



บันทึกข้อความ

ส่วนราชการ กองยุทธศาสตร์และงบประมาณ ฝ่ายสถิติข้อมูลและสารสนเทศ โทร.๓๐๕

ที่ สบ.๕๑๐๐๗/๖๖๕๔๔

วันที่ ๖ สิงหาคม ๒๕๖๘

เรื่อง ประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ องค์การบริหาร
ส่วนจังหวัดสระบุรี ประจำปี พ.ศ. ๒๕๖๘

เรียน หัวหน้าส่วนราชการในสังกัดองค์การบริหารส่วนจังหวัดสระบุรี ทุกส่วน
และหัวหน้าหน่วยตรวจสอบภายใน

ด้วย องค์การบริหารส่วนจังหวัดสระบุรี ได้จัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การบริหารส่วนจังหวัดสระบุรี ประจำปี พ.ศ. ๒๕๖๘ เพื่อเป็นเครื่องมือให้กับผู้ปฏิบัติงาน ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศเพื่อให้การปฏิบัติงานและการบริหารราชการมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับขององค์การบริหารส่วนจังหวัดสระบุรี รายละเอียดตามเอกสารที่ส่งมาพร้อมนี้

จึงเรียนมาเพื่อทราบและถือเป็นแนวทางปฏิบัติ ต่อไป

(นายสุรศักดิ์ สมภักดี)

รองนายกองค์การบริหารส่วนจังหวัด ปฏิบัติราชการแทน
นายกองค์การบริหารส่วนจังหวัดสระบุรี



ประกาศองค์การบริหารส่วนจังหวัดสระบุรี
เรื่อง แผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
องค์การบริหารส่วนจังหวัดสระบุรี
ประจำปีงบประมาณ พ.ศ.๒๕๖๘

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ เพื่อให้การปฏิบัติงานและการบริหารราชการมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับองค์การบริหารส่วนจังหวัดสระบุรี จึงเห็นควรกำหนดแผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรี เพื่อเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรี โดยมีรายละเอียดดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศองค์การบริหารส่วนจังหวัดสระบุรี เรื่อง แผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ องค์การบริหารส่วนจังหวัดสระบุรี"

ข้อ ๒ วัตถุประสงค์ เพื่อให้ผู้ใช้งานระบบสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรี ได้ทราบถึงข้อปฏิบัติในการใช้งานระบบสารสนเทศให้เกิดความมั่นคงปลอดภัย ป้องกันการกระทำที่ละเมิดระเบียบกฎหมายหรือทำให้เกิดความเสียหายเนื่องมาจากการใช้งานระบบสารสนเทศ

ข้อ ๓ ขอบเขต ผู้ใช้งานระบบสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรีทุกคน จะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อ ๔ แผนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีรายละเอียดตามเอกสารแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๖ เดือน สิงหาคม พ.ศ. ๒๕๖๘

(นายสุรศักดิ์ สมภักดี)

รองนายกองค์การบริหารส่วนจังหวัด ปฏิบัติราชการแทน

นายกองค์การบริหารส่วนจังหวัดสระบุรี

แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ขององค์การบริหารส่วนจังหวัดสระบุรี พ.ศ.2568

คำนำ

แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรีฉบับนี้ จัดทำขึ้นตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ ที่กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้รวมถึงเป็นมาตรการในการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ฝ่ายสถิติข้อมูลและสารสนเทศ กองยุทธศาสตร์และงบประมาณ

วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรีหรือต่อไปนีเรียกว่า "หน่วยงาน" เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ หน่วยงานจึงเห็นสมควรกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้มีมาตรฐานแนวปฏิบัติ ขั้นตอนปฏิบัติ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและข้อมูลส่วนบุคคล ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของหน่วยงานให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอก ที่ปฏิบัติงานให้กับหน่วยงานตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๓. เพื่อเป็นกรอบและแนวทางการพัฒนาและปรับปรุงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การบริหารส่วนจังหวัดสระบุรี พร้อมยกระดับมาตรฐานในการรักษาความมั่นคงและปลอดภัยให้มากยิ่งขึ้น

๔. เพื่อเผยแพร่ให้เจ้าหน้าที่ผู้ปฏิบัติงานทุกระดับในหน่วยงานได้รับทราบและถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด

สารบัญ

คำนิยาม	หน้า
หมวดที่ ๑ การควบคุมและการเข้าถึงการใช้งานระบบสารสนเทศ	๔
ส่วนที่ ๑. การควบคุมการเข้าถึงสารสนเทศ	๕
ส่วนที่ ๒. การบริหารจัดการการเข้าถึงของผู้ใช้	๗
ส่วนที่ ๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน	๙
ส่วนที่ ๔. การบริหารจัดการสินทรัพย์	๑๑
ส่วนที่ ๕. การควบคุมการเข้าถึงเครือข่าย	๑๒
ส่วนที่ ๖. การควบคุมการเข้าถึงระบบปฏิบัติการ	๑๗
ส่วนที่ ๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ	๑๙
ส่วนที่ ๘. การบริหารจัดการซอฟต์แวร์ลิขสิทธิ์และการป้องกันโปรแกรมที่ไม่ประสงค์ดี	๒๑
ส่วนที่ ๙. การปฏิบัติงานจากภายนอกสำนักงาน	๒๓
ส่วนที่ ๑๐. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย	๒๓
ส่วนที่ ๑๑. การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย	๒๔
ส่วนที่ ๑๒. การควบคุมการใช้จดหมายอิเล็กทรอนิกส์	๒๕
ส่วนที่ ๑๓. การควบคุมการใช้อินเทอร์เน็ต	๒๖
ส่วนที่ ๑๔. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์แบบพกพา	๒๗
ส่วนที่ ๑๕. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์	๒๙
หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและการสำรองข้อมูล	๓๐
ส่วนที่ ๑. การรักษาความปลอดภัยฐานข้อมูล	๓๐
ส่วนที่ ๒. การสำรองข้อมูล	๓๒
ส่วนที่ ๓. การกู้คืนข้อมูล	๓๓
ส่วนที่ ๔. การทดสอบสภาพพร้อมใช้งาน	๓๔
หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	๓๕
ส่วนที่ ๑. การตรวจสอบและประเมินความเสี่ยง	๓๕
ส่วนที่ ๒. แนวทางในการตรวจสอบและประเมินที่ต้องคำนึงถึง	๓๕
ส่วนที่ ๓. ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ	๓๖
หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่และสภาพแวดล้อม	๓๘
หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ	๔๒
หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศ	๔๔
หมวดที่ ๗ หน้าที่และความรับผิดชอบ	๔๖

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ขององค์การบริหารส่วนจังหวัดสระบุรี พ.ศ. ๒๕๖๘

ตามประกาศองค์การบริหารส่วนจังหวัดสระบุรี เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรีเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้น จากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อองค์กร องค์การบริหารส่วนจังหวัดสระบุรีจึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

คำนิยาม

"หน่วยงาน" หมายถึง องค์การบริหารส่วนจังหวัดสระบุรี

"ผู้ใช้งาน" หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของหน่วยงานโดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ตามที่หน่วยงานกำหนดไว้ดังนี้

๑. "ผู้บริหาร" หมายถึงผู้มีอำนาจบริหารในระดับสูงของหน่วยงาน

๒. "ผู้ดูแลระบบ" (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการบริหาร หรือดูแลรักษาระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

๓. "เจ้าหน้าที่" หมายถึง ข้าราชการ ลูกจ้าง พนักงานราชการ และเจ้าหน้าที่ผู้ปฏิบัติงาน

๔. "ผู้ใช้งานทั่วไป" หมายถึง ประชาชน หรือผู้รับบริการทั่วไปที่ไม่ใช่เจ้าหน้าที่ของหน่วยงาน

"เจ้าของข้อมูล" หมายถึง ผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

"สิทธิ์ของผู้ใช้งาน" หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิ์ในการใช้สินทรัพย์

"สินทรัพย์" หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพา อุปกรณ์สื่อสารที่สามารถเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ได้แก่ อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์ และซอฟต์แวร์ที่มีลิขสิทธิ์

"การรักษาความมั่นคงปลอดภัย" หมายถึงการรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

"หน่วยงานภายนอก" หมายถึง องค์กรหรือหน่วยงานภายนอกที่หน่วยงานอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงานโดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล

"มาตรฐาน" (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

"แนวทางปฏิบัติ" (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

"ข้อมูลคอมพิวเตอร์" หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และฉบับแก้ไขเพิ่มเติม

"จดหมายอิเล็กทรอนิกส์" (Electronic mail : e-Mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกันข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

"ชื่อผู้ใช้" (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

"รหัสผ่าน" (Password) หมายถึง ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"สารสนเทศ" (Information) หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผนการตัดสินใจและอื่น ๆ

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่ายคอมพิวเตอร์" (Computer Network System) หมายถึง ระบบคอมพิวเตอร์ที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของหน่วยงาน ได้แก่ ระบบเครือข่ายภายใน (Local Area Network :LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wireless LAN หรือ WIFI) เป็นต้น

"ระบบเทคโนโลยีสารสนเทศ" (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมประยุกต์ ข้อมูลและสารสนเทศ เป็นต้น

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้อย่างก็ได้

"ความมั่นคงปลอดภัยด้านสารสนเทศ" (Information Security) หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายถึง การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

หมวดที่ ๑

การควบคุมและการเข้าถึงการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์และการมอบอำนาจของหน่วยงาน

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ หน่วยงานต้องทำการประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามแนวนโยบายและแนวปฏิบัติได้ด้วยวิธีการใดวิธีการหนึ่ง ดังนี้

๓.๑ หนังสือเวียนภายในหน่วยงาน

๓.๒ Website ของหน่วยงาน

ผู้รับผิดชอบตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยงานกำหนดให้ผู้ใช้งานเป็นผู้รับผิดชอบตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยมีผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

๑. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมการตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติการ ผู้รับผิดชอบ ได้แก่

๑. นายกองค์การบริหารส่วนจังหวัดสระบุรี ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้ที่นายกองค์การบริหารส่วนจังหวัดสระบุรี มอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของหน่วยงาน

๒. ปลัดองค์การบริหารส่วนจังหวัดสระบุรี

๒. ระดับบริหาร

รับผิดชอบ กำกับดูแล การปฏิบัติงานของผู้ใต้บังคับบัญชา ศึกษาทบทวน วางแผน ติดตาม การบริหาร ความเสี่ยงและระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ผู้รับผิดชอบ ได้แก่

๑. ปลัดองค์การบริหารส่วนจังหวัดสระบุรี

๒. รองปลัดองค์การบริหารส่วนจังหวัดสระบุรี

๓. ผู้อำนวยการสำนัก/กอง

๔. ผู้อำนวยการส่วน/หัวหน้าฝ่าย

๓. ระดับปฏิบัติการ

๓.๑ รับผิดชอบดูแลบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่ายและความปลอดภัยของฐานข้อมูลทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไข ซ่อมกพร่องต่าง ๆ ของระบบคอมพิวเตอร์และระบบเครือข่ายรวมทั้งการทำสำเนาข้อมูล (Backup) และกู้คืนฐานข้อมูล (Recovery) ของระบบฐานข้อมูลสารสนเทศ ข้อมูลสำหรับระบบและโปรแกรมระบบ ผู้รับผิดชอบ ได้แก่

- หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ
- เจ้าหน้าที่ที่เกี่ยวข้องที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบ

๓.๒ รับผิดชอบในการอนุมัติสิทธิการเข้าใช้ระบบงาน รวมถึงการรักษาความปลอดภัยของแต่ละระบบงานสารสนเทศ ผู้รับผิดชอบ ได้แก่

- หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ
- เจ้าหน้าที่ที่เกี่ยวข้องที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑. หน่วยงาน ต้องระบุวัตถุประสงค์การใช้งานสารสนเทศแต่ละชนิด เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลให้มีความมั่นคงและปลอดภัย โดยมีข้อปฏิบัติการเข้าถึงและการใช้งานสารสนเทศ ดังนี้

๑. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศเท่านั้น

๒. เจ้าของข้อมูล และ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานนั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓. ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ และในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำบันทึกขออนุญาตจากผู้บริหารและแจ้งฝ่ายสถิติข้อมูลและสารสนเทศ เพื่อขอสิทธิ์ในการเข้าระบบเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภท ข้อมูลและชั้นความลับ เพื่อการจัดเก็บไว้เป็นหลักฐานรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ ๒. หน่วยงาน ต้องกำหนดสิทธิ์ หรือมอบอำนาจการใช้งานสารสนเทศแต่ละชนิดเพื่อควบคุมการอนุญาตให้เข้าถึงสารสนเทศที่สำคัญ โดยมีการแบ่งแยกอำนาจหน้าที่ของบุคลากรในส่วนของงานคอมพิวเตอร์ ดังนี้

๑. หน่วยงานต้องควบคุมการให้สิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับอำนาจหน้าที่และความจำเป็นของของผู้ใช้งานอย่างเคร่งครัด

๒. แบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนของการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่ดูแลระบบ ที่ปฏิบัติงานอยู่ในส่วนคอมพิวเตอร์

๓. ต้องกำหนดหน้าที่รับผิดชอบของงานในแต่ละหน้าที่ที่ปฏิบัติงานอยู่ในส่วนคอมพิวเตอร์อย่างชัดเจน เป็นลายลักษณ์อักษร

๔. ผู้ดูแลระบบ และเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer operator) ต้องสำรองในงานที่สำคัญเพื่อทำงานทดแทนในกรณีจำเป็น

๕. ต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

๖. ต้องตรวจสอบคุณสมบัติและอำนาจหน้าที่ของผู้ใช้งานอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องยกเลิกหรือเปลี่ยนแปลงสิทธิ์ให้สอดคล้องกับระดับชั้นการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศทันที

๗. ต้องมีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่เข้ามาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๘. ต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ โดยมีระบบสารสนเทศที่สำคัญ ดังนี้

- ระบบพินิจสิทธิ์ (Active Directory : AD)
- ระบบเครือข่ายไร้สาย (WIFI หรือ Wireless LAN)
- ระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail :e-Mail)
- ระบบบริหารสำนักงานอัตโนมัติ (e-Office)

ข้อ ๓. หน่วยงาน ต้องกำหนดประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับ รวมถึงระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึงสารสนเทศแต่ละชนิดอย่างเหมาะสม ดังนี้

๑. ประเภทของข้อมูลแบ่งออกเป็น ได้แก่

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลคำรับรอง ข้อมูลงบประมาณการเงินและการบัญชี ข้อมูลระบบบริหารสำนักงานอัตโนมัติ (e-Office)

- ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข่าวประชาสัมพันธ์ ข่าวจัดซื้อจัดจ้าง และข้อมูลอื่นๆที่เผยแพร่บนเว็บไซต์

๒. ลำดับความสำคัญ เป็นลำดับความสำคัญของข้อมูลที่หน่วยงานกำหนด ดังนี้

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๓. ลำดับชั้นความสำคัญของข้อมูล ได้แก่

- ลับที่สุด หมายถึง หากเปิดเผย จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงมากที่สุด

- ลับมาก หมายถึง หากเปิดเผย จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

- ลับ หมายถึง หากเปิดเผย จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๔. ระดับชั้นการเข้าถึง ได้แก่

- ระดับชั้นสำหรับผู้บริหาร สามารถเข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป สามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย มีสิทธิ์ในการบริหารจัดการระบบ และเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่

๕. เวลาเข้าถึงข้อมูล ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

๖. ช่องทางการเข้าถึงสารสนเทศ ได้แก่

- ระบบแลน (LAN) ในลักษณะ Client Server
- ระบบอินทราเน็ต (Intranet) ในลักษณะ Web Base Application
- ระบบอินเทอร์เน็ต (Internet) ในลักษณะ Web Base Application
- ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)

ข้อ ๔. ผู้ดูแลระบบต้องติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ ๕. ผู้ดูแลระบบต้องบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ และการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๖. ผู้ดูแลระบบต้องบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๗. ต้องสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงต้องกำหนดมาตรการเชิงป้องกันตามความเหมาะสม โดยมีข้อปฏิบัติ ดังนี้

๑. ต้องจัดทำคู่มือแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๒. ต้องฝึกอบรมให้ผู้ใช้งานตระหนักและเข้าใจในเรื่องภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ถูกต้อง ไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมทั้งมาตรการการป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

ข้อ ๘. การลงทะเบียนผู้ใช้งาน (User Registration Management) ผู้ดูแลระบบต้องกำหนดขั้นตอนการลงทะเบียนผู้ใช้งานใหม่ดังนี้

๑. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน เพื่อขอรับสิทธิ์ในการเข้าถึงระบบสารสนเทศที่เกี่ยวข้อง

๒. ตรวจสอบบัญชีผู้ใช้งานเพื่อไม่ให้เกิดการลงทะเบียนซ้ำซ้อน

๓. ตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๔. แจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิ์และหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ ๙. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Authentication Management)

๑. ผู้ดูแลระบบต้องกำหนดการใช้งาน ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) และระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

๒. ผู้ดูแลระบบต้องกำหนด Username และ Password เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับ

๓. ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ กำหนดสิทธิ์พิเศษที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ รวมถึงต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาหน่วยงานนั้น ๆ โดยต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง

ข้อ ๑๐. ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งานสิทธิ์การใช้งานอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตโดยปฏิบัติตามแนวทาง ดังนี้

๑. พิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงาน

๒. จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานเพื่อดำเนินการทบทวนรายชื่อและสิทธิ์การเข้าใช้งานว่าถูกต้องหรือไม่

๓. ดำเนินการแก้ไขข้อมูลสิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากหน่วยงาน

๔. ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งานเมื่อลาออก/โอน/ย้าย ต้องดำเนินการภายใน ๓ วันหรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน ๗ วัน

ข้อ ๑๑. การบริหารจัดการรหัสผ่านสำหรับผู้ดูแลระบบ

๑. กำหนดการเปลี่ยนแปลงและการยกเลิก Password เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๒. กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๓. ส่งมอบ Password ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่ง E-Mail ที่ไม่มีการป้องกันในการส่ง Password

๔. กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับ Password

๕. กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่ Password ผิดพลาดได้ไม่เกิน ๓ ครั้ง

๖. กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บ Password ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

ข้อ ๑๒. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังนี้

๑. ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒. กำหนด Username และ Password เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

๓. กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
 ๔. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล (SSL, VPN หรือ XML Encryption)
 ๕. กำหนดการเปลี่ยน Password ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
 ๖. กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ออกนอกหน่วยงาน เพื่อการบำรุงรักษา ตรวจสอบ โดยต้องให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อน
 ๗. เจ้าของข้อมูลต้องมีการตรวจสอบความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- ข้อ ๑๓.** ระบบงานสารสนเทศที่เชื่อมโยงกัน (Link Information Systems) ให้หัวหน้าหน่วยงานพิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัยและจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงาน หรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน ระหว่างหน่วยงานกับหน่วยงานหรือหน่วยงานภายนอกที่มาขอเชื่อมโยง ดังนี้
๑. กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน
 ๒. พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล
 ๓. พิจารณามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน
 ๔. พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน
 ๕. ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

- ข้อ ๑๔.** การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้
๑. ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชี Username และ Password โดยผู้ใช้งานแต่ละคนต้องมีบัญชี Username ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ Password
 ๒. กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)
 ๓. ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว
 ๔. ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
 ๕. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
 ๖. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
 ๗. กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

๘. ผู้ใช้งานต้องเปลี่ยน Password ไม่เกิน ๑๘๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๑๕. การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

ข้อ ๑๖. การกระทำใด ๆ ที่เกิดจากการใช้บัญชี Username อันมีกฎหมายกำหนดให้เป็นความผิดไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๑๗. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงานและหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล้า หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

๑. คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
๒. การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง
๓. การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

๔. เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

๕. เครื่องคอมพิวเตอร์ทุกเครื่องต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที

๖. ผู้ใช้ต้องทำการ Log out ออกจากระบบทันที เมื่อเลิกใช้ระบบสารสนเทศ

ข้อ ๑๘. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของหน่วยงานหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๙. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๒๐. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลขององค์การบริหารส่วนจังหวัดสระบุรี หากเกิดการสูญหาย นำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๑. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๒๒. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควรหน่วยงานจะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณี ที่หน่วยงานต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับหน่วยงาน ซึ่งหน่วยงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer to Peer (หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน

หมายความว่า แต่ละเครื่องต้องมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่อง File Server เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน ได้แก่บิทเทอร์เรนท์ (Bittorrent) และอีมูล (Emule) เว้นแต่จะได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๒๔. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เล่นเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๒๕. ห้ามใช้สินทรัพย์ของหน่วยงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของหน่วยงาน

ข้อ ๒๖. ห้ามใช้สินทรัพย์ของหน่วยงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูลหรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของหน่วยงาน

ข้อ ๒๗. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อประโยชน์ทางการค้า

ข้อ ๒๘. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใด ภายในเครือข่ายระบบสารสนเทศของหน่วยงานโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๒๙. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

ข้อ ๓๐. ห้ามใช้ระบบสารสนเทศของหน่วยงานเพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓๑. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๒. ห้ามติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๓๓. ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Data Center) หมายถึง สถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์บริหารจัดการเครือข่าย) ที่เป็นเขตหวงห้าม โดยเด็ดขาดเว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๔. ผู้ใช้งานต้องจัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่ที่มั่นคง ปลอดภัย จากการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๓๕. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใดเชื่อมต่อเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๓๖. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใด ๆ

ข้อ ๓๗. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว ควรใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
Flash Drive	- การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๕๒ M ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดย การเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การหันด้วยเครื่องหันทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๕๒ M ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดย การเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

ข้อ ๓๘. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่หน่วยงานมอบไว้ให้ใช้งานเสมือนเป็นสินทรัพย์ของผู้ใช้งานเอง โดยรายการสินทรัพย์ (Asset lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่พัสดุที่หน่วยงานมอบหมาย

ข้อ ๓๙. กรณีทำงานนอกสถานที่ ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมาย

ข้อ ๔๐. ผู้ใช้งานมีหน้าที่ต้องชดเชยค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สินหากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๔๑. ผู้ใช้งานต้องไม่ให้อื่นยืม คอมพิวเตอร์ โน้ตบุ๊ก หรือ แท็บเล็ต ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา

ข้อ ๔๒. ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งานโดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อหน่วยงาน

ข้อ ๔๓. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๔๒ ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นแต่เพียงผู้เดียว

ส่วนที่ ๕ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ข้อ ๔๔. การควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๑. ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตร ผู้ติดต่อ (Visitor) แล้วทำการลงบันทึกข้อมูล ลงในสมุดบันทึกการเข้าออกพื้นที่

๒. ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ ในแบบฟอร์มการขออนุญาตเข้าออกพื้นที่ ให้ถูกต้องชัดเจน

๓. ผู้ดูแลระบบ ต้องตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก แบบฟอร์มการขออนุญาตเข้าออกกับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ข้อ ๔๕. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานหรือเจ้าหน้าที่ที่หัวหน้าหน่วยงานมอบหมาย และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษร

ข้อ ๔๖. การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ ต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้งานอื่น ๆ

ข้อ ๔๗. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) และอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔๘. ผู้ดูแลระบบ ต้องควบคุมการเชื่อมต่อทางเครือข่ายคอมพิวเตอร์ เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ โดยมีแนวทางปฏิบัติ ดังต่อไปนี้

๑. จัดทำบันทึกการกำหนดขอบเขตและสิทธิ์ของผู้ใช้งานที่สามารถเข้าถึงบริการต่าง ๆ ในระบบเครือข่ายของหน่วยงานตามที่กำหนดเท่านั้น

๒. กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓. ควบคุมการเข้าถึงหรือใช้งานเครือข่ายคอมพิวเตอร์ที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

๔. ผู้ใช้งานต้องเข้าใช้งานระบบสารสนเทศที่สำคัญตามข้อปฏิบัติที่หน่วยงานกำหนดขึ้นมา ได้แก่ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (wireless LAN) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๕. ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for external connections) จะต้องมีการยืนยันตัวตนก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้ดังนี้

- ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ทุกครั้ง

- การอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานต้องขึ้นอยู่กับความจำเป็นของการดำเนินงานและด้านเทคนิค รวมทั้งต้องได้รับความเห็นชอบจากผู้บังคับบัญชา

- หากหน่วยงานหรือผู้ปฏิบัติงานที่มีความประสงค์ขอใช้ชื่อผู้ใช้งาน จะต้องได้รับความเห็นชอบจากผู้บังคับบัญชา โดยจะต้องรับผิดชอบหากเกิดข้อผิดพลาดที่เกิดขึ้นทั้งสิ้น

๖. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๗. การระบุอุปกรณ์บนเครือข่าย (Equipments Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

- การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของหน่วยงานต้องได้รับอนุญาตจากนายกองค์การบริหารส่วนจังหวัดสระบุรี ก่อนจึงจะสามารถดำเนินการได้

- ผู้ดูแลระบบเครือข่ายมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิ์ในการเชื่อมต่อตามที่นายกองค์การบริหารส่วนจังหวัดสระบุรี กำหนด และสามารถรับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

- จะต้องมีการจำกัดสิทธิ์วิธีการเข้าใช้อุปกรณ์ได้โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

๘. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

- ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทั้งทางกายภาพและโดยการล็อกอินเข้าใช้งาน

- ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่า configuration ไว้ในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

- ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

- เปิดพอร์ตที่มีความจำเป็นในการใช้งาน และยกเลิกหรือปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

- ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

- กำหนดสิทธิ์บุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

- บันทึกการเข้า - ออกพื้นที่บริเวณห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง และ เจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

- ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์หากจำเป็นให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป

- ติดตั้งเครื่องควบคุมบันทึกการเข้าออกห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ที่ประตูเข้าออกและติดตั้งกล้องโทรทัศน์วงจรปิด ป้องกันการโจรกรรม

๙. กำหนดวิธีการป้องกันช่องทางที่ใช้ในการบำรุงรักษาระบบผ่านเครือข่าย การตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

๑๐. ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๑๑. ทำการแบ่งแยกเครือข่าย (Segregation in Networks) สำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

๑๒. มีการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ที่ใช้ในการเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลไม่ถูกเปิดเผย ดังนี้

- ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) ของหน่วยงาน

- กำหนดให้มีการแปลงหมายเลขเครือข่ายย่อย

- กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย หรือจำกัดสิทธิ์ในการใช้บริการเครือข่ายของหน่วยงาน

๑๓. ผู้ดูแลระบบเครือข่ายกำหนดมาตรการควบคุมการเข้าใช้งานระบบจากภายนอก (Remote Access) เพื่อรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายของหน่วยงาน ที่ต้องผ่านการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน และต้องได้รับอนุญาตจากหน่วยงานหรือผู้ดูแลระบบเป็นลายลักษณ์อักษรเท่านั้น และผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดของหน่วยงานอย่างเคร่งครัด โดยดำเนินการ ดังนี้

- ผู้ดูแลระบบเครือข่ายต้องไม่เปิด Port และ Modem ที่เอาไว้อย่างไม่จำเป็น

- ปิดช่องทางการเชื่อมต่อเมื่อไม่ใช้งานแล้ว และเปิดใช้งานเมื่อมีการร้องขอเท่าที่จำเป็น

- มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมตามความเหมาะสม

- วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากภายนอก (Remote Access) ต้องได้รับการอนุมัติจากผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

ข้อ ๔๙. ผู้ดูแลระบบ ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อบริหารจัดการเส้นทางบนระบบเครือข่ายได้อย่างมีประสิทธิภาพ โดยมีแนวทางปฏิบัติ ดังต่อไปนี้

๑. ต้องใช้เกตเวย์ (Gateway) หรืออุปกรณ์เครือข่ายตรวจสอบ (IP Address) ของทั้งต้นทางและปลายทาง และควบคุมการไหลของข้อมูลผ่านเครือข่ายต่าง ๆ จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง

๒. ต้องควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๓. ต้องกำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อยหรือเครือข่ายภายในและภายนอก

๔. ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย เพื่อไม่อนุญาตให้ผู้ให้บริการสามารถใช้เส้นทางอื่น ๆ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

๕. ต้องกำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้

ข้อ ๕๐. ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server System) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๕๑. การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ

ข้อ ๕๒. ต้องจัดเก็บซอร์สโค้ด (Source Code) ไลบรารี (Library) และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

ข้อ ๕๓. ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางที่กำหนดไว้ใน พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ข้อ ๕๔. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายจากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังนี้

๑. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้าหน่วยงาน

๒. ต้องควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๓. วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

๔. การเข้าสู่ระบบจากระยะไกล (Remote Access) ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๕. การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้อง Login โดยแสดงตัวตนด้วย Username และ Password เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

ข้อ ๕๕. กำหนดให้มีการแบ่งแยกเครือข่าย (Segregation in Networks) ดังต่อไปนี้

๑. Internet แบ่งแยกเครือข่ายเป็นเครือข่ายภายนอก และเครือข่ายไร้สาย เพื่อควบคุมปริมาณและการเข้าถึงในแต่ละเครือข่ายอย่างปลอดภัย

๒. Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายในหน่วยงาน

ข้อ ๕๖. กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

ข้อ ๕๗. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

ข้อ ๕๘. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย จากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

ข้อ ๕๙. IP address ของระบบงานเครือข่ายภายใน จำเป็นต้องป้องกันไม่ให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้นักภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ข้อ ๖๐. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๖๑. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของหน่วยงาน (โดยปฏิบัติตามข้อ ๘) ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน (โดยปฏิบัติตามข้อ ๑๐) จากการลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน

ข้อ ๖๒. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งาน

๑. ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
๒. หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที
๓. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่ Password เพื่อเข้าใช้งาน
๔. ก่อนการเข้าใช้ระบบปฏิบัติการต้องทำการ Login ทุกครั้ง
๕. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ Username และ Password ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน
๖. ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอ
๗. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ
๘. ซอฟต์แวร์ที่หน่วยงานใช้ มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามมิให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใด ที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว
๙. ซอฟต์แวร์ที่หน่วยงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น
๑๐. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของหน่วยงาน เพื่อประโยชน์ทางการค้า

๑๑. ในกรณีผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ ห้ามผู้ใช้งานนำเสนอข้อมูล
ที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพที่ไม่เหมาะสม หรือขัดต่อศีลธรรม

๑๒. ห้ามผู้ใช้งานของหน่วยงาน ควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก
หน่วยงานโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๖๓. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)
กำหนดให้ผู้ใช้งานต้องมีข้อมูลเฉพาะเจาะจงที่ใช้ในการยืนยันตัวตนของผู้ใช้งาน สามารถตรวจสอบได้ดังนี้

๑. ผู้ใช้งานต้องระบุชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งาน
ระบบสารสนเทศของหน่วยงาน

๒. หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับ
กับความจำเป็นของหน่วยงานทางด้านภารกิจหรือด้านเทคนิค

๓. สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token Key HandScan
หรือ Finger Print เป็นต้น ตามความเหมาะสมของแต่ละระบบงานของหน่วยงานได้

ข้อ ๖๔. การบริหารจัดการรหัสผ่าน (Password Management System) มีแนวปฏิบัติดังนี้

๑. ต้องจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมี
การทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๒. ต้องจำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวน
ครั้งที่กำหนดระบบจะทำการล็อกสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบ
จะปลดล็อกให้

๓. ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่า มีความพยายามในการ
เดารหัสผ่านจากเครื่องปลายทาง

๔. มีระบบให้ผู้ใช้งาน สามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

๕. ต้องเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกออกจากข้อมูลระบบงาน

๖. ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่าน
ของตนเอง แต่แสดงเป็นเครื่องหมายจุด (.) หรือดอกจัน (*) บนหน้าจอแทน

๗. เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อ
ผู้ใช้งานที่ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

ข้อ ๖๕. การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุม
การใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรม
อรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัย
ของระบบได้ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว
ให้ดำเนินการ ดังนี้

๑. การใช้งานโปรแกรมอรรถประโยชน์ ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และต้องมีการ
พิสูจน์ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

๒. โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

๓. ต้องจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน

๔. ต้องจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์

๕. ต้องยกเลิกหรือลบทั้งโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

ข้อ ๖๖. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time - Out)

๑. ให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีการใช้งานในช่วงระยะเวลาตั้งแต่ ๑๕ นาที เป็นต้นไป

๒. ให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบสารสนเทศที่มีความเสี่ยงสูง

ข้อ ๖๗. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยง หรือมีความสำคัญสูง ดังนี้

๑. กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

๒. การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ข้อ ๖๘. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุม การเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ ดังนี้

๑. การจำกัดการเข้าถึงของผู้ใช้งาน

- เข้าได้ตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น
- กำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล
- บันทึกการออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

๒. แบ่งกลุ่มเจ้าหน้าที่ที่ปฏิบัติงานด้านสารสนเทศของหน่วยงานออกเป็น ๓ กลุ่ม ได้แก่ ผู้ดูแลระบบ ผู้พัฒนาระบบงาน และผู้ใช้งานระบบ โดยกำหนดหน้าที่รับผิดชอบอย่างชัดเจนเป็นลายลักษณ์อักษร

๓. ต้องกำหนดสิทธิ์การใช้งานระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ ดังกล่าวอย่างสม่ำเสมอ

๔. ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Login ด้วย Username และ Password ก่อนเข้าระบบสารสนเทศอีกครั้ง

๕. ต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ข้อมูลพฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ ดังนี้

- ชื่อบัญชีผู้ใช้งาน (Username)
- วัน เวลาที่เข้าถึงระบบ (Login)
- วัน เวลาที่ออกจากระบบ (Logout)
- เหตุการณ์สำคัญที่เกิดขึ้น
- การเข้าใช้ทั้งที่สำเร็จและไม่สำเร็จ
- ความพยายามในการเข้าถึงทรัพยากร ทั้งที่สำเร็จและไม่สำเร็จ
- การแสดงการใช้สิทธิ์
- การแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์
- หมายเลขไอพีแอดเดรสที่เข้าถึง
- การแสดงการหยุดทำงานของระบบป้องกันการบุกรุก
- การแสดงการหยุดทำงานของระบบงานที่สำคัญ ๆ

ข้อ ๖๙. ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๑. กำหนดการเปลี่ยนแปลงและการยกเลิก Password เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒. กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บ Password ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓. กำหนด Username หรือ Password ต้องไม่ซ้ำกัน

๔. ในกรณีที่มีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงานหรือเจ้าหน้าที่ที่หน่วยงานมอบหมาย โดยมีการกำหนดระยะเวลา การใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๗๐. ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๑. ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒. ต้องกำหนด Username และ Password เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

๓. กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๔. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล (SSL, VPN หรือ XML Encryption)

๕. กำหนดการเปลี่ยน Password ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๖. กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าสินทรัพย์ออกนอกหน่วยงาน เพื่อการบำรุงรักษา ตรวจสอบ ให้ดำเนินการสำรองและลบข้อมูล ที่เก็บอยู่ในสื่อบันทึกก่อน

ข้อ ๗๑. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

๑. ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูง ได้แก่ ระบบบริหารสำนักงานอัตโนมัติ (e-Office) ระบบบุคลากร ระบบการเงินและการบัญชี ต้องแยกออกจากระบบอื่น และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

๒. ต้องควบคุมสภาพแวดล้อมของระบบ ซึ่งไวต่อการรบกวนโดยเฉพาะ ดังนี้

- มีห้องปฏิบัติการแยกเป็นสัดส่วน และต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่มีหน้าที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

- ติดตั้งระบบแยกออกจากระบบสารสนเทศอื่น

- ทำการป้องกันการมีทรัพยากรไม่เพียงพอ

- มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

๓. ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

ข้อ ๗๒. การใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องปฏิบัติดังนี้

๑. ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

๒. ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้ มีการเผยแพร่เป็นการทั่วไป

๓. เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่แล้ว ต้องรีบนำส่งคืนเจ้าหน้าที่ผู้รับผิดชอบทันที

๔. เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เมื่อรับคืนด้วย

๕. หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นแต่เพียงผู้เดียว

ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์และการป้องกันโปรแกรมไม่ประสงค์ดี

(Software Licensing and Intellectual Property and Preventing Malware)

ข้อ ๗๓. หน่วยงานได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๗๔. ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ใช้งานเป็น Software ที่มีลิขสิทธิ์ ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

ข้อ ๗๕. คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus Software) ตามที่หน่วยงานได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๗๖. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๗๗. ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update Patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๗๘. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบทันที

ข้อ ๗๙. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบให้ทำการแก้ไขโดยเร็ว

ข้อ ๘๐. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

ข้อ ๘๑. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของหน่วยงาน โดยสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการดังนี้

๑. พัฒนาหรือติดตั้งโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่ทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

๒. พัฒนาหรือติดตั้งโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญ ในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

๓. พัฒนาหรือติดตั้งโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่น ในลักษณะเช่นเดียวกับหนอน (Worm) หรือไวรัสคอมพิวเตอร์

๔. พัฒนาหรือติดตั้งโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

๕. นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจ บนเครือข่ายคอมพิวเตอร์

ข้อ ๘๒. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

๑. ต้องควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๒. ต้องระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด สำหรับการพัฒนาซอฟต์แวร์กับผู้รับจ้างจากภายนอก

๓. ต้องสงวนสิทธิ์ในการตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๔. ต้องตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่าง ๆ ที่ จะทำการติดตั้ง ก่อนดำเนินการติดตั้ง

๕. หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงาน ต้องดำเนินการเปลี่ยน Password ต่าง ๆ เพื่อความปลอดภัย

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๘๓. ผู้ดูแลระบบต้องกำหนดมาตรการควบคุมการปฏิบัติงานของผู้ปฏิบัติงานจากภายนอก หน่วยงาน เพื่อให้มีความมั่นคงปลอดภัยเพียงพอ โดยมีแนวทางปฏิบัติ ดังนี้

๑. มีแผนและขั้นตอนการปฏิบัติงานสำหรับเจ้าหน้าที่ ที่จำเป็นต้องปฏิบัติงานของหน่วยงาน จากภายนอกหน่วยงานหรือจากระยะไกล

๒. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยี สารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัสและการใช้งาน firewall ตามที่หน่วยงานกำหนด

๓. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และ อุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

๔. ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้อง มีการตรวจสอบ ได้แก่ Password หรือวิธีการเข้ารหัส

๕. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศ ของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัย ของหน่วยงาน

(๖) ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและ บริการต่าง ๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

(๗) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนด หรือปรับปรุง สิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

(๘) การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิด Port และ Policy ที่ใช้ทั้งเอาไว้อย่างไม่จำเป็น Port และ Policy ดังกล่าวจะต้องตัดการเชื่อมต่อ เมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ข้อ ๘๔. ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) ให้รั่วไหลออกนอกพื้นที่การใช้งานน้อยที่สุด

ข้อ ๘๕. ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาใช้งาน

ข้อ ๘๖. ผู้ดูแลระบบต้องกำหนดค่า Wireless Security เป็นแบบ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point)

ข้อ ๘๗. ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุมด้วย MAC Address (Media Access Control Address) Username และ Password ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address Username และ Password ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

ข้อ ๘๘. ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๘๙. ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารกับเครือข่ายภายในหน่วยงานผ่านทาง VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๙๐. ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนระบบเครือข่ายไร้สาย

ข้อ ๙๑. ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบ รายงานต่อหัวหน้าหน่วยงานทราบทันที

ข้อ ๙๒. ผู้ดูแลระบบ ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่าง ๆ ของหน่วยงาน

ข้อ ๙๓. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากหัวหน้าหน่วยงานอย่างเป็นลายลักษณ์อักษร

ข้อ ๙๔. ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ส่วนที่ ๑๑ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

ข้อ ๙๕. หน่วยงานต้องบริหารจัดการการติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

ข้อ ๙๖. ค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

ข้อ ๙๗. ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตามข้อกำหนด (Policy) จะต้องถูกบล็อก (Block) โดย Firewall

ข้อ ๙๘. ผู้ใช้งานอินเทอร์เน็ตต้องทำการ Login ด้วย Username และ Password ก่อนการใช้งานทุกครั้ง

ข้อ ๙๙. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้งหากมีการเปลี่ยนแปลงค่าต่างๆ ของ Firewall

ข้อ ๑๐๐. การเข้าถึงตัวอุปกรณ์ Firewall ต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๑๐๑. ข้อมูลจราจรทางคอมพิวเตอร์ที่ผ่านเข้า-ออกอุปกรณ์ Firewall ต้องส่งไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยแต่ละรายการข้อมูลจะต้องจัดเก็บไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๐๒. ในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดช่องทาง (Port) การเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งาน (Port) เพื่อการเชื่อมต่อนอกเหนือจากที่กำหนด จะต้องได้รับความยินยอมจากผู้ดูแลระบบก่อน

ข้อ ๑๐๓. การให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะ (Port) การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

ข้อ ๑๐๔. ต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ Firewall เป็นประจำทุกสัปดาห์ หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ ๑๐๕. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ภายในหน่วยงาน ที่มีลักษณะที่เป็นอินเทอร์เน็ตต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๐๖. หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๐๗. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่อง Server หรือ อุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน

ข้อ ๑๐๘. ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

ข้อ ๑๐๙. ในการลงทะเบียนบัญชีผู้ใช้งานระบบ E-Mail ต้องทำการกรอกข้อมูลขอใช้บริการระบบ E-Mail โดยยื่นคำขอกับเจ้าหน้าที่หน่วยงาน

ข้อ ๑๑๐. รหัส E-Mail เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “X” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

ข้อ ๑๑๑. เมื่อได้รับ Password ในการเข้าระบบ E-Mail เมื่อมีการ Login เข้าสู่ระบบในครั้งแรก ต้องเปลี่ยน Password โดยทันที

ข้อ ๑๑๒. ผู้ดูแลระบบ ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ เช่น ไม่เกิน ๓ ครั้ง

ข้อ ๑๑๓. ไม่บันทึกหรือเก็บ Password ไว้ในระบบคอมพิวเตอร์

ข้อ ๑๑๔. เปลี่ยน Password ทุก ๓ - ๖ เดือน

ข้อ ๑๑๕. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของระบบ E-Mail เป็นผู้รับผิดชอบต่อการใช้งานในระบบ E-Mail ของตน

ข้อ ๑๑๖. หลังจากการใช้งานระบบ E-Mail เสร็จสิ้นต้อง Logout ออกจากระบบทุกครั้ง

ข้อ ๑๑๗. การส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อ E-Mail เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล e-Mail ที่หน่วยงานกำหนดไว้ โดยให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-Mail Address ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

ข้อ ๑๑๘. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

ข้อ ๑๑๙. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

ข้อ ๑๒๐. ห้ามส่ง E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น

ข้อ ๑๒๑. ห้ามส่ง E-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๒๒. ต้องระบุชื่อของผู้ส่งใน e-Mail ทุกฉบับที่ส่งไป

ข้อ ๑๒๓. ต้องสำรองข้อมูล e-Mail ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ ๑๒๔. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิด เพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file

ข้อ ๑๒๕. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๒๖. ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพ ข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน หรือทำให้เกิดความแตกแยกระหว่างหน่วยงานรับ – ส่งผ่านทาง E-Mail

ข้อ ๑๒๗. ผู้ใช้งานต้องตรวจสอบตู้เก็บ E-Mail ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและ E-Mail ของตนให้เหลือจำนวนน้อยที่สุด และควรลบ E-Mail ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบ E-Mail

ข้อ ๑๒๘. ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อ ๑๒๙. ผู้ใช้งานต้องใช้ E-Mail สำหรับใช้รับ-ส่งข้อมูลในระบบราชการ ตามมติคณะรัฐมนตรี เมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๐ เรื่อง การพัฒนาระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารในภาครัฐ

ส่วนที่ ๑๓ การควบคุมการใช้อินเทอร์เน็ต (Internet Access Control)

ข้อ ๑๓๐. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ ๑๓๑. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ ๑๓๒. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการตรวจหาไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๑๓๓. ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์ เป็นการส่วนบุคคล หรือทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจ

กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๑๓๔. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๑๓๕. รมั้ดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๑๓๖. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) จะต้องไม่เปิดเผยข้อมูลที่สำคัญ และเป็นความลับของหน่วยงาน

ข้อ ๑๓๗. ในการใช้งาน Webboard จะต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น

ข้อ ๑๓๘. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก อนาจาร และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต หรือระบบเครือข่ายของ หน่วยงาน

ข้อ ๑๓๙. หลังจากใช้งานระบบ Internet เสร็จแล้ว ต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งาน โดยบุคคลอื่น

ข้อ ๑๔๐. หลังจากใช้งานระบบ Internet เสร็จแล้ว ต้องทำการ Logout ออกจากระบบต่าง ๆ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ข้อ ๑๔๑. ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม อย่างเคร่งครัด

ส่วนที่ ๑๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal / Desktop Computer) และคอมพิวเตอร์แบบพกพา (Notebook / Tablet Computer)

ข้อ ๑๔๒. แนวทางปฏิบัติการใช้งานทั่วไป

๑. เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งาน เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ใน งานราชการ

๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรม ที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้ง บนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓. ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ ส่วนบุคคลของหน่วยงาน

๔. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการ โดยเจ้าหน้าที่ของหน่วยงาน หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญา กับหน่วยงานเท่านั้น

๕. ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อค้นหาและกำจัดไวรัสคอมพิวเตอร์ โดยโปรแกรมป้องกันไวรัส

๖. ผู้ใช้งานต้องรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๗. ปิดเครื่องคอมพิวเตอร์ที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๘. ต้องตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๕ นาที เพื่อป้องกันบุคคลอื่นมาใช้งาน

๙. ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของ หน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

๑๐. ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๑๑. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระแทกกระเทือน การตกจากโต๊ะทำงาน หรือหลุดมือ

๑๒. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑๓. ไม่วางของทับบนหน้าจอและแป้นพิมพ์ของคอมพิวเตอร์แบบพกพา

๑๔. การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๑๕. การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑๖. การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ต้องทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๗. ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๑๘. ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มี ความร้อน / ความชื้น / ผู้คนละอองสูงและต้องระวังป้องกันการตกกระแทบ

ข้อ ๑๔๓. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๑. ผู้ใช้งานต้องตรวจสอบหาไวรัสจาก Flash Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๒. ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

๓. ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ข้อ ๑๔๔. การสำรองข้อมูลและการกู้คืน

๑. ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ ได้แก่ CD, DVD หรือ External Hard Disk
๒. ผู้ใช้งานต้องเก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
๓. ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญ เกี่ยวข้องกับการทำงาน เพราะถ้าเกิด Hard Disk เสียหาย ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ ๑๕ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

ข้อ ๑๔๕. ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดขึ้นความลับในการเข้าถึง

ข้อ ๑๔๖. ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เก็บรักษาไว้

ข้อ ๑๔๗. ต้องมีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก บันทึกการเข้าสู่งาน – ออกจากระบบงาน บันทึกการพยายาม เข้าสู่ระบบงาน และเพื่อประโยชน์ในการใช้ตรวจสอบ ต้องเก็บบันทึกแต่ละรายการ (Record) ไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ข้อ ๑๔๘. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและการสำรองข้อมูล

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง
๒. เพื่อให้เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย
๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ผู้รับผิดชอบ

หน่วยงานกำหนดให้มีผู้รับผิดชอบการรักษาความปลอดภัยฐานข้อมูลและการสำรองข้อมูล ดังนี้

๑. ผู้อำนวยการกองยุทธศาสตร์และงบประมาณ
๒. หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งกำหนดขึ้นตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล

ข้อ ๑. กำหนดสิทธิ์และความสำคัญของข้อมูลและฐานข้อมูล

๑. จัดทำบัญชีฐานข้อมูลการจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่ม ผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน
๒. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- | | |
|------------------|---------------|
| - อ่านอย่างเดียว | - สร้างข้อมูล |
| - ป้อนข้อมูล | - แก้ไข |
| - อนุมัติ | - ไม่มีสิทธิ์ |

(๒) กำหนดเกณฑ์การระงับสิทธิ์ การมอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึง ของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบฐานข้อมูลของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูล ดังนี้

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ คำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี

- หนังสือภายใน หนังสือภายนอก เอกสารราชการต่าง ๆ

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๕) การกำหนดเวลาที่ได้เข้าถึง

(๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

ข้อ ๒. ข้อมูลข่าวสารและสารสนเทศทุกประเภทในฐานะข้อมูล ต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิเข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

ข้อ ๓. การปฏิบัติเกี่ยวกับข้อมูลที่เป็นความลับ ต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หมวดที่ ๑ ข้อ ๑๒

ข้อ ๔. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิและอำนาจในสายงาน ต้องเป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกการเข้า - ออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจาก ส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงานภายนอก ดังนี้

๑. กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

๒. กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกันหรือแลกเปลี่ยนข้อมูล

๓. กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

๔. กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูล เพื่อเป็นการป้องกันการปฏิเสธ

๕. กำหนดความรับผิดชอบสำหรับกรณีข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหาย หรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

๖. กำหนดสิทธิ์การเข้าถึงข้อมูล

๗. กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๘. กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๖. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญโดยมีหลักเกณฑ์ที่สำคัญ ได้แก่

๑. ต้องเป็นระบบสารสนเทศที่เกี่ยวข้องในด้านการบริหารของหน่วยงาน ได้แก่ ระบบบุคลากร ระบบงบประมาณการเงินและการบัญชีหรือระบบบริหารสำนักงานอัตโนมัติ (e-Office)

๒. ต้องเป็นระบบสารสนเทศที่เกี่ยวข้องในด้านการให้บริการ ได้แก่ ระบบข้อมูลสารสนเทศ ประชาสัมพันธ์

ข้อ ๗. ต้องจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน และสามารถกู้คืนข้อมูลได้ในสถานการณ์ปกติ และเมื่อมีระบบงานใหม่หรือข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่ ต้องกำหนดให้ใช้แนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล ดังนี้

๑. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล

๒. มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๓. กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ

วัน/เวลา ชื่อ ข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ

- ตรวจสอบการกำหนดค่า (Configuration) ต่างๆ ของระบบการสำรองข้อมูล

- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ โดยระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้เกิดผลกระทบต่อข้อมูลในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่ได้ตามปกติ
- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น
- กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ ๘. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามกระบวนการ ดังนี้

๑. ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
๒. ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงในกรณีไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้
๓. ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
๔. ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
๕. ต้องกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
๖. ต้องสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน
๗. ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓ การกู้คืนข้อมูล

ข้อ ๙. จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล ตรวจสอบประสิทธิภาพและประสิทธิผล ของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

ข้อ ๑๐. ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

ข้อ ๑๑. ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

ข้อ ๑๒. ต้องทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๔ การทดสอบสภาพพร้อมใช้งาน

ข้อ ๑๓. ทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรองข้อมูลและเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๔. ทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงานอย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นได้กับระบบสารสนเทศ
๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

ผู้รับผิดชอบ

หน่วยงานกำหนดให้ผู้รับผิดชอบการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๑. ผู้อำนวยการกองยุทธศาสตร์และงบประมาณ
๒. หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งกำหนดขึ้นตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง

- ข้อ ๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง
- ข้อ ๒. ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ ๒ แนวทางการตรวจสอบและประเมินที่ต้องคำนึงถึง

- ข้อ ๓. จัดลำดับความสำคัญของความเสี่ยง
- ข้อ ๔. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง
- ข้อ ๕. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง
- ข้อ ๖. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้
- ข้อ ๗. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
- ข้อ ๘. กำหนดมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้
 ๑. กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็น ต้องตรวจสอบได้แบบอ่านได้อย่างเดียว (Read only)
 ๒. ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๓. กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๔. กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลลงในแฟ้มบันทึกการเข้า – ออก (Log file) เพื่อแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

๕. ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือเหล่านั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๓ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงัก หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ โดยได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

๑. จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงาน ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจ การใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้อย่างมีประสิทธิภาพ ทำให้ความเสี่ยงที่เกิดจาก Human Error ลดลง

๒. จัดทำหนังสือแจ้งเวียนหน่วยงานภายใน เรื่องการใช้และการลดความเสี่ยงให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse), และข่าวไวรัสหลอกลวง (Hoax) ซึ่ง Software เหล่านี้อาจรบกวนการทำงานและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ซึ่งได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

๑. ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก

๒. ติดตั้งซอฟต์แวร์ Anti Virus ดักจับและทำลายไวรัสคอมพิวเตอร์และ Software ที่อาจก่อให้เกิดความเสียหายอื่นๆ ที่เข้ามาในระบบเครือข่าย และสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

ประเภทที่ ๓ ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ โดยได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๑. ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลได้อย่างปลอดภัย

๒. ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบและรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

๓. ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณี เหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วมจัดเป็นภัยร้ายแรง ที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ โดยได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

๑. เผื่อระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

๒. ถอดเทป Back up ข้อมูลทั้งหมดไปเก็บไว้ในที่สูงและปลอดภัย

๓. ดำเนินการตัดระบบไฟฟ้าในห้องควบคุม โดยปิดเบรกเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า

๔. เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายไว้ในที่สูงและปลอดภัย

๕. กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

๖. ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ รวมทั้งตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

๗. เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว ต้องแจ้งให้หน่วยงานที่เกี่ยวข้องทราบเพื่อสามารถเข้ามาใช้บริการได้ตามปกติ

หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล และหน่วยงานภายนอกที่มีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

ผู้รับผิดชอบ

หน่วยงานได้กำหนดให้มีผู้รับผิดชอบการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อมดังนี้

๑. ผู้อำนวยการกองยุทธศาสตร์และงบประมาณ
๒. หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งกำหนดขึ้นตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

ข้อ ๑. อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

ข้อ ๒. ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ต้องมีลักษณะ ดังนี้

๑. กำหนดเป็นเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญ
๒. ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า – ออก ของบุคคลเป็นจำนวนมาก
๓. ต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว
๔. ต้องปิดล็อกหรือใส่กุญแจประตูหน้าต่างห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่
๕. หากจำเป็นต้องใช้เครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว
๖. ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าวเป็นอันขาด
๗. จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้ง

ไว้เพื่อป้องกันการเข้าถึงระบบ ตามความเหมาะสมจากผู้ที่ไม่ได้รับอนุญาต

ข้อ ๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๑. ต้องจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๒. กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำ แผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

ข้อ ๔. การควบคุมการเข้าออก อาคารสถานที่

๑. กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้า - ออก และช่วงเวลาที่มียกสิทธิ์ในการผ่านเข้า-ออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๒. การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการแลกบัตรประชาชน ใบอนุญาตเข้า หรือบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ ทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

๓. มีการบันทึกวันและเวลาการเข้า - ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

๔. ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๕. บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๖. ต้องจัดเก็บบันทึกการเข้า - ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๗. จัดให้มีเจ้าหน้าที่ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๘. มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๙. สร้างความตระหนักให้ผู้มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๐. มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๑๑. ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๑๒. มีการพิสูจน์ตัวตน โดยใช้บัตรรูด รหัสผ่าน หรือนิ้วมือ เพื่อควบคุมการเข้า - ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

๑๓. ดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๔. ต้องมีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๑. มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

๒. ตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๓. ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงาน ผิดปกติหรือหยุดการทำงาน

ข้อ ๖. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security)

๑. หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๒. ต้องมีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๓. ต้องเดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๔. ต้องทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๕. จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๖. ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๗. ใช้งานสายไฟเบอร์ออฟติก (Fiber Optic) แทนสายสัญญาณสื่อสารแบบเดิม (coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

๘. ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณจากผู้ไม่ประสงค์ดี

ข้อ ๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๑. กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๒. ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่คุณผลิตแนะนำ

๓. จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๔. จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๕. ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๖. กำหนดการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ โดยผู้รับจ้างที่ให้บริการจากภายนอก (ทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๑. ขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๒. กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๓. กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๔. เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๕. บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

๑. กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน ทั้งอุบัติเหตุระหว่างการขนส่งหรือการเกิดอุบัติเหตุกับอุปกรณ์

๒. ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๓. เจ้าหน้าที่ที่รับผิดชอบจะต้องดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

๑. ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๒. มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญ นั้นได้

หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตีหรือเหตุการณ์ละเมิดความปลอดภัยทางระบบสารสนเทศให้มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

หน่วยงานกำหนดให้มีผู้รับผิดชอบการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ ดังนี้

๑. ผู้อำนวยการกองยุทธศาสตร์และงบประมาณ
๒. หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งกำหนดขึ้นตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

ข้อ ๑. ระบบป้องกันผู้บุกรุก ให้ปฏิบัติ ดังนี้

๑. ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก ดังนี้
 - มีการโจมตีมากน้อยเพียงใดและเป็นการโจมตีประเภทใดมากที่สุด
 - ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
 - ระดับความรุนแรงมากน้อยเพียงใด
 - หมายเลขไอพี (IP Address) ของเครือข่ายที่เป็นผู้โจมตี

ข้อ ๒. ระบบไฟร์วอลล์ให้ปฏิบัติ ดังนี้

๑. ดำเนินการตรวจสอบระบบป้องกันการบุกรุกอย่างน้อยเดือนละ ๑ ครั้ง
๒. ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของ Firewall ดังนี้
 - Packet ที่ Firewall ได้ทำการ Block
 - ลักษณะของ Packet ที่ถูก Block
 - Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

๓. กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศ ให้แจ้งหัวหน้าหน่วยงานหรือผู้รับผิดชอบซึ่งได้รับมอบหมายเพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ ๓. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต (ภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์)

๑. ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคาม ทางอินเทอร์เน็ต ดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใดและถูกส่งไปยังที่ใด

- มีการส่งมัลแวร์จากเครือข่ายภายในหน่วยงานไปยังภายนอกหรือไม่

๒. ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

๓. หากตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่ายทันทีแล้วทำการแก้ไขเครื่องนั้นให้สามารถใช้งานได้ตามปกติต่อไป

หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของหน่วยงาน
๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย
๓. เพื่อป้องกันและลดการกระทำผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

ผู้รับผิดชอบ

หน่วยงานได้กำหนดให้ผู้รับผิดชอบการสร้างความรู้ความตระหนักในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศ ดังนี้

๑. ผู้อำนวยการกองยุทธศาสตร์และงบประมาณ
๒. หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งกำหนดขึ้นตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

- ข้อ ๑. ทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง
- ข้อ ๒. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน
- ข้อ ๓. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร ซึ่งการจัดสัมมนาต้องมีแผนการดำเนินงาน อย่างน้อยปีละ ๑ ครั้ง โดยจะจัดรวมกับการสัมมนาที่เกี่ยวข้องกับด้านสารสนเทศและมีการเชิญวิทยากรจาก ภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้
- ข้อ ๔. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ
- ข้อ ๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน
- ข้อ ๖. สร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่ที่มีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

ข้อ ๗. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นและสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน

ข้อ ๘. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบของหน่วยงานและข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่ง ผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเองตามที่กฎระเบียบและข้อบังคับต่าง ๆ ที่เกี่ยวข้องของหน่วยงานได้กำหนดไว้

หมวดที่ ๗ หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูง ผู้อำนวยการสำนัก/กอง ผู้อำนวยการส่วน/หัวหน้าฝ่าย เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งกำหนดขึ้นตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

ข้อ ๑. ระดับนโยบาย ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการสำนัก / กอง ซึ่งมีหน้าที่ความรับผิดชอบ ดังนี้

๑. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

๒. รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๒. ระดับบริหาร ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการส่วน/หัวหน้าฝ่าย

๑. รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒. รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

ข้อ ๓. ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าหน่วยงาน ได้แก่ นักวิชาการคอมพิวเตอร์หรือเจ้าหน้าที่ที่ได้รับมอบหมาย มีหน้าที่ความรับผิดชอบ ดังนี้

๑. ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓. รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๔. ต้องสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๕. ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๖. ต้องรับผิดชอบในการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน รวมทั้งระบบอินเทอร์เน็ตและ Intranet

๗. ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน