นโยบายและระเบียบปฏิบัติในการรักษาความปลอดภัยของระบบสารสนเทศ

บริษัท ไทยแคปปิตอล คอร์ปอเรชั่น จำกัด (มหาชน)

วัตถุประสงค์และขอบเขต

1. เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์กรเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณ์ที่ไม่ถูกต้องและถูกคุกคามจากภัยต่างๆ ทางองค์กรจึงเห็นสมควรกำหนดนโยบายการรักษรความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยมีวัตถุประสงค์ดังต่อไปนี้

1.1 จัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ของบริษัท ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 การจัดทำนโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในบริษัทได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.3 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

1.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัท ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและสื่อสารของบริษัทในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.5 นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา 1 ครั้งต่อปีหรือตามที่ระบุไว้ในเอกสาร "การตรวจสอบประเมินนโยบาย"

2. องค์ประกอบของนโยบาย

2.1 คำนิยาม

2.2 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

2.3 การควบคุมการเข้าออกห้องศูนย์ปฏิบัติการเครือข่าย

2.4 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.5 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.6 การพิสูจน์ตัวตน

2.7 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพา

2.8 การใช้งานอินเตอร์เน็ต

2.9 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

2.10. การสำรองข้อมูลที่สำคัญ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท เพื่อที่จะทำให้บริษัทมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สินบุคลากรของบริษัท ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

ส่วนที่ 1 คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- องค์กร หมายถึง บริษัท ไทย แคปปิตอล คอร์ปอเรชั่น จำกัด (มหาชน)
- ผู้บริหาร หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างบริษัท
- ศูนย์สารสนเทศ หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายของบริษัท

- หัวหน้าศูนย์สารสนเทศ หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของบริษัท ซึ่งบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน และควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

- การรักษาความมั่นคงปลอดภัย หมายถึง การรักษามั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

- มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

- วิธีการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

- แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

- ผู้ใช้ หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของบริษัท โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งบริษัทกำหนดไว้ดังนี้

    - ผู้บริหาร หมายถึง ผู้มีอำนาจในระดับสูงของบริษัท

    - ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าให้มีหน้ารับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

    - เจ้าหน้าที่พัฒนาระบบ (Developer) หมายถึง เจ้าหน้าที่ที่ได้มอบหมายให้ดูแลเรื่อง การพัฒนาระบบ

    - เจ้าหน้าที่ หมายถึง ลูกจ้างชั่วคราว ลูกจ้างชั่วคราว และลูกจ้างประจำของบริษัท

- หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่บริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

- ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

- สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

- ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

- ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัท ดังนี้

    - ระบบ LAN หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆภายในหน่วยงานเข้าด้วยกัน

- ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายอินเตอร์เน็ตทั่วโลก

- พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น
    - พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำที่โต๊ะทำงาน
    - พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)
    - พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
    - พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
    - พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

- เจ้าของข้อมูล หมายถึง ผู้ได้รับมองอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลและระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น หรือ ได้รับผลกระทบโดยตรงหากข้อมูลนั้นสูญหาย

- ทรัพย์สิน หมายถึง ข้อมูล ระบบข้อมูล หรือทรัพย์สินด้านเทคโนโลยีสารสนเทศขององค์กร เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

- จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงกัน

- รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 2 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

1. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคารสถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ

2. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

2.1 ภายในองค์กร ควรมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

2.2 ผู้บริหาร ควรกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ ให้ชัดเจนและประกาศให้รับทราบทั่วกัน โดยกำหนดพื้นที่ดังกล่าวแบ่งออกเป็น พื้นที่ทำงานทั่วไป พื้นที่ทำงานของผู้ดูแลระบบ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ และพื้นที่ใช้เครือข่ายไร้สาย เป็นต้น

2.3 ผู้บริหาร ต้องกำหนดสิทธิ์ให้กับเจ้าหน้าที่ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

2.3.1 จัดทำ "ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่" เพื่อใช้งานระบบเทคโนโลยีสารสนเทศ

2.3.2 ทำการบันทึกเวลาเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร "บันทึการเข้าออกพื้นที่"

2.3.3 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 3 การควบคุมการเข้าออกศูนย์ปฏิบัติการเครือข่ายและการป้องกันความเสียหาย(Computer Center Entry Control)

1. **วัตถุประสงค์**

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของบริษัท โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้าออกห้องศูนย์ปฏิบัติเครือข่าย

2. **คำจำกัดความของผู้เกี่ยวข้อง**

2.1 ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศ

2.2 เจ้าหน้าที่ หมายถึง เจ้าหน้าที่องค์กรที่มีสิทธิ์ในการเข้าออกสถานที่ ห้อง ภายในองค์กร

2.3 ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาขอติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่างๆ ขององค์กร

3. **บทบาทและความรับผิดชอบ**

3.1 **หัวหน้าศูนย์สารสนเทศ**

3.1.1 อนุมัติสิทธิ์เข้าออกพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ

3.1.2 อนุมัติกระบวนการควบคุมการเข้าออกศูนย์ปฏิบัติการเครือข่าย

3.2 **ผู้ดูแลระบบเครือข่าย**

3.2.1 ตรวจสอบดูแลบุคคลที่ขออนุญาติเข้ามาภายในศูนย์ปฏิบัติการเครือข่ายให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของศูนย์ปฏิบัติการเครื่องข่ายอย่างเคร่งครัด

3.2.2 ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกศูนย์ปฏิบัติการเครือข่ายต้องได้รับอนุญาติจากผู้ดูแลระบบศูนย์ปฏิบัติการเครื่อข่าย

4.กระบวนการเข้าออกห้องปฏิบัติการศูนย์เครือข่าย

4.1 ผู้ดูแลระบบศูนย์ปฏิบัติการเครือข่ายและเจ้าหน้าที่องค์กร มีแนวทางการปฏิบัติ ดังนี้

4.1.1 ผู้ดูแลระบบฯควรจัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย ส่วนเครื่องแม่ข่าย เป็นต้นเพื่อสะดวกในการปฏิบัติงานและยังทำให้ควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิ์ภาพมากขึ้น

4.1.2 ศูนย์ศูนย์ปฏิบัติการเครือข่ายต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกศูนย์ปฏิบัติการเครือข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก "ทะเบียนผู้มีสิทธิ์เข้าออก พื้นที่" เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

4.1.3 สิทธิ์ในการเข้าออกห้องศูนย์ปฏิบัติการเครือข่ายของเจ้าหน้าที่ต่ละคนต้อง ได้รับการอนุมัติจากหัวหน้าศูนย์สารสนเทศ โดยผ่านกระบวนการลงทะเบียนที่ระบุไว้ใน เอกสาร "การบริหารจัดการสิทธิ์การใช้งานระบบ" เป็นลายลักษณ์อักษร โดยสิทธิ์ของ เจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในศูนย์ปฏิบัติการเครือข่าย

4.1.4 เจ้าหน้าที่ทุกคนต้องมีรหัสผ่านเพื่อใช้ในการเข้าออกศูนย์ปฏิบัตการเครือข่ายตามกระบวนการที่ระบบระบุบนเอกสาร "การบริหารจัดการสิทธิ์การใช้งานระบบ

4.1.5 ต้องจัดการทำระบบเก็บบันทึกการเข้าออกศูนย์ปฏิบัติการเครือข่ายตามกระบวนการที่ระบุไว้ในเอกสาร "บันทึกการเข้าออกพื้นที่"

4.1.6 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำอาจมีความจำเป็นต้องเข้าออกศูนย์ปฏิบัติการ เครือข่ายก็ต้องมีการควบคุมอย่างรัดกุมและมีระบบเก็บบันทึกการเข้าออกศูนย์ปฏิบัติการฯ

4.1.7 การเข้าถึงศูนย์ปฏิบัติการเครือข่ายและห้องคอมพิวเตอร์ต้องมีการลงบันทึกตามแบบฟอร์มที่ ระบุไว้ในเอกสาร "บันทึกการเข้าออกพื้นที่"

4.1.8 เจ้าหน้าที่ศูนย์ปฏิบัติการเครือข่ายทุกคนต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้าออกทุก คนต้องกรอกแบบฟอร์มดังกล่าว

4.2 ผู้มาติดต่อจากหน่วยงานภายน้องมีแนวทางปฏิบัติดังนี้

4.2.1 ผู้ติดต่อจากหน่วยงานภายนอกต้องได้รับอนุญาตจากหัวหน้าศูนย์สารสนเทศและแสดง เอกสารที่ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่กับเจ้าหน้าที่ควบคุมการเข้า ออกศูนย์ปฏิบัติการเครือข่าย แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ใน เอกสาร "บันทึกการเข้าออกพื้นที่"

4.2.2 พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอกสามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขอ อนุญาตเข้าออกและต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

4.2.3 เมื่อสิ้นสุดภารกิจผู้ติดต่อจากหน่วยงานภายนอก ต้องแจ้งกับเจ้าหน้าที่ควบคุมการเข้าออก ศูนย์ปฏิบัติการเครือข่ายเพื่อตรวจสอบการลงบันทึกข้อมูลในสมุดบันทึกการขออนุญาตเข้า ออกว่ามีเจ้าหน้าที่ลงนามอนุญาตแล้วทุกครั้ง

4.2.4 เจ้าหน้าที่ศูนย์ปฏิบัติการเครือข่ายควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและ แบบฟอร์มการขออนุญาตเข้าออกกับเจ้าหน้าที่ควบคุมการเข้าออกศูนย์ปฏิบัติการเครือข่าย เป็นประจำทุกเดือน

4.2.6 เจ้าหน้าที่ศูนย์ปฏิบัติการเครือขายต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้อง เหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ 2 ครั้ง

ส่วนที่ 4 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีและการสื่อสารของบริษัท และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทได้อย่างถูกต้อง

2. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

2.1 ผู้ดูแลระบบ ต้องกำหนดสิทธการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

2.2 ผู้ดูแลระบบ ควรจัดให้มีระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ

2.3 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

3. การบริหารจัดการการเข้าถึงของผู้ใช้

3.1 การลงทะเบียนเจ้าหน้าที่ใหม่ของศูนย์ปฏิบัติการเครือข่ายควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ เพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในบริษัท เป็นต้น

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

3.3 ผู้ใช้ ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

3.4 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

3.5 ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือ ในกรณีที่มีความจำเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก 90 วัน ควรใช้รหัสผ่านไม่ต่ำกว่า 8 ตัวอักษร และต้องมีตัวอักษรเล็ก ใหญ่ ตัวเลข และตัวอักษรพิเศษร่วมอยู่ด้วย

3.6 ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาที่กำหนด

3.7 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 4 ครั้ง เพื่อให้มั่นใจได้ว่า สิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

3.8 ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

4. **การบริหารจัดการเข้าถึงระบบเครือข่าย**

4.1 ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone)

4.2 ต้องมีวิธีการจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะสิทธิ์ที่ได้รับอนุญาตเท่านั้น

4.3 ระบบเครือข่ายทั้งหมดของบริษัทที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกบริษัท ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

5. การควบคุมการเข้าใช้งานระบบจากภายนอก

การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของบริษัท ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของบริษัท ซึ่งต้องมีการกำหนดมาตรการการรักษาความปลอดภัย และต้องได้รับการอนุมัติจากผู้บริหาร รวมทั้งต้องมีการควบคุมอย่างเข้มงวด

ส่วนที่ 5 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third party access control)

1. **วัตถุประสงค์**

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้ามาใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ให้เป็นไปอย่างปลอดภัย

2. **แนวทางปฏิบัติ**

2.1 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

2.1.1 บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติ

2.1.2 จัดทำเอกสารแบบฟอร์มขออนุญาตให้หน่วยงานภายนอกทำ เพื่อระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งควรมีรายละเอียด เช่น เหตุผลในการขอใช้ ระยะเวลาในการใช้ เป็นต้น

2.2 เจ้าของระบบ ซึ่งรับผิดชอบต่อข้อมูลที่มีการเข้าถึง โดยหน่วยงานภายนอก และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้ความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

ส่วนที่ 6 การพิสูจน์ตัวตน (Accountability, Identification and Authentication)

1. วัตถุประสงค์

การป้องความมั่นคงปลอดภัยของระบบและข้อมูลภายในบริษัท ถือเป็นเรื่องสำคัญในปัจจุบัน ทั้งนี้ เนื่องจากการถูกคุมคาม โดยผู้ไม่ประสงค์ดีหรือจากโปรแกรมบางประเภทได้เพิ่มมากขึ้นและอาจนำมาซึ่งความเสียหายอย่างมากต่อบริษัท เพื่อช่วยลดโอกาสเสี่ยงต่อการถูกคุกคาม การพิสูนจ์ตัวตนซึ่งเป็นขั้นตอนพื้นฐานที่สำคัญของการควบคุมความปลอดภัย

2. แนวทางปฏิบัติในการพิสูจน์ตัวตน

2.1 ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน(Username) ของตนงาน โดยห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่

2.2 ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า 8 ตัวอักษร ซึ่งต้องประกอบด้วยตัวอักษร (Alphabet) และตัวเลข (Numerical character) และตัวอักษรพิเศษ

2.3 ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย 24 รหัสผ่าน และต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ 90 วัน

2.4 ผู้ใช้งานต้องทำการพิสูนจ์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของบริษัท และหากการพิสูนจ์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากการใส่รหัสผ่านไม่ถูก หรือเป็นการเกิดจากความผิดพลาดอื่นๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดย

2.4.1 คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูนจ์ตัวตนทุกครั้ง และมีการตั้งเวลาพักหน้าจอ(screen saver) เมื่อไม่ได้มีการปฏิบัติงาน

2.4.2 การใช้งานระบบ ERP Oracle จะต้องทำการพิสูนจ์ตัวตนทุกครั้ง และมีการตั้งเวลาพักหน้าจอเมื่อไม่ได้มีการปฏิบัติงานแล้ว อย่างน้อย 15 นาที

2.4.3 ในกรณีที่การเข้าถึงระบบ มีข้อผิดพลาด เกิน 5 ครั้ง ระบบจะล็อก Account นั้นๆทันที ให้แจ้งไปที่เจ้าหน้าที่สาระสนเทศเพื่อทำการเปลี่ยนรหัสผ่านเท่านั้น

ส่วนที่ 7 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของบริษัท ให้มีความถูกต้อง เป็นความลับ และพร้อมใช้งานอยู่เสมอ

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์ที่บริษัทอนุญาตให้ผู้ใช้งาน เป็นทรัพย์สินของบริษัท ดังนั้นผู้ใช้งานควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิ์ภาพเพื่อบริษัท

2.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่บริษัทได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย และไม่อนุญาตให้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัท รวมทั้งมีการติดตั้งโปรแกรมป้องกันไวรัส

2.3 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล จะต้องกำหนด โดย ผู้ดูแลระบบหรือเจ้าหน้าที่ฝ่ายสารสนเทศเท่านั้น

2.4 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการ โดยเจ้าหน้าที่ของศูนย์สารสนเทศเท่านั้น พร้อมเอกสารการส่งมอบทรัพย์สิน

2.5 ไม่เก็บข้อมูลสำคัญของบริษัทไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้งานอยู่ ให้จัดเก็บ ณ Datacenter ที่กำหนดไว้เท่านั้น

2.6 ก่อนการใช้สื่อบันทึกพกพาต่างๆ ควรมีการตรวจสอบเพื่อหาไวรัสด้วยโปรแกรมป้องกันไวรัส

2.7 ผู้ใช้ มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติ ดังนี้

2.7.1 ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

2.7.2 ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

3. การควบคุมการเข้าถึงระบบปฏิบัติการ

3.1 ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

3.2 ผู้ใช้ ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 15 นาที เพื่อทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน

3.3 ผู้ใช้ ไม่ควรอนุญาตให้ผู้อื่น ใช้ชื่อของผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตนในการเข้าทำงานร่วมกัน

3.4 ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Logout ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver

4. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

4.1 ผู้ดูแลระบบหรือเจ้าหน้าที่สารสนเทศ มีหน้าที่รับผิดชอบในการ Update โปรแกรมป้องกันไว้รัสอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) และเป็นการป้องกันการโจมตีจากภัยคุมคามต่างๆ

4.2 ผู้ใช้ ควรตรวจสอบไวรัสจากสื่อต่างๆ เช่น Thumb Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ และควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิคส์(e-mail)หรือไฟล์ดาวน์โหลดมาจากอินเตอร์เน็ต

4.3 ผู้ใช้ ควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ เกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงาน ไม่ตรงตามคำสั่งที่กำหนดไว้

4.4 ผู้ใช้ ควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

ส่วนที่ 8 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Use of Notebook Computer)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกบริษัท เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ของบริษัทให้เกิดความปลอดภัย ผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยงในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์แบบพกพาที่บริษัทอนุญาตให้ผู้ใช้งาน เป็นทรัพย์สินของบริษัท ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิ์ภาพเพื่อบริษัท

2.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่บริษัทได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย และไม่อนุญาตให้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัท รวมทั้งมีการติดตั้งโปรแกรมป้องกันไวรัส

2.3 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพา จะต้องกำหนดโดยเจ้าหน้าที่ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศของหน่วยงานเท่านั้น

2.4 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศของหน่วยงานเท่านั้น พร้อมเอกสารการส่งมอบทรัพย์หรือเอกสารส่งซ่อม

2.5 ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

2.6 ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม เช่น การกดสัมผัสหน้าจอ LCD รวมทั้งควรมีการบำรุงดูแลรักษาคอมพิวเตอร์พกพา และอุปกรณ์ต่างๆ

2.7 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

2.8 ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไว้ในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักกดทับ หรืออาจถูกจับโยนได้

2.9 ไม่ควรวางของทับหน้าจอและแป้นพิมพ์

2.10 การเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยทำการดึงที่ส่วนหน้าจอ

2.11 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้สิ่งที่เป็นของเหลว ความชื้น น้ำ กาแฟ เครื่องดื่มต่างๆเป็นต้น

2.12 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพกไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

2.13 ไม่ควรติดตั้งหรือวางคอพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

3. ความปลอดภัยด้านกายภาพ

3.1 ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน หรือไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ในที่สาธารณะ หรือในพื้นที่ที่มีความเสื่องในการสูญหายสูง

3.2 ผู้ใช้ ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์พกพาในสถานที่ที่มีความร้อน ความชื้น ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

3.3 ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงอุปกรณ์ภายในเครื่องคอมพิวเตอร์พกพาที่ติดตั้งภายในรวมถึงแบตเตอรี่

4. การควบคุมการเข้าถึงระบบปฏิบัติการ

3.1 ผู้ใช้ ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

3.2 ผู้ใช้ ควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่กำหนด

3.3 ผู้ใช้ ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 15 นาที ให้ทำล็อคหน้าจอเมื่อไม่มีการใช้งาน

3.4 ผู้ใช้ ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

5.1 ผู้ใช้มีหน้าที่รับผิดชอบในการ update โปรแกรมป้องกันไวรัสอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ ที่เกิดขึ้นจากซอฟท์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

5.2 ห้ามมิให้ผู้ใช้ทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนคอมพิวเตอร์แบบพกพา

6.การสำรองข้อมูลและการกู้คืน

6.1 ผู้ใช้ควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

6.2 ผู้ใช้ควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

ส่วนที่ 9 การใช้งานอินเทอร์เน็ต (Use of the Internet)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การรับ-ส่งข้อมูล ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น ทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานได้ตามปกติ เป็นต้น

2. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

2.1 ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการใช้งานอินเทอร์เน็ต

2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตภายในบริษัท ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส ก่อนทำการเชื่อมต่อ

2.3 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนรับส่งข้อมูลทุกครั้ง

2.4 ผู้ใช้ต้องไม่ใช้อินเทอร์เน็ตของบริษัทเพื่อหาประโยชน์ส่วนตนในเชิงธุรกิจ และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

2.5 ผู้ใช้ต้องระมัดระวังการดาว์นโหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งจะต้องไม่ละเมิดทรัพย์สินทางปัญญา

ส่วนที่ 10 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

1.วัตถุประสงค์ป

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของบริษัทโดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงานรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบ

ต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาติจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภับของการใช้งานระบบเครือข่ายไร้สาย

2. แนวทางการปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

2.1 ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของบริษัท จะต้องได้รับการพิจารณาอนุญาติจากหัวหน้าศูนย์สารสนเทศ

2.2 ผู้ดูแลระบบ ต้องทำการกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

2.3 ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

2.4 ผู้ดูแลระบบต้องทำการเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบควรเลือกใช้ชื่อ Login และรหัสผ่านที่ยากต่อการคาดเดาเพื่อป้องกันการโจมตี

2.5 ผู้ดูแลควรเลือกใช้วิธีควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาติเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

2.6 ผู้ดูแลระบบควรจะมีการติดตั้ง Firewall ระหว่าง เครือข่ายไร้สายกับเครือข่ายภายในบริษัท

2.7 ผู้ดูแลระบบควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

ส่วนที่ 10 การสำรองข้อมูลและการเตรียมพร้อมกรณีฉุกเฉิน

1.วัตถุประสงค์

การสำรองข้อมูลและการเตรียมพร้อมกรณีฉุกเฉิน มีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ยังมีเนื้อหาครอบบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

2. แนวทางการปฏิบัติในการสำรองข้อมูลที่สำคัญ

1. จัดทำระบบสำรองที่เหมาะสมเพื่อให้ระบบอยู่ในสภาพพร้อมใช้งาน
2. มีขั้นตอนการจัดเก็บสำรองข้อมูลและการกู้คืนอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ
3. จัดเก็บข้อมูลสำรองในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บนั้น ให้สามารถแสดงถึงวันที่ และเวลาสำรองข้อมูล ไว้อย่างชัดเจนและต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

แนวทางปฏิบัติการเตรียมความพร้อมกรณีฉุกเฉิน

1. ติดตั้งอุปกรณ์ Hardware และทดสอบการใช้งานให้มีความพร้อมในกรณีที่เกิดเหตุการณ์ฉุกเฉิน
2. ทดสอบการใช้งานเพื่อเตรียมความพร้อมอย่างสม่ำเสมอ
3. กำหนดหน้าที่ความรับผิดชอบของพนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉิน

    3.1 พนักงานที่เกี่ยวข้องกับแผนสำรองฉุกเฉินต้องเข้าร่วมซ้อมในแผนสำรองฉุกเฉิน ซึ่งจะจัดขึ้นปีละ 1 ครั้ง

จึงประกาศมาเพื่อทราบโดยทั่วกัน

ประกาศ ณ วันที่ 25/2 พ.ศ. 2567

.....

กำพล พัฒนาอนุกูล

Chief Financial Officer