บันทึกข้อความ

ส่วนราชการ กองยุทธศาสตร์และงบประมาณ ฝ่ายสถิติข้อมูลและสารสนเทศ โทร.๓๐๒

ที่ สบ ๕๑๐๐๗/๖๘๐ **วันที่** ๒๐ มกราคม ๒๕๖๙

เรื่อง ประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ขององค์การบริหารส่วนจังหวัดสระบุรี ประจำปีงบประมาณ พ.ศ.๒๕๖๙

เรียน หัวหน้าส่วนราชการในสังกัดองค์การบริหารส่วนจังหวัดสระบุรี ทุกส่วน และหัวหน้าหน่วยตรวจสอบภายใน

ด้วย องค์การบริหารส่วนจังหวัดสระบุรี ได้จัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การบริหารส่วนจังหวัดสระบุรี ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ เพื่อเป็นเครื่องมือให้กับผู้ปฏิบัติงาน ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติงาน และการบริหารราชการมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับขององค์การบริหารส่วนจังหวัดสระบุรี รายละเอียดตามเอกสารที่ส่งมาพร้อมนี้

จึงเรียนมาเพื่อทราบและถือเป็นแนวทางปฏิบัติ

(นายสุรศักดิ์ สมภักดี)
รองนายกองค์การบริหารส่วนจังหวัด ปฏิบัติราชการแทน
นายกองค์การบริหารส่วนจังหวัดสระบุรี

ประกาศองค์การบริหารส่วนจังหวัดสระบุรี
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ขององค์การบริหารส่วนจังหวัดสระบุรี
ประจำปีงบประมาณ พ.ศ.๒๕๖๙

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ เพื่อให้การปฏิบัติงานและการบริหารราชการมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับ องค์การบริหารส่วนจังหวัดสระบุรี จึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรี เพื่อเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรี รายละเอียดดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศองค์การบริหารส่วนจังหวัดสระบุรี เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การบริหารส่วนจังหวัดสระบุรี"

ข้อ ๒ วัตถุประสงค์ เพื่อให้ผู้ใช้งานระบบสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรี ได้ทราบถึงข้อปฏิบัติในการใช้งานระบบสารสนเทศให้เกิดความมั่นคงปลอดภัย ป้องกันการกระทำที่ละเมิดระเบียบกฎหมายหรือทำให้เกิดความเสียหายเนื่องมาจากการใช้งานระบบสารสนเทศ

ข้อ ๓ ขอบเขต ผู้ใช้งานระบบสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรี ทุกคนจะต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ

ข้อ ๔ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีรายละเอียดตามเอกสารแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๐ เดือน มกราคม พ.ศ. ๒๕๖๙

(นายสุรศักดิ์ สมภักดี)
รองนายกองค์การบริหารส่วนจังหวัด ปฏิบัติราชการแทน
นายกองค์การบริหารส่วนจังหวัดสระบุรี

แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ขององค์การบริหารส่วนจังหวัดสระบุรี พ.ศ.2569

คำนำ

ในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทสำคัญต่อการบริหารราชการ การให้บริการประชาชน และการปฏิบัติงานของหน่วยงานภาครัฐเป็นอย่างยิ่ง องค์การบริหารส่วนจังหวัดสระบุรีได้มีการนำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานในหลายด้าน อันส่งผลให้เกิดประสิทธิภาพ ความรวดเร็ว และความโปร่งใสในการปฏิบัติราชการ อย่างไรก็ตาม การใช้เทคโนโลยีสารสนเทศดังกล่าวย่อมมีความเสี่ยงต่อภัยคุกคามด้านความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ ซึ่งอาจส่งผลกระทบต่อภารกิจของหน่วยงานได้

เพื่อให้การบริหารจัดการและการใช้งานเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรีเป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสอดคล้องกับกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง องค์การบริหารส่วนจังหวัดสระบุรีจึงได้จัดทำ หนังสือแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรี พ.ศ. ๒๕๖๙ ขึ้น เพื่อใช้เป็นกรอบ แนวทาง และมาตรการในการกำหนดการบริหารจัดการ การใช้งาน การดูแลรักษา และการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงาน โดยหนังสือฉบับนี้มุ่งหวังให้ผู้บริหาร ข้าราชการ ลูกจ้าง และบุคลากรขององค์การบริหารส่วนจังหวัดสระบุรี ตลอดจนผู้ที่เกี่ยวข้องทุกระดับ ได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และถือปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างเคร่งครัด อันจะนำไปสู่การป้องกัน ลดความเสี่ยง และสร้างความเชื่อมั่นในการดำเนินงานด้านเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรีอย่างยั่งยืน

ฝ่ายสถิติข้อมูลและสารสนเทศ กองยุทธศาสตร์และงบประมาณ

วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรี หรือเรียกว่า “หน่วยงาน” มีการใช้งานอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถสนับสนุนการดำเนินงานของหน่วยงานได้อย่างต่อเนื่อง สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยีดิจิทัลในปัจจุบัน รวมทั้งเพื่อป้องกันและลดความเสี่ยงจากการใช้งานระบบเทคโนโลยีสารสนเทศที่ไม่ถูกต้อง การคุกคามทางไซเบอร์ และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศในรูปแบบต่าง ๆ หน่วยงานจึงเห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้มีมาตรฐาน แนวทาง และขั้นตอนการปฏิบัติที่ครอบคลุมการบริหารจัดการระบบเทคโนโลยีสารสนเทศ เครือข่าย คอมพิวเตอร์ ระบบดิจิทัล และข้อมูลส่วนบุคคล ทั้งนี้ ให้เป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อสร้างความเชื่อมั่นและเสริมสร้างความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ ระบบดิจิทัล และเครือข่ายคอมพิวเตอร์ของหน่วยงาน ให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ ประสิทธิผลและมีความต่อเนื่อง

๒. เพื่อกำหนดมาตรฐาน แนวทาง และวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ ผู้ปฏิบัติงาน และบุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน ตระหนักถึงความสำคัญและปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างเคร่งครัด

๓. เพื่อป้องกัน ตรวจจับ และลดความเสี่ยงจากภัยคุกคามด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ เช่น การโจมตีทางไซเบอร์ มัลแวร์ แรนซัมแวร์ การรั่วไหลของข้อมูล และการละเมิดข้อมูลส่วนบุคคลที่อาจส่งผลกระทบต่อภารกิจของหน่วยงาน

๔. เพื่อเป็นกรอบและแนวทางในการพัฒนา ปรับปรุง และยกระดับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การบริหารส่วนจังหวัดสระบุรี ให้สอดคล้องกับเทคโนโลยีใหม่ มาตรฐานที่เกี่ยวข้อง และแนวปฏิบัติที่เป็นที่ยอมรับในปัจจุบัน

๕. เพื่อส่งเสริมให้เจ้าหน้าที่ผู้ปฏิบัติงานทุกระดับในหน่วยงานได้รับทราบ เข้าใจ และถือปฏิบัติตามแนวนโยบายและแนวปฏิบัตินี้อย่างเคร่งครัด อันจะนำไปสู่การบริหารจัดการเทคโนโลยีสารสนเทศของหน่วยงานอย่างมีความมั่นคงปลอดภัยและยั่งยืน

สารบัญ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ขององค์การบริหารส่วนจังหวัดสระบุรี พ.ศ. ๒๕๖๘

ตามประกาศองค์การบริหารส่วนจังหวัดสระบุรี เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การบริหารส่วนจังหวัดสระบุรีเป็นไปอย่างเหมาะสม มีประสิทธิ์ภาพ 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 อุปกรณ์สื่อสารที่สามามารถเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ได้แก่ อุปกรณ์ระบบเครือข่าย ฮาร์ดแวร์ และซอฟต์แวร์ที่มีลิขสิทธิ์

"การรักษาความมั่นคงปลอดภัย" หมายถึงการรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

"หน่วยงานภายนอก" หมายถึง องค์กรหรือหน่วยงานภายนอกที่หน่วยงานอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงานโดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล

"มาตรฐาน" (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

"แนวทางปฏิบัติ" (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

"ข้อมูลคอมพิวเตอร์" หมายถึงข้อมูล 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 ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผนการตัดสินใจและอื่น ๆ

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

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

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

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

"ความมั่นคงปลอดภัยด้านสารสนเทศ" (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายถึง การเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายถึงสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด 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 ติดตามการบริหาร ความเสี่ยงและระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ผู้รับผิดชอบได้แก่

๑. ปลัดองค์การบริหารส่วนจังหวัดสระบุรี

๒. รองปลัดองค์การบริหารส่วนจังหวัดสระบุรี

๓. ผู้อำนวยการสำนัก/กอง

๔. ผู้อำนวยการส่วน/หัวหน้าฝ่าย

๓. ระดับปฏิบัติการ

๓.๑ รับผิดชอบดูแลบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่ายและความปลอดภัยของฐานข้อมูลทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่าง ๆ ของระบบคอมพิวเตอร์และระบบเครือข่ายรวมทั้งการทำสำเนาข้อมูล (Backup) และกู้คืนฐานข้อมูล (Recovery) ของระบบฐานข้อมูลสารสนเทศ ข้อมูลสำหรับระบบและโปรแกรมระบบ ผู้รับผิดชอบได้แก่

- หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ
- เจ้าหน้าที่ที่เกี่ยวข้องที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบ

๓.๒ รับผิดชอบในการอนุมัติสิทธิ์การเข้าใช้ระบบงาน รวมถึงการรักษาความปลอดภัยของแต่ละระบบงานสารสนเทศ ผู้รับผิดชอบ ได้แก่

- หัวหน้าฝ่ายสถิติข้อมูลและสารสนเทศ
- เจ้าหน้าที่ที่เกี่ยวข้องที่ได้รับมอบหมายให้เป็นผู้ดูแลระบบ

แนวปฏิบัติ

ส่วนที่ ๑ การควบคุมการเข้าถึงสารสนเทศ (Access Control)

ข้อ ๑ หน่วยงานต้องกำหนดวัตถุประสงค์การใช้งานสารสนเทศแต่ละประเภทอย่างชัดเจน เพื่อใช้เป็นกรอบในการควบคุมการเข้าถึงข้อมูล ระบบสารสนเทศ และอุปกรณ์ที่ใช้ในการประมวลผลข้อมูล ให้มีความมั่นคงปลอดภัย เหมาะสม และสอดคล้องกับภารกิจของหน่วยงาน โดยมีแนวปฏิบัติในการเข้าถึงและใช้งานสารสนเทศ ดังนี้

๑. ผู้ใช้งานต้องได้รับการอนุญาตจากเจ้าหน้าที่ผู้รับผิดชอบข้อมูลหรือระบบงานนั้น ๆ ตามความจำเป็นต่อการปฏิบัติงานเท่านั้น และต้องไม่ใช้สิทธิ์เกินกว่าขอบเขตที่ได้รับอนุญาต

๒. เจ้าของข้อมูลและเจ้าของระบบงานต้องอนุญาตให้ผู้ใช้งานเข้าถึงระบบหรือข้อมูลเฉพาะส่วนที่จำเป็นต้องใช้ตามหน้าที่และความรับผิดชอบ โดยยึดหลัก “การให้สิทธิ์ขั้นต่ำที่จำเป็น” (Least Privilege) เพื่อป้องกันความเสี่ยงจากการเข้าถึงหรือใช้งานเกินอำนาจหน้าที่

๓. ผู้ดูแลระบบมีหน้าที่ตรวจสอบ อนุมัติ และกำหนดสิทธิ์การเข้าถึงระบบให้แก่ผู้ใช้งาน โดยการขอสิทธิ์เข้าถึงระบบงานต้องจัดทำเป็นลายลักษณ์อักษร ได้รับความเห็นชอบจากผู้บังคับบัญชาหรือผู้บริหารที่เกี่ยวข้อง และแจ้งฝ่ายสถิติข้อมูลและสารสนเทศ เพื่อดำเนินการกำหนดสิทธิ์ตามประเภทข้อมูลและระดับชั้นความลับ รวมทั้งต้องจัดเก็บเป็นหลักฐานและมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ ๒. หน่วยงานต้องกำหนดสิทธิ์หรือมอบอำนาจการใช้งานสารสนเทศแต่ละประเภทอย่างเป็นระบบ เพื่อควบคุมการเข้าถึงสารสนเทศที่มีความสำคัญ และต้องมีการแบ่งแยกอำนาจหน้าที่ของบุคลากรด้านเทคโนโลยีสารสนเทศอย่างชัดเจน ดังนี้

๑. ควบคุมการให้สิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับอำนาจหน้าที่ ความรับผิดชอบ และความจำเป็นของผู้ใช้งานอย่างเคร่งครัด

๒. แบ่งแยกหน้าที่ของบุคลากรที่ปฏิบัติงานด้านการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่ดูแลและบริหารจัดการระบบ (System Administrator) อย่างชัดเจน เพื่อลดความเสี่ยงด้านการควบคุมภายใน

๓. กำหนดหน้าที่ ความรับผิดชอบ และขอบเขตอำนาจของบุคลากรด้านเทคโนโลยีสารสนเทศแต่ละตำแหน่งเป็นลายลักษณ์อักษร

๔. ผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ต้องมีการจัดเตรียมบุคลากรสำรองในงานที่มีความสำคัญ เพื่อให้สามารถปฏิบัติงานทดแทนกันได้ในกรณีจำเป็นหรือเหตุฉุกเฉิน

๕. การให้สิทธิ์การเข้าถึงระบบหรืออุปกรณ์สำคัญต้องจำกัดเฉพาะการปฏิบัติงานตามหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

๖. ต้องมีการตรวจสอบและทบทวนคุณสมบัติ อำนาจหน้าที่ และสิทธิ์การเข้าถึงของผู้ใช้งานอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงตำแหน่งหน้าที่หรือพ้นจากการปฏิบัติงาน ต้องยกเลิกหรือปรับเปลี่ยนสิทธิ์การเข้าถึงให้เหมาะสมโดยทันที

๗. กรณีผู้รับจ้างหรือบุคคลภายนอกเข้ามาดำเนินการบำรุงรักษาหรือสนับสนุนระบบ หน่วยงานต้องกำหนดและอนุมัติสิทธิ์การเข้าถึงอุปกรณ์หรือระบบที่มีข้อมูลสำคัญเป็นกรณีเฉพาะ และต้องควบคุมระยะเวลาในการเข้าถึงอย่างชัดเจน

๘. ต้องมีการทบทวนสิทธิ์การเข้าถึงระบบสารสนเทศที่มีความสำคัญอย่างสม่ำเสมอ โดยครอบคลุมอย่างน้อยระบบดังต่อไปนี้

- ระบบพิสูจน์และยืนยันตัวตน (Active Directory : AD)
- ระบบเครือข่ายไร้สาย (Wireless LAN)
- ระบบจดหมายอิเล็กทรอนิกส์ (Electronic Mail : e-Mail)
- ระบบบริหารสำนักงานอัตโนมัติ (e-Office)
- ระบบสารสนเทศหรือระบบดิจิทัลอื่นของหน่วยงาน

ข้อ ๓. หน่วยงานต้องกำหนดประเภทของข้อมูล การจัดลำดับความสำคัญ ระดับชั้นความลับ และระดับการเข้าถึงสารสนเทศ รวมถึงระยะเวลาและช่องทางการเข้าถึงข้อมูลแต่ละประเภทอย่างเหมาะสม ดังนี้

๑. ประเภทของข้อมูล แบ่งออกเป็น

ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลงบประมาณ การเงินและการบัญชี และข้อมูลระบบบริหารสำนักงานอัตโนมัติ (e-Office) ข้อมูลสารสนเทศด้านการให้บริการ เช่น ข่าวประชาสัมพันธ์ ข่าวจัดซื้อจัดจ้าง และข้อมูลอื่นที่เผยแพร่ผ่านเว็บไซต์หรือช่องทางดิจิทัล

๒. ลำดับความสำคัญของข้อมูล

- ข้อมูลที่มีความสำคัญมาก
- ข้อมูลที่มีความสำคัญปานกลาง
- ข้อมูลที่มีความสำคัญน้อย

๓. ระดับชั้นความลับของข้อมูล

- ลับที่สุด
- ลับมาก
- ลับ
- ข้อมูลทั่วไป

๔. ระดับชั้นการเข้าถึงข้อมูล

- ระดับผู้บริหาร เข้าถึงข้อมูลตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชา

- ระดับผู้ใช้งานทั่วไป เข้าถึงเฉพาะข้อมูลที่ได้รับอนุญาต และสามารถจัดการข้อมูลเฉพาะที่ตนเองสร้างขึ้น

- ระดับผู้ดูแลระบบหรือผู้ได้รับมอบหมาย เข้าถึงและบริหารจัดการระบบตามขอบเขตที่ได้รับมอบหมาย

๕. เวลาในการเข้าถึงข้อมูล ให้เป็นไปตามความจำเป็นของระบบงานและภารกิจของหน่วยงาน

๖. ช่องทางการเข้าถึงสารสนเทศ

- ระบบเครือข่ายภายใน (LAN)
- ระบบอินทราเน็ต (Intranet)
- ระบบอินเทอร์เน็ต (Internet)
- ระบบจดหมายอิเล็กทรอนิกส์ และระบบดิจิทัลอื่นของหน่วยงาน

ข้อ ๔. ผู้ดูแลระบบต้องจัดให้มีระบบบันทึก ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศ (Log Monitoring) เพื่อเฝ้าระวัง ตรวจจับ และติดตามการกระทำที่อาจเป็นการละเมิดความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ ๕. ผู้ดูแลระบบต้องบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ การเปลี่ยนแปลงสิทธิ์การใช้งานและการดำเนินการที่สำคัญในระบบ เพื่อใช้เป็นหลักฐานในการตรวจสอบและติดตามย้อนหลัง

ข้อ ๖. ผู้ดูแลระบบต้องบันทึกและควบคุมการเข้า – ออกสถานที่ตั้งของระบบสารสนเทศ ห้องควบคุมระบบ หรือพื้นที่ที่มีอุปกรณ์สำคัญเพื่อใช้เป็นหลักฐานในการตรวจสอบและรักษาความมั่นคงปลอดภัยของระบบ

ส่วนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ข้อ ๗. หน่วยงานต้องสร้างความรู้ความเข้าใจ และความตระหนักให้แก่ผู้ใช้งานทุกระดับเกี่ยวกับภัยคุกคามและผลกระทบที่อาจเกิดขึ้นจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงต้องกำหนดมาตรการเชิงป้องกันด้านความมั่นคงปลอดภัยให้เหมาะสมกับลักษณะการใช้งานระบบสารสนเทศ โดยมีแนวปฏิบัติ ดังนี้

๑. จัดทำและเผยแพร่คู่มือแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้ผู้ใช้งานรับทราบและถือปฏิบัติ

๒. จัดให้มีการฝึกอบรมหรือกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ เพื่อให้ผู้ใช้งานเข้าใจถึงภัย ความเสี่ยง และผลกระทบจากการใช้งานระบบเทคโนโลยีสารสนเทศที่ไม่ถูกต้อง รวมถึงมาตรการป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

ข้อ ๘. ผู้ดูแลระบบต้องกำหนดขั้นตอนการลงทะเบียนผู้ใช้งานใหม่อย่างเป็นระบบและสามารถตรวจสอบได้ โดยมีแนวปฏิบัติ ดังนี้

๑. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานเพื่อขอรับสิทธิ์ในการเข้าถึงระบบสารสนเทศที่เกี่ยวข้อง โดยต้องได้รับความเห็นชอบจากผู้บังคับบัญชาตามลำดับชั้น

๒. ตรวจสอบบัญชีผู้ใช้งานเพื่อป้องกันการลงทะเบียนซ้ำซ้อนหรือการสร้างบัญชีผู้ใช้งานโดยไม่จำเป็น

๓. ตรวจสอบและกำหนดสิทธิ์การเข้าถึงระบบให้เหมาะสมกับหน้าที่ ความรับผิดชอบและบทบาทของผู้ใช้งาน

๔. แจ้งสิทธิ์ หน้าที่ และความรับผิดชอบของผู้ใช้งานในการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศให้ทราบเป็นลายลักษณ์อักษร

ข้อ ๙. การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Authentication Management)

๑. ผู้ดูแลระบบต้องกำหนดการให้สิทธิ์ใช้งานระบบคอมพิวเตอร์ โปรแกรมประยุกต์ ระบบจดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย และระบบอินเทอร์เน็ต ให้เป็นไปตามหน้าที่ความรับผิดชอบและได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

๒. ผู้ดูแลระบบต้องกำหนดกลไกการยืนยันตัวตนของผู้ใช้งาน เช่น Username และ Password หรือวิธีการยืนยันตัวตนเพิ่มเติมตามความเหมาะสม เพื่อใช้ตรวจสอบตัวตนของผู้ใช้งานในแต่ละระดับชั้นความลับของข้อมูล

๓. กรณีจำเป็นต้องให้สิทธิ์พิเศษแก่ผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องมีมาตรการควบคุมการใช้งานอย่างรัดกุม กำหนดขอบเขตและระดับสิทธิ์ให้ชัดเจน กำหนดระยะเวลาการใช้งาน และต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาหรือหัวหน้าหน่วยงาน โดยให้ระงับสิทธิ์ทันทีเมื่อพ้นระยะเวลาที่กำหนดหรือพ้นจากตำแหน่งหน้าที่

ข้อ ๑๐. ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งานและสิทธิ์การเข้าถึงระบบอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

๑. จัดทำรายชื่อผู้ที่ยังมีสิทธิ์ใช้งานระบบ แยกตามหน่วยงานหรือระบบงาน

๒. ส่งรายชื่อดังกล่าวให้ผู้บังคับบัญชาของแต่ละหน่วยงานพิจารณาทบทวนความเหมาะสมของสิทธิ์การเข้าใช้งาน

๓. ดำเนินการปรับปรุง แก้ไข หรือยกเลิกสิทธิ์การใช้งานให้ถูกต้องตามผลการทบทวน

๔. การยกเลิกสิทธิ์การใช้งานในกรณีลาออก โอน ย้าย หรือเปลี่ยนตำแหน่งหน้าที่ต้องดำเนินการภายใน ๓ วันทำการ และกรณีเปลี่ยนตำแหน่งหน้าที่ภายในหน่วยงาน ต้องดำเนินการภายใน ๗ วัน

ข้อ ๑๑. การบริหารจัดการรหัสผ่านสำหรับผู้ดูแลระบบ

๑. กำหนดให้มีการเปลี่ยนแปลงหรือยกเลิกรหัสผ่านทันทีเมื่อผู้ใช้งานลาออก พ้นจากตำแหน่ง หรือยกเลิกการใช้งานระบบ

๒. กำหนดให้ชื่อผู้ใช้งานและรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๓. การส่งมอบรหัสผ่านชั่วคราวต้องใช้วิธีการที่ปลอดภัย และหลีกเลี่ยงการส่งผ่านช่องทางที่ไม่มีการป้องกัน

๔. กำหนดให้ผู้ใช้งานยืนยันการได้รับรหัสผ่านก่อนเริ่มใช้งานระบบ

๕. กำหนดจำนวนครั้งที่อนุญาตให้ใส่รหัสผ่านผิดพลาดได้ไม่เกิน ๓ ครั้ง ก่อนถูกระงับการใช้งานชั่วคราว

๖. ห้ามผู้ใช้งานบันทึกหรือจัดเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์หรือสื่อบันทึกข้อมูลในลักษณะที่ไม่ปลอดภัย

ข้อ ๑๒. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทและระดับชั้นความลับของข้อมูลทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน โดยมีแนวปฏิบัติ ดังนี้

๑. ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับอย่างเหมาะสมและตรวจสอบได้

๒. กำหนดกลไกการยืนยันตัวตนของผู้ใช้งานให้สอดคล้องกับระดับชั้นความลับของข้อมูล

๓. กำหนดระยะเวลาการใช้งานและระงับสิทธิ์ทันทีเมื่อพ้นระยะเวลาที่กำหนด

๔. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะต้องใช้การเข้ารหัสข้อมูลตามมาตรฐานสากล เช่น SSL/TLS, VPN หรือการเข้ารหัสข้อมูลในระดับแอปพลิเคชัน

๕. กำหนดรอบระยะเวลาการเปลี่ยนรหัสผ่านให้เหมาะสมกับระดับความสำคัญของข้อมูล

๖. กรณีนำอุปกรณ์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงานเพื่อการบำรุงรักษาหรือซ่อมแซมต้องดำเนินการสำรองข้อมูลและลบข้อมูลสำคัญออกก่อนทุกครั้ง

๗. เจ้าของข้อมูลต้องทบทวนความเหมาะสมของสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๓. ในการเชื่อมโยงระบบงานสารสนเทศระหว่างหน่วยงาน หรือกับหน่วยงานภายนอก หัวหน้าหน่วยงานต้องพิจารณาประเด็นด้านความมั่นคงปลอดภัยและความเสี่ยงอย่างรอบคอบก่อนอนุญาตให้มีการใช้งานร่วมกัน โดยมีแนวปฏิบัติ ดังนี้

๑. กำหนดนโยบายและมาตรการควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกันอย่างชัดเจน

๒. พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลที่มีความอ่อนไหวหากไม่มีมาตรการป้องกันที่เพียงพอ

๓. กำหนดรายชื่อบุคลากรที่ได้รับอนุญาตให้เข้าถึงระบบหรือข้อมูลร่วมกันอย่างชัดเจน

๔. กำหนดกระบวนการลงทะเบียนและการยืนยันตัวตนของผู้ใช้งานระบบที่เชื่อมโยงกัน

๕. ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกัน หากระบบที่เชื่อมโยงยังไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพียงพอ

ส่วนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ข้อ ๑๔. ผู้ใช้งานต้องปฏิบัติตามแนวทางด้านความมั่นคงปลอดภัยในการใช้งานรหัสผ่าน ดังนี้

๑. ผู้ใช้งานมีหน้าที่ป้องกัน ดูแล และรักษาข้อมูลบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง โดยผู้ใช้งานแต่ละรายต้องมีบัญชีผู้ใช้งานเป็นของตนเอง ห้ามใช้ร่วมกับผู้อื่น และห้ามเผยแพร่ แจกจ่าย หรือกระทำการใด ๆ ที่ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๒. กำหนดรหัสผ่านต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร และต้องประกอบด้วยตัวอักษร ตัวเลข และอักขระพิเศษ เพื่อเพิ่มความปลอดภัยในการใช้งาน

๓. ห้ามกำหนดรหัสผ่านที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล วันเดือนปีเกิด หรือข้อมูลของบุคคลในครอบครัว

๔. ห้ามใช้รหัสผ่านส่วนบุคคลร่วมกันในการเข้าถึงแฟ้มข้อมูลหรือระบบงานผ่านเครือข่ายคอมพิวเตอร์

๕. หลีกเลี่ยงการใช้โปรแกรมหรือฟังก์ชันบันทึกรหัสผ่านอัตโนมัติ (Save Password) บนอุปกรณ์คอมพิวเตอร์ของหน่วยงานหรืออุปกรณ์ส่วนบุคคลที่ใช้เชื่อมต่อกับระบบของหน่วยงาน

๖. ห้ามจด บันทึก หรือจัดเก็บรหัสผ่านไว้ในสถานที่หรือรูปแบบที่บุคคลอื่นสามารถเข้าถึงหรือสังเกตเห็นได้โดยง่าย

๗. การกำหนดและส่งมอบรหัสผ่านเริ่มต้นให้แก่ผู้ใช้งานต้องดำเนินการด้วยวิธีการที่ปลอดภัย และต้องเปลี่ยนรหัสผ่านทันทีเมื่อเข้าสู่ระบบครั้งแรก

๘. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๑๘๐ วัน หรือเมื่อระบบแจ้งเตือน หรือเมื่อมีเหตุอันควรเชื่อได้ว่ารหัสผ่านอาจถูกล่วงรู้

ข้อ ๑๕. การเข้ารหัสข้อมูลที่เป็นความลับ ผู้ใช้งานต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากลและได้รับการยอมรับ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๑๖. การกระทำใด ๆ ที่เกิดขึ้นจากการใช้บัญชีผู้ใช้งาน (Username) หากเป็นการกระทำที่มีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานเองหรือจากผู้อื่น ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลของเจ้าของบัญชีผู้ใช้งานนั้น

ข้อ ๑๗. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนการใช้งานสินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากพบปัญหาในการพิสูจน์ตัวตน ผู้ใช้งานต้องแจ้งผู้ดูแลระบบโดยทันที โดยมีแนวปฏิบัติ ดังนี้

๑. อุปกรณ์คอมพิวเตอร์ทุกประเภทต้องทำการพิสูจน์ตัวตนก่อนเข้าสู่ระบบปฏิบัติการ

๒. การใช้งานระบบสารสนเทศหรือระบบเครือข่ายใด ๆ ของหน่วยงาน ต้องทำการพิสูจน์ตัวตนทุกครั้ง

๓. การใช้งานอินเทอร์เน็ตต้องสามารถบันทึกข้อมูลที่ระบุตัวตนของผู้ใช้งานได้ เพื่อใช้เป็นหลักฐานในการตรวจสอบ

๔. เมื่อผู้ใช้งานไม่อยู่ ณ เครื่องคอมพิวเตอร์ ต้องล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนใหม่ก่อนใช้งาน

๕. เครื่องคอมพิวเตอร์ทุกเครื่องต้องตั้งค่าโปรแกรมถนอมหน้าจอ (Screen Saver) หรือระบบล็อกหน้าจออัตโนมัติ ภายในระยะเวลาไม่เกิน ๑๕ นาที

๖. ผู้ใช้งานต้องออกจากระบบ (Log out) ทุกครั้งเมื่อเลิกใช้งานระบบสารสนเทศ

ข้อ ๑๘. ผู้ใช้งานต้องตระหนักถึงคุณค่าและความสำคัญของข้อมูล และใช้ความระมัดระวังในการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของหน่วยงานหรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๙. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ห้ามเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลายโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้มีอำนาจหน้าที่

ข้อ ๒๐. ผู้ใช้งานทุกคนมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลขององค์การบริหารส่วนจังหวัดสระบุรี หากเกิดการสูญหาย การนำไปใช้ในทางที่ผิด หรือการเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ข้อ ๒๑. ผู้ใช้งานต้องป้องกัน ดูแล และรักษาความลับ ความถูกต้อง และความพร้อมใช้งานของข้อมูล เอกสาร และสื่อบันทึกข้อมูลสารสนเทศ เพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่มีสิทธิ์

ข้อ ๒๒. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมในการเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคล หน่วยงานให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล อย่างไรก็ตาม หน่วยงานมีสิทธิ์ตรวจสอบข้อมูลที่เกี่ยวข้องกับการปฏิบัติราชการหรือเมื่อมีเหตุอันควรเชื่อว่าข้อมูลนั้นเกี่ยวข้องกับภารกิจของหน่วยงาน โดยอาจแต่งตั้งผู้มีหน้าที่ตรวจสอบได้ตามความจำเป็น

ข้อ ๒๓. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer to Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น BitTorrent, eMule เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

ข้อ ๒๔. ห้ามใช้งานโปรแกรมหรือบริการออนไลน์เพื่อความบันเทิง เช่น ดูภาพยนตร์ ฟังเพลง เล่นเกม ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๒๕. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือเนื้อหาใด ๆ ที่ขัดต่อกฎหมาย ศีลธรรม ความมั่นคงของประเทศ หรือกระทบต่อภาพลักษณ์และภารกิจของหน่วยงาน

ข้อ ๒๖. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อก่อให้เกิดความเสียหาย รบกวน หรือใช้ในการโจรกรรมข้อมูล หรือกระทำการใด ๆ อันเป็นการฝ่าฝืนกฎหมายหรือระเบียบของหน่วยงาน

ข้อ ๒๗. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อประโยชน์ทางการค้า หรือกิจกรรมส่วนตัวที่ไม่เกี่ยวข้องกับภารกิจราชการ

ข้อ ๒๘. ห้ามกระทำการดักจับข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือข้อมูลประเภทใด ๆ ภายในระบบสารสนเทศของหน่วยงานโดยเด็ดขาด

ข้อ ๒๙. ห้ามกระทำการใด ๆ ที่เป็นการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานหยุดชะงักหรือเสื่อมประสิทธิภาพ

ข้อ ๓๐. ห้ามใช้ระบบสารสนเทศของหน่วยงานเพื่อควบคุม หรือเชื่อมต่อไปยังระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบ

ข้อ ๓๑. ห้ามลักลอบใช้งานหรือพยายามล่วงรู้รหัสผ่านหรือข้อมูลยืนยันตัวตนของผู้อื่นไม่ว่ากรณีใด ๆ

ข้อ ๓๒. ห้ามติดตั้งอุปกรณ์ ซอฟต์แวร์ หรือดำเนินการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ ๔ การบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๓๓. ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Data Center) หมายถึง สถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์บริหารจัดการเครือข่าย) ที่เป็นเขตหวงห้ามโดยเด็ดขาดเว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓๔. ผู้ใช้งานต้องจัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่ที่มั่นคง ปลอดภัย จากการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

ข้อ ๓๕. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

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	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
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. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สินหากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๔๑. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ โน๊ตบุ๊ค หรือ แทปเล็ต 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 และต้องไม่ติดตั้งโปรแกรม ใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้งานอื่น ๆ

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

ข้อ ๔๘. ผู้ดูแลระบบ ต้องควบคุมการเชื่อมต่อทางเครือข่ายคอมพิวเตอร์ เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิ์ภาพ โดยมีแนวทางปฏิบัติ ดังต่อไปนี้

๑. จัดทำบันทึกการกำหนดขอบเขตและสิทธิ์ของผู้ใช้งานที่สามารถเข้าถึงบริการต่าง ๆ ในระบบเครือข่ายของหน่วยงานตามที่กำหนดเท่านั้น

๒. กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓. ควบคุมการเข้าถึงหรือใช้งานเครือข่ายคอมพิวเตอร์ที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

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

๕. ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for external connections) จะต้องมีกระบวนการ ในการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายของหน่วยงานได้ ดังนี้

- 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 และสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

- จะต้องมีการจำกัดสิทธิ์ทธิการเข้าใช้อุปกรณ์ได้โดยให้มีการกำหนดวิธีการพิสูจน์ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

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

- ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทั้งทางกายภาพและโดยการล็อกอินเข้ามาใช้งาน

- ติดตั้งอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่า configuration ไว้ในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ที่มีระบบควบคุมการเข้าออก เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

- ผู้ให้บริการภายนอกต้องขออนุมัติจากผู้บังคับบัญชาก่อนเข้าดำเนินการบำรุงรักษาหรือบริหารจัดการพอร์ตของอุปกรณ์เครือข่าย

- เปิดพอร์ตที่มีความจำเป็นในการใช้งาน และยกเลิกหรือปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

- ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็น ในการใช้งานอย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

- กำหนดสิทธิ์บุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่ายกลางโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในเท่านั้น

- บันทึกการเข้า - ออกพื้นที่บริเวณห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง และ เจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

- ห้ามบุคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง 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 ทิ้งเอาไว้โดยไม่จำเป็น

- ปิดช่องทางการเชื่อมต่อเมื่อไม่ใช้งานแล้ว และเปิดใช้งานเมื่อมีการร้องขอเท่าที่จำเป็น

- มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมตามความเหมาะสม

- วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากภายนอก (Remote Access) ต้องได้รับการอนุมัติจากผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

ข้อ ๔๙. ผู้ดูแลระบบ ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อบริหารจัดการเส้นทางบนระบบเครือข่ายได้อย่างมีประสิทธิ์ภาพ โดยมีแนวทางปฏิบัติ ดังต่อไปนี้

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

๒. ต้องควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๓. ต้องกำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อยหรือเครือข่ายภายในและภายนอก

๔. ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย เพื่อไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น 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) และเอกสารสำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ ที่มีความมั่นคงปลอดภัย

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 ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๕. การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้อง Loginโดยแสดงตัวตนด้วย 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 หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

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

ข้อ ๕๙. IP address ของระบบงานเครือข่ายภายใน จำเป็นต้องป้องกันไม่ให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

ข้อ ๖๐. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ข้อ ๖๑. ผู้ดูแลระบบต้องกำหนดกระบวนการลงทะเบียนบุคลากรใหม่ของหน่วยงานเพื่อใช้งานระบบปฏิบัติการและระบบสารสนเทศของหน่วยงานตามความจำเป็น โดยให้เป็นไปตามหลักเกณฑ์การลงทะเบียนผู้ใช้งาน และต้องกำหนดขั้นตอนการยกเลิกหรือปรับเปลี่ยนสิทธิ์การใช้งานทันทีเมื่อมีการลาออก โอน ย้าย หรือเปลี่ยนตำแหน่งหน้าที่ภายในหน่วยงาน เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

ข้อ ๖๒. การกำหนดขั้นตอนการเข้าใช้งานระบบปฏิบัติการ

๑. ผู้ใช้งานต้องกำหนดรหัสผ่านสำหรับการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์ปลายทางที่ตนรับผิดชอบ

๒. ภายหลังการติดตั้งระบบปฏิบัติการหรือซอฟต์แวร์แล้ว ต้องยกเลิกหรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้งานเริ่มต้น (Default Account) ที่มากับระบบทันที

๓. ผู้ใช้งานต้องตั้งค่าระบบล็อกหน้าจออัตโนมัติ (Screen Lock / Screen Saver) เมื่อไม่มีการใช้งาน และต้องพิสูจน์ตัวตนก่อนกลับมาใช้งานทุกครั้ง

๔. ก่อนการเข้าใช้งานระบบปฏิบัติการ ผู้ใช้งานต้องทำการเข้าสู่ระบบ (Login) ทุกครั้ง

๕. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีผู้ใช้งานและรหัสผ่านของตนในการเข้าใช้งานระบบหรืออุปกรณ์ของหน่วยงาน

๖. ผู้ใช้งานต้องออกจากระบบ (Logout) ทุกครั้งเมื่อเลิกใช้งานหรือเมื่อไม่อยู่ ณ เครื่องคอมพิวเตอร์

๗. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือซอฟต์แวร์ที่มีความเสี่ยงด้านความมั่นคงปลอดภัย เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบเป็นลายลักษณ์อักษร

๘. ซอฟต์แวร์ที่หน่วยงานจัดหาให้ต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ ผู้ใช้งานสามารถใช้งานได้ตามหน้าที่ความจำเป็น และห้ามติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบให้ถือเป็นความรับผิดชอบส่วนบุคคล

๙. ซอฟต์แวร์และโปรแกรมที่หน่วยงานติดตั้งไว้ ถือเป็นส่วนหนึ่งของระบบงาน ห้ามติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาไปใช้งานภายนอกหน่วยงานโดยไม่ได้รับอนุญาต

๑๐. ห้ามใช้ทรัพยากรของหน่วยงานเพื่อประโยชน์ทางการค้า หรือกิจกรรมส่วนตัวที่ไม่เกี่ยวข้องกับภารกิจราชการ

๑๑. ในกรณีที่ผู้ใช้งานสร้างหรือดูแลเว็บเพจหรือระบบออนไลน์ของหน่วยงาน ห้ามนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ หรือมีเนื้อหาที่ขัดต่อศีลธรรม ความมั่นคง หรือภาพลักษณ์ของหน่วยงาน

๑๒. ห้ามผู้ใช้งานควบคุม เชื่อมต่อ หรือเข้าถึงคอมพิวเตอร์หรือระบบสารสนเทศภายนอกหน่วยงานโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบ

ข้อ ๖๓. การระบุและยืนยันตัวตนของผู้ใช้งาน

๑. ผู้ใช้งานต้องมีบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เฉพาะบุคคลสำหรับเข้าใช้งานระบบปฏิบัติการและระบบสารสนเทศของหน่วยงาน

๒. การอนุญาตให้ใช้บัญชีผู้ใช้งานร่วมกัน ให้กระทำได้เฉพาะกรณีจำเป็นด้านภารกิจหรือด้านเทคนิค และต้องได้รับอนุมัติจากผู้บังคับบัญชา

๓. หน่วยงานอาจนำเทคโนโลยีการพิสูจน์ตัวตนเพิ่มเติมมาใช้ เช่น การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) บัตรอัจฉริยะ ลายนิ้วมือ หรือชีวมิติอื่น ๆ ตามความเหมาะสมของระบบงาน

ข้อ ๖๔. การบริหารจัดการรหัสผ่าน

๑. ต้องมีระบบบริหารจัดการรหัสผ่านที่รองรับการทำงานแบบอัตโนมัติหรือเชิงโต้ตอบ เพื่อส่งเสริมการกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัย

๒. ต้องจำกัดจำนวนครั้งในการป้อนรหัสผ่านผิดพลาด หากเกินกว่าที่กำหนด ระบบต้องทำการระงับการเข้าใช้งานชั่วคราว

๓. ระบบต้องสามารถตรวจจับและยุติการเชื่อมต่อจากเครื่องปลายทางที่มีพฤติกรรมพยายามเดารหัสผ่าน

๔. ผู้ใช้งานต้องสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเองผ่านระบบที่ปลอดภัย

๕. ข้อมูลรหัสผ่านต้องถูกจัดเก็บแยกจากข้อมูลระบบงาน และต้องอยู่ในรูปแบบที่ไม่สามารถอ่านค่าได้โดยตรง

๖. ระบบต้องไม่แสดงรหัสผ่านจริงบนหน้าจอ โดยแสดงเป็นสัญลักษณ์แทน

๗. ภายหลังการติดตั้งระบบ ต้องยกเลิกหรือเปลี่ยนรหัสผ่านเริ่มต้นของบัญชีผู้ใช้งานทั้งหมดทันที

ข้อ ๖๕. การใช้งานโปรแกรมอรรถประโยชน์

๑. การใช้งานโปรแกรมอรรถประโยชน์ที่เกี่ยวข้องกับระบบปฏิบัติการต้องได้รับอนุญาตจากผู้ดูแลระบบ และต้องมีการพิสูจน์ตัวตนก่อนใช้งาน

๒. โปรแกรมอรรถประโยชน์ต้องไม่ละเมิดลิขสิทธิ์และต้องผ่านการตรวจสอบด้านความมั่นคงปลอดภัย

๓. ต้องจัดเก็บโปรแกรมอรรถประโยชน์แยกจากซอฟต์แวร์ระบบงานหลัก

๔. ต้องจำกัดเฉพาะผู้ที่ได้รับมอบหมายให้สามารถใช้งานโปรแกรมอรรถประโยชน์ได้

๕. ต้องยกเลิกหรือลบโปรแกรมอรรถประโยชน์หรือซอฟต์แวร์ที่ไม่จำเป็นต่อการใช้งาน และป้องกันไม่ให้ผู้ใช้งานทั่วไปเข้าถึงได้

ข้อ ๖๖. การกำหนดเวลาการใช้งานระบบสารสนเทศ

๑. ระบบสารสนเทศต้องมีการตัดการใช้งานอัตโนมัติเมื่อไม่มีการใช้งานเกิน ๑๕ นาที

๒. สำหรับระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูง ต้องกำหนดระยะเวลา Session Time-out ให้สั้นลงตามระดับความเสี่ยง

ข้อ ๖๗. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ

๑. ต้องกำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือความสำคัญสูง โดยกำหนดให้ใช้งานได้ไม่เกิน ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง และให้ใช้งานได้เฉพาะในเวลาราชการ

๒. การเชื่อมต่อจากเครื่องปลายทาง ต้องพิจารณาระดับความเสี่ยงของสถานที่ตั้ง อุปกรณ์ และช่องทางการเชื่อมต่อประกอบการอนุญาต

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ข้อ ๖๘. การจำกัดการเข้าถึงสารสนเทศ

หน่วยงานต้องกำหนดมาตรการควบคุมและจำกัดการเข้าถึงสารสนเทศ ฟังก์ชัน และทรัพยากรต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ให้สอดคล้องกับนโยบายการควบคุมการเข้าถึงสารสนเทศที่กำหนดไว้ โดยยึดหลัก “การให้สิทธิ์เท่าที่จำเป็น” (Least Privilege) และต้องครอบคลุมถึงผู้ใช้งาน บุคลากรฝ่ายสนับสนุน และผู้ให้บริการภายนอก โดยมีแนวปฏิบัติ ดังนี้

๑. การจำกัดการเข้าถึงของผู้ใช้งาน

- ผู้ใช้งานสามารถเข้าถึงระบบและข้อมูลได้เฉพาะตามสิทธิ์ที่ได้รับอนุญาต
- ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคลให้เหมาะสมกับหน้าที่และความรับผิดชอบ
- ผู้ใช้งานต้องออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ ณ จุดใช้งาน

๒. ให้แบ่งกลุ่มบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศออกเป็นอย่างน้อย ๓ กลุ่ม ได้แก่

- ผู้ดูแลระบบ (System Administrator)
- ผู้พัฒนาระบบงาน (Developer)

- ผู้ใช้งานระบบ (User)

โดยต้องกำหนดหน้าที่ ความรับผิดชอบ และขอบเขตอำนาจอย่างชัดเจนเป็นลายลักษณ์อักษร

๓. การกำหนดสิทธิ์การใช้งานระบบโปรแกรมประยุกต์ ระบบจดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย และระบบอินเทอร์เน็ต ต้องให้สิทธิ์เฉพาะที่จำเป็นต่อการปฏิบัติงาน และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมาย พร้อมทั้งต้องมีการทบทวนสิทธิ์อย่างสม่ำเสมอ

๔. ระบบสารสนเทศต้องกำหนดระยะเวลาการเชื่อมต่อ (Session Time-out) เมื่อไม่มีการใช้งานเกิน ๑๕ นาที ระบบต้องยุติการใช้งานโดยอัตโนมัติ และผู้ใช้งานต้องทำการพิสูจน์ตัวตนใหม่ก่อนเข้าใช้งานอีกครั้ง

๕. ต้องมีการบันทึกเหตุการณ์ (Log) ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศที่สำคัญ เพื่อใช้ในการตรวจสอบและติดตาม ดังนี้

- ชื่อบัญชีผู้ใช้งาน
- วันและเวลาที่เข้าสู่ระบบและออกจากระบบ
- เหตุการณ์สำคัญที่เกิดขึ้นในระบบ
- ความพยายามในการเข้าใช้งานทั้งที่สำเร็จและไม่สำเร็จ
- การใช้สิทธิ์และการเข้าถึงไฟล์หรือข้อมูล
- หมายเลข IP Address ของผู้ใช้งาน
- สถานะการทำงานหรือการหยุดทำงานของระบบรักษาความปลอดภัย
- สถานการณ์หยุดทำงานของระบบงานที่มีความสำคัญ

ข้อ ๖๙. การบริหารจัดการสิทธิ์และรหัสผ่านของผู้ใช้งาน

๑. ต้องดำเนินการเปลี่ยนแปลงหรือยกเลิกรหัสผ่านและสิทธิ์การใช้งานทันทีเมื่อผู้ใช้งานลาออก โอน ย้าย หรือพ้นจากตำแหน่งหน้าที่

๒. ห้ามผู้ใช้งานบันทึกหรือจัดเก็บรหัสผ่านในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๓. บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ต้องไม่ซ้ำกัน

๔. ในกรณีจำเป็นต้องให้สิทธิ์พิเศษแก่ผู้ใช้งานที่มีสิทธิ์ระดับสูง ต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน พร้อมกำหนดขอบเขตสิทธิ์ ระยะเวลาการใช้งาน และต้องระงับสิทธิ์ทันทีเมื่อพ้นระยะเวลาหรือพ้นจากตำแหน่ง

ข้อ ๗๐. การบริหารจัดการการเข้าถึงข้อมูลตามชั้นความลับ

๑. ต้องควบคุมการเข้าถึงข้อมูลตามประเภทและระดับชั้นความลับ ทั้งการเข้าถึงโดยตรงและผ่านระบบงาน

๒. ต้องใช้กลไกการพิสูจน์ตัวตน เช่น Username และ Password หรือวิธีการยืนยันตัวตนเพิ่มเติมตามระดับความสำคัญของข้อมูล

๓. ต้องกำหนดระยะเวลาการใช้งานและระงับการเข้าถึงทันทีเมื่อพ้นระยะเวลาที่ได้รับอนุญาต

๔. การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะต้องมีการเข้ารหัสด้วยมาตรฐานสากล เช่น SSL/TLS, VPN

๕. ต้องกำหนดรอบระยะเวลาในการเปลี่ยนรหัสผ่านให้สอดคล้องกับระดับความสำคัญของข้อมูล

๖. ในกรณีนำอุปกรณ์หรือสื่อบันทึกข้อมูลออกนอกหน่วยงานเพื่อการบำรุงรักษาหรือซ่อมแซม ต้องดำเนินการสำรองและลบข้อมูลสำคัญออกก่อนทุกครั้ง

ข้อ ๗๑. ระบบสารสนเทศที่มีความสำคัญหรือไวต่อการรบกวน

๑. ระบบสารสนเทศที่มีความสำคัญสูง เช่น ระบบบริหารสำนักงานอัตโนมัติ (e-Office) ระบบบุคลากร ระบบการเงินและการบัญชี ต้องแยกออกจากระบบทั่วไป และต้องมีการประเมินผลกระทบต่อภารกิจของหน่วยงานอย่างชัดเจน

๒. ต้องควบคุมสภาพแวดล้อมของระบบดังกล่าวเป็นการเฉพาะ เช่น

- จัดให้มีพื้นที่หรือห้องปฏิบัติการที่แยกเป็นสัดส่วน
- จำกัดการเข้าถึงเฉพาะผู้ที่ได้รับมอบหมาย
- แยกเครือข่ายหรือระบบออกจากระบบอื่น
- มีมาตรการเฝ้าระวังและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๓. ต้องควบคุมการใช้งานอุปกรณ์เคลื่อนที่ การทำงานจากภายนอกหน่วยงาน (Mobile Computing และ Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าวอย่างรัดกุม

ข้อ ๗๒. การใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๑. ต้องตรวจสอบความพร้อมใช้งานของอุปกรณ์และซอฟต์แวร์ให้ถูกต้องตามลิขสิทธิ์ก่อนนำไปใช้งาน

๒. ต้องระมัดระวังไม่ให้บุคคลภายนอกเข้าถึงหรือคัดลอกข้อมูลจากอุปกรณ์ เว้นแต่เป็นข้อมูลที่เปิดเผยทั่วไป

๓. เมื่อหมดความจำเป็นในการใช้งาน ต้องนำอุปกรณ์ส่งคืนแก่เจ้าหน้าที่ผู้รับผิดชอบทันที

๔. เจ้าหน้าที่ผู้รับคืนต้องตรวจสอบสภาพอุปกรณ์และความสมบูรณ์ของข้อมูลเมื่อรับคืน

๕. หากความเสียหายเกิดจากความประมาทอย่างร้ายแรงของผู้ใช้งาน ผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๘ การบริหารจัดการซอฟต์แวร์ลิขสิทธิ์และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and Intellectual Property and Preventing Malware)

ข้อ ๗๓. การบริหารจัดการลิขสิทธิ์ซอฟต์แวร์

หน่วยงานให้ความสำคัญต่อการคุ้มครองทรัพย์สินทางปัญญา โดยซอฟต์แวร์ที่หน่วยงานจัดหา อนุญาตให้ใช้งาน หรือมีลิขสิทธิ์ ผู้ใช้งานสามารถใช้งานได้เฉพาะตามหน้าที่ความจำเป็นเท่านั้น และห้ามติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หรือไม่ได้รับอนุญาต หากตรวจพบการกระทำอันเป็นการละเมิดลิขสิทธิ์ ให้ถือเป็นความรับผิดชอบส่วนบุคคลของผู้ใช้งาน

ข้อ ๗๔. การควบคุมซอฟต์แวร์ที่หน่วยงานจัดเตรียม

ซอฟต์แวร์ที่หน่วยงานจัดเตรียมให้ถือเป็นทรัพย์สินของหน่วยงานและเป็นส่วนหนึ่งของระบบงาน ผู้ใช้งานห้ามถอดถอน เปลี่ยนแปลง แก้ไข ทำซ้ำ หรือโอนย้ายไปใช้งานภายนอกหน่วยงาน เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมาย

ข้อ ๗๕. มาตรการป้องกันโปรแกรมไม่ประสงค์ดี

๑. คอมพิวเตอร์และอุปกรณ์ปลายทางของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสหรือโปรแกรมป้องกันมัลแวร์ (Antivirus / Endpoint Protection) ตามที่หน่วยงานกำหนด และต้องเปิดใช้งานตลอดเวลา เว้นแต่ได้รับอนุญาตเป็นกรณีพิเศษ

๒. โปรแกรมป้องกันไวรัสหรือมัลแวร์ต้องมีการปรับปรุงฐานข้อมูล (Signature) และกลไกการตรวจจับให้เป็นปัจจุบันอย่างสม่ำเสมอ

ข้อ ๗๖. การตรวจสอบข้อมูลและซอฟต์แวร์ก่อนใช้งาน

ข้อมูล ไฟล์ ซอฟต์แวร์ หรือสื่อบันทึกข้อมูลใด ๆ ที่ได้รับจากบุคคลหรือแหล่งภายนอก ต้องผ่านการตรวจสอบไวรัสและโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือจัดเก็บทุกครั้ง

ข้อ ๗๗. ผู้การปรับปรุงระบบและซอฟต์แวร์

ผู้ใช้งานและผู้ดูแลระบบต้องดำเนินการปรับปรุงระบบปฏิบัติการ โปรแกรมประยุกต์ และแพตช์ความปลอดภัย (Security Patch / Update) ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ เพื่อป้องกันช่องโหว่ที่อาจถูกนำไปใช้โจมตีระบบ

ข้อ ๗๘. การเฝ้าระวังและแจ้งเหตุ

ผู้ใช้งานต้องมีความตระหนักและระมัดระวังต่อภัยคุกคามจากไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา หากพบพฤติกรรมหรือเหตุการณ์ที่ผิดปกติ ต้องแจ้งผู้ดูแลระบบโดยทันที

ข้อ ๗๙. การตอบสนองเมื่อพบการติดมัลแวร์

เมื่อพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดไวรัสหรือโปรแกรมไม่ประสงค์ดี ผู้ใช้งานต้องตัดการเชื่อมต่อเครือข่ายทันที และแจ้งผู้ดูแลระบบเพื่อดำเนินการแก้ไขโดยเร็ว เพื่อป้องกันการแพร่กระจายของภัยคุกคาม

ข้อ ๘๐. การคุ้มครองข้อมูลและทรัพย์สินของหน่วยงาน

ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบ ทำลาย หรือกระทำการใด ๆ ต่อข้อมูล เอกสาร ซอฟต์แวร์ หรือทรัพย์สินทางสารสนเทศของหน่วยงานหรือของผู้อื่นโดยไม่ได้รับอนุญาต

ข้อ ๘๑. การห้ามพัฒนาและใช้งานโปรแกรมหรือฮาร์ดแวร์ที่เป็นอันตราย

ห้ามพัฒนา ติดตั้ง หรือใช้งานโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่มีลักษณะดังต่อไปนี้

๑. ทำลายหรือหลีกเลี่ยงกลไกการรักษาความมั่นคงปลอดภัยของระบบ รวมถึงการลักลอบใช้รหัสผ่าน การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการแกะรหัสผ่านของผู้อื่น

๒. ทำให้ผู้ใช้งานได้รับสิทธิ์หรือทรัพยากรของระบบมากกว่าที่ได้รับอนุญาต

๓. มีลักษณะทำซ้ำตัวเอง แฝงตัว หรือแพร่กระจายเช่นเดียวกับไวรัส หนอน (Worm) หรือมัลแวร์

๔. ทำลายหรือหลีกเลี่ยงระบบจำกัดสิทธิ์การใช้งานซอฟต์แวร์ (License Protection)

๕. นำเสนอข้อมูลหรือเนื้อหาที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ หรือขัดต่อศีลธรรม ในกรณีที่มีการพัฒนาเว็บเพจหรือระบบออนไลน์ของหน่วยงาน

ข้อ ๘๒. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๑. หน่วยงานต้องควบคุมและกำกับดูแลโครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอกอย่างเหมาะสม

๒. ต้องกำหนดสิทธิ์ในทรัพย์สินทางปัญญา โดยเฉพาะซอร์สโค้ดและเอกสารระบบ ให้ชัดเจนในสัญญาจ้าง

๓. หน่วยงานต้องสงวนสิทธิ์ในการตรวจสอบคุณภาพ ความถูกต้อง และความมั่นคงปลอดภัยของซอฟต์แวร์ที่พัฒนาโดยผู้ให้บริการภายนอก

๔. ต้องตรวจสอบมัลแวร์ ช่องโหว่ และความเสี่ยงด้านความมั่นคงปลอดภัยของซอฟต์แวร์ก่อนการติดตั้งและนำไปใช้งานจริง

๕. หลังจากการส่งมอบซอฟต์แวร์ ต้องดำเนินการเปลี่ยนรหัสผ่าน บัญชีผู้ใช้งาน และข้อมูลเข้าถึงระบบทั้งหมด เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๙ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ข้อ ๘๓. ผู้ดูแลระบบต้องกำหนดมาตรการควบคุมการปฏิบัติงานของผู้ปฏิบัติงานจากภายนอกหน่วยงาน เพื่อให้มีความมั่นคงปลอดภัยเพียงพอ โดยมีแนวทางปฏิบัติ ดังนี้

๑. มีแผนและขั้นตอนการปฏิบัติงานสำหรับเจ้าหน้าที่ ที่จำเป็นต้องปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงานหรือจากระยะไกล

๒. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัสและการใช้งาน firewall ตามที่หน่วยงานกำหนด

๓. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

๔. ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ ได้แก่ Password หรือวิธีการเข้ารหัส

๕. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

(๖) ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่าง ๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

(๗) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนด หรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

(๘) การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิด Port และ Policy ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น Port และ Policy ดังกล่าวจะต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว 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 และอุปกรณ์กระจายสัญญาณแบบไร้สาย (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. ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

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) และเส้นทางเชื่อมต่ออินเตอร์เน็ตที่ไม่อนุญาตตามข้อกำหนด (Policy) จะต้องถูกบล็อก (Block) โดย Firewall

ข้อ ๙๘. ผู้ใช้งานอินเตอร์เน็ตต้องทำการ Login ด้วย Username และ Password ก่อนการใช้งานทุกครั้ง

ข้อ ๙๙. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่างๆ ของ Firewall

ข้อ ๑๐๐. การเข้าถึงตัวอุปกรณ์ Firewall ต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๑๐๑. ข้อมูลจราจรทางคอมพิวเตอร์ที่ผ่านเข้า-ออกอุปกรณ์ Firewall ต้องส่งไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยแต่ละรายการข้อมูลจะต้องจัดเก็บไว้ไม่น้อยกว่า ๙๐ วัน

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

ข้อ ๑๐๓. การให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะ (Port) การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

ข้อ ๑๐๔. ต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ Firewall เป็นประจำทุกสัปดาห์หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

ข้อ ๑๐๕. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ภายในหน่วยงานที่มีลักษณะที่เป็นอินทราเน็ตต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเตอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๐๖. หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

ข้อ ๑๐๗. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่อง Server หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน

ข้อ ๑๐๘. ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเตอร์เน็ตทันที

ส่วนที่ ๑๒ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

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

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

ข้อ ๑๑๑. เมื่อได้รับ Password ในการเข้าระบบ E-Mail เมื่อมีการ Login เข้าสู่ระบบในครั้งแรกต้องเปลี่ยน 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 หรือสิทธิ์ของบุคคลอื่น

ข้อ ๑๒๑. ห้ามส่ง E-Mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

ข้อ ๑๒๒. ต้องระบุชื่อของผู้ส่งใน e-Mail ทุกฉบับที่ส่งไป

ข้อ ๑๒๓. ต้องสำรองข้อมูล e-Mail ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ ๑๒๔. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส 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 การควบคุมการใช้อินเตอร์เน็ต (Internet Access Control)

ข้อ ๑๓๐. ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร

ข้อ ๑๓๑. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

ข้อ ๑๓๒. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการตรวจหาไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๑๓๓. ไม่ใช้ระบบอินเตอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล หรือทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๑๓๔. ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเตอร์เน็ต (Internet)

ข้อ ๑๓๕. ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเตอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๑๓๖. ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) จะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๑๓๗. ในการใช้งาน Webboard จะต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น

ข้อ ๑๓๘. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกอนาจาร และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต หรือระบบเครือข่ายของหน่วยงาน

ข้อ ๑๓๙. หลังจากใช้งานระบบ Internet เสร็จแล้ว ต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

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 เป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ

๒. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓. ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

๔. การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงาน หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

๕. ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อค้นหาและกำจัดไวรัสคอมพิวเตอร์ โดยโปรแกรมป้องกันไวรัส

๖. ผู้ใช้งานต้องรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๗. ปิดเครื่องคอมพิวเตอร์ที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๘. ต้องตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๕ นาที เพื่อป้องกันบุคคลอื่นมาใช้งาน

๙. ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของ หน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของหน่วยงานก่อนการใช้งาน

๑๐. ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๑๑. ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน การตกจากโต๊ะทำงานหรือหลุดมือ

๑๒. หลีกเลี่ยงการใช้นิ้วหรือของแข็ง กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑๓. ไม่วางของทับบนหน้าจอและแป้นพิมพ์ของคอมพิวเตอร์แบบพกพา

๑๔. การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๑๕. การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑๖. การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ต้องทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๗. ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๑๘. ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มี ความร้อน / ความชื้น / ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

ข้อ ๑๔๓. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๑. ผู้ใช้งานต้องตรวจสอบหาไวรัสจาก Flash Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๒. ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

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 ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะถ้าเกิด Hard Disk เสียหาย ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

ส่วนที่ ๑๕ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

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

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. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ 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. ข้อมูลข่าวสารและสารสนเทศทุกประเภทในฐานข้อมูล ต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิ์เข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัย

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

ข้อ ๔. หน่วยงานเจ้าของฐานข้อมูล ผู้มีสิทธิ์และอำนาจในสายงาน ต้องเป็นผู้พิจารณาคุณสมบัติของผู้ใช้งานและโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิ์และจัดให้มีแฟ้มลงบันทึกการเข้า - ออก (Log File) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

ข้อ ๕. ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างส่วนราชการ หรือแลกเปลี่ยน หรือขอใช้ข้อมูลจาก ส่วนราชการให้จัดทำข้อตกลงการใช้ข้อมูล หรือสำหรับการแลกเปลี่ยนสารสนเทศระหว่างหน่วยงานกับหน่วยงานภายนอก ดังนี้

๑. กำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรฐานเพื่อป้องกันข้อมูลและสื่อบันทึกข้อมูลที่จะมีการขนย้ายหรือส่งไปยังอีกสถานที่หนึ่ง

๒. กำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องและขั้นตอนปฏิบัติในการใช้ข้อมูลร่วมกันหรือแลกเปลี่ยนข้อมูล

๓. กำหนดหน้าที่ความรับผิดชอบในการป้องกันข้อมูล

๔. กำหนดขั้นตอนปฏิบัติสำหรับตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูล เพื่อเป็นการป้องกันการปฏิเสธ

๕. กำหนดความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหาย หรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น

๖. กำหนดสิทธิ์การเข้าถึงข้อมูล

๗. กำหนดมาตรฐานทางเทคนิคที่ใช้ในการเข้าถึงข้อมูลหรือซอฟต์แวร์

๘. กำหนดมาตรการพิเศษสำหรับป้องกันเอกสาร ข้อมูล ซอฟต์แวร์ หรืออื่น ๆ ที่มีความสำคัญ

ส่วนที่ ๒ การสำรองข้อมูล

ข้อ ๖. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญโดยมีหลักเกณฑ์ที่สำคัญ ได้แก่

๑. ต้องเป็นระบบสารสนเทศที่เกี่ยวข้องในด้านบริหารของหน่วยงาน ได้แก่ ระบบบุคลากร ระบบงบประมาณการเงินและการบัญชีหรือระบบบริหารสำนักงานอัตโนมัติ (e-Office)

๒. ต้องเป็นระบบสารสนเทศที่เกี่ยวข้องในด้านการให้บริการ ได้แก่ ระบบข้อมูลสารสนเทศประชาสัมพันธ์

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 เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่ได้ตามปกติ

- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้

- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

- กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

ข้อ ๘. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามกระบวนการ ดังนี้

๑. ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒. ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงในกรณีไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้

๓. ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๔. ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๕. ต้องกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๖. ต้องสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๗. ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓ การกู้คืนข้อมูล

ข้อ ๙. จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล ตรวจสอบประสิทธิภาพและประสิทธิผล ของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

ข้อ ๑๐. ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

ข้อ ๑๑. ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

ข้อ ๑๒. ต้องทดสอบการกู้คืนข้อมูลที่ได้สำรองไว้อย่างสม่ำเสมออย่างน้อยปีละ 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. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ

๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

ผู้รับผิดชอบ

หน่วยงานกำหนดให้มีผู้รับผิดชอบการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ 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 แนวทางในการตรวจสอบและประเมินที่ต้องคำนึงถึง

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 ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๓. กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

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

๕. ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๓ ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตาม ตรวจสอบ และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พบว่าสามารถจำแนกความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงานของหน่วยงานออกเป็น ๕ ประเภทหลัก ดังนี้

<u>ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน</u>

ภัยที่เกิดจากการขาดความรู้ ความเข้าใจ หรือความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ของเจ้าหน้าที่หรือบุคลากร เช่น การใช้งานอุปกรณ์หรือระบบสารสนเทศไม่ถูกต้อง การตั้งรหัสผ่านที่ไม่ปลอดภัย การเปิดไฟล์หรือคลิกลิงก์ที่เป็นอันตราย ซึ่งอาจส่งผลให้ระบบสารสนเทศเกิดความเสียหาย หยุดชะงัก หรือเกิดการรั่วไหลของข้อมูลสำคัญ

แนวทางการลดและควบคุมความเสี่ยง มีดังนี้

๑. จัดให้มีการอบรมและพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์แก่เจ้าหน้าที่อย่างต่อเนื่อง ครอบคลุมการใช้งาน Hardware, Software, ระบบเครือข่าย และการป้องกันภัยคุกคามทางไซเบอร์

๒. จัดทำและเผยแพร่แนวปฏิบัติ มาตรการ และคู่มือการใช้งานระบบเทคโนโลยีสารสนเทศ รวมถึงการแจ้งเตือนภัยและแนวทางลดความเสี่ยง ให้เจ้าหน้าที่ถือปฏิบัติอย่างเคร่งครัด

<u>ประเภทที่ ๒ ภัยจากซอฟต์แวร์ที่เป็นอันตราย</u>

ภัยจากซอฟต์แวร์ที่เป็นอันตราย ได้แก่ ไวรัสคอมพิวเตอร์ หนอนอินเทอร์เน็ต ม้าโทรจัน แรนซัมแวร์ สปายแวร์ รวมถึงภัยคุกคามในรูปแบบใหม่ เช่น ฟิชชิ่ง (Phishing) และการโจมตีผ่านซอฟต์แวร์จากแหล่งภายนอก ซึ่งอาจส่งผลให้ระบบสารสนเทศเสียหาย สูญหาย หรือไม่สามารถให้บริการได้

แนวทางการเตรียมความพร้อมและป้องกันภัย มีดังนี้

๑. ติดตั้งและกำหนดค่าอุปกรณ์ป้องกันเครือข่าย เช่น Firewall และระบบป้องกันการบุกรุก เพื่อควบคุมและจำกัดการเข้าถึงระบบจากภายนอก

๒. ติดตั้งโปรแกรมป้องกันไวรัสและโปรแกรมป้องกันมัลแวร์ที่เป็นมาตรฐาน พร้อมทั้งปรับปรุงฐานข้อมูลและระบบตรวจจับให้เป็นปัจจุบันอย่างสม่ำเสมอ

<u>ประเภทที่ ๓ ภัยจากอัคคีภัยและระบบไฟฟ้า</u>

ภัยจากไฟไหม้หรือระบบไฟฟ้าขัดข้องถือเป็นความเสี่ยงร้ายแรงที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญของหน่วยงาน

แนวทางการเตรียมรับสถานการณ์ มีดังนี้

๑. ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อรองรับกรณีไฟฟ้าขัดข้อง และช่วยให้สามารถปิดระบบและสำรองข้อมูลได้อย่างปลอดภัย

๒. ติดตั้งระบบตรวจจับควันและสัญญาณแจ้งเตือนเหตุฉุกเฉินในห้องควบคุมระบบ พร้อมทั้งตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

๓. จัดให้มีอุปกรณ์ดับเพลิงที่เหมาะสมกับอุปกรณ์อิเล็กทรอนิกส์ เช่น ระบบดับเพลิงชนิดก๊าซ และทดสอบการใช้งานเป็นประจำ

<u>ประเภทที่ ๔ ภัยจากอุทกภัยและภัยธรรมชาติ</u>

ความเสี่ยงจากน้ำท่วมและภัยธรรมชาติอื่น ๆ อาจส่งผลให้ระบบเทคโนโลยีสารสนเทศและศูนย์ข้อมูลของหน่วยงานได้รับความเสียหายอย่างรุนแรง

แนวทางการเตรียมความพร้อม มีดังนี้

๑. เฝ้าระวังและติดตามสถานการณ์จากหน่วยงานที่เกี่ยวข้อง เช่น กรมอุตุนิยมวิทยา และหน่วยงานด้านการป้องกันภัยพิบัติ

๒. ดำเนินการสำรองข้อมูลอย่างสม่ำเสมอ และจัดเก็บสื่อสำรองข้อมูลไว้ในสถานที่ปลอดภัยหรือพื้นที่สำรอง

๓. ตัดระบบไฟฟ้าและอุปกรณ์ที่เกี่ยวข้องเมื่อเกิดสถานการณ์ฉุกเฉิน เพื่อป้องกันความเสียหายเพิ่มเติม

๔. เคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายไปยังพื้นที่ที่ปลอดภัย

๕. ภายหลังสถานการณ์คลี่คลาย ต้องตรวจสอบระบบไฟฟ้า อุปกรณ์ และระบบเครือข่ายโดยผู้เชี่ยวชาญก่อนนำกลับมาใช้งาน

๖. ทดสอบการทำงานของระบบสารสนเทศและเครือข่ายให้สามารถให้บริการได้ตามปกติและแจ้งหน่วยงานที่เกี่ยวข้องให้ทราบ

ประเภทที่ ๕ ภัยจากระบบคลาวด์ ระบบออนไลน์ และการโจมตีทางไซเบอร์ขั้นสูง

ภัยจากระบบคลาวด์ ระบบออนไลน์ และการโจมตีทางไซเบอร์ขั้นสูง เป็นความเสี่ยงที่เพิ่มขึ้นอย่างต่อเนื่องตามการนำเทคโนโลยีดิจิทัลมาใช้ในการปฏิบัติงานของหน่วยงาน เช่น การใช้ระบบสารสนเทศบนคลาวด์ (Cloud Computing) ระบบเว็บแอปพลิเคชัน ระบบบริการออนไลน์ รวมถึงการเชื่อมต่อกับหน่วยงานภายนอก ซึ่งอาจตกเป็นเป้าหมายของการโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ ได้แก่ การโจมตีแบบฟิชชิ่ง (Phishing) การโจมตีแบบปฏิเสธการให้บริการ (DDoS Attack) การโจมตีแบบเรียกค่าไถ่ (Ransomware) การเข้าถึงระบบโดยไม่ได้รับอนุญาต (Unauthorized Access) และการรั่วไหลของข้อมูล (Data Breach)

ซึ่งภัยดังกล่าวอาจส่งผลกระทบต่อความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลและระบบสารสนเทศของหน่วยงาน รวมถึงความเชื่อมั่นของประชาชนและผู้มีส่วนได้ส่วนเสีย

แนวทางการลดและควบคุมความเสี่ยง มีดังนี้

๑. กำหนดนโยบายและมาตรการรักษาความมั่นคงปลอดภัยสำหรับระบบคลาวด์และระบบออนไลน์ โดยพิจารณาคัดเลือกผู้ให้บริการที่มีมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ และมีการรับรองตามมาตรฐานที่เกี่ยวข้อง

๒. กำหนดให้มีการบริหารจัดการสิทธิ์การเข้าถึงระบบคลาวด์และระบบออนไลน์ตามหลักการ “จำเป็นต่อการปฏิบัติงาน” (Least Privilege) พร้อมทั้งทบทวนสิทธิ์การใช้งานอย่างสม่ำเสมอ

๓. จัดให้มีมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) สำหรับการเข้าถึงระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูง

๔. จัดให้มีระบบเฝ้าระวัง ตรวจสอบ และบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย (Log Monitoring and Security Monitoring) เพื่อสามารถตรวจจับเหตุการณ์ผิดปกติและตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที

๕. จัดให้มีมาตรการป้องกันและรับมือกับการโจมตีทางไซเบอร์ขั้นสูง เช่น การทดสอบช่องโหว่ของระบบ (Vulnerability Assessment) การทดสอบเจาะระบบ (Penetration Test) และการประเมินความเสี่ยงด้านไซเบอร์อย่างสม่ำเสมอ

๖. กำหนดแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Plan) และแผนสำรองข้อมูลและกู้คืนระบบ (Backup and Disaster Recovery Plan) เพื่อรองรับกรณีเกิดเหตุโจมตีหรือระบบหยุดชะงัก

๗. เสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่เจ้าหน้าที่และบุคลากรของหน่วยงาน โดยเฉพาะการใช้งานระบบออนไลน์ การรับส่งข้อมูลผ่านเครือข่ายสาธารณะ และการป้องกันภัยจากการหลอกลวงทางไซเบอร์

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 โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบ ตามความเหมาะสมจากผู้ที่ไม่ได้รับอนุญาต

ข้อ ๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๑. ต้องจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๒. กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำ แผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน 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 และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้า-ออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

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

๓. มีการบันทึกวันและเวลาการเข้า - ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

๔. ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๕. บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๖. ต้องจัดเก็บบันทึกการเข้า - ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๗. จัดให้มีเจ้าหน้าที่ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๘. มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๙. สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง 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 และสายเคเบิ้ลอื่นๆ (Cabling Security)

๑. หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๒. ต้องมีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณหรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

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. ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๓. จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๔. จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๕. ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๖. กำหนดการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญ 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. มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญ นั้นได้

หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตีหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

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. ดำเนินการตรวจระบบป้องกันการบุกรุกอย่างน้อยเดือนละ ๑ ครั้ง

๒. ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของ Firewall ดังนี้

- Packet ที่ Firewall ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

๓. กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งหัวหน้าหน่วยงานหรือผู้รับผิดชอบซึ่งได้รับมอบหมายเพื่อตัดสินใจดำเนินการแก้ไขปัญหา

ข้อ ๓. ระบบป้องกันภัยคุกคามทางอินเตอร์เน็ต (ภัยคุกคามทางอินเตอร์เน็ตหรือมัลแวร์ประกอบด้วย ไวรัสคอมพิวเตอร์ หนอนอินเตอร์เน็ต โทรจัน รวมถึงสปายแวร์)

๑. ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคาม ทางอินเตอร์เน็ต ดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใดและถูกส่งไปยังที่ใด

- มีการส่งมัลแวร์จากเครือข่ายภายในหน่วยงานไปยังภายนอกหรือไม่

๒. ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

๓. หากตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่ายทันที แล้วทำการแก้ไขเครื่องนั้นให้สามารถใช้งานได้ตามปกติต่อไป

หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานของหน่วยงาน

๒. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย

๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

ผู้รับผิดชอบ

หน่วยงานได้กำหนดให้มีผู้รับผิดชอบการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศ 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 โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านสารสนเทศและมีการเชิญวิทยากรจาก ภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ ๔. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ข้อ ๖. สร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

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 กำกับดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

๒. รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

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. ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓. รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๔. ต้องสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๕. ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๖. ต้องรับผิดชอบในการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน รวมทั้งระบบอินเตอร์เน็ตและ Intranet

๗. ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

หมวดที่ ๘ การรักษาความมั่นคงปลอดภัยด้านไซเบอร์และเทคโนโลยีดิจิทัลสมัยใหม่

วัตถุประสงค์

เพื่อกำหนดนโยบาย มาตรการ และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการใช้เทคโนโลยีดิจิทัลสมัยใหม่ขององค์การบริหารส่วนจังหวัดสระบุรี ให้มีความมั่นคงปลอดภัย สอดคล้องกับการเปลี่ยนแปลงทางเทคโนโลยีในยุคปัจจุบัน รองรับการให้บริการภาครัฐดิจิทัล และเป็นไปตามกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง โดยให้ถือปฏิบัติเป็นนโยบายของหน่วยงานอย่างเคร่งครัด

ส่วนที่ ๑ นโยบายและมาตรการด้านความมั่นคงปลอดภัยไซเบอร์

ข้อ ๑. ให้องค์การบริหารส่วนจังหวัดสระบุรีกำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นนโยบายสำคัญของหน่วยงาน โดยต้องมีมาตรการป้องกัน ตรวจจับ เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์ทุกรูปแบบ

ข้อ ๒. ให้ผู้ดูแลระบบดำเนินการติดตามสถานการณ์ภัยคุกคามด้านไซเบอร์อย่างต่อเนื่อง และรายงานผู้บังคับบัญชาทราบทันทีเมื่อพบเหตุการณ์หรือความเสี่ยงที่อาจส่งผลกระทบต่อระบบสารสนเทศของหน่วยงาน

ข้อ ๓. ให้หน่วยงานจัดทำและบังคับใช้แผนตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Incident Response Plan) และให้มีการทบทวน ปรับปรุง และทดสอบแผนดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๒ นโยบายการใช้งานระบบคลาวด์ และระบบออนไลน์

ข้อ ๔. การนำระบบคลาวด์ ระบบออนไลน์ หรือบริการดิจิทัลจากหน่วยงานภายนอกมาใช้งาน ให้ถือเป็นเรื่องที่ต้องผ่านการพิจารณาด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลก่อนทุกครั้ง

ข้อ ๕. ระบบคลาวด์หรือระบบออนไลน์ที่หน่วยงานเลือกใช้ ต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม มีการกำหนดสิทธิ์การเข้าถึงข้อมูลอย่างชัดเจน สามารถตรวจสอบย้อนหลังได้ และไม่ขัดต่อกฎหมายหรือระเบียบของทางราชการ

ข้อ ๖. ห้ามจัดเก็บ ประมวลผล หรือส่งต่อข้อมูลที่มีระดับความลับสูงผ่านระบบที่ไม่มีมาตรการรักษาความมั่นคงปลอดภัยเพียงพอ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาระดับสูงเป็นลายลักษณ์อักษร

ส่วนที่ ๓ นโยบายการใช้งานอุปกรณ์เคลื่อนที่และการปฏิบัติงานนอกสถานที่

ข้อ ๗. การใช้อุปกรณ์เคลื่อนที่หรืออุปกรณ์พกพาเพื่อปฏิบัติราชการ ให้ผู้ใช้งานต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยที่หน่วยงานกำหนด เช่น การตั้งรหัสผ่าน การเข้ารหัสข้อมูล และการป้องกันการเข้าถึงโดยมิชอบ

ข้อ ๘. ห้ามเข้าถึงหรือดำเนินการกับข้อมูลสำคัญของหน่วยงานผ่านเครือข่ายสาธารณะหรือเครือข่ายที่ไม่มีความปลอดภัย เว้นแต่จะมีมาตรการป้องกันที่เพียงพอและได้รับอนุญาตจากผู้บังคับบัญชา

ส่วนที่ ๔ นโยบายการคุ้มครองข้อมูลส่วนบุคคลในยุคดิจิทัล

ข้อ ๙. ให้ผู้บริหาร เจ้าหน้าที่ และผู้เกี่ยวข้องทุกระดับ ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด โดยต้องใช้ข้อมูลเท่าที่จำเป็น ตามวัตถุประสงค์ของภารกิจราชการเท่านั้น

ข้อ ๑๐. เมื่อเกิดเหตุข้อมูลส่วนบุคคลรั่วไหล สูญหาย ถูกเปิดเผย หรือถูกเข้าถึงโดยมิชอบ ให้รายงานผู้บังคับบัญชาทราบโดยทันที และให้ดำเนินการแก้ไขตามแผนตอบสนองเหตุการณ์ที่กำหนดไว้โดยไม่ชักช้า

ส่วนที่ ๕ นโยบายการใช้เทคโนโลยีใหม่และปัญญาประดิษฐ์

ข้อ ๑๑. การนำเทคโนโลยีใหม่หรือระบบปัญญาประดิษฐ์ (AI) มาใช้ในการปฏิบัติงานราชการต้องอยู่ภายใต้การกำกับดูแลของหน่วยงาน และต้องไม่ก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของระบบหรือการละเมิดข้อมูลส่วนบุคคล

ข้อ ๑๒. ให้มีการติดตาม ประเมินผล และทบทวนการใช้งานเทคโนโลยีดังกล่าวอย่างต่อเนื่อง เพื่อให้มั่นใจว่าสอดคล้องกับนโยบาย กฎหมาย และประโยชน์ของทางราชการ