องค์การบริหารไนท์ซาฟารี
(องค์การมหาชน)

ประกาศองค์การบริหารไนท์ซาฟารี (องค์การมหาชน)
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
องค์การบริหารไนท์ซาฟารี (องค์การมหาชน) พ.ศ. ๒๕๖๙

ประกาศองค์การบริหารไนท์ซาฟารี (องค์การมหาชน) เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ องค์การบริหารไนท์ซาฟารี (องค์การมหาชน) พ.ศ. ๒๕๖๙

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องดำเนินการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ประกอบกับตามความในมาตรา มาตรา ๒๘ มาตรา ๒๙ และ มาตรา ๔๗ แห่งพระราชกฤษฎีกาจัดตั้งองค์การบริหารไนท์ซาฟารี (องค์การมหาชน) พ.ศ. ๒๕๖๘ ผู้อำนวยการจึงออกประกาศ ดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า "ประกาศองค์การบริหารไนท์ซาฟารี (องค์การมหาชน) เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศองค์การบริหารไนท์ซาฟารี (องค์การมหาชน) พ.ศ. ๒๕๖๙

ข้อ ๒. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศองค์การบริหารไนท์ซาฟารี (องค์การมหาชน) พ.ศ. ๒๕๖๙ ให้เป็นไปตามเอกสารแนบท้ายประกาศนี้

ข้อ ๓. ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๗ กุมภาพันธ์ พ.ศ. ๒๕๖๙

(นางสาวฐิติรัตน์ ต๊ะวันวงค์)
รองผู้อำนวยการองค์การบริหารไนท์ซาฟารี
ปฏิบัติหน้าที่ ผู้อำนวยการองค์การบริหารไนท์ซาฟารี

องค์การบริหารไนท์ซาฟารี
(องค์การมหาชน)

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์การบริหารไนท์ซาฟารี (องค์การมหาชน) พ.ศ. ๒๕๖๙

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การบริหารไนท์ซาฟารี (องค์การมหาชน) หรือต่อไปนี้เรียกว่า “องค์การ” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้ง ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์การ จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังนี้

๑. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือเครือข่ายคอมพิวเตอร์ขององค์การ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

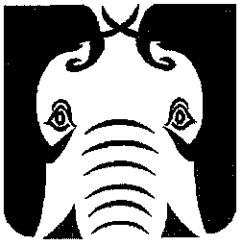
๒. เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้ผู้ปฏิบัติงานในองค์การได้รับทราบและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้ปฏิบัติงาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์การ

๔. เพื่อตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๕. เพื่อส่งเสริมให้ผู้ปฏิบัติงาน ผู้ดูแลระบบขององค์การมีความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๖. นโยบายนี้ต้องดำเนินการตรวจสอบ ประเมิน และทบทวนปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลา ๑ ครั้งต่อปี



เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

องค์การบริหารไนท์ซาฟารี (องค์การมหาชน) พ.ศ. ๒๕๖๙

สารบัญ

คำนิยามศัพท์

องค์การ หมายความว่า องค์การบริหารไนท์ซาฟารี (องค์การมหาชน)

ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) หมายความว่า ผู้อำนวยการองค์การบริหารไนท์ซาฟารี

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) หมายความว่า ผู้อำนวยการหรือผู้ที่ผู้อำนวยการมอบหมายให้ดูแลรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานด้านระบบเทคโนโลยีสารสนเทศขององค์การ

ผู้บังคับบัญชา หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์การด้านเทคโนโลยีสารสนเทศ

ผู้ใช้งาน หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์การ โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์การได้กำหนดไว้ ดังนี้

- **ผู้บริหาร** หมายความว่า เจ้าหน้าที่กลุ่มนักบริหารในระดับต้น กลาง และสูงขององค์การบริหารไนท์ซาฟารี
- **ผู้ปฏิบัติงาน** หมายความว่า เจ้าหน้าที่กลุ่มงานปฏิบัติการ ลูกจ้าง ที่ปรึกษาหรือผู้เชี่ยวชาญ และลูกจ้างโครงการต่าง ๆ ที่ใช้งานระบบเทคโนโลยีสารสนเทศขององค์การ
- **ผู้ดูแลระบบ** (System Administrator) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ รวมถึงผู้ดูแลระบบสารสนเทศที่มีหน้าที่กำหนดสิทธิบริหารจัดการบัญชีผู้ใช้ ตั้งค่าการใช้งานระบบสารสนเทศต่าง ๆ ขององค์การ เช่น ระบบ e-Office ระบบ Internet เป็นต้น
- **ผู้ดูแลข้อมูลระบบ** (Content Administrator) หมายความว่า บุคคล นิติบุคคลภายนอกที่มีสิทธิเข้าถึงและปรับปรุงข้อมูลระบบสารสนเทศขององค์การ
- **ผู้รับบริการ** หมายความว่า บุคคล นิติบุคคลภายนอก ที่เข้าใช้บริการระบบสารสนเทศขององค์การ
- **บุคคลภายนอก** หมายความว่า บุคคลที่องค์การบริหารไนท์ซาฟารี อนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศขององค์การ ได้ชั่วคราวเพื่อประโยชน์ในการดำเนินงานขององค์การ ได้แก่ พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดต่อหรือดูแลรักษาระบบให้กับองค์การ หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง

สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศขององค์การ

เจ้าของข้อมูล หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สินทรัพย์ หรือ ทรัพย์สินสารสนเทศ หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่

(๑) ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๒) ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(๓) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

ข้อมูลอิเล็กทรอนิกส์ หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

นโยบาย หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้ง คุณสมบัติอื่นได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้าม ปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่ง อาจทำให้ระบบขององค์การถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานภายนอก ที่องค์การอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ขององค์การ โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

สารสนเทศ (Information) หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

ระบบเครือข่าย (Network System) หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์การได้ เช่น ระบบ LAN ระบบ Internet เป็นต้น

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายความว่า ระบบงานขององค์การที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่องค์การสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคง ปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

สื่อโซเชียลมีเดีย (Social Media) หมายความว่า สื่อหรือช่องทางในการติดต่อในลักษณะของการสื่อสารแบบสองทางผ่านระบบเครือข่ายอินเทอร์เน็ต เป็นสื่อรูปแบบใหม่ (New Media) ที่บุคคลทั่วไปสามารถนำเสนอและเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะโดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภทต่าง ๆ ในปัจจุบันมีแหล่งให้บริการสื่อโซเชียลมีเดียเกิดขึ้นบนระบบเครือข่ายอินเทอร์เน็ตเป็นจำนวนมาก เช่น Line, Facebook, Twitter, Instagram, YouTube รวมถึงสื่อโซเชียลมีเดียอื่น ๆ และเว็บไซต์ต่าง ๆ ทั้งในประเทศและต่างประเทศ ที่เปิดให้บริการ Instant Messaging, File Sharing, Photo Sharing, Video Sharing และกระดานข่าว (Web board) เป็นต้น

หมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

ส่วนที่ ๑ การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์ (Computing System Control Room)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน การรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้ จะมีผลบังคับใช้กับผู้ใช้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ

๑.๑ แนวปฏิบัติการควบคุมการเข้าออก

ข้อ ๑ องค์การกำหนดให้พื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบ เทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสมโดยกำหนดพื้นที่รักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

ข้อ ๒ กำหนดสิทธิให้กับผู้ปฏิบัติงาน ที่มีสิทธิในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย ดังนี้

(๑) จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

(๒) กำหนดให้ผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออก ดังกล่าวโดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”

(๓) จัดให้มีผู้ปฏิบัติงานทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่เป็นประจำ และให้ปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งาน ปีละ ๑ ครั้ง เป็นอย่างน้อย

(๔) บุคคลภายนอกเข้ามาติดต่อต้องมีหนังสือแจ้งจากหน่วยงานที่เกี่ยวข้องหรือแจ้งผ่านไปรษณีย์อิเล็กทรอนิกส์หรือช่องทางสื่อสารอื่น ๆ และลงชื่อขออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกให้ถูกต้องและจะต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

(๕) บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

ข้อ ๓ ประกาศห้ามผู้ที่ไม่เกี่ยวข้องเข้าห้องควบคุมระบบคอมพิวเตอร์ เว้นแต่ได้รับอนุญาตให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว แบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) เป็นต้น

ส่วนที่ ๒ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒.๑ แนวปฏิบัติการกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

ข้อ ๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

ข้อ ๒ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่ใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

ข้อ ๓ ในการเข้าใช้ระบบปฏิบัติการต้องลงบันทึกเข้าใช้งาน (Login) โดยการใส่ Username และ Password ทุกครั้ง

ข้อ ๔ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ขององค์การร่วมกัน

ข้อ ๕ ผู้ใช้งานต้องลงบันทึกออกจากระบบ (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

ข้อ ๖ ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๗ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๘ ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไขหรือทำสำเนาซอฟต์แวร์ที่องค์การจัดเตรียมไว้ให้ผู้ใช้งาน เพื่อนำไปใช้งานที่อื่น

ข้อ ๙ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นขององค์การ เพื่อประโยชน์ทางการค้า

ข้อ ๑๐ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความ รูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๑๑ ห้ามผู้ใช้งานใช้ระบบสารสนเทศขององค์การ เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๒.๒ แนวปฏิบัติการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ข้อ ๑ ผู้ดูแลระบบต้องตั้งค่าระบบปฏิบัติการให้เชื่อมต่อเครือข่ายภายในแบบ Domain เพื่อให้ผู้ใช้ต้องใส่บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ทุกครั้งในการเข้าระบบ

ข้อ ๒ ผู้ใช้งานต้องระบุและยืนยันตัวตนทุกครั้งในการเข้าระบบปฏิบัติการตามบัญชีผู้ใช้งานและรหัสผ่านที่กำหนดเพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้ระบบปฏิบัติการ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไขทันที

ข้อ ๓ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งาน ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

ข้อ ๔ ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้งานไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอนจำหน่ายหรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๕ ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้งานของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๒.๓ แนวปฏิบัติการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

ข้อ ๑ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมอรรถประโยชน์ ระดับสิทธิของผู้ขออนุมัติและการระบุและพิสูจน์ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

ข้อ ๒ ต้องจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน

ข้อ ๓ ต้องจำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์

ข้อ ๔ กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

ข้อ ๕ ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมอรรถประโยชน์

ข้อ ๖ กำหนดให้ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

ข้อ ๗ ต้องยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

ข้อ ๘ อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือใช้งาน เฉพาะโปรแกรมหรือซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องเท่านั้น ห้ามมิให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ละเมิดลิขสิทธิ์

๒.๔ แนวปฏิบัติการหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)

ข้อ ๑ กำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงาน อุปกรณ์เครือข่าย ต้องตัดและหมดเวลาการใช้งาน หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา ๓๐ นาที

ข้อ ๒ กำหนดให้ระบบเทคโนโลยีสารสนเทศทำการพักหน้าจอหลังจากที่ไม่มีกิจกรรรมการใช้งานช่วงระยะเวลา ๓๐ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

ส่วนที่ ๓ การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์การ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การได้อย่างถูกต้อง

๓.๑ แนวปฏิบัติกระบวนการหลักในการควบคุมการเข้าถึงระบบ

ข้อ ๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่สำคัญต้องควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

ข้อ ๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูล ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งต้องทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ข้อ ๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

ข้อ ๔ ผู้ดูแลระบบต้องบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๓.๒ แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ(ครั้งแรก)ให้แก่ผู้ใช้ ในการขออนุญาตเข้าระบบงานนั้นจะต้องทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ และกำหนดให้ต้องลงนามอนุมัติเอกสารดังกล่าว และต้องจัดเก็บไว้เป็นหลักฐาน

ข้อ ๒ เจ้าของข้อมูลและ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยง ในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตาม ความจำเป็นขั้นต่ำเท่านั้น

ข้อ ๓ ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๓ แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้

ข้อ ๑ การลงทะเบียนเจ้าหน้าที่ใหม่ขององค์การต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไปต้องทำภายใน ๒๔ ชั่วโมงหรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์การต้องทำภายใน ๓ วัน

ข้อ ๒ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้ง ต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อ ๓ ผู้ใช้งานต้องลงนามรับทราบสิทธิ และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

ข้อ ๔ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

(๑) ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

(๒) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิสูงสุด ต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยพิจารณาดังนี้

(๒.๑) ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

(๒.๒) ต้องควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ต้องควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๒.๓) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้น ระยะเวลาดังกล่าว

(๒.๔) ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน

๓.๔ แนวปฏิบัติการกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๑ ข้อกำหนดเกี่ยวกับประเภทของข้อมูล แบ่งได้ดังนี้

(๑) ข้อมูลสารสนเทศด้านการบริหารจัดการและปฏิบัติงานภายใน (ข้อมูลสำคัญ)

(๑.๑) ข้อมูลบุคลากร

(๑.๒) ข้อมูลด้านงบประมาณ การเงินและบัญชี

(๑.๓) ข้อมูลพัสดุ ครุภัณฑ์ การจัดซื้อจัดจ้าง

(๑.๔) ข้อมูลกฎ ระเบียบ ข้อบังคับ

(๑.๕) ข้อมูลการติดต่อสื่อสารภายในองค์การ

(๑.๖) ข้อมูลการติดตามการใช้จ่ายงบประมาณ

(๑.๗) ข้อมูลการรายงานผลการปฏิบัติงาน

(๒) ข้อมูลสารสนเทศเกี่ยวกับองค์การ และการให้บริการ (ข้อมูลทั่วไป)

(๒.๑) นโยบาย และยุทธศาสตร์องค์การ

(๒.๒) ข้อมูลคำรับรองการปฏิบัติราชการ

(๒.๓) ข้อมูลการดำเนินงานตามภารกิจขององค์การ

ข้อ ๒ การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

(๑) กำหนดชั้นความลับตามความสำคัญของข้อมูลในเอกสารที่มีความสำคัญ กำหนดไว้ ๓ ระดับ คือ ลับ ลับมาก ลับที่สุด

(๒) ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

(๓) เจ้าของข้อมูลจะต้องตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๔) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๕) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

(๖) ต้องกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

ข้อ ๓ เวลาที่ได้เข้าถึง

(๑) การเข้าถึงสารสนเทศในเวลาปฏิบัติงาน (๐๗.๓๐-๑๗.๓๐ น.)

(๒) การเข้าถึงสารสนเทศนอกเวลาปฏิบัติงาน (นอกช่วงเวลา ๐๗.๓๐-๑๗.๓๐ น.)

(๓) การเข้าถึงสารสนเทศในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนักขัตฤกษ์)

ข้อ ๔ ช่องทางการเข้าถึง

(๑) ระบบเครือข่ายสื่อสารภายในองค์การ (Local Area Network)

(๒) ระบบเครือข่ายสื่อสารภายนอกองค์การ (Internet)

ส่วนที่ ๔ การควบคุมการเข้าถึงและการใช้บริการระบบเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหาย ต่อข้อมูลและระบบสารสนเทศขององค์การ โดยกำหนดนโยบายและแนวปฏิบัติควบคุมการเข้าใช้งานเครือข่ายที่ แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายเป็นระบบเครือข่ายเสมือน Virtual Local Area Network (VLAN)

๔.๑ แนวปฏิบัติการควบคุมการเข้าถึงและการใช้บริการระบบเครือข่าย

ข้อ ๑ การใช้งานบริการเครือข่าย

(๑) ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชนโดยผู้ใช้งานรับรองว่าหากกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบขององค์การ

(๒) องค์การไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การซื้อหรือการจำหน่ายสินค้าการนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

(๓) กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๔) ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว องค์การไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

(๕) ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางองค์การ

(๖) องค์การให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

(๗) บัญชีผู้ใช้งาน (User Account) ที่องค์การให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

(๘) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

(๙) ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง ในระหว่างปฏิบัติงาน ยกเว้นเป็นการใช้เพื่อปฏิบัติงานขององค์การ

ข้อ ๒ ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่องค์การมีแนวทางปฏิบัติดังนี้

(๑) ผู้ดูแลระบบห้องควบคุมระบบเครือข่ายต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและต้องบันทึก "ทะเบียนผู้มีสิทธิเข้าออกพื้นที่" เช่น เจ้าหน้าที่เทคโนโลยีสารสนเทศ ผู้ดูแลระบบ เป็นต้น

(๒) สิทธิในการเข้าออกภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

(๓) ต้องจัดทำระบบเก็บบันทึกการเข้าออกตามกระบวนการที่ระบุไว้ในเอกสาร "แบบฟอร์มการเข้าออกพื้นที่"

(๔) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายก็ต้องควบคุมอย่างรัดกุม

(๕) การเข้าถึงห้องควบคุมระบบเครือข่ายต้องลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร "แบบฟอร์มการเข้าออกพื้นที่"

ข้อ ๓ ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติดังนี้

(๑) ผู้ติดต่อจากหน่วยงานภายนอกที่จะเข้าใช้งานระบบเครือข่ายต้องแจ้งความประสงค์พร้อมลงทะเบียนผู้ใช้ด้วยชื่อนามสกุลจริงและหมายเลขบัตรประชาชนทุกครั้ง

(๒) ผู้ติดต่อจากหน่วยงานภายนอกจะต้องแสดงตัวตน (Identification) ด้วยชื่อบัญชีผู้ใช้งาน (Username) ทุกครั้ง

(๓) ให้ตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงด้วยการใช้รหัสผ่าน (Password)

(๔) ต้องบันทึกข้อมูลการใช้งานระบบเครือข่ายและตรวจสอบผู้ใช้งานเมื่อเข้าสู่ระบบสารสนเทศขององค์การจากอินเทอร์เน็ต

ข้อ ๔ การระบุอุปกรณ์บนเครือข่าย

(๑) ผู้ดูแลระบบต้องเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ และรายชื่อบัญชีผู้ใช้งาน (Username)

(๒) กรณีอุปกรณ์ที่เชื่อมต่อจากเครือข่ายภายนอก ต้องระบุ IP Address ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

(๓) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

(๔) ผู้ขอใช้บริการเชื่อมต่ออุปกรณ์ส่วนตัวอื่น ๆ กับเครือข่ายขององค์การ ต้องกรอกแบบฟอร์ม "ขอใช้ Hot Spot"

ข้อ ๕ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

(๑) ผู้ดูแลระบบต้องกำหนดการเปิดปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่ก่อให้เกิดความเสียหายต่อระบบเครือข่าย

(๒) บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องควบคุมระบบคอมพิวเตอร์จะต้องลงชื่ออนุญาตการเข้าออกใน “แบบฟอร์มการเข้าออกพื้นที่” ให้ถูกต้องและได้รับการอนุมัติจากผู้บังคับบัญชาก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

(๓) บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาก่อน

(๔) ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๕) ต้องตรวจสอบพอร์ตที่ไม่ได้ใช้งานและให้ทำการปิด

ข้อ ๖ การแบ่งแยกเครือข่าย

(๑) องค์การแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามสิทธิของผู้ใช้งานเพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาตดังนี้ เครือข่ายสำหรับกลุ่มผู้ใช้งานภายใน เครือข่ายสำหรับกลุ่มบุคคลภายนอก เครือข่ายสำหรับกลุ่มงานเทคโนโลยีสารสนเทศ

(๒) องค์การจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ โดยผู้ใช้งานสามารถใช้งานระบบสารสนเทศผ่านระบบเครือข่ายภายในและเชื่อมต่อไปเครือข่ายภายนอกตามที่กำหนดได้ เพื่อความปลอดภัยของฐานข้อมูล

(๓) องค์การต้องติดตั้งอุปกรณ์ Firewall เพื่อป้องกันทางเข้าเครือข่ายขององค์การจากผู้ไม่หวังดี

ข้อ ๗ การควบคุมการเชื่อมต่อทางเครือข่าย

(๑) ต้องตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

(๓) ระบุหมายเลข IP Address และชนิดของอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ควบคุมไม่ให้เปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

ข้อ ๘ การควบคุมการจัดเส้นทางบนเครือข่าย

(๑) ควบคุมไม่ให้เปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

(๒) กำหนดให้แปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

ส่วนที่ ๕ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์การ โดยการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งต้องทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๕.๑ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ข้อ ๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์การ หากเป็นอุปกรณ์ขององค์การ ผู้ดูแลระบบจะทำการลงทะเบียนให้ตามสิทธิ ถ้าเป็นอุปกรณ์ส่วนตัวจะต้องทำการลงทะเบียนกับผู้ดูแลระบบ

ข้อ ๒ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนการเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งต้องทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

ข้อ ๓ ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

ข้อ ๔ ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตี สามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

ข้อ ๕ ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและต้องสำรวจว่า สัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

ข้อ ๖ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าตั้งต้น (Default) มาจากผู้ผลิต ทันทีที่นำ AP มาใช้งาน

ข้อ ๗ ผู้ดูแลระบบต้องเปลี่ยนค่า ชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบ ต้องเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

ข้อ ๘ ผู้ดูแลระบบต้องกำหนดค่าใช้ WPA WPA๒ หรือดีกว่าในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

ข้อ ๙ ผู้ดูแลระบบต้องติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายใน

ข้อ ๑๐ ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application Information Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศขององค์การ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหาย แก่ ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงักและทำให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ ได้อย่างถูกต้อง

๖.๑ แนวปฏิบัติการจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

ข้อ ๑ ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ขององค์การ โดยกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้ง ขั้นตอนปฏิบัติ สำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๒ ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญคือระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบอินเทอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wireless LAN) โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มี การใช้งานระบบสารสนเทศเกินกว่า ๓๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องลงบันทึกเข้าระบบ (Login) อีกครั้ง

ข้อ ๔ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน ของ บุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

(๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-Mail) ที่ไม่ได้ป้องกันในการส่งรหัสผ่าน (Password)

(๓) กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(๔) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ ในรูปแบบที่ ไม่ได้ป้องกันการเข้าถึง

(๕) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความ เห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยต้องกำหนดระยะเวลาการใช้งานและระงับการใช้ งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และต้องกำหนดสิทธิพิเศษที่ได้รับว่า เข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๕ ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่าน ระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

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

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน การส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

ข้อ ๖ การควบคุมการเข้าถึงสารสนเทศของหน่วยงานภายนอก

(๑) หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าถึงสารสนเทศขององค์การ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้บังคับบัญชา

(๒) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

(๒.๑) เหตุผลในการขอใช้

(๒.๒) ระยะเวลาในการใช้

(๒.๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๒.๔) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

(๓) หน่วยงานภายนอกที่ทำงานให้กับองค์การทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์การหรือนอกสถานที่จำเป็นต้องลงนามในสัญญา ไม่เปิดเผยข้อมูลขององค์การ โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

(๔) เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่ต้องเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๖.๒ แนวปฏิบัติการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

ข้อ ๑ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น

ข้อ ๒ ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศซึ่งเป็นระบบงานที่มีความสำคัญสูง ระบบงานที่ต้องใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกองค์การ) ต้องจำกัดช่วงระยะเวลาการเชื่อมต่อ

๖.๓ แนวปฏิบัติการจัดการกับระบบซึ่งไวต่อการรบกวน

ข้อ ๑ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์การ ได้แก่ ระบบ GFMIS หรือระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ เป็นระบบที่ใช้ในการปฏิบัติงานด้านการงบประมาณ การบัญชี การจัดซื้อจัดจ้าง การเบิกจ่าย และการบริหารทรัพยากร ซึ่งดูแลรับผิดชอบโดยกรมบัญชีกลางจะได้รับการแยกออกจากระบบงานอื่น ๆ ขององค์การ

ข้อ ๒ ระบบซึ่งไวต่อการรบกวน ต้องควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ และต้องกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น

ข้อ ๓ ต้องควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกองค์การ (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๖.๔ แนวปฏิบัติการปฏิบัติงานจากภายนอกองค์การ (Teleworking)

ข้อ ๑ ต้องกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์การ

ข้อ ๒ ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบสารสนเทศขององค์การในสถานที่ดังกล่าว

ข้อ ๓ ต้องตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศขององค์การจากระยะไกลต้องป้องกันไวรัสและการใช้งาน Firewall ตามที่องค์การต้องการ

ข้อ ๔ ต้องจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

ข้อ ๕ องค์การต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่าง ๆ ขององค์การที่อนุญาตให้เข้าถึงได้จากระยะไกล

ข้อ ๖ องค์การต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกลการกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อยกเลิกการปฏิบัติงาน

๖.๕ แนวปฏิบัติข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

ข้อ ๑ กำหนดให้ต้องควบคุมการเข้าถึงสารสนเทศ โดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

ข้อ ๒ ต้องปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ส่วนที่ ๗ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการ การเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ

๗.๑ การลงทะเบียนผู้ใช้งาน (User Registration)

ข้อ ๑ จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบเทคโนโลยีสารสนเทศขององค์การ

ข้อ ๒ ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยต้องไม่ลงทะเบียนผู้ใช้งานมาก่อน

ข้อ ๓ ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

ข้อ ๔ ผู้ดูแลระบบต้องกำหนดให้แจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้ง กำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

ข้อ ๕ ผู้ดูแลระบบต้องกำหนดให้ถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกต้องทำภายใน ๒๔ ชั่วโมงหรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์การต้องทำภายใน ๓ วัน

ข้อ ๖ การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๗.๒ แนวปฏิบัติการบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

ข้อ ๑ ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อ ๒ ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศ

ข้อ ๓ ผู้ดูแลระบบต้องมอบหมายสิทธิให้มีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

ข้อ ๔ ผู้ดูแลระบบต้องจัดเก็บเอกสารการมอบหมายสิทธิให้แก่ผู้ใช้งาน

ข้อ ๕ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และต้องกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๗.๓ แนวปฏิบัติระบบบริหารจัดการรหัสผ่าน (Password Management System)

ข้อ ๑ ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ต้องใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

ข้อ ๒ ระบบบริหารจัดการรหัสผ่านต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเองและมีขั้นตอนปฏิบัติ เพื่อยืนยันรหัสผ่านใหม่

ข้อ ๓ ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเลือกรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

ข้อ ๔ ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้อย่างน้อยทุก ๆ ๖ เดือน

ข้อ ๕ ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชีผู้ใช้งานหรือหลังทำการบันทึกเข้าใช้งานระบบเป็นครั้งแรก

ข้อ ๖ ระบบบริหารจัดการรหัสผ่านต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน

ข้อ ๗ ระบบบริหารจัดการรหัสผ่านต้องป้องกันรหัสผ่านที่ได้จัดเก็บไว้หรือที่จำเป็นต้องส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๗.๔ แนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

ข้อ ๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

ข้อ ๒ ผู้ดูแลระบบต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านที่มีความยากต่อการเดาโดยผู้อื่น

ข้อ ๓ ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและต้องกำหนดรหัสผ่านที่แตกต่างกัน

ข้อ ๔ ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่งและกำหนดให้ผู้ใช้งานตอบกลับหลังจากที่ได้รับรหัสผ่านแล้ว

๗.๕ แนวปฏิบัติการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Rights)

ข้อ ๑ ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ๑ ครั้ง / ปี เป็นอย่างน้อย

ข้อ ๒ ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิในระดับสูง สิทธิในระดับผู้ดูแลระบบด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

ข้อ ๓ ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อเปลี่ยนแปลง การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงานหรือสิ้นสุดการจ้างงาน

ข้อ ๔ ผู้ดูแลระบบต้องกำหนดให้บันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

ส่วนที่ ๘ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา การนำไปปฏิบัติงานภายนอกองค์การ เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ให้เกิดความปลอดภัย การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศขององค์การ เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๘.๑ แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer)

ข้อ ๑ เครื่องคอมพิวเตอร์ที่องค์การอนุญาตให้ผู้ใช้งานใช้เป็นทรัพย์สินขององค์การ ดังนั้น ผู้ใช้งานต้องใช้เครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์การ

ข้อ ๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์การ เป็นโปรแกรมที่องค์การได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

ข้อ ๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์การ

ข้อ ๔ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคลจะต้องกำหนดโดยผู้ดูแลระบบหรือเจ้าหน้าที่เทคโนโลยีสารสนเทศขององค์การเท่านั้น

ข้อ ๕ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยผู้ดูแลระบบหรือเจ้าหน้าที่เทคโนโลยีสารสนเทศขององค์การเท่านั้น

ข้อ ๖ ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์ส่วนบุคคล และรักษาสภาพของเครื่องให้มีสภาพเดิม

ข้อ ๗ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสที่องค์การจัดหาให้

ข้อ ๘ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบในการเก็บและสำรองข้อมูลจากเครื่องคอมพิวเตอร์ส่วนบุคคลดังนี้

(๑) ต้องเก็บข้อมูลสำคัญขององค์การไว้บนพื้นที่จัดเก็บหรือระบบที่องค์การจัดหาให้เพิ่มเติมจากเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

(๒) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ ได้แก่ CD, DVD, External Hard Disk เป็นต้น

(๓) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๔) ผู้ใช้ต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์การ

ข้อ ๙ ต้องไม่สร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์การ

ข้อ ๑๐ ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยต้องปฏิบัติ ดังนี้

(๑) ต้องไม่นำอาหารหรือเครื่องดื่มวางอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

(๒) ต้องไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๘.๒ แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ข้อ ๑ เครื่องคอมพิวเตอร์แบบพกพาที่องค์การอนุญาตให้ผู้ใช้งานใช้เป็นทรัพย์สินขององค์การ ดังนั้น ผู้ใช้งานต้องใช้เครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์การ

ข้อ ๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์การ เป็นโปรแกรมที่องค์การได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

ข้อ ๓ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์แบบพกพาขององค์การ

ข้อ ๔ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) แบบพกพาจะต้องกำหนดโดยผู้ดูแลระบบหรือเจ้าหน้าที่เทคโนโลยีสารสนเทศขององค์การเท่านั้น

ข้อ ๕ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยผู้ดูแลระบบหรือเจ้าหน้าที่เทคโนโลยีสารสนเทศขององค์การเท่านั้น

ข้อ ๖ ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์แบบพกพาและรักษาสภาพของเครื่องให้มีสภาพเดิม

ข้อ ๗ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน การตกจากโต๊ะทำงานหรือหลุดมือ

ข้อ ๘ ต้องไม่ใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจ จากการมีของหนักทับบนเครื่องหรืออาจถูกจับโยนได้

ข้อ ๙ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

ข้อ ๑๐ หลีกเลี่ยงการใช้ของแข็งกดสัมผัสหน้าจอให้เป็นรอยขีดข่วนหรือทำให้หน้าจอของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

ข้อ ๑๑ ห้ามวางของทับบนหน้าจอและแป้นพิมพ์

ข้อ ๑๒ การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามเคลื่อนย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

ข้อ ๑๓ ห้ามเคลื่อนย้ายเครื่องในขณะที่ Hard Disk Drive กำลังทำงาน ให้ยกเว้นกรณีเป็นชนิด Solid State Drive

ข้อ ๑๔ ห้ามใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น ได้แก่ อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ

ข้อ ๑๕ ไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

ข้อ ๑๖ ห้ามวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ ได้แก่ แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น

ข้อ ๑๗ ห้ามใช้คอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือนหรือในยานพาหนะที่กำลัง เคลื่อนที่

ข้อ ๑๘ การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

ข้อ ๑๙ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๘.๓ แนวปฏิบัติการใช้งานรหัสผ่าน (Password Use)

ผู้ใช้งานระบบเทคโนโลยีสารสนเทศต้องปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

ข้อ ๑ ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

ข้อ ๒ ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

ข้อ ๓ ผู้ใช้งานต้องจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

ข้อ ๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือมีผู้อื่นล่วงรู้

ข้อ ๕ ผู้ใช้งานต้องตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำที่กำหนดไว้ไม่น้อยกว่า ๘ หลัก

ข้อ ๖ ผู้ใช้งานต้องตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

ข้อ ๗ ผู้ใช้งานต้องไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

ข้อ ๘ ผู้ใช้งานต้องหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน ได้แก่ ๑๒๓ , abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน ๑๑๑ , aaa

ข้อ ๙ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

ข้อ ๑๐ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

ข้อ ๑๑ ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไปคือทุก ๆ ๓ เดือน สำหรับผู้ดูแลระบบ และ ทุก ๆ ๖ เดือน สำหรับผู้ใช้งาน

ข้อ ๑๒ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวโดยทันทีที่ทำการบันทึกเข้าสู่ระบบงานครั้งแรก

ข้อ ๑๓ ผู้ใช้งานต้องไม่กำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการบันทึกเข้าในภายหลัง

ข้อ ๑๔ ผู้ใช้งานต้องไม่ใช้รหัสผ่านของตนร่วมกับผู้อื่น

๘.๔ แนวปฏิบัติการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

ข้อ ๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน จากระบบงาน เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แบบพกพาที่ใช้งาน

ข้อ ๒ ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน

ข้อ ๓ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

ข้อ ๔ ผู้ดูแลระบบต้องกำหนดให้เครื่องคอมพิวเตอร์ทำการพักหน้าจอหลังจากที่ไม่มีกิจกรรรมการใช้งานช่วงระยะเวลา ๓๐ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

๘.๕ แนวปฏิบัติการควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

ข้อ ๑ ต้องกำหนดรหัสผ่านการเข้าใช้งานเครื่องคอมพิวเตอร์ และผู้ใช้งานควรกำหนดรหัสผ่านให้กับเอกสารแนบในการส่งจดหมายอิเล็กทรอนิกส์ (e-Mail) ที่เป็นความลับ

ข้อ ๒ การควบคุมสินทรัพย์สารสนเทศ ทางด้านกายภาพ โดยนำสินทรัพย์สารสนเทศที่มีความสำคัญมาก จัดเก็บรักษาไว้ในห้องควบคุมระบบ ที่มีระบบรักษาความปลอดภัย โดยในการเข้าออกห้องทุกครั้งจะต้องล็อคกุญแจหรือจัดให้มี Door Access Control ด้วยการสแกนลายนิ้วมือ หรือ รหัสผ่าน โดยอนุญาตเฉพาะผู้ที่มีสิทธิ์ในการเข้าถึง

ข้อ ๓ การควบคุมการเข้าถึงสินทรัพย์สารสนเทศ ทางด้านกายภาพโดยการล็อคกุญแจตู้ที่เก็บรักษาสินทรัพย์ และอนุญาตให้เฉพาะผู้มีหน้าที่เกี่ยวข้องเก็บรักษาลูกกุญแจไว้ โดยในการนำสินทรัพย์สารสนเทศออกมาใช้งานทุกครั้งจะมีการทำเอกสารขอใช้งานเป็นลายลักษณ์อักษร และได้รับอนุญาตโดยผู้มีอำนาจ จากนั้นจึงมีการเก็บบันทึกไว้ในแฟ้มหรือในระบบ

ข้อ ๔ การควบคุมการเข้าถึงสินทรัพย์สารสนเทศและการเข้าถึงระบบงานสานสนเทศ โดยการจำกัดสิทธิผู้ใช้งานที่สามารถบันทึกเข้ามาใช้งานเฉพาะบุคคลที่มีความเกี่ยวข้องกับสินทรัพย์สารสนเทศดังกล่าว และเมื่อไม่มีการเรียกใช้งานในเวลาที่กำหนด ระบบจะทำการบันทึกออกจากระบบโดยอัตโนมัติ

ข้อ ๕ การป้องกันสินทรัพย์สารสนเทศที่สำคัญและการเข้าถึงระบบงานสารสนเทศ ต้องมีความสอดคล้องกับวัฒนธรรมของหน่วยงานในการป้องกันสินทรัพย์ ได้แก่ วัฒนธรรมการปฏิบัติตามนโยบาย ๕ ส. ซึ่งจะกำหนดให้มีการจัดการกับเอกสารสำคัญอย่างเหมาะสม ได้แก่ การจัดใส่ไว้ในตู้และมีกุญแจล็อค การแยกเอกสารสำคัญไว้สำหรับทำลายต่างหาก

ข้อ ๖ ต้องทำการทำลายข้อมูลที่บันทึกอยู่ใน Hard Disk หรือสื่อบันทึกข้อมูล ก่อนทำการทำลายหรือจำหน่าย

ข้อ ๗ ต้องทำการฟอร์แมต Hard Disk เพื่อป้องกันการกู้คืนข้อมูลใน Hard Disk โดยการใช้วิธีแบบเขียนทับซ้ำจำนวน ๑ ครั้ง ตามมาตรฐาน NIST ๘๐๐-๘๘ สำหรับข้อมูลที่มีความลับระดับต่ำหรือแบบเขียนทับซ้ำจำนวน ๓ ครั้ง ตามมาตรฐาน DoD ๕๒๒๐.๒๒-M สำหรับข้อมูลที่มีความลับระดับปานกลางหรือแบบเขียนทับซ้ำจำนวน ๗ ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลที่มีความลับระดับสูง

ข้อ ๘ ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายสื่อบันทึกข้อมูลหรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

๘.๖ แนวปฏิบัติผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

ข้อ ๑ ผู้ใช้งานต้องทำการเข้ารหัสข้อมูล (Encryption) ที่เป็นมาตรฐานสากล เมื่อมีการรับส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับผ่านทางเครือข่ายสาธารณะ

ข้อ ๒ การส่งข้อมูลหรือเอกสารที่เป็นความลับให้ผู้ส่งต้องตั้งรหัสผ่านให้กับเอกสารแนบในการส่งจดหมายอิเล็กทรอนิกส์ (e-Mail) ที่เป็นความลับ เพื่อป้องกันไม่ให้ผู้ที่ไม่เกี่ยวข้องหรือไม่มีสิทธิ์อ่านหรือล่วงรู้ความลับได้

ส่วนที่ ๙ การใช้งานอินเทอร์เน็ต (Use of the Internet)

วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และ เป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ พ.ศ. ๒๕๖๐ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์การถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

ข้อ ๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์การจัดสรรไว้เท่านั้น ได้แก่ Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็น

ข้อ ๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์

ข้อ ๓ การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางระบบอินเทอร์เน็ตจะต้องสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๔ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์การ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

ข้อ ๕ ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์การ

ข้อ ๖ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ละเมิดสิทธิของผู้อื่น และข้อมูลที่อาจก่อความเสียหายให้กับองค์การ

ข้อ ๗ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์การ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

ข้อ ๘ ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้ายหรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

ข้อ ๙ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย

ข้อ ๑๐ ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

ข้อ ๑๑ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ การดาวน์โหลดทุกประเภทต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญา

ข้อ ๑๒ ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์การ รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

ข้อ ๑๓ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ ๑๐ การใช้งานสื่อโซเชียลมีเดีย (Social Media)

วัตถุประสงค์

เพื่อกำหนดขอบเขตในการใช้สื่อโซเชียลมีเดีย กำหนดมาตรฐานแนวทางปฏิบัติของผู้ใช้งานภายในองค์การ ให้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลในการใช้ประโยชน์จากเครือข่ายสื่อโซเชียลมีเดีย ซึ่งเป็นหน้าที่ของผู้บริหาร ผู้ปฏิบัติงาน และผู้ใช้งานที่ต้องปฏิบัติตามอย่างเคร่งครัด ให้เป็นไปอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด เพื่อลดความเสี่ยงหรือหลีกเลี่ยงปัญหาอันอาจจะเกิดขึ้นจากการใช้สื่อโซเชียลมีเดียที่ก่อให้เกิดความเสียหายต่อตนเอง ต่อผู้อื่น และต่อองค์การ

แนวทางปฏิบัติสำหรับผู้ที่ใช้สื่อโซเชียลมีเดีย (Social Media)

ข้อ ๑ พึงตระหนักว่า ข้อความหรือความเห็นที่เผยแพร่บน Social Media เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบ ทั้งทางด้านสังคม และด้านกฎหมาย นอกจากนี้ ยังอาจมีผลกระทบต่อชื่อเสียง การทำงานและอนาคตของวิชาชีพของตนได้

ข้อ ๒ ใช้ความระมัดระวังอย่างยิ่ง ในการเผยแพร่ความคิดเห็นที่อาจกระตุ้นหรือนำไปสู่การโต้แย้งที่รุนแรง เช่น เรื่องเกี่ยวกับการเมืองหรือศาสนา

ข้อ ๓ ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

ข้อ ๔ พึงตระหนักว่า การใช้ Social Media นั้น การแบ่งแยกระหว่างเรื่องส่วนตัว และเรื่องหน้าที่การงานเป็นสิ่งที่ทำได้ยาก หากประสงค์จะใช้ Social Media เพื่อเผยแพร่ข้อมูลเกี่ยวกับเรื่องหน้าที่การงานหรือข้อมูลเกี่ยวกับหน่วยงาน ควรแยกบัญชีผู้ใช้ (Account) ระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่การงานออกจากกัน ยกตัวอย่างเช่น การใช้ Facebook ของผู้ที่ทำหน้าที่ประชาสัมพันธ์ของส่วนงาน ควรมีการแยก Facebook Profile ที่ใช้สำหรับติดต่อกับเครือข่ายของตนในเรื่องส่วนตัว เรื่องครอบครัว ออกจาก Facebook Profile ที่ใช้ประชาสัมพันธ์ส่วนงาน หรืออาจตั้งเป็น Facebook Page ประจำส่วนงานขึ้นแทนที่จะใช้ Profile ส่วนตัว

ข้อ ๕ หากต้องการสร้าง Page หรือ Account ที่เป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการขององค์การ ต้องแจ้งรายชื่อของผู้ดูแล Page (Admin) หรือเจ้าของ Account นั้นให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรืองานสื่อสารองค์กรรับทราบ และผู้ดูแลมีหน้าที่ต้องมอบสิทธิ์ในการดูแล Page หรือ Account นั้นคืนแก่ส่วนงานหรือองค์การเมื่อพ้นจากหน้าที่ที่ต้องดูแล หรือพ้นสภาพจากการเป็นบุคลากรขององค์การ

ข้อ ๖ การเผยแพร่ข้อมูล หรือแสดงความเห็นที่อาจทำให้เข้าใจว่าเป็นความเห็นขององค์การต้องมีการแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่า เป็นความเห็นส่วนตัว มิใช่ความเห็นขององค์การ เว้นแต่จะเป็นความเห็นขององค์การอย่างแท้จริง หรือได้รับอนุญาตจากผู้มีอำนาจที่เกี่ยวข้องแล้ว

ข้อ ๗ ผู้บริหาร พึงระมัดระวังในการเผยแพร่ข้อมูล หรือการแสดงความเห็นเนื่องจากจะถูกมองว่าเป็นความเห็นของส่วนงานของตนได้ง่าย และอาจมีผลกระทบต่อความเข้าใจของผู้ปฏิบัติงานได้ ทั้งนี้ ให้มีการแสดงข้อความจำกัดความรับผิดชอบอย่างชัดเจนเช่นเดียวกับข้อ ๖

ข้อ ๘ ห้ามเผยแพร่ข้อมูลที่เป็นทรัพย์สินขององค์การ หรือข้อมูลที่ใช้ภายในองค์การ ก่อนได้รับอนุญาตอย่างเป็นทางการจากผู้มีอำนาจ

ข้อ ๙ ผู้บริหารและผู้ปฏิบัติงานขององค์การ อาจใช้ตราสัญลักษณ์ (Logo) ขององค์การบนรูปประกอบ Profile ของตนได้ หาก Profile นั้นระบุชื่อและนามสกุลจริงอย่างถูกต้อง แต่หากจะใช้เพื่อโฆษณาประชาสัมพันธ์ สินค้า ผลิตภัณฑ์ หรือการบริการใด ๆ จะต้องได้รับอนุญาตจากผู้มีอำนาจก่อน

ข้อ ๑๐ หากพบผู้ใช้งานขององค์การ ใช้ Social Media อย่างไม่เหมาะสม ขอให้ตักเตือนโดยตรง หากไม่ได้รับการตอบสนองที่ดี ให้แจ้งต่อผู้บังคับบัญชาของผู้นั้นรับทราบ

ข้อ ๑๑ ควรแจ้งให้ผู้บังคับบัญชาทราบ หากพบว่ามีข้อความบน Social Media ที่อาจทำให้เกิดความเสื่อมเสียชื่อเสียงขององค์การ หรือกระทบกับความสัมพันธ์กับเพื่อนร่วมงาน

ข้อ ๑๒ ศึกษาการใช้ “การตั้งค่าความเป็นส่วนตัว” หรือ “Privacy Settings” ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับบริบท การถูกละเมิดความเป็นส่วนตัวโดยไม่เหมาะสมนอกเหนือจากส่งผลกระทบต่อตนเองแล้ว อาจส่งผลต่อองค์การได้ด้วย

ส่วนที่ ๑๑ การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์การ ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

ข้อ ๑ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงจดหมายอิเล็กทรอนิกส์ขององค์การ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งต้องทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

ข้อ ๒ ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่ และรหัสผ่าน สำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์การ

ข้อ ๓ รหัสผ่านจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษร

ข้อ ๔ ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ต้องบันทึกออกจากหน้าจอ และตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ ๓๐ นาที เมื่อต้องการเข้าใช้งานต้องให้ใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

ข้อ ๕ ผู้ใช้งานต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๖ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด ต้องเปลี่ยนรหัสผ่านทุก ๆ ๖ เดือน

ข้อ ๗ ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์การหรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์การ

ข้อ ๘ ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-Mail Address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

ข้อ ๙ ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์การ เพื่อการทำงานขององค์การเท่านั้น

ข้อ ๑๐ ผู้ใช้งานห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ส่วนตัว ได้แก่ Hotmail Gmail Yahoo เป็นต้น ในการติดต่อสื่อสารเพื่อการปฏิบัติงานขององค์การ

ข้อ ๑๑ หลังจากการใช้งานจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการบันทึกออก (Logout) จากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

ข้อ ๑๒ ผู้ใช้งาน ต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file (.exe)

ข้อ ๑๓ ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๔ ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์การ ทำให้เกิดความแตกแยกระหว่างส่วนงานผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ ๑๕ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

ข้อ ๑๖ ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

ข้อ ๑๗ ผู้ใช้งานต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๑๘ ข้อควรระวัง ผู้ใช้งานต้องโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นต้องไม่จัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและการสำรองข้อมูล

ส่วนที่ ๑ การสำรองข้อมูล (Backup System)

วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการสำรองข้อมูล โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ ในกรณีที่จำเป็น

แนวปฏิบัติการคัดเลือกการสำรองข้อมูล

ข้อ ๑ ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดขององค์การ พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรองข้อมูล

ข้อ ๒ กำหนดให้ต้องสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

ข้อ ๓ กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมี ๓ ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) การสำรองข้อมูลแบบส่วนต่างล่าสุด (Incremental Backup) และการสำเนาข้อมูลระหว่างไซต์ (Off-Site Backup Replication)

ข้อ ๔ ผู้ดูแลระบบคอมพิวเตอร์ ต้องทำการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์การ

ข้อ ๕ การจัดทำบันทึกการสำรองข้อมูล (Backup Logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก

ข้อ ๖ มีขั้นตอนการปฏิบัติการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

ข้อ ๗ การรายงานข้อผิดพลาด (Fault Logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

ข้อ ๘ ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลให้กับเจ้าหน้าที่คนอื่น เพื่อช่วยสำรองข้อมูล ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

ข้อ ๙ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บังคับบัญชา

ข้อ ๑๐ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted Backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีรหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

ข้อ ๑๑ แนวทางที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

๑.๒ แนวปฏิบัติการสำรองข้อมูล

ข้อ ๑ ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการคัดเลือกระบบสารสนเทศที่มีความสำคัญต่อองค์การ เพื่อทำการสำรองข้อมูลแต่ละรายการและตามความถี่ ดังนี้

ลำดับ	รายการ	รูปแบบการสำรองข้อมูล	ความถี่ในการสำรองข้อมูล
๑	ระบบสารสนเทศและข้อมูลบนเครื่องแม่ข่ายที่ฝากไว้ที่ IDC (Primary Site) - ระบบ e-Office - ระบบจำหน่ายบัตรเข้าชม - ระบบ POS - ระบบ e-Mail - ระบบ Website	- Full Backup - Incremental Backup	ทุกวัน
๒	ระบบสารสนเทศและข้อมูลทุกระบบบนเครื่องแม่ข่ายที่ห้อง Server สำนักงานส่วนกลาง (Primary Site) - ระบบ Internet - ระบบ File Server	- Full Backup - Incremental Backup	ทุกวัน
๓	ทำสำเนาข้อมูลจาก IDC (Primary Site) ไปยัง Cloud Server (Secondary Site)	- Off-site Backup Replication	ทุกวัน
๔	ทำสำเนาข้อมูลจากห้อง Server สำนักงานส่วนกลาง (Primary Site) ไปยัง Cloud Server (Secondary Site)	- Off-site Backup Replication	ทุกวัน

ข้อ ๒ ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการสำรองข้อมูลตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

ส่วนที่ ๒ การกู้คืนระบบ (Recovery System)

วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติการกู้คืนระบบ โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ ในกรณีที่จำเป็น

แนวปฏิบัติการกู้คืนระบบ

ข้อ ๑ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงานต่อผู้บังคับบัญชา

ข้อ ๒ ให้ใช้ข้อมูลทันสมัยที่สุด (Lastest Update) ที่ได้สำรองไว้หรือข้อมูลที่สมบูรณ์ที่สุดตามความเหมาะสมเพื่อกู้คืนระบบ

ข้อ ๓ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

ข้อ ๔ ต้องดำเนินการซักซ้อมการกู้คืนระบบ อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี หรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

แนวปฏิบัติการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤติด้านเทคโนโลยีสารสนเทศ

ข้อ ๑ กำหนดกระบวนการในการวางแผนบริหารความต่อเนื่องในสภาวะวิกฤติสำหรับระบบที่มีความสำคัญสูง

ข้อ ๒ กำหนดชนิดของสภาวะวิกฤติที่มีผลกระทบต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

ข้อ ๓ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากสภาวะวิกฤติที่กำหนดไว้

ข้อ ๔ จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤติสำหรับระบบที่มีความสำคัญสูง

ข้อ ๕ ทดสอบ/ประเมินและปรับปรุงแผนบริหารความต่อเนื่องในสภาวะวิกฤติสำหรับระบบที่มีความสำคัญสูง อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๔ การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ
(Third party access control)

วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่ต้องการเข้าใช้งานระบบสารสนเทศขององค์การ เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบ การใช้บริการของผู้รับจ้าง การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

แนวทางปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

ข้อ ๑ กำหนดให้ต้องประเมินความเสี่ยงจากการเข้าถึงระบบสารสนเทศหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตราการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศได้

ข้อ ๒ การควบคุมการเข้าใช้งานระบบสารสนเทศของหน่วยงานภายนอก

(๑) หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศขององค์การจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้บังคับบัญชา

(๒) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

(๒.๑) เหตุผลในการขอใช้

(๒.๒) ระยะเวลาในการใช้

(๒.๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๒.๔) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

(๓) หน่วยงานภายนอกที่ทำงานให้กับองค์การทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์การหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาไม่เปิดเผยข้อมูลขององค์การ โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

(๔) เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่ต้องเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

(๕) สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์การ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

(๖) “องค์การ” มีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบสารสนเทศ เพื่อให้มั่นใจได้ว่า “องค์การ” สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

(๗) กำหนดให้ผู้ให้บริการหน่วยงานภายนอก จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งต้องปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบ การให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

(๘) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของหน่วยงานต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๙) การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

(๑๐) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้างานเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

(๑๑) ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอและต้องได้รับอนุญาตจากหัวหน้างานเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย

(๑๒) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่ควรเปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรจัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วและจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

หมวดที่ ๕ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Information Security Audit and Assessment)

วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติในการตรวจสอบ การประเมินความเสี่ยง และมาตรการในการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อความมั่นคงปลอดภัยในการให้บริการเทคโนโลยีสารสนเทศ และระบบงานคอมพิวเตอร์

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ ๑ กำหนดให้ต้องตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๒ ต้องตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบภายนอกองค์การ (External Auditor)

ข้อ ๓ ต้องกำหนดความรับผิดชอบของผู้ใช้งานหรือผู้บริหาร ให้ผู้ใช้งานและผู้บริหารรับผิดชอบในกรณีเกิดความเสียหายหรืออันตรายเนื่องมาจากผู้ใช้งานหรือผู้บริหารบกพร่องหรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศแล้วแต่กรณี

หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัย ของระบบเทคโนโลยีสารสนเทศ (Information Security Awareness Training)

วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้องได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑ จัดฝึกอบรมหรือให้ความรู้แนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ เช่น การจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน เป็นต้น

ข้อ ๒ ควรจัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาให้มีแผนการดำเนินงานอย่างน้อยปีละ ๑ ครั้ง ซึ่งอาจจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

ข้อ ๓ เผยแพร่ประกาศ ประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อพึงระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยต้องปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

ข้อ ๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

หมวดที่ ๗ การกำหนดแบ่งอำนาจหน้าที่ผู้รับผิดชอบ

วัตถุประสงค์

การกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์การหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แบ่งอำนาจหน้าที่มีวัตถุประสงค์เพื่อลดความเสี่ยงด้านโครงสร้างพื้นฐาน ซึ่งมีแนวทางปฏิบัติดังนี้ คือ ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ ในส่วนการพัฒนาระบบงานออกจากบุคลากรที่ทำหน้าที่บริหารระบบ ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริงและต้องระบุหน้าที่ความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคน ภายในงานเทคโนโลยีสารสนเทศ สำนักบริหารกลาง อย่างชัดเจนเป็นลายลักษณ์อักษร ซึ่งต้องจัดให้มีบุคลากรสำรองในงานที่มีความสำคัญ เพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น โดยกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ รายละเอียดดังนี้

แนวปฏิบัติ

ข้อที่ ๑ ระดับนโยบาย

(๑) รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์การหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ ได้แก่

- ผู้อำนวยการ อบน.

(๒) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา การตัดสินใจ ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

ผู้รับผิดชอบ ได้แก่

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง อบน.

ข้อที่ ๒ ระดับปฏิบัติ

(๑) รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ให้ความเห็น เสนอแนะวิธีการและแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยง ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยงและระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

ผู้รับผิดชอบ ได้แก่

ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ของ อบน.

(๒) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบเครื่องคอมพิวเตอร์ ห้องควบคุมระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ ระบบฐานข้อมูล ระบบเครือข่าย

มีหน้าที่รับผิดชอบ ดังนี้

(๒.๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศหมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ส่วนที่ ๑ การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์ ส่วนที่ ๒ การควบคุมการเข้าถึงระบบปฏิบัติการ ส่วนที่ ๓ การควบคุมการเข้าถึงและการใช้งานสารสนเทศ ส่วนที่ ๔ การควบคุมการเข้าถึงและการใช้บริการระบบเครือข่าย ส่วนที่ ๕ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

(๓) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย บำรุงรักษา ระบบเครื่องคอมพิวเตอร์ระบบเครือข่าย ให้คำปรึกษาแนะนำ รวมทั้งการสำรองข้อมูลและกู้คืนระบบ

มีหน้าที่รับผิดชอบ ดังนี้

(๓.๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศหมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ ส่วนที่ ๗ การบริหารจัดการการเข้าถึงของผู้ใช้งาน ส่วนที่ ๘ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน ส่วนที่ ๙ การใช้งานอินเทอร์เน็ต ส่วนที่ ๑๐ การใช้งานสื่อโซเชียลมีเดีย ส่วนที่ ๑๑ การใช้งานจดหมายอิเล็กทรอนิกส์ หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและการสำรองข้อมูล ส่วนที่ ๑ การสำรองข้อมูล ส่วนที่ ๒ การกู้คืนระบบ หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

(๓.๒) ประสานการปฏิบัติงานตามแผนบริหารความพร้อมต่อสภาวะวิกฤติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและระบบสารสนเทศ (IT Continuity Plan) จากสถานการณ์ความไม่แน่นอน ภัยพิบัติและเหตุการณ์ฉุกเฉินที่ไม่อาจคาดคิด

(๓.๓) ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่าย(Server Computer) และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมด

(๓.๔) ควบคุม ติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

(๓.๕) ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(๓.๖) ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก

(๔) รับผิดชอบในการรักษาความปลอดภัย การใช้ระบบอินเทอร์เน็ต

(๕) รับผิดชอบความปลอดภัยทั่วไป

<u>ผู้รับผิดชอบ ได้แก่</u>

เจ้าหน้าที่เทคโนโลยีสารสนเทศ ของ อบน.