ประกาศกรมควบคุมมลพิษ

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเทคโนโลยีสารสนเทศ กรมควบคุมมลพิษ

พ.ศ. ๒๕๖๕

โดยเป็นการสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเทคโนโลยีสารสนเทศกรมควบคุมมลพิษ เพื่อกำหนดขอบเขตของการบริหารจัดการ และรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ ให้สอดคล้องตามมาตรฐาน ISO/IEC 27001 อันเป็นการสร้างความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานให้มีประสิทธิภาพและประสิทธิผล รวมทั้งเผยแพร่ให้เจ้าหน้าที่ทุกระดับในกรมควบคุมมลพิษได้รับทราบ ยอมรับ และปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

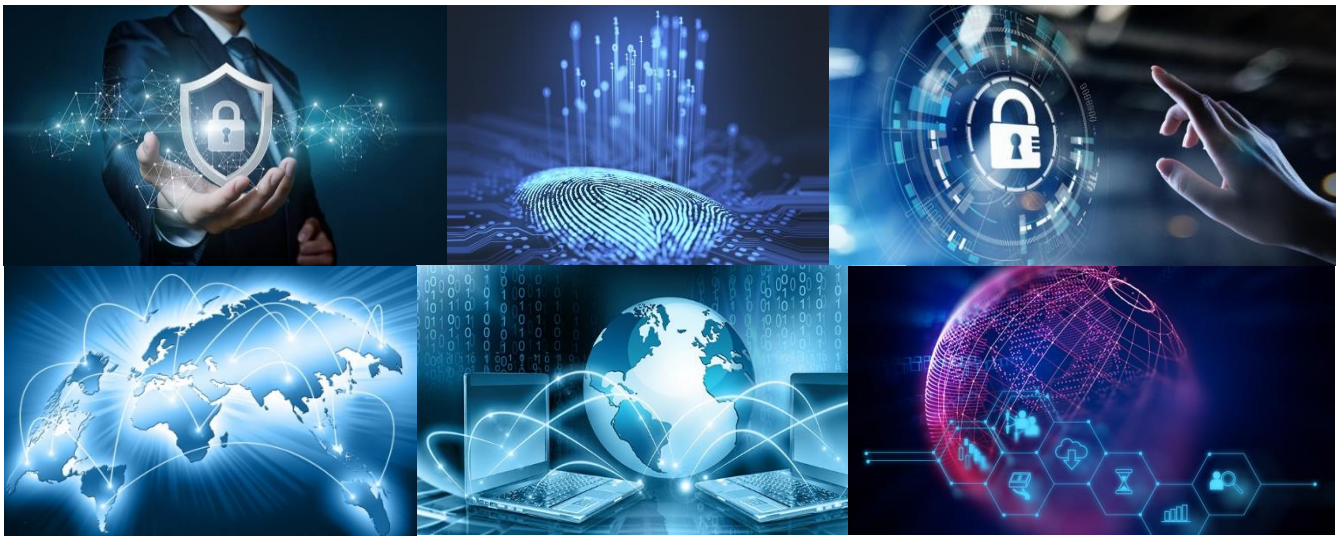
ดังนั้น เพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐมีหน้าที่ดำเนินมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ อธิบดีกรมควบคุมมลพิษจึงอาศัยอำนาจตามมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม ออกประกาศกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเทคโนโลยีสารสนเทศกรมควบคุมมลพิษไว้ ดังรายละเอียดกำหนดไว้ในภาคผนวกท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๗ กรกฎาคม พ.ศ. ๒๕๖๕

(นายอรรถพล เจริญชันษา)

อธิบดีกรมควบคุมมลพิษ

นโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเทคโนโลยีสารสนเทศ กรมควบคุมมลพิษ



ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมควบคุมมลพิษ

สารบัญ

นโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเทคโนโลยีสารสนเทศ กรมควบคุมมลพิษ

๑. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กรมควบคุมมลพิษ หรือต่อไปนี้เรียกว่า “องค์กร” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ จึงเห็นควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเทคโนโลยีสารสนเทศ ตามมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ดังต่อไปนี้

๑.๑ เพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเทคโนโลยีสารสนเทศ สร้างความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้การดำเนินงานมีประสิทธิภาพและประสิทธิผล

๑.๒ เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ให้กับระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ให้สอดคล้องตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๑.๓ นโยบายนี้มีการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบผ่านระบบอินทราเน็ตและ/หรือวิธีการอื่นที่เปิดเผย และถือว่าเจ้าหน้าที่ใช้งานเครื่องมืออุปกรณ์ต่างๆ อันเป็นส่วนหนึ่งของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ยินยอมและยอมรับที่จะปฏิบัติตามนโยบายนี้ (Acceptable Use Policy : AUP) โดยทันทีที่มีการใช้งาน

๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธิปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กรในการปฏิบัติงานด้วยความรับผิดชอบ

๑.๕ นโยบายนี้จะมีการตรวจสอบและประเมินนโยบายตามระยะเวลาประมาณ ๑ ครั้ง ต่อปี หรือตามที่คณะทำงานเทคโนโลยีสารสนเทศและศูนย์บริการประชาชนกรมควบคุมมลพิษจะกำหนดไว้

๒. องค์ประกอบของนโยบาย

- คำนิยาม
- ส่วนที่ ๑ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- ส่วนที่ ๒ การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายส่วนกลาง
- ส่วนที่ ๓ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- ส่วนที่ ๔ การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
- ส่วนที่ ๕ การป้องกันระบบฐานข้อมูล
- ส่วนที่ ๖ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
- ส่วนที่ ๗ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
- ส่วนที่ ๘ การใช้งานอินเทอร์เน็ต
- ส่วนที่ ๙ การใช้งานจดหมายอิเล็กทรอนิกส์
- ส่วนที่ ๑๐ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

องค์ประกอบของนโยบายการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัย เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน รวมทั้งบุคลากรขององค์กร

นโยบายขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ ซึ่งเจ้าหน้าที่ขององค์กร และหน่วยงานภายนอกที่ปฏิบัติงานภายในองค์กรจะต้องถือปฏิบัติ

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **องค์กร** หมายถึง กรมควบคุมมลพิษ
- **ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO)** หมายถึง รองอธิบดีผู้มีอำนาจในการตัดสินใจด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในการกำหนดนโยบายการบริหารระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กร
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร
- **ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง ศูนย์เทคโนโลยีสารสนเทศสารสนเทศและการสื่อสาร กรมควบคุมมลพิษ เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและเครือข่ายส่วนกลางขององค์กรที่ใช้งานร่วมกัน รวมทั้งให้คำปรึกษา พัฒนา ปรับปรุง และบำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายส่วนกลางขององค์กรเป็นหลัก
- **ผู้อำนวยการ** หมายถึง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งมีบทบาทหน้าที่ในส่วนของการร่วมกำหนดนโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบคอมพิวเตอร์และเครือข่ายส่วนกลางขององค์กร
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรที่เป็นการใช้งานระบบคอมพิวเตอร์และเครือข่าย
- **มาตรฐาน** (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- **วิธีการปฏิบัติ** (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์ หรือเป้าหมาย
- **แนวทางปฏิบัติ** (Guideline) หมายถึงแนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- **ผู้ใช้** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กรโดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งองค์กำหนดไว้ดังนี้
  - **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงขององค์กร เช่น อธิบดี รองอธิบดี ผู้อำนวยการกอง
  - **ผู้ดูแลระบบ** (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบในทางนิตินัย และ/หรือทางพฤตินัย ทั้งนี้ในส่วนของระบบคอมพิวเตอร์และเครือข่ายส่วนกลางขององค์กร ผู้ดูแลระบบ หมายถึง ผู้รับผิดชอบดูแลรักษาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลผู้ใช้บริการตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

- **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ ลูกจ้างปฏิบัติงาน รวมถึงเจ้าหน้าที่ประจำโครงการ/กิจกรรมต่างๆ ขององค์กร

❖ **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่กรมควบคุมมลพิษอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ขององค์กร โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูลขององค์กร

❖ **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และหมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และข้อมูลตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์และข้อมูลตามระเบียบกรมควบคุมมลพิษว่าด้วยเรื่องการใช้ระบบคอมพิวเตอร์และเครือข่ายกรมควบคุมมลพิษ พ.ศ. ๒๕๕๔

❖ **สารสนเทศ** (Information) หมายถึงข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

❖ **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

❖ **ระบบเครือข่าย** (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆขององค์กรได้ เช่น ระบบเครือข่ายระยะใกล้ (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

- ระบบเครือข่ายระยะใกล้ (LAN) และ ระบบอินทราเน็ต (Intranet) หมายถึงระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
- ระบบอินเทอร์เน็ต (Internet) หมายถึงระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

❖ **ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และ/หรือระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุม การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

❖ **ระบบฐานข้อมูล** (Database System) หมายถึง โครงสร้างสารสนเทศที่ประกอบด้วยรายละเอียดของข้อมูลที่เกี่ยวข้องกันที่จะนำมาใช้ในระบบต่าง ๆ ร่วมกัน

- **<u>พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร</u>** (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น
  - พื้นที่ทำงานทั่วไป (General Working Area) หมายถึงพื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
  - พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)
  - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Networking Area)
  - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และ/หรือพื้นที่จัดเก็บข้อมูลสำรอง (Data Backup Area)
  - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area)
- **<u>เจ้าของข้อมูล</u>** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- **<u>ทรัพย์สิน</u>** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
- **<u>จดหมายอิเล็กทรอนิกส์</u>** (E-Mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP POP๓ IMAP เป็นต้น
- **<u>รหัสผ่าน</u>** (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- **<u>ชุดคำสั่งไม่พึงประสงค์</u>** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ส่วนที่ ๑
การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

๑. วัตถุประสงค์

เพื่อควบคุม ป้องกันและรักษาความมั่นคงปลอดภัยในการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมีผลบังคับใช้กับผู้ใช้ และ หน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๒. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๒.๑ ภายในองค์กรมีการจำแนก และกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ต่างๆ ตามความเหมาะสม เพื่อการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้น

๒.๒ การกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร จะแบ่งเป็นพื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) พื้นที่จัดเก็บข้อมูลสำรอง (Data Backup Area) และ พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

๒.๓ การกำหนดสิทธิ์และการให้สิทธิ์การเข้าถึงในแต่ละพื้นที่ ขึ้นอยู่กับหน้าที่ความรับผิดชอบของผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อการปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย

๓. การควบคุมการเข้าออก อาคารสถานที่ขององค์กร

๓.๑ การเข้าถึงอาคารขององค์กรของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะมีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลในสมุดบันทึก และ/หรือติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจน ตลอดเวลาที่อยู่ในองค์กรและส่งคืนเมื่อออกจากองค์กร

๓.๒ กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์พกพา หรือ อุปกรณ์เครือข่ายเข้ามาใช้งานร่วมกับระบบเครือข่ายและ/หรือระบบเครือข่ายไร้สายในบริเวณอาคารเป็นการชั่วคราว โดยผู้ดูแลระบบเปิดระบบให้สามารถเชื่อมต่อสัญญาณคอมพิวเตอร์ได้แบบชั่วคราว บุคคลภายนอกหรือผู้ติดต่อจะต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยในการนำอุปกรณ์ออกจากอาคาร รวมทั้งบันทึกเวลาใช้งานให้ถูกต้องตามจริงในแบบฟอร์มหลังออกจากอาคารทุกครั้ง

๓.๓ กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์พกพา หรือ อุปกรณ์เครือข่ายเข้ามาใช้งานร่วมกับระบบเครือข่ายและ/หรือระบบเครือข่ายไร้สายในบริเวณอาคาร ซึ่งผู้ดูแลระบบมิได้เปิดระบบให้สามารถเชื่อมต่อ

สัญญาณคอมพิวเตอร์ได้แบบอัตโนมัติ บุคคลภายนอกหรือผู้ติดต่อจะต้องติดต่อผู้ดูแลระบบเพื่อขออนุญาตใช้งานเป็นกรณีๆ และลงบันทึกไว้เป็นหลักฐานตาม ๓.๒

ส่วนที่ ๒
การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายส่วนกลาง
(Computer & Network Room Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายส่วนกลาง

๒. คำจำกัดความของผู้เกี่ยวข้อง

๒.๑ ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาระบบคอมพิวเตอร์และเครือข่ายส่วนกลางขององค์กร ทั้งในทางนิตินัย และ/หรือทางพฤตินัย

๒.๒ เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ ลูกจ้างปฏิบัติงาน รวมถึงเจ้าหน้าที่ประจำโครงการ/กิจกรรมต่างๆ ภายใต้ความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓ เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ ลูกจ้างปฏิบัติงาน รวมถึงเจ้าหน้าที่ประจำโครงการ/กิจกรรมต่างๆ ภายใต้ความรับผิดชอบขององค์กร ยกเว้นเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๔ ผู้ติดต่อ หมายถึง บุคคลจากหน่วยงานภายนอก หรือประชาชนที่มาทำการติดต่อ ขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่างๆ ที่เกี่ยวข้องกับระบบคอมพิวเตอร์และเครือข่ายส่วนกลางขององค์กร หรือของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓. บทบาทและความรับผิดชอบ

๓.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓.๑.๑ อนุมัติสิทธิ์เข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายส่วนกลาง

๓.๑.๒ อนุมัติกระบวนการควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายส่วนกลาง

๓.๒ ผู้ดูแลระบบ และ เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓.๒.๑ ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายส่วนกลางให้ปฏิบัติตามระเบียบและกฎเกณฑ์

๓.๒.๒ ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกห้องควบคุมระบบฯ จะต้องติดบัตรผู้ติดต่อ (Visitor) หรือบัตรประจำตัวขององค์กร

๔. กระบวนการควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายส่วนกลาง

๔.๑ ผู้ดูแลระบบ เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และเจ้าหน้าที่มีแนวทางปฏิบัติดังนี้

๔.๑.๑ ผู้ดูแลระบบจะทำการจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนของอุปกรณ์ควบคุมระบบเครือข่าย (Network Equipment Zone) ส่วนเครื่องแม่ข่ายงานต่างๆ (Server Zone) ส่วนเครื่องพิมพ์ (Printer Zone) ส่วนของระบบสำรองไฟฟ้า (UPS Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์ต่างๆ มีประสิทธิภาพมากขึ้น

๔.๑.๒ เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จะต้องบันทึกการเข้าการยืนยันลายนิ้วมือที่ระบบประตูล็อคด้วยไฟฟ้า (Access Control) และตรวจสอบปิดประตูให้ล็อคสนิททุกครั้ง

๔.๑.๓ การเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายส่วนกลาง กรณีที่เป็นเจ้าหน้าที่ซึ่งมีบัตรแสดงตนเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะต้องลงบันทึกการเข้าที่ระบบประตูล็อคด้วยไฟฟ้า (Access Control) และลงบันทึกในเอกสารลงทะเบียนการเข้าออกห้องควบคุมระบบฯ ด้วย

๔.๒ ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติดังนี้

๔.๒.๑ กรณีผู้ติดต่อเป็นบุคคลภายนอก เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จะต้องตรวจสอบการติดบัตรผู้ติดต่อ (Visitor) หรือบัตรประจำตัวขององค์กร กับเจ้าหน้าที่รักษาความปลอดภัยในเบื้องต้นก่อน และจะต้องลงบันทึกในเอกสารลงทะเบียนการเข้าออกห้องควบคุมระบบฯ รวมทั้งสอดส่องดูแลบุคคลที่เข้าออกเพื่อความมั่นคงปลอดภัยของระบบอย่างรอบคอบทุกครั้ง

๔.๒.๒ ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องดำเนินการตามข้อกำหนดในส่วนที่ ๑ ข้อ ๓ การควบคุมการเข้าออกอาคารสถานที่ขององค์กร

ส่วนที่ ๓
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Information Technology System Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบคอมพิวเตอร์และเครือข่ายส่วนกลางขององค์กร ได้อย่างถูกต้อง

๒. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๒.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารจะมีการควบคุมการเข้าออกสถานที่ที่รัดกุม และอนุญาตให้เฉพาะผู้มีสิทธิและหน้าที่เข้าใช้งานเท่านั้น

๒.๒ ผู้ดูแลระบบ จะมีการกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๓ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

๒.๔ ผู้ดูแลระบบ จะจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ รวมทั้งติดตามการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ อย่างสม่ำเสมอ

๓. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓.๑ ผู้ดูแลระบบ มีหน้าที่ตรวจสอบการอนุมัติและ/หรือการให้สิทธิ์ในการใช้งานระบบให้แก่ผู้ใช้ โดยผู้ใช้อาจทำเอกสารขอสิทธิ์ในการใช้ระบบ ซึ่งอาจมีการกำหนดให้มีการลงนามอนุมัติโดยผู้มีอำนาจ หรืออยู่ในดุลพินิจของผู้ดูแลระบบ และเก็บเอกสารไว้เป็นหลักฐาน

๓.๒ เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓.๓ ผู้ใช้งานจะได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและ/หรือ เจ้าของระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศเท่านั้น

๔. การบริหารจัดการการเข้าถึงระบบสารสนเทศของผู้ใช้

๔.๑ มีการกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยผู้ดูแลระบบจะให้สิทธิ์เฉพาะการ

ปฏิบัติงานในหน้าที่ และจะมีการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น ทั้งนี้จะมีการทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๔.๒ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

๔.๒.๑ ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ จะกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ แยกตามหน้าที่ที่รับผิดชอบ รวมทั้งรับผิดชอบการเปลี่ยนแปลง และการยกเลิกรหัสผ่านของเจ้าหน้าที่

๔.๒.๒ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

๔.๒.๒.๑ ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้นๆ

๔.๒.๒.๒ ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๔.๒.๒.๓ ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๔.๒.๒.๔ ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๔.๓ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๔.๓.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔.๓.๒ เจ้าของข้อมูล ควรจะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔.๓.๓ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๔.๓.๔ กรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๕. การบริหารจัดการการเข้าถึงระบบเครือข่าย

๕.๑ ผู้ดูแลระบบ จะต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๕.๒ การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับความเห็นชอบจากผู้บริหารระดับสูง ผู้อำนวยการศูนย์ฯ หรือผู้ดูแลระบบ ก่อนการใช้งานในทุกกรณี

๕.๓ ผู้ดูแลระบบ จะต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๔ ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๕.๕ ผู้ดูแลระบบ ควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้

๕.๖ ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกองค์กรควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (firewall) หรือฮาร์ดแวร์อื่นๆ ซึ่งอาจรวมถึงความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๕.๗ มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๕.๘ การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการล๊อกอินและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

๕.๙ IP address ภายในของระบบงานเครือข่ายภายในขององค์กร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของระบบคอมพิวเตอร์และเครือข่ายส่วนกลางได้โดยง่าย

๕.๑๐ มีการจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๑๑ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยหรือภายใต้การควบคุมดูแลของเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

๖. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๖.๑ ผู้ดูแลระบบ เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) แก้ไข หรือเปลี่ยนแปลงค่าต่างๆของโปรแกรมระบบ (System Software) อย่างชัดเจน

๖.๒ ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) จะต้องตรวจสอบระบบคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติจะต้องดำเนินการแก้ไข รวมทั้งรายงานผู้บังคับบัญชาโดยทันที

๖.๓ ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการป้องกันเพิ่มเติมด้วย

๖.๔ ควรดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่างๆของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น web server เป็นต้น

๖.๕ ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๖.๖ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยหรือภายใต้การควบคุมดูแลของเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

๗. การบริหารจัดการการบันทึกและตรวจสอบ

๗.๑ กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๗.๒ จะต้องมีการป้องกันการเปลี่ยนแปลง แก้ไขบันทึกต่างๆ และมีการจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๘. การควบคุมการเข้าใช้งานระบบจากภายนอก

การควบคุมดูแลรักษาความปลอดภัยการใช้งานระบบคอมพิวเตอร์และเครือข่ายส่วนกลาง หรือต่อไปนี้เรียกว่า ระบบ โดยการเข้าใช้งานจากภายนอก จะต้องดำเนินการตามแนวทางปฏิบัติดังนี้

๘.๑ วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล (Remote Access) ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน และมีการควบคุมอย่างเข้มงวดโดยผู้ดูแลระบบ ทั้งนี้ผู้ใช้ต้องปฏิบัติตามมาตรฐานการรักษาความปลอดภัยที่เป็นวิธีการที่เป็นมาตรฐานสากลอย่างเคร่งครัด

๘.๒ ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐาน/เหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ที่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มอบหมายก่อน

๘.๓ ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้าองค์กรนั้นต้องมีการดูแลและการจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๘.๔ การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นจึงไม่ควรเปิดพอร์ตที่ไม่ได้ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวจะมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๙. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

๙.๑ ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

๙.๑.๑ การแสดงตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้ (Username)

๙.๑.๒ การพิสูจน์ยืนยันตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ด หรือการใช้ USB token ที่มีความสามารถ PKI เป็นต้น

๙.๒ การเข้าสู่ระบบสารสนเทศขององค์กรนั้นจะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย ๑ วิธี

๙.๓ การเข้าสู่ระบบสารสนเทศขององค์กรจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย

๙.๔ การเข้าสู่ระบบจากระยะไกล (Remote Access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ส่วนที่ ๔
การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Information Technology Access Control for The Third Party)

๑. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ให้เป็นไปอย่างมั่นคงปลอดภัยจึงได้กำหนดแนวทางปฏิบัติงานของหน่วยงานภายนอก อาทิ การพัฒนาระบบ การใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก ดังนี้

๒. แนวทางปฏิบัติ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จะพิจารณา หรือมอบหมายเจ้าหน้าที่ที่เกี่ยวข้องพิจารณาความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผลของหน่วยงานภายนอก และมอบผู้ดูแลระบบพิจารณาแนวทางรองรับในการแก้ไขปัญหาที่เหมาะสมและเป็นไปได้ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

๒.๒ การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

๒.๒.๑ บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติ/อนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดต่างๆ ดังนี้

๒.๒.๑.๑ เหตุผลในการขอใช้

๒.๒.๑.๒ ระยะเวลาในการใช้

๒.๒.๑.๓ ความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๒.๒.๑.๔ รหัสอ้างอิง เช่น MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

๒.๒.๑.๕ การป้องกันและความรับผิดชอบในเรื่องการเปิดเผยข้อมูล โดยจะไม่เปิดเผยข้อมูลใดๆ ขององค์กรหากไม่ได้รับอนุญาตจากผู้บริหารเป็นลายลักษณ์อักษร

๒.๒.๒ เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกจะต้องกำหนดการใช้งานให้เฉพาะบุคคลที่จำเป็นเท่านั้น โดยให้หน่วยงานภายนอกมีหนังสือระบุชื่อเป็นลายลักษณ์อักษร หรือมีหนังสือสัญญารับรองไว้

๒.๒.๓ องค์กรมีสิทธิ์ในการตรวจสอบการปฏิบัติตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจได้ว่าองค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

ส่วนที่ ๕
การป้องกันระบบฐานข้อมูล
(Database System Protection)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบฐานข้อมูลสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบฐานข้อมูลส่วนกลางขององค์กรได้อย่างถูกต้อง

๒. กระบวนการหลักในการควบคุมการเข้าถึงระบบฐานข้อมูล

๒.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลจะมีการควบคุมการเข้าออกสถานที่ที่รัดกุม และอนุญาตให้เฉพาะผู้มีสิทธิและหน้าที่เข้าใช้งานเท่านั้น

๒.๒ ผู้ดูแลระบบ จะมีการกำหนดสิทธิ์การเข้าถึงระบบฐานข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๓ ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบฐานข้อมูลได้

๓. การควบคุมการเข้าถึงระบบฐานข้อมูล

๓.๑ ผู้ดูแลระบบ มีหน้าที่ตรวจสอบ อนุมัติ และ/หรือการให้สิทธิ์ในการใช้งานระบบให้แก่ผู้ใช้

๓.๒ เจ้าของฐานข้อมูล และ/หรือ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบฐานข้อมูลต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๓.๓ ผู้ใช้งานจะได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบฐานข้อมูลและ/หรือ เจ้าของระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลเท่านั้น

๔. การบริหารจัดการการเข้าถึงระบบสารสนเทศของผู้ใช้

๔.๑ มีการกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูล โดยผู้ดูแลระบบจะให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และจะมีการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น ทั้งนี้จะมีการทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๔.๒ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

๔.๒.๑ ผู้ดูแลระบบ ที่รับผิดชอบระบบฐานข้อมูลนั้น ๆ จะกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลแต่ละระบบ แยกตามหน้าที่ที่รับผิดชอบ รวมทั้งรับผิดชอบการเปลี่ยนแปลง และการยกเลิกรหัสผ่านของเจ้าหน้าที่

๔.๒.๒ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

๔.๒.๒.๑ ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้นๆ

๔.๒.๒.๒ ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๔.๒.๒.๓ ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๔.๒.๒.๔ ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๔.๓ การบริหารจัดการการเข้าถึงระบบฐานข้อมูลตามระดับชั้นความลับ

๔.๓.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของฐานข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๔.๓.๒ เจ้าของข้อมูล ควรจะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๔.๓.๓ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๔.๓.๔ กรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๔.๓.๕ ผู้ดูแลระบบควรมีการป้องกันการเข้าถึงฐานข้อมูล และระบบจัดการฐานข้อมูลได้เฉพาะจากไอพีที่กำหนด จากผู้ใช้งานที่มีสิทธิเข้าถึงและที่ได้รับอนุญาตเท่านั้น

๔.๓.๖ มีการตรวจสอบ และปิดกั้นไอพีที่มีพฤติกรรม น่าสงสัยไม่ให้สามารถเข้าถึงระบบฐานข้อมูลได้

๔.๓.๗ มีการตรวจสอบการร้องขอการเข้าถึงระบบฐานข้อมูลที่น่าสงสัย เช่น มีลักษณะการร้องขอการเข้าถึงแบบซ้ำซ้อน อย่างต่อเนื่อง (Brute Force) และควรมีการดำเนินการป้องกันพฤติกรรมการเข้าถึงที่ไม่ใช่การกระทำจากมนุษย์ (ReCAPTCHA) เป็นต้น

๕. การควบคุมการเข้าใช้งานระบบจากภายนอก

การควบคุมดูแลรักษาความปลอดภัยการใช้งานระบบฐานข้อมูล โดยการเข้าใช้งานจากภายนอกจะต้องดำเนินการตามแนวทางปฏิบัติดังนี้

๕.๑ วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ระบบฐานข้อมูลได้จากระยะไกล (Remote Access) ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อน

และมีการควบคุมอย่างเข้มงวดโดยผู้ดูแลระบบ ทั้งนี้ผู้ใช้ต้องปฏิบัติตามมาตรฐานการรักษาความปลอดภัยที่เป็นวิธีการที่เป็นมาตรฐานสากลอย่างเคร่งครัด

๕.๒ ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐาน/เหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ที่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มอบหมายก่อน

๕.๓ ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ผ่านระบบไฟร์วอลล์ (Firewall)

๕.๔ การอนุญาตให้ผู้ใช้เข้าสู่ระบบฐานข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นจึงไม่ควรเปิดพอร์ตที่ไม่ได้ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวจะมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว

๕.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบฐานข้อมูลจากระยะไกลต้องผ่านช่องทางที่ปลอดภัยและทำการเข้ารหัสที่องค์กรกำหนดไว้เท่านั้น เช่น ช่องทางเครือข่ายเสมือนส่วนตัว (VPN) และช่องทางดังกล่าวจะมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๖. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

๖.๑ ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

๖.๑.๑ การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้ (Username/Identification) โดยการพิสูจน์ยืนยันตัวตน (Authentication) ร่วมกับการใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ด หรือการใช้ USB token ที่มีความสามารถ PKI หรือการใช้ Biometric Authentication เป็นต้น

๖.๒ การเข้าสู่ระบบฐานข้อมูลขององค์กรนั้นจะต้องผ่านวิธีการในการรักษาความปลอดภัยไม่น้อยกว่า ๒ ขั้นตอน (Two Factor Authentication)

ส่วนที่ ๖
การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
(Use of Personal Computer)

๑. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กรให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

๒. การใช้งานทั่วไป

๒.๑ เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ ผู้ใช้ ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร

๒.๒ ผู้ใช้เครื่องคอมพิวเตอร์เป็นผู้รับผิดชอบต่อโปรแกรมที่ติดตั้ง โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย

๒.๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคลจะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

๒.๔ ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ซึ่งมีการปรับข้อมูลชื่อและชนิดของไวรัสให้ทันสมัยอยู่ตลอดเวลา

๒.๕ ไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่ และไม่ควรสร้าง short-cut บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์กร

๒.๖ ผู้ใช้ มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยจะต้องไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์ และไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ disk drive

๓. การควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑ ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๓.๒ ผู้ใช้ ควรตั้งใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) แนะนำเป็นแบบ Blank Screen เพื่อประหยัดพลังงาน โดยตั้งเวลาไม่เกิน ๑๕ นาที เพื่อให้เครื่องทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน ทั้งนี้ควรกำหนดรหัสผ่านเพื่อความปลอดภัยของข้อมูลก่อนเข้าสู่หน้าจอปรกติ

๓.๓ ในระหว่างเวลาพักกลางวันผู้ใช้ควรล็อคหน้าจอด้วยโปรแกรมรักษาจอภาพ (Screen Saver)และหลังเลิกงาน ผู้ใช้ ควรออกจากเครื่องคอมพิวเตอร์ (Shutdown)

๔. แนวทางปฏิบัติในการใช้รหัสผ่าน

๔.๑ ผู้ใช้ ห้ามบอกชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกันกับผู้อื่น

๕. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๕.๑ ผู้ใช้ ต้องทำการอัพเดทระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๕.๒ ผู้ใช้ มีหน้าที่รับผิดชอบในการดูแลติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์ของตน หรือที่ตนใช้งานอยู่

๕.๓ ผู้ใช้ ควรตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น handy drive ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๕.๔ ผู้ใช้ ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๕.๕ ผู้ใช้ ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลายถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๖. การสำรองข้อมูลและการกู้คืน

๖.๑ ผู้ใช้ ต้องรับผิดชอบในการสำรองข้อมูลสำคัญจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น Hard disk แบบติดตั้งภายนอก เป็นต้น

๖.๒ ผู้ใช้ มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

ส่วนที่ ๗
การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
(Use of Notebook Computer)

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกองค์กร เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์กรให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยงในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

๒. การใช้งานทั่วไป

๒.๑ เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ ผู้ใช้ ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร

๒.๒ ผู้ใช้เป็นผู้รับผิดชอบโปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาว่าเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์อื่นๆ หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

๒.๔ ผู้ใช้ ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๒.๕ ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

๒.๖ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

๒.๗ ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกโยนได้

๒.๘ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๒.๙ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่นปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๒.๑๐ ห้ามวางของทับบนหน้าจอและแป้นพิมพ์

๒.๑๑ การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๒.๑๒ ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard disk กำลังทำงาน

๒.๑๓ ไม่ควรใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น

๒.๑๔ ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส

๒.๑๕ ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

๒.๑๖ ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน เช่นในยานพาหนะที่กำลังเคลื่อนที่

๒.๑๗ การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๓. ความปลอดภัยทางด้านกายภาพ

๓.๑ ผู้ใช้ มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๓.๒ ผู้ใช้ ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

๓.๓ ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ

๔.๑ ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

๔.๒ ผู้ใช้ ควรกำหนดรหัสผ่านให้มีคุณภาพ ไม่สามารถเดาได้ง่าย โดยประกอบด้วยตัวอักษรและตัวเลขจำนวนไม่น้อยกว่า ๘ หลักโดยประมาณ

๔.๓ ผู้ใช้ ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ ๑๕ นาทีให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน แนะนำแบบ Blank Screen เพื่อประหยัดพลังงาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๔.๔ ผู้ใช้ ต้องทำการออกจากระบบ (Log out) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๕. แนวทางปฏิบัติในการใช้รหัสผ่าน

๕.๑ ผู้ใช้ ห้ามบอกชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตนให้ผู้อื่นทราบ

๖. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๖.๑ ผู้ใช้ ต้องทำการอัพเดทระบบปฏิบัติการเว็บบราวเซอร์ และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๖.๒ ห้ามมิให้ ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

๖.๓ หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่นๆ ได้

๗. การสำรองข้อมูลและการกู้คืน

๗.๑ ผู้ใช้ ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาโดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

๗.๒ ผู้ใช้ควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๗.๓ แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

๗.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

ส่วนที่ ๘
การใช้งานอินเทอร์เน็ต
(Use of the Internet)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และระเบียบกรมควบคุมมลพิษว่าด้วยเรื่องการใช้ระบบคอมพิวเตอร์และเครือข่ายกรมควบคุมมลพิษ พ.ศ. ๒๕๕๔ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กร ถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

๒.๑ ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Firewall IPS-IDS เป็นต้น ห้ามผู้ใช้ ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็น และทำการขออนุญาตจากผู้บริหารระดับสูง หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร แล้ว

๒.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

๒.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัส ก่อนการรับส่งข้อมูลทุกครั้ง

๒.๔ ผู้ใช้ จะถูกกำหนดสิทธิ์โดยผู้ดูแลระบบในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กรเป็นสำคัญ

๒.๕ ผู้ใช้ ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

๒.๖ ห้ามผู้ใช้ เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๒.๗ ผู้ใช้ ไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือ ภาพที่มีลักษณะอันลามกอนาจาร และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๒.๘ ผู้ใช้ ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๒.๙ ผู้ใช้ มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๒.๑๐ ผู้ใช้ ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่างๆ จากผู้ขาย ซึ่งต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๒.๑๑ การใช้งานเว็บบอร์ด (Web board) ขององค์กร ผู้ใช้ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์กร

๒.๑๒ ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร การทำลายความสัมพันธ์กับเจ้าหน้าที่ ทั้งในหน่วยงานและระหว่างหน่วยงาน

๒.๑๓ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ส่วนที่ ๙
การใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

๑. วัตถุประสงค์

การกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร เพื่อให้ผู้ใช้ให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด ซึ่งจะช่วยให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

๒.๑ ผู้ดูแลระบบ จะกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กร ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

๒.๒ ผู้ดูแลระบบ จะกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร

๒.๓ สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรกในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกแล้ว ควรเปลี่ยนรหัสผ่านในการใช้งานระบบโดยทันที

๒.๔ การกำหนดรหัสผ่านที่ดี ควรประกอบด้วยตัวอักษรและตัวเลขจำนวนไม่น้อยกว่า ๘ - ๑๐ หลักโดยประมาณ ทั้งนี้ขอให้ดูคำแนะนำการใช้งานแต่ละระบบประกอบด้วย

๒.๕ รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘x’ หรือ ‘o’ ในการพิมพ์แต่ละตัวอักษร

๒.๖ ผู้ดูแลระบบ ควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการล๊อกเอ้าท์ออกจากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

๒.๗ ผู้ใช้ ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์

๒.๘ ผู้ใช้ ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร

๒.๙ ผู้ใช้ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๒.๑๐ ผู้ใช้ ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น

๒.๑๑ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการออกจากระบบ (Log out) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ของตน

๒.๑๒ ผู้ใช้ ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

๒.๑๓ ผู้ใช้ ต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๒.๑๔ ผู้ใช้ ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

๒.๑๕ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อ หรือหัวเรื่องของจดหมายอิเล็กทรอนิกส์

๒.๑๖ ผู้ใช้ ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๒.๑๗ ผู้ใช้ ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๒.๑๘ ผู้ใช้ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ส่วนที่ ๑๐
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๒.๑ ผู้ใช้ ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับอนุญาตจากผู้บริหาร หรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ก่อนใช้งาน

๒.๒ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๒.๓ ผู้ดูแลระบบ จะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๒.๔ ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๒.๕ ผู้ดูแลระบบ ควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

๒.๖ ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (default) มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

๒.๗ ผู้ดูแลระบบ ควรเปลี่ยนค่า ชื่อ Log in และ รหัสผ่าน สำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบควรเลือกใช้ชื่อ Log in และ รหัสผ่าน ที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๒.๘ ผู้ดูแลระบบ ต้องกำหนดค่าการใช้ WEB หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ เพื่อช่วยให้ปลอดภัยมากยิ่งขึ้น

๒.๙ ผู้ดูแลระบบ ควรเลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ (Username) รหัสผ่าน(Password) ของผู้ใช้ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะ

อนุญาตเฉพาะอุปกรณ์ที่มี MAC address และชื่อผู้ใช้รหัสผ่าน ตามที่กำหนดไว้เท่านั้น ให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

๒.๑๐ ผู้ดูแลระบบ ควรจะมีการติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

๒.๑๒ ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย