นโยบายด้านเทคโนโลยีสารสนเทศ

(Information Technology Policy)

บริษัท ยูโร ครีเอชั่นส์ จำกัด (มหาชน)

เวอร์ชั่น 1.0.0

สารบัญ

บทนำ

บริษัท ยูโร ครีเอชั่นส์ จำกัด (มหาชน) ("บริษัทฯ") ตระหนักว่าระบบเทคโนโลยีสารสนเทศเป็นทรัพยากรที่มีคุณค่า ซึ่งจำเป็นต้องมีมาตรการปกป้องระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย ภายใต้หลักสำคัญ 3 ประการ คือ เก็บรักษาเป็นความลับ มีความถูกต้องและให้บริการได้อย่างต่อเนื่อง ผู้ใช้งานระบบเทคโนโลยีสารสนเทศภายในบริษัทฯ มีสิทธิใช้ระบบเทคโนโลยีสารสนเทศเพื่อสนับสนุนภารกิจภายใต้กรอบนโยบายและข้อปฏิบัติเพื่อให้มั่นใจได้ว่าระบบเทคโนโลยีสารสนเทศทุกภาคส่วน ได้รับการคุ้มครองให้มีความมั่นคงปลอดภัย นโยบายฉบับนี้จัดทำขึ้นเพื่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทและตามกรอบพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2950

วัตถุประสงค์

1. สร้างความมั่นใจการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศภายในบริษัทฯ เป็นไปอย่างถูกต้องตามกฎหมายและข้อบังคับที่เกี่ยวข้อง
2. มีข้อปฏิบัติที่รัดกุมเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้บุคลากรในบริษัทฯ ตลอดจนบุคคลอื่นใดที่ได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศทราบ และเข้าใจถึงข้อปฏิบัติ ข้อห้าม และความรับผิดชอบถึงการใช้งานนั้นๆ ที่จะส่งผลให้เกิดความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและใช้งานตรงตามวัตถุประสงค์ของการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ รวมทั้งไม่ละเมิดระเบียบกฎหมาย หรือทำให้เกิดการเสียหายในการปฏิบัติงาน
4. ปกป้องระบบเทคโนโลยีสารสนเทศให้ปลอดภัยจาก การสูญหาย การถูกทำลาย การแก้ไขโดยไม่ได้รับอนุญาต การลักลอบนำข้อมูลไปใช้หรือเปิดเผย ตลอดจนสร้างความมั่นใจว่าระบบเทคโนโลยีสารสนเทศมีความถูกต้องน่าเชื่อถือ มีประสิทธิภาพและประสิทธิผล สามารถให้บริการได้ต่อเนื่อง

ขอบเขต

1. การจัดทำนโยบายงานระบบเทคโนโลยีสารสนเทศให้มีเนื้อหาครอบคลุมเรื่องที่สำคัญ รวมถึงบริษัทอื่นที่เกี่ยวข้องอย่างเป็นลายลักษณ์อักษร และเสนอผู้บริหารระดับสูงเพื่อสอบทานและลงนาม
2. การจัดทำขั้นตอนการปฏิบัติงานระบบเทคโนโลยีสารสนเทศให้สอดคล้องและครอบคลุมนโยบายอย่างเป็นลายลักษณ์อักษร เสนอผู้บริหารระดับสูงสอบทานและลงนาม รวมถึงสื่อสารนโยบายและขั้นตอนการปฏิบัติงานระบบเทคโนโลยีสารสนเทศให้กับพนักงานรับทราบผ่านวิธีการสื่อสารต่างๆ อย่างสม่ำเสมอ เช่น การจัดอบรมอย่างน้อยปีละ 1 ครั้ง เรื่องนโยบายและขั้นตอนการปฏิบัติงานระบบเทคโนโลยีสารสนเทศ เพื่อให้พนักงานได้เข้าใจและปฏิบัติตามโดยเคร่งครัด
3. ทบทวนหรือปรับปรุงและขั้นตอนการปฏิบัติงานให้เป็นปัจจุบัน และเหมาะสมอย่างน้อยทุกปีและทุกครั้งที่นโยบายเปลี่ยนแปลง โดยต้องมีการลงลายมือชื่อของผู้บริหารระดับสูงใหม่ทุกครั้งและจัดเก็บเอกสารนโยบายที่เป็นลายลักษณ์อักษรไว้ในที่ที่ผู้ใช้งานและบุคคลที่เกี่ยวข้องสามารถเข้าถึงได้โดยง่าย และทำบันทึกการเปลี่ยนแปลงและจัดเก็บทุกครั้ง

การปฏิบัติตามนโยบาย

1. ต้องประกาศใช้และสื่อสารนโยบาย ให้ความรู้แก่ผู้ใช้ เผยแพร่ข้อมูล และกำกับดูแลการปฏิบัติตามนโยบายและขั้นตอนการปฏิบัติงานที่กำหนด เช่น ควรจัดให้มีการฝึกอบรมเรื่องนโยบายความปลอดภัยและรหัสผ่าน ระเบียบการควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์และการเข้าศูนย์คอมพิวเตอร์อย่างทั่วถึงเพื่อให้สามารถปฏิบัติตามได้
2. ต้องมีการติดตามการปฏิบัติงานของเจ้าหน้าที่ให้เป็นไปตามนโยบายอย่างเคร่งครัด
3. ต้องมีการตรวจสอบ รวมทั้งประเมินความเพียงพอของนโยบายและระบบควบคุมภายในระบบเทคโนโลยีสารสนเทศโดยหน่วยงานที่เป็นอิสระอย่างน้อยปีละ 1 ครั้ง ซึ่งอาจเป็นหน่วยงานตรวจสอบภายในของบริษัทฯ หรือผู้ตรวจสอบภายนอก
4. ต้องมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง ซึ่งต้องมีการระบุความเสี่ยงที่เกี่ยวข้อง จัดลำดับความสำคัญของข้อมูลและระบบคอมพิวเตอร์ กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง
5. ต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศโดยเร็ว เมื่อมีกรณีที่ส่งผลกระทบต่อการรักษาความปลอดภัยด้านระบบเทคโนโลยีสารสนเทศที่มีนัยสำคัญ
6. ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน และบุคคลที่เกี่ยวข้องอย่างชัดเจน เช่น หน้าที่ของผู้ใช้งานในกรณีที่พบว่าเครื่องคอมพิวเตอร์มีการติดไวรัส หน้าที่และความรับผิดชอบของเจ้าหน้าที่รักษาความปลอดภัยระบบเครือข่าย เป็นต้น

วัตถุประสงค์

1. เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (Access Risk) แก้ไขเปลี่ยนแปลง (Integrity Risk) หรือก่อให้เกิดความเสียหายต่อข้อมูล (Availability Risk) และระบบเทคโนโลยีสารสนเทศ
2. เพื่อป้องกันความเสียหายกับข้อมูลและระบบเทคโนโลยีสารสนเทศจากปัจจัยสภาวะแวดล้อมต่างๆ ซึ่งอาจเป็นผลให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและอุปกรณ์อื่น ๆ รวมทั้งสื่อบันทึกที่ส่งผลให้เสื่อมสภาพเร็วกว่ากำหนด
3. ป้องกันการสูญหาย เสียหาย การถูกขโมยของ ทรัพย์สินต่าง ๆ ในศูนย์ข้อมูล (Data Center)

แนวทางปฏิบัติการควบคุมการเข้าถึงและสภาพแวดล้อมศูนย์ข้อมูล

1. บริษัทฯ มีการกำหนดให้พื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบเทคโนโลยีสารสนเทศต่างๆอย่างเหมาะสม โดยกำหนดพื้นที่รักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อป้องกันและควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต ที่อาจจะทำให้เกิดความเสียหายอื่นๆ ได้
2. กำหนดสิทธิให้กับเจ้าหน้าที่ที่มีสิทธิในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย ดังนี้
   2.1 กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า - ออก ดังกล่าวโดยจัดทำเป็นเอกสาร " บันทึกการเข้าออกห้องควบคุมระบบคอมพิวเตอร์ "
   2.2 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกห้องควบคุมระบบ ปีละ 1 ครั้ง เป็นอย่างน้อย
   2.3 บุคคลภายนอกเข้ามาติดต่อต้องลงชื่อขออนุญาตการเข้า – ออก ในแบบฟอร์มการเข้า – ออกให้ถูกต้อง และจะต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา
   2.4 บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าห้องควบคุมระบบคอมพิวเตอร์ ต้องตรวจสอบเหตุผลและ ความจำเป็นก่อนที่จะอนุญาต
3. ประกาศห้ามผู้ไม่เกี่ยวข้องเข้าห้องควบคุมระบบคอมพิวเตอร์ เว้นแต่ได้รับอนุญาตให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว แบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General working area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) เป็นต้น

1. วัตุประสงค์

เพื่อกำหนดมาตราการควบคุมและป้องกันบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย จากผู้บุกรุกหรือโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายหยุดทำงาน และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของบริษัทฯ ได้อย่างถูกต้อง

2. กระบวนการหลักในการควบคลุมเข้าถึงระบบ

2.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

2.2 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูล ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการทำงาน

2.3 ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้องมูลและระบบได้

2.4 ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของบริษัทฯ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

2.5 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า – ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

3. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1 ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ใน ระบบงานนั้นๆ

3.2 ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นเท่านั้น

3.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

4. การบริหารจัดการการเข้าถึงของผู้ใช้

4.1 ขั้นตอนการเตรียมพนักงานใหม่ของบริษัทฯ ควรกำหนดสิทธิต่างๆ ให้ตรงตามนโยบายควบคุมการใช้งานโปรแกรม และการเข้าถึงข้อมูลต่างๆ รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ สำหรับกรณีพนักงานลาออก – พักงาน ต้องทำภายใน 24 ชั่วโมง หรือ เมื่อเปลี่ยนตำแหน่งงานภายใน ต้องทำภายใน 7 วัน

4.2 ขั้นตอนการกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น โปรแกรมประยุกต์ (Application) จดหมาย อีเมล์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ และกรรมการผู้จัดการใหญ่เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

4.3 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่านของเจ้าหน้าที่

4.3.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของพนักงานในการเข้าระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบให้ตรงตามนโยบาย

4.3.2 กรณีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยพิจารณาดังนี้

- ควรได้รับความเห็นชอบและอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศและกรรมการผู้จัดการใหญ่
- ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว
- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุกๆ 3 เดือน
- ควรมีการบังคับไม่สามารถเปลี่ยนรหัสซ้ำของเดิมได้ย้อนหลัง อย่างน้อย 5 เวอร์ชั่น รวมถึงมีการบังคับการล็อกกรณีที่ผู้ใช้งานมีการใส่รหัสผิดมากกว่า 5 ครั้ง
- ควรมีการบังคับการใช้รหัสผ่านที่มีตัวอักษรณ์ไม่ต่ำกว่า 8 ตัว รวมถึงมีอักขระพิเศษ 1 ตัว

4.4 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

4.4.1 ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

4.4.2 เจ้าของข้อมูล จะต้องมีการตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4.4.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ล่ะประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้เข้าใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

4.4.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

4.4.5 ควรมีกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลประมาณ 1-3 เดือนต่อครั้ง

4.4.6 ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัทฯ เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

5. การบริหารจัดการการเข้าถึงระบบเครือข่าย

5.1 ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายที่มีการใช้งาน กลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

5.2 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

5.3 ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

5.4 ผู้ดูแลระบบ ควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆได้

5.5 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆของระบบเครือข่ายและอุปกรณ์ต่างๆที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและควรมีการทบทวนการกำหนด parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

5.6 ระบบเครือข่ายทั้งหมดของบริษัทฯ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกบริษัทฯ ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้ง ต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) / ไวรัส (Virus) ด้วย

5.7 การเข้าสู่ระบบงานเครือข่ายภายในบริษัทฯ โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการล็อกอินและต้องมีการพิสูจน์ ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง IP address ภายในของระบบงานข่ายภายในของบริษัทฯ จำเป็นต้องมีการป้องกันมิให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

5.8 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยกับขอบเขตของเครืองข่ายภายในและภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.9 การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็นการติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

6. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

6.1 กำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของระบบคอมพิวเตอร์อย่างชัดเจน

6.2 มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในการณีที่พบว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งรายงานโดยทันที

6.3 เปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น ftp หรือ ping เป็นต้น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการเพิ่มเติมด้วย

6.4 ติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น web server เป็นต้น

6.5 ทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

6.6 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์สารสนเทศเท่านั้น

7. การบริหารจัดการการบันทึกและตรวจสอบ

7.1 กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย 3 เดือน

7.2 มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

7.3 มีวิธีป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

8. การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์สารสนเทศ

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติดังนี้

8.1 การเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายขององค์กร ต้องควบคุมบุคคลที่จะเข้าสู่ระบบองค์กรจากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

8.2 วิธีการใดๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ ผู้ใช้ต้องปฏิบัติตามข้อกำหนดของบริษัทฯ ในการเข้าสู่ระบบและข้อมูลเคร่งครัด การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการ ดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้จัดการฝ่ายและผู้จัดการฝ่ายเทคโนโลยีสารสนเทศอย่างเป็นทางการมีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

8.3 การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น (Remote Access Management)

9. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

9.1 ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร ดังนี้

9.1.1 แสดงชื่อผู้ใช้งาน (Username)

9.1.2 ใส่รหัส (Password)

9.1.3 การตรวจสอบโดยระบบผ่านการเช็ค Mac Address/IP Address หรือวิธีการตรวจสอบอย่างอื่น

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทฯ ให้มีความลับความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานระบบปฏิบัติการ

2.1 ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

2.2 ผู้ใช้งานต้องตั้งค่าการใช้โปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพ เมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

2.3 ในการเข้าใช้ระบบปฏิบัติการใส่ User และ Password ทุกครั้ง

2.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของบริษัทฯ ร่วมกัน

2.5 ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

2.6 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer – to - Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา หรือผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

2.7 ห้ามไม่ให้ผู้ใช้ทำการติดตั้งหรือใช้งานซอฟท์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

2.8 ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟท์แวร์ที่บริษัทฯ จัดเตรียมไว้ให้ผู้ใช้งานเพื่อนำไปใช้งานที่อื่น

2.9 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของบริษัทฯ เพื่อประโยชน์ทางการค้า

2.10ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

2.11ห้ามผู้ใช้งานใช้ระบบเทคโนโลยีสารสนเทศของบริษัทฯ เพื่อควบคุมคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

3. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)
   3.1 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไขทันที
   3.2 ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลสียหายนั้นเกิดจากการกระทำของผู้อื่น
   3.3 ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอนจำหน่ายหรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
   3.4 ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการงานชั่วคราว

4. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)
   4.1 มีการกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ ระดับสิทธิของผู้ขออนุมัติและการระบุและพิสูจน์ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน
   4.2 ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟท์แวร์สำหรับระบบงาน
   4.3 มีการจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้
   4.4 ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟท์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

5. การหมดเวลาให้ระบบสารสนเทศ (Session time – out) ผ่าน Computer Server
   5.1 กำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการตัดและหมดเวลาการใช้งาน หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 15 นาที
   5.2 กำหนดให้ระบบเทคโนโลยีสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมใช้งานช่วงระยะ 15 นาทีเพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ
   5.3 กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนยีสารสนเทศที่มีความเสี่ยงสูง เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของบริษัทฯ โดยการกำหนดสิทธิของผู้ใช้งานการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้ง มีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

2.1 ผู้ใช้งานที่ต้องการเข้าระบบเครือข่ายไร้สายของบริษัทฯ จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ สำหรับกรณีนำเครื่องส่วนบุคคลมาใช้งานที่บริษัทฯ

2.2 ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3 ผู้ดูแลระบบ จะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

2.4 ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

2.5 ผู้ดูแลระบบ ควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

2.6 ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (default) มาจากผู้ผลิตทันทีที่นำ Access Point (AP) มาใช้งาน

2.7 ผู้ดูแลระบบ ควรเปลี่ยนค่า ชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบ ควรเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

2.8 ผู้ดูแลระบบ ต้องกำหนดค่าใช้ WPA หรือ WPA2 ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

2.9 ผู้ดูแลระบบ ควรจะมีการติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายใน

2.10ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย อย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2950 เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสั่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของบริษัทฯ ถูกระงับ ชะลอ ขัดขวางหรือรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

2.1 ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่บริษัทฯ จัดสรรไว้เท่านั้น เช่น Proxy, Firewall, LPSIDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่ออินเทอร์เน็ตผ่านช่องทางอื่น เช่น การนำ Wireless Router มาต่อใน ระบบเครือข่ายเพื่อใช้งาน เป็นต้น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้จัดการฝ่ายไอที

2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Wed browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

2.3 การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

2.4 ผู้ใช้งาน ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัทฯ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

2.5 ผู้ใช้งาน จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัทฯ

2.6 ผู้ใช้งาน ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ละเมิดสิทธิของผู้อื่น และข้อมูลที่อาจก่อความเสียหายให้กับบริษัทฯ

2.7 ใช้งาน ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทฯ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

2.8 ผู้ใช้งาน ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้ายหรือภาพที่มีลักษณะอันลามก และไม่ ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

2.9 ผู้ใช้งาน ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติม หรือดัดแปลงด้วยวิธิการทางอีเมล์ หรือวิธีการอื่นใด ทั้งนี้ จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

2.10ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

2.11ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่างๆ การดาวน์โหลดทุกประเภทต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

2.12ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของบริษัทฯ รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

2.13หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

1. วัตถุประสงค์

กำหนดมาตรการการใช้งานอีเมล์ผ่านระบบเครือข่ายของบริษัทฯ ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอีเมล์บนเครือข่าอินเทอร์เน็ตผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูและระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใดๆ ที่จะสร้าง ปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอีเมล์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการส่งอีเมล์

2.1 ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงระบบอีเมล์ของบริษัทฯ ให้เหมาะสมกับการ เข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การพักงานชั่วคราว เป็นต้น

2.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบอีเมล์ของบริษัทฯ

2.3 รหัสอีเมล์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น (*) ในการพิมพ์แต่ละตัวอักษร

2.4 ผู้ดูแลระบบ ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง

2.5 ผู้ใช้งาน ไม่ต้องตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ระบบอีเมล์

2.6 ผู้ใช้งาน ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุกๆ 3 เดือน

2.7 ผู้ใช้งาน ควรระมัดระวังในการใช้อีเมล์เพื่อไม่ให้เกิดความเสียหายต่อบริษัทฯ หรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงผลประโยชน์ในเชิงธุรกิจจากการใช้อีเมล์ผ่านระบบเครือข่ายของบริษัทฯ

2.8 ข้อห้าม ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กททรอนิกส์ (e - mail address) ของผู้อื่นเพื่ออ่าน รับ-ส่ง ข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของอีเมล์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในอีเมล์ของตน

2.9 ผู้ใช้งาน ควรใช้ที่อยู่จดหมายอีเมล์ของบริษัทฯ เพื่อการทำงานของบริษัทฯ เท่านั้น

2.10หลังจากการใช้งานระบบจดหมายอีเมล์เสร็จสิ้น ควรทำการล็อกเอ้าท์ออกจากระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอีเมล์

2.11ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอีเมล์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable fie เช่น .exe เป็นต้น

2.12ผู้ใช้งาน ไม่เปิดหรือส่งต่อจดหมายอีเมล์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

2.13ผู้ใช้งาน ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอีเมล์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของบริษัทฯ ทำให้เกิดความแตกแยกระหว่างบริษัทฯ ผ่านทางจดหมายอีเมล์

2.14ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอีเมล์

2.15ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอีเมล์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและ จดหมายอีเมล์ของตนให้เหลือจำนวนน้อยที่สุด

2.16ผู้ใช้งาน ควรลบจดหมายอีเมล์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณใช้เนื้อที่ระบบบน Host ที่ได้ทำการเช่าพื้นที่ในการเก็บเมล์

2.17ข้อควรระวังผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทอรนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอีเมล์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอีเมล์

1. วัตถุประสงค์

เพื่อการบริหารความปลอดภัยระบบเทคโนโลยีสารสนเทศและข้อมูล ระบบเครือข่าย โดยใช้ไฟร์วอลล์ ทำหน้าที่ควบคุมข้อมูลที่ผ่านเข้าออก ทั้งในด้านของการจำกัดการเชื่อมต่อและการจำกัดการใช้งานไฟร์วอลล์ จะทำหน้าที่กำหนดขอบเขตที่ควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ข้อมูลที่ผ่านเข้าออกไฟร์วอลล์จะเป็นข้อมูลที่ตรงตามที่นโยบายขององค์กรกำหนดไว้เท่านั้น

2. แนวทางปฏิบัติการใช้งานไฟร์วอลล์

2.1 ไฟร์วอลล์ต้องกำหนดเงื่อนไขของการเชื่อมต่อหรือการให้บริการที่ได้รับอนุญาตเท่านั้น

2.2 ในทุกเส้นทางการสื่อสารคอมพิวเตอร์ที่เข้าและออกจากบริษัทฯ จะต้องผ่านไฟร์วอลล์ ในการตรวจจับและกรองข้อมูล เพื่อความปลอดภัยในการรับส่ง-ข้อมูล

2.3 เครื่องคอมพิวเตอร์แม่ข่ายที่มีการเชื่อมต่อไปยังภายนอกองค์กร จะต้องจัดให้อยู่ใน DMZ (De - Militarize Zone) เสมอ

2.4 ผู้ดูแลระบบจะต้องตรวจสอบการทำงานของไฟร์วอลล์ จากบันทึกการทำงาน (log file) อย่างสม่ำเสมอ โดยอย่างน้อยทุกวันสุดสัปดาห์ และรายงานให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศทราบเป็นรายเดือน

2.5 การเปลี่ยนแปลงใดๆ ที่เกี่ยวกับไฟร์วอลล์ จะต้องได้รับการบันทึก อย่างน้อยต้องประกอบด้วยการตั้งค่าการเชื่อมต่อหรือบริการที่ได้รับอนุญาตตามที่ได้ตั้งกฎเอาไว

2.6 อุปกรณ์ไฟร์วอลล์จะต้องได้รับการป้องกันจากการเข้าถึงทางกายภาพ โดยจะต้องติดตั้งในห้องที่มีการรักษาความปลอดภัย มีการล็อกห้องโดยอนุญาตให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศที่ดูแลระบบเครือข่ายเท่านั้นที่สามารถเข้าถึงได้

2.7 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

2.8 จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุก3 เดือน หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

2.9 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

2.10บริษัทฯ มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

2.11การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายในจะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้จัดการฝ่ายที่สังกัดและผู้จัดฝ่ายเทคโนโลยีสารสนเทศก่อน

2.12ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

3. แนวทางปฏิบัติการใช้งานระบบเซิร์ฟเวอร์

3.1 เครื่องเซิร์ฟเวอร์มีการอัพเดทระบบปฏิบัติการให้เป็นรุ่นเวอร์ชั่นใหม่อยู่เสมอ

3.2 เครื่องเซิร์ฟเวอร์มีการติดตั้งโปรแกรมป้องกันไวรัส ทุกเครื่อง และ รุ่นเวอร์ชั่นจะต้องใหม่อยู่เสมอ

3.3 เครื่องเซิร์ฟเวอร์มีการบังคับเปลี่ยนรหัสเข้าใช้งานระบบทุกๆ 3 เดือน และ การตั้งรหัสผ่านไม่น้อยกว่า 8 ตัวอักษร

3.4 เครื่องเซิร์ฟเวอร์มีการบันทึกกิจกรรมของผู้ใช้งาน และ กิจกรรมของระบบอย่างน้อยเป็นเวลา 3 เดือน

3.5 เครื่องเซิร์ฟเวอร์มีการตั้ง Policy ในการปิด และ เปิดช่องทางเชื่อมต่อ(Port) การใช้งานให้ตรงกับระบบนั้นๆ เพื่อความปลอดภัย และป้องกันการโจมตี เช่น ระบบ SAPB1 ใช้งานพอร์ท (Port) 40000 ส่วนที่เหลือก็ทำการปิดการใช้งาน

1. วัตถุประสงค์

เพื่อป้องกันระบบเทคโนโลยีสารสนเทศและข้อมูลระบบเครือข่ายจากซอฟต์แวร์ไม่ประสงค์ดีและไวรัสต่าง ๆ

2. แนวทางปฏิบัติการป้องกันไวรัสและซอฟต์แวร์ไม่ประสงค์ดี

2.1 เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสรุ่นล่าสุดที่ได้รับการอนุมัติจากบริษัทฯ และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง

2.2 เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุด (Update Latest Pattern) อยู่เสมอ เครื่องให้บริการ เครื่องตั้งโต๊ะ และโน้ตบุ๊ค ทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส

2.3 การติดตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุกเดือน

2.4 ห้ามทำการดาวน์โหลดแชร์แวร์หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต โดยปราศจากการอนุมัติจากบริษัทฯ หลังจากการอนุมัติแล้ว เจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัสก่อนการใช้งาน

2.5 ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมลล์ สำเนาจากแผ่นดิสค์หรือไฟล์แชร์ต่างๆ ต้องได้รับการสแกนหาไวรัส

2.6 ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใดๆ ตัวอย่างเช่น ไวรัส หนอนอินเทอร์เน็ตโปรแกรมแฝง (ม้าโทรจัน) อีเมลล์บอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ขององค์กร

2.7 ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

2.8 ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้นที่ได้รับอนุญาตให้สามารถรับ – ส่งผ่านระบบเครือข่ายขององค์กรได้ ทั้งนี้ ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักและจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสขององค์กร ก่อนเปิดใช้งานเสมอ

2.9 เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชั่นการทำงานเชื่อมต่อกับอินเทอร์เน็ต ยกเว้น ในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

1. วัตถุประสงค์

1.1 เพื่อสำรองข้อมูลของระบบต่างๆ อย่างสม่ำเสมอ ป้องกันการสูญเสียและสูญหายของข้อมูลและสามารถนำข้อมูลดังกล่าวมาใช้เมื่อยามจำเป็น

1.2 เพื่อป้องกันความเสี่ยงที่บริษัทฯ อาจสูญเสียข้อมูลจากสื่อบันทึก หรือกรณีเกิดสถานการณ์ฉุกเฉินกับศูนย์คอมพิวเตอร์ ทำให้ไม่สามารถนำระบบกลับคืนสู่จุดที่เป็นปัจจุบันได้

1.3 เพื่อเตรียมความพร้อมให้ระบบการทำงานสามารถทำงานได้อย่างต่อเนื่อง

1.4 เพื่อให้มั่นใจว่าสื่อบันทึกข้อมูลที่ได้ทำการสำรองไปนั้น สามารถนำกลับมาใช้ได้จริง

2. แนวทางปฏิบัติในการสำรองข้อมูลและกู้คืนระบบคอมพิวเตอร์

2.1 ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และ ให้เป็นไปตามนโยบายการสำรองข้อมูลของบริษัทฯ

2.2 มีขั้นตอนการปฏิบัติการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์ และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

2.3 การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

2.4 ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลให้กับเจ้าหน้าที่คนอื่นเพื่อช่วยสำรองข้อมูลในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ / หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

2.5 ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ให้ดำเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อกรรมการผู้จัดการใหญ่

2.6 ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมี 2 ชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Back up) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

2.7 การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

2.8 นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup and Restore Procedure โดยเคร่งครัด

3. การปฏิบัติเกี่ยวกับการสำรองข้อมูล

3.1 ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูล

3.2 ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการแบ็คอัพถูกต้องสมบูรณ์หรือไม่

4. การกู้คืนระบบ

4.1 ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงานต่อผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

4.2 ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

4.3 หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะๆ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์ให้กรรมการผู้จัดการใหญ่

4.4 ต้องมีการทดสอบการกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง

4.5 นอกจากนี้ บริษัทฯ จะจัดให้มีการทบทวนนโยบายฝ่ายไอที เพื่อให้สอดคล้องกับสภาวการณ์และธุรกิจของบริษัทฯ ทั้งนี้ต้องได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัทเสมอ

1. วัตถุประสงค์

นโยบายนี้มีแนวทางการบริหารงานของสินทรัพย์และทรัพยากรเทคโนโลยีสารสนเทศในธุรกิจ ซึ่งเป็นแนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศในระดับองค์กร เพื่อเป็นแนวทางปฏิบัติในการกำกับดูแลและบริหารจัดการทางด้านเทคโนโลยีสารสนเทศของบริษัทฯ เพื่อสามารถการจัดสรรทรัพยากรสารสนเทศอย่างมีประสิทธิภาพ ประสิทธิผล ปลอดภัย สร้างความมั่นใจถึงคุณภาพของเทคโนโลยีสารสนเทศเพื่อใช้ในการตัดสินใจในทุกระดับ ความมั่นใจต่อการให้คำแนะนำในการดูแลระบบต่างๆ ถูกดำเนินไปตามจริยธรรมและเป็นที่ยอมรับได้ รวมถึงการบริหารงานและการปฏิบัติหน้าเป็นไปตามกฎหมาย ระเบียบข้อบังคับหรือมาตรฐานสากลทางด้านไอทีที่เกี่ยวข้อง

2. แนวทางปฏิบัติในการควบคุมผู้ดูแลระบบ(Administrator)

2.1 เมื่อผู้ดูแลระบบมีเหตุอันควรหรือสงสัยสำหรับสาเหตุที่เกี่ยวข้องกับการเกิดผลกระทบต่างๆต่อระบบ และ การใช้งานระบบ ผู้ดูแลระบบมีสิทธิที่จะตรวจสอบทุกแง่มุมของกิจกรรมของผู้ใช้งานเพื่อตรวจสอบว่าผู้ใช้ได้ละเมิดกฎหรือนโยบายต่างๆหรือไม่ รวมถึงการเข้าถึงระบบการล็อกอินบัญชีผู้ใช้ ข้อมูลไฟล์ ประวัติการใช้งานต่างๆ อีเมล์ และ ข้อความสนทนา

2.2 ผู้ดูแลระบบจะต้องเคารพสิทธิความเป็นส่วนตัวของผู้ใช้งานและจะได้มีส่วนในการดำเนินการที่จะละเมิดต่อ การทำงาน ข้อมูลต่างๆ ที่นอกเหนือจากหน้าที่ปฏิบัติ ในการเข้าถึงหรือตรวจสอบโดยไม่มีสาเหตุ นอกจากนี้ผู้ดูแลระบบจะต้องได้รับความยินยอมที่จะเข้าสู่บัญชีของผู้ใช้จากการร้องขอ หรือ ได้รับอนุมัติจากผู้ใช้งาน หัวหน้าฝ่าย กรรมการบริษัท หรือผู้มีอำนาจในการตัดสินใจในแต่ละเคสของการแจ้งเรื่องเท่านั้น ถ้านอกเหนือจากการร้องขออนุมัติตรวจสอบ จะถือว่าเป้นการทำเกินหน้าที่ เข้าข่ายขัดต่อจริยธรรมองค์กร พยายามล่วงรู้ข้อมูลอันไม่พึงทราบ ซึ่งจะถือว่าผิดวินัยบริษัทฯ และ จะต้องถูกคาดโทษและดำเนินตามกฎบริษัทฯ ต่อไป

2.3 ผู้ดูแลระบบมีสิทธิที่จะสร้าง แก้ไข เพิ่ม ลบไฟล์ระบบ แต่ต้องผ่านการเห็นชอบจากหัวหน้างานฝ่ายไอทีเสมอ

2.4 ผู้ดูแลระบบจะต้องมีการแจ้งหรือประกาศอย่างเป็นทางการทุกครั้งเมื่อมีการปรับปรุงระบบ ที่สร้างผลกระทบโดยรวมต่อการทำงาน หรือ การปิดระบบเพื่อบำรุงรักษาต่างๆ เช่น การอัพเกรด ซ่อมแซม ปิดระบบชั่วคราวจากภัยธรรมชาติ ระบบไฟฟ้าท้องถิ่นขัดข้อง หรือ ปัจจัยต่างๆ เพื่อให้ผู้ใช้งานระบบทราบข้อมูลข่าวสารในการเตรียมแผนการทำงานระหว่างช่วงระบบปิด และ การเลือกวันเวลาในการปิดระบบถ้าไม่ใช่เหตุสุดวิสัย ควรจะต้องคำนึงถึงวันเวลาที่มีการใช้งานน้อย

2.5 ผู้ดูแลระบบมีหน้าที่รับผิดชอบอุปกรณ์ไอทีทั้งหมด ที่อยู่ในความรับผิดชอบของฝ่ายไอที

2.6 ผู้ดูแลระบบมีสิทธิ์เข้าถึงข้อมูลระบบ บริหารจัดการทรัพยาการระบบต่างๆ ทั้งทางกายภาพ และ เชิงโปรแกรม แต่ต้องปฏิบัติหน้าที่โดยซอบธรรม ไม่เป็นส่วนที่สร้างภัยคุกคามต่อตัวระบบเอง ต้องอยู่บนบรรทัดฐานการทำงานแบบรัดกุม รอบครอบ รวมถึงต้องมีการรายงานการทำงาน หรือ การปฏิบัติหน้าที่ทุกครั้งต่อหัวหน้างานฝ่ายไอทีเสมอ เพื่อตรวจสอบขั้นตอนก่อนการทำงาน หรือ ขออนุมัติการทำงานที่มีความเสี่ยงสูงต่อระบบ ทั้งทางกายภาพ และ ทางโปรแกรม

2.7 ผู้ดูแลระบบจะไม่มีส่วนในการรับผิดซอบต่อการกระทำของผู้ใช้ที่สร้างความเสียหายต่อข้อมูล ระบบบริษัทฯ ทั้งทางกายภาพ และ ทางระบบของส่วนบุคคล แต่จะเป็นฝ่ายสนับสนุนให้ความช่วยเหลือในกรณีต่างๆ หรือ การหาแนวทางเพื่อป้องกันภัย

1. วัตถุประสงค์

เพื่อเป็นแนวทางในการเลือกซอฟต์แวร์ทั้งหมด และ การนำมาใช้งาน ถูกลิขสิทธิ์ เหมาะสม คุ้มค่า และทำงานรวมกับเทคโนโลยีต่างในองค์กร หรือ ทำงานร่วมกับระบบธุรกิจต่างๆที่เกี่ยวข้องได้เป็นอย่างดี เพื่อป้องกันความเสี่ยงของทางบริษัทฯ ที่เกี่ยวกับซอฟต์แวร์ไม่ถูกลิขสิทธิ์ หรือ ไม่ได้มาตรฐาน ที่จะมีการแอบแฝงด้วย Spam, Malware หรือช่วงโหว่ที่จะถูก Hacker โจมตี รวมถึงการป้องกันชื่อเสียงและภาพลักษณ์ที่ดีให้กับองค์กร

2. แนวทางปฏิบัติในการเลือกและนำซอฟต์แวร์มาใช้งาน(Software Management)

2.1 การควบคุมการติดตั้งใช้งานซอฟต์แวร์ต่างๆ อยู่ภายใต้การดูแลควบคุมจากฝ่ายไอที และ จากระบบเพื่อป้องกันการติดตั้งซอฟต์แวร์ที่ผิดลิขสิทธิ์ หรือ ไม่ได้มาตรฐานต่างๆ

2.2 การขอใช้งานซอฟต์แวร์ทางเลือก(Open Source) นอกจากชุดซอฟต์แวร์มาตรฐานที่ทางฝ่ายไอทีจะต้องทำการตรวจสอบซอฟต์แวร์ดังกล่าวในแง่ ความปลอดภัย ประสิทธิ์ภาพการใช้งาน อยู่เสมอ

2.3 การขอใช้งานซอฟต์แวร์มาตรฐานหรือซอฟต์แวร์ที่มีลิขสิทธิ์ในการน าไปใช้งาน

2.3.1 จะต้องอยู่ภายใต้นโยบายฝ่ายไอที ที่ระบุถึงการแจ้งเรื่องขออนุมัติผ่านแบบฟอร์มไอที (IT REQUEST FORM)

2.3.2 เนื้อหาแบบฟอร์มจะประกอบไปด้วยข้อมูลชื่อผู้ประสงค์ใช้งาน ตำแหน่ง ฝ่าย สถานที่ปฏิบัติงาน และข้อมูลซอฟต์แวร์ที่ต้องการใช้งาน

2.3.3 การอนุมัติการใช้งานประกอบไปด้วยหัวหน้าฝ่าย หัวหน้าฝ่ายไอที และกรรมการผู้จัดการใหญ่

2.4 การตรวจสอบการใช้งานซอฟต์แวร์มาตรฐานหรือซอฟต์แวร์ที่มีลิขสิทธิ์ประจำปี อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าการใช้งานคอมพิวเตอร์ และ เครื่องแม่ข่ายทุกเครื่องใช้งานด้วยซอฟต์แวร์ที่มีลิขสิทธิ์

1. วัตถุประสงค์

นโยบายการรายงานข้อมูลการปฏิบัติงานฝ่ายไอทีจัดทำขึ้นเพื่อเป็นมาตรฐานในการรายงานการปฏิบัติงานทั้งในส่วนการดำเนินงานทั่วไป การร้องขอช่วยเหลือผู้ใช้งานระบบ ข้อมูลรายงานทรัพย์สิน การดำเนินงานแบบโปรเจค การจัดซื้ออุปกรณ์ไอทีต่างๆ งบประมาณการเบิกจ่ายต่างๆ รวมถึงข้อมูลสถานะของระบบ ทั้งในส่วนสถานะการทำงานของเซิฟเวอร์ สถานะการสำรองข้อมูล เป็นต้น เพื่อให้ทุกๆการปฏิบัติงาน และระบบต่างๆเป็นไปด้วยความเรียบร้อย และ มั่นใจว่ายังทำงานปกติ ไม่ได้มีส่วนบกพร่อง สามารถรองรับการทำงานได้อย่างต่อเนื่อง และ มีความน่าเชื่อถืออยู่เสมอ

2. แนวทางปฏิบัติการรายงานทั่วไปต่อผู้จัดการฝ่าย

2.1 การแจ้งรายงานสถานการณ์แก้ไขปัญหาไอทีและการร้องขอต่างๆ (Issue & Request Status)

2.2 การแจ้งรายงานสถานะการจัดซื้ออุปกรณ์ฝ่ายไอทีต่างๆ (Purchasing Status)

2.3 การแจ้งรายงานสถานะการทำงานและข้อมูลกิจกรรม (Log) ของระบบเครือข่ายคอมพิวเตอร์ต่างๆ (Network Status)

2.4 การแจ้งรายงานสถานะและข้อมูลกิจกรรม (Log) การทำงานของระบบเซิร์ฟเวอร์ ต่างๆ (Server System Status)

2.5 การแจ้งรายงานสถานะการทำงานและข้อมูลกิจกรรม (Log) ของระบบป้องกันภัยต่างๆ (Cyber Security Status)

3. แนวทางปฏิบัติการรายงานปัญหาเร่งด่วน และ วิกฤตต่างๆ ต่อกรรมการผู้บริหารใหญ่ ทันที

3.1 การแจ้งรายงานสถานะการทำงานผิดปกติของระบบเครือข่ายคอมพิวเตอร์ต่างๆ (Network Status)

3.1.1 รายงานระบบเครือข่ายทำงานผิดปกติ ล้าช้า และ แนวทางการแก้ไขปัญหา

3.1.2 รายงานระบบอินเตอร์เน็ตล่ม เชื่อมต่อไม่ได้ และ แนวทางการแก้ไขปัญหา

3.2 การแจ้งรายงานสถานะการทำงานผิดปกติของระบบเซิร์ฟเวอร์ต่างๆ (Server System Status)

3.2.1 รายงานระบบเซิร์ฟเวอร์ทำงานผิดปกติ ล่าช้า และ แนวทางการแก้ไขปัญหา

3.2.2 รายงานระบบเซิร์ฟเวอร์ล่ม เชื่อมต่อไม่ได้ และ แนวทางการแก้ไขปัญหา

3.2.3 รายงานระบบเซิร์ฟเวอร์ทรัพยากรเต็ม เช่น ซีพียู หน่วยความจำ พื้นที่ และ แนวทางการแก้ไขปัญหา

3.3 การแจ้งรายงานสถานะการทำงานผิดปกติของระบบป้องกันภัยต่างๆ (Cyber Security Status)

3.3.1 ระบบเครือข่ายคอมพิวเตอร์ถูกโจมตี ส่งผลให้ระบบเครือข่ายล่ม และ แนวทางการแก้ไขปัญหา

3.3.2 ระบบเซิร์ฟเวอร์ถูกโจมตีส่งผลทบต่อระบบ ฐานข้อมูลต่างๆ และ แนวทางการแก้ไขปัญหา

4. แนวทางปฏิบัติในการรายงานรายเดือน และ รายไตรมาสต่อกรรมการผู้จัดการใหญ่
   4.1 รายงานสรุปสถานะการทำงานและปัญหาต่างๆของไอทีโปรเจคประจำปี และ แผนงานปรับปรุงแก้ไข
   4.2 รายงานสรุปสถานการณ์ทำงานและปัญหาต่างๆของระบบเซิร์ฟเวอร์และระบบเครือข่าย รวมถึงแผนงานปรับปรุงแก้ไข
   4.3 รายงานสรุปสถานะการทำงานและปัญหาต่างๆของระบบสำรองข้อมูล และ แผนงานปรับปรุงแก้ไข
   4.4 รายงานสรุปสถานะการทำงานและปัญหาต่างๆของระบบความปลอดภัย และ แผนงานปรับปรุงแก้ไข

5. แนวทางปฏิบัติในการรายงานประจำปีต่อกรรมการผู้บริหารใหญ่
   5.1 รายงานสรุปการสิทธิ์ในการเข้าถึงข้อมูลระบบต่างๆ (Authorization Matrix)
   5.2 รายงานสรุปการจัดซื้อและยอดเบิกจ่ายประจำปี (IT Yearly Budget)
   5.3 รายงานสรุปโปรเจคประจำปี (IT Yearly Project)
   5.4 รายงานสรุปการทำงานและปัญหาต่างๆ ของระบบเซิร์ฟเวอร์ (System Performance)
   5.5 รายงานการทำงานและปัญหาต่างๆ ของระบบสำรองข้อมูล การทดสอบการกู้คืนระบบประจำปี (Backup and Recovery)
   5.6 รายงานสรุปการทำงานและปัญหาต่างๆ ของระบบความปลอดภัย (Cyber Security)

คำนิยาม ที่ใช้ในนโยบายนี้ ประกอบด้วย

- องค์กร หมายถึง บริษัท ยูโร ครีเอชั่นส์ จำกัด (มหาชน)
- หน่วยงาน หมายถึง ฝ่ายรวมถึงฝ่ายงานย่อยต่างๆ ในองค์กร
- ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างขององค์กร
- พนักงาน หมายถึง พนักงานและลูกจ้างขององค์กร รวมถึงบุคคลอื่นที่องค์กรมอบหมายให้ปฏิบัติงานตามสัญญาข้อตกลง
- หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานที่บริษัทฯ อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
- เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆหรือเป็นผู้ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
- การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง กรตรวจสอบ การอนุมัติ และการกำหนดสิทธิในการผ่านเข้าสู่ระบบสารสนเทศให้แก่ผู้ใช้งาน โดยที่เจ้าของข้อมูลอนุญาตให้ใช้งานระบบสารสนเทศนั้นได้
- การพิสูจน์ยืนยันตัวตน (Authentication) หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
- ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงาน ที่นำเอาเทคโนโลยีสารสนเทศของคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศ ที่หน่วยงานที่สามารถ นำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูล และสารสนเทศ เป็นต้น
- ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- ระบบแลน (LAN) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
- ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

- จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้
- ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ
- ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของบริษัทฯ ได้ เช่น ระบบแลน (LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น
- รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
- Virus และชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ลบไฟล์ของผู้ใช้ ทำงานช้าลงเรื่อยๆ โปรแกรมสำเร็จรูปต่างๆไม่ทำงานและทำความเสียหายต่อฮาร์ดดิสก์ เป็นต้น
- ไฟร์วอลล์ (Firewall) หมายถึง ระบบควบคุมการเข้า - ออกของข้อมูลบนเครือข่าย สำหรับป้องกันการบุกรุกหรือการโจมตี จากเครือข่ายภายในและภายนอก
- ระบบเครือข่ายไร้สาย (Wireless) หมายถึง ระบบเครือข่ายสื่อสารข้อมูล โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ
- WEP (Wired Equivalent Privacy) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าตัวเลขนี้
- WPA (Wi Fi Protected Access) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

- แผนสถานการณ์ฉุกเฉิน หมายถึง ข้อปฏิบัติในการแก้ไขปัญหาเมื่อเกิดสถานการณ์ฉุกเฉิน แบ่งเป็น 3 ด้าน ได้แก่ แผนรองรับสถานการณ์ฉุกเฉิน BCP (Business Contingency Plan) แผนดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ ใช้งานได้ต่อเนื่อง (Continuity of Operation Plan) และแผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure)
- สถานการณ์ความเสี่ยง หมายถึง ความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศ สามารถแยกเป็นภัยต่างๆ ได้แก่ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error), ภัยที่เกิดจากไฟไหม้หรือระบบไฟฟ้า และภัยที่เกิดจากน้ำท่วม (อุทกภัย) เป็นต้น
- ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิด ของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
- Powerful User หมายถึง ผู้จัดการสูงสุดในแต่ละระบบในด้านระบบคอมพิวเตอร์ เช่น OS, Application ต่างๆ ฐานข้อมูล (Database)
- Account / User Account หมายถึง บัญชีของผู้ใช้งานในระบบคอมพิวเตอร์ เพื่อเข้าใช้งานในระบบต่างๆ
- IP Address หมายถึง หมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอลแบบ TCP/IP
- Application หมายถึง ระบบงานประยุกต์ หรือโปรแกรมสำเร็จรูป
- Encryption หมายถึง เทคโนโลยีการเข้าและถอดรหัสข้อมูลด้วยโปรโตคอล
- Network Diagram หมายถึง รูปแบบระบบเครือข่าย
- OS (Operating System) หมายถึง ระบบปฏิบัติการที่ใช้กับระบบคอมพิวเตอร์
- Peer-to-Peer หมายถึง เครือข่ายแบบนี้จะเก็บไฟล์และการเชื่อมต่อกับอุปกรณ์ต่างๆ ไว้ที่เครื่องคอมพิวเตอร์ของ ผู้ใช้แต่ละคน โดยไม่มีคอมพิวเตอร์ส่วนกลางที่ทำหน้าที่นี้
- Internal Zone หมายถึง ระบบเครือข่ายภายในองค์กรของเรา ซึ่งถือว่าเป็น Zone ที่มีความปลอดภัยและน่าเชื่อถือสูงสุด
- External Zone หมายถึง ระบบเครือข่ายภายนอก ซึ่งถือว่าเป็น zone ที่มีความปลอดภัยต่ำมาก (ทั้งนี้ไม่ได้หมายความว่า เครือข่ายนอกองค์ของเรานั้น จะเป็นเครือข่ายที่ไม่น่าเชื่อถือ) อย่างไรก็ตามเนื่องเราอาจจำเป็นต้องมีการติดต่อกับเครือข่ายภายนอก ดังนั้น เราจำเป็นจะต้องมีการควบคุมในเรื่องของการสื่อสาร ตัวอย่าง External Zone เช่น คอมพิวเตอร์ต่างๆ ภายนอกองค์กร รวมทั้งระบบเครือข่าย internet ที่เราติดต่ออยู่ด้วย เป็นต้น

- Demilitarized Zone (DMZ) หมายถึง Zone พิเศษที่ไม่ใช่ทั้ง Internal Zone และ External Zone การทำงานของ DMZ นั้น จะติดต่อโดยตรงทั้ง Internal และ External Zone ตัวอย่างของ DMZ เช่น Mail server, Web server เป็นต้น
- Parameter หมายถึง ค่า ซึ่งอาจจะเป็นจำนวนเลข หรือตัวอักขระ ที่ใช้ในการสร้างสมการหรือคำสั่ง
- Log file หมายถึง ข้อมูลที่ถูกส่งออกไปและข้อมูลที่เข้ามาในองค์กรด้วยการเชื่อมต่อกับอินเตอร์เน็ต ซึ่งถือว่าเป็นการจราจรบนอินเตอร์เน็ต
- SSID หมายถึง ชื่อของ Wireless LAN ซึ่งผู้ให้บริการแต่ละรายจะมี SSID ที่แตกต่างกัน
- Remote access หมายถึง การเข้าถึงคอมพิวเตอร์หรือเครือข่ายจากระยะทางไกล ในบริษัทฯ หรือ สาขาของบริษัทฯ
- Gateway หมายถึง เป็นอุปกรณ์ที่มีความสามารถสูงในการเชื่อมต่อเครือข่ายต่างๆ เข้าด้วยกัน โดยสามารถเชื่อมต่อ LAN หลายๆ เครือข่ายที่ใช้โปรโตคอลต่างกัน

นอกจากนี้ บริษัทฯ จะจัดให้มีการทบทวนนโยบายด้านเทคโนโลยีสารสนเทศ เพื่อให้สอดคล้องกับสภาวการณ์และธุรกิจของบริษัทฯ

นโยบายด้านเทคโนโลยีสารสนเทศฉบับนี้ได้รับการทบทวนจากที่ประชุมคณะกรรมการบริษัทครั้งที่ 5/2568 เมื่อวันที่ 14 พฤศจิกายน 2568 และมีผลใช้บังคับทันที

(.....)

นายโกมล กัมบีร์

ประธานกรรมการบริษัท

บริษัท ยูโร ครีเอชั่นส์ จำกัด (มหาชน)

การจัดการเอกสาร

ชื่อเอกสาร:	นโยบายด้านเทคโนโลยีสารสนเทศ
ชื่อไฟล์:	นโยบายด้านเทคโนโลยีสารสนเทศ.docx
ผู้ดูแลเอกสาร	แผนกเทคโนโลยีสารสนเทศ

การจัดทำ/แก้ไข

เวอร์ชั่น	วันที่จัดทำ/แก้ไข	ผู้จัดทำ	ผู้ทบทวน/อนุมัติ
1.0.0	30 มิถุนายน 2566 / -	นาย พิทักษ์สิน สมวงศ์	คณะกรรมการบริหาร / คณะกรรมการบริษัท
1.0.0	- / 12 พฤศจิกายน 2567	แผนกเทคโนโลยีสารสนเทศ	คณะกรรมการบริหาร / คณะกรรมการบริษัท
1.0.0	23 กันยายน 2568 / 14 พฤศจิกายน 2568 /	แผนกเทคโนโลยีสารสนเทศ	คณะกรรมการบริหาร / คณะกรรมการบริษัท