นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. การบริหารจัดการสินทรัพย์ (Asset Management)

1.1. การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์

วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบถึงหน้าที่และรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลของบริษัทให้ปลอดภัย ถูกต้องและพร้อมใช้งานอยู่เสมอ

แนวทางปฏิบัติ

- ผู้ใช้งาน ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน อาทิเช่น เครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่างๆ
- ห้ามใช้เพื่อประกอบธุรกิจการค้า หรือวัตถุประสงค์ที่เป็นของส่วนตัวและไม่เหมาะสม
- หากผู้ใช้งาน ต้องการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัท จะต้องให้ผู้ดูแลระบบเป็นคนกระทำให้
- ห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์
- ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น และต้องระวังการตกกระทบ
- ห้ามวางหรือจัดเก็บอุปกรณ์คอมพิวเตอร์ใกล้สิ่งที่เป็นของเหลว สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสถานที่ที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
- หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ ห้ามเช็ดทำความสะอาดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- ผู้ใช้งานที่พ้นสภาพต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดในสภาพที่พร้อมใช้งาน
- การนำอุปกรณ์คอมพิวเตอร์ไปปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหายในทุกกรณี

1.2. การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ที่ถูกต้องลิขสิทธิ์และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานให้มีความมั่นคงปลอดภัยและสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง
แนวทางปฏิบัติ

ข้อกำหนดสำหรับผู้ดูแลระบบ

- เป็นผู้ควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัทตามสิทธิ์การใช้งาน
- รับผิดชอบในการติดตั้ง อัพเกรด ถอด และยกเลิกสิทธิ์ในการใช้งานโปรแกรมคอมพิวเตอร์

ข้อกำหนดสำหรับผู้ใช้งาน

- ต้องใช้โปรแกรมคอมพิวเตอร์อย่างพึงจะใช้ทรัพย์สินของตนเอง ไม่นำไปใช้ในทางที่ผิดกฎหมาย หรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับบริษัท
- โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกไปติดตั้งบนเครื่องคอมพิวเตอร์เพื่อให้ผู้อื่นใช้งาน
- ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ โดยไม่ได้รับอนุญาต
- ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ด
- ขาด หากมีความเสียหายหรือละเมิดเกิดขึ้นผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

1.3. การควบคุมสินทรัพย์ด้านสารสนเทศและการเข้าใช้งานระบบคอมพิวเตอร์

แนวทางปฏิบัติ

ป้องกันไม่ให้ผู้ซึ่งไม่มีสิทธิ์ เข้าถึงสินทรัพย์ด้านสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ และข้อมูลสารสนเทศ ขณะที่ไม่มีผู้ใช้งานอุปกรณ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบทุกครั้ง ดังต่อไปนี้

- เมื่อเสร็จสิ้นงาน ให้ออกจากระบบสารสนเทศ (Log out) ทันที
- เก็บและสำรองข้อมูลสารสนเทศไว้ในที่ที่ปลอดภัย

ข้อมูลของผู้ใช้งาน จะจัดเก็บได้อยู่ในรูปแบบดังนี้

- ในฐานข้อมูลของระบบ Application นั้น ๆ ที่จัดเก็บภายใน Data Center ของบริษัท ไม่สามารถนำข้อมูลออกจากระบบได้
- สามารถจัดเก็บใน Shared File (Drive กลาง) ใน Folder ตามสิทธิ์ที่ได้รับ
- ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อไม่มีการใช้งานนานเกิน 1 ชั่วโมง
- การตั้งค่าให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติ กรณีไม่ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 10 นาที
- ดูแลทรัพย์สินของบริษัท เสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายต้องรับผิดชอบ

1.4. การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

เพื่อให้การใช้งานจดหมายอิเล็กทรอนิกส์ สามารถปฏิบัติงานอย่างถูกต้อง สะดวก รวดเร็ว มีประสิทธิภาพ ปลอดภัย ตลอดจนเพื่อให้ผู้ใช้งานเข้าใจถึงความสำคัญและระวังต่อปัญหาที่อาจเกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้จะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด

แนวทางปฏิบัติ

ต้องพึงระวังไม่ให้สินทรัพย์ด้านสารสนเทศเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ์ ดังต่อไปนี้

- ผู้ใช้ต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายที่เกี่ยวข้อง และนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศที่บริษัทกำหนด
- ใช้จดหมายอิเล็กทรอนิกส์ เพื่อผลประโยชน์ของบริษัทเท่านั้น
- ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น
- การส่งจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมาย อิเล็กทรอนิกส์ของบริษัทขัดข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
- การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุ
- เสียดสี ส่อไปในทางผิดกฎหมาย
- ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมี
- ลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์ หรือกระทบต่อการ
- ดำเนินงานของบริษัท ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของบริษัท
- ห้ามผู้ใช้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการงานส่วนบุคคล
- ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับบริษัท

- การส่งข้อมูลข่าวสารที่เป็นความลับบริษัท ควรมีการเข้ารหัสข้อมูลข่าวสารนั้น
- เมื่อใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ให้ออกจากระบบ (Log out) ทุกครั้ง
- กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับ
- การบริการชั่วคราวแก่ผู้ปฏิบัติงานนั้น ๆ เพื่อทำการสอบสวน และตรวจสอบสาเหตุ
- หากผู้ใช้บริการพบการกระทำที่ไม่เหมาะสม หรือการกระทำความผิด เกิดขึ้นในบริษัท ให้แจ้งเบาะแสมที่บริษัท
- การกระทำใด ๆ ที่เกี่ยวข้องกับการเผยแพร่ ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์ และโฮมเพจของผู้ใช้
- บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการเท่านั้น ผู้ดูแลระบบและบริษัทไม่เกี่ยวข้องใด ๆ

2. การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานระบบอินเทอร์เน็ตผ่านระบบเครือข่ายของบริษัท

แนวทางปฏิบัติ

ต้องควบคุมไม่ให้สินทรัพย์ด้านสารสนเทศอยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ์ ต้องกำหนดให้ผู้ใช้งานออกจากระบบสารเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

- ใช้งานผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy เป็นต้น
- เครื่องคอมพิวเตอร์ของบริษัท ก่อนทำการเชื่อมต่อระบบเครือข่าย ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส
- หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บบราวเซอร์ทุกครั้ง
- ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของบริษัท
- ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
- ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลที่อยู่บนอินเทอร์เน็ตก่อนนำไปใช้งาน
- ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่
- เหมาะสม เช่น เว็บไซต์ที่มีเนื้อหาเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ลามกอนาจาร เป็นต้น
- ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่นๆ และจะต้องไม่ก่อให้เกิด
- ความเสียหายขึ้นต่อบริษัท การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่บริษัทกำหนดไว้อย่างเคร่งครัด

3. การเข้ารหัสลับข้อมล (Cryptographic Control)

วัตถุประสงค์

เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ข้อมูลหรือการทำงานของระบบสารสนเทศในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง

แนวทางปฏิบัติ

3.1. การบริหารจัดการข้อมูล

- ต้องมีการจัดลำดับชั้นความลับ ต้องมีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของ
- ข้อมูล
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องมีการเข้ารหัส (Encryption) ที่เป็นมาตรฐาน
- สากล เช่น การใช้ VPN (Virtual Private Network) การใช้ SSL(Secure Socket Layer) เป็นต้น
- มีการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output)
- ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท

3.2. การควบคุมการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Privilege)

- ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล คำนึงถึงการใช้งานและความมั่นคง
- ปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับ
- ต้องกำหนดสิทธิ์การใช้ข้อมูลและระบบสารสนเทศ สิทธิ์การใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิ์การใช้งานอินเทอร์เน็ต แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ
- ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องออกจากระบบงาน (Log Out) ทุกครั้ง
- ในกรณีที่มีความจำเป็นต้องให้สิทธิ์บุคคลอื่น ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3.3. การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

- มีการตรวจสอบตัวตนจริงและสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบสารสนเทศที่รัดกุม กำหนดรหัสผ่านให้ยากแก่การคาดเดา และให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง
    - ควรกำหนดให้รหัสผ่านมีความยาวขั้นต่ำ 8ตัวอักษร (Alphabet + Numeric)
    - ควรใช้อักขระพิเศษประกอบ เช่น : ; < > $ @ # เป็นต้น
    - สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 6 เดือน

- ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน หรือคาดเดาได้ง่าย เช่น “aaaaaa” “123456” “P@ssw0rd” เป็นต้น
- ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น
- ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 5 ครั้ง
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

- ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง

4. ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับระบบสารสนเทศของบริษัทเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ป้องกันการสูญหายของข้อมูล

แนวทางปฏิบัติ

- จัดทำคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับระบบสารสนเทศที่สำคัญของบริษัท
- กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศ เช่น ต้องมีการขออนุมัติจากผู้บังคับบัญชาก่อน เป็นต้น
- ตรวจสอบติดตามทรัพยากรของระบบสารสนเทศ เช่น CPU, Memory, Hard Disk ว่าเพียงพอหรือไม่
- ข้อมูลที่มีความสำคัญสูง ต้องจัดให้มีความถี่การสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกบริษัท
- ต้องทดสอบสภาพพร้อมใช้งานระบบสำรอง ปีละ 1 ครั้ง
- ต้องมีมาตรการป้องกันโปรแกรมไม่ประสงค์ดี เช่น
  - ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการและโปรแกรมที่ใช้งาน ที่ได้มีการออก Patch และ/หรือ
  - Hotfix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลดจากเว็บไซต์ของเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่
  - ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอีเมล จะต้องตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการรับ
  - ส่งข้อมูลทุกครั้ง

5. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

วัตถุประสงค์

เพื่อป้องกันข้อมูลสารสนเทศในเครือข่ายจากบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ

แนวทางปฏิบัติ

- การบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย (Network Security Management)
  - กำหนดการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย
  - ต้องจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับบริษัท
- การถ่ายโอนข้อมูล (Information Transfer)
  - ต้องคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
  - ต้องมีการลงนามในสัญญาระหว่างบริษัทและหน่วยงานภายนอกว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement: NDA)
  -

6. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information Security Incident Management)

วัตถุประสงค์

เพื่อให้มีการแจ้งสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ และจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศให้ได้รับทราบ

แนวทางปฏิบัติ

- กำหนดหน้าที่รับผิดชอบและการปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท
- กำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน
- หากผู้ใช้งานตรวจพบเหตุอาจส่งผลต่อความปลอดภัยต้องแจ้งเหตุการณ์ดังกล่าวต่อส่วนเทคโนโลยีสารสนเทศ
- กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรงของ
- เหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว
- ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

7. ความมั่นคงปลอดภัยด้านสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อเป็นการป้องกันการหยุดในการดำเนินงานของบริษัท อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของบริษัท

แนวทางปฏิบัติ

- ส่วนเทคโนโลยีสารสนเทศ ต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดขึ้นกับระบบสารสนเทศ
- ตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้น พร้อมเตรียมแผนกรณีฉุกเฉิน ปีละ 1 ครั้ง หรือมากกว่า
- ตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรอง ปีละ 1 ครั้ง หรือมากกว่า

8. การบริหารจัดการความเสี่ยง (Risk Management)

เพื่อให้สอดคล้องกับการบริหารความเสี่ยงองค์กร ครอบคลุมในเรื่องดังต่อไปนี้

- การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk)
- ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของบริษัท เพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัยหรือไม่ประสงค์ดี
- ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ของบริษัท ต้องมีตรวจสอบและเฝ้าระวังการใช้งานเครือ
- ข่ายภายในและระบบอินเทอร์เน็ต โดยมีการจัดทำระบบป้องกันการเข้าถึงและการโจมตีจากภายนอกให้กับเครื่อง
- คอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงานใช้งาน เช่น ระบบป้องกันการเข้าออกใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ การกรองข้อมูลรับส่งอีเมล เป็นต้น
- ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิ์การใช้งานเข้าถึงระบบเครื่องคอมพิวเตอร์ ให้เป็นไปตามสิทธิ์ที่พึงมี เพื่อป้องกันการเข้าแก้ไขหรือเปลี่ยนแปลงข้อมูล
- การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความ
- สำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ดังนี้
- ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี

- ความเสี่ยงจากผู้ปฏิบัติงาน ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลเกินกว่าหน้าที่และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้
- ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้งสถานการณ์อื่น
- ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากแนวนโยบายที่ทำการใช้งานอยู่อาจไม่สอดคล้องกับความเสี่ยงที่อาจ
- เกิดขึ้น
- การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่บริษัทยอมรับได้
- กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างทันที

9. การทบทวนนโยบายการเข้าถึงข้อมูลส่วนบุคคล

บริษัทจะทำการทบทวนนโยบายนี้อย่างน้อยปีละ 1 ครั้ง หรือตามกฎหมายกำหนด