นโยบายรักษาความมั่นคงของข้อมูล
(Information Security Policy)

เวอร์ชั่นเอกสาร : 1.0@2019
เลขที่เอกสาร :
เจ้าของเอกสาร : ฝ่ายพัฒนาเทคโนโลยีสารสนเทศ
ปรับปรุงล่าสุด : 25-Feb-2021

สารบัญ

1. นโยบายการรักษาความมั่งคงปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์ เพื่อกำหนดทิศทางและ ให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัท เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกาหนดทางธุรกิจ กฎหมายและ ระเบียบปฏิบัติที่เกี่ยวข้อง

ขอบข่าย

ข้อมูลทั้งหมด (ทั้งที่อยู่ในรูปเอกสาร และอิเล็กทรอนิกส์ไฟล์) ที่ได้รับการ จัดเก็บ ได้รับการใช้งานหรือใช้ในการสื่อสารเพื่อดำเนินกิจการขององค์กร

บุคคลทั้งหมดที่มีส่วนเกี่ยวข้องในการใช้งานข้อมูลและระบบคอมพิวเตอร์ขององค์กรได้แก่ ผู้บริหาร พนักงานประจำ พนักงานชั่วคราว หุ้นส่วน ตัวแทน ธุรกิจ บุคคลภายนอกที่ถูกว่าจ้างโดยองค์กร บริษัทคู่ค้า บริษัทหรือบุคคลที่เป็น คู่สัญญา และ ผู้ให้บริการ

ทรัพย์สินทั้งหมดที่เกี่ยวข้องกับข้อมูล และที่ใช้ในการจัดเก็บ ส่งผ่าน หรือ ประมวลผลข้อมูล ได้แก่ อุปกรณ์ เครื่องเซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ ซอฟต์แวร์ โปรแกรม เอกสารอิเล็กทรอนิกส์ เอกสารตีพิมพ์ เครื่องมือ สิ่งอำนวย ความสะดวก ตลอดจนบริการที่ได้รับ

นโยบาย

1.1 นโยบายการรักษาความมั่นคงของข้อมูล เพื่อคุ้มครองผลประโยชน์และชื่อเสียงขององค์กร พนักงานทุกคนต้อง

1.2 ปกป้องข้อมูล (ไม่ว่าจะถูกเก็บอยู่ในรูปแบบใดก็ตาม) ให้พ้นจากเหตุละเมิดต่างๆ ซึ่งอาจส่งผลกระทบต่อความลับของข้อมูล (Confidentiality) ความถูกต้องและสมบูรณ์ครบถ้วนของข้อมูล (Integrity) หรือความมีพร้อมใช้งานของข้อมูล (Availability)

1.3 ปฏิบัติตามมาตรฐาน ISO 27001 และมาตรฐานอื่นๆ ตลอดจนนโยบายด้านความมั่นคงที่องค์กรกำหนด เพื่อความมั่นคงปลอดภัยของข้อมูล

1.4 ปฏิบัติตามข้อกฎหมายอื่น ๆ ที่เกี่ยวข้องทั้งหมด โดยองค์กรมีนโยบายดังต่อไปนี้

1.4.1 ข้อมูลที่สำคัญขององค์กรต้องได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต

1.4.2 ข้อมูลที่สำคัญขององค์กรต้องได้รับการรักษาความลับอย่างเหมาะสม

1.4.3 ข้อมูลที่สำคัญขององค์กรต้องมีความถูกต้องและสมบูรณ์ครบถ้วน

1.4.4 ข้อมูลที่สำคัญขององค์กรต้องมีพร้อมใช้งานอยู่เสมอ

1.4.5 กฎหมาย กฎระเบียบและข้อบังคับที่เกี่ยวข้องต่างๆ ต้องได้รับการปฏิบัติตามอย่างถูกต้องครบถ้วน

1.4.6 พนักงานทุกคนต้องได้รับการฝึกอบรมด้านการรักษาความมั่นคงของข้อมูล

1.4.7 จัดให้มีการบริหารจัดการความเสี่ยง (Risk management)ที่เกี่ยวข้องกับความมั่นคงของข้อมูลขึ้นในองค์กร

1.4.8 จัดทำแผนการจัดการเพื่อให้ธุรกิจดำเนินได้อย่างต่อเนื่อง พร้อมทั้งทำการดูแล รักษา และทดสอบแผนอย่างเหมาะสม

1.4.9 จัดให้มีชุดเอกสารนโยบายด้านความมั่นคงของข้อมูลและ เอกสารสนับสนุนที่เกี่ยวข้อง เพื่อกำหนดระเบียบปฏิบัติ ตลอดจนแนวทางการปฏิบัติงานและ การใช้งานข้อมูลอย่างมั่นคงปลอดภัย

1.4.10 จัดให้มีกระบวนการในการรายงาน สืบสวน รับมือ และจัดการกับเหตุละเมิดความมันคงอย่างเหมาะสม โดยเหตุละเมิดความมั่นคง ตลอดจนสิ่งผิดปกติและเหตุการณ์ที่น่าสงสัยอื่นๆ ต้องมีการรายงานไปยังผู้อำนวยการ ฝ่ายเทคโนโลยีสารสนเทศ เพื่อดำเนินการตรวจสอบและแก้ไข

1.5 การปฏิบัติตามนโยบายและการตรวจสอบ

พนักงานและบุคคลที่เกี่ยวข้องทุกคนต้องลงนามในเอกสารข้อตกลงการไม่เปิดเผย ข้อมูล (Non-Disclosure Agreement) และ / หรือ เอกสารอื่นๆ ที่เกี่ยวข้อง เพื่อเป็น การยอมรับว่าข้อมูลต่างๆ ที่ได้รับทราบและ ใช้งานในระหว่างการจ้างงาน เป็น ทรัพย์สินขององค์กร และ ไม่สามารถนำไปใช้เพื่อการอื่น โดยมิได้รับอนุญาต ทั้งนี้ ในการใช้งานข้อมูลทั้งหลายในองค์กร จะถือว่าทุกคนรับทราบและยินยอมปฏิบัติตามเงื่อนไขของนโยบายนี้ทุกประการ

การเจตนาเข้าถึงระบบโดยไม่ได้รับอนุญาต การจงใจใส่ข้อมูลที่ผิดพลาดและ การเจตนาเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต ถือเป็นสิ่งต้องห้ามทั้งสิ้น การไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงของข้อมูลนี้ถือว่ามีความผิดทางวินัยและ เพื่อให้มั่นใจได้ว่ามีการปฏิบัติตามนโยบายนี้อย่างเคร่งครัด องศักรจึงจำเป็นต้องจัด ให้มีการตรวจติดตามการปฏิบัติงานของพนักงานตลอดจนบุคคลอื่นที่เกี่ยวข้องเป็น ระยะๆ ผ่านการตรวจติดตามการปฏิบัติงานภายใน (Internal audit) และการตรวจสอบ Security logs / Audit trails ที่เกี่ยวข้อง ทั้งนี้ องค์กรขอสงวนสิทธิ์ใน การกระทำการใดๆ ที่เห็นว่าจำเป็นเพื่อจัดการและป้องกันความมั่นคงปลอดภัยให้แก่ข้อมูลและ ระบบเทคโนโลยีสารสนเทศขององค์กร

1.5 การทบทวนและปรับปรุงนโยบาย

นโยบายการรักษาความมั่นคงของข้อมูลนี้ ต้องได้รับการทบทวน และประเมินผล เพื่อปรับปรุงเนื้อหา หรือยืนยันเนื้อหาเดิม โดย Steering Committee อย่างน้อยปีละหนึ่งครั้ง เพื่อให้มั่นใจได้ว่าเนื้อหาของนโยบาย ยังคงไว้ซึ่งความสมบูรณ์ มีประสิทธิภาพ และสามารถนำไปใช้งานได้อย่างเหมาะสม

1.6 บทลงโทษ

การละเมิด ฝ่าฝืน ละเลย หรือไม่ปฏิบัติตามนโยบาย ตลอดจนวิธีการปฏิบัติงาน และเอกสารสนับสนุนต่างๆ ที่เกี่ยวข้อง ไม่ว่าโดยเจตนาหรือไม่ก็ตามถือเป็นความผิดทางวินัย ซึ่งต้องถูกพิจารณาลงโทษทางวินัยโดยคณะกรรมการพิจารณาความผิดทางวินัยขององค์กร และหากการละเมิดหรือฝ่าฝืนนโยบายนั้นเข้าข่ายการกระทำที่ผิดกฎหมาย ผู้ละเมิดก็ต้องได้รับการดำเนินคดีตามที่กฎหมายระบุไว้

4.เอกสารอ้างอิง

4.1 ข้อตกลงการไม่เปิดเผยข้อมูล (Non - Disclosure Agreement)

2. โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ
(Organizational of Information Security)

วัตถุประสงค์ : เพื่อให้มีการกาหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสาหรับสารสนเทศของบริษัทฯ ตั้งแต่การเริ่มต้นและการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย

นโยบาย

2.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities) ต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ ในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัทฯ ไว้อย่างชัดเจน และ ต้องมีการแต่งตั้งผู้ทำงานหลักตลอดจนทรัพยากรที่จำเป็น เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสรสนเทศของบริษัทฯ

2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) ต้องแบ่งหน้าที่และกำหนดความรับผิดชอบที่ชัดเจนในการปฏิบัติงาน เพื่อลดโอกาสที่จะทำให้มีการเปลี่ยนแปลงทรัพย์สินของบริษัทฯ หรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์ โดยไม่ได้รับอนุญาต หรือโดยไม่ได้เจตนาก็ตาม

2.1.3 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with Authorities) ต้องมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น ๆ เช่นสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น และเอกสารกำหนดให้มีการระบุวันที่จัดทำเอกสาร

2.1.4 การบริหารจัดการโครงการเพื่อให้มีความมั่นคงปลอดภัย (Information Security in Project Management)

การดำเนินงานและการเข้าถึงข้อมูลเพื่อให้งานโครงการมีความมั่นคงปลอดภัยนั้น สิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน ผู้ใช้งานจะมีสิทธิในการเข้าถึงข้อมูลตามหน้าที่ความรับผิดชอบในสายงานของผู้ใช้งานท่านนั้น ๆ ตามประกาศโครงสร้างของบริษัท

2.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก (Mobile Devices and Teleworking)

วัตถุประสงค์ : เพื่อรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศของการปฏิบัติการระยะไกลหรือการปฏิบัติงานภายนอกและการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา

นโยบาย

2.2.1 นโยบายสาหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

การใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Notebook) เพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว อุปกรณ์คอมพิวเตอร์แบบพกพา (Notebook) จะต้องเป็นอุปกรณ์ที่จัดหาจากหน่วยงานเทคโนโลยีสารสนเทศจากทางบริษัทฯ เท่านั้น และจะต้องใช้งานโดยผ่านทาง Active Directory เท่านั้น

การพกพาคอมพิวเตอร์แบบพกพาใช้งานนอกสถานที่ ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบการใช้งานและอุปกรณ์โดยคำนึงถึงความปลอดภัยขอข้อมูลและทรัพย์สินอย่างสูงสุด โดยจะขณะใช้งานจะต้องดูแลอุปกรณ์ดังกล่าวตลอดเวลาไม่วางไว้ในสถานที่ ที่ไม่ปลอดภัยหรือมีความเสี่ยงต่อการสูญหายของข้อมูลและทรัพย์สิน เช่นห้ามวางไว้ในพื้นที่สาธารณะโดยปราศจากผู้ดูแล และ ห้ามไว้ในรถยนต์ด้านส่วนของผู้โดยสาร ห้ามเปิดเผย ชื่อและรหัสผู้ใช้งาน แก่ผู้อื่นโดยเด็จขาด

หากมีความเสียหายของข้อมูล และ อุปกรณ์ดังกล่าว โดยเกิดจากการใช้งานผิดวิธีด้วยการจงใจหรือไม่ได้เจตนาของผู้ใช้งาน ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบตามกฎหมายและกฎของบริษัท

2.2.2 การปฏิบัติงานจากระยะไกล (Teleworking)

อนุญาตให้บุคลากรของบริษัทฯ ที่จำเป็นต้องปฏิบัติงานจากภายนอกบริษัทฯ โดยปฏิบัติตามวิธีปฏิบัติงานเรื่องการควบคุมการเข้าถึง (Access Control) และวิธีปฏิบัติงานเรื่องการลงทะเบียนใช้งานระบบสารสนเทศ เพื่อให้มีการพิสูจน์ตัวตนและควบคุมการทำงานจากระยะไกลโดยการแบ่งระหว่างระบบที่เชื่อต่ออินเทอร์เน็ตกับระบบอินทราเน็ตภายในที่ใช้งานในบริษัทฯ และใช้งานเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) โดยผู้บริหารฝ่ายงานเป็นผู้พิจารณาอนุญาตให้สิทธิ กาปฏิบัติงานจากระยะไกล

3 การรักษาความปลอดภัยด้านทรัพยากรมนุษย์
(Human resource security)

3.1 การจัดหาบุคลากรก่อนการจ้างงาน (Prior to Employment)

วัตถุประสงค์ : เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ที่ได้รับพิจารณาจ้างงานจากบริษัทฯ

นโยบาย

3.1.1 การสรรหาบุคลากร (Screening)

เจ้าหน้าที่กลุ่มบริหารทรัพยากรบุคคล ต้องทาการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นผู้บริหาร เจ้าหน้าที่ชั่วคราวหรือนักศึกษาฝึกงาน โดยต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของหน่วยงานใดมาก่อน

เจ้าหน้าที่ประสานงานกลุ่มบริหารทรัพยากรบุคคล ต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่” และหน่วยงาน ว่าจะไม่เปิดเผยความลับของหน่วยงาน (Non Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างเจ้าหน้าที่นั้นๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ ทางานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

ปฏิบัติตามวิธีปฏิบัติงานเรื่อง: การบริหารจัดการทรัพยากรบุคคลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Human resources security)

3.1.2 ข้อกำหนดและเงื่อนไขของการจ้างงาน (Terms and conditions of employment)

เจ้าหน้าที่ประสานงานกลุ่มบริหารทรัพยากรบุคคล ต้องกาหนดเงื่อนไขการจ้างงานที่รวมถึง หน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ โดยเจ้าหน้าที่กลุ่มบริหาร ทรัพยากรบุคคล ต้องแจ้งให้ผู้บริหารสายงานทราบทันทีเมื่อมีเหตุดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร เจ้าหน้าที่และลูกจ้าง หรือการถึงแก่กรรม - การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

3.2 การสร้างความมั่นคงปลอดภัยขณะเป็นเจ้าหน้าที่ (During Employment)

วัตถุประสงค์ : เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

นโยบาย

3.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management Responsibilities)

ผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Representative) ต้องกำหนดให้เจ้าหน้าที่ของบริษัทฯ และ เจ้าหน้าที่หน่วยงานภายนอกที่ว่าจ้างมา ปฏิบัติงานรับทราบและ ปฏิบัติตามนโยบาย กฎ ระเบียบและขั้นตอนทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ด้วย

3.2.2 การสร้างความตระหนัก การให้ความรู้และการอบรมให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

เจ้าหน้าที่บริษัทฯ ผู้รับจ้างขององค์กรทุกคนต้องได้รับการอบรมให้ความรู้ โดยเนื้อหาที่แต่ละ บุคคลจะได้รับการฝึกอบรมต้องเหมาะสมกับบทบาทหน้าที่ในการปฏิบัติงานของแต่ละบุคคล เพื่อเป็นการ สร้างความตระหนัก และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

ต้องจัดอบรมให้ความรู้แก่เจ้าหน้าที่บริษัทฯ เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้าง ความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับ นโยบายความมั่นคงปลอดภัย และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของบริษัทฯ ด้วย

เจ้าหน้าที่บริษัทฯ ใหม่ทุกคน ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคง ปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือได้รับเอกสารนโยบายการรักษาความมั่นคง ปลอดภัยสารสนเทศฯและ ระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานภายใน30 วันนับจากเข้าทำงานในหน่วยงาน เพื่อให้พนักงาน หรือผู้ที่เกี่ยวข้องได้ศึกษาและถือปฏิบัติ โดยอาจเป็น ส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย

เจ้าหน้าที่ประสานงานกลุ่มบริหารทรัพยากรบุคคล และ คณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่ในการแจ้งให้ทราบ เกี่ยวกับนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้าน ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทฯ ให้แก่บุคลากรด้วย

3.2.3 กระบวนการทางวินัย (Disciplinary Process)

ผู้บริหารต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือ ระเบียบปฏิบัติของบริษัทฯ แต่หากเป็นการละเมินข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุในแต่ละข้อกฎหมายนั้น ๆ

3.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์ : เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของการเปลี่ยนหน้าที่ หรือสิ้นสุดการแจ้งงาน

นโยบาย

3.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

มีการกาหนดและสื่อสารให้พนักงานหรือผู้ทำสัญญาได้รับทราบ รวมทั้งมีการควบคุมให้ ปฏิบัติตามข้อกำหนดในสัญญา

เจ้าหน้าที่กลุ่มบริหารทรัพยากรบุคคลมีหน้าที่ดูแลหากมีการแต่งตั้งโยกย้าย ปลดหรือ เปลี่ยนแปลงตำแหน่งใด ๆ ที่เกี่ยวข้องกับความรับผิดชอบในบริษัทฯ

เจ้าหน้าที่ผู้เกี่ยวข้องเมื่อได้รับเรื่องของผู้ใช้งานที่สิ้นสุดสภาพการจ้างงานหรือเปลี่ยนหน้าที่ความรับผิดชอบจากฝ่ายบุคคล ให้ปฏิบัติตามคู่มือการปฏิบัติงานเรื่องการลงทะเบียนใช้งานระบบสารสนเทศ เพื่อดำเนินการเพิกถอนสิทธิ์หรือเปลี่ยนแปลงสิทธิ์

4 การบริหารจัดการสินทรัพย์

(Asset Management)

4.1 การความรับผิดชอบต่อสินทรัพย์ (Responsibility of Assets)

วัตถุประสงค์ : เพื่อให้สินทรัพย์ของบริษัทฯ ได้รับการป้องกันและ ปกป้องอย่างเหมาะสม

นโยบาย

4.1.1 ทะเบียนสินทรัพย์ (Inventory of assets)

บริหารจัดการสินทรัพย์ ต้องจัดทาและเก็บทะเบียนสินทรัพย์ซึ่งรวมถึงสินทรัพย์ข้อมูล และเอกสาร (Information and Document Asset) สินทรัพย์ซอฟต์แวร์ (Software Asset) สินทรัพย์ อุปกรณ์ (Hardware Asset) สินทรัพย์งานบริการ (Service Asset) และบุคลากร (People Asset) เพื่อ เป็นข้อมูลเบื้องต้นสาหรับการนาไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อ สินทรัพย์อย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการสินทรัพย์ของสานักงานฯ โดยปฏิบัติตาม

ต้องมีการตรวจสอบสินทรัพย์ (Inventory Check) จัดให้มีการ ตรวจสอบบัญชีสินทรัพย์ทุกประเภทตามระยะเวลาที่กาหนดไว้ เช่น ปีละ 1 ครั้ง หรือภายใน 1 เดือน เมื่อมี การเปลี่ยนแปลงที่สาคัญเกิดขึ้น เป็นต้น

ประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของ สินทรัพย์ เมื่อมีสินทรัพย์ใหม่ หรือสินทรัพย์ที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

4.1.2 ความเป็นเจ้าของสินทรัพย์ (Ownership for Assets)

กำหนดบุคคลหรือหน่วยงานผู้รับผิดชอบข้อมูลและสินทรัพย์ ทั้งหมดด้านเทคโนโลยีสารสนเทศและการสื่อสารของสานักงานฯ อย่างชัดเจน

4.1.3 การอนุญาตให้ใช้สินทรัพย์ (Acceptable Use for Assets)

การอนุญาตให้ใช้งานสินทรัพย์ด้านอุปกรณ์คอมพิวเตอร์มีดังนี้

ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมด ที่บริษัทฯ เป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของบริษัทฯ การใช้งานระบบและ อุปกรณ์ต่างๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่

เจ้าหน้าที่ ตลอดจนหน่วยงานภายนอก ที่ได้รับการว่าจ้างโดยบริษัทฯ จะต้องมีความ รับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้

มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศของบริษัทฯ

ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของบริษัทฯ อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นสินทรัพย์ของตน

เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์พกพาทั้งหมดของบริษัทฯ ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุก ครั้งเมื่อไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง

ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์ส่วนตัวของตนเข้าระบบเครือข่ายของบริษัทฯ รวมถึงต้องไม่ติดตั้งซอฟต์แวร์ใด ๆ ลงในเครื่องคอมพิวเตอร์ของบริษัทฯ ก่อนได้รับอนุญาตจากผู้บริหารฝ่าย และผู้บริหารความมั่นคงปลอดภัยสารสนเทศ

เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายในบริษัทฯ อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกัน สปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอฯลฯ ทั้งนี้ผู้ใช้งานต้องทาการปกป้อง อุปกรณ์และข้อมูลในอุปกรณ์ตามคาแนะนำที่ระบุไว้ใน เอกสารขั้นตอนการปฏิบัติงาน เรื่องการใช้ เครื่องคอมพิวเตอร์ประเภทพกพาในการปฏิบัติงานนอกสถานที่ (Mobile Computing and Communications)

อุปกรณ์คอมพิวเตอร์ของบริษัทฯ ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และ ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการ ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ของบริษัทฯ อย่างเด็ดขาด

การอนุญาตให้ใช้งานสินทรัพย์ด้านซอฟต์แวร์มีดังนี้

ห้ามเจ้าหน้าที่ ทาการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของบริษัทฯ

ซอฟต์แวร์ที่นามาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของบริษัทฯ ทั้งที่ ได้มาจากการพัฒนาขึ้นโดยเจ้าหน้าที่ หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และ อนุมัติอย่างเหมาะสมโดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบ เทคโนโลยีสารสนเทศของบริษัทฯ

ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของสานักงานฯ มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้

รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของ บริษัทฯ เท่านั้น

การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้

บริษัทฯ จัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดาเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการดำเนินงาน และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่ม ประสิทธิภาพในการทำงานและการให้บริการของบริษัทฯ

ผู้ใช้งาน ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้ บริษัทฯ และบุคคลผู้ที่เกี่ยวข้องกับบริษัทฯ เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทาที่ ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดาเนินคดี ตามกฎหมาย

การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้บริษัทฯ ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใดๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของ ผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย

บริษัทฯ ไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บ บอร์ด หรือบล็อก) ของเจ้าหน้าที่ ทั้งนี้ความเสียหายใดๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็น ดังกล่าว ถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้นั้น

การอนุญาตให้ใช้งานอีเมล์มีดังนี้

ผู้ใช้งานอีเมล์ทั้งหมดของบริษัทฯ ต้องมี E-mail Account เป็นของตนเอง

E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมล์ไปใช้ในทางที่ผิด

E-mail Account ที่มีวัตถุประสงค์พิเศษ เช่น hr@tsi.co.th อาจได้รับการสร้างขึ้นเพื่อเป็น E-mail Account กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทาหน้าที่เป็นเจ้าของ E-mail Account นั้น

E-mail Account ทั้งหมด และอีเมล์ทุกฉบับ (รวมถึงอีเมล์ส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัทฯ ถือเป็นสินทรัพย์ของบริษัทฯ

ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบอีเมล์ของบริษัทฯ

พื้นที่เก็บอีเมล์บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้ เมื่อปริมาณของอีเมล์มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ และถ้าหากปริมาณของอีเมล์มากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับ-

ส่งอีเมล์ได้ตามปกติอีกต่อไป

ขนาดของอีเมล์และไฟล์แนบได้รับการจากัดไว้ โดยหากอีเมล์และไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายตีกลับแจ้งว่าไม่สามารถส่งอีเมล์ดังกล่าวได้

ผู้ใช้งานต้องลบอีเมล์ที่ไม่จาเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมล์ให้เป็นไปตามขนาดที่บริษัทฯ กำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมล์ที่เกี่ยวข้องกับการทำงานและอีเมล์ตามที่กฎหมายกาหนดไว้เท่านั้น

ห้ามใช้ E-mail Account ของสานักงานฯ เพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น

ห้ามใช้ E-mail Account ของบริษัทฯ ในการประกาศข้อมูลใด ๆ ในชุมชนอิเล็กทรอนิกส์ เช่น เว็บบอร์ด บล็อก กระดานข่าว เป็นต้น เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทางานให้กับบริษัทฯ

ซอฟต์แวร์สาหรับใช้งานอีเมล์ต้องได้รับการตั้งค่าให้อีเมล์ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-สกุล ตำแหน่ง ชื่อหน่วยงาน บริษัทฯ และเบอร์โทรศัพท์ติดต่อ

ห้ามผู้ใช้งานทำสำเนาข้อความ หรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมล์ของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล

ผู้ใช้งานต้องร่างเนื้อหาของอีเมล์ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมล์นั้นในนามตัวแทนของบริษัทฯ

ห้ามผู้ใช้งานทาการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นในอีเมล์ หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด

ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ E-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม

ผู้ใช้งานต้องหลีกเลี่ยงการใช้คาสั่ง “Reply with History” ซึ่งเป็นการตอบกลับอีเมล์พร้อมไฟล์แนบไปยังผู้รับ ยกเว้นในกรณีที่จำเป็นต้องใช้งานเท่านั้น อย่างไรก็ตาม เมื่อมีการใช้งานคาสั่ง “Reply with History” ผู้ใช้งานควรทำการลบไฟล์แนบทิ้งเสียก่อนที่จะทำการส่งอีเมล์

ผู้ใช้งานต้องทำการส่งอีเมล์ให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้นและห้ามใช้คำสั่ง “Reply All” ถ้าหากอีเมล์ฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน -ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการตัวอย่างเช่นอีเมล์ขยะ(Junk Mail) หรือโฆษณาสินค้า ต่าง ๆ (Spam Mail) เป็นต้น

ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่ง อีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด

ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มี เนื้อหาสุ่ม

เสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

ห้ามผู้ใช้งานส่งอีเมล์ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อบริษัทฯ

ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมล์บอมบ์ หรือโปรแกรมแฝง (ม้าโทรจัน)

เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งอีเมล์โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่ สภาพปกติ

การอนุญาตให้ใช้งานโทรศัพท์โทรสารเครื่องพิมพ์และเครื่องถ่ายเอกสารมีดังนี้

ผู้ใช้งานต้องปกป้องความมั่นคงปลอดภัยของข้อมูลลับอย่างเต็มที่ เมื่อจำเป็นต้องส่งข้อมูลนั้นผ่านเครื่องโทรสาร ทั้งนี้ รายละเอียดเพิ่มเติมดูได้จาก ระเบียบว่าด้วยการรักษาความลับของบริษัท

ถ้าหากผู้ใช้งานได้รับข้อมูลจากการส่งโทรสารที่ผิดพลาด ตัวอย่างเช่น ส่งโทรสารผิด หมายเลข ผิดส่วนงานเป็นต้น ผู้ใช้งานต้องแจ้งให้ผู้ส่งโทรสารนั้นรับทราบ และทำลายเอกสารข้อมูลนั้น

ห้ามผู้ใช้งานสั่งพิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในพื้นที่ส่วนกลาง เว้นแต่จะมีบุคคลที่ได้รับอนุญาตรอรับเอกสารที่ออกมาจากเครื่องพิมพ์นั้น

ห้ามผู้ใช้งานบันทึกหรือฝากข้อความที่มีข้อมูลลับในเครื่องตอบรับโทรศัพท์อัตโนมัติหรือ ระบบวอยซ์เมล์โดยเด็ดขาด

ห้ามสนทนาเกี่ยวกับข้อมูลลับผ่านลาโพงของเครื่องโทรศัพท์ (Speakerphones) หรือผ่านสื่ออิเล็กทรอนิกส์ใด ๆ เช่นVoice Over IP หรือในระหว่างการประชุมทางไกลเว้นแต่ผู้เข้าร่วมการ ประชุมทุกหน่วยงานได้รับการพิสูจน์ตัวตนแล้วว่า เป็นผู้ที่เกี่ยวข้องและมีสิทธิ์รับทราบข้อมูล

ผู้ที่เกี่ยวข้องตรวจสอบจนมั่นใจแล้วว่า ไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณใกล้เคียงที่อาจได้ยิน ข้อมูลลับที่สนทนาอยู่

การประชุมทางไกลถูกจัดขึ้นในบริเวณที่มีความมั่นคงปลอดภัย เช่น ห้องประชุมที่มีผนังและประตูที่เหมาะสมสามารถปูองกันเสียงลอดออกมาได้ เป็นต้น

ผู้ใช้งานต้องสนทนาโทรศัพท์ด้วยความระมัดระวัง เพื่อป้องกันข้อมูลลับถูกแอบฟังโดยบุคคลที่ไม่ได้รับอนุญาต

ในกรณีที่ต้องมีการเปิดเผยข้อมูลลับใด ๆ ทางโทรศัพท์ ผู้ให้ข้อมูลต้องทำการตรวจสอบให้มั่นใจว่าคู่สนทนานั้น เป็นผู้ได้รับอนุญาตให้รับทราบข้อมูลดังกล่าว ก่อนที่จะเปิดเผยข้อมูล

ผู้ใช้งานต้องขออนุญาตจากเจ้าของข้อมูลก่อนทำการถ่ายเอกสารหรือสแกนเอกสารที่มีข้อมูลลับ โดย สำเนาเอกสารนั้นต้องได้รับการปกป้องดูแลในระดับเทียบเท่ากับเอกสารต้นฉบับตามระเบียบว่าด้วย การรักษาความลับของบริษัท

เจ้าหน้าที่ต้องไม่เปิดเผยสถานที่ตั้งของห้องเครื่องคอมพิวเตอร์แม่ข่ายต่อบุคคลภายนอกโดยเด็ดขาด เว้นแต่บุคคลภายนอกนั้นมีความจำเป็นต้องรับทราบเพื่อการปฏิบัติงาน

กรณีที่เจ้าหน้าที่ ไม่ปฏิบัติตามที่บริษัทฯ กำหนดให้ดำเนินการตามระเบียบบริษัท

การคืนสินทรัพย์ (Return on Assets)

เจ้าหน้าที่ ซึ่งพ้นสภาพจากการจ้างงานต้องคืนสินทรัพย์ทั้งหมดซึ่งเกี่ยวข้องกับ ระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้า-ออก คอมพิวเตอร์และ อุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน โดยปฏิบัติ ตามวิธีปฏิบัติงานเรื่องการส่งคืนทรัพย์สิน (Return of assets)

4.2 การจัดหมวดหมู่ข้อมูลและสินทรัพย์สารสนเทศ (InformationClassification)

วัตถุประสงค์ : เพื่อทาให้แน่ใจว่าสารสนเทศของบริษัทฯ ได้รับการปกปูองในระดับที่เหมาะสม

นโยบาย

4.2.1 การกำหนดชั้นความลับของสารสนเทศ (Classification of Information)

สารสนเทศต้องมีการจัดชั้นความลับโดยพิจารณาจากความต้องการด้านกฎหมายคุณค่าระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

เจ้าหน้าที่ต้องทาการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดยให้ปฏิบัติระเบียบว่าด้วยการรักษาความลับของบริษัท

เอกสารหรือสิ่งตีพิมพ์ที่พิมพ์หรือทาซ้ำขึ้นมาจากต้นฉบับซึ่งมีการกาหนดชั้นความลับไว้ทั้งใน กรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับต้นฉบับข้อมูลดิจิตอลหรือสารสนเทศดิจิตอล

4.2.2 การจัดทาป้ายชื่อ ของข้อมูล (Labeling of Information)

ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลและอุปกรณ์สินทรัพย์สารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัย อย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทาป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการ ทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุม และรักษาความปลอดภัย

4.2.3 การจัดการสินทรัพย์ (Handling of Asset)

ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น

ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้อง โดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม

ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทางาน

ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่นเครื่องพิมพ์เครื่องโทรสารเครื่องถ่ายเอกสาร ฯลฯ โดยทันที

เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอกยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

เจ้าหน้าที่ต้องไม่พูดคุยหรือใช้งานข้อมูลลับของบริษัทฯ ในพื้นที่สาธารณะเช่น ลิฟท์ ร้านอาหาร ฯลฯ สื่อบันทึกข้อมูลและ อุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น, โทรศัพท์มือถือ,PDA,USB-Drive,CD-Romเป็นต้น)ที่ มีข้อมูลลับของบริษัทฯ บันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

4.3 การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media Handing)

วัตถุประสงค์ : เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของบริษัทฯ โดยการถูกเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทาลายข้อมูล

นโยบาย

4.3.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)

การบริหารจัดการสาหรับสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ต้องมีการจัดทาขั้นตอนสาหรับบริหารจัดการสื่อบันทึกข้อมูล โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกาหนดไว้ สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างนี้ที่นาส่งหรือขนย้ายสื่อบันทึก ข้อมูลนั้น ต้องกำหนดวิธีปฏิบัติและสิทธิ์สำหรับการใช้งานสื่อบันทึกข้อมูลโดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการลงทะเบียนสื่อเคลื่อนที่ และสอบทานการใช้งาน

4.3.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

บริษัทฯ จัดทำระเบียบวิธีปฏิบัติงานสาหรับการทำลายสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็น ลายลักษณ์อักษรโดยปฏิบัติตามวิธีปฏิบัติงานเรื่องการทำลายสื่อบันทึกข้อมูลและข้อมูลบนสื่อบันทึก ข้อมูล (Disposal of media procedure)

การทาลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูล จะต้องได้รับการอนุมัติจากเจ้าของข้อมูล รวมทั้งบันทึกรายละเอียดอย่างเหมาะสม

ควรทำลายสื่อที่ใช้ในการบันทึกข้อมูลเอกสารและอุปกรณ์สานักงานภายใต้สิ่งแวดล้อมที่ได้มี การควบคุม (Controlled Environment)

4.3.3 การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

ต้องมีวิธีการจัดส่งสื่อบันทึกข้อมูล(สารสนเทศหรือซอฟต์แวร์)ให้มีความมั่นคงปลอดภัยโดย ปฏิบัติตามวิธีปฏิบัติงานเรื่องการส่งผ่านสื่อบันทึกข้อมูล (Physical Media In Transit)

5. ความการควบคุมการเข้าถึง
(Access Control)

5.1 การควบคุมการเข้าถึงระบบสารสนเทศ(BusinessRequirementforAccessControl)

วัตถุประสงค์ : เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย

นโยบาย

5.1.1 นโยบายควบคุมการเข้าถึง (Access Control Policy)

มีการกาหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึง ให้ เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น โดยปฏิบัติตามวิธีปฏิบัติงานเรื่องการควบคุมการเข้าถึง (Access Control) และ เจ้าหน้าที่จะต้องลงทะเบียนใช้งานระบบสารสนเทศ โดยขออนุมัติผ่านทางระบบ TSI Service Request โดยมีการพิจรณาอนุมัติจาก ผู้บริหารฝ่าย และ ผู้บริหารเทคโนโลยีสารสนเทศ

ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวน สิทธิ์การเข้าถึงอย่างน้อยปีละ 1 ครั้ง (Review of User Access Rights Procedure)ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาต จากผู้บังคับบัญชาตามความจำเป็นในการใช้งาน

ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้

ต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ฯ และเฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

ต้องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของทั้งผู้ที่ได้รับ อนุญาต และไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

ต้องกำหนดกฎเกณฑ์ข้อห้ามและบทลงโทษการเข้าถึงข้อมูลและระบบสารสนเทศ

การเข้าถึงข้อมูล และระบบสารสนเทศของบริษัทฯ จะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดยผู้บังคับบัญชาของบุคคลนั้น ๆ และสามารถเข้าใช้ข้อมูล และระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น ๆ เท่านั้น ความปลอดภัยของข้อมูล และกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วน หนึ่งในการกำหนดนโยบาย และขั้นตอนการทำงานของระบบสารสนเทศ กระบวนการเหล่านี้หมาย รวมถึงการให้สิทธิ์ และการบริหารจัดการรหัสในการเข้าใช้งาน การกำหนดขอบเขตในการเข้าถึงข้อมูล หรือระบบคอมพิวเตอร์ และอุปกรณ์ที่เก็บข้อมูลประเภทอื่น ๆ การสำรองข้อมูลและการกู้ข้อมูลที่ เสียหายกลับคืนมา

5.1.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services)

ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึง เท่านั้น

ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะ เพื่อรักษาความมั่นคง ปลอดภัยให้แก่ข้อมูลและระบบเทคโนโลยีสารสนเทศ อาทิ

ใช้งานโปรโตคอลที่มั่นคงปลอดภัยในการบริหารจัดการระบบเครือข่าย อาทิ Secure Socket Layer (SSL) Simple Network Management Protocol (SNMP)

จากัดการใช้งานเครือข่ายที่ส่งผลกระทบต่อ Bandwidth เช่น การรับ-ส่งไฟล์ขนาดใหญ่ ฟังเพลงออนไลน์ ดูทีวีออนไลน์ หรือ เล่นเกมส์ออนไลน์ ในช่วงเวลาทาการ ยกเว้นกรณีที่ได้รับอนุญาต

ผู้ใช้งานจะต้องสามารถเข้าถึงระบบเครือข่ายและระบบสารสนเทศได้ แต่เพียงบริการที่ได้รับ อนุญาตให้เข้าถึงเท่านั้น

ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสม เพื่อรักษาความมั่นคงปลอดภัย ให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ

อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายทั้งหมดต้องได้รับการตั้งค่าให้มีความปลอดภัยและการมีการตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับระบบเครือข่าย

ระบบสายสัญญาณต้องได้รับมาตรฐานอุตสาหกรรมและได้รับการติดตั้งโดยผู้ที่มีความชำนาญที่ผ่านการพิจารณาอนุมัติแล้ว

อุปกรณ์เครือข่าย อาทิ Router, Firewall, Switch, Wireless Access Point ต้องได้รับการตั้งค่าตามความจำเป็นด้านความมั่นคงปลอดภัยของอุปกรณ์นั้น ๆ หรือตามคำแนะนาของบริษัทฯ ด้านความมั่นคงปลอดภัยต่าง ๆ อาทิ SANS Institute หรือ NSA

อุปกรณ์เครือข่ายที่สำคัญ เช่น Router, Core Switch ต้องมีอุปกรณ์สารองไฟฟ้า (UPS) เสมอ

การเปลี่ยนแปลงระบบเครือข่ายหรืออุปกรณ์เครือข่ายต้องได้รับการควบคุมโดยปฏิบัติตาม เอกสารวิธีการปฏิบัติงานเรื่องการจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management)

ระบบเครือข่ายต้องได้รับการออกแบบหรือตั้งค่าให้ทำงานได้อย่างมีประสิทธิภาพ (Reliable) มีความยืดหยุ่น (Flexible) รวมถึงสามารถรองรับการขยายตัวและความต้องการใช้งานในอนาคต (Scalable)

ข้อตกลงการให้บริการเครือข่ายต้องระบุถึงรายละเอียด และข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ และการบริหารจัดการบริการเครือข่ายทั้งหมด หากบริการเครือข่าย นั้นได้รับการดำเนินการโดยหน่วยงานภายนอก ต้องมีการระบุถึงสิทธิของบริษัทฯ ในการติดตามตรวจสอบ และตรวจประเมินการทำงานของหน่วยงานภายนอกด้วย

5.2 การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

วัตถุประสงค์: เพื่อปูองกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

นโยบาย

5.2.1 การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration)

การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการ ลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจาเป็น รวมทั้งระเบียบปฏิบัติสำหรับ การยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในสานักงานฯ เป็นต้น โดย ปฏิบัติตามวิธีปฏิบัติงานเรื่องการควบคุมการเข้าถึง (Access Control) และวิธีปฏิบัติงาน เรื่องการลงทะเบียนใช้งานระบบสารสนเทศ โดยผู้ใช้งานต้องได้รับการทบทวนและ พิจารณาอนุมัติตามขั้นตอนของสานักงานฯ อย่างเคร่งครัด

5.2.2 การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning)

ผู้ใช้งานมีสิทธิ์การเข้าถึงข้อมูลตามหน้าที่ความรับผิดชอบในส่วนงานนั้น ๆ โดยการเข้าถึงข้อมูลจะต้องได้รับการอนุมัติจากผู้บริหารสายงาน และ ฝ่ายบุคคลเป็นผู้แจ้งดำเนินการกำหนดสิทธิ์การเข้าถึงข้อมูลในกรณีพนักงานเข้างานใหม่ ย้ายสายงาน หรือ พ้นสถาพการเป็นพนักงาน กรณีเป็นการขอสิทธิ์เข้าถึงข้อมูลข้ามสายงาน จะต้องได้รับการอนุมัติจากผู้บริหารของหน่วยงานเจ้าของข้อมูลเพิ่มเติม

5.2.3 การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง ทบทวนสิทธิ์โดยหัวหน้างานหรือ ผู้บริหารสายงาน

5.2.4 การถอนหรือการจัดการสิทธิ์การเข้าถึง (Removal or Adjustment of Access Rights)

สิทธิ์การเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง และต้องได้รับการปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ

ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน(Userresponsibilies)

วัตถุประสงค์: เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลที่ใช้ในการพิสูจน์ตัวตน

นโยบาย

5.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

- พนักงานต้องเก็บรักษา Username และ Password ต้องเป็นความลับห้ามเปิดเผยให้บุคคลอื่นทราบ
- พนักงานต้องหลีกเลี่ยงการเก็บบันทึกข้อมูลการตรวจสอบความลับ เว้นแต่สามารถเก็บไว้อย่างปลอดภัย
- เมื่อพนักงานได้รับข้อมูล Password ซึ่งเป็นข้อมูล Default ควรมีการแก้ไขทันทีเมื่อเข้าใช้งานระบบครั้งแรก

5.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

วัตถุประสงค์: เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

นโยบาย

5.4.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จาเป็นต้องใช้งาน

บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจาเป็นและมีการกาหนดระยะเวลาในการเข้าถึง อย่างเหมาะสมกับการทางานเท่านั้น

บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ของบริษัทฯ อย่างเคร่งครัด ก่อนที่จะ ได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ

5.4.2 ขั้นตอนปฏิบัติสาหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure)
กำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย กำหนดให้ระบบปฏิเสธ การให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน 5 ครั้ง

5.4.3ระบบบริหารจัดการรหัสผ่าน (Password Management System)

กำหนดให้ระบบตรวจสอบคุณภาพของรหัสผ่านและ มีวิธีการควบคุมดูแลให้ ผู้ใช้งานระบบเปลี่ยนรหัสผ่านทุก 90 วัน

5.4.4 การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบต้องมีการขออนุมัติจากหัวหน้าสายงาน และ ต้องได้รับการตรวจสอบ จากฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้ รับอนุญาต ได้แก่

- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน

- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ผู้ใช้งานระบบ เป็นต้น

5.4.5 การควบคุมการเข้าถึงซอร์สโค้ดสาหรับระบบ (Access Control to Program Source Code)

ผู้พัฒนาระบบสารสนเทศควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริง หรือให้บริการ โดย

- ไม่เก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย

- ไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริง

แล้ว

6 การเข้ารหัสข้อมูล (Cryptography)

6.1 การกำหนดการควบคุมการเข้ารหัสข้อมูล (Cryptographic controls)

วัตถุประสงค์: เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผลและเพื่อป้องการความลับการปลอมแปลงหรือความถูกต้องของสารสนเทศ

นโยบาย

6.1.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)
การควบคุมการเข้ารหัสข้อมูลตามข้อตกลง โดยอยู่ภายใต้กฎหมาย และระเบียบที่ เกี่ยวข้อง

6.1.2 การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management)
นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจต้องมีการจัดทำและปฏิบัติตามตลอด วงจรชีวิตของกุญแจ โดยกำหนดให้มีการเปลี่ยนทุกครั้งที่มีการร้องขอ

6.1.3 การเก็บข้อมูลหรือไฟล์อิเล็กทรอนิกส์บนสื่อบันทึกข้อมูลอิเล็กทรอนิกส์มีระดับชั้นความลับ ได้แก่ ลับที่สุด ลับมาก และ ลับ ให้ใช้มาตรฐาน Advance Encryption Standard AES256 ในการเข้ารหัสข้อมูลอิเล็กทรอนิกส์

7 ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and Environmental Security)

7.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย(SecureAreas)

วัตถุประสงค์: เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและ พื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นสินทรัพย์ สานักงานฯ

เพื่อป้องกันการสูญหาย ความเสียหาย การขโมย หรือภาวะเป็นอันตรายต่อทรัพย์สินสารสนเทศและป้องกันการหยุดชะงักต่อการดำเนินงานของบริษัท

นโยบาย

7.1.1 การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)

จำแนก และกำหนดพื้นที่ในการใช้งานระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม และรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับ อนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ เมื่อมีการกำหนดพื้นที่แล้วให้มีการควบคุม การเข้าออก

จำแนก กำหนด และแบ่งบริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspaces)” รวมทั้งจัดทำแผนผังแสดงตำแหน่ง และชนิดของพื้นที่ใช้งาน ระบบเทคโนโลยีสารสนเทศ และประกาศให้ทราบทั่วกัน (หน่วยงานควรระบุให้ชัดเจนว่ามีพื้นที่ใช้งาน ระบบเทคโนโลยีสารสนเทศประเภทใดบ้าง และมีพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศใดที่อาจจำแนก ได้มากกว่า 1 ประเภท)

การติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศใน “พื้นที่ใช้งานระบบ เทคโนโลยีสารสนเทศ” จะต้องสอดคล้องกับหมวดหมู่และ ความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

เจ้าหน้าที่บริษัทฯ ต้องดูแลรักษาสภาพแวดล้อมในการทำงานเสมือนดูแลบ้านของตน

7.1.2 การควบคุมการเข้าออก (Physical Entry Controls)

การควบคุมการเข้าออกใน บริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” โดยให้ผ่านเข้าออกได้เฉพาะ “เจ้าหน้าที่ที่มี สิทธิ์เท่านั้น และมีแนวทางปฏิบัติ ดังนี้

1) ต้องกำหนดเจ้าหน้าที่ ที่มีสิทธิ์ผ่านเข้าออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกใน แต่ละ“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” อย่างชัดเจน

2) เจ้าหน้าที่ จะได้รับสิทธิ์ให้เข้าออกสถานที่ทางานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ ในการทำงานเท่านั้น

3) หากมีบุคคลอื่นใดที่ไม่ใช่เจ้าหน้าที่ที่ได้รับอนุญาติ ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็น การล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่ เป็นการชั่วคราว ต้องมีการบันทึกข้อมูลการเข้าออกห้องคอมพิวเตอร์แม่ข่าย (Data Center) ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี

4) บุคคลภายนอกต้องทำการแลกบัตรประจำตัวของตนที่ออกให้โดยหน่วยงานของรัฐ ตัวอย่างเช่น บัตรประชาชน ใบขับขี่ พาสปอร์ต ฯลฯ กับบัตรผู้มาติดต่อของหน่วยงาน ก่อนได้รับอนุญาตให้เข้าถึงพื้นที่สำนักงาน

5) บุคคลภายนอกต้องติดบัตรผู้มาติดต่อตลอดเวลาที่ อยู่ในพื้นที่บริษัท ทั้งนี้ บัตรประจำตัวและบัตรผู้มาติดต่อ ไม่อนุญาตให้โอนกรรมสิทธิ์หรือหยิบยืมกัน ใช้งาน
6) เจ้าหน้าที่บริษัทฯ ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายใน พื้นที่สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้ เพื่อ เป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับ อนุญาต
7) ผู้ใช้งานต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยทันที เมื่อพบเห็นบุคคลแปลกหน้าหรือบุคคลที่ไม่ แขวนบัตรผู้มาติดต่อในพื้นที่สานักงาน
8) เจ้าหน้าที่บริษัทฯ ควรติดตาม ควบคุมดูแล และให้คำแนะนาผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่สำนักงาน

7.1.3 การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูง ห้ามตั้งอยู่ในบริเวณที่มีการผ่านเข้า ออกของบุคคลเป็นจำนวนมาก ไม่มีป้าย หรือ สัญลักษณ์ ที่บ่งบอกถึงการมีระบบ สำคัญอยู่ภายในสถานที่ดังกล่าว ประตู หน้าต่างของสานักงาน หรือห้องต้องใส่กุญแจเสมอ เมื่อไม่มีคนอยู่ ต้องตั้งเครื่องโทรสารหรือเครื่องถ่ายเอกสารแยกออก มาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น
2) เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อค อย่างเหมาะสม และกุญแจถูก เก็บรักษาไว้อย่างปลอดภัย
3) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้อง ประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด
4) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม วิธีการทำลายข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์เหล่านี้โดยปฏิบัติตามเอกสารวิธีปฏิบัติงาน เรื่องการทำลายสื่อบันทึกข้อมูลและข้อมูลบนสื่อบันทึกข้อมูล (Disposal of Media Procedure)
5) เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทาการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจาก พื้นที่ทางานของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดาเนินการ และเป็นการ ดาเนินการที่มีคาสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

7.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อมอื่น ๆ (Protecting against External and Environmental Threats)

เพื่อประโยชน์ในการรักษาความปลอดภัยสถานที่ติดตั้งและเก็บรักษาทรัพย์สินสารสนเทศต้องจัดให้มีการป้องกันต่อภัยคุกคามต่าง ๆ ได้แก่ อัคคีภัย ความไม่สงบของบ้านเมือง หรือหายนะอื่น ๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ พร้อมทั้งให้ทดสอบระบบรักษาความปลอดภัยภายในอย่างน้องปีละ 1 ครั้ง

7.1.5 การปฏิบัติงานในพื้นที่มั่นคงปลอดภัย (Working in Secure Areas)

หัวหน้าของแต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวีดีโอในบริเวณนั้น เป็นต้น
หน่วยงานต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวีดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

7.1.6 การกำหนดพื้นที่สำหรับบุคคลภายนอกใช้รับส่งสิ่งสิ่งของ (Delivery and Loading Areas)

หน่วยงานต้องมีการจากัดพื้นที่การเข้าถึงของบุคคลภายนอกที่อาจเข้ามาในพื้นที่ได้ หากเป็นไปได้ควรแบ่งแยกพื้นที่ที่เกี่ยวข้องกับการทางานออกจากพื้นที่ที่บุคคลภายนอกเข้ามาได้ เช่น บริเวณเก็บและจัดส่งสินค้าจะต้องไม่อยู่ในพื้นที่ ที่บุคคลภายนอกเข้าถึงได้

เจ้าหน้าที่และเจ้าหน้าที่ของหน่วยงานภายนอก (Third Party) ต้องติดบัตรประจาตัวตลอดเวลา ขณะปฏิบัติหน้าที่ในบริเวณสำนักงาน และหากผู้ใดพบเห็นผู้ที่ไม่ติดบัตรประจาตัวถือเป็นหน้าที่ที่จะต้องแจ้ง เจ้าหน้าที่รักษาความปลอดภัยโดยทันที

7.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment)

วัตถุประสงค์: เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ

นโยบาย

7.2.1 การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Seting and Protection)

1) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อให้เกิดความเป็นระเบียบเรียบร้อย และไม่เกิดความเสี่ยงจากความร้อน แสงแดด ฝุ่นละออกและความชื้น
2) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัย
3) ดำเนินการตรวจสอบ สอดส่ง และดุแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบสารสนเทศอยู่ภายใน เพื่อห้องกันความเสียหายต่ออุปกรณ์ ตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติ
4) ไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของบริษัทโดยมิได้รับอนุญาติ

7.2.2 การดูแลอุปกรณ์ต่าง ๆ (Supporting Utilities)

1) มีระบบสนับสนุนการทำงานของระบบสารสนเทศที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้
    1. ระบบสำรองกระแสไฟฟ้า (UPS)
    2. เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
    3. ระบบระบายอากาศ
    4. ระบบปรับอากาศ และควบคุมความชื้น
    5. ระบบดังเพลิง
    6. ระบบกล้องวงจรปิด
2) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านี้อย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

7.2.3 การเดินสายไฟและสายเคเบิล (Cabling Security)

1) สายเคเบิ้ลที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้นั้น ต้องให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณและป้องกันสัตว์ต่าง ๆ กัดแทะสาย

2) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากัน เพื่อป้องกันการรบกวนของสัญญาณซึ่งกันและกัน

3) ทำป้านชื่อสำหรับสายสัญญาณ

4) จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

7.2.3 การดูแลรักษาอุปกรณ์ (Equipment Maintenance)

1) ให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนดและต้องปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ
2) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ทุกครั้ง เพื่อใช้ในการตรวจในภายหลัง
3) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
4) ควบคุมและสอดส่งดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในบริษัท
5) ควบคุมการส่งอุปกรณ์ที่นำออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือส่งอุปกรณ์ดังกล่าวไปซ่อมบำรุง ทั้งนี้เพื่อเป็นการป้องกันการรั่วไหลของข้อมูล

7.2.4 การนำสินทรัพย์ขององค์กรออกนอกสำนักงาน (Removal of Asset)

1) ห้ามนำทรัพย์สินสารสนเทศออกนอกสำหนัก โดยไม่ได้รับอนุญาต
2) ให้มีปันทึกการนำทรัพย์สินสารสนเทศก่อนนำออกนอกสำนักงานและบันทึกการส่งคืน เพื่อเก็บเป็นหลักฐานป้องกันการสูญหาย

7.2.6 การป้องกันอุปกรณ์และสินทรัพย์สารสนเทศที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment and asset Off-Premises)

1) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินสารสนเทศของบริษัทไว้นอกพื้นที่สำนักงานโดยไม่มีผู้ดูแล
2) ผู้ใช้งานต้องรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์ของบริษัทเสมือนเป็นสินทรัพย์ของตนเอง

7.2.7 การจัดการอุปกรณ์หรือการนาอุปกรณ์กลับมาใช้ใหม่ (Secure Disposal or Re-use of Equipment)

ผู้ดูแลระบบฯ หรือผู้ใช้งานต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ ทั้งนี้เพื่อเป็นการป้องกันการรั่วไหลของข้อมูลดังกล่าว

7.2.8 การป้องกันอุปกรณ์ของผู้ใช้งานที่ไม่มีผู้ดูแล (Unattended User Equipment)

1) ผู้ใช้งานต้องออกจากระบบสารสนเทศโดยทันทีเมื่อเสร็จสิ้นการปฏิบัติงาน และปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการปฏิบัติงานประจำวัน หรือเมื่อไม่มีการใช้งานเกิน 1 ชั่วโมง

2) ผู้ใช้งานต้องล๊อคอุปกรณ์เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

3) ผู้ใช้งานต้องปิด ล็อกพื้นที่เพื่อจัดเก็บอุปกรณ์ในสถานที่ปลอดภัยเมื่อไม่มีการใช้งาน

4) กำหนดให้เครื่องคอมพิวเตอร์พักหน้าจอเมื่อไม่มีผู้ใช้งานนานเกินกว่า 15 นาที และมีการใส่รหัสผ่านในการเข้าถึงใหม่อีกครั้ง

7.2.9 การควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศที่สาคัญไว้ในที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy)

1) ข้อมูลความลับหรือข้อมูลที่มีความสำคัญที่บันทึกอยู่ในเอกสารในรูปแบบกระดาษ หรือที่จัดเก็บในสื่อบันทึกข้อมูลทางอิเล็กทรอนิกส์ ต้องมีการจัดเก็บอย่างปลอดภัยเมื่อไม่มีความจำเป็นต้องใช้งาน

2) ต้องล็อกหน้าจอเครื่องคอมพิวเตอร์ด้วยรหัสผ่าน หรือระบบการยืนยันตัวตนอื่นเมื่อไม่ได้ใช้งาน

3) ไม่วางเอกสารที่มีชั้นความลับหรือเอกสารสำคัญ ซึ่งสั่งพิมพ์ผ่านเครื่องพิมพ์ทิ้งไว้

8 ความมั่นคงปลอดภัยสาหรับการดำเนินงาน (Operation Security)

8.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

วัตถุประสงค์: เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

นโยบาย

8.1.1 ขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)

1) ผู้ดูแลระบบฯ ต้องจัดทำเอกสารวิธีปฏิบัติที่เหมาะสมสำหรับแต่ละระบบสารสนเทศที่อยู่ในความรับผิดชอบของตนและประกาศให้ผู้ปฏิบัติงานทราบ

2) ผู้ดูแลระบบฯ ต้องปรับปรุงเอกสารวิธีปฏิบัติตามความเหมาะสมต่อสภาวะแวดล้อมการปฏิบัติงาน

3) ผู้ดูแลระบบฯ มีการป้องกันมิให้ข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศถูกเข้าถึงโดยมิได้รับอนุญาติ

8.1.1 การจัดการการเปลี่ยนแปลง (Change Management)

1) ก่อนทำการเปลี่ยนแปลงกับระบบสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ หรือฐานข้อมูล โดยผู้ดูแลระบบฯ หรือผู้ให้บริการภายนอกต้องดำเนินการขออนุมัติการดำเนินการเปลี่ยนแปลงจากผู้บริหาร ฝ่ายเทคโนโยยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

2) การเปลี่ยนแปลงกับระบบเครือข่าย ระบบคอมพิวเตอร์ ซอฟต์แวร์ หรือฐานข้อมูลโดยผู้ใช้บริการภายนอกต้องได้รับการควบคุมดูแลจากผู้ดูแลระบบฯ

3) ผู้ดูแลระบบฯ หรือผู้ให้บริการภายนอกต้องมีการประเมินผลกระทบการเปลี่ยนแปลงระบบ ก่อนที่จะทำการเปลี่ยนแปลงนั้น เพื่อป้องกันกระทบกับการทำงานของระบบ ที่ใช้ดำเนินงานอยู่ในปัจจุบัน

4) ผู้ดูแลระบบฯ ต้องบันทึกรายละเอียดการเปลี่ยนแปลงระบบสารสนเทศ

5) ผู้ดูแลระบบฯ หรือผู้ใช้บริการภายนอกต้องมีการทดสอบการเปลี่ยนแปลงนั้นก่อนเสมอ

6) ผู้ดูแลระบบฯ หรือผู้ให้บริการภายนอกต้องกำหนดแผนย้อนคืน (Fallback Plan) เพื่อรองรับหากการเปลี่ยนแปลงไม่เป็นไปตามที่คาดคิด

7) ผู้ดูแลระบบฯ หรือผู้ให้บริการจากภายนอกต้องกำหนดระยะเวลาในการติดตามการเปลี่ยนแปลงนั้น เพื่อตรวจสอบผลกระทบที่อาจเกิดขึ้นกับระบบหลังจากการเปลี่ยนแปลง

8.1.3 การจัดการขีดความสามารถ (Capacity Management)

ผู้ดูแลระบบฯต้องเฝ้าติดตามสังเกตการใช้งานทรัพยากรสารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ เพื่อวางแผนบริหารทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม อย่างน้องปีละ 1 ครั้ง

8.1.4 การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนา ทดสอบและสภาพแวดล้อมในการปฏิบัติงาน (Separation of Development, Testing and Operational Environment)

กำหนดให้มีการแยกระบบสารสนเทศสำหรับการทดสอบ และใช้งานจริง ออกจากกันเพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาติ

8.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์: เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

นโยบาย

8.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

1) เครื่องคอมพิวเตอร์ลูกขาย และเครื่องคอมพิวเตอร์แบบพกพาต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัสที่ได้รับการ อัฟเดทข้อมูลจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส และต้องเปิดใช้งานตลอดเวลาที่ใช้เครื่อง

2) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริหารป้องกันไวรัส ต้องมีการอัพเดทข้อมูลล่าสุดอยู่สมอ

3) ผู้ใช้งานต้องตรวจสอบไฟล์แนบที่มากับจดหมายอิเล็กทรอนิกส์ (e-mail) หรือไฟล์ที่ได้รับมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

4) ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมไม่ประสงค์ดีเข้าสู่ระบบคอมพิวเตอร์ ขอบบริษัท

5) ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

6) เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ต ยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

8.3 การสารองข้อมูล (Backup)

วัตถุประสงค์: เพื่อเป็นแนวทางในกำหนดการสารองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ เช่น ภัย ธรรมชาติ ระบบเสียหาย ฯลฯ

นโยบาย

8.3.1 การสำรองข้อมูล (Information Backup)

1) ผู้ดูแลระบบฯ และเจ้าของข้อมูลทำบัญชีรายชื่อข้อมูลที่มีความสำคัญและปรับปรุงบัญชีรายชื่อให้มีความทันสมัยอยู่เสมอ

2) ผู้ดูแลระบบฯ กำหนดชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลไว้อย่างน้อยต้องประกอบด้วยข้อมูลในฐานข้อมูลของระบบสารสนเทศหรือไฟล์ข้อมูลที่เกี่ยวข้อง

3) ผู้ดูแลระบบฯ กำหนดความถี่ในการสำรอบข้อมูล

8.3.2 แนวปฏิบัติการสำรองข้อมูล

1) ผู้ดูแลระบบฯ ต้องจัดให้มีการสำรองและทดสอบการกู้คนข้อมูลอย่างน้องปีละ 1 ครั้ง

2) ผู้ดูแลระบบฯ ต้องจัดทำบันทึกการสำรองข้อมูล (Operation Logs)

3) ผู้ดูแลระบบฯ ต้องจัดทำรายงานข้อผิดพลาด (Fault Logging) ที่เกิดจากการสำรองข้อมูล รวมทั้งวิธีการแก้ไข

4) กำหนดชนิดและช่วงเวลาของการสำรองข้อมูล พร้อมทั้งสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมี 2 ชนิด คือ การสำรองข้อมูลแบบเต็ม และ การสำรองข้อมูลแบบเพิ่มส่วนต่าง

5) ในกรณีพบปัญหาทำให้ไม่สามารสำรองข้อมูลได้อย่างครบถ้วนสมบูรณ์ให้ผู้ดูแล จัดการระบบงานดำเนินการแก้ไขปัญหา และ สรุปผลให้ผู้บังคับบัญชาทราบ

6) ผู้ดูแลระบบฯ ต้องสำรองข้อมูลตามความถี่ที่ผู้วิเคราะห์ระบบแนะนำ หรือดังนี้เป็นอย่างน้อย

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูลแบบเต็ม
ระบบ Web Server	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ข้อมูลบนเว็บที่เผยแพร่	1 ครั้งแต่เดือน
ระบบ Database server	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ฐานข้อมูลที่มีความสำคัญ	1 ครั้งแต่เดือน
อุปกรณ์ Firewall	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
อุปกรณ์ Server อื่น ๆ	ค่าคอนฟิกกุเรชั่นของระบบ (Configuration)	ช่วงก่อนและหลังการเปลี่ยนแปลงค่า
	ฐานข้อมูลที่มีความสำคัญต่อระบบ	1 ครั้งแต่เดือน

7) ผู้ใช้งานต้องสำรองข้อมูลตามความจำเป็นและเหมาะสมไว้บนสื่อบันทึกอื่น ๆ เป็นประจำทุกเดือน
8) ผู้ใช้งานต้องรักษาสื่อบันทึกข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และ ห้ามนำข้อมูลไปเปิดเผยต่อบุคคลภายนอกบริษัทฯ โดยตั้งใจ หรือไม่ตั้งใจ

8.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

วัตถุประสงค์: เพื่อให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน

นโยบาย

8.4.1 การบันทึกข้อมูลเหตุการณ์ (Event logging)

1) ระบบคอมพิวเตอร์หรือระบบเครือข่ายต้องมีการเก็บบันทึกข้อมูลล็อก ต้องบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวนในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง รวมทั้งให้มีการวิเคราะห์ข้อมูลล็อกดังกล่าวอย่างสม่ำเสมอ และจัดการแก้ไขข้อผิดพลาดอย่างเหมาะสม

2) มีการติดตามสังเกต และประเมินผลการติดตามดังกล่าวอย่างสม่ำเสมอ

3) ต้องจัดเก็บข้อมูลล็อกทางคอมพิวเตอร์เป็นระยะเวลาไม่น้อยกว่า 90 วัน

8.4.2 การป้องกันข้อมูลล็อก (Protection of Log Information)

ระบบสารสนเทศที่จัดเก็บข้อมูลล็อก ต้องได้รับการปกป้องเพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาติ

8.4.3 ข้อมูลล็อกของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ (Administrator and Operator Logs)

กำหนดให้มีการเก็บข้อมูลล็อกที่เกี่ยวข้องกับการดูแลระบบโดยผู้ดูแลระบบฯ

8.4.4 การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

ต้องตั้งเวลาของเครื่องคอมพิวเตอร์และระบบเครือข่ายให้มีเวลาตรงกันทั้งหมดโดยให้อ้างอิงเวลาสากล (Stratum 0) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที

8.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Control of Operation Software)

วัตถุประสงค์ เพื่อให้ระบบที่ให้บริการ สามารถให้บริการและมีการทำงานที่ถูกต้อง

นโยบาย

8.5.1 การติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of Software on Operational Systems)

ผู้ดูแลระบบฯ ต้องควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี ซอฟต์แวร์อุดช่องโหว่า ลงในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการอยู่ โดยต้องมีการทดสอบซอฟต์แวร์เหล่านั้นก่อน เพื่อให้มั่นใจ ว่าจะไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่

8.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์ เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์ระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจาการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

นโยบาย

8.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ผู้ดูแลระบบฯ ต้องปรับปรุงระบบซอฟต์แวร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่าง ๆ อย่าสม่ำเสมอ

ผู้ดูแลระบบฯ ต้องประเมินความเสี่ยงของช่องโหว่ทางเทคนิค และกำหนดมาตรการเพื่อลดความเสี่ยงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

ผู้ดูแลระบบคอมพิวเตอร์ต้องกำหนดและจำกัดรายการของซอฟต์แวร์ที่ติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่าย

8.7 การพิจารณาการตรวจสอบระบบสารสนเทศ(InformationSystemAuditConsiderations)

วัตถุประสงค์: เพื่อให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมด มีผลกระทบน้อยที่สุดต่อการดาเนินงานของหน่วยงาน

นโยบาย

8.7.1 การวางแผนการตรวจสอบระบบสารสนเทศทั้งหมด (Information System Audit Controls)

ผู้ตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต้องตรวจสอบและประเมินความเสี่งด้านสารสนเทศตามแนวทาง ดังนี้

1) ให้มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศโดยเจ้าของระบบสารสนเทศ
2) ให้มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
3) ให้มีการตรงจสอบและประเมินความเสี่ยงของระบบสารสนเทศที่ให้บริการ
4) ให้มีการตรวจสอบและประเมนความเสี่ยงอย่างน้อยปีละ 1 ครั้ง
5) ภายหลังการตรวจสอบให้รายงานผลการตรวจสอบ และประเมินความเสี่ยงของระบบ สารสนเทศต่อเจ้าของระบบสารสนเทศทราบต่อไป
6) เจ้าของระบบสารสนเทศที่ได้รับการตรวจสอบและประเมินความเสี่ยงต้องจัดทำ แผนดำเนินการเพื่อบริหารจัดการความเสี่ยงที่ตรวจพบเหล่านั้น
7) รายการที่ต้องมีการตรวจประเมินอย่างน้อยดังนี้
    a. การป้องกันการบุกรุกระบบสารสนเทศ
    b. การสำรองข้อมูล
    c. การควบคุมการเข้าถึงพื้นที่ Data Center
    d. การควบคุมการเข้า-ออกอาคาร
    e. การเตรียมความพร้องรับสถานการณ์ฉุกเฉิน
    f. การเข้าถึงระบบสารสนเทศ
    g. การกำหนดใช้งานตามภารกิจ

9 ความมั่นคงปลอดภัยสาหรับการสื่อสารข้อมูล
(Communications Security)

9.1 การการจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

วัตถุประสงค์: เพื่อปูองกันข้อมูลในระบบเครือข่าย และปูองกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของ สานักงานฯ

นโยบาย

9.1.1 การควบคุมการเข้าถึงเครือข่าย (Network Control)

ผู้ดูแลระบบเครือข่ายต้องจำกัดการเข้าถึงระบบเครือข่ายและ ระบบสารสนเทศที่เชื่อมต่ออยู่กับ ระบบเครือข่าย โดยกำหนดให้ผู้ใช้งานในเครือข่ายสามารถเข้าถึงระบบสรสนเทศผ่านทางเครือข่ายที่ได้รับการอนุญาติเท่านั้น

ผู้ดูแลระบบฯ ต้องควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาติ

การเข้าถึงอุปกรณ์เครือข่ายเพื่อการตรวจสอบและปรับแต่งระบบทั้งทางกายภาย และการเข้าถึงจากระยะไกลต้องมีการควบคุม และทำได้เพียงแต่เฉพาะผู้ดูแลระบบฯ ที่ได้รับอนุญาต

ในกรณีที่ต้องกำหนดสิทธิการเข้าถึงแบบชั่วคราวแก่บุคคลภายนอก ผู้ดูแลระบบเครือข่ายต้องให้มีผู้ควบคุม ตรวจสอบและยกเลิกสิทธิการเข้าถึงทันทีที่ปฏิบัติงานเสร็จ

ผู้ดูแลระบบฯ ต้องตรวจสอบและปิดพอร์ตของอุปกรณ์เครือข่ายที่ไม่ใช้งาน

การให้บริการทางเครือข่ายสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบเครือข่าย ต้องอนุญาติเฉพาะพอร์ต การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

ผู้ดูแลระบบฯ ต้องมี Security Log เพื่อค้นหาร Invalid Attempt Access ของผู้บุกรุกและตรวจสอบ Fault Alarm Log เพื่อสามารถตรวจสอบปัญหาที่เกิดขึ้นประจำวัน

ต้อง ปรับปรุง Security patch ของอุปกรณ์ เครือข่ายอย่างสม่ำเสมอ

ต้องสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์เครือข่ายเป็นประจำหรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

จัดทำแผนผังเครือข่าย ซึ่งมีรายละเอียดเกี่ยวข้องกับขอบเขตของระบบเครือข่ายภายในบริษัท พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

มีการระบุอุปกรณ์ที่เชื่อต่อเข้ากับ ระบบสารสนเทศโดยอัตโนมัติ เพื่อตรวจสอบการเชื่อมต่อของอุปกรณ์ดังกล่าวว่ามาจากอุปกรณ์ดังกล่าจริง

9.1.2 การความมั่นคงปลอดภัยสาหรับการใช้บริการเครือข่าย (Security of Network Service)

การเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องผ่าน Fire Wall หรือ ฮาร์ดแวร์อื่น ๆ ที่มีความสามารถในการตรวจจับไวรัส

ต้องจำกัดจำนวนการเชื่อต่อจากภายนอกเข้ามายังระบบของบริษัท และกำหนดช่องทางการเชื่อมต่อเฉพาะเท่านั้น และ กำหนดเครื่องคอมพิวเตอร์ที่จะทำการเชื่อมต่อ

ห้ามผู้ใช้งานติดตั้งโมเด็มเข้ากับเครื่องคอมพิวเตอร์ของตนเอง หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของบริษัท โดยไม่ได้รับอนุญาตจากฝ่ายเทคโนโนยีสารสนเทศ

9.1.3 การจัดแบ่งเครือข่ายภายในสานักงานฯ (Segregation in Network)

กลุ่มที่ให้บริการสารสนเทศ เป็นระบบเครือข่ายที่สามารถเข้าถึงและใช้งานโดยผู้ใช้งาน เช่น ระบบอินทราเน็ต ระบบจดหมายอิเล็กทรอนิกส์

กลุ่มผู้ใช้งาน Guest สามารถ ใช้งาน เฉพาะ Internet เท่านั้น

9.2 การถ่ายโอนข้อมูล (InformationTransfer)

วัตถุประสงค์: เพื่อให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศ ที่มีการถ่ายโอนข้อมูลกันภายในบริษัท และถ่ายโอนข้อมูลกับภายนอก

นโยบาย

9.2.1 นโยบายและขั้นตอนปฏิบัติสาหรับการถ่ายโอนสารสนเทศ (Information Transfer Policies and Procedures)

การรับ-ส่งข้อมูลหรือไฟล์อิเล็กทรอนิกส์ที่เป็นความลับระหว่างหน่วยงานภายใจหรือ ภายนอกบริษัท ต้องได้รับการเข้ารหัสข้อมูลตามนโยบายและแนวปฏิบัติฯ การเข้ารหัสข้อมูล การความคุมการเข้ารหัส (Cryptography Control

กำหนดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลหรือไฟล์อิเล็กทรอนิกส์ระหว่างหน่วยงานภายในกับบุคคลหรือหน่วยงานภายนอก (Electronic Messaging)

กำหนดให้มีข้อตกลงในการรักษาความลับหรือไม่เปิดเผยความลับอย่างเป็นลักลักษณ์อักษร กับผู้ให้บริการภายนอก (Confidentiality or Non-Disclosure Agreements)

10 การจัดหา พัฒนา และดูแลระบบสารสนเทศ
(Systems Acquisition, Development and Maintenance)

10.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

วัตถุประสงค์: เพื่อให้แน่ใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดวงจรการพัฒนา ระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ

นโยบาย

10.1.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัย (Information Security Requirements nalysisand Specification)

กำหนดให้มีเกณฑ์การตรวจรับ ระบบสารสนเทศที่มีการปรับปรุง หรือที่มีเวอร์ชันใหม่ หรือควรมีการทดสอบ ระบบสารสนเทศก่อนการตรวจรับ

กำหนดให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยของระบบสารสนเทศในการจัดทำข้อกำหนดขั้นต่อของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม

ข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธรณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

กำหนดให้มีข้อกำหนดขั้นต่ำสำหรับการรักษาความถูกต้องแท้จริง Authenticity และความถูกต้องครบถ้วน Integrity ของข้อมูลใน แอพพลิเคชั่น รวมทั้งมีการระบุและปฏิบัติตามวิธีการป้องกันที่เหมาะสม

ต้องมีการดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์

10.1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะ ต้องได้รับการป้องกัน และการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

10.2.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protectingapplicationservicestransactions)

สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่ สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับ อนุญาต การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

10.2 ความมั่นคงปลอดภัยสาหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

วัตถุประสงค์: เพื่อให้มั่นใจได้ว่ามีระบบสารสนเทศมีความมั่นคงปลอดภัย ครอบคลุมทั้งวงจรการพัฒนาระบบ สารสนเทศ (development lifecycle)

นโยบาย

10.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย(Secure developmentpolicy)

มีการแยกระบบสารสนเทศสำหรับการพัฒนาและใช้งานจริงออกจากกันเพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต

10.2.2 กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (SystemChangeControlProcedures)

ผู้ดูแลระบบต้องแจ้งให้ผู้ที่เกี่ยวข้องทราบเกี่ยวกับการปรับปรุงหรือเปลี่ยนแปลงระบบเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบ และทบทวนก่อนที่จะดำเนินการปรับปรุงหรือเปลี่ยนแปลงระบบ

ผู้ดูแลระบบ ต้องวางแผนดำเนินการปรับปรุงหรือเปลี่ยนแปลงระบบ ก่อนเปลี่ยนไปใช้ระบบใหม่

ผู้ดูแลระบบ ต้องทดสอบโปรแกรมระบบ (System Software) ที่มีความสำคัญ และ ประสิทธิภายการใช้งานโดยทั่วไป หลังจากการแก้ไข หรือบำรุงรักษาระบบ

10.2.3 การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes)

เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบ ซอฟต์แวร์ต่างๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทางานและความมั่นคงปลอดภัย

10.2.4 การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จาเป็น และการเปลี่ยนแปลง ทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ใน อนาคต

10.2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Securesystemengineeringprinciples)

เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรมระบบ ต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดย มีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ

10.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Securedevelopmentenvironment)

ต้องมีการจัดทำหรือป้องกันสภาพแวดล้อมในการทำงานต่างๆ ให้มีความเหมาะสมและปลอดภัยทั้งการพัฒนา และปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ

10.2.7 การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบงาน (OutsourcedDevelopment)

ในการทำสัญญาว่าจ้างการพัฒนาระบบของสานักงานฯ ต้องมีความชัดเจนและครอบคลุมถึงสัญญา ทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึง การรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

10.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (Systemsecuritytesting)

โปรแกรมหรือระบบที่พัฒนาขึ้นมา ควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมีการ ทดสอบอยู่ในช่วงระหว่างการพัฒนา

10.2.9 การทดสอบเพื่อรับรองระบบ (Systemacceptancetesting)

มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบ ใหม่ และระบบที่ปรับปรุง

ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ระบบที่จัดซื้อเข้ามาใช้งานหรือทรัพยากรสารสนเทศอื่นๆ ก่อน การใช้งาน รวมทั้งต้องจัดทำเอกสาร Checklist หัวข้อที่ทำการทดสอบระบบก่อนที่จะตรวจรับระบบนั้น และให้มี การเซ็นชื่อเจ้าหน้าที่ทำการทดสอบและลายเซ็นผู้ส่งมอบ

10.3 ข้อมูลสำหรับการทดสอบ (Test data)

วัตถุประสงค์: เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

นโยบาย

10.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

11 ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

11.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

วัตถุประสงค์: เพื่อให้มีการปูองกันสินทรัพย์ขององค์กร ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

นโยบาย

11.1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

1) กำหนดให้มีเจ้าหน้าที่ผู้ควบคุมงานเพื่อคอยกำกับดูแลการดำเนินงานต่าง ๆ ของผู้ให้บริการภายนอกซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

2) กำหนดให้ผู้ให้บริการภายนอกต้องรับทราบและปฏิบัติตามระเบียบ นโยบาย แนวปฏิบัติขั้นตอนการปฏิบัติงานและวิธีการปฏิบัติงานต่าง ๆ ของบริษัทอย่างเคร่งครัด

11.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก(Assessing security within supplier agreements)

1) ผู้ให้บริการภายนอกต้องติดบัตรผู้มาติดต่อตลอดเวลาที่ปฏิบัติงานในพื้นที่

2) ผู้ให้บริการภายนอกทุกคน ต้องรักษาข้อมูลต่าง ๆ ที่ได้รับทราบระหว่างการปฏิบัติงานให้แก่บริษัทไว้เป็นความลับ และอนุญาตให้ใช้ข้อมูลเพื่อการปฏิบัติงานให้กับทางบริษัทเท่านั้น ห้ามมิให้ทำการเปิดเผยต่อบุคคลอื่นก่อนได้รับอนุญาตจากทางบริษัทอย่างเป็นลายลักษณ์อักษร

3) กรณีที่ผู้ให้บริการภายนอกมีความจำเป็นต้องขอใช้งานข้อมูลสำคัญของบริษัทให้ทำการแจ้งต่อพนักงานที่เป็นผู้ติดต่อประสานงานเพื่อขออนุญาติให้งานข้อมูลจาก เจ้าของข้อมูลหรือผู้มีอำนาจโดยผู้ให้บริการภายนอกได้รับอนุญาติให้ใช้งานข้อมูลเท่าที่จำเป็นต้องรับรู้หรือใช้เพื่อการปฏิบัติงานเท่านั้น

4) ผู้ให้บริการภายนอกต้องแจ้งรายชื่อของเจ้าหน้าที่ที่จะเข้าปฏิบัติงานต่อบริษัทก่อนเริ่มการปฏิบัติงาน และหากมีการเปลี่ยนแปลงบุคคลที่เข้าปฏิบัติงาน หรือมีการเปลี่ยนแปลงตำแหน่งหน้าที่ที่อาจส่งผลกระทบต่อบริษัท ต้องแจ้งให้ทางบริษัททราบล่วงหน้าทุกครั้ง

5) ผู้ใช้บริการภายนอกสามารถนำอุปกรณ์สารสนเทศส่วนบุคคล เช่น คอมพิวเตอร์พกพาเข้าใช้งานในพื้นที่สำนักงานของบริษัทได้โดยห้ามเชื่อต่อกับระบบเครือข่ายหรือระบบคอมพิวเตอร์ภายใจของบริษัท กรณีที่มีความจำเป็นต้องเชื่อต่อต้องแจ้งความจำนงต่อพนักงานที่เป็นผู้ติดต่อประสานงาน เพื่อดำเนินการขออนุมัติตามชั้นตอนของบริษัท

6) ห้ามผู้ใช้บริการภายนอกนำสื่อบันทึกข้อมูลใด ๆ มาเชื่อต่อกับอุปกรณ์สารสนเทศภายในพื้นที่ของบริษัทฯ หากมีความจำเป็นต้องถ่ายโอนข้อมูลให้ดำเนินการโดยพนักงานที่เป็นผู้ติดต่อประสานงานเท่านั้น

7) หากผู้ให้บริการภายอกมีความจำเป็น ต้อง เข้าใช้งานระบบสารสนเทศของบริษัทเข้าปฏิบัติงานในพื้นที่ควบคุมเฉพาะ ต้องแจ้งความจำนงต่อพนักงานที่เป็นผู้ติดต่อประสานงาน เพื่อดำเนินการขออนุมัติตามความเหมาะสม โดยบริษัทจะอนุญาตให้สามารถเข้าใช้งานได้ตามความจำเป็นเท่านั้น ทั้งนี้ เจ้าหน้าที่จากผู้ให้บริการภายนอกต้องให้ความร่วมมือกับบริษัทในการตรวจสอบอุปกรณ์ที่นำเข้ามาใช้งานอย่างเหมาะสม

8) ผู้ให้บริการภายนอกต้องไม่นำเอกสารหรือซอฟต์แวร์ที่มีลิขสิทธิ์ของบริษัทไปใช้งานส่วนตัวหรือใช้งานในทางที่ผิด และห้ามมิให้นำเอกสารหรือซอฟต์แวร์ที่ไม่มีสิขสิทธิ์มาใช้งานในบริษัท

9) ในการปฏิบัติงาน หากผู้ใช้บริการภายนอกต้องการติดตั้งโปรแกรมปรับแต่งระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย หรือกระทำการใด ๆ ที่ก่อให้เกิดความเปลี่ยนแปลงต่อระบบ สารสนเทศของบริษัท ต้องแจ้งต่อพนักงานผู้ติดต่อประสานงานเพื่อดำเนินการขออนุมัติ ผู้ดูแลระบบฯ ก่อนดำเนินการทุกครั้ง

10) ห้ามผู้ใช้บริการภายนอกทำการสแกนระบบเครือข่ายดักฟังข้อมูลบนระบบเครือข่ายหรือพยายามเข้าถึงระบบสารสนเทศของบริษัทโดยไม่ได้รับอนุญาต

12) ผู้ให้บริการภายนอกต้องไม่นำบุคคลอื่นที่ไม่เกี่ยวข้อง เข้ามาในพื้นที่บริษัทโดยไม่ได้รับอนุญาต

13) ห้ามผู้ให้บริการภายนอกทำการถ่ายรูป หรือ บันทึกเสียง ภายในพื้นที่บริษัทก่อนได้รับอนุญาต

14) ขณะปฏิบัติงานหากพบว่ามีสิ่งผิดปกติใด ๆ เกิดขึ้น ผู้ให้บริการภายนอกต้องรายงานให้พนักงานที่เป็นผู้ติดต่อประสานงานทราบทันที

15) บริษัทสงวนสิทธิ์ในการตรวจสอบการทำงานของผู้ให้บริการภายนอกรวมถึง การเพิกถอนสิทธิต่าง ๆ ในการเข้าใช้ข้อมูลและระบบสารสนเทศ เมื่อพบสิ่งผิดปกติหรือมีเหตุการะทบด้านความมั่นคง โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

16) ผู้ให้บริการภายนอกต้องปฏิบัติงานตามขอบเขตและหน้าที่ความรับผิดชอบที่ได้รับมอบหมายหรือที่ระบุไว้ในสัญญาเท่านั้น

17) ผู้ให้บริการภายนอกต้องปฏิบัติงานด้วยความระมัดระวัง เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อบริษัท

18) การกระทำใด ๆ ของผู้ให้บริการภายนอกที่ก่อให้เกิดความเสียหายหรือละเมิดข้อตกลงหรือสัญญาต่าง ๆ ที่ได้ทำไว้กับบริษัท ผู้ให้บริการภายนอกต้องรับผิดชอบต่อความเสียหายทั้งหมด

19) ในวันสุดท้ายของการปฏิบัติงานตามข้อตกลงหรือสัญญาผู้ให้บริการภายนอกต้องทำการส่งคืนทรัพย์สินต่าง ๆ เช่น กุญแจ อุปกรณ์ต่าง ๆ และรหัสเข้าระบบ ให้แก่พนักงาน ผู้ติดต่อประสานงานอย่างครบถ้วน

20) กรณีที่ผู้ให้บริการภายนอกมีการดำเนินการเปลี่ยนแปลงใด ๆ ที่อาจะส่งผลกระทบต่อการให้บริการตามข้อตกลงหรือสัญญา ผู้ให้บริการภายนอก ต้องแจ้งต่อทางบริษัทอย่างเป็นลายลักษณ์อักษรล่วงหน้าอย่างน้อง 30 วัน เพื่อให้บริษัททำการพิจารณา วิเคราะห์ผลกระทบและหาวิธีในการแก้ไขควบคุมความเสี่ยงได้อย่างเหมาะสม

11.2 การบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

วัตถุประสงค์: เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ ของผู้ให้บริการภายนอก

นโยบาย

11.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of Supplier Services)

ผู้ดูแลผู้ให้บริการภายนอกจะต้องตรวจสอบสภาพแวดล้อมการ ทำงาน รวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของ หน่วยงานภายนอกต้องมีการทบทวนติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

11.2.2 การบริหารจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Chages to Supplier Services)

การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอก ที่เกี่ยวข้องกับบริการด้านสารสนเทศ จะต้องแจ้งก่อนการเปลี่ยนแปลงล่วงหน้าอย่างน้อย 30 วันทำการ

การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติและมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของ สารสนเทศและกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องมีการทบทวนการประเมิน ความเสี่ยงใหม่

12 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

12.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์: เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของสานักงาน ได้รับการดาเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

นโยบาย

12.1.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

1) ผู้ใช้งานระบบสารสนเทศของบริษัทมีหน้าที่ในการรายงานเหตุละเมิดหรือจุดอ่อนด้านความมั่นคงใดๆ ที่พบเห็น หรือที่ต้องสงสัยต่อผู้บังคับบัญชาและ/ หรือผู้ดูแลระบบ โดยทันที เพื่อให้สามารแก้ไขปัญหาได้อย่างรวดเร็ว ตัวอย่างของเหตุละเมิดความมั่นคงที่ต้องรายงาน

ตรวจพบไวรัส หรือโปรแกรมไม่ประสงค์ดีต่าง ๆ
ตรวจพบความพยายามเจาะระบบ หรือเครื่องมือเจาะระบบ
การใช้งานข้อมูลหรือระบบสารสนเทศอย่างไม่เหมาะสม
การเข้าถึงข้อมูลหรือระบบสารสนเทศโดยไม่ได้รับอนุญาต
ช่องโหว่หรือจุดอ่อนของซอฟต์แวร์
การละเมิดนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย
การกระทำที่ผิดกฎหมาย หรือข้อบังคับของบริษัท

2) ผู้ใช้งานระบบสารสนเทศของบริษัทซึ่งพบเห็นเหตุละเมิน หรือจุดอ่อนด้านความมั่นคงต้องไม่บอกเล่าถึงเหตุที่ตนพบเห็นนั้นกับบุคคลอื่นใด ยกเว้นผู้บังคับบัญชาและผู้ดูแลระบบฯ ทั้งนี้ ผู้ใช้งานต้องหลีกเลี่ยงการพิสูจน์จุดอ่อนด้านความมั่นคงที่ต้องสงสัยด้วยตนเอง

3) ผู้ดูแลระบบฯ มีหน้าที่ต้องรับผิดชอบต่อการรับมือเหตุละเมิดความมั่นคงปลอดภัยต้องดำเนินการตอบสอนต่อเหตุด้วยความรวดเร็ว มิสติรอบคอบ และต้องติดต่อประสานงานกับหน่วยงานต่าง ๆ ที่เกี่ยวข้องอย่างเหมาะสม รวมถึง บันทึกข้อมูล และจัดทำเอกสารเกี่ยวกับเหตุละเมิดความมั่นคงปลอดภัยโดยละเอียด

4) ข้อมูลและหลักฐานที่เกี่ยวข้องกบเหตุละเมิดความมั่นคงที่เกิดขึ้นทั้งหมด ต้องได้รับการบันทึกและจัดเก็บอย่างปลอดภัยโดยผู้ดูและระบบฯ เพื่อนำมาศึกษาและป้องกันไม่ให้เกิดเหตุซ้ำในอนาคต

5) จัดฝึกอบรมในหัวข้อที่เกี่ยวข้องกับการตอบสนอง รับมือต่อเหตุละเมิดความมั่นคงโดยผู้เชี่ยวชาญจากหน่วยงานภายนอกให้แก่ผู้ดูแลระบบฯ ที่มีหน้าที่รับผิดชอบในการรับมือเหตุละเมิดความมั่นคง

6) เครื่องคอมพิวเตอร์ของผู้ใช้งานที่ถูกปลอดออก โอนย้าย และลดตำแหน่งจากการกระทำผิดที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ ต้องถูกแยกออกจากเครือข่ายทั้งภายในและภายนอกโดยทันที และก่อนที่จะนำกลับมาใช้ใหม่ ต้องมีการสำรองข้อมูลจากฮาร์ดไดรฟ์เสียก่อน แล้วจึงทำการฟอร์แมตเครื่องคอมพิวเตอร์นั้น เพื่อป้องกันการแพร่กระจายของซอฟต์แวร์มุ่งร้าย หรือเพื่อกำจัดซอฟต์แวร์ที่ไม่ได้รับอนุญาติซึ่งอาจถูกติดตั้งไว้ในระบบเครือข่าย

7) กระบวนการที่ใช้คอมพิวเตอร์ในการประมวลผลข้อมูลสำคัญต้องได้รับการควบคุมด้วยมาตรการต่าง ๆ ได้แก่ การตรวจสอบภูมิหลังของผู้ใช้งาน การแบ่งแยกอำนานหน้าที่ของผู้ใช้งานการบังคับให้ผุ้ใช้งาน

หยุดพักร้อนหรือหมุนเวียนตำแหน่งงานเพื่อทำการตรวจสอบ หรือมาตรการอื่น ๆ เพื่อให้แน่นใจว่าไม่มีผู้ใดมีสิทธิขาดในการควบคุมข้อมูลสำคัญเพียงลำพัง ทั้งนี้เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยของข้อมูล

13 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหาร จัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security - aspects of business continuity management)

13.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

วัตถุประสงค์: เพื่อป้องกันการหยุดชะงักในการดำเนินงานของบริษัทฯ ที่เป็นผลมาจากความล้มเหลวหรือการ หยุดทำงานของระบบ

นโยบาย

13.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

การจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน

ผู้ดูแลระบบฯ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (Contingency Plan) เพื่อรับมือสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นได้ ทั้งวิธีการทางอิเล็กทรอนิกส์และทางกายภายโดยแผนเตรียมความพร้อมกรณีฉุกเฉิน ต้องมีรายละเอียดอย่างน้อย ดังนี้

- การกำหนดหน้าที่และความรับผิดชอบของบุคคลที่เกี่ยวข้อง
- การกำหนดขั้นตอนการปฏิบัติในการกู้คืนระบบสารสนเทศ
- การกำหนดขั้นตอนการปฏิบัติในการสำรองข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้
- กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก
- ให้ปรับปรุงแผนเตรียมความพร้อมฉุกเฉินอย่างน้อยปีละ 1 ครั้ง
- ให้ทำการทดสอบแผนเตรียมความพร้อมฉุกเฉินอย่างน้อยปีละ 1 ครั้ง หากมีปัญหาเกิดขึ้นในระหว่าการกู้คืน ให้ดำเนินการแก้ไข และบันทึกข้อมูลปัญหาเหล่านั้น พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

13.2 การเตรียมอุปกรณ์ประมวลผลสารอง (Redundancies)

วัตถุประสงค์: เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

นโยบาย

13.2.1 สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนทศ (Availability of information processing facilities)

ระบบปฏิบัติงานสำรอง

กำหนดให้ผู้ดูแลระบบฯ ประเมินและกำหนดระบบสารสนเทศสำหรับระบบสำคัญรวมไปถึงจัดเตรียมอุปกรณ์ที่สามารถทำงานทดแทนได้อย่างเหมาะสม

กำหนดให้ผู้ดูแลระบบฯ กำหนดสถานที่และตรียมพื้นที่ให้อยู่ในสภาพพร้อมใช้งานสำหรับระบบทำงานทดแทน

กำหนดให้ผู้ดูแลระบบฯ ทดสอบระบบปฏิบัติงานสำรองอย่างสม่ำเสมอเพื่อมั่นใจได้ว่า จะสามารถทำงานทดแทนระบบหลักได้ เมื่อมีความจำเป็นต้องใช้งาน

14 การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน (Compliance)

14.1 การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

วัตถุประสงค์: เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับ รวมทั้งสัญญาต่าง ๆ

นโยบาย

14.1.1 การระบุข้อกำหนด และความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

ผู้ใช้งานทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบายกฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด โดยมีรายการดังต่อไปนี้เป็นอย่างน้อย

- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- พระราชบัญญัติว่าด้วยการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์
- พระราชบัญญัติลิขสิทธิ์
- พระรากฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์
- พระราชกฤษฎีการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
- กฎ นโยบาย และแนวปฏิบัติสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)
- นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของบริษัทฯ ถือเป็น สินทรัพย์ของบริษัท (ยกเว้น ข้อมูลที่เป็นสินทรัพย์ของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้บริษัทฯ สามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จาเป็นต้องแจ้ง ให้ผู้ใช้งานทราบล่วงหน้า

เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยี สารสนเทศของบริษัทฯ และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบ คอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ของ บริษัทฯ กำหนดไว้

บริษัทฯ ขอสงวนสิทธิ์ในการเข้าถึง ทบทวน และตรวจสอบอีเมลของผู้ใช้งาน โดยไม่จำเป็นต้อง แจ้งให้ทราบล่วงหน้า อย่างไรก็ตามบริษัทฯ จะดำเนินการตรวจสอบดังกล่าวต่อเมื่อมีความ จำเป็นเท่านั้น

ห้ามเจ้าหน้าที่บริษัทฯ ใช้งานสินทรัพย์และระบบเทคโนโลยีสารสนเทศของบริษัทฯ กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออกนอกประเทศ ไม่ขัดต่อข้อกฎหมายใดๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

14.1.2 สินทรัพย์ทางปัญญา (IntellectualPropertyRights)

ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่บริษัทจัดหามาใช้ใช้งาน

ผู้ดูแลระบบฯ ต้องมีการบริหารจัดการและควบคุมดูแลการใช้งานซอฟต์แวร์ให้เป็นไปตามลิขสิทธิ์ที่ได้รับ

ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดสิทธิ์บนเครื่องคอมพิวเตอร์แท็บเล็ต หรือสมาร์โฟนของบริษัทโดยเด็จขาด

14.1.3 การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

ผู้ดูแลระบบฯ ต้องป้องกันมิให้ข้อมูลที่สำคัญเกิดความเสียหายสูญหายหรือถูกปลอมแปลงโดยให้สอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่าง ๆ ของบริษัทและข้อกำหนดการให้บริการ

14.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personally identifiable information)

กำหนดให้มีการคุ้มครอบข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของบริษัท

14.1.5 การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

บริษัทฯ ต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

14.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

วัตถุประสงค์: เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ อย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

นโยบาย

14.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

กำหนดให้มีการทบทวนวัตถุประสงค์ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงของสภาวะแวดล้อมของบริษัท

14.2.2 การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)

กำหนดให้มีการทบทวนขั้นตอนการปฏิบัติงานโดยเทียบกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

14.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

กำหนดให้มีการทบทวนความสอดคล้องของระบบสารสนเทศเทียบกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และดำเนินการแก้ไขความไม่สอดคล้องที่ตรวจสอบของบริษัท

ให้ผู้บังคับบาเป็นผู้กำกับดูแล ให้ผู้ใต้บังคับบัญชาปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทอย่างเคร่งครัด

ในกรณีที่มีการฝ่าฝืนหรือละเลยการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท ให้ผู้บังคับบัญชาชาดำเนินการเพื่อยับยั้งเหตุการณ์ฝ่าฝืนหรือละเลยการปฏิบัติดังกล่าวตามสมควร และรายงานตามสายบังคับบัญชาไปยังผู้บริหารเทคโนโลยีสารสนเทศระดับสูงเพื่อพิจารณาดำเนินการต่อไป

หากบุคคลใดจงใจฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท จะถือว่าเป็นความผิดทางวินัยและให้ดำเนินการตาม ข้อบังคับเกี่ยวกับพนักงาน ทั้งนี้ หากการกระทำนั้นเป็นเหตุให้บริษัทได้รับความเสียหาย บริษัทจะพิจารณาดำเนินคดีตามกฎหมายอีกทางหนึ่งด้วย