บริษัท จีเอฟพีที จำกัด (มหาชน)

นโยบายการรักษาความมั่นคงปลอดภัย
ระบบเทคโนโลยีสารสนเทศและการสื่อสาร
(Information Technology Security Policy)

สารบัญ

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร
บริษัท จีเอฟพีที จำกัด (มหาชน)

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท จีเอฟพีที จำกัด (มหาชน) หรือต่อไปนี้เรียกว่า “องค์กร” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารและมีการปรับปรุงอย่างต่อเนื่อง

1.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กรตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.4 เพื่อเป็นการป้องกันการกระทำผิดตามกฎหมาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560, กฎหมายและระเบียบอื่น ๆ ที่เกี่ยวข้อง

1.5 นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2. องค์ประกอบของนโยบาย

คำนิยาม
การควบคุมการรักษาความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
การควบคุมการเข้า-ออกห้อง Data Center
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
การควบคุมการใช้งานเครื่องคอมพิวเตอร์แบบพกพา
การควบคุมการใช้งานระบบอินเตอร์เน็ต
การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
การควบคุมระบบสำรอง

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของ มาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

ดังนั้นจึงจัดทำนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรฉบับนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ต้องได้รับความร่วมมือในการปฏิบัติตามจากทุกหน่วยงานอย่างต่อเนื่อง มีการตรวจสอบ และปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว คณะผู้บริหารจึงหวังเป็นอย่างยิ่งว่า นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับนี้จะเป็นเครื่องมือและแนวทางปฏิบัติให้กับผู้ใช้ ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรต่อไป

นพ.อนันต์ ศิริมงคลเกษม
ประธานกรรมการบริหาร
บริษัท จีเอฟพีที จำกัด (มหาชน)

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

องค์กร

หมายถึง บริษัท จีเอฟพีที จำกัด (มหาชน) และบริษัทย่อย

ผู้บังคับบัญชา

หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร

กลุ่มสารสนเทศและเทคโนโลยี

หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ และเครือข่ายภายในองค์กร

ผู้อำนวยการสารสนเทศและเทคโนโลยี

หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

การรักษาความมั่นคงปลอดภัย

หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

มาตรฐาน (Standard)

หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

แนวทางปฏิบัติ (Guideline)

หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ขั้นตอนวิธีการปฏิบัติ (Procedure)

หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

ผู้ใช้

หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งองค์กรกำหนดไว้ ดังนี้

ผู้บริหาร

หมายถึง ผู้มีอำนาจบริหารในระดับสูงขององค์กร เช่น ผู้อำนวยการฝ่ายฯ เป็นต้น

ผู้ดูแลระบบ

หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

เจ้าหน้าที่

หมายถึง พนักงาน ลูกจ้างชั่วคราว ลูกจ้างประจำ และเจ้าหน้าที่ประจำขององค์กร

หน่วยงานภายนอก

หมายถึง องค์กรหรือหน่วยงานภายนอกที่องค์กร อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ 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 อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System)

หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กรได้ เช่น ระบบ LAN, ระบบ Intranet, ระบบ Internet เป็นต้น

ระบบ LAN และ ระบบ Intranet

หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบ Internet

หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

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 (1) พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน (2) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) (3) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area) (4) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Center Area) (5) พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless Network Area)

เจ้าของข้อมูล

หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

ทรัพย์สิน

หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟท์แวร์ที่มีลิขสิทธิ์ เป็นต้น

จดหมายอิเล็กทรอนิกส์ (e-mail)

หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

ชื่อผู้ใช้ (Username)

หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่กำหนดสิทธิการใช้งานไว้

รหัสผ่าน (Password)

หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์

หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

การควบคุมการรักษาความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environment Security Control)

1. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

2. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

2.1 ภายในองค์กร มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เช่น ติดประกาศกำหนดเป็นพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้เห็นชัดเจน เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

2.2 ผู้บริหาร กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน, พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area), พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area), พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Center Area), พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless Network Area) เป็นต้น

2.3 ผู้บริหาร กำหนดสิทธิ์ให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

2.3.1 จัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.3.2 ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว

2.3.3 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำและให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ 1 ครั้ง

3. การควบคุมการเข้าออก อาคาร สถานที่

3.1 จัดทำเอกสารระบุสิทธิ์ของผู้ใช้ และ “หน่วยงานภายนอก” ในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้

3.1.1 องค์กรได้กำหนดสิทธิ์ ผู้ใช้ ที่มีสิทธิ์ผ่านเข้าออกและช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละพื้นที่อย่างชัดเจน

3.1.2 การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยกำหนดให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น ทำการลงบันทึกข้อมูลบัตรในแบบฟอร์มการเข้าออก และมอบบัตร ผู้ติดต่อ (Visitor) ให้บุคคลภายนอกหรือผู้มาติดต่อ

3.1.3 บุคคลภายนอกหรือผู้มาติดต่อต้องติดบัตร ผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในองค์กร

3.1.4 เมื่อบุคคลภายนอกหรือผู้มาติดต่อจะออกจากอาคาร สถานที่ เจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบแลกบัตรคืน พร้อมบันทึกข้อมูลเวลาออกในแบบฟอร์มการเข้าออก

3.2 บุคคลภายนอกหรือผู้มาติดต่อ จะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

3.3 หากมีบุคคลอื่นใด ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรผู้ติดต่อ (Visitor) โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกการขอเข้าออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

การควบคุมการเข้า-ออกห้อง Data Center

(Data Center Entry Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคลต่างๆ ที่มีความจำเป็นต้องเข้าออกห้อง Data Center

2. คำจำกัดความของผู้เกี่ยวข้อง

2.1 ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในกลุ่มสารสนเทศและเทคโนโลยี

2.2 เจ้าหน้าที่ หมายถึง เจ้าหน้าที่องค์กรที่มีสิทธิ์ในการเข้าออกอาคาร สถานที่ ห้องต่างๆ ภายในองค์กร

2.3 ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่างๆ ของกลุ่มสารสนเทศและเทคโนโลยี

3. บทบาทและความรับผิดชอบ

3.1 ผู้อำนวยการฝ่ายสารสนเทศ

3.1.1 อนุมัติสิทธิ์เข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

3.1.2 อนุมัติกระบวนการควบคุมการเข้าออก กลุ่มสารสนเทศและเทคโนโลยี

3.2 ผู้ดูแลระบบ กลุ่มสารสนเทศและเทคโนโลยี

3.2.1 ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของกลุ่มสารสนเทศและเทคโนโลยีอย่างเคร่งครัด

3.2.2 ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกกลุ่มสารสนเทศและเทคโนโลยี ติดบัตรประจำตัวขององค์กร หรือบัตรผู้ติดต่อ (Visitor) เท่านั้น

4. กระบวนการควบคุมการเข้าออกห้อง Data Center

4.1 ผู้ดูแลระบบ กลุ่มสารสนเทศและเทคโนโลยี และเจ้าหน้าที่ องค์กร มีแนวทางปฏิบัติ ดังนี้

4.1.1 ผู้ดูแลระบบ ควรจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) ส่วนเครื่องพิมพ์ (Printer Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น

4.1.2 กลุ่มสารสนเทศและเทคโนโลยี ต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกกลุ่มสารสนเทศและเทคโนโลยี โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ผู้มีสิทธิ์เข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

4.1.3 สิทธิ์ในการเข้าออกห้องต่างๆ ภายในกลุ่มสารสนเทศและเทคโนโลยี ของเจ้าหน้าที่แต่ละคนต้องได้รับการอนุมัติจากผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยี โดยผ่านกระบวนการลงทะเบียนที่เป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในกลุ่มสารสนเทศและเทคโนโลยี

4.1.4 เจ้าหน้าที่ทุกคนต้องทำบัตรผ่านเพื่อใช้ในการเข้าออกกลุ่มสารสนเทศและเทคโนโลยี และต้องจัดทำระบบเก็บบันทึกการเข้าออกกลุ่มสารสนเทศและเทคโนโลยี

4.1.5 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกกลุ่มสารสนเทศและเทคโนโลยี ต้องมีการควบคุมอย่างรัดกุม

4.1.6 การเข้าถึงกลุ่มสารสนเทศและเทคโนโลยี และห้องคอมพิวเตอร์ ต้องมีการลงบันทึกการเข้าออกทุกครั้ง

4.1.7 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีทุกคนต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้าออกทุกคนได้มีการบันทึกการเข้าออกเรียบร้อยแล้ว

4.2 ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติดังนี้

4.2.1 ผู้ติดต่อจากหน่วยงานภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ (Visitor)

4.2.2 ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในกลุ่มสารสนเทศและเทคโนโลยี

4.2.3 ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าออกกลุ่มสารสนเทศและเทคโนโลยี ได้ด้วยบัตรผู้ติดต่อ (Visitor) โดยสิทธิ์จะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าปฏิบัติงานภายในกลุ่มสารสนเทศและเทคโนโลยี

4.2.4 พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าได้ตามที่ขออนุญาตเข้าออกเท่านั้น และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

4.2.5 ผู้ติดต่อจากหน่วยงานภายนอก สามารถนำผู้ติดตามเข้ามาช่วยงานได้ไม่เกินครั้งละ 5 คน และทุกคนจะต้องถูกบันทึกการเข้าออกเช่นกัน

4.2.6 ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรและลงบันทึกการขออนุญาตเข้าออกทุกครั้ง

4.2.7 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยี ควรตรวจสอบความถูกต้องของข้อมูลบันทึกการเข้าออกของหน่วยงานภายนอกกับเจ้าหน้าที่รักษาความปลอดภัยอย่างน้อยเดือนละ 1 ครั้ง

4.2.8 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยี ต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

(Access Information System Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรได้อย่างถูกต้อง

2. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

2.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

2.2 ผู้ดูแลระบบ ได้ทำการกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

2.4 ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ

2.5 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

3. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1 ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ได้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

3.2 เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

3.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

4. การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

4.1 กำหนดให้ผู้ใช้งานเข้าถึงระบบสารสนเทศการสื่อสาร หรือระบบอื่นๆ ที่เกี่ยวข้องต้องมี ชื่อผู้ใช้ (Username) เป็นตัวอักษร หรือตัวเลข อย่างน้อย 6 ขึ้นไป

4.2 กำหนดให้ผู้ใช้งานเข้าถึงระบบสารสนเทศการสื่อสาร หรือระบบอื่นๆ ที่เกี่ยวข้องต้องมีรหัสผ่าน (Password) มากกว่าหรือเท่ากับ 6 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรตัวพิมพ์ปกติ, ตัวอักษรตัวพิมพ์ใหญ่, ตัวเลข และอักขระพิเศษ เข้าด้วยกัน

4.3 กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้ ส่งมอบให้ถึงมือผู้ใช้อย่างปลอดภัย และกำหนดให้ผู้ใช้เปลี่ยนรหัสใหม่ทันทีหลังจากการเข้าใช้งานครั้งแรก

4.4 กำหนดให้ผู้ใช้เปลี่ยนรหัสใหม่เป็นประจำทุก ๆ 90 วัน และใช้รหัสซ้ำเดิมไม่ได้อย่างน้อย 1 ครั้ง

4.5 กำหนดให้ผู้ใช้งานใส่ชื่อผู้ใช้ (Username) หรือรหัสผ่าน (Password) ผิดได้ไม่เกิน 3 ครั้ง

4.6 ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม

4.7 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

4.8 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่

4.9 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

4.10 ผู้ใช้งานต้องรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

4.11 เมื่อผู้ใช้งานลาออกหรือมีการยกเลิกการใช้งานชื่อผู้ใช้ (Username) ให้หน่วยงานที่เกี่ยวข้องทำหนังสือแจ้งยกเลิกการใช้งานให้ฝ่ายสารสนเทศเป็นลายลักษณ์อักษรเพื่อทำการลบชื่อผู้ใช้(Username) ออกจากระบบ

5. ข้อตกลงการใช้เครื่องคอมพิวเตอร์

5.1 ผู้ใช้ตกลงจะตั้งรหัสผ่าน (Password) ของตนเองสำหรับ Login โดยไม่บอกให้ผู้อื่นทราบ

5.2 ผู้ใช้ตกลงที่จะใช้เครื่องคอมพิวเตอร์สำหรับงานของบริษัทฯ เท่านั้น และจะไม่นำข้อมูล โปรแกรม และเกมใดๆ ที่ไม่เกี่ยวข้องกับบริษัทฯ มาติดตั้งบนเครื่องคอมพิวเตอร์

5.3 ผู้ใช้ตกลงจะดูแลความสะอาดและสภาพทั่วไปของเครื่องคอมพิวเตอร์ให้อยู่สภาพใช้งานได้ตามปกติและทำการแจ้งฝ่ายสารสนเทศเมื่อพบปัญหา

5.4 ผู้ใช้ตกลงจะปกป้องข้อมูลของบริษัทฯ และจะไม่นำข้อมูลของบริษัทฯ ไปเผยแพร่ต่อบุคคลภายนอก หรือบุคคลที่ไม่เกี่ยวข้องกับงานบริษัทฯ โดยมิได้รับอนุญาตจากผู้บริหาร

5.5 ผู้ใช้ยินยอมให้เจ้าหน้าที่ผู้ที่มีอานาจของบริษัทฯ ทำการตรวจสอบข้อมูล หรือ E-mail ในกรณีที่จำเป็นเพื่อความเป็นระเบียบเรียบร้อย ในการจัดการข้อมูลบนเครื่องคอมพิวเตอร์

5.6 ผู้ใช้จะไม่เผยแพร่ข้อมูลข่าวสาร, E-mail หรือกระทำการใดๆ ที่ส่งผลให้ผู้อื่นได้รับความเสียหาย และกระทำผิดกฎหมาย ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

6. การบริหารจัดการการเข้าถึงของผู้ใช้

6.1 การลงทะเบียนเจ้าหน้าที่ใหม่ของกลุ่มสารสนเทศและเทคโนโลยี ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

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

6.3 ผู้ใช้ ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

6.4 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของเจ้าหน้าที่

6.4.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ ซึ่งมีแนวทางปฏิบัติ ตามที่กำหนดไว้ใน “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

6.4.2 การกำหนด การเปลี่ยนแปลงและการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

6.4.3 กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

6.4.3.1 ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้นๆ

6.4.3.2 ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

6.4.3.3 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

6.4.3.4 ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

6.5 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

6.5.1 ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

6.5.2 เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

6.5.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

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

6.5.5 ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ตามที่ระบุไว้ใน “การบริหารจัดการการใช้งานระบบ และรหัสผ่าน”

6.5.6 ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

7. การบริหารจัดการการเข้าถึงระบบเครือข่าย

7.1 ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

7.2 การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางอินเตอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบเทคโนโลยีสารสนเทศและการสื่อสารก่อนที่จะสามารถใช้งานได้ในทุกกรณี

7.3 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

7.4 ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

7.5 ผู้ดูแลระบบ ควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้

7.6 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

7.7 ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กร ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

7.8 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

7.9 การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเตอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

7.10 IP address ภายในของระบบงานเครือข่ายภายในขององค์กร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของฝ่ายสารสนเทศได้โดยง่าย

7.11 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

7.12 การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

7.13 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีเท่านั้น

8. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

8.1 ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

8.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขและรายงานผู้บริหารให้ทราบโดยทันที

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

8.4 ควรดำเนินการติดตั้งอัพเดทระบบซอฟท์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

8.5 ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

8.6 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยี เท่านั้น

9. การบริหารจัดการการบันทึกและตรวจสอบ

9.1 ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน

9.2 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

9.3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

10. การใช้งานระบบจากระยะไกล Virtual Private Network (VPN)

10.1 ผู้ขอใช้ ต้องเป็นพนักงาน, ลูกจ้างของบริษัทฯ หรือผู้ที่ได้รับอนุญาตจากฝ่ายบริหารเป็นลายลักษณ์อักษรเท่านั้น

10.2 ผู้ขอใช้ต้องมีชื่อผู้ใช้ (Username) และรหัส (Password) ที่ได้มาจากการยื่นเอกสารการขอใช้งาน VPN

10.3 ผู้ขอใช้ต้องเก็บรหัสผ่านเป็นความลับ

10.4 ผู้ขอใช้ต้องหลีกเลี่ยงการจดรหัสผ่านกระดาษ เว้นแต่ว่าได้มีการเก็บอย่างปลอดภัย

10.5 ผู้ขอใช้ต้องทำการเปลี่ยนรหัสผ่านทุกครั้งที่มีสิ่งบอกเหตุที่เป็นไปได้ถึงอันตรายที่จะเกิดขึ้นกับระบบหรือรหัสผ่าน

10.6 ผู้ขอใช้ควรเลือกรหัสผ่านที่มีความปลอดภัยด้วยความยาวขั้นต่ำ 6 ตัวอักษรขึ้นไป

10.7 รหัสผ่านต้องไม่มีความคล้ายคลึง Username

10.8 มากกว่าหรือเท่ากับ 6 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรตัวพิมพ์ปกติ, ตัวอักษรตัวพิมพ์ใหญ่, ตัวเลข และอักขระพิเศษ เข้าด้วยกัน

10.9 กำหนดรหัสผ่านที่ง่ายต่อการจดจำ แต่ต้องเป็นคำที่ไม่สามารถคาดเดาได้ง่ายเช่น qwerty, abcde, 12345, ชื่อ, นามสกุล, วัน เดือน ปี เกิด, ที่อยู่, เบอร์โทรศัพท์ หรือหมายเลขประจำตัวอื่นๆ เป็นต้น

10.10 เปลี่ยนรหัสผ่านเป็นช่วงๆ อย่างสม่ำเสมออย่างน้อย 90 วันต่อ 1 ครั้ง และหลีกเลี่ยงการใช้ซ้ำหรือวนกลับมาใช้รหัสผ่านเดิม

10.11 เปลี่ยนรหัสผ่านใหม่ทันทีหลังจากได้รับรหัสผ่านเข้าใช้งานครั้งแรก และห้ามใช้รหัสผ่านร่วมกับคนอื่น

10.12 ผู้ขอใช้ต้องปฏิบัติตามข้อกำหนดของบริษัทฯ ว่าด้วย “นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ”

11. การควบคุมการเข้าใช้งานระบบจากภายนอก

กลุ่มสารสนเทศและเทคโนโลยี ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

11.1 การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กร ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์กร การควบคุมบุคคลที่เข้าสู่ระบบขององค์กรจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานเข้าสู่ระบบภายใน ตาม “การใช้งานระบบจากระยะไกล”

11.2 วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากฝ่ายบริหารหรือผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยี เป็นลายลักษณ์อักษร มีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบอย่างเคร่งครัด ตาม “การใช้งานระบบจากระยะไกล”

11.3 ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

11.4 ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบจากอินเตอร์เน็ต หรือระบบโทรศัพท์ ภายนอกนั้น ต้องดูแลและจัดการ โดยผู้ดูแลระบบและวิธีการเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

11.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port, Modem หรือ ช่องทางการเชื่อมต่ออื่นๆ จากภายนอก ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

12. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

12.1 ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

12.1.1 การแสดงตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้ (Username)

12.1.2 การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน (Password), การใช้สมาร์ทการ์ดหรือการใช้ USB token ที่มีความสามารถ PKI เป็นต้น

12.2 การเข้าสู่ระบบสารสนเทศขององค์กรนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี

12.3 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบผู้ใช้งาน เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส

การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

(Outsource Access Control)

1. วัตถุประสงค์

การใช้บริการจากหน่วยภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลหรือปรับเปลี่ยนการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบการใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

2. แนวทางปฏิบัติ

2.1 ผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยี ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

2.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

2.2.1 หน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยี

2.2.2 จัดทำแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร 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 ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

2.2.4 องค์กร ควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน

2.2.5 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

2.2.6 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษา

ความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

2.2.7 องค์กรมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจว่า องค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

2.2.8 ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

(Personal Computer Control)

1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าขององค์กร ให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้ ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร

2.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.3 ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร

2.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ของกลุ่มสารสนเทศและเทคโนโลยีเท่านั้น

2.5 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของกลุ่มสารสนเทศและเทคโนโลยี เท่านั้น

2.6 ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ 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) โดยตั้งเวลาอย่างน้อยประมาณ 15 นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

3.3 ผู้ใช้ ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3.4 ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Log-out ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver

3.5 ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) หรือพักหน้านจอ (Sleep Mode) อัตโนมัติโดยตั้งเวลาประมาณ 15 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

3.6 ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง

4. แนวทางปฏิบัติในการใช้รหัสผ่าน

4.1 ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

5.1 ผู้ดูแลระบบ ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

5.2 ผู้ดูแลระบบ มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

5.3 ผู้ใช้ ควรตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Thumb Drive และ Data Storage อุปกรณ์อื่นๆ ที่นำมาใช้ต่อกับเครื่องคอมพิวเตอร์ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

5.4 ผู้ใช้ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

5.5 ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

6. การสำรองข้อมูลและการกู้คืน

6.1 ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้ที่อื่นๆ เช่น พื้นที่เก็บข้อมูลส่วนกลาง, CD, DVD, Flash Drive, External Hard Disk เป็นต้น

6.2 ผู้ใช้มีหน้าที่เก็บรักษาข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

6.3 ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

การควบคุมการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

(Portable Computer Control)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกองค์กร เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ขององค์กรให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยง ในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร

2.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาขององค์กรต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.3 การตั้งชื่อเครื่องคอมพิวเตอร์ (computer name) แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยี เท่านั้น

2.4 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของกลุ่มสารสนเทศและเทคโนโลยีเท่านั้น

2.5 ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

2.6 ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

2.7 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

2.8 ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสียงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

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 เครื่องดื่มต่างๆ เป็นต้น

2.15 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส

2.16 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

2.17 ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน 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 ผู้ใช้ควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ใน “การบริหารจัดการการใช้งานระบบและรหัสผ่าน”

4.3 ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) หรือพักหน้านจอ (Sleep Mode) อัตโนมัติโดยตั้งเวลาประมาณ 15 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

4.4 ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

5. แนวทางปฏิบัติในการใช้รหัสผ่าน

5.1 ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

6. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

6.1 ผู้ใช้ ต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

6.2 ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

6.3 หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้เชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่นๆ ได้

7. การสำรองข้อมูลและการกู้คืน

7.1 ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

7.2 ผู้ใช้ควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

7.3 สื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

7.4 สื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

การควบคุมการใช้งานระบบอินเตอร์เน็ต

(Internet System Control)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเตอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวทางปฏิบัติในการใช้งานอินเตอร์เน็ต

2.1 ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเตอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IP-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่นยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้บริหาร ผู้อำนวยการฝ่ายสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมายเป็นลายลักษณ์อักษรแล้วเท่านั้น

2.2 ผู้ดูแลระบบควรจัดหาระบบการจัดเก็บข้อมูลการใช้งานอินเตอร์เน็ต (Log File) ของผู้ใช้งานเพื่อตรวจสอบดูย้อนหลังได้ไม่น้อยกว่า 90 วัน

2.3 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเตอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

2.4 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

2.5 ผู้ใช้ต้องไม่ใช้เครือข่ายอินเตอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

2.6 ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลขององค์กร

2.7 ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลข่าวสารที่ละเมิดลิขสิทธิ์ต่างๆ ที่สร้างความเสียหายให้กับองค์กร และผู้อื่นตามกฎหมาย “พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560”

2.8 ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเตอร์เน็ต

2.9 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ต

2.10 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็น ภาพ, เสียง, ข้อความ หรือข้อมูลใดๆ ของผู้อื่นที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ตามกฎหมาย “พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560”

2.11 ผู้ใช้มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเตอร์เน็ตก่อนนำข้อมูลไปใช้งาน

2.12 ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเตอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่างๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

2.13 การใช้งานเว็บบอร์ด (Web Board) ขององค์กร ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับขององค์กร

2.14 ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่นๆ

2.15 หลังจากใช้งานอินเตอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์

(Electronic Mail System Control)

1. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเตอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัดจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

2.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กร ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

2.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร

2.3 สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

2.4 การกำหนดรหัสผ่านที่ดี มีแนวทางปฏิบัติตามที่ระบุไว้ใน “การบริหารจัดการสิทธิ์การใช้งานระบบ และรหัสผ่าน”

2.5 รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ “O” 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 และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร

2.11 ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

2.12 ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น

2.13 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

2.14 ผู้ใช้ควรทำการตรวจสอบแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

2.15 ผู้ใช้ไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

2.16 ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสื่อมเสียชื่อเสียงขององค์กร ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

2.17 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในเอกสารจดหมายอิเล็กทรอนิกส์

2.18 ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

2.19 ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

2.20 ข้อควรระวัง ผู้ใช้ไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(Wireless Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

2.1 ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการกลุ่มสารสนเทศและเทคโนโลยี อย่างเป็นลายลักษณ์อักษร

2.2 ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3 ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

2.4 ผู้ดูและระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน 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 และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

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

2.9 ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

2.10 ผู้ดูแลระบบควรจะมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

2.11 ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

2.12 ผู้ดูแลระบบ ควรใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่อาจเกิดขึ้นในระบบเครือข่ายไร้สาย

การควบคุมระบบสำรอง

(Backup System Control)

1. วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรองให้ระบบสารสนเทศขององค์กรมีสภาพพร้อมใช้งานและให้บริการได้อย่างต่อเนื่อง ผู้ดูแลระบบเครือข่าย ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและผู้ดูแลระบบสารสนเทศ ถือปฏิบัติ เพื่อสร้างความมั่นใจว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหา และต้องสำรองข้อมูลและสามารถกู้คืนระบบ และข้อมูลได้ในระยะเวลาเหมาะสม

2. กระบวนการระบบสำรอง (disaster recovery site: DR site)

2.1 จัดทำรายการระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรอง และทบทวนรายการอย่างน้อยปีละ 1 ครั้ง

2.2 ระบบสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม ดังนี้

2.2.1 มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง

2.2.2 มีระบบไฟฟ้าสำรอง

2.2.3 มีระบบปรับอากาศและความชื้นที่เหมาะสม

2.2.4 มีระบบป้องกันอัคคีภัย

2.2.5 มีระบบส่องสว่างที่เหมาะสม

2.2.6 มีระบบสื่อสารหรือระบบเครือข่ายสำรอง

2.2.7 มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

2.2.8 มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

3. การสำรองข้อมูล (Data Backup)

3.1 จัดทำรายการระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการสำรองข้อมูล และทบทวนรายการอย่างน้อยปีละ 1 ครั้ง

3.2 กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

3.3 กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

3.4 บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานะการทำงานสำเร็จ/ไม่สำเร็จ เป็นต้น

3.5 ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และ ข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆ เป็นต้น

3.6 จัดเก็บข้อมูลสำรองไว้ในระบบสำรอง

3.7 ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลสำรอง

3.8 มีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

3.8.1 ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

3.8.2 ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

3.8.3 ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

3.8.4 ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

3.8.5 ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการทำงานอย่างน้อยปีละ 1 ครั้ง

4. การกู้คืนระบบ (System Recovery)

4.1 ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบ เครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/ หรือผู้ดูแลระบบเครือข่าย ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้ รายงานสรุปผลการปฏิบัติงานต่อผู้บริหาร หรือผู้ที่ได้รับมอบหมายจากผู้บริหารให้รับทราบ

4.2 ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

4.3 หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

5. การกู้คืนข้อมูล (Data Recovery)

5.1 จัดทำขั้นตอนปฏิบัติสาหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

5.2 ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

5.3 ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

5.4 ทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่าเสมออย่างน้อยปีละ 1 ครั้ง

6. การทดสอบสภาพพร้อมใช้งาน

6.1 ต้องทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรอง ระบบสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง