นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

บริษัท ซัคเซสมอร์ บีอิ้งค์ จำกัด (มหาชน)

วันที่ 20 กุมภาพันธ์ 2562

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร
(ICT Security Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ซัคเซสมอร์ บีอิ้งค์ จำกัด (มหาชน) เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่บริษัท อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายอื่นที่เกี่ยวข้อง บริษัทจึงได้กำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศและการสื่อสารขององค์กรขึ้นดังนี้

1. การจัดหา การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศ
2. การบริหารจัดการผู้ให้บริการภายนอก
3. การควบคุมการเข้าถึง
4. การแลกเปลี่ยนข้อมูลสารสนเทศ
5. ความมั่นคงปลอดภัยในการดำเนินการ
6. ความมั่นคงปลอดภัยในระบบเครือข่าย
7. การเข้ารหัส
8. ความมั่นคงปลอดภัยพื้นที่

หมวดที่ 1
การจัดหา การพัฒนา และการบำรุงรักษาระบบทางเทคโนโลยีสารสนเทศ

วัตถุประสงค์: เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นส่วนหนึ่งตลอดอายุของระบบเทคโนโลยีสารสนเทศ

การจัดหาและการพัฒนา:

1. การจัดหาและพัฒนาระบบงานมีการเก็บข้อมูลความต้องการทางธุรกิจและออกแบบระบบให้สอดคล้องกับความต้องการการปฏิบัติงาน (Operation) ความมั่นคงปลอดภัยสารสนเทศ (Information Security) และการทำงาน (Functionality)

2. ก่อนเริ่มดำเนินการจัดหาพัฒนาจะต้องมีการอนุมัติอย่างเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและเจ้าของระบบงาน และมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) การทำงาน (Functionality) ข้อกำหนดด้านกฎหมายหรือระเบียบของบริษัท (Compliance) และความเสี่ยง (Risk)
3. การพัฒนาเป็นไปตามหลักวิศวกรรมด้านความมั่นคงปลอดภัย (Secure System Engineering Principles) ซึ่งรวมถึงวงจรการพัฒนาระบบสารสนเทศ (SDLC) และการเขียนซอร์สโค้ดแบบปลอดภัย (Secure Coding)
4. กำหนดให้จัดทำเอกสารที่จำเป็นในการออกแบบระบบงาน ได้แก่
    4.1 User Specification
    4.2 Functional Specification
    4.3 System Document เช่น Data Flow Diagram, Data Dictionary, File Layout, ER Diagram, Structure Chart, Screen Layout, Report Layout เป็นต้น
    4.4 เอกสารอื่น ๆ ตามความเหมาะสม
5. เจ้าของข้อมูลและเจ้าของระบบงานตรวจสอบและติดตามผลการดำเนินงานภายใต้แผนการดำเนินงานโครงการที่กำหนดไว้
6. มีการควบคุมการเข้าถึงและใช้งานซอร์สโค้ดและข้อมูลที่จำเป็นในการพัฒนาระบบงาน ซึ่งการเข้าถึงดังกล่าวจะต้องครอบคลุมไปถึงหน่วยงานภายนอกที่จ้างในการพัฒนาระบบ
7. จัดให้มีการควบคุมเวอร์ชันของระบบงานที่พัฒนาเพื่อป้องกันการแก้ไขไม่ถูกต้อง
8. การจ้างหน่วยงานภายนอกพัฒนาระบบงาน จะต้องกำหนดให้หน่วยงานภายนอกเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบ (Development Environment) เท่านั้น และไม่สามารถเข้าถึงระบบการใช้งานจริง (Production Environment)
9. การนำระบบที่พัฒนาไปใช้งานจริงจะต้องได้รับอนุมัติจากผู้มีอำนาจ และมีการทดสอบก่อนโอนย้ายไปใช้งานจริง
10. จำกัดการแก้ไขซอฟต์แวร์สำเร็จรูป หากมีความจำเป็นต้องแก้ไขจะต้องได้รับการอนุมัติจากผู้มีอำนาจก่อนเสมอ

การแบ่งแยกสภาพแวดล้อม

1. จะต้องแบ่งแยกสภาพแวดล้อมระบบที่ใช้สำหรับการพัฒนา (Development Environment) การทดสอบ (Testing Environment) และการใช้งานจริง (Production Environment) ออกจากกัน และควบคุมการเข้าถึงได้เฉพาะผู้มีส่วนเกี่ยวข้องเท่านั้น
2. สภาพแวดล้อมระบบที่ใช้สำหรับการพัฒนา (Development Environment) การทดสอบ (Testing Environment) และการใช้งานจริง (Production Environment) จะต้องเหมือนหรือใกล้เคียงกัน เพื่อป้องกันความผิดพลาดจากการใช้สภาพแวดล้อมต่างกัน
3. ระบบสารสนเทศที่มีความสำคัญสูง ให้แยกออกจากระบบเครือข่ายที่ใช้งานทั่วไป

ความมั่นคงปลอดภัยของข้อมูลที่ใช้ทดสอบ

1. หลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลเพื่อทดสอบ หากจำเป็นให้กำหนดวิธีการทำให้ไม่สามารถย้อนกลับไปยังข้อมูลจริงได้ ได้แก่ การสลับตำแหน่ง (Scrambling) การลบข้อมูลระบุตัวตน เช่น หมายเลขบัตรประจำตัวประชาชน เป็นต้น
2. การส่งออก (Extract) ข้อมูลจากระบบใช้งานจริง กระทำโดยบุคคลที่ได้รับอนุญาตเท่านั้น
3. ไม่นำข้อมูลที่ใช้ทดสอบระบบไปใช้ผิดวัตถุประสงค์และลบข้อมูลทันทีภายหลังการทดสอบเสร็จสิ้น

การทดสอบระหว่างการพัฒนาและบำรุงรักษา

1. ผู้ที่ร้องขอและฝ่ายคอมพิวเตอร์ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง มีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการ
2. ระบบงานสำคัญควรมีหน่วยงานหรือทีมงานอิสระ เข้าตรวจสอบว่ามีการปฏิบัติตามขั้นตอนการพัฒนาและการทดสอบระบบ ก่อนที่จะโอนย้ายไปใช้งานจริง
3. ระบบงานที่เชื่อมต่อกับระบบเครือข่ายสาธารณะจะต้องมีการทดสอบเจาะระบบ (Penetration Test) เพื่อสร้างความเชื่อมั่นด้านความมั่นคงปลอดภัยสารสนเทศ

การบำรุงรักษา

1. การบำรุงรักษาดำเนินการโดยบุคคลที่มีความรู้ และได้รับการอบรมเพียงพอ
2. หากมีความจำเป็นต้องแก้ไขเปลี่ยนแปลง ให้ขออนุญาตอย่างเป็นลายลักษณ์อักษร และนำเข้ากระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management Procedure)

3. ตรวจสอบการทำงานและความถูกต้องของระบบงานทุกครั้งที่มีการเปลี่ยนแปลง ซึ่งรวมถึงการเปลี่ยนแปลงในระบบปฏิบัติการ
4. จัดทำและปรับปรุงคู่มือบำรุงรักษาระบบงานให้เป็นปัจจุบันอยู่เสมอ ซึ่งรวมถึงเอกสารระบบงาน (System Document) และเอกสารจำเป็นอื่น ๆ เช่น Data Dictionary เป็นต้น
5. จัดให้มีการควบคุมเวอร์ชันของระบบงานที่พัฒนาสำเร็จ (Compiled Code) แยกออกจากเวอร์ชันของระบบที่ใช้ในการพัฒนา และกำหนดสิทธิเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

หมวดที่ 2
การบริหารจัดการผู้ให้บริการภายนอก

วัตถุประสงค์: เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับผู้ให้บริการภายนอก

การคัดเลือกผู้ให้บริการ:

1. หลักเกณฑ์ด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการคัดเลือกผู้ให้บริการภายนอก มีดังนี้
   1.1 ผู้ให้บริการภายนอกที่เชื่อถือได้นำเสนอผลงานคุณภาพ และไม่มีประวัติการทิ้งงาน
   1.2 พนักงานของผู้ให้บริการภายนอกมีความรู้ความสามารถ ซึ่งอาจรวมถึงประกาศนียบัตรรับรองความรู้ความสามารถ
   1.3 มีประวัติการให้บริการ ประวัติการรับรองผลงาน หรือรายชื่อลูกค้า หรือผู้รับบริการอ้างอิง
2. มีความสามารถในการรองรับแผนการบริหารความต่อเนื่อง หรือแผนฉุกเฉินในสถานการณ์ต่าง ๆ
3. ยอมรับหลักเกณฑ์ในการเข้าตรวจสอบวิธีการปฏิบัติงาน รวมถึงการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศอื่น ๆ ตามที่ได้ร้องขอ

การบริหารความเสี่ยง:

บริษัท ซัคเซสมอร์ บีอิ้งค์ จำกัด (มหาชน) ดำเนินการประเมินความเสี่ยง และแนวทางจัดการความเสี่ยงที่เกิดจากบริการของผู้ให้บริการภายนอกหยุดชะงัก

การจัดทำสัญญาและข้อตกลงในการรักษาความลับ

1. สัญญา รวมถึงข้อตกลงที่ทำร่วมกันต้องส่งให้หน่วยงานด้านกฎหมายตรวจพิจารณา เพื่อลดช่องโหว่จากการระบุข้อความไม่ถูกต้องครบถ้วน
2. สัญญาต้องระบุขอบเขตงานและเงื่อนไขในการให้บริการ (Service Level Agreement) รวมทั้งสิ่งส่งมอบและเงื่อนไขการตรวจรับงาน

3. กรณีระบบงานที่มีความสำคัญสูงควรมีจัดตั้งคณะกรรมการเพื่อพิจารณาการตรวจรับ
4. สัญญา รวมถึงข้อตกลงที่ทำร่วมกัน จะต้องระบุข้อตกลงรักษาความลับไว้ในสัญญาเสมอ รวมทั้งพิจารณาเซ็นสัญญารักษาความลับ (Non-disclosure Agreement) เพิ่มเติม ตามความเหมาะสมของลักษณะของงานที่ใช้บริการ
5. การรักษาความมั่นคงปลอดภัยสารสนเทศของวิธีการที่ใช้สำหรับรับ-ส่งระหว่างซัคเซสมอร์ บีอิ้งค์ จำกัด (มหาชน) รวมถึงบริษัทย่อย และผู้ให้บริการภายนอก เป็นหน้าที่ที่ปฏิบัติร่วมกัน และใช้ความระมัดระวัง หรือมาตรการป้องกันการรับ-ส่งข้อมูลที่มีความสำคัญสูง
6. เมื่อสิ้นสุดสัญญา ต้องยกเลิกสิทธิการเข้าถึงของผู้ให้บริการภายนอกทั้งหมด ทั้งส่วนที่เป็นการเข้าถึงกายภาพ (Physical Access) และการเข้าถึงระบบงาน (Logical Access)
7. ข้อตกลงด้านความมั่นคงปลอดภัยอื่น ๆ ที่ควรระบุในสัญญา ตัวอย่างเช่น
   7.1 การปฏิบัติตามกฎหมาย และกฎระเบียบที่เกี่ยวข้อง
   7.2 การให้สิทธิการตรวจสอบคุณสมบัติ ประวัติของผู้ปฏิบัติงาน
   7.3 การรักษาความมั่นคงปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคล
   7.4 การคืน ทำลาย หรือลบข้อมูลส่วนบุคคล
   7.5 การรายงานถึงความผิดปกติและการรายงานถึงการละเมิดข้อมูลส่วนบุคคล
   7.6 การป้องกันการจ้างช่วง
   7.7 การให้สิทธิในการเข้าตรวจสอบ (Audit)
   7.8 การรายงานจุดอ่อนใด ๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศ
   7.9 ผลของการละเมิดเงื่อนไข
8. การเปลี่ยนแปลงใด ๆ ในสัญญา ให้จัดทำข้อตกลงที่เป็นลายลักษณ์อักษร รวมทั้งประเมินผลกระทบและความเสี่ยงจากการเปลี่ยนแปลงข้อตกลง

การติดตามประเมินผลและตรวจสอบการให้บริการ:

1. จัดให้มีการติดตามประเมินผลและตรวจสอบการให้บริการตามที่ได้ระบุไว้ในสัญญา
2. การติดตามประเมินประเมินผลจะต้องรวมถึงการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ
3. จัดให้มีการตรวจสอบ (Audit) การให้บริการที่มีความสำคัญสูงตามข้อกำหนดที่ระบุไว้ในสัญญา

หมวดที่ 3
การควบคุมการเข้าถึง

วัตถุประสงค์: เพื่อป้องกันความเสียหายจากการเข้าถึงโดยไม่ได้รับอนุญาต

ข้อกำหนดทั่วไป:

1. สิทธิการเข้าถึงอยู่บนหลักการอนุญาตให้เข้าถึงให้น้อยที่สุด (Least Privilege)
2. การเข้าถึงข้อมูลสารสนเทศ และข้อมูลในแอปพลิเคชันเป็นไปตามหลักการ Need-to-know และระดับชั้นความลับที่กำหนด
3. ออกแบบแอปพลิเคชันให้แสดงหน้าจอ หรือเมนูตามสิทธิที่ได้รับ
4. การขอสิทธิการเข้าถึงจะต้องขออนุญาตและบันทึกไว้เป็นลายลักษณ์อักษรทุกครั้ง โดยกำหนดไม่ให้สิทธิการเข้าถึงก่อนที่มีการอนุมัติ และผู้อนุมัติจะต้องไม่เป็นบุคคลเดียวกับผู้ร้องขอ
5. การขอสิทธิพิเศษ (Privilege Access) เช่น Administrator, Super User เป็นต้น จะต้องได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่ซึ่งดูแลสิทธิพิเศษนั้น ๆ
6. การขอสิทธิในลักษณะฉุกเฉินหรือชั่วคราว จะต้องบันทึกเหตุผลและความจำเป็น รวมถึงระยะเวลาสิ้นสุด และยกเลิกสิทธิทันทีเมื่อพ้นระยะเวลาดังกล่าว
7. สิทธิการเข้าถึงของหน่วยงานภายนอก และผู้ให้บริการต่าง ๆ จะต้องระบุระยะเวลาสิ้นสุด และให้สิทธิสูงสุดไม่เกิน 1 ปี โดยจะต้องขออนุญาตใหม่ทุกครั้ง
8. ผู้มีสิทธิอนุมัติการเข้าถึง ได้แก่ เจ้าของข้อมูล และ/หรือระบบงาน โดยมีฝ่ายคอมพิวเตอร์ให้เป็นผู้ให้คำแนะนำในการจัดสรรสิทธิได้อย่างถูกต้อง
9. การเข้าถึงจะต้องใช้วิธีการพิสูจน์ตัวตนที่มีความปลอดภัย และสามารถตรวจสอบข้อมูลย้อนหลังได้ เช่น การใช้ User Name และ Password เป็นต้น
10. จัดให้มีการทบทวนสิทธิการเข้าถึงอยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง
11. เมื่อสิ้นสุดความจำเป็นที่ต้องใช้งาน การเปลี่ยนแปลงโยกย้าย การสิ้นสุดสัญญาให้ยกเลิกสิทธิการการเข้าถึงทันที

การเข้าถึงระบบเครือข่ายและบริการเครือข่าย:

1. จัดให้มีการแบ่งแยกระบบเครือข่าย โดยแยกระบบสารสนเทศที่มีความสำคัญสูงออกจากระบบเครือข่ายที่ใช้งานทั่วไป
2. ก่อนเข้าถึงระบบเครือข่ายและบริการเครือข่ายจะต้องพิสูจน์ตัวตนก่อนทุกครั้ง
3. การอนุญาตให้เข้าถึงบริการเครือข่ายด้วยวิธีการรีโมท จะต้องดำเนินการผ่าน Protocol ที่มีความปลอดภัย เช่น SSH เป็นต้น

4. การอนุญาตให้เข้าถึงระบบเครือข่ายด้วยวิธีการรีโมทจะต้องอยู่ในโซน หรืออุปกรณ์ที่ได้รับอนุญาตเท่านั้น เช่น กำหนด Management Zone หรือการลงทะเบียน MAC Address เป็นต้น
5. จำกัดเวลารีโมท โดยให้ตัดการเชื่อมต่อทุก 5 นาที เมื่อไม่มีการใช้งาน (Inactive Session)

การเชื่อมต่อจากระยะไกล:

1. การเชื่อมต่อจากระยะไกลให้ใช้งานผ่าน VPN เพื่อให้ข้อมูลที่รับ-ส่งมีความปลอดภัย
2. กำหนดระยะเวลาเชื่อมต่อสูงสุดในระบบ VPN โดยให้ตัดการเชื่อมต่อ และพิสูจน์ตัวตนใหม่ทุก 12 ชั่วโมง
3. เครื่องคอมพิวเตอร์ที่ใช้เชื่อมต่อจากระยะไกลมีการป้องกันไวรัส และปรับปรุงแพทช์ให้เป็นปัจจุบันเสมอ

การพิสูจน์ตัวตนและการจัดการรหัสผ่านา:

1. ห้ามไม่ให้ใช้บัญชีผู้ใช้และรหัสผ่านที่เป็น Default หรือข้อมูลตั้งต้นที่มาจากผู้ผลิต
2. บัญชีผู้ใช้งานไม่ควรสื่อถึงตำแหน่งและความรับผิดชอบ เช่น Administrator เป็นต้น
3. บัญชีผู้ใช้งานของแต่ละคนไม่ซ้ำกัน (Unique User Account) หากมีความจำเป็นต้องใช้บัญชีผู้ใช้งานร่วมกัน (Shared User Account) ให้ระบุรายชื่อผู้ใช้งาน และทบทวนให้เป็นปัจจุบันอยู่เสมอ
4. การใช้งานบัญชีผู้ใช้กลาง (Shared Account) ให้เปลี่ยนรหัสผ่านทันทีที่สมาชิกในกลุ่มสิ้นสุดหน้าที่ความรับผิดชอบในการปฏิบัติงาน
5. การแจ้งรหัสผ่านให้กับผู้ใช้งานให้ใช้วิธีการที่ปลอดภัย
6. ข้อกำหนดการตั้งรหัสผ่าน มีดังนี้
    6.1 รหัสผ่านจะต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร
    6.2 รหัสผ่านจะต้องประกอบด้วยตัวอักษรพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และตัวอักขระพิเศษ
    6.3 ระบบจะไม่ยอมรับรหัสผ่านหลังป้อนผิด 3 ครั้ง
    6.4 ระบบไม่ยอมรับรหัสผ่านที่เคยใช้ย้อนหลัง 3 ครั้งล่าสุด
    6.5 ระบบบังคับให้มีการเปลี่ยนรหัสผ่านทันทีที่ใช้งานครั้งแรก
    6.6 ระบบบังคับให้เปลี่ยนรหัสผ่านทุก 60 วัน
7. รหัสผ่านตั้งต้นไม่ควรซ้ำกัน หรือให้กำหนดอายุรหัสผ่านตั้งต้น ไม่ให้การใช้งานครั้งแรกเกินระยะเวลาที่กำหนด
8. ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านเองได้
9. การส่งรหัสผ่านไม่ใช้รูปแบบ Plain Text

10. ไม่อนุญาตให้ติดตั้งโปรแกรม เอเจ้นท์ โปรแกรมอรรถประโยชน์ ยูทิลิตี้ หรือคำสั่งใด ๆ ที่ลัดขั้นตอนการพิสูจน์ตัวตนก่อนเข้าถึงระบบสารสนเทศ

หมวดที่ 4
การแลกเปลี่ยนข้อมูลสารสนเทศ

วัตถุประสงค์: เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลที่แลกเปลี่ยนภายในและภายนอกองค์กร

ข้อกำหนดทั่วไป:

1. เลือกใช้ช่องทางแลกเปลี่ยนข้อมูลมีความปลอดภัย และรักษาความถูกต้องสมบูรณ์ของข้อมูลจนถึงปลายทาง
2. เลือกใช้ช่องทางที่มีความปลอดภัย และสามารถแจ้งเตือน หรือป้องกันไวรัส รวมถึงมัลแวร์ประเภทต่าง ๆ
3. การเลือกใช้วิธีการแลกเปลี่ยนข้อมูลเป็นไปตามระดับชั้นความลับของข้อมูลที่ต้องการแลกเปลี่ยน
4. เลือกใช้ช่องทางแลกเปลี่ยนข้อมูลสามารถตรวจสอบข้อมูลย้อนหลังได้ ได้แก่ ข้อมูลผู้ส่ง ปลายทางที่รับข้อมูล รวมถึงสาระและเนื้อหาสำคัญ
5. การแลกเปลี่ยนข้อมูลที่เป็นข้อมูลส่วนบุคคลให้ปฏิบัติตามนโยบายข้อมูลส่วนบุคคล (Data Privacy Policy)

การแลกเปลี่ยนข้อมูลโดยใช้ระบบอีเมล์:

1. ผู้ใช้งานตรวจสอบชื่อผู้รับให้ถูกต้องก่อนส่งอีเมล์
2. ระบบอีเมล์แสดงข้อความระบุความรับผิดชอบและข้อควรปฏิบัติหากผู้รับอีเมล์ไม่ใช่ผู้รับที่แท้จริง (Disclaimer) อัตโนมัติ ในส่วนท้ายของอีเมล์ที่ส่งออกไปภายนอกองค์กร
3. ห้ามไม่ให้ใช้ระบบอีเมล์สาธารณะ เช่น Gmail เป็นต้น ในการรับ-ส่งข้อมูลที่มีความสำคัญสูง
4. ไม่ควรเปิดอ่านอีเมล์ไม่ทราบแหล่งที่มา หรือมีเหตุต้องสงสัย และแจ้งให้ฝ่ายคอมพิวเตอร์เข้าตรวจสอบ
5. งดใช้ฟังก์ชันช่วยจำเพื่อลัดขั้นตอนพิสูจน์ตัวตนในระบบอีเมล์
6. ตรวจสอบและสำรองข้อมูลในระบบอีเมล์อยู่เสมอ

การแลกเปลี่ยนข้อมูลโดยใช้สื่อบันทึกแบบพกพา:

1. เลือกใช้สื่อบันทึกแบบพกพา เช่น Flash Drive, USB เป็นต้น ที่มีความสามารถในการเข้ารหัส หรือสามารถยืนยันตัวตนผู้ใช้งาน
2. ตรวจสอบไวรัส และมัลแวร์ประเภทต่าง ๆ ในสื่อบันทึกแบบพกพาอยู่เสมอ

3. ตรวจสอบข้อมูลที่บันทึกไว้ในสื่อบันทึกแบบพกพาอยู่เสมอ และเก็บข้อมูลในสื่อบันทึกแบบพกพาให้น้อยที่สุด เนื่องจากเป็นสื่อบันทึกที่สูญหายได้ง่าย

การแลกเปลี่ยนข้อมูลโดยใช้ File Sharing

1. ให้ประเมินความเสี่ยงและผลกระทบทุกครั้งก่อนนำข้อมูลสำคัญไปเก็บไว้ที่ File Sharing โดยจะต้องขออนุญาตจากเจ้าของข้อมูลเสมอ ซึ่งการแลกเปลี่ยนข้อมูลโดยใช้ File Sharing รวมถึงแหล่งเก็บข้อมูลประเภท Google Drive, Dropbox เป็นต้น
2. ห้ามไม่ให้แลกเปลี่ยนข้อมูลโดยใช้โปรโตคอลที่ไม่ปลอดภัย เช่น FTP เป็นต้น
3. ตรวจสอบรายชื่อผู้มีสิทธิในระดับในโฟลเดอร์อยู่เสมอ

การแลกเปลี่ยนข้อมูลโดยใช้โปรแกรมประเภท Messaging

1. ห้ามไม่ให้ส่งข้อมูลสำคัญโดยใช้โปรแกรมประเภท Messaging เช่น Line, WhatsApp เป็นต้น
2. เลือกใช้โปรแกรมประเภท Messaging ที่มีการเข้ารหัสข้อมูลให้มีความปลอดภัย

หมวดที่ 5
ความมั่นคงปลอดภัยในการดำเนินการ

วัตถุประสงค์: เพื่อให้มีกระบวนการดำเนินการมีความมั่นคงปลอดภัย

ข้อกำหนดทั่วไป:

1. เจ้าหน้าที่ปฏิบัติงานจัดทำเอกสารขั้นตอนหรือวิธีปฏิบัติในการปฏิบัติงานประจำในด้านต่าง ๆ ที่สำคัญเป็นลายลักษณ์อักษรเพื่อเป็นแนวทางให้แก่เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Computer Operator) เช่น ขั้นตอนในการเปิด-ปิดระบบ ขั้นตอนการประมวลผล ขั้นตอนการตรวจสอบประสิทธิภาพการทำงานของระบบ และตารางเวลาในการปฏิบัติงาน เป็นต้น และปรับปรุงขั้นตอนหรือวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ
2. การปฏิบัติงานผ่านทางเมนู โปรแกรม และใช้ Command Line เท่าที่จำเป็น
3. ห้ามไม่ให้ติดตั้งซอฟต์แวร์ที่ไม่เกี่ยวข้องกับการดำเนินงานในระบบสารสนเทศ และห้ามไม่ให้ใช้งานซอฟต์แวร์ผิดกฎหมายโดยเด็ดขาด
4. เปิดใช้บริการ (Service) ในระบบสารสนเทศเท่าที่จำเป็น
5. จัดทำบันทึกงาน (Log Book) ที่เกี่ยวกับการปฏิบัติงานประจำ และรายงานให้กับ Operation Manager ได้รับทราบอย่างสม่ำเสมอ
6. กำหนดรายชื่อ หน้าที่และความรับผิดชอบในการแก้ไขปัญหาอย่างชัดเจน รวมถึงข้อมูลการติดต่อผู้ที่เกี่ยวข้องเพื่อใช้ติดต่อในกรณีที่มีปัญหา

การแบ่งแยกอำนาจหน้าที่:

1. ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ในส่วนการพัฒนาระบบงาน (Developer) ออกจากบุคลากรที่ทำหน้าที่บริหารควบคุมระบบ (Operation support) ซึ่งควบคุมการปฏิบัติงานในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริง (Production Environment)
2. ต้องจัดให้มี Job Description ซึ่งระบุหน้าที่และความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายในฝ่ายคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร
3. จัดให้มีบุคลากรสำรองในงานที่มีความสำคัญเพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น เช่น ผู้บริหารระบบ (System Administrator) เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ (Operation Support) เป็นต้น

การบริหารการเปลี่ยนแปลง:

1. จัดทำเอกสารกระบวนการเพื่อใช้บริหารจัดการการเปลี่ยนแปลง
2. ก่อนการดำเนินการเปลี่ยนแปลงใด ๆ จะต้องได้รับการอนุมัติจากเจ้าของข้อมูลและ/หรือเจ้าของระบบงานเสมอ
3. จัดทำเกณฑ์เพื่อใช้ประเมินผลกระทบ และความเสี่ยงที่เกิดจากการเปลี่ยนแปลง
4. กำหนดแผนสำรองหรือแผนกู้คืน (Fallback Plan) เพื่อใช้ดำเนินการหากการเปลี่ยนแปลงไม่สำเร็จ
5. ก่อนการเปลี่ยนแปลงใด ๆ ควรมีจัดให้มีการทดสอบอยู่เสมอ ยกเว้นมีข้อจำกัดทางเทคนิค
6. ภายหลังการเปลี่ยนแปลงใด ๆ ในระบบปฏิบัติการ ควรแจ้งให้เจ้าของระบบ หรือผู้ใช้งานตรวจสอบความถูกต้องในการประมวลผลระบบสารสนเทศอยู่เสมอ

การบริหารทรัพยากรในระบบ:

1. จัดให้มีการตรวจสอบการใช้งานทรัพยากรในระบบ เช่น CPU, Memory, Disk เป็นต้น อยู่เสมอ
2. การจัดหาและการเปลี่ยนแปลงในระบบสารสนเทศ จะต้องพิจารณาความเพียงพอของทรัพยากรในระบบเสมอ
3. การจัดหาทรัพยากรในระบบเพิ่มเติมจะต้องคำนึงถึงอัตราการเติบโตของข้อมูลเพื่อให้สามารถรองรับกับความต้องการทางธุรกิจ

การสำรองข้อมูล:

1. การออกแบบและเลือกใช้วิธีการสำรองข้อมูลเป็นไปตามความสำคัญของข้อมูลทางธุรกิจ
2. มีการทดสอบข้อมูลที่ได้สำรองไว้อยู่เสมอ หรืออย่างน้อยปีละ 1 ครั้ง
3. สื่อบันทึกที่ใช้สำรองข้อมูลสามารถรองรับความต้องการทางด้านอายุการจัดเก็บ รวมถึงมีเทคโนโลยีที่ใช้รองรับการเรียกดูข้อมูลในอนาคต

4. ข้อมูลที่สำรอง รวมถึงสื่อบันทึกข้อมูลจะต้องไม่จัดเก็บไว้ในตำแหน่ง หรือสถานที่เดียวกับการเก็บข้อมูลตามปกติ

การจัดเก็บข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs):

1. จัดให้มีการเก็บข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) เช่น System Access Logs, Application Logs เป็นต้น ตามความต้องการทางธุรกิจ และข้อกำหนดทางกฎหมาย
2. จัดให้มีการเก็บข้อมูลบันทึกกิจกรรมที่เกิดจากการดูแลระบบ (Administrator and Operator Logs)
3. ข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) จะต้องได้รับการป้องกันการแก้ไข ลบ หรือทำลาย
4. ข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) อ้างอิงสัญญาณนาฬิกาจากแหล่งเดียวกัน และผิดพลาดได้ไม่เกิน 10 มิลลิวินาที
5. ข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) มีอายุอย่างน้อย 90 วัน

การบริหารจัดการแพทช์:

1. จัดทำเอกสารกระบวนการเพื่อใช้บริหารจัดการแพทช์
2. ตรวจสอบและติดตามให้มีการติดตั้งแพทช์อย่างสม่ำเสมอ การยกเว้นหรือไม่ติดตั้งแพทช์จะต้องได้รับการอนุมัติจากผู้มีอำนาจ
3. จัดให้มีหน่วยงาน และผู้รับผิดชอบติดตามข่าวสารแพทช์โดยตรง โดยเฉพาะแพทช์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัย (Security Patch) ที่ต้องรีบดำเนินการตามคำแนะนำของผู้ผลิต

การจัดการช่องโหว่ (System Hardening):

1. จัดทำเอกสาร Security Baseline ในระบบที่มีความสำคัญ เพื่อใช้กำหนดค่าพารามิเตอร์ได้อย่างถูกต้อง
2. จัดให้มีการตรวจสอบทางเทคนิคเพื่อหาจุดอ่อนในระบบสารสนเทศสำคัญอยู่เสมอ

หมวดที่ 6
ความมั่นคงปลอดภัยในระบบเครือข่าย

วัตถุประสงค์: เพื่อบริหารจัดการระบบเครือข่ายให้มีความปลอดภัย

การออกแบบและจัดการระบบเครือข่าย:

1. ผู้ดูแลระบบออกแบบและจัดการให้ระบบเครือข่ายมีความปลอดภัย และมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย เช่น Firewall, IPS, IDS, Data Leak เป็นต้น
2. ออกแบบและเลือกใช้โปรโตคอลที่มีความปลอดภัยในระบบเครือข่าย

3. ตรวจสอบและควบคุมเส้นทางเครือข่ายให้เป็นไปตามกระบวนการทางธุรกิจ และสอดคล้องตามข้อกำหนดด้านความมั่นคงปลอดภัย
4. ปิดพอร์ตที่ไม่มีความจำเป็นต้องใช้งาน หรืออาจทำให้เกิดผลเสียต่อระบบ ทั้งพอร์ตทางกายภาพและพอร์ตสำหรับ Diagnostic and Configuration Port
5. จัดทำเอกสารระบบ ได้แก่ Network Diagram และคู่มือปฏิบัติงานต่าง ๆ ให้เป็นปัจจุบันเสมอ
6. ระบบเครือข่ายมีความสามารถในการตรวจจับ และป้องกันเหตุการณ์ ดังต่อไปนี้
   6.1 ความพยายามในการบุกรุกผ่านระบบเครือข่าย
   6.2 การใช้งานในลักษณะที่ผิดปกติ
   6.3 การใช้งานและการแก้ไขระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง
7. ต้องแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามหลักความมั่นคงปลอดภัย โดยอย่างน้อยแบ่งออกเป็น 3 ส่วน ได้แก่ ส่วนเซิร์ฟเวอร์ ส่วนสำนักงาน และส่วน DMZ
8. ตรวจสอบสิทธิในการเข้าถึงและความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่น ตรวจสอบระบุตัวตนเครื่องที่เข้าถึงเครือข่าย ตรวจสอบไวรัสและภัยคุกคามที่อาจมีในเครื่อง ตรวจสอบการกำหนดค่า Parameter ต่าง ๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องปิดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Filter MAC Address) และจุดเชื่อมต่อ (Disable Port) ที่ไม่รับอนุญาตให้ใช้งานหรือไม่มีความจำเป็นต้องเชื่อมต่อกับระบบเครือข่าย ออกจากระบบเครือข่ายโดยสิ้นเชิง
9. การแก้ไข หรือเปลี่ยนแปลงค่าพารามิเตอร์ต่าง ๆ ในระบบเครือข่าย และอุปกรณ์เครือข่าย ให้สำรองข้อมูลพารามิเตอร์ก่อนการเปลี่ยนแปลงทุกครั้ง
10. จัดทำเอกสาร Security Baseline ในอุปกรณ์เครือข่ายที่มีความสำคัญ เพื่อใช้กำหนดค่าพารามิเตอร์ได้อย่างถูกต้อง
11. การตรวจสอบโดยใช้เครื่องมือทางเทคนิคในระบบเครือข่ายจะต้องจัดทำแผน ขอบเขต วันที่ดำเนินการ เครื่องมือที่ใช้ และผู้ดำเนินการ เพื่อขออนุมัติก่อนดำเนินงาน
12. ข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) สามารถตรวจสอบหมายเลขเครือข่ายของอุปกรณ์ทั้งจากต้นทางและปลายทางได้
13. การจัดเก็บข้อมูลบันทึกเหตุการณ์ในระบบ (Audit Logs) รวมถึงการเก็บข้อมูลการจราจร (Traffic Logs) ให้เป็นไปตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่น ๆ ที่เกี่ยวข้อง

หมวดที่ 7
การเข้ารหัส

วัตถุประสงค์: เพื่อให้มีควบคุมการใช้งานเทคโนโลยีการเข้ารหัสที่มีคุณภาพ และสอดคล้องกับความต้องการองค์กร

นโยบายการเข้ารหัส:

1. ไม่อนุญาตให้ใช้เทคโนโลยีการเข้ารหัสที่ผิดกฎหมายหรือไม่ได้รับการยอมรับจากหน่วยงานกำกับดูแล
2. การรับ-ส่งข้อมูลที่มีการเข้ารหัสระหว่างประเทศจะต้องเป็นไปตามกฎหมายของประเทศของประเทศที่เกี่ยวข้อง และไม่ขัดต่อหลักสากล
3. ออกแบบและใช้งานเทคโนโลยีการเข้ารหัสที่ปลอดภัยและเชื่อถือได้ โดยอย่างน้อยต้องมีความยาวรหัสที่ 256 บิต หรือเทียบเท่า
4. กำหนดให้ใช้ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) เพื่อรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูล
5. ระบบสารสนเทศที่เชื่อมต่อกับระบบเครือข่ายสาธารณะจะต้องใช้โปรโตคอลเข้ารหัสที่มีความปลอดภัย ได้แก่ SSH, S-HTTP หรือโปรโตคอลที่เทียบเท่าหรือมีความปลอดภัยมากกว่า

การจัดการกุญแจเข้ารหัส

1. การสร้างกุญแจเข้ารหัสจะต้องใช้วิธีการที่ปลอดภัย และดำเนินการโดยผู้ที่มีหน้าที่รับผิดชอบ
2. เก็บรักษากุญแจเข้ารหัสไว้ในที่ปลอดภัยเพื่อป้องกันการสูญหาย ขโมย และการลักลอบใช้งานตลอดอายุการใช้งาน
3. กุญแจเข้ารหัสจะต้องเก็บไว้เป็นความลับ และไม่แจกจ่ายไปยังผู้ที่ไม่เกี่ยวข้อง
4. มีการเก็บรักษาและสำเนากุญแจเข้ารหัสให้สอดคล้องกับอายุของข้อมูลเพื่อให้สามารถอ่านข้อมูลได้

หมวดที่ 8
ความมั่นคงปลอดภัยพื้นที่

วัตถุประสงค์: เพื่อป้องกันความเสียหายที่เกิดจากการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงภัยธรรมชาติ และอุบัติเหตุ

ต่าง ๆ

ข้อกำหนดทั่วไป:

1. ออกแบบพื้นที่สำคัญสูง ให้แยกออกจากพื้นที่สำนักงานทั่วไป
2. ติดตั้งระบบยืนยันตัวบุคคลควบคุมการเข้าออกในจุดสำคัญ
3. ติดตั้งอุปกรณ์ป้องกันภัยและรักษาสภาพแวดล้อมให้เหมาะสม อาทิเช่น ระบบป้องกันไฟไหม้ ระบบป้องกันกระแสไฟฟ้าขัดข้อง ระบบป้องกันน้ำรั่วซึม ระบบควบคุมอุณหภูมิและความชื้น ระบบกล้องวงจรปิด และระบบยืนยันตัวบุคคลควบคุมการเข้าออก เป็นต้น
4. ติดป้ายแสดงตำแหน่งที่อยู่ (Floor Plan) และแสดงป้ายทางหนีไฟชัดเจน
5. ดำเนินการซ้อมอพยพเหตุการณ์ฉุกเฉิน และตรวจสอบความพร้อมใช้งานของอุปกรณ์ เช่น ไฟส่องสว่างตามทางเดิน รวมทั้งการใช้อุปกรณ์ และปุ่มกดฉีดสารดับเพลิงต่างๆ เป็นต้น
6. ไม่ติดป้ายแสดงข้อความหรือระบุพื้นที่สำคัญ
7. จัดพื้นที่ส่งของ (Loading Area) แยกออกจากพื้นที่ใช้งานทั่วไป
8. สายไฟและสายเคเบิลจะต้องแยกจากกันหรือมีวิธีการป้องกันสัญญาณรบกวนที่เหมาะสม

ความมั่นคงปลอดภัยในศูนย์คอมพิวเตอร์ (Data Center Security)

1. จัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในศูนย์คอมพิวเตอร์หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิการเข้าออกศูนย์คอมพิวเตอร์ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเข้าถึงได้เท่านั้น
2. จัดทำข้อควรปฏิบัติติดไว้ที่ศูนย์คอมพิวเตอร์ เพื่อให้ผู้ปฏิบัติงานได้รับทราบ
3. อุปกรณ์คอมพิวเตอร์ที่สำคัญจะต้องจัดวางในตู้เซิร์ฟเวอร์ และล็อกตู้อยู่เสมอ
4. ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้าออกศูนย์คอมพิวเตอร์ จะต้องได้รับการอนุมัติจาก Operation Manager และกำหนดให้มีเจ้าหน้าที่ Operation Support ควบคุมดูแลการทำงานตลอดเวลา
5. มีระบบเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออก วัตถุประสงค์ และขั้นตอนการปฏิบัติงานในศูนย์คอมพิวเตอร์ และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
6. การจัดพื้นที่ในศูนย์คอมพิวเตอร์แยกเป็นสัดส่วน ได้แก่ ส่วนของระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) ส่วนอุปกรณ์สนับสนุน (Facility Zone) เป็นต้น เพื่อจำกัดการเข้าถึงพื้นที่ให้เป็นไปตามหน้าที่และความรับผิดชอบของเจ้าหน้าที่

1) การนำอุปกรณ์สารสนเทศและเครือข่ายออกนอกพื้นที่ศูนย์คอมพิวเตอร์จะต้องได้รับการอนุมัติจาก Operation Manager หรือ Operation Support

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารนี้ มีผลบังคับใช้ตั้งแต่วันที่ 20 กุมภาพันธ์ 2562 เป็นต้นไป

.....

(นายณรงค์ฤทธิ์ ถาวรวิศิษฐพร)
ประธานกรรมการบริษัท
บริษัท ซัคเซสมอร์ บีอิ้งค์ จำกัด (มหาชน)