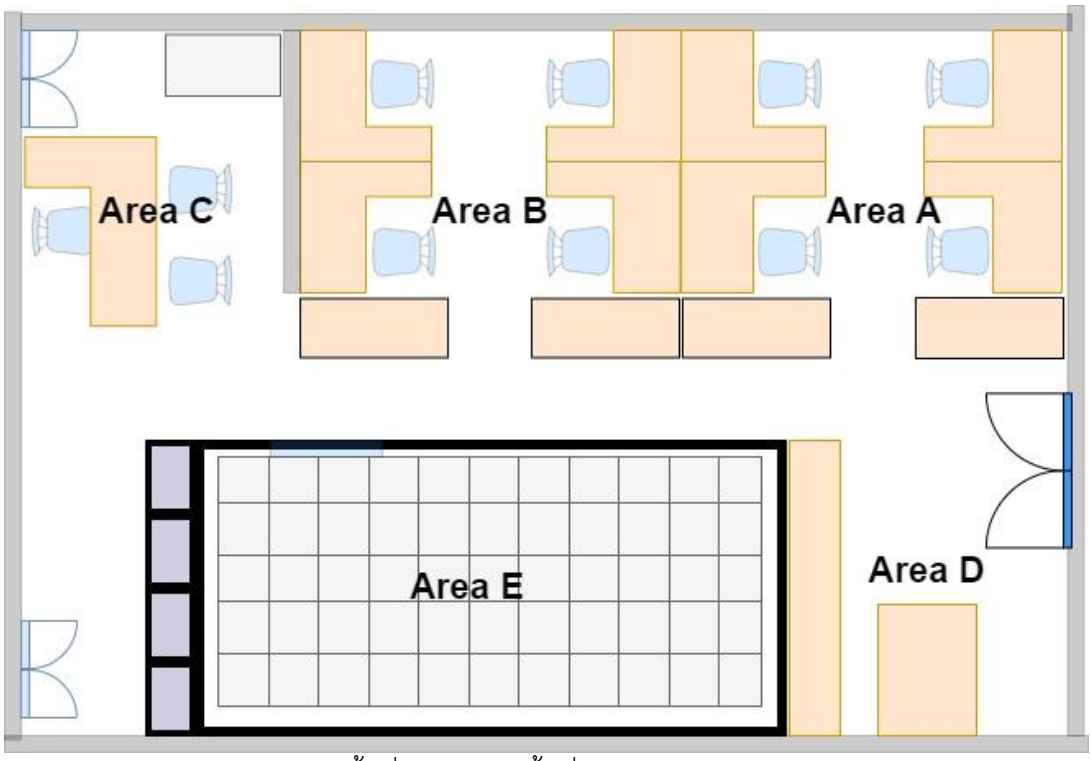
การประเมินความเสี่ยงเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศนั้น สถาบันถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงและการจัดทำแผนบริหารความเสี่ยงทั่วทั้งองค์กร ซึ่งมีการปฏิบัติตามกระบวนการอย่างจริงจัง เป็นระบบและมีความต่อเนื่องทุกปีอย่างน้อยปีละ ๑ ครั้ง โดยสำนักตรวจสอบ ซึ่งเป็นหน่วยงานภายในและทุก ๓ ปี จะมีการจ้างหน่วยงานภายนอกให้ทำการศึกษาประเมินผลการดำเนินงาน รวมทั้งประมวลผลการดำเนินงานเพื่อจัดทำข้อเสนอเป็นแนวทางในการพัฒนา และปรับปรุงยุทธศาสตร์ของสถาบัน เพื่อใช้เป็นกรอบชี้นำการดำเนินงานต่อไปในอนาคต โดยให้เป็นไปตามแผนปฏิบัติการหรือแผนฉุกเฉินที่ได้กำหนดไว้

ส่วนที่ ๑๓
แนวปฏิบัติการกำหนดพื้นที่เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๑. วัตถุประสงค์

เพื่อเป็นแนวปฏิบัติในการกำหนดพื้นที่เพื่อรักษาความปลอดภัยทางกายภาพสำหรับโครงสร้างและทรัพยากรทางด้านสารสนเทศ รวมถึงการจัดการการเข้าถึงทรัพยากรทางกายภาพโดยมีการอนุญาตให้เฉพาะผู้ที่เกี่ยวข้องและมีความจำเป็นเท่านั้น โดยในที่นี่จะกล่าวถึงเฉพาะในส่วนของห้องสำนักเทคโนโลยีสารสนเทศ

๒. แนวปฏิบัติการกำหนดและจัดสรรพื้นที่



แผนภาพแสดงการกำหนดพื้นที่และจัดสรรพื้นที่การใช้งานห้องสำนักเทคโนโลยีสารสนเทศ

จากแผนภาพด้านบน หัวหน้าสำนักเทคโนโลยีสารสนเทศ ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) และพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

พื้นที่	ชื่อพื้นที่	ลักษณะของพื้นที่			
		พื้นที่ทำงานทั่วไป	พื้นที่ทำงานของผู้ดูแลระบบ	พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ	พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์
Area : A	ส่วนของงานระบบฐานข้อมูล งานบริหารสำนักและหัวหน้างาน	/			
Area : B	ส่วนของงานระบบเทคโนโลยีสารสนเทศ	/	/		
Area : C	ส่วนของผู้บริหาร	/			
Area : D	พื้นที่ที่สำหรับประชุม	/			
Area : E	ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Server Room)		/	/	/

ตารางที่ ๑ การกำหนดพื้นที่การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

จากตารางด้านบน แต่ละพื้นที่จะมีการแบ่งลักษณะของพื้นที่ออกเป็น ๔ ลักษณะดังนี้ คือ

๑. พื้นที่ทำงานทั่วไป คือ พื้นที่ปฏิบัติงานของผู้ปฏิบัติงานสถาบัน แต่ละส่วนงาน ซึ่งเป็นพื้นที่ราชการ ห้ามบุคคลภายนอกเข้า ยกเว้นกรณีเข้ามาติดต่อราชการ โดยต้องแสดงตนเข้าทำการแลกบัตรผู้ติดต่อและระบุเหตุผลที่เข้ามาติดต่อ

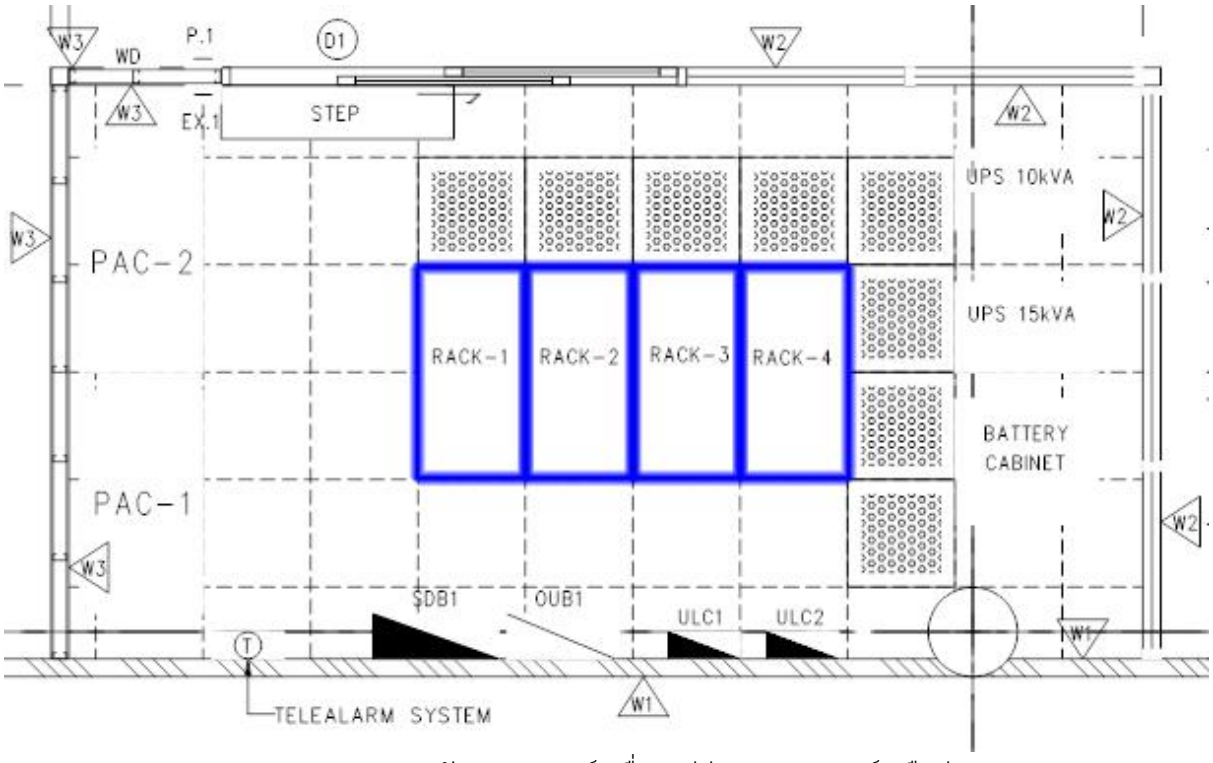
๒. พื้นที่ทำงานของผู้ดูแลระบบ คือ พื้นที่ทำงานสำหรับผู้ปฏิบัติงานของสำนักเทคโนโลยีสารสนเทศ ซึ่งได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่ดูแลระบบสารสนเทศ โดยไม่อนุญาตให้ผู้ปฏิบัติงานของสถาบัน ซึ่งสังกัดส่วนงานอื่น ๆ รวมถึงบุคคลภายนอกเข้าพื้นที่ ยกเว้นได้รับการอนุญาตจากเจ้าหน้าที่ผู้ดูแลหรือผู้บังคับบัญชาของสำนักเทคโนโลยีสารสนเทศเท่านั้น

๓. พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ คือ พื้นที่หวงห้าม เช่น ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Server Room) ซึ่งอนุญาตให้เฉพาะสำหรับผู้ปฏิบัติงานของสำนักเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ดูแลเท่านั้น

๔. พื้นที่สำหรับประชุมสำนัก คือพื้นที่สำหรับการวางแผนการปฏิบัติงานของสำนักเทคโนโลยีสารสนเทศ

๕. พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ คือ พื้นที่ติดตั้งอุปกรณ์จัดเก็บข้อมูลของระบบงานสารสนเทศ ซึ่งมีผู้ปฏิบัติงานของสำนักเทคโนโลยีสารสนเทศผู้ที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศ และได้รับอนุญาตเป็นจากหน่วยงานเจ้าของระบบ ให้เป็นผู้ทำหน้าที่จัดเก็บ สำรองข้อมูลระบบสารสนเทศที่รับผิดชอบดูแล

๓. การจัดสรรพื้นที่ภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์



แผนภาพแสดงการจัดวางอุปกรณ์เครื่องแม่ข่ายและอุปกรณ์เครือข่าย
ซึ่งจัดเป็นสัดส่วนในตู้จัดเก็บอุปกรณ์ระบบสารสนเทศ (RACK)
ภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

จากแผนภาพข้างบน เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ ผู้ที่ได้รับมอบหมายให้ดูแลห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Server Room) ต้องจัดระบบเทคโนโยลีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อความสะดวกและปลอดภัยในการปฏิบัติงาน และยังทำให้การเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

๔. การจัดสรรพื้นที่ใช้งานระบบเครือข่ายไร้สาย

สถาบัน มีการให้บริการอินเทอร์เน็ตไร้สายแก่ผู้ปฏิบัติงานและบุคคลภายนอกที่เข้าร่วมกิจกรรมที่จัดขึ้นภายในสถาบัน ครอบคลุมพื้นที่บริเวณอาคารสำนักงาน โดยผู้ใช้งานเครือข่ายจะต้องเข้าใช้ช่องสัญญาณ

(SSID) ตามสิทธิที่ได้รับเท่านั้น เช่น CODI_Staff สำหรับเจ้าหน้าที่ CODI_Contractor สำหรับลูกจ้างโครงการ ผู้ประสาน และ CODI_Guest สำหรับผู้มาติดต่อโดยจะต้องลงทะเบียนการใช้งานผ่านระบบ

๕. แนวปฏิบัติสำหรับระบบซึ่งไวต่อการรบกวน

ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสถาบัน ได้แก่ ระบบที่เกี่ยวข้องกับด้านการเงินและงบประมาณ หรือ โปรแกรมระบบที่ใช้ในการปฏิบัติงานด้านงบประมาณ ให้ติดตั้งในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Server Room) ซึ่งอนุญาตให้เฉพาะสำหรับผู้ปฏิบัติงานของสำนักเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ดูแลเท่านั้นที่จะสามารถเข้าถึงได้

ส่วนที่ ๑๔
แนวปฏิบัติการบริหารจัดการรหัสผ่าน

๑. วัตถุระสงค์

เพื่อเป็นแนวปฏิบัติในการบริหารจัดการรหัสผ่านของผู้ใช้งาน ทั้งในส่วนของการกำหนด เปลี่ยนแปลง ยกเลิกรหัสผ่าน และการทบทวนสิทธิการเข้าถึงระบบสารสนเทศและการสื่อสาร เพื่อให้เกิดความมั่นคงปลอดภัยในการเข้าใช้งานระบบสารสนเทศและการสื่อสาร ซึ่งเป็นข้อมูลที่เป็นความลับส่วนบุคคลและถือว่าเป็นสิทธิและความรับผิดชอบของผู้ใช้งานระบบสารสนเทศที่ต้องปฏิบัติ

๒. แนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๒.๑ กรณีการเข้าใช้งานระบบโปรแกรมสารสนเทศ ผู้ใช้งานต้องลงนามในแบบฟอร์ม *“ลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ”* ซึ่งเป็นการยอมรับที่จะเก็บรักษารหัสผ่านให้เป็นความลับเฉพาะตนและเก็บรหัสผ่านของกลุ่มไว้เฉพาะสมาชิกในกลุ่ม

๒.๒ กรณีรหัสผ่านสำหรับระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ผู้ดูแลระบบควรสร้างรหัสผ่านชั่วคราวให้ก่อน ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านทันทีที่เข้าใช้งานระบบครั้งแรก

๒.๓ ระบบต้องกำหนดกระบวนการเพื่อตรวจสอบตัวตนของผู้ใช้งานก่อนที่จะสร้างรหัสผ่านใหม่ เปลี่ยนรหัสผ่าน หรือรหัสผ่านชั่วคราว

๒.๔ การส่งรหัสผ่านชั่วคราวให้กับผู้ใช้งาน ควรใช้วิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลที่สามหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๒.๕ รหัสผ่านชั่วคราวควรมีความเป็นหนึ่งเดียว ไม่ซ้ำกับคนอื่นและไม่ควรใช้คำที่เดาได้

๒.๖ ผู้ใช้งานต้องตอบยืนยันการได้รับรหัสผ่านด้วยตัวเอง

๒.๗ ผู้ใช้งานไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์โดยอยู่ในรูปแบบที่ไม่ได้ป้องกัน

๒.๘ รหัสผ่านที่กำหนดไว้โดยผู้ผลิตตั้งแต่แรกควรได้รับการตั้งค่าใหม่ทันทีโดยผู้ดูแลระบบหลังจากติดตั้งระบบซอฟท์แวร์

๓. แนวปฏิบัติการใช้งานรหัสผ่าน

๓.๑ ผู้ใช้งานต้องเก็บรหัสผ่านไว้เป็นความลับ

๓.๒ ผู้ใช้งานต้องหลีกเลี่ยงการบันทึกรหัสผ่าน เช่น บันทึกลงในกระดาษ ในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่าง ๆ นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัย และวิธีการในการบันทึกได้รับการอนุมัติแล้ว

๓.๓ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่า รหัสผ่านอาจรั่วไหล

๓.๔ กำหนดรหัสผ่านที่มีคุณภาพและมีความยาวที่เหมาะสม ซึ่งต้องคำนึงหลักปฏิบัติดังนี้

๓.๔.๑ กำหนดเป็นแบบ complex อย่างน้อย ๘ ตัวอักษร โดยต้องมีอักขระพิเศษผสมด้วย

๓.๔.๒ ให้ง่ายสำหรับจดจำ

๓.๔.๓ ไม่ให้อยู่บนพื้นฐานของสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย หรือสามารถหาได้จากข้อมูล

ส่วนตัว เช่น ชื่อ หมายเลขโทรศัพท์ และวันเกิด เป็นต้น

๓.๔.๔ ไม่สร้างจุดอ่อนโดยการใช้คำที่อยู่ในพจนานุกรม

๓.๔.๕ ไม่มีคำซ้ำหรือตัวอักษรซ้ำ ไม่ควรเป็นตัวเลขทั้งหมด หรือไม่ควรเป็นตัวอักษรทั้งหมด

๓.๕ ผู้ใช้งานควรเปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้งานที่ได้สิทธิพิเศษควรได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) หรืออย่างน้อยทุก ๓ เดือน และหลีกเลี่ยงการวนใช้รหัสผ่านเดิมที่เคยใช้แล้ว

๓.๖ ระบบควรกำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

๓.๗ ผู้ใช้งานต้องไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ login อัตโนมัติ

๓.๘ ผู้ใช้งานต้องไม่ใช้รหัสผ่านร่วมกับผู้อื่น

๓.๙ ผู้ใช้งานต้องไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงานและในกรณีใช้ส่วนตัว

๓.๑๐ ถ้าผู้ใช้งานจำเป็นต้องเข้าถึงข้อมูล หรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว ควรแนะนำให้ใช้รหัสผ่านเดียวกันที่มีคุณภาพ โดยปฏิบัติตามข้อ ๓.๔ ข้างต้นสำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

๔. แนวปฏิบัติของระบบบริหารจัดการรหัสผ่าน

๔.๑ ผู้ใช้งานต้องใช้ ID และรหัสผ่านของตนเองในการใช้งานระบบ เพื่อป้องกันการปฏิเสธความรับผิดชอบ

๔.๒ อนุญาตให้ผู้ใช้งานสามารถกำหนดรหัสผ่านของตนเองได้ และมีกระบวนการตรวจสอบอีกครั้งก่อนยืนยันการเปลี่ยนแปลงรหัสผ่านเพื่อป้องกันความผิดพลาด

๔.๓ ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีคุณภาพ

๔.๔ ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านเมื่อเข้าระบบเป็นครั้งแรก

๔.๕ ผู้ใช้งานควรบันทึกประวัติการเปลี่ยนรหัสผ่านเพื่อป้องกันการใช้ซ้ำ

๔.๖ ระบบต้องไม่แสดงรหัสผ่านให้เห็นบนหน้าจอ

๔.๗ ผู้ใช้งานต้องเก็บข้อมูลรหัสผ่านไว้ต่างหากจากข้อมูลอื่น

๕. แนวปฏิบัติการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

๕.๑ ผู้ดูแลระบบจะต้องทำการทบทวนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ ทุกครั้งที่มีการเปลี่ยนแปลงสิทธิ อันเนื่องมาจากการเปลี่ยนตำแหน่งงานหรือการปรับโครงสร้างการทำงานภายในสถาบัน

๕.๒ ผู้ดูแลระบบจะต้องทำการเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลเมื่อได้รับการแจ้งจากหน่วยงานที่เกี่ยวข้อง

๕.๓ ผู้ดูแลระบบจะต้องทำการทบทวนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ สำหรับผู้ได้รับสิทธิพิเศษต้องทบทวนสิทธิการเข้าถึงระบบทุก ๓ เดือน

๕.๔ ผู้ดูแลระบบต้องบันทึกความเปลี่ยนแปลงสิทธิของผู้ใช้งานที่ได้รับสิทธิเข้าใช้งานระบบและ

ผู้ใช้งานที่ได้รับสิทธิพิเศษ

ส่วนที่ ๑๕
แนวปฏิบัติการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อให้มีกระบวนการการกำหนดสิทธิของผู้ใช้งานในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ โดยมีการอนุญาตให้เฉพาะผู้ที่เกี่ยวข้องและมีความจำเป็น

๒. การบริหารจัดการสิทธิการใช้งานระบบสารสนเทศ

การใช้งานระบบสารสนเทศและการสื่อสารจำเป็นต้องได้รับสิทธิ กระบวนการที่เกี่ยวข้องกับการบริหารจัดการสิทธิมีดังต่อไปนี้

๒.๑ การลงทะเบียนขอสิทธิใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๑.๑ กรณีเป็นผู้ปฏิบัติงานของสถาบัน ให้ผู้ใช้งานกรอกข้อมูลลงแบบฟอร์ม *“ขอใช้สิทธิใช้โปรแกรมระบบสารสนเทศของ พอช.”* และให้ผู้อำนวยการสำนัก หรือผู้ช่วยผู้อำนวยการภาค (บริหาร) ให้ความเห็นชอบ แล้วนำส่งสำนักเทคโนโลยีสารสนเทศเพื่อพิจารณาให้สิทธิตามความเหมาะสม

๒.๑.๒ กรณีเป็นบุคคภายนอก ให้ผู้อำนวยการสำนัก หรือผู้ช่วยผู้อำนวยการภาค (บริหาร) ส่งบัญชีรายชื่อผู้ขอใช้สิทธิ พร้อมรายละเอียดส่วนบุคคล มายังสำนักเทคโนโลยีสารสนเทศเพื่อพิจารณาให้สิทธิตามความเหมาะสม

๒.๒ การให้สิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย จะเป็นผู้พิจารณาอนุญาตการให้สิทธิตามที่ผู้ขอใช้งานเสนอโดย ปฏิบัติตามแนวทางที่ระบุไว้ใน *“แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ” (ส่วนที่ ๑๕)* และ *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ ๑๔)*

๒.๓ การแจ้งยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

เมื่อผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ต้องการยกเลิกสิทธิในการเข้าใช้งานระบบที่ได้รับแจ้งบัญชีรายชื่อจากสำนักทรัพยากรบุคคล หรือหัวหน้าหน่วยงานที่เกี่ยวข้อง เห็นว่าผู้ปฏิบัติงานของสถาบันหรือบุคคลภายนอก ที่ได้รับสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศไม่มีความจำเป็นที่จะต้องเข้าใช้งานระบบอีกต่อไป ให้หัวหน้าหน่วยงานนั้น ๆ แจ้งไปยังสำนักเทคโนโลยีสารสนเทศให้ดำเนินการยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

เมื่อสำนักเทคโนโลยีสารสนเทศได้ยกเลิกสิทธิดังกล่าวแล้ว ให้บันทึกประวัติการเปลี่ยนแปลงสิทธิไว้เป็นหลักฐาน

ส่วนที่ ๑๖
แนวปฏิบัติการบริหารจัดการครุภัณฑ์คอมพิวเตอร์และเครือข่าย

๑. วัตถุระสงค์

เพื่อช่วยให้เจ้าหน้าที่ผู้ดูแลรับผิดชอบงานในส่วนครุภัณฑ์คอมพิวเตอร์และเครือข่าย สามารถใช้เป็นแนวปฏิบัติในการจัดสรรครุภัณฑ์ให้สอดคล้องกับการดำเนินงานของสถาบันและความต้องการของผู้ใช้งาน รวมถึงการควบคุมทะเบียนและบำรุงรักษาครุภัณฑ์ที่ใช้งานอยู่ในสถาบันได้อย่างมีประสิทธิภาพ ซึ่งนำไปสู่การใช้งานทรัพยากรสารสนเทศที่มีอยู่ในสถาบันได้อย่างมีประสิทธิภาพ เกิดประโยชน์สูงสุด

๒. แนวปฏิบัติการลงทะเบียนครุภัณฑ์คอมพิวเตอร์และเครือข่าย

ให้สำนักบริหารงานกลางจัดทำทะเบียน ครุภัณฑ์ที่เกี่ยวกับคอมพิวเตอร์และเครือข่ายตามระบบของสถาบัน และนำส่งให้สำนักเทคโนโลยีสารสนเทศ เพื่อบริหารจัดการในส่วนที่เกี่ยวข้องต่อไป

๓. แนวปฏิบัติการเบิกใช้ครุภัณฑ์คอมพิวเตอร์และเครือข่าย

ผู้ใช้งานต้องการใช้งานครุภัณฑ์คอมพิวเตอร์และเครือข่าย ให้ขออนุมัติการยืมและการส่งคืนครุภัณฑ์จากผู้มีอำนาจอนุมัติตามระบบของสถาบัน

๔. แนวปฏิบัติการแจ้งซ่อมบำรุงครุภัณฑ์คอมพิวเตอร์และเครือข่าย

๔.๑ เมื่อผู้ใช้งานพบการทำงานที่ผิดไปจากปกติของครุภัณฑ์ หรือไม่สามารถใช้งานครุภัณฑ์ในการดำเนินงานได้ ผู้ใช้งานต้องทำการปรึกษากับเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ ที่ทำหน้าที่ให้คำปรึกษาในการแก้ไขปัญหาจากการใช้งานครุภัณฑ์คอมพิวเตอร์และเครือข่ายในเบื้องต้นก่อน หากไม่สามารถแก้ไขปัญหาที่พบได้ ประกอบกับจากการวินิจฉัยปัญหาจากเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศแล้ว ให้ดำเนินการแจ้งซ่อมบำรุง โดยกรอกข้อมูลครุภัณฑ์ที่ต้องการแจ้งลงใน *“แบบฟอร์มบันทึกแจ้งซ่อมครุภัณฑ์คอมพิวเตอร์ในโปรแกรม Helpdesk”* และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการส่งซ่อม

๔.๒ เจ้าหน้าที่ผู้รับผิดชอบวิเคราะห์อาการเสียหายของครุภัณฑ์จากข้อมูลใน *“แบบฟอร์มบันทึกแจ้งซ่อมครุภัณฑ์คอมพิวเตอร์ในโปรแกรม Helpdesk”* และจากการทดสอบการทำงานด้วยตนเอง รวมถึงพิจารณาข้อมูลประกอบโดยเฉพาะในส่วนของระยะเวลาประกันของครุภัณฑ์ดังกล่าว ซึ่งหากอยู่ในระยะเวลาประกันเจ้าหน้าที่สามารถส่งครุภัณฑ์เข้ารับการซ่อมบำรุงที่ศูนย์บริการของบริษัทผู้ผลิตครุภัณฑ์ได้ โดยไม่เสียค่าใช้จ่ายในส่วนที่ระบุในประกัน หากครุภัณฑ์ดังกล่าวไม่อยู่ในระยะเวลาประกัน เจ้าหน้าที่ผู้รับผิดชอบต้องพิจารณาจากความเสียหายของครุภัณฑ์ หากเสียหายมากอาจจำเป็นจะต้องจำหน่ายครุภัณฑ์ดังกล่าวหรือหากความเสียหายของครุภัณฑ์สามารถแก้ไขได้ให้ดำเนินการแก้ไข

๔.๓ ในระหว่างที่เจ้าหน้าที่ผู้รับผิดชอบส่งครุภัณฑ์เข้ารับการซ่อมบำรุงนั้น หากมีครุภัณฑ์อื่นที่สามารถใช้งานทดแทนครุภัณฑ์ดังกล่าวได้ ให้เจ้าหน้าที่ดำเนินการแจ้งแก่ผู้ใช้งาน โดยให้ผู้ใช้งานทำเรื่องเบิกใช้งานครุภัณฑ์ โดยกรอกข้อมูลลงใน *“แบบฟอร์มการขอเบิกใช้ครุภัณฑ์คอมพิวเตอร์และเครือข่าย”* โดยระบุ

รายการครุภัณฑ์ที่ต้องการเบิกใช้รวมถึงสถานที่จัดเก็บหรือติดตั้ง และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการพิจารณาอนุมัติ และเจ้าหน้าที่ผู้ดูแลทะเบียนครุภัณฑ์ทำการบันทึกข้อมูลครุภัณฑ์ใหม่ลงใน *“แบบฟอร์มทะเบียนครุภัณฑ์คอมพิวเตอร์และเครือข่าย”* เพื่อจัดเก็บเป็นประวัติครุภัณฑ์ของสถาบัน

๔.๔ หลังจากที่เจ้าหน้าที่ผู้รับผิดชอบส่งครุภัณฑ์ที่พบความเสียหายเข้ารับการแก้ไขเรียบร้อยแล้ว ต้องดำเนินการทดสอบในส่วนที่พบความเสียหายอีกครั้ง ก่อนจัดส่งครุภัณฑ์คืนผู้ใช้งาน โดยเจ้าหน้าที่ผู้รับผิดชอบกรอกข้อมูลรายละเอียดการซ่อมบำรุง และการทดสอบครุภัณฑ์ลงใน *“แบบฟอร์มบันทึกแจ้งซ่อมครุภัณฑ์คอมพิวเตอร์ในโปรแกรม helpdesk”* ในส่วนของเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ และส่งคืนครุภัณฑ์พร้อมเอกสารดังกล่าวให้กับผู้ใช้งาน

๕. แนวปฏิบัติการจำหน่ายครุภัณฑ์คอมพิวเตอร์และเครือข่าย

ในกรณีที่สำนัก/ภาค พบว่าครุภัณฑ์เสียหายเกินกว่าที่จะแก้ไขได้ รวมถึงไม่อยู่ในระยะเวลาประกันหรือเสื่อมสภาพตามอายุการใช้งาน ประกอบกับเมื่อพิจารณาถึงมูลค่าของครุภัณฑ์กับค่าใช้จ่ายในการซ่อมบำรุงแล้ว จำเป็นต้องดำเนินการจำหน่ายครุภัณฑ์ดังกล่าว ให้สำนักเทคโนโลยีสารสนเทศให้ความเห็นประกอบและให้สำนัก/ภาค ดังกล่าว จัดส่งครุภัณฑ์ดังกล่าว ให้กับสำนักบริหารงานกลางดำเนินการตามระเบียบต่อไป

ส่วนที่ ๑๗
แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจะถูกนำไปปฏิบัติให้เกิดผลได้เพียงใดนั้นขึ้นอยู่กับหลายปัจจัย และปัจจัยที่สำคัญประการหนึ่งก็คือความเข้าใจและความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของบุคลากรที่เกี่ยวข้อง ดังนั้นการเผยแพร่แนวนโยบายและแนวปฏิบัติ การฝึกอบรม เพื่อสร้างความคุ้นเคยกับแนวปฏิบัติ เพื่อสร้างความตระหนักให้กับบุคลากรที่เกี่ยวข้องเป็นเรื่องที่สำคัญ และจำเป็นต้องมีแนวปฏิบัติเพื่อการนั้น

๒. แนวทางวิธีการและรูปแบบการสร้างความตระหนัก

สำนักเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานที่มีหน้าที่ในการดูแลเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน ควรมีการสร้างความตระหนักให้แก่บุคลากร โดยสามารถทำได้ในหลายรูปแบบ เช่น การจัดฝึกอบรม การจัดสัมมนา และการประชาสัมพันธ์ผ่านสื่อต่าง ๆ รวมทั้ง การมีข้อสั่งการจากผู้บริหารในบางกรณีที่เห็นว่ามีการละเลยข้อกำหนดต่าง ๆ ในแนวนโยบายฉบับนี้

ส่วนที่ ๑๘
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย

๑. วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบเครือข่ายของสถาบันได้อย่างมีประสิทธิภาพ จำเป็นต้องมีการกำหนดแนวปฏิบัติที่เกี่ยวข้องกับการควบคุมการเข้าถึงระบบเครือข่าย เอกสารฉบับนี้จัดทำขึ้นเป็นแนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายของหน่วยงาน โดยมีการอธิบายแนวปฏิบัติแยกเป็นข้อ ๆ เพื่อสะดวกแก่การนำไปใช้

๒. แนวปฏิบัติในการแบ่งแยกเครือข่าย (Segregation in networks)

๒.๑ ให้มีการแบ่งแยกเครือข่ายออกเป็นส่วน ๆ เพื่อควบคุมการเข้าถึงเครือข่าย ดังนี้

๒.๑.๑ ส่วนที่เป็นสาธารณะ (External Zone)

๒.๑.๒ ส่วนที่เชื่อมต่อภายใน (Internal Zone)

๒.๑.๓ ส่วนที่เชื่อมต่อภายในและที่เป็นสาธารณะ (DMZ Zone)

2.1.4 ส่วนที่เชื่อมต่อเป็นเครือข่ายไร้สาย (Wi-Fi Zone)

๒.๒ เพื่อการแบ่งเขตโซนอย่างชัดเจนให้ติดตั้งอุปกรณ์ Gateway กั้นไว้ระหว่างเครือข่ายเพื่อเป็นตัวควบคุมการไหลของข้อมูลระหว่างกัน เช่น Firewall ซึ่งมีการปรับแต่งให้สามารถควบคุมหรือกรองข้อมูลที่สื่อสารกันระหว่างเครือข่ายได้

๒.๓ การแบ่งแยกส่วนเครือข่ายจะต้องได้รับการพิจารณา รวมถึงเครือข่ายไร้สายจากภายในและจากเครือข่ายส่วนตัว เนื่องจากขอบเขตการเชื่อมต่อของเครือข่ายไร้สายไม่สามารถนิยามให้ชัดเจนได้ ดังนั้นจึงต้องมีการประเมินความเสี่ยงเพื่อหาแนวทางการควบคุมและป้องกัน เช่น การใช้การตรวจสอบตัวตนที่เข้มข้นขึ้น วิธีการเข้ารหัสและการเลือกกำหนดความถี่ช่องสัญญาณเอง เป็นต้น เพื่อที่จะรักษาการแบ่งแยกส่วนได้อย่างปลอดภัยและมีประสิทธิภาพ

๓. แนวปฏิบัติการควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

๓.๑ การควบคุมการเชื่อมต่อทางเครือข่าย ผู้ดูแลระบบจะต้องดูแลให้มีการปฏิบัติตาม แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศร และแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอกสถาบัน ที่ระบุใน *“แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ”* (ส่วนที่ ๓)

๓.๒ ความสามารถในการเชื่อมต่อของผู้ใช้งาน จะต้องถูกจำกัดโดยอุปกรณ์ Gateway ซึ่งจะกรองการรับ-ส่งข้อมูลได้

๓.๓ ให้มีการจำกัดช่วงเวลาหรือช่วงวันที่ในการอนุญาตให้เชื่อมต่อในกรณีที่มีความจำเป็น

๔. แนวปฏิบัติการควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

๔.๑ การควบคุมการกำหนดเส้นทางบนเครือข่าย ผู้ดูแลระบบจะต้องดูแลให้มีการปฏิบัติตามแนวปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ที่ระบุใน *“แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ” (ส่วนที่ ๓)*

๔.๒ การควบคุมเส้นทางสื่อสาร จะต้องอยู่บนพื้นฐานของต้นทางที่สามารถแน่ใจได้และปลายทางที่สามารถตรวจสอบได้

๔.๓ ใช้อุปกรณ์ Gateway ในการตรวจสอบต้นและปลายทาง ณ จุดควบคุมที่อยู่ระหว่างเครือข่ายภายในและเครือข่ายภายนอก เช่น การใช้ Firewall หรือ proxy เป็นต้น

๕. ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

๕.๑ ไม่แสดงเลขที่ระบบหรือเลขที่โปรแกรมจนกว่ากระบวนการ login จะเสร็จสิ้นสมบูรณ์

๕.๒ แสดงข้อความเตือนว่าคอมพิวเตอร์จะถูกใช้งานโดยผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

๕.๓ ไม่แสดง help ระหว่างกระบวนการ login ซึ่งอาจเป็นการช่วยให้ผู้ที่ไม่ได้รับอนุญาตค้นหาช่องทางเข้าได้

๕.๔ ตรวจสอบความถูกต้องของข้อมูลที่ Input เฉพาะเมื่อการ Input เสร็จสิ้นสมบูรณ์แล้ว ถ้ามีความผิดพลาด ระบบต้องไม่แสดงว่าข้อมูลที่ Input ส่วนไหนไม่ถูกต้อง

๕.๕ จำกัดจำนวนครั้งของการพยายามเข้าใช้ระบบ เช่น ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง เป็นต้น และจะต้องพิจารณาเพิ่มเติมประเด็นต่อไปนี้

๕.๕.๑ บันทึกการพยายามทั้งที่สำเร็จและไม่สำเร็จ

๕.๕.๒ หลังจากใส่ข้อมูล login ผิดพลาด บังคับระยะเวลาทิ้งช่วงก่อนที่จะยอมให้พยายามครั้งต่อไป

๕.๕.๓ ตัดการเชื่อมโยงเครือข่าย

๕.๕.๔ ส่งข้อความเตือนไปยังหน้าจอของระบบ ถ้ามีความพยายามในการ login หลายครั้งเกินจำนวนครั้งมากที่สุดที่ยอมรับได้

๕.๕.๕ กำหนดรหัสผ่านให้เหมาะสมกับความยาวของรหัสผ่านและมูลค่าของระบบที่จะต้องได้รับการป้องกัน

๕.๖ จำกัดจำนวนครั้งสูงสุดและจำนวนครั้งต่ำสุดสำหรับกระบวนการ login ถ้าเกินกว่านั้นระบบจะหยุดการให้ login

๕.๗ แสดงข้อมูลต่อไปนี้หลังจากที่ login สำเร็จแล้ว

๕.๗.๑ วันที่และเวลาของการเข้า login ครั้งที่แล้ว

๕.๗.๒ รายละเอียดของการพยายาม login ที่ไม่สำเร็จตั้งแต่การ login ครั้งที่แล้ว

๕.๘ ไม่แสดงรหัสผ่านที่ได้ input หรือซ่อนไม่ให้มองเห็นหรือเข้าใจได้

๕.๙ ไม่ส่งรหัสผ่านผ่านเครือข่ายโดยไม่เข้ารหัสเพื่อรักษาความลับก่อน

๖. แนวปฏิบัติในการระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)

๖.๑ แนวปฏิบัติดังกล่าวให้ใช้สำหรับผู้ใช้งานทุกประเภท (รวมถึง เจ้าหน้าที่สนับสนุน เจ้าหน้าที่ปฏิบัติการ ผู้บริหารระบบ โปรแกรมเมอร์ระบบ และผู้บริหารฐานข้อมูล)

๖.๒ ID ของผู้ใช้งานจะถูกใช้เพื่อการติดตามสืบหาร่องรอยกิจกรรมของผู้ใช้งานแต่ละคนได้ภายหลัง

๖.๓ กิจกรรมงานประจำไม่ควรดำเนินการโดยผู้ใช้งานที่ได้สิทธิพิเศษ

๖.๔ หากจำเป็นต้องมีการใช้งาน ID ร่วมสำหรับกลุ่มของผู้ใช้งานหรือในเฉพาะบางงาน ในกรณีดังกล่าวต้องมีการจัดทำเอกสารอนุมัติรับรองจากผู้บริหาร ซึ่งจะต้องกำหนดตัวควบคุมอื่นเพิ่มเติมเพื่อดูแลการรับผิดชอบต่อข้อมูลในกรณีใช้ ID ร่วมกัน

๖.๕ การใช้รหัสผู้ใช้งาน ID ร่วมดังกล่าว จะถูกใช้เฉพาะกรณีที่การใช้งานนั้นไม่จำเป็นต้องบันทึกประวัติการใช้งาน (เช่น การดูอย่างเดียว เป็นต้น) หรือในกรณีที่มีการควบคุมอื่นควบคู่ไปด้วย เช่น อนุญาตให้เข้าใช้เพียงครั้งเดียว

กรณีมีความจำเป็นต้องตรวจยืนยันตัวตนอย่างเข้มข้น อาจใช้วิธีอื่นแทนการใช้รหัสผ่านในการตรวจยืนยันตัวตนได้ เช่น วิธีการใช้การเข้ารหัสเพื่อรักษาความลับ, การยืนยันตัวตนสองชั้น (2FA), Smart Card, Token หรือวิธีการทาง Bio-Metrix

๗. แนวปฏิบัติในการพัฒนาระบบบริหารจัดการรหัสผ่าน (Password management system)

กำหนดให้ผู้ใช้งานใช้ ID และรหัสผ่านของตนเองในการใช้งาน สำหรับการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบเครือข่าย ระบบปฏิบัติการ และโปรแกรมประยุกต์และสารสนเทศ เพื่อป้องกันการปฏิเสธความรับผิดชอบ (ดูรายละเอียดส่วนที่ ๑๔ แนวปฏิบัติการบริหารจัดการรหัสผ่าน)

๘. แนวปฏิบัติในการกำหนดการหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

๘.๑ กำหนดให้แต่ละระบบมีกลไกในการ Clear Session เมื่อไม่ได้มีการใช้งานตามระยะเวลาที่กำหนด (time-out)

๘.๒ time-out ต้องกำหนดให้เหมาะสมกับ ประเภทข้อมูลที่เกี่ยวข้อง และระบบสารสนเทศนั้น ซึ่งอาจกำหนดไม่เกิน ๓๐ นาที

๘.๓ บางระบบอาจใช้รูปแบบเพียง clear และ lock หน้าจอโดยไม่ต้องยกเลิก session ก็ได้

๙. แนวปฏิบัติการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

ให้มีการจำกัดระยะเวลาการใช้งานเครือข่ายที่เชื่อมต่อที่เพียงพอและเหมาะสมต่อการใช้งานระบบสารสนเทศแต่ละระบบ โดยกำหนดระยะเวลาสำหรับการใช้งานไม่น้อยกว่า ๓ ชั่วโมง และตัดการเชื่อมต่อเมื่อไม่มีการใช้งานในช่วงระยะเวลา ๑๐ นาที ทั้งนี้ให้พิจารณาจากระบบสารสนเทศที่มีความเสี่ยงสูง ได้แก่ ระบบที่เกี่ยวข้องกับด้านการเงิน ให้มีการจำกัดระยะเวลาการใช้งานเครือข่ายที่เชื่อมต่อที่สั้นขึ้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑๐. แนวปฏิบัติในการแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)

๑๐.๑ จัดลำดับความสำคัญ (sensitivity) ของระบบ application ต้องมีการระบุอย่างชัดเจน และจัดทำเป็นเอกสารโดยเจ้าของระบบ

๑๐.๒ เมื่อจำเป็นต้องใช้ระบบร่วมกันกับระบบอื่นหรือผู้ใช้งานอื่น จะต้องมีการระบุความเสี่ยงและมีการยอมรับโดยเจ้าของระบบนั้น

๑๑. แนวปฏิบัติในการป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)

๑๑.๑ การป้องกันอุปกรณ์สื่อสารประเภทพกพา ให้ปฏิบัติตาม *“แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา” (ส่วนที่ ๖)*

๑๑.๒ ผู้ใช้งานต้องดำเนินการเพื่อระมัดระวังเป็นพิเศษตามสมควรในการประมวลผลและการสื่อสารโดยใช้อุปกรณ์มือถือ

๑๑.๓ ผู้ใช้งานต้องระมัดระวังในการใช้อุปกรณ์ประมวลผลบนอุปกรณ์มือถือนอกสถานที่ทำงานที่ได้รับการป้องกัน

๑๑.๔ ผู้ใช้งานต้องมีระบบป้องกันการเข้าถึงข้อมูลหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

๑๑.๕ ผู้ใช้งานอุปกรณ์มือถือต้องระมัดระวังการแอบดูข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต

๑๑.๖ ผู้ใช้งานต้องมีกระบวนการเพื่ออัพเดตระบบป้องกันซอฟท์แวร์ไม่พึงประสงค์

๑๒. แนวปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๑๒.๑ สถาบันอนุญาตกิจกรรมการใช้งานระบบทางไกลให้เฉพาะกิจกรรมที่มีการบริหารจัดการความปลอดภัยที่ดีสอดคล้องกับ *“แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันพัฒนาองค์กรชุมชน”* ซึ่งจัดให้มีการป้องกันที่เหมาะสมต่อการขโมย การเปิดเผยข้อมูล และการเข้าถึงข้อมูลที่ไม่เหมาะสม

๑๒.๒ การทำงานทางไกลจะต้องได้รับอนุญาต จากหัวหน้าส่วนงานและมีการควบคุมด้านความปลอดภัยอย่างเหมาะสมจากสำนักเทคโนโลยีสารสนเทศ โดยเฉพาะการเข้าถึงข้อมูลจากระยะไกล (Remote Access)

๑๓. แนวปฏิบัติการใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities)

๑๓.๑ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ ผู้ดูแลระบบจะต้องทำการกำหนดระดับสิทธิของผู้ขอใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

๑๓.๒ โปรแกรมอรรถประโยชน์ที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของสถาบัน ต้องเป็นโปรแกรมที่สถาบันได้ซื้อลิขสิทธิ์ หรือได้รับอนุญาตอย่างถูกต้องตามกฎหมายเท่านั้น

๑๓.๓ มีการจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์

๑๓.๔ ต้องยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์และซอฟท์แวร์ที่เกี่ยวข้องที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

ส่วนที่ ๑๙
แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

๒. แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

ให้เป็นไปตามระเบียบของสถาบันที่ออกตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ส่วนที่ ๑๘
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๑. วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันพัฒนาองค์กรชุมชน สามารถปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยซเบอร์อันเป็นข้อกำหนดขั้นต่ำ ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง กรตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากลเพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอกอย่างน้อย ปีละ ๑ (หนึ่ง ครั้ง โดยมีขอบเขตของการตรวจสอบอย่างน้อย ดังนี้

๑) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน

หน่วยงานต้องจัดส่งรายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก มายังคณะอนุกรรมการ ภายในสามสิบ (๓๐) วันนับถัดจากวันที่ได้รับรายงานการตรวจสอบ

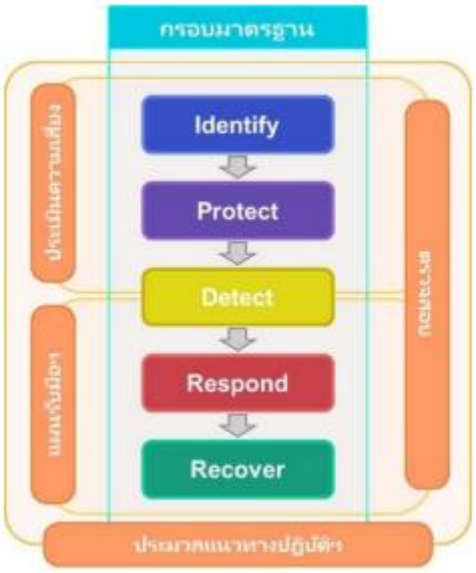
แผนการรับมือภัยคุกคามทางไซเบอร์

หน่วยงานต้องดำเนินการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

- จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response plan)
- ตรวจสอบแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากร ที่เกี่ยวข้อง
- ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง
- ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมี

นัยสำคัญ

- ในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงาน หรือข้อกำหนด ในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- ฝึกซ้อมการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ ๑๗.๑ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคง ปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด

๑๗.๒ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบ ด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา ๕๔ พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

ทั้งนี้ รูปแบบและรายละเอียดผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ให้สำนักงานประกาศกำหนด

๑๗.๓ ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑๗.๑ เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ส่ง

แผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบโดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ

(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ ๑๗.๓ (ก) - 4 –

๑๗.๔ ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

๑๗.๕ เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม

แผนการรับมือภัยคุกคามทางไซเบอร์

ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ

(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆเพื่อสนับสนุนการสอบสวน

(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ(ฌ) กระบวนการทบทวนหลังการ

ดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

ส่วนที่ ๒๐
แนวปฏิบัติการควบคุมแอพพลิเคชั่น

๑. วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยไม่ได้รับอนุญาต

๒. แนวทางการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

แนวทางการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการ ดังนี้

๒.๑ ผู้ดูแลระบบ (Administrator) ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User) การกำหนดสิทธิ์ตามตำแหน่งและหน้าที่ที่ได้รับมอบหมาย และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Right อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้างซึ่งรวมถึงบุคคลภายนอกหรือผู้รับจ้าง (Outsource) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศด้วย

๒.๒ ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งาน (User) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายภายนอกให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (VPN : Visual Private Network) โดยมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL)

๒.๓ ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญเช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒.๔ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

- กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
- กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับ
- ความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่า เข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๕ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึง

ข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

- ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล
- กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น
- กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
- กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงานเช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒.๖ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

- แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่นๆ
- มีการควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน
- มีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น

๒.๗ การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

- ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพ พร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์
- ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป
- เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที
- เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย
- หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๒.๘ การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) ผ่านระบบ

๒.๘.๑ ก่อนปฏิบัติงาน

- ผู้รับจ้าง (Outsource) ต้องขออนุญาตผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศสำหรับผู้รับจ้างพร้อมแนบสำเนาสัญญาจ้างหรือเหตุผลในการปฏิบัติงาน
- ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายพิจารณาเหตุผลการขออนุญาตดังกล่าวและต้องอนุมัติเป็นลายลักษณ์อักษร
- ผู้ดูแลระบบ (Administrator)ดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านชั่วคราว (Temporary Password) สำหรับเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ
- ผู้ดูแลระบบ (Administrator) แจ้งให้ผู้รับจ้าง (Outsource) ได้รับทราบ

๒.๘.๒ ระหว่างปฏิบัติงาน

- ผู้รับจ้าง (Outsource) ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน
- เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศต้องกำกับดูแลการปฏิบัติงานของผู้รับจ้าง (Outsource) ตลอดระยะเวลาการดำเนินการ
- ผู้รับจ้าง (Outsource) ต้องปฏิบัติงานตามหน้าที่ที่ได้ รับมอบหมายเท่านั้น และต้องคำนึงถึงการรักษาความลับข้อมูลของทางราชการเป็นสำคัญ หากเกิดปัญหาระหว่างการปฏิบัติงานให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศที่กำกับดูแลการปฏิบัติงานทันที

๒.๘.๓ หลังปฏิบัติงาน

- ผู้รับจ้าง (Outsource) แจ้งความประสงค์ต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือตัวแทนฝ่ายบริหาร SMR เพื่อยกเลิกสิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศทันทีเมื่อปฏิบัติงานแล้วเสร็จ
- ผู้ดูแลระบบ (Administrator) จะยกเลิกสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนทศและลบข้อมูลสารสนเทศของผู้รับจ้าง (Outsource) เป็นการถาวรเมื่อพ้นกำหนด ๙๐ วัน

๒.๘.๔ การรักษาความลับ

ผู้รับจ้าง (Outsource) ต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงานโดยสัญญาหรือข้อตกลงดังกล่าว ต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าถึงระบบ

คอมพิวเตอร์และระบบสารสนเทศ

ส่วนที่ ๒๑
แนวปฏิบัติการเข้ารหัสข้อมูล (Cryptographic)

๑. วัตถุประสงค์

เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึงหรือ เปลี่ยนแปลง แก้ไขข้อมูลที่เป็นความลับ หรือ มีความสำคัญ

๒. แนวทางการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

แนวทางการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการ ดังนี้

๒.๑ ผู้ดูแลระบบ (Administrator) ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User) การกำหนดสิทธิ์ตามตำแหน่งและหน้าที่ที่ได้รับมอบหมาย และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Right อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้างซึ่งรวมถึงบุคคลภายนอกหรือผู้รับจ้าง (Outsource) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศด้วย

๒.๒ ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งาน (User) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายภายนอกให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (VPN : Visual Private Network) โดยมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL)

๒.๓ ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญเช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๒.๔ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

- กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
- กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับ
- ความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่า เข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๕ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึง

ข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

- ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล
- กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น
- กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
- กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงานเช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒.๖ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

- แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่นๆ
- มีการควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน
- มีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น

๒.๗ การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

- ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพ พร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์
- ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป
- เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที
- เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย
- หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๒.๘ การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) ผ่านระบบ

๒.๘.๑ ก่อนปฏิบัติงาน

- ผู้รับจ้าง (Outsource) ต้องขออนุญาตผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศสำหรับผู้รับจ้างพร้อมแนบสำเนาสัญญาจ้างหรือเหตุผลในการปฏิบัติงาน
- ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายพิจารณาเหตุผลการขออนุญาตดังกล่าวและต้องอนุมัติเป็นลายลักษณ์อักษร
- ผู้ดูแลระบบ (Administrator)ดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านชั่วคราว (Temporary Password) สำหรับเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ
- ผู้ดูแลระบบ (Administrator) แจ้งให้ผู้รับจ้าง (Outsource) ได้รับทราบ

๒.๘.๒ ระหว่างปฏิบัติงาน

- ผู้รับจ้าง (Outsource) ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน
- เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศต้องกำกับดูแลการปฏิบัติงานของผู้รับจ้าง (Outsource) ตลอดระยะเวลาการดำเนินการ
- ผู้รับจ้าง (Outsource) ต้องปฏิบัติงานตามหน้าที่ที่ได้ รับมอบหมายเท่านั้น และต้องคำนึงถึงการรักษาความลับข้อมูลของทางราชการเป็นสำคัญ หากเกิดปัญหาระหว่างการปฏิบัติงานให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศที่กำกับดูแลการปฏิบัติงานทันที

๒.๘.๓ หลังปฏิบัติงาน

- ผู้รับจ้าง (Outsource) แจ้งความประสงค์ต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือตัวแทนฝ่ายบริหาร SMR เพื่อยกเลิกสิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศทันทีเมื่อปฏิบัติงานแล้วเสร็จ
- ผู้ดูแลระบบ (Administrator) จะยกเลิกสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนทศและลบข้อมูลสารสนเทศของผู้รับจ้าง (Outsource) เป็นการถาวรเมื่อพ้นกำหนด ๙๐ วัน

๒.๘.๔ การรักษาความลับ

ผู้รับจ้าง (Outsource) ต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงานโดยสัญญาหรือข้อตกลงดังกล่าว ต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ