บริษัท สุพรีม ดิสทิบิวชั่น จำกัด (มหาชน)

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

Rev.02

ผ่านการพิจารณาจากคณะกรรมการบริหาร เมื่อวันที่ 6 กันยายน 2567

1. วัตถุประสงค์

1.1 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ของบริษัท สุพรีม ดิสทิบิวชั่น จำกัด (มหาชน) (“บริษัทฯ”) เพื่อให้การดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล บริษัทฯ จึงกำหนดนโยบายการควบคุมระบบเทคโนโลยีสารสนเทศไว้

1.2 เพื่อกำหนดแนวทางปฏิบัติและวิธีปฏิบัติ การควบคุมดูแล ติดตาม ให้ผู้บริหาร พนักงาน ผู้ดูแลระบบ ผู้เกี่ยวข้อง และบุคคลภายนอกที่ปฏิบัติงานให้กับบริษัทฯ ได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ รวมทั้งการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2. ขอบเขต

นโยบายฉบับนี้ครอบคลุมทรัพยากรต่างๆ ระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ของบริษัทฯ ประกอบด้วย

2.1 พนักงานและลูกจ้างของบริษัทฯ ทั้งหมด

2.2 เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต่าง ๆ

2.3 เครื่องคอมพิวเตอร์ส่วนบุคคล

2.4 อุปกรณ์เครือข่าย อุปกรณ์เครือข่ายไร้สาย

2.5 ระบบไฟฟ้าสำรอง

2.6 ระบบข้อมูลสารสนเทศของบริษัทฯ ทั้งหมด

2.7 อุปกรณ์จัดเก็บข้อมูลของบริษัทฯ

2.8 ซอฟท์แวร์ระบบงานต่างๆ ซอฟท์แวร์พัฒนาเองหรือจ้างพัฒนา ซอฟท์แวร์สำเร็จรูป

3. คำนิยามศัพท์

บริษัทฯ : บริษัท สุพรีม ดิสทิบิวชั่น จำกัด (มหาชน)

ผู้ใช้งาน : พนักงานและลูกจ้างของบริษัทฯ ที่ได้รับอนุญาตให้ใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ

ผู้ดูแลระบบ : พนักงานและลูกจ้างของบริษัทฯ ที่ทำหน้าที่รับผิดชอบในการบริหารจัดการดูแลระบบสารสนเทศต่างๆ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อจัดการฐานข้อมูล รวมถึง System Administrator, Network Administrator, Database Administrator

บุคคลภายนอก: บุคคลซึ่งบริษัทฯ อนุญาตให้ใช้สิทธิในการเข้าถึงข้อมูลหรือระบบสารสนเทศที่ได้รับสิทธิ์ตามประเภทการใช้งาน และต้องรับผิดชอบในการไม่เปิดเผยข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต

4. ความรับผิดชอบ

ผู้อำนวยการ : รับผิดชอบการอนุมัติใช้งาน ติดตามใช้งานและเก็บรักษารหัสผู้ใช้สิทธิสูง

ผู้จัดการฝ่าย : รับผิดชอบการอนุมัติสิทธิการใช้งานระบบต่างๆ ให้กับผู้ใช้งานตามหน้าที่ความรับผิดชอบตำแหน่งงาน

ผู้ดูแลระบบ : รับผิดชอบในการบริหารจัดการดูแลระบบสารสนเทศต่างๆ การควบคุมสิทธิการใช้งานของผู้ใช้งาน

พนักงานและลูกจ้าง : รับผิดชอบปฏิบัติตามนโยบายอย่างเคร่งครัด

เจ้าหน้าที่ IT : ดูแล บริหารจัดการ การแก้ไขและบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมถึงระบบเครือข่าย

5. รายละเอียดนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

5.1 นโยบายรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Policy)

วัตถุประสงค์

เพื่อให้การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นทรัพยากรที่สำคัญที่เอื้ออำนวยความสะดวกและก่อประโยชน์ต่อการดำเนินธุรกิจ ให้สามารถดำเนินงานได้อย่างต่อเนื่อง ให้ผู้บริหาร พนักงานและผู้เกี่ยวข้องถือปฏิบัติ รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ หากไม่ระมัดระวังรอบคอบหรือใช้งานไปในทางมิชอบก็เกิดผลเสียหายต่อบริษัทฯและผู้ใช้เช่นกัน

แนวทางปฏิบัติ

1. จัดทำนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและมีการทบทวน ปรับปรุงสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และนโยบายต้องได้รับการอนุมัติจากผู้บริหารหรือผู้มีอำนาจที่ได้รับมอบหมาย
2. จัดทำนโยบายเป็นลายลักษณ์อักษรและสื่อสารให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องรับทราบ เข้าถึงได้ง่าย

5.2 การแบ่งแยกอำนาจหน้าที่

วัตถุประสงค์

มอบหมายแบ่งแยกอำนาจหน้าที่ ความรับผิดชอบให้เหมาะสม เพื่อควบคุมกำกับดูแล และบริหารจัดการ ลดความเสี่ยง และการรักษาความมั่งคงปลอดภัยของระบบสารสนเทศ ให้สามารถนำระบบเทคโนโลยีสารสนเทศมาใช้ประกอบธุรกิจให้บรรลุเป้าหมายได้ตลอดเวลา

แนวทางปฏิบัติ

1. จัดให้มีการกำหนดหน้าที่ ความรับผิดชอบให้เหมาะสมของแต่ละตำแหน่งไว้ชัดเจน
2. สื่อสารให้พนักงานทราบถึงขอบเขต และวิธีการปฏิบัติงานของตนที่ได้กำหนดไว้

5.3 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

วัตถุประสงค์

เพื่อให้มีมาตรการ การป้องกันความปลอดภัยต่อศูนย์คอมพิวเตอร์และระบบเครือข่ายของบริษัทฯ ไม่ให้มีผลกระทบกับระบบงาน และการใช้งานระบบต่างๆ และการบริหารจัดการทรัพยากรได้อย่างมีประสิทธิภาพ ซึ่งไม่ให้เกิดช่องโหว่หรือระบบถูกโจมตีจากผู้ไม่ประสงค์ดีกับบริษัทฯ ให้ได้รับความเสียหาย รวมถึงข้อมูลและระบบข้อมูลที่อาจรั่วไหลไปยังผู้ไม่ประสงค์ดีได้

แนวทางปฏิบัติ การเข้าออกศูนย์คอมพิวเตอร์

1. กำหนดการเข้าออกศูนย์คอมพิวเตอร์ ทั้งบุคคลภายในและบุคคลภายนอก ต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติทุกครั้ง
2. กำหนดให้มีการบันทึกการเข้าออกศูนย์คอมพิวเตอร์ของบริษัทฯ ต้องมีรายละเอียดเกี่ยวกับบุคคลที่เข้าออก วัน/เวลาที่เข้าออก เหตุผลการเข้าถึงพื้นที่ศูนย์คอมพิวเตอร์ และมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
3. สำหรับบุคคลที่ไม่มีหน้าที่เกี่ยวข้องหรือบุคคลภายนอก หากมีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ ต้องกำหนดให้มีเจ้าหน้าที่ปฏิบัติประจำศูนย์คอมพิวเตอร์ ควบคุมดูแลตลอดเวลาระหว่างบุคคลดังกล่าวอยู่ในศูนย์คอมพิวเตอร์
4. กำหนดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานในศูนย์คอมพิวเตอร์ สำหรับบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ หรือบุคคลภายนอกตามที่บริษัทฯ กำหนด

แนวทางปฏิบัติ การป้องกันความเสียหาย

1. มีอุปกรณ์ตรวจจับควันหรืออุปกรณ์ตรวจจับความร้อน เพื่อป้องกันหรือระงับเหตุได้ทันเวลา
2. มีการติดตั้งถังดับเพลิงไว้ในศูนย์คอมพิวเตอร์ โดยสารเคมีที่ใช้ต้องเป็นสารที่ใช้สำหรับประเภทคอมพิวเตอร์โดยเฉพาะ
3. จัดให้มีเครื่องสำรองไฟฟ้าสำหรับเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย ซึ่งเครื่องสำรองไฟฟ้าต้องสามารถสำรองไฟฟ้าได้ไม่น้อยกว่า 10 นาที และทำการตรวจสอบเครื่องสำรองไฟทุกๆ 3 เดือน
4. กำหนดให้ควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม และต้องตรวจสอบอุณหภูมิและความชื้นอย่างสม่ำเสมอ

5.4 การควบคุมการใช้บริการด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

วัตถุประสงค์

เพื่อให้บริษัทฯ ได้ใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ มั่งคงปลอดภัยและสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการรวมถึงระบบข้อมูลที่อาจก่อให้เกิดความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูล และการประมวลผลของระบบงานบริษัทฯ ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการและอาจรั่วไหลไปยังผู้ไม่พึงประสงค์ได้

แนวทางปฏิบัติ

1. ต้องกำหนดวิธีการคัดเลือกและประเมินผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติที่รัดกุมและเป็นที่น่าเชื่อถือ
2. ต้องมีข้อตกลงเกี่ยวกับการรักษาความปลอดภัย การรักษาความลับของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร รวมถึงขอบเขตเงื่อนไขต่างๆ ในการให้บริการ
3. ต้องกำหนดให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงานและ/หรือเอกสารที่เกี่ยวข้อง
4. ต้องมีการควบคุมดูแลและตรวจสอบการทำงานของผู้ให้บริการอย่างละเอียด กรณีที่เป็นการให้บริการในลักษณะ Remote access และปด Remote ทันทีที่การให้บริการเสร็จสิ้น
5. ต้องกำหนดสิทธิการเข้าถึงเฉพาะส่วนงานที่จำเป็น และต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติเท่านั้น
6. ต้องให้ผู้ให้บริการดำเนินการรายงานผลการปฏิบัติ ปัญหาและแนวทางการแก้ไขต่างๆ ให้ผู้รับบริการทราบ
7. ต้องมีขั้นตอนดำเนินการตรวจรับงานของผู้ให้บริการ

5.5 การควบคุมการเข้าถึงระบบและข้อมูล

วัตถุประสงค์

เพื่อควบคุมดูแลและบริหารจัดการการเข้าถึงข้อมูลและระบบต่างๆ รวมถึงระบบบัญชีผู้ใช้งานให้มีการระบุตัวตน (Identity) สำหรับการทำการพิสูจน์ตัวตน (Authentication) รวมถึงบัญชีผู้ใช้งานหรือบัญชีผู้ใช้งานที่มีสิทธิพิเศษ (Admin User/Super User) รหัสผู้ใช้งานและสิทธิของบัญชีผู้ใช้งานให้เหมาะสมตามตำแหน่งและอำนาจหน้าที่ความรับผิดชอบในระบบงานแต่ละระบบต่างๆ ทั้งจากบุคคลภายในและจากบุคคลภายนอกสถานที่ และต้องตรวจสอบการเข้าถึงระบบให้มีความปลอดภัย มีประสิทธิภาพ ป้องกันทรัพยากรและข้อมูลของบริษัทฯ โดยป้องกันไม่ให้ระบบถูกโจมตีจากผู้ไม่ประสงค์ดีกับบริษัทฯ ระบบได้รับความเสียหาย รวมถึงข้อมูลที่อาจรั่วไหลไปยังผู้ไม่ประสงค์ดี

แนวทางปฏิบัติ การควบคุมทั่วไป

1. ผู้ใช้งานต้องได้รับการอนุญาตจากผู้มีอำนาจอนุมัติ
2. ต้องตรวจสอบการอนุญาตและกำหนดสิทธิในการเข้าถึงข้อมูลกลางและระบบต่างๆ ตามตำแหน่งและหน้าที่ความรับผิดชอบเพื่อการปฏิบัติงาน
3. ต้องทบทวนสิทธิการใช้งานอย่างสม่ำเสมอและสามารถยกเลิกสิทธิ แก้ไขเปลี่ยนแปลงสิทธิต่างๆ ที่ไม่มีความจำเป็นในการเข้าถึงข้อมูลโดยทันทีและต้องบันทึกรายละเอียดให้ชัดเจน
4. ต้องจัดทำทะเบียนรายชื่อผู้ใช้ระบบและสิทธิการใช้งานแต่ละระบบ
5. ต้องเปลี่ยนรหัสผู้ใช้งานที่มีสิทธิพิเศษ (Admin User/Super User) ทุก 6 เดือน
6. กำหนดให้มีช่องทางการเชื่อมต่อเข้าถึงข้อมูลกลางและระบบต่างๆ จากภายนอกโดยผ่าน VPN ที่กำหนด และเมื่อใช้งานเสร็จแล้วให้ยกเลิก (Disable) ทันที

แนวทางปฏิบัติ การจัดการบัญชีและการระบุตัวตนของผู้ใช้งาน (Identity Account)

ข้อกำหนดทั่วไป

1. ต้องให้มีผู้ใช้งานและรหัสผู้ใช้งานที่มีสิทธิพิเศษ (Admin User/Super User) เพื่อบริหารจัดการบัญชีผู้ใช้งานและรหัสผู้ใช้งาน และต้องได้รับการอนุมัติสิทธิพิเศษ (Admin User/Super User) จากผู้มีอำนาจอนุมัติเท่านั้น โดยระบุหน้าที่ความรับผิดชอบให้ครอบคลุม
2. ต้องควบคุม ติดตามการใช้งานของผู้ใช้งานที่มีสิทธิพิเศษ (Admin User/Super User) อย่างน้อยเดือนละ 1 ครั้ง
3. ต้องกำหนดบัญชีผู้ใช้งานและสิทธิในการใช้งานระบบงานต่างๆ ตามตำแหน่งและหน้าที่ความรับผิดชอบ และต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติ
4. ต้องทบทวนบัญชีผู้ใช้งานและสิทธิการใช้งานแต่ละระบบ ให้เหมาะสมกับตำแหน่งและหน้าที่ความรับผิดชอบ อย่างน้อยปีละ 1 ครั้ง
5. ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบต่าง ๆ ตามความสามารถของระบบ
6. ต้องจัดทำระบบบัญชีผู้ใช้งานเพื่อระบุตัวตน (Identity) สำหรับการทำการพิสูจน์ตัวตน (Authentication) และการให้สิทธิการใช้งาน (Authorization)
7. การลบหรือแก้ไขบัญชีผู้ใช้งานหรือรหัสผู้ใช้งานหรือสิทธิการใช้งานระบบงานต่างๆ ต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติ
8. เมื่อมีพนักงานลาออกต้องลบบัญชีผู้ใช้งานทันทีที่สิ้นสุดการเป็นพนักงาน

ข้อกำหนดสำหรับชื่อผู้ใช้งาน (Username Account)

1. กำหนดให้ใช้ ลักษณะ ชื่อภาษาอังกฤษ ตามด้วยจุดและตามด้วยชื่อนามสกุลภาษาอังกฤษตัวแรก
2. อนุญาตให้ใช้ชื่อสำรอง (Alias) ตามความเหมาะสมของแต่ละระบบงานได้

ข้อกำหนดสำหรับรหัสผ่านผู้ใช้งาน (Password)

1. กำหนดให้ใช้รหัสผ่านต้องมีความยาวอย่างน้อย 8 ตัวอักษร โดยมีตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวอักขระและตัวเลขผสมอยู่
2. กรณีระบบงานต่างๆ ไม่สามารถกำหนดรหัสผ่านตามข้อ 1 ได้ ต้องกำหนดรหัสผ่านตามข้อกำหนดสูงสุดของระบบงานนั้นๆ
3. ไม่กำหนดรหัสผ่านจากชื่อหรือนามสกุลของผู้ใช้งาน
4. ผู้ใช้รายใหม่ต้องได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าใช้งานระบบปฏิบัติการ และเมื่อมีการเข้าสู่ระบบในครั้งแรกต้องเปลี่ยนรหัสผ่านโดยทันที

5.6 การสำรองข้อมูลและการกู้คืนข้อมูล

วัตถุประสงค์

เพื่อให้มีมาตรการการสำรองและการกู้คืนข้อมูลสำคัญทางธุรกิจในการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ เพื่อป้องกันการสูญหายของข้อมูล ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

แนวทางปฏิบัติ

1. กำหนดให้มีการเก็บสำรองข้อมูลระบบต่างๆ ดังนี้

ระบบงาน	สำรองข้อมูล	ระยะเวลาจัดเก็บ	Location		
			เครื่องแม่ข่ายบริษัทฯ	One Drive บริษัทฯ	NAS Storage ภายนอกบริษัทฯ
Hero	Database	ทุกวันทำการ	✓	✓	✓
	Incremental	ทุกวันทำการ			✓
	Full VM	ทุกสัปดาห์			✓
Nimbus	Database	ทุกวันทำการ	✓	✓	✓
	Incremental	ทุกวันทำการ			✓
	Full VM	ทุกสัปดาห์			✓
Payday	Database	ทุกวันทำการ	✓	✓	✓
3CX	Config	ทุกวันทำการ	✓	✓	✓
Intranet	File Shared	ทุกสัปดาห์		✓	✓
ระบบรักษาความปลอดภัย (Firewall)	Firewall Configuration	ทุกสัปดาห์	On Cloud		

2. ต้องทำทะเบียนควบคุมบันทึกการนำข้อมูลออกภายนอกบริษัทฯ
3. ต้องตรวจสอบสถานะการสำรองข้อมูล (Backup Log) ของระบบต่างๆ ทุกครั้งที่มีการสำรองข้อมูล
4. ต้องจัดทำเอกสาร (Check list) การสำรองข้อมูล (Backup Log) ของระบบต่างๆ ทุกครั้งตามการตรวจสอบ
5. ต้องทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

5.7 การใช้งานระบบเครือข่าย (Network)

วัตถุประสงค์

เพื่อควบคุมและดูแลบริหารจัดการระบบเครือข่ายของบริษัทฯ ให้มีการระบุตัวตน (Identity) สำหรับการทำการพิสูจน์ตัวตน (Authentication) โดยกำหนดสิทธิของผู้ใช้งานและเข้าถึงระบบเครือข่าย โดยแยกการใช้งานผู้ใช้งานภายในบริษัทฯ กับผู้ใช้งานจากบุคคลภายนอกที่มาปฏิบัติงานให้กับบริษัทฯ ให้เหมาะสมหน้าที่ความรับผิดชอบที่ได้รับอนุญาตจากผู้บริหาร เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานข้อมูลและเครือข่ายไร้สายภายในบริษัทฯ

แนวทางปฏิบัติ การใช้งานระบบเครือข่ายทั่วไป

1. ต้องจัดทำระบบบัญชีผู้ใช้งาน เพื่อการระบุตัวตน (Identity) สำหรับการทำการพิสูจน์ตัวตน (Authentication) และการให้สิทธิการใช้งาน (Authorization) ในระบบเครือข่าย
2. ต้องออกแบบระบบเครือข่ายแยกตามกลุ่มของผู้ใช้งานโซนภายใน (Internal zone) และผู้ใช้งานโซนภายนอก (External zone) เพื่อควบคุมและป้องกันการบุกรุก
3. ระบบเครือข่ายของบริษัทฯที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอกบริษัทฯ ต้องใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่นๆ
4. การเข้าสู่ระบบงานเครือข่ายภายในบริษัทฯ (Login) ต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง
5. ต้องดำเนินการติดตั้งและการเชื่อมต่ออุปกรณ์ต่างๆ ในระบบเครือข่ายให้สามารถใช้งานได้
6. ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่าย LAN และระบบเครือข่ายไร้สายให้เหมาะสมกับตำแหน่งและหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ
7. ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย
8. กำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตี สามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
9. ต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหล ออกไปภายนอกหรือไม่

10. ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (Default) มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน
11. ต้องกำหนดค่า SSID (Service Set Identifier) แยกระหว่างผู้ใช้งานภายในบริษัทฯ กับบุคคลภายนอก
12. ต้องทำแผนผังระบบเครือข่าย (Network Diagram) และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
13. ต้องทำการทบทวน แก้ไขหรือเปลี่ยนแปลงค่า Parameter ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อในระบบเครือข่าย อย่างน้อยปีละ 1 ครั้ง

5.8 การใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ Firewall

วัตถุประสงค์

เพื่อให้มีการควบคุมดูแลและบริหารจัดการระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ Firewall ให้มีประสิทธิภาพและมีความปลอดภัย มีการตรวจจับการบุกรุก ตรวจสอบการใช้งานของบุคคลที่เข้าใช้ระบบเครือข่าย ป้องกันไม่ให้เกิดช่องโหว่หรือทำให้ระบบถูกโจมตีจากผู้ไม่ประสงค์ดีกับบริษัทฯ จนระบบได้รับความเสียหายรวมถึงมีข้อมูลที่อาจรั่วไหลไปยังผู้ไม่ประสงค์ดี รวมถึงเพื่อให้บริษัทฯ มีระบบที่สามารถป้องกันและตรวจสอบเหตุการณ์ที่ผิดปกติร้ายแรงได้

แนวทางปฏิบัติ

1. ปิดกั้นการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม (Web Filter) เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์การพนัน เว็บไซต์ที่มีเนื้อหาผิดกฎหมาย เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม
2. ตรวจจับไวรัสในระบบเครือข่ายคอมพิวเตอร์
3. ปิดกั้น Application ที่ไม่เหมาะสม
4. ติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของบริษัทฯ ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย
5. ตรวจสอบ Firewall Log ในเหตุการณ์ที่ผิดปกติร้ายแรง (Critical) อย่างน้อยเดือนละ 1 ครั้ง

5.9 การจัดเก็บและสอบทาน Audit Log

วัตถุประสงค์

เพื่อให้มีการจัดเก็บและสอบทาน Audit Log บริหารจัดการการใช้งานของผู้ใช้งานในระบบสารสนเทศของบริษัทฯ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายอื่นที่เกี่ยวข้องอย่างเคร่งครัด ให้มีประสิทธิภาพและมีความปลอดภัยสามารถตรวจสอบการใช้งานได้

แนวทางปฏิบัติ

1. ต้องบันทึกการเข้าถึงและการใช้งานระบบเครือข่ายบริษัทฯ ของผู้ใช้งาน โดยมีรายละเอียดการจัดเก็บบัญชีผู้ใช้งาน หมายเลข IP Address วันเวลาที่มีการใช้งาน เป็นต้น ไม่น้อยกว่า 6 เดือน
2. ต้องบันทึกการใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายคอมพิวเตอร์ โดยมีรายละเอียดการจัดเก็บบัญชีผู้ใช้งาน หมายเลข IP Address วันเวลาที่มีการใช้งาน ที่อยู่เว็บไซต์ปลายทาง เป็นต้น ไม่น้อยกว่า 6 เดือน
3. ต้องบันทึกข้อมูลจราจรคอมพิวเตอร์ (Log file) ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ หรือกฎหมายอื่นที่เกี่ยวข้อง ไม่น้อยกว่า 3 เดือน

5.10 การใช้งานระบบคอมพิวเตอร์

วัตถุประสงค์

ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่ใช้สำหรับปฏิบัติงานเป็นทรัพยากรที่บริษัทฯ จัดเตรียมไว้เพื่อการใช้งานในธุรกิจของบริษัทฯ เท่านั้น ห้ามมิให้บุคคลใดใช้คอมพิวเตอร์ของบริษัทฯ ในกิจกรรมที่ไม่อยู่ในวัตถุประสงค์ของบริษัทฯ หรือไม่ได้อยู่ในภารกิจงานของบริษัทฯ หรือทำให้เกิดความเสียหายต่อบริษัทฯ ห้ามทำการเปลี่ยนแปลง ทำซ้ำ ลบทิ้งหรือทำลายข้อมูลของบริษัทฯ และหากเกิดความเสียหายใดๆ ที่เกิดจากการละเมิดดังกล่าวให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น และห้ามนำคอมพิวเตอร์ส่วนบุคคลมาปฏิบัติงานภายในบริษัทฯ ดังนั้นผู้ใช้งานควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของบริษัทฯ ให้มีความลับ ความถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชกฤษฎีกาที่กำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายอื่นที่เกี่ยวข้องอย่างเคร่งครัด และมีความพร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

1. ต้องกำหนดและลงทะเบียน IP Address และ MAC Address ในการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตที่บริษัทฯ จัดสรรไว้ เพื่อความปลอดภัยระบบเครือข่ายเท่านั้น
2. ต้องติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บบราวเซอร์ก่อนเสมอ
3. ต้องตั้งค่าคอมพิวเตอร์ปิดกั้นการติดตั้งโปรแกรม/ซอฟต์แวร์อื่นๆ นอกเหนือจากโปรแกรม/ซอฟต์แวร์ที่บริษัทฯ อนุญาตเท่านั้น
4. ต้องตั้งค่าการใช้งาน Screen saver เพื่อทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน โดยตั้งเวลาประมาณ 10 นาที เมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน
5. ผู้ใช้งานต้องการติดตั้งโปรแกรม/ซอฟต์แวร์อื่นเพิ่มเติมที่จำเป็น ผู้ใช้งานต้องขออนุมัติจากผู้มีอำนาจอนุมัติเท่านั้น และติดตั้งโดยเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น

6. ผู้ใช้งานต้องสำรองข้อมูลใน One Drive ที่บริษัทฯจัดเตรียมไว้ให้
7. ผู้ใช้งานต้องกำหนดการเข้ารหัส (Encrypt) ในการใช้อุปกรณ์จัดเก็บข้อมูลส่วนตัว เช่น External Hard disk, Thumb Drive เป็นต้น
8. ผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์มีการติดไวรัส ต้องทำการยกเลิกการเชื่อมต่อระบบเครือข่ายทันที แล้วแจ้งเจ้าหน้าที่ผู้ดูแลระบบทราบ
9. ไม่ใช้โปรแกรมช่วยในการจำรหัสผ่านอัตโนมัติ สำหรับเครื่องคอมพิวเตอร์ผู้ใช้งาน
10. ผู้ใช้งานต้องเก็บรักษารหัสผ่านเป็นความลับและไม่จดหรือบันทึกรหัสผ่านไว้ในที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
11. ต้องเปลี่ยนรหัสผ่านสำหรับคอมพิวเตอร์ผู้ใช้งาน ทุก 6 เดือน
12. ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ไม่เกิน 3 ครั้ง
13. ผู้ใช้งานห้ามเผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับบริษัทฯ ผ่านระบบเครือข่ายอินเทอร์เน็ต
14. ผู้ใช้งานห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัทฯ ผ่านระบบเครือข่ายอินเทอร์เน็ต
15. ผู้ใช้งานห้ามนำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคง การก่อการร้าย หรือ ภาพลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านระบบเครือข่ายอินเทอร์เน็ต
16. ผู้ใช้งานห้ามนำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่น ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
17. ผู้ใช้งานต้องปฏิบัติตามข้อกฎหมาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายอื่นที่เกี่ยวข้องอย่างเคร่งครัด

5.11 การใช้งานระบบจดหมายอิเล็กทรอนิกส์

<u>วัตถุประสงค์</u>

เพื่อมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการปฏิบัติงานผ่านระบบเครือข่ายของบริษัทฯ ห้ามใช้งานจดหมายอิเล็กทรอนิกส์ที่เกี่ยวข้องกับเรื่องส่วนตัว การส่งต่อข้อความหรือรูปภาพที่ให้ร้าย ทำให้เสื่อมเสีย หรือหยาบคาย ลามก ข่มขู่ ก่อกวน สร้างความรำคาญให้กับผู้อื่นหรือขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายอื่นที่เกี่ยวข้องผ่านระบบเครือข่ายของบริษัทฯ ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้จดหมายอิเล็กทรอนิกส์บนเครือข่าย ผู้ใช้จะต้องไม่ละเมิดสิทธิ์หรือกระทำ

การใดๆ ที่จะสร้างปัญหาใดๆ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด ทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

<u>แนวทางปฏิบัติ</u>

1. ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ไม่เกิน 3 ครั้ง
2. ต้องให้ระบบจดหมายอิเล็กทรอนิกส์ควรมีการล็อกเอาท์ออกจากการใช้งานเมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาเกิน 15 นาที ถ้าต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้ (Username) รหัสผ่าน (Password) อีกครั้ง
3. รหัสผ่านระบบจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงตัวอักษร เช่น ‘x’ หรือ ‘o’ ในการพิมพ์แต่ละตัวอักษรแทน
4. ผู้ใช้งานไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ
5. ผู้ใช้งานควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อ บริษัทฯ หรือละเมิดสิทธิสร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของบริษัทฯ
6. ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ
7. ผู้ใช้งานควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของบริษัทฯ เพื่อการทำงานของบริษัทฯเท่านั้น
8. หลังจากไม่ได้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ ควรทำการออกจากระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งาน
9. ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความจากผู้ส่งที่ไม่รู้จัก
10. ผู้ใช้งานไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมที่ทำให้เสียชื่อเสียงของบริษัทฯ และทำให้เกิดความแตกแยกระหว่างบริษัทฯ
11. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อ จดหมายอิเล็กทรอนิกส์
12. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลของตนให้เหลือจำนวนน้อยที่สุดและควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์
13. ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้

5.12 การควบคุมการจัดหา พัฒนา และ/หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์

วัตถุประสงค์

เพื่อให้การจัดหา พัฒนาหรือปรับปรุงระบบงานคอมพิวเตอร์มาสนับสนุนการปฏิบัติงานภายในบริษัทฯ ให้มีประสิทธิภาพมากขึ้น ประมวลผลถูกต้องครบถ้วน เป็นไปตามความต้องการของผู้ใช้งาน เพื่อเป็นการป้องกันไม่ให้ระบบงานคอมพิวเตอร์ของบริษัทฯ เกิดความเสียหาย

แนวทางปฏิบัติ

1. ถ้าต้องการปรับปรุงระบบงานคอมพิวเตอร์ที่จำเป็นต่อการปฏิบัติงาน ไม่ว่าจะเป็นการจัดหาหรือพัฒนาโปรแกรม/ซอฟต์แวร์ ทั้งกรณีมีค่าใช้จ่ายและไม่มีค่าใช้จ่าย ต้องมีการทบทวนขอบเขตความต้องการของระบบงานให้ชัดเจน และต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติให้แก้ไข/ปรับปรุงส่วนงานนั้น เท่านั้น
2. การจัดหาหรือพัฒนาโปรแกรม/ซอฟต์แวร์ ต้องเปรียบเทียบคุณลักษณะพื้นฐานให้ได้ตามความต้องการของผู้ใช้งานและต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติเท่านั้น
3. ต้องจัดให้มีการทดสอบระบบบนสภาพแวดล้อมสำหรับการทดสอบ ก่อนนำไปใช้งานจริงบนสภาพแวดล้อมสำหรับปฏิบัติงานจริงเสมอและต้องได้รับการอนุมัติใช้สภาพแวดล้อมสำหรับการทดสอบจากผู้มีอำนาจอนุมัติเท่านั้น
4. ผู้ใช้งานร่วมกับเจ้าหน้าที่ที่ได้รับมอบหมายทดสอบ โปรแกรม/ซอฟต์แวร์ เพื่อให้มั่นใจได้ว่าโปรแกรม/ซอฟต์แวร์ทำงานได้อย่างมีประสิทธิภาพ สามารถประมวลผลได้อย่างถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน
5. การปรับปรุงแก้ไขที่พัฒนาเสร็จแล้ว ที่สามารถทำงานบนสภาพแวดล้อมสำหรับปฏิบัติงานจริงต้องได้รับการอนุมัติจากผู้มีอำนาจอนุมัติเท่านั้น
6. ต้องสื่อสารให้กับผู้ใช้งานที่เกี่ยวข้องได้รับทราบและสามารถปฏิบัติงานได้อย่างถูกต้อง

5.13 การควบคุมการปฏิบัติงานประจำด้านระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

เพื่อให้มีการควบคุมการปฏิบัติงานประจำด้านระบบสารสนเทศและระบบคอมพิวเตอร์โดยครอบคลุมการติดตามการทำงานของระบบสารสนเทศและระบบคอมพิวเตอร์ การจัดการปญหาและแก้ไข การบำรุงรักษาและการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยง เพื่อให้มีการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ

แนวทางปฏิบัติ

1. ต้องติดตามการทำงานระบบคอมพิวเตอร์ การทำงานระบบเครื่องแม่ข่ายและการทำงานระบบเครือข่ายเป็นประจำ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

2. ต้องติดตามตรวจสอบสภาพแวดล้อมศูนย์คอมพิวเตอร์เป็นประจำ ถ้ามีสิ่งผิดปกติให้เร่งดำเนินการแก้ไขโดยทันที
3. ต้องบันทึกรายละเอียดการตรวจสอบ ดังนี้
    3.1 ผู้ปฏิบัติงาน
    3.2 เวลาปฏิบัติงาน
    3.3 รายละเอียดการตรวจสอบ
    3.4 ปัญหาที่พบและการแก้ไข
    3.5 สถานะของระบบ
    3.6 ผู้ตรวจทานการปฏิบัติ
4. ต้องจัดทำรายงานต่างๆ ให้ผู้บริหารทราบอย่างสม่ำเสมอ