

## นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ วิทยาลัยเทคนิคกำแพงเพชร

---

### 1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของวิทยาลัยเทคนิคกำแพงเพชร หรือต่อไปนี้อธิบายว่า “องค์กร” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน(Standard) แนวปฏิบัติ(Guideline) ขั้นตอนปฏิบัติ(Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

- 1.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล
- 1.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง
- 1.3 นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด
- 1.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด
- 1.5 นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปี หรือตามที่ระบบไว้ในเอกสาร “การตรวจสอบประเมินนโยบาย”

### 2. องค์ประกอบของนโยบาย

- 2.1 คำนิยาม
- 2.2 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- 2.3 การควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์
- 2.4 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- 2.5 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- 2.6 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพา
- 2.7 การใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์
- 2.8 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรแต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน(Standard) แนวทางปฏิบัติ(Guideline) และขั้นตอนวิธีการปฏิบัติ(Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

## คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **องค์กร** หมายถึง วิทยาลัยเทคนิคกำแพงเพชร
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร
- **งานศูนย์ข้อมูลสารสนเทศ** หมายถึง ฝ่ายงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร
- **หัวหน้างานศูนย์ข้อมูลสารสนเทศ** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร
- **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
- **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- **แนวทางปฏิบัติ (Guideline)** หมายถึง หมายถึงแนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- **ผู้ใช้** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ ดังนี้
  - **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงขององค์กร เช่น หัวหน้าหน่วยงานราชการ เป็นต้น
  - **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษา ระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
  - **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว และเจ้าหน้าที่ประจำโครงการขององค์กร
- **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่วิทยาลัยเทคนิคกำแพงเพชรอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
- **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ ระบบคอมพิวเตอร์ อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

- **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กรได้ เช่น ระบบ LAN, ระบบ Intranet, ระบบ Internet เป็นต้น
  - ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
  - ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
- **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
- **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace)** หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น
  - พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
  - พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)
  - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
  - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
  - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)
- **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- **ทรัพย์สิน** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

- จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น
- รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

## ส่วนที่ 1

### การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and environment security)

#### 1. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

#### 2. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

2.1 ภายในองค์กร ควรมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม อนุรักษ์ความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

2.2 ผู้บริหาร ควรกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานเครือข่ายไร้สาย(Wireless LAN coverage area) เป็นต้น

2.3 ผู้บริหาร ต้องกำหนดสิทธิ์ให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วนประกอบด้วย

2.3.1 จัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.3.2 ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”

2.3.3 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ 1 ครั้ง

#### 3. การควบคุมการเข้าออก อาคาร สถานที่

3.1 จัดทำเอกสารระบุสิทธิ์ของผู้ใช้ และ “หน่วยงานภายนอก” ในการเข้าถึงสถานที่ โดยแบ่งแยกได้ดังนี้

3.1.1 องค์กรต้องกำหนดสิทธิ์ ผู้ใช้ ที่มีสิทธิ์ผ่านเข้าออกและช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

- 3.1.2 การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)
- 3.1.3 บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในองค์กร
- 3.1.4 กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายเข้าบริเวณอาคาร เจ้าหน้าที่รักษาความปลอดภัยจะต้องลงบันทึกในแบบฟอร์มการเข้าออกในรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้อง
- 3.1.5 เจ้าหน้าที่ ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกได้ถูกต้อง
- 3.1.6 บุคคลภายนอกหรือผู้ติดต่อ ต้องคืนแบบฟอร์มการเข้าออกและบัตรผู้ติดต่อ(Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และ **ร่ำ**. ต้องตรวจสอบผู้ติดต่ออุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง
- 3.2 ผู้ใช้ จะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น
- 3.3 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้ ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่องค์กรออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

## ส่วนที่ 2

### การควบคุมการเข้าออกห้องศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (Computer Center Entry Control)

#### 1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์

#### 2. คำจำกัดความของผู้เกี่ยวข้อง

- 2.1 ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในกลุ่มสารสนเทศและเทคโนโลยี
- 2.2 เจ้าหน้าที่ หมายถึง เจ้าหน้าที่องค์กรที่มีสิทธิ์ในการเข้าออกสถานที่ อาหาร ห้อง ภายในองค์กร
- 2.3 ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของกลุ่มงานศูนย์ข้อมูลสารสนเทศ

#### 3. บทบาทและความรับผิดชอบ

- 3.1 หัวหน้างานศูนย์ข้อมูลสารสนเทศ
  - 3.1.1 อนุมัติสิทธิ์เข้าออกพื้นที่ใช้งานศูนย์ข้อมูลสารสนเทศ
  - 3.1.2 อนุมัติกระบวนการควบคุมการเข้าออก กลุ่มงานศูนย์ข้อมูลสารสนเทศ
- 3.2 ผู้ดูแลระบบ
  - 3.2.1 ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในงานศูนย์ข้อมูลสารสนเทศให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของงานศูนย์ข้อมูลสารสนเทศ อย่างเคร่งครัด
  - 3.2.2 ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกงานศูนย์ข้อมูลสารสนเทศ ต้องติดบัตรผู้ติดต่อ (Visitor) หรือบัตรประจำตัวขององค์กรเท่านั้น

#### 4. กระบวนการควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์

- 4.1 ผู้ดูแลระบบ งานศูนย์ข้อมูลสารสนเทศ และเจ้าหน้าที่ องค์กร มีแนวทางปฏิบัติ ดังนี้
  - 4.1.1 ผู้ดูแลระบบ ควรจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย(Server Zone) ส่วนเครื่องพิมพ์(Printer Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น
  - 4.1.2 กลุ่มงานศูนย์ข้อมูลสารสนเทศ ต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกกลุ่มสารสนเทศและเทคโนโลยี โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการ



- บันทึก “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น
- 4.1.3 สิทธิ์ในการเข้าออกห้องต่าง ๆ ภายในงานศูนย์ข้อมูลสารสนเทศ ของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจากหัวหน้างานศูนย์ข้อมูลสารสนเทศ โดยผ่านกระบวนการลงทะเบียนที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบ” เป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในกลุ่มสารสนเทศและเทคโนโลยี
- 4.1.4 เจ้าหน้าที่ทุกคนต้องทำบัตรผ่านเพื่อใช้ในการเข้าออกกลุ่มงานศูนย์ข้อมูลสารสนเทศ ตามกระบวนการที่ระบุในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบ”
- 4.1.5 ต้องจัดทำระบบเก็บบันทึกการเข้าออกกลุ่มงานศูนย์ข้อมูลสารสนเทศ ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”
- 4.1.6 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกกลุ่มงานศูนย์ข้อมูลสารสนเทศ ก็ต้องมีการควบคุมอย่างรัดกุม
- 4.1.7 การเข้าถึงกลุ่มงานศูนย์ข้อมูลสารสนเทศ และห้องคอมพิวเตอร์ ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”
- 4.1.8 เจ้าหน้าที่งานศูนย์ข้อมูลสารสนเทศ ทุกคนต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้าออกทุกคนต้องกรอกแบบฟอร์มดังกล่าว
- 4.2 ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติดังนี้
- 4.2.1 ผู้ติดต่อจากหน่วยงานภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”
- 4.2.2 ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน
- 4.2.3 ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในกลุ่มงานศูนย์ข้อมูลสารสนเทศ
- 4.2.4 ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าออกกลุ่มงานศูนย์ข้อมูลสารสนเทศ ได้ด้วยบัตรผู้ติดต่อ “Visitor” โดยสิทธิ์จะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าปฏิบัติงานภายในกลุ่มสารสนเทศและเทคโนโลยี
- 4.2.5 พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้าออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา
- 4.2.6 ผู้ติดต่อจากหน่วยงานภายนอก สามารถนำผู้ติดตามเข้ามาช่วยงานได้ไม่เกินครั้งละ 2 คน และทุกคนจะต้องถูกบันทึกการเข้าออกเช่นกัน

- 4.2.7 ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรและตรวจสอบแบบฟอร์มการขออนุญาตเข้าออกว่ามีเจ้าหน้าที่ลงนามอนุญาตแล้วทุกครั้ง
- 4.2.8 เจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มการขออนุญาตเข้าออกและตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง
- 4.2.9 เจ้าหน้าที่กลุ่มงานศูนย์ข้อมูลสารสนเทศ ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้าออกกับเจ้าหน้าที่รักษาความปลอดภัย เป็นประจำทุกเดือน
- 4.2.10 เจ้าหน้าที่กลุ่มงานศูนย์ข้อมูลสารสนเทศ ต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ 2 ครั้ง

### ส่วนที่ 3

#### การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control)

#### 1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรได้อย่างถูกต้อง

#### 2. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

- 2.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น
- 2.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
- 2.3 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้
- 2.4 ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ
- 2.5 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหากเกิดขึ้น

#### 3. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

- 3.1 ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ได้แก่ ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน
- 3.2 เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น
- 3.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

#### 4. การบริหารจัดการการเข้าถึงของผู้ใช้

- 4.1 การลงทะเบียนเจ้าหน้าที่ใหม่ของกลุ่มงานศูนย์ข้อมูลสารสนเทศ ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการทำงานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น
- 4.2 กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
- 4.3 ผู้ใช้ ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด
- 4.4 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่
  - 4.4.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติ ตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
  - 4.4.2 การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
  - 4.4.3 กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา
    - 4.4.3.1 ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ
    - 4.4.3.2 ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
    - 4.4.3.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
    - 4.4.3.4 ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น
- 4.5 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ
  - 4.5.1 ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

- 4.5.2 เจ้าของข้อมูล จะต้องมีการสอบถามความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 4 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- 4.5.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทขึ้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล
- 4.5.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น
- 4.5.5 ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
- 4.5.6 ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

## 5. การบริหารจัดการการเข้าถึงระบบเครือข่าย

- 5.1 ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ และการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ
- 5.2 การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบเทคโนโลยีสารสนเทศและการสื่อสารก่อนที่จะสามารถใช้งานได้ในทุกกรณี
- 5.3 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
- 5.4 ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน
- 5.5 ผู้ดูแลระบบ ควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้
- 5.6 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง
- 5.7 ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กร ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

- 5.8 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
- 5.9 การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง
- 5.10 IP address ภายในของระบบงานเครือข่ายภายในขององค์กร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันมิให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย
- 5.11 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- 5.12 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น
- 5.13 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่งานศูนย์ข้อมูลสารสนเทศ เท่านั้น

## 6. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

- 6.1 ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน
- 6.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่มีพบการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที
- 6.3 ต้องเปิดให้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย
- 6.4 ควรดำเนินการติดตั้งอัปเดตระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น
- 6.5 ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา
- 6.6 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่งานศูนย์ข้อมูลสารสนเทศ เท่านั้น

## 7. การบริหารจัดการการบันทึกและตรวจสอบ

- 7.1 ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน
- 7.2 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
- 7.3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

## 8. การควบคุมการเข้าใช้งานระบบจากภายนอก

งานศูนย์ข้อมูลสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

- 8.1 การเข้าสู่ระบบจากระยะไกล (Remote access) เข้าสู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กร ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์กร การควบคุมบุคคลที่เข้าสู่ระบบขององค์กรจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน
- 8.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยี ก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด
- 8.3 ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ
- 8.4 ต้องมีการควบคุมพอร์ต(Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้าองค์กรนั้น ต้องดูแลและการจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น
- 8.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรมีเปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

## 9. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

- 9.1 ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ
  - 9.1.1 การแสดงตัวตน(Identification) คือขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้ (Username)

- 9.1.2 การพิสูจน์ยืนยันตัวตน(Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน>Password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB token ที่มีความสามารถ PKI เป็นต้น
- 9.2 การเข้าสู่ระบบสารสนเทศขององค์กรนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี
- 9.3 การเข้าสู่ระบบสารสนเทศขององค์กรจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย
- 9.4 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

#### ส่วนที่ 4

#### การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third party access control)

##### 1. วัตถุประสงค์

การใช้บริการจากหน่วยภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบการใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

##### 2. แนวทางปฏิบัติ

- 2.1 หัวหน้างานศูนย์ข้อมูลสารสนเทศ ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้
- 2.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก
- 2.2.1 บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากหัวหน้างานศูนย์ข้อมูลสารสนเทศ
- 2.2.2 จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร 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 หน่วยงานภายนอก ที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กร หรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญา ต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ
- 2.2.4 องค์กร ควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการศึกษาควบคุมภายในของ หน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการ สื่อสารที่เข้าไปปฏิบัติงาน
- 2.2.5 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนาม ในสัญญาไม่เปิดเผยข้อมูล
- 2.2.6 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของ องค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
- 2.2.7 องค์กรมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการ สื่อสารเพื่อให้มั่นใจว่า องค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น
- 2.2.8 ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการ ปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตาม ขอบเขตที่ได้กำหนดไว้

## ส่วนที่ 5

### การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer)

#### 1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กร ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

#### 2. การใช้งานทั่วไป

- 2.1 เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้ ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร
- 2.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- 2.3 ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร
- 2.4 การตั้งชื่อเครื่องคอมพิวเตอร์(Computer name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ขององค์กรเท่านั้น
- 2.5 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการโดยเจ้าหน้าที่ของกลุ่มงานศูนย์ข้อมูลสารสนเทศ เท่านั้น
- 2.6 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
- 2.7 ไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่
- 2.8 ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์กร
- 2.9 ผู้ใช้ มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติ ดังนี้
  - 2.9.1 ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
  - 2.9.2 ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

#### 3. การควบคุมการเข้าถึงระบบปฏิบัติการ

- 3.1 ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ
- 3.2 ผู้ใช้ ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที เพื่อให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

- 3.3 ผู้ใช้ ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน
- 3.4 ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Log-out ออกจากเครื่องคอมพิวเตอร์หรือ ล็อกหน้าจอด้วยโปรแกรม Screen Saver

#### 4. แนวทางปฏิบัติในการใช้รหัสผ่าน

- 4.1 ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

#### 5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

- 5.1 ผู้ใช้ ต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
- 5.2 ผู้ใช้ มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์
- 5.3 ผู้ใช้ ควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์
- 5.4 ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน
- 5.5 ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

#### 6. การสำรองข้อมูลและการกู้คืน

- 6.1 ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น
- 6.2 ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
- 6.3 ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

## ส่วนที่ 6

### การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Use of Notebook Computer)

#### 1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกองค์กร เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์กรให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยง ในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

#### 2. การใช้งานทั่วไป

- 2.1 เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร
- 2.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- 2.3 การตั้งชื่อเครื่องคอมพิวเตอร์ (computer name) แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่กลุ่มงานศูนย์ข้อมูลสารสนเทศ เท่านั้น
- 2.4 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจสอบจะต้องดำเนินการโดยเจ้าหน้าที่ของกลุ่มงานศูนย์ข้อมูลสารสนเทศ เท่านั้น
- 2.5 ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- 2.6 ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม
- 2.7 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
- 2.8 ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจ็อบโยนได้
- 2.9 การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
- 2.10 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
- 2.11 ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์
- 2.12 การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
- 2.13 ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

- 2.14 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น
- 2.15 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ควรอยู่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
- 2.16 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น
- 2.17 ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
- 2.18 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

### 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 ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา
- 4.2 ผู้ใช้ควรกำหนดรหัสผ่านให้มีคุณภาพอย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
- 4.3 ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน
- 4.4 ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

### 5. แนวทางปฏิบัติในการใช้รหัสผ่าน

- 5.1 ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

### 6. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

- 6.1 ผู้ใช้ ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

- 6.2 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา
- 6.3 หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

## 7. การสำรองข้อมูลและการกู้คืน

- 7.1 ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล
- 7.2 ผู้ใช้ควรจะทำเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล
- 7.3 แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ
- 7.4 แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้นำไปใช้งานได้อีก

## ส่วนที่ 7 การใช้งานอินเทอร์เน็ต (Use of the Internet)

### 1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็น การป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ชัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

### 2. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

- 2.1 ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IP-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-Up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการศูนย์ เทคโนโลยี ฯ เป็นลายลักษณ์อักษรแล้ว
- 2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่อ อินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำ การอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่
- 2.3 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
- 2.4 ผู้ใช้ต้องไม่ใช่เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการ เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
- 2.5 ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของ เครือข่ายและความปลอดภัยทางข้อมูลขององค์กร
- 2.6 ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร
- 2.7 ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต
- 2.8 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มี ลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

- 2.9 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
- 2.10 ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บน อินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
- 2.11 ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
- 2.12 การใช้งานเว็บบอร์ด (Web Board) ขององค์กร ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็น ความลับขององค์กร
- 2.13 ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช่ข้อความที่ยั่ว ุให้ร้าย ที่จะทำให้เกิดความเสียหายต่อ ชื่อเสียงขององค์กร การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ
- 2.14 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดย บุคคลอื่น ๆ



## ส่วนที่ 8

### การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

#### 1. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

#### 2. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

- 2.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กร ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น
- 2.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานใหม่และรหัสผ่าน สำหรับการเข้าใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร
- 2.3 สำหรับผู้ใช้งานใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที
- 2.4 การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
- 2.5 รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ 0 ในการพิมพ์แต่ละตัวอักษร
- 2.6 ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน 3 ครั้ง
- 2.7 ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการ Logout ออกจากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง
- 2.8 ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
- 2.9 ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน
- 2.10 ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่

แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร

- 2.11 ข้อห้าม ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
- 2.12 ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น
- 2.13 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
- 2.14 ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น
- 2.15 ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
- 2.16 ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์
- 2.17 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
- 2.18 ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
- 2.19 ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์
- 2.20 ข้อควรระวัง ผู้ใช้ไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

## ส่วนที่ 9 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

### 1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีกาทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

### 2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

- 2.1 ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการวิทยาลัยเทคนิคกำแพงเพชร อย่างเป็นทางการ
- 2.2 ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
- 2.3 ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนระบบเครือข่ายไร้สาย
- 2.4 ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกระยะที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
- 2.5 ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น
- 2.6 ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน
- 2.7 ผู้ดูแลระบบ ควรเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดายากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
- 2.8 ผู้ดูแลระบบต้องกำหนดค่าใช้ Web หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น
- 2.9 ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะ

อุปกรณ์ที่มี MAC Address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

- 2.10 ผู้ดูแลระบบควรมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร
- 2.11 ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี
- 2.12 ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

## การตรวจสอบและประเมินนโยบาย

การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่

บันทึกการเข้าออกพื้นที่

การแบ่งส่วนจัดวางอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร

## การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

### วิธีการบริหารจัดการรหัสผ่านของเจ้าหน้าที่ให้มีความมั่นคงปลอดภัย

กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น ต้องให้พนักงานลงนามเพื่อเก็บรักษาบัตรรหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ กำหนดรหัสผ่านเริ่มต้นให้กับพนักงานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับพนักงานต้องเป็นไปอย่างปลอดภัย

### การตรวจสอบและประเมินความเสี่ยง

การรักษาความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลจำเป็นต้องคำนึงถึงหลายด้านหลายมิติ แต่ ละด้านก็มีความจำเป็นในการตรวจสอบและประเมินความเสี่ยงแตกต่างกัน ซึ่งสามารถแยกประเภทได้ ดังต่อไปนี้

1. การตรวจสอบและประเมินนโยบาย
2. การตรวจสอบและประเมินความพร้อมทางด้านโครงสร้างองค์กร
3. การตรวจสอบและประเมินด้านการบริหารสินทรัพย์(ข้อมูลและระบบข้อมูล)
4. การตรวจสอบและประเมินด้านบุคลากร
5. การตรวจสอบและประเมินด้านกายภาพและสิ่งแวดล้อม
6. การตรวจสอบและประเมินด้านการสื่อสารและการปฏิบัติการ
7. การตรวจสอบและประเมินการควบคุมการเข้าถึง
8. การตรวจสอบและประเมินด้านการพัฒนาระบบ จัดซื้อจัดหาระบบและการดูแลระบบ
9. การตรวจสอบและประเมินด้านความพร้อมรับมือกับเหตุการณ์
10. การตรวจสอบและประเมินด้านผลกระทบและความต่อเนื่องของการปฏิบัติการกิจ
11. การตรวจสอบและประเมินด้านการปฏิบัติตามกฎหมายและสัญญา

เมื่อได้มีการประเมินความเสี่ยงด้านต่าง ๆ แล้ว ควรดำเนินการจัดลำดับความสำคัญของความเสี่ยงนั้น และค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยงนั้น (Control) พร้อมทั้งข้อดีข้อเสียของวิธีการเหล่านั้นเพื่อให้ ผู้บริหารขององค์กรตัดสินใจ ที่จะเลือกวิธีการดำเนินการเพื่อลดความเสี่ยงหรือเลือกที่จะยอมรับความเสี่ยงนั้น เมื่อเลือกวิธีการดำเนินการเพื่อลดความเสี่ยง (Control Selection) แล้ว ผู้บริหารควรจัดสรรทรัพยากรอย่าง เพียงพอเพื่อดำเนินการ แนวทางการดำเนินการเพื่อลดความเสี่ยงซึ่งมีหลายวิธี สามารถแบ่งได้เป็นสามรูปแบบ คือ การเลือกใช้เทคโนโลยี (Technology) การปรับเปลี่ยนกระบวนการ (Procedure) และการกำหนดให้ เจ้าหน้าที่ดำเนินการปฏิบัติ (Person)

สำหรับการเลือกใช้วิธีการนำเทคโนโลยีมาใช้ในการลดความเสี่ยงเพื่อเพิ่มความมั่นคงปลอดภัยให้กับ ข้อมูลและระบบข้อมูลเป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ Firewall มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้อุปกรณ์ สมาร์ทการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอกองค์กร เป็นต้น

สำหรับการเลือกใช้วิธีการปรับเปลี่ยนกระบวนการ (Procedure) ก็อาจจำเป็นต้องมีการออกแบบ กระบวนการใหม่ที่รัดกุมและสามารถรักษาความมั่นคงปลอดภัยของข้อมูลได้ดีขึ้น เมื่อออกแบบกระบวนการ ใหม่แล้วควรมีการพิจารณาหรือความเหมาะสม ความเป็นไปได้ และผู้บริหารจะต้องเป็นผู้อนุมัติให้มีการบังคับ ใช้กระบวนการใหม่นั้น โดยอาจจำเป็นต้องมีการประชาสัมพันธ์ให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งอาจ จำเป็นต้องมีการจัดฝึกอบรมเจ้าหน้าที่ที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามกระบวนการใหม่ได้อย่างราบรื่น และมีประสิทธิภาพ

\*\*\*\*\*