นโยบายความมั่นคงปลอดภัย
ของระบบเทคโนโลยีสารสนเทศองค์การสวนพฤกษศาสตร์
ฉบับปรับปรุง พ.ศ. 2563

ส่วนเทคโนโลยีสารสนเทศ สำนักบริหาร
องค์การสวนพฤกษศาสตร์

นโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ องค์การสวนพฤกษศาสตร์

ฉบับปรับปรุงตามข้อเสนอคณะทำงานBCM และ จากสำนักตรวจสอบภายใน พ.ศ.๒๕๖๓

1. หลักการและเหตุผล

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การสวนพฤกษศาสตร์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ องค์การสวนพฤกษศาสตร์จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

2. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การสวนพฤกษศาสตร์หรือต่อไปนี้เรียกว่า “องค์การฯ” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่างๆ องค์การฯ จึงเห็นสมควรกำหนดนโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน แนวทางปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆโดยมีวัตถุประสงค์ดังต่อไปนี้

2.1การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสานหรือเครือข่ายคอมพิวเตอร์ขององค์การฯ ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

2.2กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO / IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

2.3นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์การฯ ได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2.4เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์การฯ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การ ในการดำเนิน งานและปฏิบัติตามอย่างเคร่งครัด

2.5นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปีหรือตามที่ระบุไว้ในเอกสาร “การตรวจสอบประเมินนโยบาย”

1. องค์ประกอบของนโยบาย

1.1 คำนิยาม

1.2 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

1.3 การควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายคอมพิวเตอร์

1.4 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

1.5 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

1.6 การพิสูจน์ตัวตน

1.7 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพา

1.8 การใช้งานอินเตอร์เน็ต

1.9 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1.10 การสำรองข้อมูลที่สำคัญ

1.11 การใช้ซอฟต์แวร์และลิขสิทธิ์

1.12 การโจมตีผ่านระบบเครือข่ายโทรคมนาคมและคอมพิวเตอร์

1.13 การบริหารจัดการสินทรัพย์และการจัดการบันทึกและเปลี่ยนแปลงค่าระบบของทุกอุปกรณ์ระบบและระบบงาน

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และการสื่อสารขององค์การฯ แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน แนวทางปฏิบัติ และขั้นตอนวิธีการปฏิบัติ ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์การฯ เพื่อที่จะทำให้องค์การฯ มีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินการ ทรัพย์สิน บุคคลากร ขององค์การฯ ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การฯนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การฯ ซึ่งเจ้าหน้าที่ขององค์การฯและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- องค์การฯ หมายถึง องค์การสวนพฤกษศาสตร์
- ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์การฯ
- งานเทคโนโลยีสารสนเทศ หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายขององค์การฯ
- หัวหน้างานเทคโนโลยีสารสนเทศ หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์การฯ ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การฯ
- มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- วิธีการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- ผู้ใช้ หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์การฯ โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท(Role) ซึ่งองค์การกำหนดไว้ดังนี้
    - ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงขององค์การ เช่น ผู้อำนวยการองค์การสวนพฤกษศาสตร์ รองผู้อำนวยการองค์การสวนพฤกษศาสตร์ ผู้อำนวยการสำนัก หัวหน้าส่วน เป็นต้น

- ผู้บริหารด้านเทคโนโลยีสารสนเทศ หมายถึง ผู้มีอำนาจในการกำกับดูแลการบริหารงานด้านเทคโนโลยีสารสนเทศขององค์การสวนพฤกษศาสตร์
- ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
- เจ้าหน้าที่ หมายถึง พนักงานของรัฐ ลูกจ้างชั่วคราว ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการที่สังกัดภายใต้องค์การสวนพฤกษศาสตร์

- หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่องค์การฯ อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆขององค์การฯ โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดในการรักษาความลับของข้อมูล
- ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
- สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ
- ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์การฯ ได้ เช่น ระบบ Lan , ระบบ Intranet, ระบบ Internet เป็นต้น
    - ระบบ Lan และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในองค์การฯ
    - ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆขององค์การฯเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

- ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานขององค์การฯ ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่ายโปรแกรม ข้อมูลและสารสนเทศ เป็นต้น
- พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึงพื้นที่ที่องค์การฯ ได้ให้มีการใช้งานและบริการระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น
    - พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพา (Notebook) ที่ประจำโต๊ะทำงาน
    - พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)
    - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or network area)
    - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)
    - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless Lan coverage area)
- เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบหมายอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- ทรัพย์สิน หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์การฯ เช่น อุปกรณ์ระบบเครือข่าย ซอฟท์แวร์ที่มีลิขสิทธิ์ เป็นต้น
- จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายเชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น
- รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขจำนวนไม่ต่ำกว่าแปดตัวอักษร ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่งคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

- ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ส่วนที่ 1

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and environment security)

1. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุม และป้องกันเพื่อการรักษาความมั่งคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

2. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

2.1 ภายในองค์การฯ มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆอย่างเหมาะสม โดยจัดทำเป็นแผนผัง เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆที่อาจเกิดขึ้นได้

2.2 ควรกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ(System Administrator Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์(Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย(Wireless Lan Coverage Area) เป็นต้น

2.3 มีการกำหนดสิทธิ์ให้กับเจ้าหน้าที่ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

2.3.1 จัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.3.2 ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”

2.3.3 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำ และให้มีการปรับปรุงรายการมีสิทธิ์เข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 2

การควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์

(Computer Center Entry Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์การฯ โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของบุคคลต่างๆที่มีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์

2. คำจำกัดความของผู้ที่เกี่ยวข้อง

2.1 ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับการปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์

2.2 เจ้าหน้าที่ หมายถึง เจ้าหน้าที่องค์การฯที่มีสิทธิ์ในการเข้าออกสถานที่ อาคาร ห้อง ภายในองค์การฯ

2.3 ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่างๆของห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์

3. บทบาทและความรับผิดชอบ

3.1 หัวหน้างานเทคโนโลยีสารสนเทศ

3.1.1 อนุมัติเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

3.1.2 อนุมัติกระบวนการควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์

3.2 ผู้ดูแลระบบห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์

3.2.1 ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของศูนย์ปฏิบัติการเครือข่ายอย่างเคร่งครัด

3.2.2 ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ต้องได้รับอนุญาตจากผู้ดูแลระบบห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์

4. กระบวนการควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์

4.1 ผู้ดูแลระบบห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์และเจ้าหน้าที่องค์การฯ มีแนวทางปฏิบัติ ดังนี้

4.1.1 ผู้ดูแลระบบฯ ควรจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์ต่างๆมีประสิทธิภาพมากขึ้น

4.1.2 ศูนย์คอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายคอมพิวเตอร์ต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกศูนย์คอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายคอมพิวเตอร์โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในและมีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

4.1.3 สิทธิ์ในการเข้าออกห้องต่างๆ ภายในศูนย์คอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายคอมพิวเตอร์ของเจ้าหน้าที่แต่ละคนต้องได้รับการอนุมัติจากหัวหน้างานเทคโนโลยีสารสนเทศโดยผ่านกระบวนการลงทะเบียนที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบ” เป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่ปฏิบัติงานภายในห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์

4.1.4 เจ้าหน้าที่ทุกคนต้องทำบัตรผ่านหรือมีรหัสผ่านเพื่อใช้ในการเข้าออกศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ตามกระบวนการที่ระบุในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบ”

4.1.5 ต้องจัดทำระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายคอมพิวเตอร์ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

4.1.6 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ ซึ่งอาจมีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายคอมพิวเตอร์ก็ต้องมีการควบคุมอย่างรัดกุมและมีระบบเก็บบันทึกการเข้าออกห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์

4.1.7 การเข้าถึงห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

4.1.8 เจ้าหน้าที่ห้องศูนย์คอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายคอมพิวเตอร์ทุกคนต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้าออกทุกคนต้องกรอกแบบฟอร์มดังกล่าว

4.2 ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติดังนี้

4.2.1 ผู้ติดต่อจากหน่วยงานภายนอกต้องได้รับอนุญาตจากหัวหน้างานเทคโนโลยีสารสนเทศ และแสดงเอกสารที่ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่กับเจ้าหน้าที่ควบคุมการเข้าออกศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

4.2.2 พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอกสามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้าออกและต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

4.2.3 ผู้ติดต่อจากหน่วยงานภายนอก สามารถนำผู้ติดตามเข้ามาช่วยงานได้ และทุกคนจะต้องถูกบันทึกการเข้าออกเช่นกัน

4.2.4 เมื่อสิ้นสุดภารกิจผู้ติดต่อจากหน่วยงานภายนอก ต้องแจ้งกับเจ้าหน้าที่ควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์เพื่อตรวจสอบการลงบันทึกข้อมูลในสมุดบันทึกการขออนุญาตเข้าออกว่ามีเจ้าหน้าที่ลงนามอนุญาตแล้วทุกครั้ง

4.2.5 เจ้าหน้าที่ห้องศูนย์คอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายคอมพิวเตอร์ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึก และแบบฟอร์มการขออนุญาตเข้าออกกับเจ้าหน้าที่ควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายคอมพิวเตอร์ เจ้าหน้าที่ห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 3

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

(Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศ และการสื่อสารขององค์การฯ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การฯได้อย่างถูกต้อง

2. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

2.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

2.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

2.4 ผู้ดูแลระบบ ควรจัดให้มีการระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การฯ และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ

2.5 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ใช้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

3. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1 ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารการกำหนดสิทธิ์ในการเข้าสู่ระบบและต้องมีการจัดเก็บเอกสารดังกล่าวไว้เป็นหลักฐาน

3.2 เจ้าของข้อมูลและ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็น ต้องรู้ตามหน้าที่ที่งานระบุเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

3.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

4. การบริหารจัดการเข้าถึงของผู้ใช้

4.1 การลงทะเบียนเจ้าหน้าที่ใหม่ของศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์การฯ เป็นต้น

4.2 กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

4.3 ผู้ใช้ ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

4.4 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

4.4.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติ ตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

4.4.2 การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

4.4.3 กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

4.4.3.1 ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้นๆ

4.4.3.2 ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

4.4.3.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

4.4.3.4 ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุกครั้ง เป็นต้น

4.5 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

4.5.1 ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

4.5.2 เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4.5.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงระบบงาน ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

4.5.4 ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

4.5.5 ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์การฯ เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

5. การบริหารจัดการการเข้าถึงระบบเครือข่าย

5.1 ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำการควบคุมและป้องกันการบุกรุก ได้อย่างเป็นระบบ

5.2 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์ในการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

5.3 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆอย่างน้อยปีละ 1 ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

5.4 ระบบเครือข่ายทั้งหมดขององค์การฯที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกองค์การฯ ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

5.5 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์การฯในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

5.6 การเข้าสู่ระบบงานเครือข่ายภายในองค์การฯ โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

5.7 IP Address ภายในของระบบงานเครือข่ายภายในขององค์การฯ จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกันโครงสร้างของระบบเครือข่ายและส่วนประกอบของห้องศูนย์คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ได้

5.8 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆพร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.9 การใช้เครื่องมือต่างๆ(Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

5.10 การติดตั้งและการเชื่อต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์ปฏิบัติการเครือข่ายเท่านั้น

6. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

6.1 ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือมีการเปลี่ยนแปลงค่าต่างๆของโปรแกรมระบบ(System Software) อย่างชัดเจน

6.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

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

6.4 ควรดำเนินการติดตั้งอัพเดทระบบซอฟท์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

6.5 ควรมีการทดสอบโปรแกรมระบบ(System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

6.6 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่งานเทคโนโลยีสารสนเทศเท่านั้น

7. การบริหารจัดการการบันทึกและตรวจสอบ

7.1 ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน ตามพรบ.ความผิดทางคอมพิวเตอร์ พ.ศ.๒๕๕๐

7.2 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

7.3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆและจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

8. การควบคุมการเข้าใช้งานระบบจากภายนอก

ศูนย์ปฏิบัติการเครือข่ายต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์การฯ เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

8.1 การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์การฯ ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์การฯ การควบคุมบุคคลที่เข้าสู่ระบบขององค์การฯจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

8.2 วิธีการใดๆก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับอนุมัติจากหัวหน้างานเทคโนโลยีสารสนเทศก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

8.3 ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์การฯอย่างพอเพียงและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

8.4 ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้าองค์การฯนั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

8.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่ควรเปิด port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

9. การพิสูจน์ตัวตนสำหรับผู้ใช้อยู่ภายนอก

9.1 ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานะระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์การฯ สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

9.1.1 การแสดงตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้ (Username)

9.1.2 การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน (Password) เป็นต้น

9.1.3 การเข้าสู่ระบบสารสนเทศขององค์การฯนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี

9.1.4 การเข้าสู่ระบบสารสนเทศขององค์การจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย

9.1.5 การเข้าสู่ระบบจากระยะไกล (Remote Access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ส่วนที่ 4

การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

(Third party access control)

1. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การฯ ให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบการใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

2. แนวทางปฏิบัติ

2.1 หัวหน้างานเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

2.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อของหน่วยงานภายนอก

2.2.1 บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์การฯจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากหัวหน้างานเทคโนโลยีสารสนเทศ

2.2.2 จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อ ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

2.2.2.1 เหตุผลในการขอใช้

2.2.2.2 ระยะเวลาในการใช้

2.2.2.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

2.2.2.4 การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

2.2.2.5 การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

2.2.3 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น

2.2.4 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์การฯ ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และ การรักษาความพร้อมที่จะให้บริการ (Availability)

2.2.5 ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ 5

การพิสูจน์ตัวตน

(Accountability, Identification and Authentication)

1. วัตถุประสงค์

การปกป้องความมั่นคงปลอดภัยของระบบและข้อมูลภายในองค์การฯ ถือเป็นเรื่องสำคัญในปัจจุบัน ทั้งนี้เนื่องจากการถูกคุกคามโดยผู้ไม่ประสงค์ดีหรือจากโปรแกรมบางประเภทได้เพิ่มมากขึ้นและอาจนำมาซึ่งความเสียหายอย่างมากต่อองค์การฯ ดังนั้น ถ้าภายในระบบมีการควบคุมความปลอดภัยที่ดีจะช่วยลดโอกาสเสี่ยงต่อการถูกคุกคาม การพิสูจน์ตัวตนซึ่งเป็นขั้นตอนพื้นฐานที่สำคัญของการควบคุมความปลอดภัยในกระบวนการพิสูจน์ตัวตนจะนำหลักฐานที่ผู้ใช้กล่าวอ้างมาตรวจสอบว่าบุคคลที่กล่าวอ้างนั้นเป็นใครและได้รับอนุญาตให้สามารถเข้ามาภายในระบบได้หรือไม่ การพิสูจน์ตัวตนมีหลายประเภทที่ใช้อยู่ในปัจจุบัน เช่น การพิสูจน์ตัวตนโดยใช้รหัสผ่าน ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล หรือโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว เป็นต้น แต่ละชนิดนั้นจะมีข้อดีข้อเสียแตกต่างกันไป ขึ้นอยู่กับความจำเป็นในใช้งาน ในระบบเครือข่ายแบบเปิดหรืออินเตอร์เน็ตนั้น การพิสูจน์ตัวตนถือได้ว่าเป็นกระบวนการเริ่มต้นและมีความสำคัญที่สุดในการปกป้องเครือข่ายให้ปลอดภัย

2. แนวทางปฏิบัติในการพิสูจน์ตัวตน

2.1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

2.2 ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ไม่ว่าการกระทำนั้นเกิดจากผู้ใช้งานหรือไม่ก็ตาม

2.3 ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า 8 ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special Character)

2.4 ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย 5 รหัสผ่าน

2.5 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) เป็นประจำหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

2.6 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศขององค์การฯและหากการพิสูจน์ตัวตนนั้นมีปัญหา ซึ่งอาจจะเกิดจากรหัสผ่าน การโดนบล๊อค หรือ เกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

2.6.1 คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

2.6.2 การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจนตัวตนทุกครั้ง

2.6.3 การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

2.6.4 เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการบล็อกหน้าจอทุกครั้งและต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

2.6.5 เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (Screen Saver) กรณีผู้ใช้งานไม่อยู่ปฏิบัติงาน

ส่วนที่ 6

การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

(Use of Personal Computer)

1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์การฯ ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์ที่องค์การฯอนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินขององค์การฯ ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์การฯ

2.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์การฯ เป็นโปรแกรมที่องค์การฯได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.3 ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์การฯ

2.4 การตั้งชื่อคอมพิวเตอร์และคอมพิวเตอร์แม่ข่าย จะต้องกำหนดให้สอดคล้องกับภาระหน้าที่ใช้งาน

2.5 การเคลื่อนย้ายหรือส่งคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของงานเทคโนโลยีสารสนเทศเท่านั้น

2.6 ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

2.7 ไม่ควรเก็บข้อมูลสำคัญขององค์การฯไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่ ให้จัดเก็บ ณ FTP Server ที่กำหนดไว้

2.8 ผู้ใช้งานควรบันทึกข้อมูลต่างๆไว้ที่ Drive อื่นๆ หรือจัดเก็บ ณ FTP Server ที่กำหนดไว้ ยกเว้น Drive C และหน้า Desktop

2.9 ควรกำหนดการเข้ารหัสในระหว่างที่พักหน้าจอหรือไม่ได้ใช้งานชั่วขณะเป็นเวลาอย่างน้อยไม่ต่ำกว่า 15 นาที

2.10 ไม่ควรสร้าง Short – Cut หรือปุ่มกดง่ายๆบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์การ

2.11 ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติ ดังนี้

2.11.1 ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

2.11.2 ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

3. การควบคุมการเข้าถึงระบบปฏิบัติการ

3.1 ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

3.2 ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลา เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

3.3 ผู้ใช้ ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3.4 ในระหว่างพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Logout ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver

4. แนวทางปฏิบัติในการใช้รหัสผ่าน

4.1 ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์(Malware)

5.1 ผู้ใช้มีหน้าที่รับผิดชอบในการ Update โปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

5.2 ผู้ใช้ มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

5.3 ผู้ใช้ควรตรวจหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

5.4 ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

5.5 ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

6. การสำรองข้อมูลและการกู้คืน

6.1 ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกสื่ออื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น

6.2 ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนที่สำรองไว้อย่างสม่ำเสมอ

6.3 ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์การฯ

ส่วนที่ 7

การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

(Use of Note computer)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพา และการนำไปปฏิบัติงานภายนอกองค์การฯ เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์การฯให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยงในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์แบบพกพาที่องค์การฯ อนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินขององค์การฯ ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์การฯ

2.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกขององค์การฯ เป็นโปรแกรมที่องค์การฯได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่างๆและนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.3 การตั้งชื่อเครื่องคอมพิวเตอร์และคอมพิวเตอร์แม่ข่าย แบบพกพาจะต้องกำหนดให้สอดคล้องกับรับผิดชอบในงานนั้นๆ

2.4 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศเท่านั้น

2.5 ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

2.6 ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

2.7 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์พกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

2.8 ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่องหรืออาจถูกจับโยนได้

2.9 การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

2.10 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่นปลายปากกา กดสัมผันหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

2.11 ไม่ควรวางทับบนหน้าจอและแป้นพิมพ์

2.12 การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

2.13 ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

2.14 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น

2.15 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ควรอยู่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

2.16 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

2.17 ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

2.18 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกัน ห้ามแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

2.19 เพื่อรักษาข้อมูลความปลอดภัยภายในเครื่องคอมพิวเตอร์ ผู้ใช้งานควรกำหนดรหัสรักษาความปลอดภัยในช่วงพักหน้าจอหรือช่วงเวลาที่เครื่องเปิดรอการใช้งานจากผู้ใช้งานไม่ควรเกิน 10 นาที หลังจากไม่มีการปฏิบัติงานบนเครื่องคอมพิวเตอร์ดังกล่าว

3. ความปลอดภัยทางด้านกายภาพ

3.1 ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

3.2 ผู้ใช้ ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน / ความชื้น / ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

3.3 ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

4. การควบคุมการเข้าถึงระบบปฏิบัติการ

4.1 ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน(User name) และรหัสผ่าน(Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

4.2 ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

4.3 ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

5. แนวทางปฏิบัติในการใช้รหัสผ่าน

5.1 ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

6. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์(Malware)

6.1 ผู้ใช้มีหน้าที่รับผิดชอบในการ Update โปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

6.2 ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

6.3 หากผู้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์(Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่นๆได้

7. การสำรองข้อมูลและการกู้คืน

7.1 ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่างๆเพื่อป้องกันการสูญหายของข้อมูล

7.2 ผู้ใช้ควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

7.3 แผ่นสื่อสำรองข้อมูลต่างๆที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

7.4 แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

ส่วนที่ 8

การใช้งานอินเทอร์เน็ต

(Use of the Internet)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์การฯถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

2.1. ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์การฯจัดสรรไว้เท่านั้น เช่น proxy, Firewall, IP-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่นด้วยตนเอง ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากหัวหน้างานเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษรแล้ว

2.2. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

2.3. ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

2.4. ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์การฯ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

2.5. ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่รับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์การฯ

2.6. ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับองค์การฯ

2.7. ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์การฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

2.8. ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

2.9. ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย

2.10. ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

2.11. ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่างๆจากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

2.12. การใช้งานเว็บบอร์ด (Web Board) ขององค์การฯ ผู้ใช้ต้องใช้ข้อความที่สุภาพและต้องไม่เปิดเผยข้อมูลที่สำคัญที่เป็นความลับขององค์การฯ

2.13. ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์การฯ การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่นๆ

2.14. หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ส่วนที่ 9

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(Wireless LAN Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan) ขององค์การฯโดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงานรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

2.1. ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์การฯ จะต้องได้รับการพิจารณาอนุญาตจากหัวหน้างานเทคโนโลยีสารสนเทศ

2.2. ผู้ดูแลระบบ ต้องทำการกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3. ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

2.4. ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

2.5. ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น

2.6. ผู้ดูแลระบบ ควรทำการเปลี่ยน SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

2.7. ผู้ดูแลระบบควรเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และดูแลระบบควรเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

2.8. ผู้ดูแลระบบต้องกำหนดค่าใช้ WEP หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น

2.9. ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ที่มีสิทธิ์ใช้ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้น ให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

2.10. ผู้ดูแลระบบควรจะมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์การฯ

2.11. ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

2.12. ผู้ดูแลระบบ ควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

ส่วนที่ 10

การสำรองข้อมูลที่สำคัญ

(Backup Policy)

1. วัตถุประสงค์

การสำรองข้อมูลและระบบคอมพิวเตอร์และการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและในเวลาที่ต้องการ (Availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

2. แนวทางปฏิบัติในการสำรองข้อมูลที่สำคัญ

2.1. จัดทำสำเนาข้อมูลและซอฟท์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

2.2. มีขั้นตอนการการปฏิบัติการจัดทำสำรองและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟท์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

2.3. จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟท์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ในสถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

2.4. ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

ส่วนที่ 11

การใช้ซอฟท์แวร์และลิขสิทธิ์

(Software Licensing and intellectual property)

1. วัตถุประสงค์

ลิขสิทธิ์เป็นทรัพย์สินทางปัญญาอย่างหนึ่ง ที่กฎหมายให้ความคุ้มครองโดยให้เจ้าของลิขสิทธิ์ถือสิทธิแต่เพียงผู้เดียวที่จะกระทำการใดๆ เกี่ยวกับงานสร้างสรรค์ที่ตนได้กระทำขึ้น กฎหมายลิขสิทธิ์จึงมีวัตถุประสงค์ให้ความคุ้มครอง ป้องกันผลประโยชน์ทั้งทางเศรษฐกิจและทางศีลธรรม ซึ่งบุคคลพึงได้รับจากผลงานสร้างสรรค์อันเกิดจากความนึกคิด และสติปัญญาของตน นอกจากนี้ยังมุ่งที่จะสนับสนุนส่งเสริมให้เกิดการสร้างสรรค์ผลงาน กล่าวคือ เมื่อผู้สร้างสรรค์ได้รับผลตอบแทนจากหยาดเหงื่อแรงกายและสติปัญญาของตน ก็ย่อมจะเกิดกำลังใจที่จะคิดค้นสร้างสรรค์และเผยแพร่ผลงานให้แพร่หลายออกไปมากยิ่งขึ้น อันจะเป็นประโยชน์ต่อการพัฒนาประเทศชาติทั้งด้านเศรษฐกิจ สังคม และเทคโนโลยี การกระตุ้นให้เกิดการพัฒนาสติปัญญาของคนในชาติ เป็นปัจจัยสำคัญที่สุดที่จะนำไปสู่การพัฒนาที่ยั่งยืนต่อไปในอนาคต

2. แนวทางปฏิบัติในการใช้ซอฟท์แวร์และลิขสิทธิ์

2.1. องค์การฯ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น ซอฟท์แวร์ที่องค์การฯอนุญาตให้ใช้งานหรือที่องค์การฯมีลิขสิทธิ์ ผู้ใช้สามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และองค์การฯห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟท์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ องค์การฯ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

2.2. ซอฟท์แวร์(Software) ที่องค์การฯ ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงานห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

ส่วนที่ 12

การโจมตีผ่านระบบเครือข่ายโทรคมนาคมและคอมพิวเตอร์

(Cyber Attack)

1. วัตถุประสงค์

การโจมตีผ่านระบบเครือข่ายโทรคมนาคมและคอมพิวเตอร์ (Cyber Attack) คือ การกระทำใด ๆ ที่ใช้ชุดคำสั่งทางภาษาคอมพิวเตอร์ เพื่อให้ส่งผลต่อคอมพิวเตอร์, เครือข่าย หรือระบบ รวมทั้งอุปกรณ์ที่เกี่ยวข้อง เพื่อตั้งใจเป็นภัยคุกคาม ขัดขวาง หรือทำลายระบบ โดยผลกระทบที่ต้องการของการโจมตีไม่จำเป็นต้องจำกัดเพียงระบบคอมพิวเตอร์ และข้อมูลที่เป็นเป้าหมายเนื่องจากระบบโครงข่ายอินเทอร์เน็ตมีขอบเขตที่กว้าง และครอบคลุมการปฏิบัติในหลากหลาย ดังนั้น มาตรการในการรักษาความปลอดภัยไซเบอร์จึงมีระบบในการรักษาความปลอดภัยที่หลากหลาย ทั้งนี้จึงจำเป็น จะต้องมีมาตรการรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศขององค์การฯ ขึ้น ตามมาตรฐานสากล

2. แนวทางปฏิบัติกรณีเมื่อเกิด Cyber Attack

(1) รายงานผู้อำนวยการองค์การสวนพฤกษศาสตร์

(2) รายงานประธานคณะทำงานบริหารความพร้อมต่อสภาวะวิกฤต

(3) ดำเนินการกู้ข้อมูลในระบบสารสนเทศ พร้อมเปิดระบบสำรอง

(4) สืบค้นเหตุการณ์ที่เกิดขึ้นเพื่อปิดช่องโหว่และรวบรวมข้อมูล จากแหล่งข้อมูลที่มาต่างๆ รวมทั้งขอความร่วมมือจากภายนอก เช่น

- ผู้ดูแลระบบ
- ไฟร์วอลล์
- พันธมิตรทางธุรกิจ
- ฝ่ายรักษาความปลอดภัยหรือบุคคลที่รักษาความปลอดภัย
- กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
- กลุ่มองค์กรทางด้านรักษาความปลอดภัยหรือบุคคลที่รักษาความปลอดภัย

(5) วิเคราะห์ปัญหาช่องโหว่ โดยนำผลจากการรวบรวมข้อมูลทำการวิเคราะห์ในมุมมองด้านกระบวนการและด้านเทคโนโลยี พร้อมประเมินความเสียหายของข้อมูลและอุปกรณ์ เพื่อกำหนดเป็นนโยบายด้านการรักษาความปลอดภัยในระบบเทคโนโลยีสารสนเทศต่อไป

(6) กำหนดนโยบายด้านการรักษาความปลอดภัยในระบบเทคโนโลยีสารสนเทศและทำการบริหารจัดการติดตั้ง Patch ให้กับระบบคอมพิวเตอร์ในองค์กรใหม่ โดยทำอย่างเป็นระบบเพื่อปิดช่องโหว่ (Vulnerabilities) ที่อาจถูกโจมตี ในอนาคต กระบวนการ Patch Management ประกอบด้วยมุมมองทางด้านกระบวนการ และ มุมมองทางด้านเทคโนโลยี

(7) ทดสอบระบบ และแก้ไขส่วนที่

(8) รายงานผู้อำนวยการองค์การสวนพฤกษศาสตร์และประธานคณะทำงานบริหารความพร้อมต่อสภาวะวิกฤต และขอดำเนินการเปิดใช้งานระบบ

(9) เปิดระบบเพื่อใช้งานจริง

ส่วนที่ 13

การบริหารจัดการสินทรัพย์ และการจัดการบันทึกและเปลี่ยนแปลง

ค่าระบบของทุกอุปกรณ์ ระบบและระบบงาน

(Asset & Configuration Management)

1. วัตถุประสงค์

เพื่อกำหนดให้มีการบริหารจัดการสินทรัพย์และการควบคุมการกำหนดค่าของระบบเครือข่ายและระบบสารสนเทศที่สำคัญ รวมถึงการระบุทรัพย์สินสารสนเทศและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สิน สารสนเทศที่เหมาะสมทั้งนี้จึงจำเป็น จะต้องมีมาตรการรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศขององค์การฯ ขึ้น ตามมาตรฐานสากล

2. แนวทางปฏิบัติที่สำคัญ

2.1 จัดทำเอกสารกำหนดค่าความมั่นคงปลอดภัยพื้นฐาน ของระบบเครือข่ายและระบบสารสนเทศ ที่มีคุณสมบัติอย่างน้อยดังนี้

– ขีดความสามารถสำคัญในการดำเนินงาน

– ข้อจำกัดการใช้งาน

– กำหนดค่าความมั่นคงปลอดภัยเริ่มต้น

– พอร์ตโพรโทคอล และ หรือบริการที่ได้รับการอนุญาตจากเจ้าหน้าที่

2.2 ทบทวนการกำหนดค่าความมั่นคงปลอดภัยพื้นฐาน ของระบบเครือข่ายและระบบสารสนเทศอย่างสม่ำเสมอ

2.3 จัดทำบัญชีทรัพย์สินสารสนเทศที่สำคัญขององค์กร รวมถึงสินทรัพย์ที่สำคัญ

2.4 ทบทวนบัญชีทรัพย์สินสารสนเทศ อย่างสม่ำเสมอ

2.5 เมื่อมีการใช้งานทรัพย์สินสารสนเทศ จะต้องให้บุคลากรที่เกี่ยวข้องและผู้ใช้งานภายนอกที่มีสิทธิเข้าถึงระบบสารสนเทศขององค์กรได้รับทราบถึงข้อกำหนดการใช้งานทรัพย์สินสารสนเทศที่กำหนดไว้ พร้อมจัดทำบันทึกการการใช้งานทรัพย์สินสารสนเทศ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง องค์การสวนพฤกษศาสตร์นี้ เพื่อใช้เป็นแนวทางในการดำเนินงานด้านดิจิทัล ให้ครอบคลุมการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องความครบถ้วน (Integrity) และ การสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามมาตรฐานการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ และกฎหมายระเบียบปฏิบัติที่เกี่ยวข้อง และให้บุคลากรภายในทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

(นายรณรงค์ เส็งเอี่ยม)

ผู้อำนวยการองค์การสวนพฤกษศาสตร์

๖ สิงหาคม ๒๕๖๓

นโยบายความมั่นคงปลอดภัย
ของระบบเทคโนโลยีสารสนเทศองค์การสวนพฤกษศาสตร์
ฉบับปรับปรุง พ.ศ. 2563

ส่วนเทคโนโลยีสารสนเทศ สำนักบริหาร
องค์การสวนพฤกษศาสตร์