

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ กองประเมินผลกระทบต่อสุขภาพ

๑. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกองประเมินผลกระทบต่อสุขภาพ หรือต่อไปนี้จะเรียกว่า “องค์กร” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ กองประเมินผลกระทบต่อสุขภาพจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน(Standard) แนวปฏิบัติ(Guideline) ขั้นตอนปฏิบัติ(Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๑.๑ การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และมีการปรับปรุงอย่างต่อเนื่อง

๑.๓ นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๔ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๑.๕ นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี หรือตามที่ระบุไว้ในเอกสาร “การตรวจสอบประเมินนโยบาย”

๒. องค์ประกอบของนโยบาย

๒.๑ คำนิยาม

๒.๒ การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

๒.๓ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพา

๒.๔ การใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์

๒.๕ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน(Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ(Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบ

เทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรนี้ จัดเป็นมาตรฐาน ด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งเจ้าหน้าที่ขององค์กร และหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- ❖ **องค์กร** หมายถึง กองประเมินผลกระทบต่อสุขภาพ
- ❖ **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร
- ❖ **กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร** หมายถึง กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายขององค์กร
- ❖ **หัวหน้ากลุ่มงานข้อมูลสารสนเทศและการสื่อสาร** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- ❖ **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร
- ❖ **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์ หรือเป้าหมาย
- ❖ **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
- ❖ **แนวทางปฏิบัติ (Guideline)** หมายถึง หมายถึงแนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
- ❖ **ผู้ใช้** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ดังนี้
 - **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงขององค์กร เช่น หัวหน้าหน่วยงานราชการ เป็นต้น
 - **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรม เครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
 - **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการขององค์กร
- ❖ **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่กองประเมินผลกระทบต่อสุขภาพอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
- ❖ **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

- ❖ **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
- ❖ **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- ❖ **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้ เช่น ระบบ LAN, ระบบ Intranet, ระบบ Internet เป็นต้น
 - ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
 - ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ 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 และคอมพิวเตอร์พกพา (Notebook) ที่ประจำโต๊ะทำงาน
 - พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)
 - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
 - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
 - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)
- ❖ **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ 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, POP๓ และ IMAP เป็นต้น

- ❖ **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- ❖ **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ส่วนที่ ๑

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and environment security)

๑. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๒. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๒.๑ ภายในองค์กร ควรมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

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

๒.๓ ผู้บริหาร ต้องกำหนดสิทธิ์ให้กับเจ้าหน้าที่ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

๒.๓.๑ จัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓.๒ ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”

๒.๓.๓ จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๒

การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

(Use of Personal Computer)

๑. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กร ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

๒. การใช้งานทั่วไป

- ๒.๑ เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร
- ๒.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร เป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- ๒.๓ ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร
- ๒.๔ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ขององค์กรเท่านั้น
- ๒.๕ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการโดยเจ้าหน้าที่ของกลุ่มงานข้อมูลสารสนเทศและการสื่อสารเท่านั้น
- ๒.๖ ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
- ๒.๗ ไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่
- ๒.๘ ผู้ใช้งานควรบันทึกข้อมูลต่างๆ ไว้ที่ Drive อื่นๆ ยกเว้น Drive C และหน้า Desktop
- ๒.๙ ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญขององค์กร
- ๒.๑๐ ผู้ใช้บริการทุกคนต้องผ่านการพิสูจน์ตัวตนจากระบบ กรมนามัย เมื่อจะเข้าใช้งานระบบ
- ๒.๑๑ การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย ผู้ใช้บริการต้องปฏิบัติตามระเบียบกรมนามัย ว่าด้วยการใช้งานระบบคอมพิวเตอร์ พ.ศ. ๒๕๕๑
- ๒.๑๒ ผู้ใช้ มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติ ดังนี้
 - ๒.๑๒.๑ ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
 - ๒.๑๒.๒ ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๓. การควบคุมการเข้าถึงระบบปฏิบัติการ

- ๓.๑ ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

- ๓.๒ ผู้ใช้ ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที เพื่อให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน
- ๓.๓ ผู้ใช้ ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน
- ๓.๔ ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Logout ออกจากเครื่องคอมพิวเตอร์หรือล็อกหน้าจอด้วยโปรแกรม Screen Saver

๔. แนวทางปฏิบัติในการใช้รหัสผ่าน

- ๔.๑ ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๕. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

- ๕.๑ ผู้ใช้ มีหน้าที่รับผิดชอบในการ Update โปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ
- ๕.๒ ผู้ใช้ มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์
- ๕.๓ ผู้ใช้ ควรตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Thumb Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์
- ๕.๔ ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน
- ๕.๕ ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๖. การสำรองข้อมูลและการกู้คืน

- ๖.๑ ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น
- ๖.๒ ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
- ๖.๓ ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

ส่วนที่ ๓

การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

(Use of Notebook Computer)

๑. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกองค์กร เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์กรให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยงในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

๒. การใช้งานทั่วไป

- ๒.๑ เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร
- ๒.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กร เป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- ๒.๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (computer name) แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร เท่านั้น
- ๒.๔ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจสอบจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มงานข้อมูลสารสนเทศและการสื่อสารเท่านั้น
- ๒.๕ ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- ๒.๖ ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม
- ๒.๗ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
- ๒.๘ ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้
- ๒.๙ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
- ๒.๑๐ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
- ๒.๑๑ ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์
- ๒.๑๒ การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
- ๒.๑๓ ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

- ๒.๑๔ ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น
- ๒.๑๕ ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ควรอยู่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส
- ๒.๑๖ ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรศัพท์มือถือ ไมโครเวฟ ตู้เย็น เป็นต้น
- ๒.๑๗ ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
- ๒.๑๘ การเชื่อมต่อความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้าม เช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

๓. ความปลอดภัยทางด้านกายภาพ

- ๓.๑ ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
- ๓.๒ ผู้ใช้ ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ
- ๓.๓ ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ

- ๔.๑ ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา
- ๔.๒ ผู้ใช้ควรกำหนดรหัสผ่านให้มีคุณภาพอย่างน้อยตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
- ๔.๓ ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน
- ๔.๔ ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๕. แนวทางปฏิบัติในการใช้รหัสผ่าน

- ๕.๑ ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๖. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

- ๖.๑ ผู้ใช้ มีหน้าที่รับผิดชอบในการ Update โปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ
- ๖.๒ ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา
- ๖.๓ หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่นๆ ได้

๗. การสำรองข้อมูลและการกู้คืน

- ๗.๑ ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล
- ๗.๒ ผู้ใช้ควรจะได้เก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล
- ๗.๓ แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ
- ๗.๔ แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้นำไปใช้งานได้อีก

ส่วนที่ ๔

การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

๑. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

- ๒.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กรให้เหมาะสมกับการใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น
- ๒.๒ ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร
- ๒.๓ สำหรับผู้ใช้งานใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที
- ๒.๔ การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”
- ๒.๕ รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ ○ ในการพิมพ์แต่ละตัวอักษร
- ๒.๖ ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน ๓ ครั้ง
- ๒.๗ ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการ Logout ออกจากหน้าจอจัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง
- ๒.๘ ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
- ๒.๙ ผู้ใช้ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน
- ๒.๑๐ ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์

หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร

- ๒.๑๑ ห้าม ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน
- ๒.๑๒ ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น
- ๒.๑๓ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
- ๒.๑๔ ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น
- ๒.๑๕ ผู้ใช้ไม่ควรเปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
- ๒.๑๖ ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์
- ๒.๑๗ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
- ๒.๑๘ ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
- ๒.๑๙ ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์
- ๒.๒๐ ข้อควรระวัง ผู้ใช้ไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ส่วนที่ ๕

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าเป็นผู้อนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

- ๒.๑ ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร จะต้องได้รับการพิจารณาอนุญาตจากหัวหน้ากลุ่มงานข้อมูลสารสนเทศและการสื่อสาร
- ๒.๒ ผู้ดูแลระบบ ต้องทำการกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
- ๒.๓ ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อกับระบบเครือข่ายไร้สาย
- ๒.๔ ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
- ๒.๕ ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น
- ๒.๖ ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน
- ๒.๗ ผู้ดูแลระบบ ควรเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
- ๒.๘ ผู้ดูแลระบบต้องกำหนดค่าใช้ Web หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น
- ๒.๙ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิ์ในการใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง
- ๒.๑๐ ผู้ดูแลระบบควรมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร
- ๒.๑๑ ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

๒.๑๒ ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย