นโยบายและระเบียบปฏิบัติเกี่ยวกับระบบงานเทคโนโลยีสารสนเทศ

บริษัท มาร์เก็ต คอนเน็กชั่นส์ เอเชีย จำกัด (มหาชน)

สารบัญ

นโยบายและระเบียบปฏิบัติเกี่ยวกับระบบงานเทคโนโลยีสารสนเทศ
บริษัท มาร์เก็ต คอนเน็ตกชั่นส์ เอเชีย จำกัด (มหาชน)

1. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

1.1 ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Directions for Information Security)

วัตถุประสงค์เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและการสนับสนุนด้านความมั่นคง ปลอดภัยสารสนเทศโดยสอดคล้องกับความต้องการทางธุรกิจและกฎหมายและระเบียบข้อบังคับที่ เกี่ยวข้อง

1.1.1 นโยบายตำรับความมั่นคงปลอดภัยสารสนเทศ (Policies for information security) นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศต้องมีการจัดทำ อนุมัติโดยผู้บริหาร เผยแพร่ และสื่อสารให้พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบ

1.1.2 การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the policies for information security) นโยบายความมั่นคงปลอดภัยต้องมีการทบทวนตามรอบระยะเวลาที่กำหนดไว้หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร เพื่อให้นโยบายมีความเหมาะสม เพียงพอ และได้ผล

2. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security)

2.1 โครงสร้างภายในองค์กร (Internal organization)

วัตถุประสงค์เพื่อให้มีการกำหนดกรอบการบริหารจัดการโดยต้องมีการเริ่มต้นและควบคุม การปฏิบัติและการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

2.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities) หน้าที่ความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนดและมอบหมายความรับผิดชอบ

2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) หน้าที่และส่วนงานที่รับผิดชอบที่จะทำให้เกิดการขัดต่อการปฏิบัติงานโดยจะทำให้มีการ เปลี่ยนแปลงทรัพย์สินขององค์กรหรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์โดยไม่ได้รับอนุญาตหรือโดย ไม่ได้เจตนาก็ตาม ต้องมีการแยกหน้าที่ดังกล่าวออกจากกัน เพื่อลดโอกาสการเกิดขึ้นนั้น

2.1.3 การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with authorities) การติดต่อกับหน่วยงานผู้มีอำนาจที่เกี่ยวข้องต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้ สามารถติดต่อได้อย่างต่อเนื่อง

2.1.4 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups) การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่มีความเชี่ยวชาญด้านความ มั่นคงปลอดภัยสารสนเทศ และสมาคมอาชีพ ต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อ ได้อย่างต่อเนื่อง

2.1.5 ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management) การบริหารโครงการไม่ว่าจะเป็นประเภทใดของโครงการก็ตามต้องมีการระบุความมั่นคง ปลอดภัยสารสนเทศของโครงการนั้น

2.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (**Mobile devices and teleworking)**

วัตถุประสงค์เพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและของการใช้ งานอุปกรณ์คอมพิวเตอร์แบบพกพา

2.2.1 นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy) นโยบายและมาตรการสนับสนุนสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาต้องมีการ นำมาใช้งานเพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว

2.2.2 การปฏิบัติงานจากระยะไกล (Teleworking) นโยบายและมาตรการสนับสนุนสำหรับการปฏิบัติงานจากสถานที่หนึ่งในระยะไกลต้องมีการ นำมาใช้งานเพื่อป้องกันข้อมูลที่มีการเข้าถึง การประมวลผล หรือการจัดเก็บ จากสถานที่ดังกล่าว

3. **ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล** (Human Resource Security)

(อ้างอิงจาก นโยบายการสรรหาบุคลากร แผนกทรัพยากรบุคคล)

3.1 ก่อนการจ้างงาน **(**Prior to employment)

วัตถุประสงค์เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเอง และมีความเหมาะสมตามบทบาทของตนเองที่ได้รับการพิจารณา

3.1.1 การคัดเลือก (Screening) การตรวจสอบภูมิหลังของผู้สมัครงานต้องมีการดำเนินการโดยมีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับความต้องการทางธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง

3.1.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment) ข้อตกลงและเงื่อนไขในสัญญาจ้างกับพนักงานและผู้ที่ทำสัญญาจ้างต้องกล่าวถึงหน้าที่ความ รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของพนักงาน ของผู้ที่ทำสัญญาจ้าง และขององค์กร

3.2 ระหว่างการจ้างงาน (During employment)

วัตถุประสงค์เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความ รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง

3.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities) ผู้บริหารต้องกำหนดให้พนักงานและผู้ที่ทำสัญญาจ้างทั้งหมดรักษาความมั่นคงปลอดภัย สารสนเทศโดยปฏิบัติให้สอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กรที่กำหนดไว้

3.2.2 การสร้างความตระหนัก การให้ความรู้และการฝึกอบรมด้านความมั่นคงปลอดภัย สารสนเทศ (Information security awareness, education and training) พนักงานขององค์กรทั้งหมดและผู้ที่ทำสัญญาจ้างที่เกี่ยวข้อง ต้องได้รับการสร้างความ ตระหนัก ให้ความรู้และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ และต้องมีการเรียนรู้และทบทวนเพิ่มเติมในนโยบายและขั้นตอนปฏิบัติขององค์กรที่เกี่ยวข้องกับงานที่ตนเองปฏิบัติ

3.2.3 กระบวนการทางวินัย (Disciplinary process) กระบวนการทางวินัยต้องมีการกำหนดอย่างเป็นทางการและมีการสื่อสารให้พนักงานได้รับ ทราบ เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศขององค์กร

3.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยน หรือสิ้นสุดการจ้างงาน

3.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities) หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่ยังต้องคงไว้หลังการสิ้นสุดหรือเปลี่ยนการจ้างงาน ต้องมีการกำหนดและสื่อสารให้ได้รับทราบต่อพนักงานหรือผู้ที่ทำสัญญาจ้าง รวมทั้งควบคุมให้ปฏิบัติตามอย่างสอดคล้อง

4. การบริหารจัดการทรัพย์สิน (Asset Management)

4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

วัตถุประสงค์เพื่อให้มีการระบุทรัพย์สินขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการ ป้องกันทรัพย์สินอย่างเหมาะสม

4.1.1 บัญชีทรัพย์สิน (Inventory of assets) ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องมีการระบุจัดทำ เป็นทะเบียนทรัพย์สิน และปรับปรุงให้ทันสมัย

4.1.2 ผู้ถือครองทรัพย์สิน (Ownership of assets) ทรัพย์สินในทะเบียนทรัพย์สินต้องมีผู้ถือครองทรัพย์สิน

4.1.3 การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets) กฎเกณฑ์การใช้อย่างเหมาะสมสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับ สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการระบุจัดทำเป็นลายลักษณ์อักษร และบังคับ ใช้ให้เป็นไปอย่างสอดคล้อง

4.1.4 การคืนทรัพย์สิน (Return of assets) พนักงานและลูกจ้างของหน่วยงานภายนอกทั้งหมดต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง

4.2 การจัดชั้นความลับของสารสนเทศ (Information classification)

วัตถุประสงค์ เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสมโดยสอดคล้องกับ ความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร

4.2.1 ชั้นความลับของสารสนเทศ (Classification of information)สารสนเทศต้องมีการจัดชั้นความลับโดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

4.2.2 การบ่งชี้สารสนเทศ (Labeling of information) ขั้นตอนปฏิบัติสำหรับการบ่งชี้สารสนเทศต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความ สอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

4.2.3 การจัดการทรัพย์สิน (Handling of assets) ขั้นตอนปฏิบัติสำหรับการจัดการทรัพย์สินต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความ สอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

4.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)

วัตถุประสงค์เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้ายการ ลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

4.3.1 การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of removable media) ขั้นตอนปฏิบัติสำหรับการบริหารจัดการกับสื่อบันทึกข้อมูลที่ถอดแยกได้ต้องมีการจัดทำและ ปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กร กำหนดไว้

4.3.2 การทำลายสื่อบันทึกข้อมูล (Disposal of media) สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย เมื่อหมดความต้องการใน การใช้งาน โดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายซึ่งกำหนดไว้อย่างเป็นทางการ

4.3.3 การขนย้ายสื่อบันทึกข้อมูล (Physical media transfer) สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การ นำไปใช้ผิดวัตถุประสงค์หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

5. การควบคุมการเข้าถึง (Access Control)

5.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of access control)

วัตถุประสงค์เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

5.1.1 นโยบายควบคุมการเข้าถึง (Access control policy) นโยบายควบคุมการเข้าถึงต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร และทบทวนตาม ความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

5.1.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to networks and network services) ผู้ใช้งานต้องได้รับสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุมัติ การเข้าถึงเท่านั้น

5.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

วัตถุประสงค์เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการ เข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต

5.2.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User registration and deregistration) กระบวนการลงทะเบียนและถอดถอนสิทธิผู้ใช้งานอย่างเป็นทางการต้องมีการปฏิบัติตามเพื่อ เป็นการให้สิทธิการเข้าถึง

5.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User access provisioning) กระบวนการจัดการสิทธิการเข้าถึงของผู้ใช้งานต้องมีการปฏิบัติตาม ทั้งให้และถอดถอนสิทธิ การเข้าถึงสำหรับผู้ใช้งานทุกประเภทและทุกระบบและบริการทั้งหมดขององค์กร

5.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of privileged access right) การให้และใช้สิทธิการเข้าถึงตามระดับสิทธิต้องมีการจำกัดและควบคุม

5.2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users) การมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ ต้องมีการควบคุมโดยผ่าน กระบวนการบริหารจัดการที่เป็นทางการ

5.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) เจ้าของทรัพย์สินต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนดไว้

5.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or adjustment of access rights) สิทธิการเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลง การจ้าง หรือต้องได้รับการปรับปรุงให้ถูกต้องเมื่อมีการเปลี่ยนการจ้างงาน

5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

5.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of secret authentication information) ผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูลการพิสูจน์ตัวตนซึ่งเป็น ข้อมูลลับ

5.4 การควบคุมการเข้าถึงระบบ (System and application access control)

วัตถุประสงค์เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

5.4.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบาย ควบคุมการเข้าถึง

5.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures) กรณีมีการกำหนดโดยนโยบายควบคุมการเข้าถึง การเข้าถึงระบบต้องมีการควบคุมโดยผ่าน ทางขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

5.4.3 ระบบบริหารจัดการรหัสผ่าน (Password management system) ระบบบริหารจัดการรหัสผ่านต้องมีปฏิสัมพันธ์กับผู้ใช้งานและบังคับการตั้งรหัสผ่านที่มี คุณภาพ

5.4.4 การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs) การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมี การจำกัดและควบคุมการใช้อย่างใกล้ชิด

5.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code) การเข้าถึงซอร์สโค้ดของโปรแกรมต้องมีการจำกัดและควบคุม

6. **การเข้ารหัสข้อมูล** (Cryptography)

6.1 มาตรการเข้ารหัสข้อมูล (Cryptographic controls)

วัตถุประสงค์เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผลและป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

6.1.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

นโยบายการใช้มาตรการเข้ารหัสข้อมูลเพื่อป้องกันสารสนเทศต้องมีการจัดทำและปฏิบัติตาม

6.1.2 การบริหารจัดการกุญแจ (Key management) นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจต้องมีการจัดทำและปฏิบัติ ตามตลอดวงจรชีวิตของกุญแจ

7. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)

7.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)

วัตถุประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการ แทรกแซงการทำงาน ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

7.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter) ขอบเขตหรือบริเวณโดยรอบพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการกำหนด ขึ้นมาเพื่อใช้ในการป้องกันพื้นที่สำคัญดังกล่าวอันประกอบไปด้วยสารสนเทศหรืออุปกรณ์ประมวลผล สารสนเทศที่มีความสำคัญ

7.1.2 การควบคุมการเข้าออกทางกายภาพ (Physical entry controls) พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัยต้องมีการป้องกันโดยมีการควบคุมการเข้า ออกอย่างเหมาะสม โดยกำหนดให้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้นที่สามารถเข้าถึงพื้นที่สำคัญได้

7.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และอุปกรณ์ (Securing office, room and facilities) ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และอุปกรณ์ต่างๆ ต้องมีการ ออกแบบและดำเนินการ

7.1.4 การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against external end environmental threats) การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติการโจมตีหรือการบุกรุก หรืออุบัติเหตุ ต้องมีการออกแบบและดำเนินการ

7.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas) ขั้นตอนปฏิบัติสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมี การจัดทำและปฏิบัติตาม

7.1.6 พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)จุดหรือบริเวณที่สามารถเข้าถึงองค์กร เช่น พื้นที่สำหรับรับส่งสิ่งของบริเวณอื่นๆ ที่ผู้ที่ไม่ได้ รับอนุญาตสามารถเข้าถึงพื้นที่ขององค์กรได้ต้องมีการควบคุม และหากเป็นไปได้จุดหรือบริเวณดังกล่าวควรแยกออกมาจากบริเวณที่มีอุปกรณ์ประมวลผลสารสนเทศ เพื่อหลีกเลี่ยงการเข้าถึงโดย ไม่ได้รับอนุญาต

7.2 อุปกรณ์ (Equipment)

วัตถุประสงค์เพื่อป้องกันการสูญหาย การเสียหาย การขโมย หรือการเป็นอันตรายต่อ ทรัพย์สินและป้องกันการหยุดชะงักต่อการดำเนินงานขององค์กร

7.2.1 การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection) อุปกรณ์ต้องมีการจัดตั้งและป้องกันเพื่อลดความเสี่ยงจากภัยคุกคามและอันตรายด้าน สภาพแวดล้อม และจากโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต

7.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities) อุปกรณ์ต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่นๆ ที่มี สาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่างๆ

7.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security) การเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคม ซึ่งส่งข้อมูลหรือสนับสนุนบริการสารสนเทศ ต้องมีการป้องกันจากการขัดขวางการทำงาน การแทรกแซงสัญญาณ หรือการทำให้เสียหาย

7.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance) อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้องเพื่อให้มีสภาพความพร้อมใช้งานและการ ทำงานที่ถูกต้องอย่างต่อเนื่อง

7.2.5 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of assets) อุปกรณ์สารสนเทศ หรือซอฟต์แวร์ต้องไม่มีการนำออกนอกสำนักงาน โดยปราศจากการขอ อนุญาตก่อน

7.2.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of equipment and assets off- premises) ทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัยโดยพิจารณาจากความเสี่ยงของการปฏิบัติงานอยู่ภายนอกสำนักงาน

7.2.7 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์หรือการนำอุปกรณ์ไปใช้ งานอย่างอื่น (Secure disposal or re-use of equipment) อุปกรณ์ที่มีสื่อบันทึกข้อมูลต้องมีการตรวจสอบเพื่อให้มั่นใจว่าข้อมูลสำคัญและซอฟต์แวร์ที่มี ใบอนุญาตมีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการกำจัดอุปกรณ์หรือก่อนการนำอุปกรณ์ไปใช้งานอย่างอื่น

7.2.8 อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment) ผู้ใช้งานต้องมีการป้องกันอุปกรณ์อย่างเหมาะสม ซึ่งเป็นอุปกรณ์ที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล

7.2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy) นโยบาย โต๊ะทำงานปลอดเอกสารสำคัญ' เพื่อป้องกันเอกสารกระดาษและสื่อบันทึกข้อมูลที่ ถอด

แยกได้และนโยบาย 'การป้องกันหน้าจอคอมพิวเตอร์' เพื่อป้องกันสารสนเทศในอุปกรณ์ ประมวลผลสารสนเทศ ต้องมีการนำมาใช้งาน (เพื่อป้องกันการเข้าถึงทางกายภาพต่อเอกสารและ ข้อมูลสำคัญขององค์กร

8. **ความมั่นคงปลอดภัยสำหรับการดำเนินงาน** (Operations Security)

8.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities)

วัตถุประสงค์เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและ มั่นคงปลอดภัย

8.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures) ขั้นตอนการปฏิบัติงานต้องมีการจัดทำเป็นลายลักษณ์อักษรและต้องสามารถเข้าถึงได้โดยผู้ที่ จำเป็นต้องใช้งาน

8.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change management) การเปลี่ยนแปลงต่อองค์กร กระบวนการทางธุรกิจ อุปกรณ์ประมวลผลสารสนเทศ และ ระบบที่มีผลต่อความมั่นคงปลอดภัยสารสนเทศ ต้องมีการควบคุมการดำเนินการ

8.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity management) การใช้ทรัพยากรของระบบต้องมีการติดตาม ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติม ในอนาคตเพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ

8.1.4 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, testing and operational environments) สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการจัดทำแยกกัน เพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับ อนุญาต

8.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจาก โปรแกรมไม่ประสงค์ดี

8.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against malware) มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดีต้องมีการ ดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

8.3 การสำรองข้อมูล (Backup)

วัตถุประสงค์เพื่อป้องกันการสูญหายของข้อมูล

8.3.1 การสำรองข้อมูล (Information backup) ข้อมูลสำรองสำหรับสารสนเทศ ซอฟต์แวร์และอิมเมจของระบบ ต้องมีการดำเนินการสำรอง ไว้และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอตามนโยบายการสำรองข้อมูลที่ได้ตกลงไว้

8.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

วัตถุประสงค์เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

8.4.1 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event logging) ข้อมูลล็อกแสดงเหตุการณ์ซึ่งบันทึกกิจกรรมของผู้ใช้งาน การทำงานของระบบที่ไม่เป็นไป ตามขั้นตอนปกติความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัย ต้องมี การบันทึกไว้จัดเก็บ และทบทวนอย่างสม่ำเสมอ

8.4.2 การป้องกันข้อมูลล็อก (Protection of log information) อุปกรณ์บันทึกข้อมูลล็อกและข้อมูลล็อกต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและ การเข้าถึงโดยไม่ได้รับอนุญาต

8.4.3 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs) กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการต้องมีการบันทึกไว้เป็นข้อมูลล็อก ข้อมูล ดังกล่าวต้องมีการป้องกันและทบทวนอย่างสม่ำเสมอ

8.4.4 การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization) นาฬิกาของระบบที่เกี่ยวข้องทั้งหมดภายในองค์กรหรือในขอบเขตหนึ่ง ต้องมีการตั้งให้ตรง และถูกต้องเทียบกับแหล่งอ้างอิงเวลาแห่งหนึ่ง

8.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational software)

วัตถุประสงค์เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง

8.5.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems) ขั้นตอนปฏิบัติสำหรับการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการต้องมีการปฏิบัติ ตามให้สอดคล้อง

8.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

8.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities) ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบที่ใช้งานต้องมีการติดตามอย่างทันกาล จุดอ่อน ต่อช่องโหว่ดังกล่าวขององค์กรต้องมีการประเมินและมาตรการที่เหมาะสมต้องถูกนำมาใช้เพื่อจัดการ กับความเสี่ยงที่เกี่ยวข้อง

8.6.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on software installation) กฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งานต้องมีการกำหนดและปฏิบัติตาม

8.7 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)

วัตถุประสงค์เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบให้บริการ

8.7.1 มาตรการการตรวจประเมินระบบ (Information systems audit controls) ความต้องการในการตรวจประเมินและกิจกรรมการตรวจประเมินระบบให้บริการต้องมีการ วางแผนและตกลงร่วมกันอย่างระมัดระวังเพื่อลดโอกาสการหยุดชะงักที่มีต่อกระบวนการทางธุรกิจ

9. **ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล** (Communications security)

9.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

วัตถุประสงค์เพื่อให้มีการป้องกันสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ

9.1.1 มาตรการเครือข่าย (Network controls) เครือข่ายต้องมีการบริหารจัดการและควบคุมเพื่อป้องกันสารสนเทศในระบบต่างๆ

9.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services) กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และความต้องการในส่วนของผู้บริหาร สำหรับบริการเครือข่ายทั้งหมด ต้องมีการระบุและรวมไว้ในข้อตกลงการให้บริการเครือข่าย ไม่ว่า บริการเหล่านี้จะมีการให้บริการโดยองค์กรเองหรือจ้างการให้บริการก็ตาม

9.1.3 การแบ่งแยกเครือข่าย (Segregation in networks) กลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบ ต้องมีการจัดแบ่งเครือข่ายตามกลุ่มที่กำหนด

9.2 การถ่ายโอนสารสนเทศ (Information transfer)

วัตถุประสงค์เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายใน องค์กรและถ่ายโอนกับหน่วยงานภายนอก

9.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures) นโยบาย ขั้นตอนปฏิบัติและมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการต้องมี การปฏิบัติเพื่อป้องกันสารสนเทศที่มีการถ่ายโอน โดยผ่านทางการใช้อุปกรณ์การสื่อสารทุกประเภท

9.2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on information transfer) ข้อตกลงสำหรับการถ่ายโอนสารสนเทศทางธุรกิจให้มีความมั่นคงปลอดภัยต้องมีการระบุ ระหว่างองค์กรกับหน่วยงานภายนอก

9.2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging) สารสนเทศที่เกี่ยวข้องกับการส่งข้อความทางอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่าง เหมาะสม

9.2.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or nondisclosure agreements) ความต้องการในการรักษาความลับหรือการไม่เปิดเผยความลับซึ่งสะท้อนถึงความจำเป็นของ องค์กรในการป้องกันสารสนเทศ ต้องมีการระบุ ทบทวนอย่างสม่ำเสมอ และบันทึกไว้อย่างเป็นลาย ลักษณ์อักษร

10. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)

10.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)

วัตถุประสงค์เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบ ตลอดวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่าย สาธารณะด้วย

10.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information security requirements analysis and specification) ความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศต้องมีการรวมเข้ากับความ ต้องการสำหรับระบบใหม่ หรือการปรับบปรุงระบบที่มีอยู่แล้ว

10.1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks) สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกันจากการฉ้อโกง การโต้เถียง และการเปิดเผยและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับ อนุญาต

10.1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions) สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่ง ข้อมูลที่ไม่สมบูรณ์การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การ เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต

10.2 ความมนคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)

วัตถุประสงค์เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบและดำเนินการตลอด วงจรชีวิตของการพัฒนาระบบ

10.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy) กฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบต้องมีการกำหนดและปฏิบัติตามสำหรับการ พัฒนาระบบขององค์กร

10.2.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change control procedures) การเปลี่ยนแปลงระบบในวงจรชีวิตของการพัฒนาระบบต้องมีการควบคุมโดยปฏิบัติตาม ขั้นตอนปฏิบัติสำหรับการเปลี่ยนแปลงระบบที่กำหนดไว้อย่างเป็นทางการ

10.2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes) เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบสำคัญต้องมีการทบทวนและ ทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือด้านความมั่นคงปลอดภัยของ องค์กร

10.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages) การเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูปต้องไม่อนุญาตการดำเนินการ จำกัดการเปลี่ยนแปลง เท่าที่จำเป็น และต้องมีการควบคุมอย่างรัดกุม

10.2.5 หลักการวิศวะกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles) หลักการวิศวกรรมระบบให้มีความมั่นคงปลอดภัยต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์ อักษร ปรับปรุงอย่างต่อเนื่อง และประยุกต์กับงานการพัฒนาระบบ

10.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment) องค์กรต้องจัดทำและป้องกันอย่างเหมาะสมต่อสภาพแวดล้อมของการพัฒนาระบบที่มีความ มั่นคงปลอดภัย ทั้งการพัฒนาและปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ

10.2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced development) องค์กรต้องกำกับดูแล เฝ้าระวัง และติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงาน ภายนอกเป็นผู้ดำเนินการ

10.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing) การทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการในระหว่างที่ ระบบอยู่ในช่วงการพัฒนา

10.2.9 การทดสอบเพื่อรับรองระบบ (System acceptance testing) แผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ ต้องมีการจัดทำสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชั่นใหม่

10.3 ข้อมูลสำหรับการทดทดสอบ (Test data)

วัตถุประสงค์เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

10.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data) ข้อมูลสำหรับการทดสอบระบบต้องมีการคัดเลือกอย่างระมัดระวัง มีการป้องกัน และควบคุม การนำมาใช้งาน

11. ระเบียบการปฏิบัติงานเรื่องการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management)

11.1 วัตถุประสงค์

จัดทำขึ้นเพื่อกำหนดกระบวนการในการบริหารจัดการผู้ให้บริการภายนอก เพื่อให้บริษัทมั่นใจได้ว่าบริษัทมีกระบวนการและหลักเกณฑ์ในการประเมินและคัดเลือกผู้ให้บริการภายนอก ต้องจัดทำสัญญาจ้างการให้บริการและกำหนดเงื่อนไขให้ผู้ให้บริการภายนอกปฏิบัติตามการรักษาความปลอดภัยของบริษัท รวมถึงต้องกำหนดข้อตกลงการให้บริการ (Service Level Agreement : SLA) พร้อมทั้งมีการตรวจสอบและติดตามการให้บริการ

11.2 บทบาท หน้าที่และความรับผิดชอบ

แผนกเทคโนโลยีสารสนเทศ มีหน้าที่กำหนดให้การบริหารจัดการผู้ให้บริการภายนอกภายในบริษัทเป็นไปตามขั้นตอนและแนวทางในการบริหารจัดการผู้ให้บริการภายนอก

11.3 แนวทางและขั้นตอนในการดำเนินงาน

แผนกเทคโนโลยีสารสนเทศมีหน้าที่ในการกำกับดูแลให้บริษัทมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยจากภัยไซเบอร์ที่ครอบคลุมการใช้บริการจากผู้ให้บริการภายนอก

11.3.1 กำหนดหลักเกณฑ์ที่ชัดเจนในการตัดสินใจใช้บริการจากผู้ให้บริการภายนอกเช่น เหตุผลความจำเป็นทางธุรกิจประโยชน์ที่ได้รับและต้นทุน รวมทั้งต้องพิจารณาว่าการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศไม่ขัดต่อกฎหมายและข้อบังคับที่บริษัทต้องปฏิบัติตาม และไม่ก่อให้เกิดช่องโหว่ที่นำไปสู่การเกิดการทุจริตที่ร้ายแรง หรือก่อให้เกิดภัยคุกคามด้านเทคโนโลยีสารสนเทศทั้งจากภายในและภายนอก

11.3.2 กำหนดการบริหารจัดการความเสี่ยงที่เกี่ยวเนื่องกับการใช้บริการผู้ให้บริการภายนอกอย่างเหมาะสม

11.4 หลักเกณฑ์การเลือกใช้บริการจากผู้ให้บริการภายนอก

บริษัทกำหนดแนวทางการคัดเลือกผู้ให้บริการภายนอกอย่างเหมาะสมก่อนที่จะทำสัญญาใหม่หรือทบทวนเพื่อต่ออายุสัญญาการใช้บริการจากผู้ให้บริการภายนอกรายเดิมโดยต้องพิจารณาให้ครอบคลุมประเด็นสำคัญดังนี้

11.4.1 ศักยภาพและความสามารถในการให้บริการทั้งในภาวะปกติและไม่ปกติ โดยเฉพาะอย่างยิ่งกรณีที่ผู้ให้บริการภายนอกนั้นมีการให้บริการแก่ผู้ใช้บริการหลายราย (Concentration Risk)

11.4.2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

11.4.3 การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ

11.4.4 การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เป็นต้น

11.4.5 การปฏิบัติตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ เช่น การขอตรวจสอบ หรือสามารถแสดงเอกสารหลักฐานการได้รับการรองรับตามมาตรฐาน ISO 27001 เป็นต้น

ทั้งนี้หน่วยงานที่เกี่ยวข้องในการเลือกใช้บริการผู้ให้บริการภายนอกต้องร่วมพิจารณาการดัดเลือกผู้ใช้บริการภายนอกร่วมกับแผนกเทคโนโลยีสารสนเทศ ก่อนสรุปเลือกผู้ให้บริการภายนอกต่อไป

11.5 สัญญาและข้อตกลง

สัญญาและข้อตกลงกับผู้ให้บริการภายนอกเป็นลายลักษณ์อักษร โดยต้องพิจารณาให้ครอบคลำคัญดังต่อไปนี้

11.5.1 ผู้ให้บริการภายนอกคิดค่า บริการต่ำกว่า 50,000 บาท หรือ หรือระยะเวลาที่ใช้บริการ น้อยกว่า 1 ปีไม่จำเป็นต้องทำการประเมินผู้ให้บริการภายนอก แต่สำหรับกรณีจำเป็นต้องทำการพิจารณา ให้พิจารณาตามความเหมาะสม

11.5.2 กำหนดรายละเอียดประเภทของการใช้บริการ ขอบเขตความรับผิดชอบ การบริหารความเสี่ยง ระบบควบคุมภายในระบบรักษาความปลอดภัยในการเก็บรักษาข้อมูลและทรัพย์สินของบริษัท

11.5.3 ข้อตกลงการให้บริการ (Service Level Agreement) เพื่อกำหนดเป็นมาต รฐานการให้บริการขั้นต่ำที่ผู้ให้บริการภายนอกต้องปฏิบัติทั้งภายใต้สถานการณ์ปกติและไม่ปกติ

11.5.4 แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Pian) ของผู้ให้บริการภายนอก เพื่อรองรับกรณีงานที่ใช้บริการจากผู้ให้บริกาวภายนอกมีปัญหาหยุดชะงักลง และไม่สามารถให้บริการได้อย่างต่อเนื่อง

11.5.5 ขั้นตอนการติดตาม ตรวจสอบ และประเมินประสิทธิภาพการปฏิบัติงานของผู้ให้บริการภายนอก

11.5.6 อายุสัญญา ข้อทำหนด และเงื่อนไขการยกเลิกสัญญา ซึ่งรวมถึงสิทธิของบริษัทในการเปลี่ยนแปลงแก้ไขและต่ออายุสัญญา เพื่อให้มีความคล่องตัวในการปรับปรุงการให้บริการหากจำเป็น รวมทั้งเพื่อไม่ให้เป็นอุปสรรคต่อการดำเนินงานของบริษัทในอนาคต

11.5.7 ขอบเขตความรับผิดชอบของคู่สัญญาในกรณีการให้บริการเกิดปัญหาขัดข้อง เช่น การบริการล่าช้า และความผิดพลาดในการให้บริการ เป็นต้น ตลอดจนแนวทางแก้ไขปัญหาต่าง ๆ หรือการรดใช้ค่าเสียหายที่เกิดขึ้น

11.5.8 การรักษาความปลอดภัยของข้อมูล การรักษาความลับ และความเป็นส่วนตัวของข้อมูลของลูกค้า และข้อมูลของบริษัทรวมถึงสิทธิในการเข้าถึง และความเป็นเจ้าของข้อมูล ตลอดจนบทลงโทษอย่างชัดเจน หากมีการเปิดเผยข้อมูลของลูกค้าและหรือข้อมูลของบริษัท ให้อ้างอิงผลของการผิดสัญญาตาม เอกสารสัญญารักษาความลับฉบับปรับปรุงล่าสุดของบริษัท

11.6 การติดตามและประเมินการให้บริการ

หน่วยงานที่เกี่ยวข้องในการใช้บริการผู้ให้บริการภายนอกต้องร่วมกับ แผนกเทคโนโลยีสารสนเทศ เพื่อทำการกำกับดูแลติดตาม ตรวจสอบ และประเมินผลผู้ให้บริการภายนอกอย่างเหมาะสม เพื่อให้มีมาตรฐานการควบคุมภายในและการให้บริการเช่นเดียวกับบริษัทดำเนินการเอง และตรงตามสัญญาหรือข้อตกลงการให้บริการ (Service Level Agreement) ที่ได้ทำการตกลงกันไว้ โดยจะต้องทำการประเมินการให้บริการอย่างน้อยทุก 1 ปี

12. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

12.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและ จุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ

12.1.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการบริหารจัดการต้องมีการกำหนดเพื่อให้มี การตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

12.1.2 การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events) สถานการณ์ความมั่นคงปลอดภัยสารสนเทศต้องมีการรายงานผ่านทางช่องทางการบริหาร จัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

12.1.3 การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting information security weaknesses) พนักงานและผู้ที่ทำสัญญาจ้างซึ่งใช้ระบบและบริการสารสนเทศขององค์กรต้องสังเกตและ รายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศในระบบหรือบริการที่สังเกตพบหรือที่สงสัย

12.1.4 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events) สถานการณ์ความมั่นคงปลอดภัยสารสนเทศต้องมีการประเมินและต้องมีการตัดสินว่า สถานการณ์นั้นเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่

12.1.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents) เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตาม ขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

12.1.6 การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents) ความรู้ที่ได้รับจากการวิเคราะห์และแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องถูก นำมาใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ความมั่นคงปลอดภัยที่จะเกิดขึ้นในอนาคต

12.1.7 การเก็บรวบรวมหลักฐาน (Collection of evidence) องค์กรต้องกำหนดและประยุกต์ใช้ขั้นตอนปฏิบัติสำหรับการระบุการรวบรวม การจัดหา และการจัดเก็บสารสนเทศซึ่งสามารถใช้เป็นหลักฐาน

13. ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความ ต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)

13.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

13.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศและด้านความต่อเนื่อง ในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติหนึ่ง

13.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity) องค์กรต้องกำหนด จัดทำเป็นลายลักษณ์อักษร ปฏิบัติและปรับปรุง กระบวนการ ขั้นตอน ปฏิบัติและมาตรการ เพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

13.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัย สารสนเทศ (Verify, review and evaluate information security continuity) องค์กรต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมการไว้ตามรอบระยะเวลา ที่กำหนดไว้เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้องและได้ผลเมื่อมีสถานการณ์ความเสียหาย เกิดขึ้น

13.2 การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

วัตถุประสงค์เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

13.2.1 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities) อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอเพื่อให้ตรงตาม ความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

14. ความสอดคล้อง (Compliance)

14.1 **ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง** (Compliance with legal and contractual requirements)

วัตถุประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญา จ้าง ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และที่เป็นความต้องการด้านความมั่นคงปลอดภัย

14.1.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements) ความต้องการทั้งหมดที่เกี่ยวข้องกับกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง รวมทั้งวิธีการขององค์กรเพื่อให้สอดคล้องกับความต้องการดังกล่าว ต้องมีการระบุอย่างชัดเจน จัดทำเป็น ลายลักษณ์อักษร และปรับปรุงให้ทันสมัย สำหรับแต่ละระบบและสำหรับองค์กร

14.1.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual property rights) ขั้นตอนปฏิบัติที่เหมาะสมต้องได้รับการปฏิบัติอย่างสอดคล้อง เพื่อให้มั่นใจว่ามีความ สอดคล้องกับความต้องการของกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้างที่ว่าด้วยเรื่องสิทธิใน ทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์

14.1.3 การป้องกันข้อมูล (Protection of records) ข้อมูลขององค์กรต้องได้รับการป้องกันจากการสูญหาย การถูกทำลาย การปลอมแปลง การ เข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่โดยไม่ได้รับอนุญาต โดยต้องสอดคล้องกับความต้องการ ของกฎหมาย ระเบียบข้อบังคับ สัญญาจ้าง และความต้องการทางธุรกิจ

14.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information) ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคลต้องมีการดำเนินการให้สอดคล้องกับ กฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

14.1.5 ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Regulation of cryptographic controls) มาตรการเข้ารหัสข้อมูลต้องมีการใช้ให้สอดคล้องกับข้อตกลง กฎหมาย และระเบียบ ข้อบังคับทั้งหมดที่เกี่ยวข้อง

14.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)

วัตถุประสงค์เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับ นโยบายและขั้นตอนปฏิบัติขององค์กร

14.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security) วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติขององค์กร (กล่าวคือ วัตถุประสงค์ มาตรการ นโยบาย กระบวนการ และขั้นตอนปฏิบัติเพื่อความมั่นคงปลอดภัย สารสนเทศ) ต้องมีการทบทวนอย่างอิสระตามรอบระยะเวลาที่กำหนดไว้หรือเมื่อมีการเปลี่ยนแปลง องค์กรที่มากเกิดขึ้น

14.2.2 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards) ผู้จัดการต้องดำเนินการทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลผล สารสนเทศและขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง โดยเทียบกับนโยบาย มาตรฐาน และความต้องการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

14.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review) ระบบต้องได้รับการทบทวนอย่างสม่ำเสมอเพื่อพิจารณาความสอดคล้องกับนโยบายและ มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

15. ระเบียบการปฏิบัติงานเรื่องการบริหารโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management)

15.1 วัตถุประสงค์

ทำขึ้นเพื่อกำหนดกระบนการในการบริหารโครงการด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถมั่นใจได้ว่า มีการบริหารจัดการความเสี่ยงของการดำเนินโครงการด้านเทคโนโลยีสารนเทศอย่างมีประสิทธิภาพและ ไม่ก่อให้เกิดผลกระทบต่อการดำเนินงาน โดยให้บริษัทพิจารณาประเด็นความเสี่ยง และความสำคัญของโครงการ

15.2 บทบาทหน้าที่และความรับผิดชอบ

แผนกเทคโนโลยีสารสนเทศจะพิจารณาโครงการตามประเด็นความเสี่ยงอย่างรอบคอบและเหมาะสม

15.3 แนวทางและขั้นตอนในการดำเนินงาน

15.3.1 การบริหารจัดการความเสี่ยงของการดำเนินโครงการด้านเทคโนโลยีสารสนเทศ

- ผู้จัดการโครงการ (Project Manager) ต้องประเมินความเสี่ยงและการจัดลำดับความสำคัญของโครงการด้านเทคโนโลยีสารสนเทศ เพื่อนำเสนอขอการอนุมัติโครงการ โดยจะต้องมีการดำเนินการอย่างน้อยดังต่อไปนี้
- ศึกษาความจำเป็นและประโยชน์ที่คาดว่าจะได้รับของโครงการที่มีการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจก่อนเริ่มโครงการ โดยต้องมีการพิจารณาเลือกใช้เทคโนโลยีอย่างเหมาะสม
- มีการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับฝ่ายงานอื่นและระบบที่เกี่ยวข้อง โดยถ้าพบว่ามีผลกระทบหรือมีความเกี่ยวข้องกับฝ่ายงานอื่น จำเป็นต้องเชิญผู้เกี่ยวข้องนั้น ๆ เข้าร่วมโครงการและในกรณี ที่พบว่ามีความเสี่ยงใด ๆ เกิดขึ้น จำเป็นต้องนำเสนอการควบคุมหรือกระจายความเสี่ยงนั้น ๆ เข้ามาในแผนการนำเสนอโครงการ
- มีการจัดลำดับความสำคัญของโครงการ และนำเสนอขออนุมัติโครงการต่อ คณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย เมื่อมีการนำเทคโนโลยีใดมาใช้เป็นครั้งแรก ที่อาจมีผลกระทบหรือมีความเสี่ยงอย่างมีนัยสำคัญต่อการดำเนินธุรกิจในภาพรวมบริษัท บริษัทต้องมีข้อกำหนดที่ชัดเจนในการพิจารณา รวมไปถึงต้อง จัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือ พิจารณาประเด็นความเสี่ยงที่เกี่ยวข้อง รวมทั้งผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของบริษัทในภาพรวม และให้คณะกรรมที่ได้รับมอบหมาย พิจารณาอนุมัติแผนงานในการนำเทคโนโลยีดังกล่าวมาใช้งาน

16. ระเบียบการปฏิบัติงานเรื่องการบริหารจัดการภัยคุกคามทางไซเบอร์

16.1. วัตถุประสงค์

เพื่อให้มั่นใจว่าบริษัทมีมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่องมีการบันทึกกิจกรรมหรือเหตุการณ์ ซึ่งบันทึกกิจกรรมของผู้ใช้งาน การทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศและอุปกรณ์ต่าง ๆ ที่เกี่ยวข้อง ต้องมีการบันทึกไว้ จัดเก็บ และทบทวนอย่างสม่ำเสมอ มีมาตรฐานและระเบียบวิธีปฏิบัติในการติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม เพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง

16.2 ขอบเขตของเอกสาร

ขั้นตอนและแนวทางในการปฏิบัติงานฉบับนี้ ใช้กับการปฏิบัติงานการติดตามดูแลระบบและการเฝ้าระวังภัยคุกคาม

16.3 บทบาท หน้าที่และความรับผิดชอบ

ขั้นตอนและแนวทางในการติดตามดูแลระบบและการเฝ้าระวังภัยคุกคามในเอกสารฉบับนี้ จะเกี่ยวข้องกับผู้ที่มีบทบาทหน้าที่และความรับผิดชอบดังต่อไปนี้

- ผู้ดูแลระบบ มีหน้าที่ในการจัดเก็บหลักฐาน ติดตามดูแล ระบบ เฝ้าระวังภัยคุกคามและรายงานช่องโหว่ที่เกี่ยวข้องกับระบบงานของบริษัท
- หัวหน้าแผนกเทคโนโลยีสารสนเทศ มีหน้าที่ในการพิจารณาวางแผนจัดการภัยคุกคาม และการปิดช่องโหว่ที่เกี่ยวข้องกับระบบงานของบริษัท

16.4 แนวทางและขั้นตอนในการดำเนินงาน

16.4.1 การเตรียมความพร้อม (Preparation)

แผนกเทคโนโลยีสารสนเทศ ต้องจัดให้มีทรัพยากรที่สำคัญต่อการตอบสนองต่อภัยคุกคามทางไซเบอร์ มีกระบวนการและกลไกในการป้องกันระบบที่ดี เพื่อช่วยลดโอกาสที่การโจมตีจะสำเร็จ หรือลดผลกระทบจาก การโจมตี และช่วยทำหน้าที่ในการตรวจจับความพยายามในการบุกรุก โดยจะต้องจัดเตรียมทรัพยากรและกระบวนการป้องกัน

16.4.2 การตรวจจับและวิเคราะห์ (Detection & Analysis)

การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident มีการกำหนดการแจ้งเตือนที่ใช้ในการตรวจจับดังนี้

- Anti-Malware Software ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ปัจจุบันทำงานได้ทั้งในระดับเครือข่าย และ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งความพยายามในการโจมตีหรือการโจมตีได้สำเร็จลุล่วงแล้ว
- Operating System and Application Log ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วยบันทึกเหตุการณ์หลากหลายประเภท สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์
- Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย ก็สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้เช่นเดียวกัน ขึ้นอยู่กับประเภทของ Log และ Ruleset ที่ใช้ในการวิเคราะห์
- บุคคลภายในองค์กร บุคลากรทุกตำแหน่งสามารถ ข้ารับการฝึกฝนเพื่อช่วยสอดส่องดูแลความผิดปกติที่เกิดกับระบบเทคโนโลยีสารสนเทศได้
- บุคคลภายนอกองค์กร บุคคลภายนอก เช่น ลูกค้าก็สามารถเป็นแหล่งข้อมูลการทำงานผิดปกติของระบบได้
- ทั้งนี้แผนกเทคโนโลยีสารสนเทศอาจเลือกใช้อุปกรณ์ป้องกันและตรวจจับ โดยพิจารณาความเหมาะสมกับระบบที่ต้องการจะป้องกันแล้ว ควรต้องมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ เป็นสำคัญ

16.4.3 การบันทึกข้อมูลเหตุการณ์ภัยคุกคาม แผนกเทคโนโลยีสารสนเทศต้องจัดให้มีการบันทึกข้อมูลเหตุการณ์ภัยคุกคามซึ่งจะช่วยให้การรับมือและตอบสนองภัยคุกคามมีประสิทธิภาพและเป็นระบบมากขึ้น โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้น ตั้งแต่การตรวจพบจนถึงการสิ้นสุดของเหตุการณ์ภัยคุกคาม

16.4.4 การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจเชิงกลยุทธ์ เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสม ภายใต้ทรัพยากรที่มีอยู่อย่างจำกัดของบริษัท และลดผลกระทบทางธุรกิจให้น้อยลงที่สุด โดยอย่างน้อยการวิเคราะห์ผลกระทบและความรุนแรงควรครอบดลุมในด้านผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อข้อมูล (Information Impact) และความสามารถในการฟื้นฟูระบบ (Recoverability)

16.4.4 ผลกระทบต่อการให้บริการ (Functional Impact)

ผลกระทบต่อการให้บริการ และการดำเนินงานของหน่วยงานที่เกิด ภัยคุกคาม โดยควรพิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาสเกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันทีซึ่งรวมถึง

ผลกระทบทางด้านการปฏิบัติงานของระบบ IT ซึ่งส่งผลโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหายต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมีผลเสียมากยิ่งขึ้น

16.4.5 ผลกระทบต่อข้อมูล (Information Impact)

ผลกระทบต่อข้อมูล ควรพิจารณา 3 ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อมใช้ (Availability) รวมทั้งควร พิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมของบริษัทอย่างไร และส่งผลต่อ ข้อมูลสำคัญของบริษัท (Sensitive Information)อย่างไร เช่น ข้อมูลถูกทำลาย หรือสูญหาย หรือ รั่วไหล หรือการแก้ไขโดยไม่ได้รับอนุญาตเป็นต้น

16.4.6 ความสามารถในการฟื้นฟูระบบ (Recoverability)

ความสามารถในการฟื้นฟูระบบ ควรพิจารณาจาก ระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟู ระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของเหตุภัยคุกคามและประเภทของทรัพย์สินสารสนเทศเช่น ระบบ และข้อมูล เป็นต้นที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณา ความสามารถ หรือความยากง่ายในการฟื้นฟูระบบ รวมทั้งทรัพยากรที่จำเป็นต้องใช้

16.5 การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery)

1. พิจารณาวิธีการในการควบคุมความเสียหายการควบคุมความเสียหายมีความจำเป็นอย่าง ยิ่ง ที่จะป้องกันไม่ให้ความเสียหายกระจายออกไปเป็นวงกว้าง สร้างผลกระทบต่อทรัพยากรในการดำเนินธุรกิจอื่นๆ และยังเป็นการเปิดพื้นที่เพิ่มระยะเวลาให้ทีมที่รับมือ Incident มีเวลาในการคิดหาสาเหตุ และวิธีการแก้ปัญหาที่ถาวรได้ ข้อสำคัญของการควบคุมความเสียหาย คือการตัดสินใจเลือกใช้วิธีการที่เหมาะสมโดยวิธีการทั่วไปมีดังต่อไปนี้

- ปิดระบบ (Shut Down) ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network Disconnection) ทั้งนี้อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint
- Detection & Response Agent (กระบวนการตรวจสอบและตราจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใดๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions) Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/Sandbox / Honeypot

2. การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัลแผนกเทคโนโลยีสารสนเทศมีหน้าที่ในการจัดเก็บหลักฐานเพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อยที่สุด (Minimizing impact to the business) นอกจากนี้หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการตามขั้นตอนทางกฎหมาย รายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

- ข้อมูลเฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) และ Address เป็นต้น
- ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident
- สถานที่จัดเก็บหลักฐาน

3. การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติหลังจากดำเนินการควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว แผนกเทคโนโลยีสารสนเทศมีหน้าที่ทำการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติ และควรมีการเตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย
- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

16.6 การดำเนินการหลังจากการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น (Post-Incident Activity)

บริษัทมีการเรียนรู้จากเหตุภัยคุกคามที่เกิดขึ้น เพื่อนำมาปรับปรุงและพัฒนาแนวทางในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์รวมทั้งจัดสรรทรัพยากรและเทคโนโลยีให้มีความพร้อมต่อการรับมือเหตุภัยคุกคามต่อไปในอนาคต นอกจากนี้บริษัทควรจัดให้มีการประชุมของฝ่ายหรือหน่วยงานที่มี ความเกี่ยวข้องกับเหตุการณ์ภัยดุกคามทางไซเบอร์ที่เกิดขึ้น โดยวัตถุประสงค์ของการประชุมเพื่อให้ทุกหน่วยงานที่เกี่ยวข้องได้มีการแลกเปลี่ยนข้อมูล รวมทั้งทบทวนเหตุภัยคุกคาม และวิธีการรับมือและตอบสนองต่อภัยดุกคามที่เกิดขึ้น

17. ระเบียบการปฏิบัติงานเรื่องการจัดหาและพัฒนาระบบ (System Acquisition and Development)

17.1. วัตถุประสงค์

เพื่อกำหนดกระบวนการในการสร้างและพัฒนาระบบ เพื่อให้บริษัทลามารถมั่นใจได้ว่าบริษัทมีหลักเกณฑ์และกระบวนการในการสร้างและพัฒนาระบบ (System Development) ที่คำนึงถึงความมั่นคงปลอดภัยของข้อมูลในทุกขั้นตอนของการพัฒนาระบบ

17.2 ขอบเขตของเอกสาร

ขั้นตอนและแนวทางในการปฏิบัติงานฉบับนี้ ใช้กับการสร้างและพัฒนาระบบด้านเทคโนโลยีสารสนเทศทั้งหมด

17.3 บทบาท หน้าที่และความรับผิดชอบ

ขั้นตอนและแนวทางในการปฏิบัติงานเรื่องการบริหารโครงการด้านเทคโนโลยีสารสนเทศในเอกสารฉบับนี้ จะเกี่ยวข้องกับผู้ที่มีบทบาทหน้าที่และความรับผิดชอบดังต่อไปนี้

- ผู้จัดการโครงการ (Project Manager) เป็นผู้รับผิดชอบในการดำเนินการวางแผนและกำกับดูแลการปฏิบัติงานการบริหารโครงการด้านเทคโนโลยีสารสนทศให้เป็นไปตามแนวทางที่ได้
- คณะทำงานบริหารโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management) มีหน้าที่ในการอนุมัติแผนงานตลอดจนให้ความเห็น คำแนะนำหรือข้อเสนอแนะที่เป็นประโยชน์ต่อการบริหารโครงการ

17.4 แนวทางและขั้นตอนในการดำเนินงาน

17.4.1 การจัดหาระบบ

บริษัทพิจารณาใช้ผู้ให้บริการภายนอกในการพัฒนาระบบ ผู้จัดการโครงการ (Project Manager) ต้องปฏิบัติตามระเบียบการปฏิบัติงานเรื่องการบริหารจัดการผู้ให้บริการภายนอก

17.4.2 แนวทางและขั้นตอนในการพัฒนาระบบเทคโนโลยีสารสเทศ

- ฝ่ายงานที่ขอให้ดำเนินการ มีหน้าที่จัดทำเอกสารสรุปความต้องการของผู้ใช้งาน (User Requirement) และกำหนดขอบเขต
- ฝ่ายงานที่ขอให้ดำเนินการ นำเสนอเอกสารสรุปความต้องการของผู้ใช้งาน (User Requirement) และแผนการดำเนินงานการพัฒนาระบบเทคโนโลยีสารสนเทศแก่ที่ประชุมคณะทำงานบริหารโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management) ซึ่งประกอบไปด้วยตัวแทนแต่ละฝ่ายที่มีส่วนเกี่ยวข้องเพื่อขอการอนุมัติแผนการดำเนินงาน และร่วมกันสรุปต้องการของผู้ใช้งาน (User Requirement) เพื่อสรุปจัดทำเอกสารความต้องการของระบบงาน (Requirement) รายละเอียดคุณสมบัติทางเทคนิค (Technical Specification) โดยครอบคลุมถึงเรื่องการรักษาความมั่นคงปลอดภัยซึ่งรวมถึงกระบวนการในการทดสอบระบบงาน รวมทั้งทำการแต่งตั้งผู้จัดการโครงการ (Project Manager)
- เมื่อได้รับการอนุมัติจากคณะทำงานบริหารโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management) ผู้จัดการเทคโนโลยีสารสนเทศจะดำเนินการมอบหมายให้ทีมพัฒนาระบบทำการพัฒนาระบบเทคโนโลยีสารสนเทศตามแผนงานที่วางไว้
- ในระหว่างการพัฒนาระบบเทคโนโลยีสารสนเทศ ผู้จัดการโครงการ (Project Manager) จะจัดประชุมเพื่อรายงานความคืบหน้าคณะทำงานบริหารโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management) ตามความเหมาะสมหรือตามแผนงานที่กำหนดไว้

17.4.3 แนวทางและขั้นตอนในการดำเนินการนำระบบขึ้นใช้งานจริง

- เมื่อผู้จัดการโครงการ (Project Manager) ได้รับรายงานการทดสอบระบบจากฝ่ายงานที่ขอให้ดำเนินการ ผู้จัดการการ (Project Manager) จะจัดทำแผนงานในการดำเนินงานนำระบบงานขึ้นใช้งานจริงรวมทั้งนำเสนอแก่คณะทำงานบริหารโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management)
- ในกรณีที่การนำระบบงานขึ้นสู่ระบบงานจริงต้องดำเนินการโดยผู้ให้บริการภายนอก ผู้ดูแลระบบจะกำหนดรหัสผู้และสิทธิให้ผู้ให้บริการภายนอกเข้ามาดำเนินการตามระยะเวลาที่กำหนดให้เท่านั้น หลังจากดำเนินการเสร็จ ผู้ดูแลระบบต้องดำเนินการดัดสิทธิการใช้งานรหัสผู้ใช้งานของผู้ให้บริการภายนอกโดยทันที
- ในระหว่างการดำเนินการนำระบบงานขึ้นใช้งานจริง ผู้จัดการโครงการ (Project Manager) จะต้องทำหน้าที่ในการประสานงาน ติดตามการทำงาน รวมถึงแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นระหว่างดำเนินการเพื่อให้ การดำเนินงานสำเร็จตามแผนงานที่วางไว้
- เมื่อระบบงานจริงสามารถใช้งานได้อย่างปกติ ผู้จัดการโครงการ (Project Manager) จะทำการตรวจสอบความเรียบร้อยในขั้นสุดท้าย และแจ้งให้คณะทำงานบริหารโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management) รับทราบ เพื่อเป็นการยืนยันความเรียบร้อยในการนำระบบงานขึ้นใช้งานจริง

อนุมัติโดย

มติที่ประชุมคณะกรรมการบริษัทครั้งที่ 1/2568 เมื่อวันที่ 26 กุมภาพันธ์ 2568 และมีผลบังคับใช้ในวันเดียวกัน

บริษัท มาร์เก็ต คอนเน็กชั่นส์ เอเชีย จำกัด (มหาชน)

.....

(ดร.กนกพร สัยยะสิทธิพานิชย์)

ประธานกรรมการบริษัท