นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติ พระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน)

โดย

สำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติ
พระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน)

คำนำ

ระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับสำนักงานในปัจจุบัน เพราะเข้ามาช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่าง ๆ ของสำนักงาน แต่ในขณะเดียวกันก็ทำให้สำนักงานมีความเสี่ยงเพิ่มขึ้นจากภัยคุกคามของระบบเทคโนโลยีสารสนเทศ ซึ่งอาจสร้างความเสียหายต่อการปฏิบัติราชการได้เนื่องจากระบบเทคโนโลยีสารสนเทศมีการเชื่อมโยงข้อมูลไปยังสำนักงานต่าง ๆ ส่งผลให้ช่องทางในการถูกบุกรุกเปิดกว้างขึ้นและอาจก่อให้เกิดเหตุอาชญากรรมทางคอมพิวเตอร์กับสำนักงานได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ส่งผลให้สำนักงานสูญเสียชื่อเสียงหรือภาพพจน์ได้ ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

ดังนั้น สำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) จึงจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ และเพื่อให้มีมาตรการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และให้การดำเนินการของหน่วยงานภายใน เป็นไปในทิศทางเดียวกัน สอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

ทั้งนี้ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานนั้นต้องได้รับความร่วมมือในการปฏิบัติตามอย่างเคร่งครัดและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอและปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว จึงหวังเป็นอย่างยิ่งว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) ทุกคน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานต่อไป

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน)

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อกำหนดทิศทางและเป็นกรอบแนวทางการดำเนินงานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางกฎหมาย และนโยบายฯ ที่เกี่ยวข้อง รวมถึงการกำหนดบทบาท หน้าที่ความรับผิดชอบ แนวทางปฏิบัติ ด้านความมั่นคงปลอดภัย และการควบคุมความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อคงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) ของข้อมูลสารสนเทศและระบบสารสนเทศของสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน)

๒. วัตถุประสงค์

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อกำหนดให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ มีแผนเตรียมความพร้อมสำหรับกรณีฉุกเฉิน และให้สามารถกู้ระบบกลับคืนได้ภายในระยะเวลาที่เหมาะสม เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานสามารถใช้งานได้เป็นปกติอย่างต่อเนื่อง เหมาะสม และสอดคล้องตามภารกิจ

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๔ นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้ง ต่อปี

๓. องค์ประกอบของนโยบาย

๓.๑ คำนิยาม

๓.๒ หมวดที่ ๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๓.๓ หมวดที่ ๒ นโยบายการจัดทำระบบสำรองข้อมูลและการเตรียมความพร้อมกรณีฉุกเฉิน

๓.๔ หมวดที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๕ หมวดที่ ๔ หน้าที่และความรับผิดชอบ

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

สำนักงาน หมายถึง สำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน)

ผู้อำนวยการ หมายถึง ผู้อำนวยการสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว

รองผู้อำนวยการ หมายถึง รองผู้อำนวยการสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว

ผู้บริหารสูงสุด (Chief Executive Officer : CEO) หมายถึง ผู้อำนวยการ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

ผู้อำนวยการสำนัก หมายถึง ผู้อำนวยการสำนักอำนวยการ ผู้อำนวยการสำนักพัฒนาพิพิธภัณฑ์และองค์ความรู้ ผู้อำนวยการสำนักนวัตกรรมการเกษตรเศษฐกิจพอเพียง ผู้อำนวยการสำนักสารสนเทศและการสื่อสาร และผู้อำนวยการสำนักพัฒนากิจการ

หัวหน้าหน่วยงาน และหัวหน้ากลุ่มงาน หมายถึง หัวหน้าหน่วยงานตรวจสอบภายใน หัวหน้ากลุ่มงานกฎหมาย และหัวหน้ากลุ่มงานแผน ติดตามและประเมินผล

ผู้บริหาร หมายถึง ผู้อำนวยการ รองผู้อำนวยการ ผู้อำนวยการสำนัก หัวหน้าหน่วยงาน และหัวหน้ากลุ่มงาน

สำนักสารสนเทศและการสื่อสาร หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน)

ผู้อำนวยการสำนักสารสนเทศและการสื่อสาร หมายถึง หัวหน้าในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของสำนักงาน และรับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ดูแลระบบ อย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการและแนวทางแก้ไขปัญหาจากสถานการณ์ ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศวางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัย ของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ

ที่ปรึกษาหรือผู้เชี่ยวชาญ หมายถึง ที่ปรึกษาหรือผู้เชี่ยวชาญตามมาตรา ๓๐ (๒) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) พ.ศ. ๒๕๕๒

เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ตามมาตรา ๓๐ (๑) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน) พ.ศ. ๒๕๕๒

ผู้ใช้งาน หมายถึง ผู้บริหาร เจ้าหน้าที่ ที่ปรึกษาหรือผู้เชี่ยวชาญ เจ้าหน้าที่จ้างเหมาบริการของสำนักงานหรือบุคคลภายนอกที่ได้รับอนุญาต (Authorized user) ให้ใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน

ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และ/หรือ ผู้อำนวยการสำนักสารสนเทศและการสื่อสาร ให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่สำนักงาน อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน โดยผู้บริหารสูงสุดจะเป็นผู้พิจารณาสิทธิในการใช้สินทรัพย์หรือสารสนเทศ

สารสนเทศ หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปตัวเลข ข้อความ หรือกราฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ ได้

ข้อมูล หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

ระบบงาน หมายถึง การนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบงานสารบรรณ ระบบจัดเก็บเอกสาร

ระบบปฏิบัติการ (operating system) หมายถึง ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุมการทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) และอุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์)

ระบบเครือข่าย (network) หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของสำนักงานพิพิธภัณฑ์เกษตรเฉลิมพระเกียรติพระบาทสมเด็จพระเจ้าอยู่หัว (องค์การมหาชน)

ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในสำนักงาน เข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในสำนักงาน

ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของสำนักงาน เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

เครื่องคอมพิวเตอร์แม่ข่าย (server) หมายถึง เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน อาทิจัดเก็บข้อมูลซอฟต์แวร์ สำหรับให้บริการแก่เครื่องคอมพิวเตอร์อื่นๆ หรือควบคุมการทำงานในเครือข่าย

สินทรัพย์ หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลภายใต้การดูแลของสำนักสารสนเทศและการสื่อสาร

ความมั่นคงปลอดภัยของสารสนเทศ (information security) หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของสำนักงานถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ความเสี่ยง หมายถึง โอกาสของทรัพยากรสารสนเทศในการถูกละเมิดการรักษาความปลอดภัย

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (access control) หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง การรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น

รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ไฟล์วอลล์ (firewall) หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

หมวดที่ ๑
นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ต้องมีมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานระบบสารสนเทศ การเข้าถึงระบบคอมพิวเตอร์อุปกรณ์เครือข่าย และการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้ายที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของสำนักงานได้อย่างถูกต้อง และจะต้องเป็นไปโดยสอดคล้องกับภารกิจของสำนักงาน

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการเข้าถึงและการใช้งานระบบสารสนเทศของสำนักงาน

๒. เพื่อให้ผู้บริหาร ผู้ดูแลระบบ ผู้ใช้งาน และผู้เกี่ยวข้องได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. สำนักสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบ

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน มีดังนี้

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)

๑. กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบเทคโนโลยีสารสนเทศของสำนักงาน เพื่อดูแลรักษาความปลอดภัยโดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการสำนักสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

๓. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือ มอบอำนาจ ดังนี้

๓.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้

- อ่านอย่างเดียว
- ลบข้อมูล
- แก้ไขข้อมูล
- สร้างข้อมูล
- อนุมัติ
- ป้อนข้อมูล
- ไม่มีสิทธิ

๓.๒ กำหนดเกณฑ์การระงับสิทธิมอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งานที่กำหนดไว้

๓.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของสำนักงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับพิจารณาอนุญาตจาก ผู้อำนวยการสำนักสารสนเทศและการสื่อสารหรือ ผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๔ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของสำนักงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการสำนักสารสนเทศและการสื่อสาร หรือ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔. การแบ่งประเภทข้อมูลและการจัดลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลสำนักงาน ดังนี้

๔.๑ กำหนดแบ่งประเภทข้อมูล

• ฐานข้อมูลระบบสารสนเทศ ได้แก่ ระบบสารบรรณอิเล็กทรอนิกส์ ข้อมูลบุคลากร ข้อมูลงบประมาณ การเงินและบัญชี เป็นต้น

• ข้อมูลประเภทสื่อต่าง ๆ ได้แก่ งานเอกสาร ภาพถ่าย เสียง วีดิทัศน์

๔.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับดังนี้

• ข้อมูลที่มีระดับความสำคัญมากที่สุด

• ข้อมูลที่มีระดับความสำคัญปานกลาง

• ข้อมูลที่มีระดับความสำคัญน้อย

๔.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

• ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

• ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

• ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

• ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผย หรือเผยแพร่ทั่วไปได้

๔.๔ จัดแบ่งระดับชั้นการเข้าถึงข้อมูลสารสนเทศ

• ระดับชั้นสำหรับผู้บริหาร

• ระดับชั้นสำหรับผู้ใชงาน

• ระดับชั้นสำหรับผู้ดูแลระบบ

๔.๕ การกำหนดเวลาในการเข้าถึงข้อมูล

• กำหนดการเข้าถึงและการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศ ผู้ใช้งานเข้าถึงและใช้งานได้ดังนี้

(ก) ระบบงานบริการ e-services สำหรับผู้ใช้งานภายนอก สามารถเข้าใช้งานได้ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

(ข) ระบบงานภายใน สำหรับผู้ใช้งานภายใน สามารถเข้าถึงระบบได้ตลอดเวลา ๒๔ ชั่วโมง ๗ วันเมื่ออยู่ในพื้นที่ของสำนักงาน

๔.๖ การกำหนดช่องทางการเข้าถึง

• เว็บไซต์ (เขาถึงได้ทุกช่วงเวลา)

• ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

• ระบบอินทราเน็ต (เข้าถึงได้ทุกช่วงเวลาเมื่ออยู่ในพื้นที่ของสำนักงาน)

• ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

ส่วนที่ ๒ ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirement for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

๑. มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และ สิทธิที่เกี่ยวข้องกับระบบสารสนเทศ ดังนี้

๑.๑ การควบคุมการเข้าถึงสารสนเทศ

๑.๑.๑ ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของสำนักงาน และตรวจสอบการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๑.๑.๒ ผู้ดูแลระบบ ควรจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

๑.๒ จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ และภารกิจดังนี้

๑.๒.๑ จำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ์ และภารกิจดังนี้

- ผู้บริหาร
- ผู้ดูแลระบบ
- ผู้ใช้งาน
- ที่ปรึกษาหรือผู้เชี่ยวชาญ
- ประชาชนทั่วไป

๑.๒.๒ เกณฑ์การแบ่งระดับการเข้าถึงข้อมูลและสารสนเทศ

- ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น
- ผู้ดูแลระบบ มีสิทธิในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่
- ผู้ใช้งาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย
- ที่ปรึกษาหรือผู้เชี่ยวชาญ เข้าถึงได้ตามภารกิจในสัญญาจ้าง
- ประชาชนทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างเท่านั้น

๑.๒.๓ การกำหนดสิทธิพิเศษสามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจ หรือเจ้าของข้อมูลเท่านั้น

๑.๒.๔ การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้ เมื่อได้รับความยินยอมจากเจ้าของสิทธิเท่านั้น

๒. มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

เพื่อควบคุม การเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว สร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

๑. การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงมีมาตรการเชิงป้องกันตามความเหมาะสม โดยปฏิบัติตามแนวทางดังนี้

๑.๑ ต้องกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ โดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของสำนักงาน

๑.๒ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงมีมาตรการเชิงป้องกันตามเหมาะสม

๑.๓ จัดฝึกอบรมการใช้งานสารสนเทศของสำนักงาน อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุง หรือเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๑.๔ จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของสำนักงาน

๑.๕ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือ ข้อควรระวังในรูปแบบที่สามารถ เข้าใจและนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ ได้แก่ การติดประกาศประชาสัมพันธ์ แผ่นพับ เผยแพร่ผ่านเว็บไซต์

๑.๖ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

๑.๗ ผู้ใช้งานจากภายนอกที่ได้รับสิทธิเพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เมื่อได้รับสิทธิการเข้าใช้งานระบบสารสนเทศของสำนักงาน

๒. การลงทะเบียนผู้ใช้งาน (user registration) มีขั้นตอนในการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว โดยปฏิบัติตามแนวทางดังนี้

๒.๑ ผู้ดูแลระบบจัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบสารสนเทศ

๒.๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

๒.๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามรายละเอียดสิทธิในแต่ละภารกิจในส่วนที่ ๒

๒.๔ ผู้ดูแลระบบจัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานเป็นลายลักษณ์อักษรเพื่อให้ผู้ใช้งานทราบถึงสิทธิ หน้าที่รับผิดชอบ และมาตรการด้านความมั่นคงปลอดภัยในการเข้าถึงระบบสารสนเทศ

๒.๕ มีการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๒.๖ การอนุญาตให้เข้าถึงระบบสารสนเทศต้องได้รับการพิจารณาอนุญาตจากผู้บริหารเจ้าของระบบสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๗ กำหนดให้มีการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและตัดออกจากทะเบียนผู้ใช้งานทันที เมื่อได้รับแจ้งจากต้นสังกัด หรือเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆที่เกี่ยวข้องกับการเข้าถึง โดยปฏิบัติตามแนวทางดังนี้

๓.๑ เมื่อเจ้าหน้าที่ของสำนักงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิการใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนสิทธิ หรือถอดถอนสิทธิออกจากระบบทันที และให้ทบทวนสิทธิอย่างสม่ำเสมอ

๓.๒ ผู้ดูแลระบบต้องปรับปรุงสิทธิการเข้าถึงข้อมูล และระบบสารสนเทศตามหน้าที่รับผิดชอบ และจัดเก็บข้อมูลการมอบสิทธิให้แก่ผู้ใช้งานไว้เป็นฐานข้อมูล

๓.๓ การแจ้งขอใช้สิทธิ หรือเปลี่ยนแปลงสิทธิในการเข้าถึงและใช้งานข้อมูลสารสนเทศ และระบบสารสนเทศต้องทำเป็นลายลักษณ์อักษร ระบุเหตุผลและความจำเป็น

๓.๔ ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ ในกรณีตรวจพบว่ามีการกระทำความผิดตามนโยบายการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

๓.๕ กรณีมีความจำเป็นต้องให้สิทธิพิเศษนอกเหนือจากภาระงานที่กำหนดกับผู้ใช้ ต้องพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยผู้ใช้จัดทำคำร้องเป็นลายลักษณ์อักษร และต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการสำนักสารสนเทศและการสื่อสาร โดยมีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น รวมทั้งกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว และต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้อย่างรัดกุม โดยปฏิบัติตามแนวทางดังนี้

๔.๑ กระบวนการจัดสรร หรือแจกจ่ายรหัสผ่านให้แก่ผู้ใช้งาน

• ผู้ดูแลระบบกำหนดการใช้งาน บัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

• ผู้ดูแลระบบกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสชั่วคราว และเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

• ผู้ดูแลระบบต้องให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน ได้แก่ ลงนามเอกสารแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของสำนักงาน

• ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดา และกำหนดรหัสผ่านที่แตกต่างกัน

• ผู้ดูแลระบบจัดส่งรหัสผ่านชั่วคราวให้ผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นและการใช้จดหมายอิเล็กทรอนิกส์เป็นช่องทางในการจัดส่ง

• ผู้ดูแลระบบมีการแจ้งหน้าที่รับผิดชอบของผู้ใช้งานให้ดูแลรหัสผ่านและดูแลการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ในทางที่ถูกต้อง โดยไม่ผิดต่อพระราชบัญญัติที่ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พ.ศ. ๒๕๖๐

• หากผู้ใช้งานจำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแล จดจำรหัสผ่านหลายตัว สามารถใช้รหัสผ่านเดียวที่มีคุณภาพ สำหรับการเข้าถึงทุกระบบได้ ซึ่งระบบเหล่านั้นต้องมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

• ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และกำหนดรหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

๔.๒ ขั้นตอนการเปลี่ยนรหัส

• ผู้ดูแลระบบอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเองผู้ใช้ต้องการเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะเปลี่ยนรหัสใหม่

• ผู้ใช้งานทำการล็อกอินเข้าใช้งานระบบงานครั้งแรกและทำการเปลี่ยนรหัสผ่านทันที หลังจากได้รับรหัสผ่านชั่วคราว

• ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะ หรือทุกครั้งที่มีการแจ้งเตือน หรือบังคับให้เปลี่ยนรหัสผ่านจากผู้ดูแลระบบ

• กรณีผู้ดูแลระบบตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูกนำไปใช้โดยผู้อื่น ผู้ใช้งานรายนั้นจะถูกตัดสิทธิการใช้งานชั่วคราวจนกว่าจะดำเนินการ เปลี่ยนรหัสผ่านเป็นที่เรียบร้อย

๕. การทบทวนสิทธิการเข้าถึง (review of user access rights) ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีอย่างน้อยปีละ ๑ ครั้ง หรือ เมื่อมีการเปลี่ยนแปลง ได้แก่ มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทางดังนี้

๕.๑ พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามหน่วยงาน พร้อมรายละเอียดสิทธิที่ได้รับของแต่ละบุคคล

๕.๒ จัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงาน เพื่อดำเนินการทบทวนรายชื่อและสิทธิการเข้าใช้งานว่าถูกต้องหรือไม่

๕.๓ ผู้ดูแลระบบดำเนินการแก้ไขข้อมูลสิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากผู้ใช้งาน

๕.๔ ขั้นตอนการปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๗ วัน หรือเมื่อเปลี่ยนตำแหน่งภายในต้องดำเนินการภายใน ๗ วัน

ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือ การลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีแนวปฏิบัติ ดังนี้

๑. การใช้งานรหัสผ่าน (password use)

๑.๑ เปลี่ยนรหัสผ่านชั่วคราวทันที เมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

๑.๒ กำหนดรหัสผ่านให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๑.๓ ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อ หรือนามสกุลของตนเอง หรือข้อมูลที่เกี่ยวข้องกับตนเองที่ผู้อื่นสามารถนำมาใช้เพื่อเดารหัสผ่านได้ หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๑.๔ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๑.๕ เก็บบัญชีและรหัสผ่านของตนเองไว้เป็นความลับ

๑.๖ ผู้ใช้ต้องทำการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้ และรหัสผ่าน โดยผู้ใช้แต่ละคนต้องมีบัญชีชื่อผู้ใช้ของตนเอง และห้ามทำการเผยแพร่แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๑.๗ ผู้ใช้ต้องเปลี่ยนรหัสผ่านทันที เมื่อสงสัยว่ารหัสผ่านอาจถูกเปิดเผย หรือล่วงรู้

๑.๘ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๒. การป้องกันอุปกรณ์ขณะที่ไม่มีผู้ใช้งานอุปกรณ์

๒.๑ ผู้ใช้งานต้องตั้งค่าการใช้โปรแกรมถนอมหน้าจอ (screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้น เมื่อต้องการใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

๒.๒ ผู้ดูแลระบบต้องสร้างความตระหนัก เพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกันผู้ไม่มีสิทธิเข้าถึงอุปกรณ์ขณะที่ไม่มีผู้ดูแล

๒.๓ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๒.๔ ผู้ใช้งานต้องล็อคใส่รหัสป้องกันการเข้าถึงอุปกรณ์ และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ได้ถูกใช้งานหรือปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๓. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

๓.๑ มีการป้องกันสินทรัพย์ของสำนักงาน และควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยมีการจัดการบริเวณล้อมรอบ การควบคุม การเข้า-ออกการจัดบริเวณการเข้าถึงการส่งผลิตภัณฑ์โดยบุคคลภายนอก การวางอุปกรณ์ และระบบสนับสนุนการทำงาน

๓.๒ มีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันสินทรัพย์ของสำนักงาน
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ไม่เก็บข้อมูลสำคัญของสำนักงาน ไว้บนเครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูลที่เป็นสมบัติส่วนบุคคล
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร
- ข้อมูลสำคัญที่บันทึกไว้ใน กระดาษ สื่อบันทึกข้อมูลแฟลชไดร์ฟ หรือ ฮาร์ดดิสก์ เมื่อไม่ใช้งานต้องจัดเก็บไว้ในที่ปลอดภัย ไม่ทิ้งวางไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๓.๓ ควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยผู้เป็นเจ้าของ หรือผู้ที่ได้รับมอบหมายเท่านั้น

๓.๔ การลบ หรือเขียนข้อมูลทับบนข้อมูลที่สำคัญ ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เปลี่ยนทดแทน หรือ ทำลาย เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญได้

๓.๕ สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๖ ในการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่าง ๆ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

สื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
flash drive, thumb drive, USB drive	- ใช้การทำลายข้อมูล โดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิกส์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD ๕๒๒๐.๒๒-M
แผ่น CD/DVD	ใช้วิธีการหักให้เสียหาย หรือเผาทำลาย

๔. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบเครือข่าย (network access control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตให้ดำเนินการ ดังนี้

๑. การใช้งานบริการเครือข่าย ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๑.๑ การเข้าถึงระบบเครือข่ายต้องพิสูจน์ตัวตนผู้ใช้งานด้วยบัญชีผู้ใช้งานที่สำนักงาน ออกให้

๑.๒ ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบเครือข่ายตามสิทธิที่ได้รับอนุญาตเท่านั้น

๑.๓ การเข้าถึงระบบเครือข่ายของสำนักงาน จากภายนอก ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นเป็นพิเศษจากมาตรการเข้าถึงระบบเครือข่ายสำนักงาน จากภายใน

๑.๔ การใช้เครื่องมือต่าง ๆ เพื่อตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connection) ต้องได้รับการอนุมัติจากผู้อำนวยการสำนักสารสนเทศและการสื่อสาร และยืนยันตัวบุคคลสำหรับการใช้งานด้วยชื่อผู้ใช้งานและรหัสผ่านกับระบบไฟล์วอลล์ หรือระบบ VPN ที่สำนักงาน จัดเตรียมไว้ให้จึงจะสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงาน ได้

๓. การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการหรือกระบวนการ ที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึงดังนี้

๓.๑ จัดทำบัญชีทะเบียนสินทรัพย์อุปกรณ์ที่เชื่อมต่อเข้ากับระบบเครือข่าย เพื่อการตรวจสอบยืนยันอุปกรณ์บนเครือข่าย

๓.๒ อุปกรณ์ที่เชื่อมต่อเข้ากับระบบเครือข่ายต้องมีการลงทะเบียน mac address ของอุปกรณ์และชื่อผู้ใช้งานอุปกรณ์

๓.๓ การตรวจสอบยืนยันอุปกรณ์บนเครือข่ายสามารถใช้ตรวจสอบได้จาก mac address หรือการตรวจสอบผ่านการตั้งค่าการใช้งาน IEEE ๘๐๒.๑x

๓.๔ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดย ผู้ดูแลระบบเท่านั้น

๔. การป้องกันพอร์ตที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ (remote diagnostic and configurationport protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพ และทางเครือข่าย โดยปฏิบัติดังนี้

๔.๑ ควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม

๔.๒ กำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

๔.๓ ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอกสำนักงาน แต่ให้เชื่อมต่อผ่านช่องทางที่จัดเตรียมให้

๔.๔ อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องควบคุมเครือข่ายที่ควบคุมความปลอดภัย

๔.๕ ปิดพอร์ตหรือปิดบริการบนอุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งาน ตรวจสอบอุปกรณ์อย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๕. การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยปฏิบัติดังนี้

๕.๑ จัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตการแบ่งแยกเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่ายปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๒ แบ่งแยกเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้งาน และระบบงานต่าง ๆ

๕.๓ ใช้ไฟล์วอลล์กันหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย

๕.๔ ใช้เกตเวย์ เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกสำนักงาน

๖. การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้ งานเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง โดยต้องปฏิบัติดังนี้

๖.๑ การเชื่อมต่อระหว่างเครือข่าย อนุญาตให้มีการเชื่อมต่อผ่านหมายเลขไอพีแอดเดรสที่สำนักงาน กำหนดให้เท่านั้น

๖.๒ ผู้ใช้งานต้องเชื่อมต่ออุปกรณ์ผ่านช่องทางที่สำนักงาน จัดเตรียมให้เท่านั้น

๖.๓ ระบบเครือข่ายทั้งหมดต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall, IDS/IPS)

๖.๔ ไม่อนุญาตให้ผู้ใช้งานทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณเครือข่ายภายในสำนักงาน โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๖.๕ ใช้ระบบตรวจสอบจับผู้บุกรุกในระดับเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๖.๖ กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง หากมีการแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๖.๗ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๗. การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ โดยปฏิบัติดังนี้

๗.๑ อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลยไอพีแอดเดรสที่กำหนด

๗.๒ มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย

๗.๓ ควบคุมการไหลของข้อมูลผ่านเครือข่าย

๗.๔ ตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง

๗.๕ กำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย

๗.๖ จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อระงับการใช้จากเส้นทางอื่น

๗.๗ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๗.๘ กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก

๗.๙ ต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (operation system access control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้อนุญาต โดยมีแนวปฏิบัติดังนี้

๑. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้อง ควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยปฏิบัติดังนี้

๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๑.๒ หลังจากระบบติดตั้งเสร็จ ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

๑.๓ ผู้ใช้งานต้องตั้งค่าโปรแกรมพักหน้าจอ (screen saver) ให้มีรหัสผ่านเพื่อทำการล็อค หน้าจอภาพเมื่อไม่มีการใช้งานเกินกว่า ๕ นาที

๑.๔ ผู้ดูแลระบบต้องตั้งค่าไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๑.๕ ผู้ดูแลระบบต้องตั้งค่าให้ระบบยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดา รหัสผ่านจากเครื่องปลายทาง

๑.๖ ผู้ดูแลระบบต้องตั้งค่าให้มีการจำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

๑.๗ ผู้ใช้งานต้องทำการลงบันทึกออก (logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ผู้ใช้งานต้องแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านสำหรับการใช้งานระบบสารสนเทศดังนี้

๒.๑ การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบต้องให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

๒.๒ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนโดยใช้ username และ password ของตนเองทุกครั้งก่อนใช้ระบบสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๒.๓ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้งานไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๒.๔ ผู้ใช้งานต้องลงบันทึกเข้า (login) โดยใช้ชื่อบัญชีผู้ใช้งานของตนเอง และทำการลงบันทึกออก (logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๓. การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยต้องปฏิบัติดังนี้

๓.๑ จำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานปอนรหัสผ่านผิดเกินจำนวนครั้งที่กำหนด ระบบจะทำการล็อคสิทธิการเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบจะปลดล็อคให้

๓.๒ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีความพยายามในการเดารหัสผ่านจากเครื่องปลายทาง

๓.๓ มีระบบให้ผู้ใช้งานสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

๓.๔ จัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

๓.๕ ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

๓.๖ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให่ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มตนที่มาพร่อมกับการติดตั้งระบบโดยทันที

๓.๗ ผู้ดูแลระบบไม่สามารถเข้าดูรหัสผ่านผู้ใช้งานได้

๔. การใช้งานโปรแกรมอรรถประโยชน์

๔.๑ จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๔.๒ กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๔.๓ จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ตองใช้งานเป็นประจำ

๔.๔ ถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็น ออกจากระบบ

๔.๕ กรณีผู้ใช้งานต้องการติดตั้งโปรแกรมใดๆ เพิ่มเติมต้องแจ้งผู้ดูแลระบบ

๔.๖ ห้ามใช้งานโปรแกรมละเมิดลิขสิทธิ์

๔.๗ ห้ามผู้ใช้งานปรับแต่งโปรแกรมอรรถประโยชน์

๔.๘ ห้ามผู้ใช้งานคัดลอกโปรแกรมไปใชผิดวัตถุประสงค์

๕. การหมดเวลาใช้งานระบบสารสนเทศ (session time-out)

๕.๑ กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที เป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงสูงหรือความสำคัญสูงใช้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาที ตามความเหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๕.๒ ถ้าไม่มีการใช้งานระบบต่องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๕.๓ กำหนดให้สารสนเทศที่มีความสำคัญสูง หรือระบบงานที่มีการใช้งานที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อไม่เกิน ๒ ชั่วโมงต่อครั้ง

๖. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time)

ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๖.๑ กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของสำนักงาน ตามปกติเท่านั้น

๖.๒ การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๖.๓ กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุมดังนี้

๑. จำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน โดยกำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึง ดังนี้

๑.๑ การจำกัดการเข้าถึงของผู้ใช้งาน

- เข้าได้ตามสิทธิที่ได้รับอนุญาตเท่านั้น
- กำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคล
- บันทึกการออกจากระบบโดยทันทีที่ใช้งานเสร็จ

๑.๒ การบันทึกเหตุการณ์ที่เกี่ยวข่องกับการใช้งานระบบสารสนเทศ ต้องบันทึกข้อมูลพฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ ดังนี้

- ชื่อบัญชีผู้ใช้งาน
- วันเวลาที่เข้าถึงระบบ
- วันเวลาที่ออกจากระบบ
- แสดงการใช้สิทธิ ได้แก่ สิทธิของผู้ดูแลระบบ
- แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ ได้แก่ เปิด ปิด เขียน อ่านไฟล์ เป็นต้น
- หมายเลขไอพีแอดเดรสที่เข้าถึง
- แสดงการหยุดการทำงานของระบบป้องกันการบุกรุก
- แสดงการหยุดการทำงานของระบบงานที่สำคัญ

๑.๓ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของสำนักงาน ตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศและข้อมูล

๑.๔ การควบคุมผู้รับจ้าง (outsource) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และพัฒนาระบบสารสนเทศ

- กำหนดคุณสมบัติของผู้รับจ้างที่ชัดเจน ต้องมีประสบการณ์ที่นาเชื่อถือ หรือใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล มีความพร้อมด้านเทคโนโลยีของการรับจ้าง ทั้งในส่วนของฮาร์ดแวร์และซอฟท์แวร์รวมถึงระบบสนับสนุนอื่น ๆ เพื่อให้ได้ผู้รับจ้างที่มีคุณสมบัติตรงตามมาตรฐานที่สำนักงานต้องการ
- มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับจ้าง และต้องกำหนดขอบเขตและระดับการรับจ้างอย่างชัดเจน และต้องไม่เปิดเผยข้อมูลของสำนักงาน ทั้งในช่วงของการว่าจ้าง และเสร็จสิ้นการจ้างไปแล้ว
- ควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลองแทนข้อมูลจริง
- ตรวจรับงานที่ส่งมอบจากผู้รับจ้างให้ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

• ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้รับจ้าง (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

ทั้งนี้ ผู้รับจ้าง (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยของสำนักงาน และต้องลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของสำนักงาน

๒. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสำนักงาน จะต้องดำเนินการดังนี้

๒.๑ แยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่นๆ

๒.๒ ควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ โดยการติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่น ทำการป้องกันการมีทรัพยากรไม่เพียงพอ และเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

๒.๓ กำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเทานั้น

๒.๔ ติดตามเฝ้าระวังการใช้งานระบบซึ่งไวต่อการรบกวน และระงับการใช้งานทันทีเมื่อพบเหตุการณผิดปกติ

๓. การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

๓.๑ ตรวจสอบความพร้อมของคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

๓.๒ ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

๓.๓ เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

๓.๔ เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่รับคืนด้วยความรอบคอบ

๓.๕ เมื่อเกิดความเสียหายขึ้นจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๓.๖ มีการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณไม่น้อยกว่า ๑๕ นาที เพื่อล็อคเมื่อไม่ได้ใช้งาน

๓.๗ กำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๓.๘ ติดตั้งโปรแกรมตรวจจับ กำจัดโปรแกรมไม่ประสงค์ดี และปรับปรุงให้ทันสมัย

๓.๙ มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ ต่าง ๆ ที่จะทำการติดตั้งก่อนทำการติดตั้งเพื่อใช้งาน

๓.๑๐ หลีกเลี่ยงการใช้อุปกรณ์คอมพิวเตอร์แบบพกพาร่วมกับผู้อื่น

๔. การปฏิบัติงานจากภายนอกสำนักงาน (teleworking)

๔.๑ ผู้ใช้งานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

๔.๒ การรักษาความปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในสำนักงาน

๔.๓ ผู้ใช้งานต้องระมัดระวังรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการควบคุมอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

๔.๔ ผู้ใช้งานต้องไม่อนุญาตให้ครอบครัวหรือผู้อื่นเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน

๔.๕ ตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศของสำนักงานจากระยะไกลมีระบบป้องกันไวรัสและการใช้งานไฟล์วอลล์อย่างเหมาะสม

ส่วนที่ ๘ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (wireless access control)

๑. ห้ามผู้ใช้งานดำเนินการติดตั้งอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบไร้สาย (wireless access point) ภายในสำนักงาน

๒. ให้ผู้ใช้งานใช้เฉพาะอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบไร้สายที่เตรียมไว้เท่านั้น หากมีความประสงค์จะใช้งานอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบไร้สายเพิ่มเติม ต้องแจ้งให้ทางผู้ดูแลระบบทราบและเป็นผู้ดำเนินการติดตั้ง

๓. ผู้ดูแลระบบ (system administrator) ต้องดำเนินการดังต่อไปนี้

๓.๑ ทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓.๒ ทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๓.๓ ควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๓.๔ ทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

๓.๕ มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในสำนักงาน

ส่วนที่ ๙ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์

๑. ผู้ใช้งานจะต้องลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) กับทางสำนักสารสนเทศและการสื่อสาร ก่อนจึงจะสามารถใช้งานได้

๒. เมื่อผู้ใช้งานได้รับรหัสผ่าน (password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (password) โดยทันที

๓. ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (password) ไว้ในระบบคอมพิวเตอร์

๔. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะ หรือทุกครั้งที่มีการแจ้งเตือน หรือบังคับให้เปลี่ยนรหัสผ่านจากผู้ดูแลระบบ

๕. การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๖. ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์นั้น

๗. การส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้งานต้องระบุชื่อผู้รับ หัวข้อ ให้ชัดเจน และใช้ภาษาสุภาพไม่ขัดต่อจริยธรรม ไม่ปลุกปั่น ยั่วยุ เสียดสีหรือส่อในทางผิดกฎหมาย

๘. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องบันทึกการออกทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ของตน

ส่วนที่ ๑๐ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (firewall control)

๑. ผู้ใช้งานสามารถใช้บริการการเชื่อมต่อเครือข่ายเฉพาะที่ไฟล์วอลล์อนุญาตให้ใช้งานเท่านั้น

๒. ทุกบริการ (services) และเส้นทางเชื่อมต่ออินเตอร์เน็ตที่ไม่อนุญาตตาม policy จะต้องถูกบล็อก (block) โดย firewall

๓. การเข้าถึงอุปกรณ์ firewall สามารถเข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

๔. ผู้ดูแลระบบหรือผู้ใช้งานที่มีความจำเป็นต้องใช้งานเซิรฟเวอร์นอกเหนือจากบริการปกติจะต้องลงทะเบียนขออนุญาตการใช้งานเป็นลายลักษณ์อักษรก่อนจึงจะสามารถใช้งานได้

๕. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยจะต้องจัดเก็บไม่น้อยกว่า ๙๐ วัน

ส่วนที่ ๑๑ การบริหารจัดการสินทรัพย์

๑. ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ที่มีการติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และ/หรือ อุปกรณ์บริหารจัดการเครือข่ายโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

๒. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

๓. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของสำนักงาน ที่ยืมไป

๔. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์หรือโน้ตบุ๊ค ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการสำนักสารสนเทศและการสื่อสาร

๕. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุดหรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

๖. ทรัพย์สินและระบบสารสนเทศต่าง ๆ ที่สำนักงาน จัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของ สำนักงาน เท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่สำนักงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อ สำนักงาน

๗. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๖. ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๑๒ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log file)

๑. จัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

๒. มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะ บุคคลที่เกี่ยวของเท่านั้น

๓. มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบเพื่อประโยชน์ในการใช้ตรวจสอบและตองเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

หมวดที่ ๒
นโยบายการจัดทำระบบสำรองข้อมูลและการเตรียมความพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของสำนักงาน มีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง

๒. เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล การกู้คืนข้อมูล และการเตรียมความพร้อมกรณีฉุกเฉิน ให้ผู้ดูแลระบบ ถือปฏิบัติ

๓. เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหาต้องสำรองข้อมูลและสามารถกู้คืนข้อมูล ได้ในกรณีที่จำเป็น

ผู้รับผิดชอบ

๑. สำนักสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบ

แนวปฏิบัติ

๑. การพิจารณาคัดเลือกระบบสารสนเทศที่มีความสำคัญ และจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๑.๑ จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่มีความสำคัญ ที่ต้องมีระบบสำรอง และทบทวนบัญชี อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ระบบสำรองต้องอยู่ในห้อง หรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุมดังนี้

๑.๒.๑ มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง

๑.๒.๒ มีระบบไฟฟ้าสำรอง

๑.๒.๓ มีระบบปรับอากาศและความชื้นที่เหมาะสม

๑.๒.๔ มีระบบป้องกันอัคคีภัย

๑.๒.๕ มีระบบแสงสว่างที่เหมาะสม

๑.๒.๖ มีระบบสื่อสารหรือระบบเครือข่ายสำรอง

๑.๒.๗ มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

๑.๓ มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

๑.๔ การสำรองข้อมูล (data backup)

๑.๔.๑ จัดทำขั้นตอนปฏิบัติสำหรับการสำรองข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

๑.๔.๒ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของสำนักงาน ที่จะทำการสำรองข้อมูล และ ทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

๑.๔.๓ กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

๑.๔.๔ กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อยให้มีความถี่ในการสำรองข้อมูลมากขึ้น

๑.๔.๕ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานการณ์ทำงานสำเร็จ/ไม่สำเร็จ เป็นต้น

๑.๔.๖ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ ซอฟตแวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และข้อมูลการตั้งค่าระบบและอุปกรณ์ต่าง ๆ เป็นต้น

๑.๔.๗ จัดเก็บข้อมูลสำรองไว้ในระบบสำรอง

๑.๔.๘ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลสำรอง

๑.๕ การกู้คืนข้อมูล (data recovery)

๑.๕.๑ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

๑.๕.๒ ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๑.๕.๓ ให้ใช้ข้อมูลทันสมัยที่สุด ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

๑.๕.๔ ทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

๒. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน ดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๒.๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

๒.๑.๑ กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๑.๒ ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยง เหล่านั้น

๒.๑.๓ การกูคืนระบบสารสนเทศ

๒.๑.๔ การสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๒.๑.๕ กำหนดช่องทางในการติดต่อกับผู้บริการภายนอก ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ และ ซอฟท์แวร์ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๒.๑.๖ สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒ ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์

๔. มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณี ฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๕. ความถี่ของการปฏิบัติในแต่ละข้อ เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้

๖. การติดตามและรายงานผล กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ ผู้อำนวยสำนักสารสนเทศและการสื่อสาร ทราบเป็นประจำทุกเดือน เพื่อรายงานสรุปให้ผู้บริหารสูงสุด (Chief Executive Officer : CEO) ทราบและหากมีเหตุฉุกเฉินร้ายแรงต้องรายงานให้ผู้บริหารระดับสูงสุดของหน่วยงานทราบทันที

หมวดที่ ๓
นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. สำนักสารสนเทศและการสื่อสาร

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ผู้ตรวจสอบภายใน (internal auditor) หรือผู้ตรวจสอบจากภายนอก (external auditor)

แนวปฏิบัติ

๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง มีวิธีการปฏิบัติ ดังนี้

- มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ
- มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
- มีการตรวจสอบและประเมินความเสี่ยงของระบบให้บริการ
- มีการตรวจประเมินระบบสารสนเทศ (information system audit considerations) อย่างน้อย ๑ ครั้งต่อปี เพื่อให้มั่นใจได้ว่าการตรวจประเมินมีประสิทธิภาพและผลการตรวจสอบเป็นที่น่าเชื่อถือได้

๒. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึงอย่างน้อยดังนี้

๒.๑ แนวทางในการตรวจสอบและประเมินความเสี่ยง

- กำหนดเกณฑ์การประเมินความเสี่ยง
- การประเมินความเสี่ยง
- การจัดลำดับความสำคัญของความเสี่ยง
- ค้นหาวิธีเพื่อลดความเสี่ยงและจัดทำแผนลดความเสี่ยง
- รายงานผลการประเมินความเสี่ยงต่อคณะทำงานตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
- มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง
- มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง
- มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายการพร้อมข้อเสนอแนะให้ผู้บริหารพิจารณาระดับความเสี่ยงที่เป็นอยู่และกำหนดแนวทางการปรับปรุง และแจ้งให้หน่วยงานที่เกี่ยวข้องทราบเพื่อนำไปปฏิบัติ

๒.๒ มาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อยดังนี้

- ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
- ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งดำเนินการทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้ โดยมีการป้องกันเป็นอย่างดี

• มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

• มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึก Log File แสดงการเข้าถึงนั้น ซึ่งรวมถึงวัน และเวลาที่เข้าถึงระบบงานที่สำคัญๆ

• ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ต้องแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

หมวดที่ ๔
หน้าที่และความรับผิดชอบ

วัตถุประสงค์

เพื่อกำหนดหน้าที่และความรับผิดชอบของผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ

แนวปฏิบัติ

๑. ระดับนโยบาย ได้แก่

๑) ผู้อำนวยการ

๒) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

๓) ผู้อำนวยการสำนักสารสนเทศและการสื่อสาร โดยมีหน้าที่และความรับผิดชอบ ดังนี้

๑.๑ กำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

๑.๒ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่สำนักงาน หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ระดับบริหาร ได้แก่ ผู้อำนวยการสำนัก หัวหน้าหน่วยงาน หัวหน้ากลุ่มงาน โดยมีหน้าที่และความรับผิดชอบ ดังนี้

๒.๑ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผนติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒.๒ ควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

๒.๓ วางแผน ทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๓ ระดับปฏิบัติ ได้แก่ เจ้าหน้าที่ฝ่ายสารสนเทศ สำนักสารสนเทศและการสื่อสาร หรือผู้ดูแลระบบที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และ/หรือ ผู้อำนวยการสำนักสารสนเทศและการสื่อสาร โดยมีหน้าที่และความรับผิดชอบ ดังนี้

๓.๑ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๒ ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๓.๓ ดำเนินการสำรองข้อมูลและเรียกคืนข้อมูล (backup and recovery) ตามรอบระยะเวลาที่กำหนด

๓.๔ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (hacker) โดยไม่ได้รับอนุญาต

๓.๕ การรักษาความปลอดภัย ระบบอินเทอร์เน็ต

๓.๖ รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

๓.๗ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ