ภาคผนวก 2 นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1.วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัท ที เอส ฟลาวมิลล์ จำกัด (มหาชน) หรือต่อไปนี้เรียกว่า "องค์กร" เป็นไปอย่าเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่ามีประสิทธิภาพและประสิทธิผล

1.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร และมีการปรับปรุงอย่างต่อเนื่อง

1.3 นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2. องค์ประกอบของนโยบาย

2.1 คำนิยาม

2.2 การควบคุมการใช้งานการเข้าถึงระบบเทคโนโลยีสารสนเทศและการจัดการการเข้าถึงเครือข่าย

2.3 การบริหารจัดการทรัพย์ที่เกี่ยวข้องกับระบบสารสนเทศ

2.4 การจัดการความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมพื้นที่ควบคุม

2.5 การจัดทำทะเบียนความเสี่ยงและแผนฉุกเฉิน

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด และควรมีการจัดอบรมเพื่อให้ความรู้พนักงานเกี่ยวกับเทคโลยีสารสนเทศใหม่ๆและความปลอดภัยในการใช้เครือข่ายเป็นประจำทุกปี

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **องค์กร** หมายถึง บริษัท ที เอส ฟลาวมิลล์ จำกัด (มหาชน)
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร
- **กลุ่มสารสนเทศและเทคโนโลยี** หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร
- **หัวหน้าศูนย์สารสนเทศและเทคโนโลยี** 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 หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท(Role) ซึ่งองค์กรกำหนดไว้ ดังนี้
  - **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงขององค์กร
  - **ผู้ดูแลระบบ (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
  - **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการขององค์กร
- **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่กรมกิจการผู้สูงอายุอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง 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 อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง 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
- **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ 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
- **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ส่วนที่ 1

การควบคุมการใช้งานการเข้าถึงระบบเทคโนโลยีสารสนเทศและการจัดการการเข้าถึงเครือข่าย

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรได้อย่างถูกต้อง

2. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

2.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

2.2 กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

2.3 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

2.4 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

3. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1 ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ได้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

3.2 เจ้าของข้อมูล และ "เจ้าของระบบงาน" จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นเท่านั้น

3.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

4. การบริหารจัดการการเข้าถึงของผู้ใช้

4.1 การลงทะเบียนเจ้าหน้าที่ใหม่ของกลุ่มสารสนเทศและเทคโนโลยี ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น

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

4.3 ผู้ใช้ ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

4.4 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

4.4.1 รหัสผ่านต้องประกอบด้วย ตัวอักษรพิมพ์ใหญ่ + ตัวอักษรพิมพ์เล็ก + ตัวเลข จำนวนรวมไม่ต่ำกว่า 8 ตัวอักษร

4.4.2 มีการกำหนดรหัสผ่าน และให้ผู้ใช้เปลี่ยนแปลงรหัสผ่านด้วยตนเอง

4.4.3 รหัสผ่านจะต้องไม่ซ้ำกับรหัสผ่านย้อนหลัง 3 ครั้งหลังสุด

4.4.4 รหัสผ่านชุดหรือรูปแบบคล้ายเดิมจะไม่สามารถใช้งานได้ เช่น เดิม Test12345 ใหม่ Test123456 ระบบจะไม่ยินยอมให้เปลี่ยนรหัสผ่าน

4.4.5 กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างน้อย 6 เดือน/ครั้ง หลังจากเปลี่ยนรหัสผ่านครั้งล่าสุด (เมื่อครบกำหนดระบบจะให้ทำการเปลี่ยนรหัสผ่าน หากไม่เปลี่ยนรหัสผ่านจะไม่สามารถเข้าใช้งานคอมพิวเตอร์ได้)

4.4.6 หากผู้ใช้งานใส่รหัสผิดติดกัน 10 ครั้งระบบจะทำการล็อคบัญชีผู้ใช้งานนั้นทันที และปลดล็อคอัตโนมัติภายในเวลา 10 นาที

4.4.7 กรณีลืมรหัสผ่านหรือใส่รหัสผิดพลาดจนบัญชีผู้ใช้งานล็อค ให้ลงบันทึกในเอกสารใบแจ้งแก้ไข/ซ่อม/ติดตั้งอุปกรณ์ เพื่อให้เจ้าหน้าที่เทคโนโลยีสารสนเทศปลดล็อคหรือรีเซ็ตรหัสผ่าน

4.4.8 ทำการปิดการใช้งานหรือยกเลิกผู้ใช้ เมื่อไม่มีผู้ใช้งาน (User account) นั้นๆ

4.5 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

4.5.1 เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4.5.2 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบ ต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

4.5.3 ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร หรือกรณีขายหรือทำลายคอมพิวเตอร์ เช่น ถอด / ทำลาย/ สำรองข้อมูลบนอุปกรณ์บันทึกข้อมูลก่อน

5. การบริหารจัดการการเข้าถึงระบบเครือข่าย

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

5.2 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

5.3 ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

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

5.5 IP address ภายในของระบบงานเครือข่ายภายในขององค์กร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

5.6 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.7 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

5.8 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีเท่านั้น

6. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

6.1 ผู้ดูแลระบบ รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) และการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software)

6.2 ตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

6.3 ควรดำเนินการติดตั้งอัพเดทระบบซอฟท์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Window Update เป็นต้น

6.4 ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากกการแก้ไขหรือบำรุงรักษา

6.5 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยีเท่านั้น

6.6 ควรทำการบันทึกพื้นที่ใช้งานและพื้นที่ว่างบนเครื่องแม่ข่ายทุกวันและลงบันทึกไว้เป็นเอกสาร

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

ส่วนที่ 2

การบริหารจัดการทรัพย์ที่เกี่ยวข้องกับระบบสารสนเทศ

1. วัตถุประสงค์

1.1 เพื่อควบคุมการเพิ่มเติม, การเปลี่ยนแปลง และการยกเลิก การใช้งานทรัพย์สิน (Asset) ในระบบสารสนเทศ และปรับปรุงให้ทะเบียนทรัพย์สิน (Inventory of Assets) มีความถูกต้องและทันสมัยอยู่เสมอ

1.2 เพื่อให้มีการบันทึกรายละเอียดของทรัพย์สิน (Asset) แต่ละประเภทอย่างครบถ้วน

1.3 เพื่อให้มีการกำหนดค่าระดับความสำคัญให้แก่ทรัพย์สิน (Asset) และการกำหนดระดับชั้นความลับให้แก่ข้อมูล

1.4 เพื่อใช้เป็นข้อมูลตั้งต้นสำหรับการประเมินความเสี่ยง และแก้ไขควบคุมความเสี่ยง

2. ขอบข่าย

ทรัพย์สินทั้งหมดที่เกี่ยวข้องกับข้อมูลที่อยู่ในขอบเขตของแผนกเทคโนโลยีสารสนเทศ เช่น SOFTWARE , HARDWARE , อุปกรณ์สำนักงานอื่นๆ (โต๊ะ , ตู้เอกสาร)

3. การลงทะเบียนทรัพย์สิน

3.1 ควรมีการลงทะเบียนทรัพย์สินกับฝ่ายบัญชีทุกครั้งก่อนนำทรัพย์สินไปใช้งาน

3.2 การลงทะเบียนทรัพย์สินควรระบุ รายเอียดการใช้งาน สถานที่ติดตั้ง ให้ครบถ้วน

3.3 ควรติดสติ๊กเกอร์บ่งชี้ทรัพย์สินในตำแหน่งที่เห็นได้ชัดเจน และไม่หลุดลอกง่าย

4. การยกเลิกหรือเปลี่ยนแปลงข้อมูลทรัพย์สิน

4.1 ควรมีการแจ้งฝ่ายบัญชีทุกครั้งที่มีการเปลี่ยนแปลงข้อมูลทรัพย์สิน เช่น ย้ายสถานที่ติดตั้ง , การปรับเปลี่ยน SPECS เป็นต้น

4.2 ในกรณีขอยกเลิก / ขาย / ทำลายทรัพย์สิน ควรมีการบันทึกเป็นเอกสาร

4.3 เพื่อป้องกันข้อมูลรั่วไหลจากองค์กรทรัพย์สินที่มีสื่อบันทึกข้อมูล เช่น Harddisk ควรมีการถอดหรือทำลายทิ้งก่อนนำทรัพย์สินออกขาย หรือทำลายและควรมีการบันทึกไว้เป็นเอกสาร

ส่วนที่ 3

การจัดการความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมพื้นที่ควบคุม

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 ของกลุ่มสารสนเทศและเทคโนโลยี

3. บทบาทและความรับผิดชอบ

3.1 ผู้ดูแลระบบ และเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ

3.1.1 ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของศูนย์เทคโน ฯ อย่างเคร่งครัด

3.1.2 ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกกลุ่มสารสนเทศและเทคโนโลยี ต้องติดบัตรผู้ติดต่อ (Visitor) หรือบัตรประจำตัวขององค์กรเท่านั้น

4. กระบวนการควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์

4.1 ผู้ดูแลระบบ กลุ่มสารสนเทศและเทคโนโลยี และเจ้าหน้าที่ องค์กร มีแนวทางปฏิบัติ ดังนี้

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

4.1.2 กลุ่มสารสนเทศและเทคโนโลยี ต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกกลุ่มสารสนเทศและเทคโนโลยี โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก "ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่" เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์(Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ(System Administrator) เป็นต้น

4.1.3 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกกลุ่มสารสนเทศและเทคโนโลยี ก็ต้องมีการควบคุมอย่างรัดกุม

4.1.4 การเข้าถึงกลุ่มสารสนเทศและเทคโนโลยี และห้องคอมพิวเตอร์ ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร "ตารางบันทึกการเข้า-ออกห้องServer"

4.1.5 เจ้าหน้าที่กลุ่มสารสนเทศและเทคโนโลยี ทุกคนต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้าออกทุกคนต้องกรอกแบบฟอร์มดังกล่าว

4.2 ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติดังนี้

4.2.1 ผู้ติดต่อจากหน่วยงานภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ "Visitor" แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร "บันทึกการเข้าออกพื้นที่"

4.2.2 ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในกลุ่มสารสนเทศและเทคโนโลยี

ส่วนที่ 4
การสำรองและการกู้คืนข้อมูล

1. วัตถุประสงค์

เพื่อให้แน่ใจว่าข้อมูลที่สำคัญของคุณสามารถอยู่รอดได้ในอันตรายที่รอคอยในอนาคตได้ ในหลักการนี้เป็นกระบวนการที่ซับซ้อน คัดลอกไฟล์ทั้งหมดของคุณไปยังอุปกรณ์อื่น ๆ เก็บสำรองไว้ที่ปลอดภัย และเพื่อกู้คืนข้อมูลในกรณีที่เกิดปัญหาได้อย่างรวดเร็ว

2. แนวทางปฏิบัติ

2.1 ผู้ดูแลระบบติดตั้งระบบสำรองข้อมูลสำคัญอัตโนมัติ

2.2 กำหนดเวลาสำรองข้อมูลให้เหมาะสม ไม่ควรสำรองข้อมูลในระหว่างผู้ใช้กำลังใช้งานระบบ

2.3 ตรวจสอบรายการที่สำรองข้อมูลและบันทึกไว้เป็นเอกสาร

2.4 ควรมีการทดสอบการกู้คือข้อมูลอย่างน้อยเดือนละครั้ง และลงบันทึกไว้เป็นเอกสาร

2.5 ควรมีการเคลื่อนย้ายสื่อบันทึกข้อมูลสำรองไว้ภายนอกองค์กร อย่างอาทิตย์ละครั้ง

ส่วนที่ 5
การจัดทำทะเบียนความเสี่ยงและแผนฉุกเฉิน

1. วัตถุประสงค์

เพื่อค้นหาและทราบถึงความเสี่ยงภายในแผนกเทคโนโลยีสารสนเทศ และหามาตรการป้องกัน หรือแก้ไขความเสี่ยงนั้นๆ เมื่อได้มีการประเมินความเสี่ยงด้านต่าง ๆ แล้ว ควรดำเนินการจัดลำดับความสำคัญของความเสี่ยงนั้นและค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยงนั้น พร้อมทั้งนำเสนอต่อผู้บริหารขององค์กรตัดสินใจ ที่จะเลือกวิธีการดำเนินการเพื่อลดความเสี่ยงหรือเลือกที่จะยอมรับความเสี่ยงนั้น เมื่อเลือกวิธีการดำเนินการเพื่อลดความเสี่ยง

2. แนวทางปฏิบัติ

2.1 จัดทำทะเบียนความเสี่ยงของแผนก ระบุความเสี่ยงทั้งภายใน และภายนอกองค์กร

2.2 นำความเสี่ยงที่มีโอกาสและผลกระทบที่อยู่ในเกณฑ์สูงและสูงมากเข้านำเสนอผู้บริหารถึงแนวทางป้องกัน / แก้ไข

2.3 จัดทำแผนฉุกเฉินเพื่อรองรับความเสี่ยง

2.4 ควรมีการทบทวนทะเบียนความเสี่ยงและแผนฉุกเฉินอย่างน้อยปีละครั้ง

ส่วนที่ 6

การเข้ารหัสไฟล์หรือโฟล์เดอร์

1. วัตถุประสงค์

เพื่อป้องกันการสูญหายของข้อมูลส่วนบุคคล ในกระบวนการส่งมอบหรือส่งต่อไปยังบุคคลอื่น ทั้งทางอีเมล์ภายในหรือภายนอก และเพื่อไม่ให้บุคคลที่ไม่เกี่ยวข้องหรือผู้ไม่หวังดีสามารถเปิดดูข้อมูลได้

2. แนวทางปฏิบัติ

2.1 ผู้ปฏิบัติงานที่ต้องการส่งข้อมูลส่วนบุคคล ต้องเข้ารหัสไฟล์หรือโฟล์เดอร์ทุกครั้งก่อนส่งข้อมูลให้กับหน่วยงานอื่นหรือบุคคลอื่นทั้งภายในและภายนอก

2.2 ในการส่งข้อมูลทางอีเมล์จะต้องแยกเมล์ออกเป็น 2 ฉบับ ฉบับแรกเป็นไฟล์ที่เข้ารหัส ฉบับที่ 2 เป็นรหัสผ่านที่ใช้ในการเปิดไฟล์