นโยบายเทคโนโลยีสารสนเทศ

(Information Technology Policy)

มีผลบังคับใช้ตั้งแต่วันที่ 10 พฤศจิกายน 2566 เป็นต้นไป

หมวดที่ 1 บทสรุปผู้บริหาร

บริษัท พรีไซซ คอร์ปอเรชั่น จำกัด (มหาชน) คำนึงถึงความสำคัญในการเพิ่มสมรรถนะองค์กร (Performance Improvement) ด้วยการนำเทคโนโลยีสารสนเทศเข้ามาสนับสนุน (Resource Acquisition) ช่วยเพิ่มศักยภาพการดำเนินงานขององค์กร (Acquisition) เพื่อใช้เป็นแนวทางในการพัฒนาระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ ส่งผลให้เกิดการใช้งานสารสนเทศ เพื่อบรรลุภารกิจในด้านต่างๆ ขององค์กร รองรับการดำเนินงานตามนโยบายของผู้บริหาร ตลอดจนนโยบายสำคัญด้านการพัฒนาเทคโนโลยีสารสนเทศและสื่อสารของประเทศ เพื่อการทำงานประสานและร่วมมือกับองค์กรอื่นๆ ที่เกี่ยวข้องได้ เพื่อก่อให้เกิดการไหลของข้อมูลอย่างรวดเร็วในกระบวนการบริหารจัดการที่เป็นระบบ มีระเบียบ เป็นขั้นตอน ลดความซ้ำซ้อน ตอบสนองความพึงพอใจของลูกค้า และพัฒนาทรัพยากรที่มีอยู่อย่างต่อเนื่อง (Capability Development) ให้เกิดประโยชน์สูงสุด มีความมั่นคงปลอดภัย และมีกรอบในการบริหารจัดการเทคโนโลยีสารสนเทศที่ดี

บริษัทจึงได้เล็งเห็นว่า การนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินงานจำเป็นต้องกำหนดแนวทางการพัฒนาเพื่อให้เกิดการเติบโตอย่างยั่งยืน (Sustainable Development) ให้สอดคล้องกับกลยุทธ์ และวิสัยทัศน์ขององค์กร รวมถึงกฎหมาย ข้อบังคับ มาตรฐานสากลต่างๆ ที่เกี่ยวข้อง (Compliance) สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ และมีประสิทธิผลเพื่อให้เกิดการพัฒนาตามวัตถุประสงค์ขององค์กรต่อไป

หมวดที่ 2 บททั่วไป

2.1 วัตถุประสงค์

7.1.1 เพื่อให้องค์กรมีแนวนโยบายในการดำเนินงาน หรือการจัดการทางด้านเทคโนโลยีสารสนเทศ การบริหารจัดการข้อมูลของหน่วยงาน และให้ผู้ที่เกี่ยวข้องกับสารสนเทศ ทั้งผู้บริหาร บุคลากรในองค์กร หน่วยงานภายนอก และบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับสารสนเทศขององค์กรได้มีแผนงาน และกรอบการปฏิบัติที่ชัดเจน และมีมาตรฐานยิ่งขึ้น อีกทั้งกำหนดมาตรการป้องกันที่เหมาะสม เพื่อควบคุม และลดความเสียหายต่างๆ ที่อาจเกิดขึ้นจากกรณีที่ทรัพย์สินไม่สามารถใช้งานได้ สูญหาย เสียหาย บกพร่อง หรือ ถูกคุกคามด้านความมั่นคงปลอดภัยทางสารสนเทศ

2.2 กฎหมาย และกฎระเบียบที่เกี่ยวข้อง

2.2.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไข เพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560

2.2.2 พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2558 (ฉบับที่ 3) พ . ศ . 2558 และ (ฉบับที่ 4) พ.ศ. 2561

2.2.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2564

2.2.4 พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

2.2.5 ประกาศกระทรวงเทคโนโลยีสารสนเทศ และการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

2.2.6 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2556

2.2.7 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

2.2.8 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2.3 บทบังคับใช้ และบทลงโทษ

นโยบายเทคโนโลยีสารสนเทศฉบับนี้ให้มีผลบังคับใช้นับจากวันที่ประกาศให้มีผลบังคับใช้ต่อผู้ใช้งานระบบสารสนเทศของบริษัท พรีไซซ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทย่อยทั้งหมด โดยไม่มีการยกเว้น พนักงานและลูกจ้างที่ฝ่าฝืนนโยบายฉบับนี้โดยจงใจและประมาทเลินเล่อ ไม่ว่าจะก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กรหรือบุคคลใดหรือไม่ จะมีความผิด และต้องได้รับการลงโทษทางวินัยตามระเบียบที่องค์กรกำหนดไว้ รวมถึงบริษัทอาจพิจารณาดำเนินการเกี่ยวกับความผิดทางแพ่งและอาญา แก่พนักงานและลูกจ้างนั้น ตามกฎหมาย ข้อบังคับ ระเบียบหรือประกาศที่เกี่ยวข้อง

2.4 การเผยแพร่นโนบาย

ฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการประกาศ และเผยแพร่นโยบายไปยังผู้ใช้งานระบบสารสนเทศขององค์กร เพื่อช่วยให้เกิดความเข้าใจในบทบาทของตนเองในการใช้งานเทคโนโลยีสารสนเทศ และปกป้องทรัพย์สินขององค์กร

2.5 การทบทวนนโยบาย

นโยบายเทคโนโลยีสารสนเทศฉบับนี้ต้องได้รับการทบทวน ปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญของสภาพแวดล้อมต่างๆ เช่น สภาพธุรกิจ กฎเกณฑ์ กฎหมาย เทคโนโลยี เป็น

ต้น โดยถือเป็นหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ ในการทบทวน และปรับปรุง โดยมีผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้ควบคุมดูแลให้เกิดการทบทวน และปรับปรุงตามที่ได้กำหนดไว้

หมวดที่ 3 คำจำกัดความ

นโยบายเทคโนโลยีสารสนเทศ ได้กำหนดคำนิยามของคำศัพท์ที่ใช้ในนโยบายฉบับนี้ เพื่อให้เข้าใจถึงความหมายตรงกัน และอ้างอิงได้ถูกต้อง ดังต่อไปนี้

คำศัพท์	ความหมาย
องค์กร	บริษัท พรีไซซ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทย่อย
บริษัทย่อย	บริษัท พรีไซซ คอร์ปอเรชั่น จำกัด (มหาชน) มีอำนาจควบคุมได้
ฝ่ายเทคโนโลยีสารสนเทศ	หน่วยงานซึ่งอยู่ภายใต้หน่วยงานพัฒนาสถาปัตยกรรมและทุนทางปัญญาองค์กร (~~EA and~~ Intellectual Capital & Digital Organization Development Management) ที่รับผิดชอบในการสนับสนุน ส่งเสริม การดำเนินงาน การบริหารจัดการเทคโนโลยีสารสนเทศขององค์กร
กรรมการผู้จัดการ (Managing Director)	กรรมการผู้จัดการบริษัท
ผู้บริหารระดับฝ่าย (Division Manager)	ผู้บริหารสูงสุดของแต่ละฝ่ายงาน
ผู้บริหารระดับแผนก (Section Manager)	ผู้บริหารสูงสุดของแต่ละแผนกงาน
ผู้มีอำนาจ	ผู้บังคับบัญชาระดับผู้บริหารระดับฝ่ายขึ้นไป หรือผู้ที่ได้รับมอบหมายให้มีหน้าที่ตัดสินใจ
ผู้ดูแลระบบ (Administrator)	เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบ หรือเครือข่ายคอมพิวเตอร์ รวมไปถึงการแก้ไขปัญหาการใช้งานระบบสารสนเทศในด้านต่างๆ ซึ่งสามารถเข้าถึงโปรแกรม หรือเครือข่ายคอมพิวเตอร์เพื่อการจัดการต่างๆ ได้
บุคลากร	บุคลากรบริษัท พรีไซซ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทย่อย

คำศัพท์	ความหมาย
บุคคลภายนอก	บุคคล หรือพนักงานของหน่วยงานภายนอกที่มาติดต่อสื่อสารและมีการเข้าถึงทรัพย์สินสารสนเทศขององค์กร
ผู้ให้บริการภายนอก/ หน่วยงานภายนอก (Third party)	คู่ค้า หุ้นส่วนการค้า ผู้ให้บริการ/จำหน่ายระบบ (Vendor) พนักงานสัญญาจ้าง (Outsource) และบุคคล หรือนิติบุคคลอื่นใดทั้งในประเทศ และต่างประเทศ ที่ให้บริการด้านเทคโนโลยีสารสนเทศ ซึ่งเข้ามาทำสัญญา หรือทำข้อตกลงในการให้บริการให้กับองค์กร รวมถึงหน่วยงานผู้รับจ้างช่วงที่ผู้ให้บริการภายนอกเป็นผู้จัดจ้าง โดยได้รับอนุญาตให้มีสิทธิ์เข้าถึงสถานที่ หรือทรัพย์สินสารสนเทศขององค์กร และใช้งานระบบสารสนเทศขององค์กรตามอำนาจหน้าที่ที่รับผิดชอบ
ผู้ใช้งาน (User)	บุคลากรภายใน บุคคลภายนอก และหน่วยงานภายนอก ที่ใช้งานระบบงานคอมพิวเตอร์ขององค์กร
เจ้าของโครงการ	หน่วยงานภายในบริษัท พรีไซซ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทย่อย ที่เป็นผู้รับผิดชอบในการดำเนินงานโครงการที่มีการจัดจ้างผู้ให้บริการภายนอก/หน่วยงานภายนอกเข้ามาปฏิบัติงานให้กับองค์กร
เจ้าของทรัพย์สิน/เจ้าของข้อมูล (Data Owner)	บุคคล ส่วนงาน ฝ่ายงานผู้เป็นเจ้าของทรัพย์สินที่อยู่ในการดูแลและเจ้าของข้อมูล หรือเป็นผู้ที่ได้รับความเสียหายสูงสุด เมื่อข้อมูลนั้นเสียหาย หรือถูกเปิดเผย
ข้อมูล	ข้อความ ข่าวสาร เอกสาร เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ ที่อยู่ในรูปของตัวเลข ภาษา ภาพ สัญลักษณ์ต่างๆ ที่ยังไม่ผ่านการประมวลผล ทั้งที่อยู่ในรูปอิเล็กทรอนิกส์ หรือที่อยู่ในรูปสื่อสิ่งพิมพ์ และให้ความหมายรวมถึงข้อมูลคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

คำศัพท์	ความหมาย
ข้อมูลอิเล็กทรอนิกส์	ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร
ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
ชุดข้อมูล (Dataset)	การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะ โครงสร้างของข้อมูล หรือจากการใช้ประโยชน์ของข้อมูล
บัญชีข้อมูล (Data Catalog)	เอกสารแสดงบรรดารายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน
ธรรมาภิบาทข้อมูล (Data Governance)	การกำหนดสิทธิ หน้าที่ และ ความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานอย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนตัวและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย
หมวดหมู่ของข้อมูล (Data Category)	เช่น ข้อมูลส่วนบุคคล ข้อมูลความลับขององค์กร เป็นต้น
การจัดชั้นความลับของข้อมูล	การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของ ข้อมูลเพื่อกำหนดสิทธิในการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ซึ่งกำหนดให้มีชั้นความลับทั้งหมด 5 ชั้น กล่าวคือ เปิดเผยสาธารณะ ใช้ภายใน ลับ ลับมาก หรือ ลับที่สุด
วงจรชีวิตของข้อมูล (Data Life Cycle)	ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการ ทำลายข้อมูล
ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data	เป็นการบริหารจัดการข้อมูลเพื่อให้ ทั้งหน่วยงานสามารถเข้าถึงและใช้ข้อมูลร่วมกันได้ โดยข้อมูลถูกจัดเก็บไว้แหล่งเดียว มีการกำหนดมาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูลและทำให้ข้อมูลมีคุณภาพ ซึ่ง Master data เป็นข้อมูลที่สร้าง และถูกใช้งานอยู่

คำศัพท์	ความหมาย
	ภายในหน่วยงาน มีโอกาสเปลี่ยนแปลงได้และมีรายละเอียดหรือจำนวนพิลด์ข้อมูลที่มาก เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้าและบริการ และข้อมูลสถานที่ ในขณะที่ Reference data มีความเป็นสากลถูกสร้างและใช้งานโดยทั่วไป โดยหลากหลายองค์กรหรือแม้กระทั่งใช้งาน ไปทั่วโลก เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง
บัญชีผู้ใช้ (User Name หรือ Account)	กลุ่มของข้อมูลที่ใช้ในการอ้างถึงเพื่อระบุตัวตน สิทธิการเข้าถึง และข้อจำกัดต่างๆ ในการเข้าถึงระบบสารสนเทศ
รหัสผ่าน (Password)	กลุ่มอักขระที่ใช้ในการพิสูจน์ตัวตน ใช้เพื่อควบคุมการเข้าถึงระบบสารสนเทศ หรือข้อมูลสารสนเทศ
สิทธิระดับสูง (Privilege)	สิทธิที่สามารถใช้งาน โดยได้รับสิทธิที่มากกว่าสิทธิของผู้ดูแลระบบหรือผู้ใช้งานทั่วไปในระบบ เช่น Root หรือ Administrator
ระบบสารสนเทศ	ระบบคอมพิวเตอร์ ระบบเก็บข้อมูล ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบสื่อสารข้อมูลทุกประเภท อุปกรณ์สื่อสาร เครื่องพิมพ์ เครื่องสแกน หรืออุปกรณ์ใดๆ ที่เกี่ยวข้องที่เป็นกรรมสิทธิ์ขององค์กรและ/หรือที่องค์กรได้รับอนุญาตให้ใช้ได้ตามกฎหมาย
ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)	การรักษาความลับให้กับข้อมูล (Confidentiality) การปกป้องสารสนเทศให้มีความถูกต้องสมบูรณ์ (Integrity) การทำให้ระบบตอบสนองความต้องการของผู้ใช้งานที่มีสิทธิ์เข้าถึงระบบได้เมื่อต้องการ และสภาพพร้อมใช้งาน (Availability) รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธ ความรับผิด (Non-repudiation และความน่าเชื่อถือ (Reliability) ระบบสารสนเทศมีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตราย และได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจ หรือบังเอิญ
เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)	เหตุขัดข้องที่ส่งผลทำให้ระบบสารสนเทศไม่สามารถให้บริการได้ตามที่กำหนดไว้ หรือคุณภาพในการให้บริการลดลง เช่น เครื่องแม่ข่ายขัดข้อง ระบบอีเมลใช้งานไม่ได้ หรือระบบงานประมวลช้าผิดปกติ เป็นต้น

คำศัพท์	ความหมาย
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
ช่องโหว่ (Vulnerability)	สภาพ หรือสภาวะที่เป็นข้อบกพร่อง หรือไม่สมบูรณ์ของทรัพย์สินสารสนเทศ ซึ่งอาจเกิดจากความบกพร่องในการผลิต หรือการออกแบบ หรือการบริหารจัดการทำให้เกิดจุดอ่อน โดยมีความเสี่ยงที่จะเกิดภัยคุกคามจากช่องโหว่ที่เกิดขึ้น เช่น ช่องโหว่ของโปรแกรมที่ทำให้บุคคลภายนอกสามารถเข้าใช้โปรแกรมได้โดยไม่ต้องผ่านการพิสูจน์ตัวตน
การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัย (Security Awareness)	การให้ความรู้ ความเข้าใจทางด้านความมั่นคงปลอดภัยของสารสนเทศ เพื่อสร้างความตระหนักถึงภัยคุกคาม และปัญหาทางด้านความมั่นคงปลอดภัยสารสนเทศแก่บุคลากร
การสำรองข้อมูล (Data Backup)	การทำสำเนาข้อมูลทั้งหมดในระบบที่ต้องการ เพื่อเป็นการสำรองข้อมูลที่อาจมีการแก้ไข เปลี่ยนแปลง หรือสูญหาย ให้สามารถนำกลับมาใช้งานได้
แหล่งข้อมูล (Source of Data and Information)	ที่เก็บข้อมูล หรือสารสนเทศที่อยู่ในรูปแบบต่างๆ เช่น ข้อมูลแหล่งข้อมูลเฉพาะ และแหล่งข้อมูลส่วนกลาง เป็นต้น
ทรัพย์สินสารสนเทศ	1. อุปกรณ์เทคโนโลยีสารสนเทศ และอุปกรณ์ต่อพ่วงอื่นใดที่ใช้งานร่วมกับอุปกรณ์เทคโนโลยีสารสนเทศ 2. ชุดคำสั่ง โปรแกรมระบบงานสารสนเทศ และโปรแกรมอื่นใดที่ใช้งานร่วมกับโปรแกรมระบบงานสารสนเทศ 3. ข้อมูล ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ และ/หรือทรัพย์สินทางปัญญาใด ๆ
พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure Area)	บริเวณที่ใช้เก็บรักษาอุปกรณ์สารสนเทศที่ใช้ในงานระบบสารสนเทศ แบ่งได้เป็น 3 ประเภท คือ 1. พื้นที่ห้อง Patching Room 2. พื้นที่ห้องปฏิบัติการคอมพิวเตอร์ 3. พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

คำศัพท์	ความหมาย
พื้นที่ห้องปฏิบัติการคอมพิวเตอร์ (Computer Operation)	พื้นที่ที่ใช้ในการป้อนข้อมูล ออกรายงาน และปฏิบัติงานเกี่ยวกับระบบงานสารสนเทศขององค์กร
พื้นที่ห้อง Patching Room	พื้นที่ที่ใช้เก็บอุปกรณ์ในการเชื่อมต่อเครือข่ายคอมพิวเตอร์ และโทรศัพท์ในแต่ละชั้น
พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)	พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ที่ใช้เก็บอุปกรณ์คอมพิวเตอร์และเครื่องคอมพิวเตอร์หลักที่สำคัญในระบบงาน เช่น เครื่องคอมพิวเตอร์แม่ข่าย
บันทึกเหตุการณ์ (Logs)	บันทึกเหตุการณ์การใช้งานของระบบสารสนเทศ การประมวลผลกิจกรรมของระบบสารสนเทศ และเหตุการณ์ทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบถึงประสิทธิภาพความปลอดภัย และความผิดปกติ ที่เกิดจากการประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศ
การเฝ้าระวัง (Monitoring)	การเฝ้าระวังทางด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อตรวจสอบความผิดปกติจาก การประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศจากบันทึกเหตุการณ์ (Logs) เช่น การเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต การใช้งานสารสนเทศผิดวัตถุประสงค์ และปัญหาที่เกิดจากระบบงาน
ความเสี่ยง (Risk)	โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคต และมีผลกระทบ หรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์ และเป้าหมายของการให้บริการ
โปรแกรมที่ไม่พึงประสงค์ (Malicious Code or Malware)	โปรแกรม หรือ Code ที่เป็นอันตรายต่อประสิทธิภาพ และความปลอดภัยของระบบสารสนเทศไม่ทางใดก็ทางหนึ่ง เช่น ไวรัส (Virus), เวิร์ม (Worm) หรือโทรจัน (Trojan) เป็นต้น
แผนการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Plan)	การสร้างความต่อเนื่องทางธุรกิจ เพื่อป้องกันการติดขัด หรือการหยุดชะงักของระบบงานธุรกรรมที่สำคัญ ซึ่งอาจมีสาเหตุมาจาก

คำศัพท์	ความหมาย
	ภัยทางด้านสิ่งแวดล้อม เหตุการณ์ทางด้านความมั่นคงปลอดภัย หรือภัยคุกคามอื่นๆ
แผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRP: Disaster Recovery Plan)	การเตรียมความพร้อมรองรับเหตุฉุกเฉิน และแผนการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน เช่น การย้ายสถานที่ปฏิบัติงาน ไปจนถึงการใช้งานระบบสารสนเทศสำรอง
แผนสำหรับย้อนกลับสู่สภาวะเดิม (Fallback Plan)	แผนการดำเนินงานเพื่อใช้ในการกลับสู่สถานการณ์ดำเนินงานครั้งล่าสุด เพื่อใช้ในกรณีที่การแก้ไขเหตุฉุกเฉินไม่เป็นผลสำเร็จ
ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective: RTO)	ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อส่งมอบผลิตภัณฑ์ บริการ และกิจกรรม หรือกระบวนการกลับสู่สภาวะปกติหลังจากเกิดสถานการณ์ไม่พึงประสงค์ที่มีความเสียหายระดับรุนแรง
ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหายจากระบบได้ และเพื่อเป็นข้อมูลในการออกแบบวิธีการสำรองข้อมูลเพื่อให้ข้อมูลไม่สูญหายเกินกว่าที่กำหนดไว้
ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD)	ช่วงเวลาสูงสุดที่การดำเนินงานหยุดชะงัก หากเกินกำหนดช่วงเวลานี้แล้ว จะไม่สามารถทำให้การดำเนินงานฟื้นคืนสู่สภาพปกติได้
ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)	ข้อตกลงร่วมกันระหว่างผู้ให้บริการ และผู้รับบริการที่อธิบายถึงรายละเอียดการบริการ ระดับการให้บริการที่จะถูกวัด และประเมินผล เป้าหมายของระดับการให้บริการ รวมไปถึงระบุหน้าที่ความรับผิดชอบที่ชัดเจนของทั้งผู้ให้บริการ และผู้รับบริการ
ข้อตกลงการให้บริการ ระดับปฏิบัติงาน (Operational Level Agreement: OLA)	ข้อตกลงในการให้บริการ สำหรับปฏิบัติงานร่วมกันระหว่างหน่วยงานภายใน เพื่อสนับสนุนให้การบริการของผู้รับบริการเป็นไปตามข้อตกลงระดับการให้บริการ
สัญญาการให้บริการ (Underpinning Contracts: UC)	ข้อตกลงร่วมกันระหว่างผู้ให้บริการ และผู้ให้บริการ/ผู้จำหน่ายระบบ (Vendor) เพื่อให้บริการผู้รับบริการได้ตามข้อตกลงการให้บริการ (SLA)

คำศัพท์	ความหมาย
ระบบงานที่สำคัญ (High Priority Application System)	ระบบที่ให้บริการธุรกรรมหลักที่ใช้ในการให้บริการลูกค้า หรือระบบงานที่นำส่งข้อมูลรายงานแก่ทางราชการ
ระบบพัฒนา (Development Area)	ระบบสารสนเทศที่ใช้ในการพัฒนาระบบงาน โดยเป็นการจำลองทรัพยากร และสภาพแวดล้อมของระบบให้บริการจริงเพื่อใช้พัฒนาระบบงานใหม่
ระบบทดสอบ (User Acceptance Area)	ระบบสารสนเทศที่ใช้ในการทดสอบโดยเป็นการจำลองทรัพยากรและสภาพแวดล้อมของระบบให้บริการจริงมาเพื่อทดสอบประสิทธิภาพ และความปลอดภัยของระบบที่ได้พัฒนาขึ้น
ระบบสารสนเทศสำรอง (Disaster Recovery Center: DRC)	ระบบงาน ข้อมูล และระบบเครือข่ายสำรองนอกเหนือจากระบบสารสนเทศหลัก เพื่อให้สามารถทำธุรกรรมหลักได้อย่างต่อเนื่องและลดผลกระทบเมื่อเกิดเหตุการณ์ฉุกเฉิน
ระบบให้บริการจริง (Production Area)	ระบบสารสนเทศที่ให้บริการจริงแก่ผู้ใช้งาน ซึ่งต้องมีการรักษาความมั่นคงปลอดภัย และการควบคุมการเข้าถึงจากการพัฒนาระบบ และการทดสอบระบบอย่างเคร่งครัด
อุปกรณ์สื่อสารประเภทพกพา (Mobile Device)	เครื่องคอมพิวเตอร์พกพา (Laptop Computer) สมาร์ทโฟน (Smartphone) แท็บเล็ตคอมพิวเตอร์ (Tablet Computer) ที่องค์กรอนุญาตให้เชื่อมต่อ และใช้งานระบบสารสนเทศขององค์กรได้
สื่อบันทึกข้อมูล (Media)	อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Hard Drive หรือ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard drive เป็นต้น

หมวดที่ 4 บทบาท และความรับผิดชอบ

4.1 ประธานกรรมการบริษัท

4.1.1 อนุมัตินโยบายเทคโนโลยีสารสนเทศ รวมถึงการเปลี่ยนแปลงที่อาจจะมีขึ้น

4.1.2 อนุมัติเรื่องที่คณะกรรมการบริษัทนำเสนอ ซึ่งเกี่ยวข้องกับนโยบายเทคโนโลยีสารสนเทศ

4.1.3 รับผิดชอบโดยรวมในความมั่นคงปลอดภัยด้านสารสนเทศของทรัพย์สิน เพื่อให้มั่นใจว่านโยบายเทคโนโลยีสารสนเทศที่ถูกจัดทำขึ้นครอบคลุมสารสนเทศที่มีความสำคัญ การปฏิบัติสอดคล้องกับวัตถุประสงค์ทางธุรกิจขององค์กร และความต้องการของผู้ใช้งาน

4.2 ประธานเจ้าหน้าที่บริหาร กรรมการผู้จัดการใหญ่ และ ผู้ช่วยกรรมการผู้จัดการใหญ่

4.2.1 อนุมัติระเบียบปฏิบัติ รวมถึงการเปลี่ยนแปลงที่อาจจะมีขึ้น

4.2.2 กำหนดทิศทาง และให้การสนับสนุนในการจัดทำนโยบายเทคโนโลยีสารสนเทศ รวมถึงระเบียบปฏิบัติที่เกี่ยวข้อง

4.2.3 ตัดสินใจในการติดต่อกับหน่วยงานบังคับใช้กฎหมาย และหน่วยงานสืบสวน เมื่อมีข้อสงสัยว่ามีการกระทำผิดร้ายแรงเกิดขึ้น

4.2.4 อนุมัติ และสนับสนุนกิจกรรมโครงการความมั่นคงปลอดภัยด้านสารสนเทศ และเป็นหลักในการริเริ่มให้มีการสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4.2.5 ทบทวน สรุป และนำเสนอต่อประธานกรรมการบริษัท เพื่อขออนุมัติประกาศใช้นโยบายเทคโนโลยีสารสนเทศ รวมถึงการเปลี่ยนแปลงที่อาจจะมีขึ้น

4.3 ผู้บริหารระดับฝ่ายทุกฝ่ายงาน

4.3.1 กำหนดผู้รับผิดชอบต่อทรัพย์สิน และวิเคราะห์ความเสี่ยงของทรัพย์สิน รวมถึงบริหารจัดการทรัพย์สินที่อยู่ภายใต้การดูแลให้คงสภาพ ป้องกันความลับ ความสมบูรณ์ครบถ้วน และความพร้อมใช้งานของทรัพย์สินนั้นๆ

4.3.2 กำหนดบทบาทหน้าที่ และความรับผิดชอบ ในการปฏิบัติงานด้านความมั่นคงปลอดภัยของบุคลากรโดยยึดถือตามนโยบายเทคโนโลยีสารสนเทศที่กำหนดไว้

4.3.3 กำหนดให้มีการให้ความรู้ในเรื่องของนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้องต่อบุคลากรภายในองค์กร และหน่วยงานภายนอกที่เกี่ยวข้อง

4.3.4 กำหนดความสำคัญ การริเริ่ม และลงมือปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศ เพื่อให้บุคลากรในหน่วยงานปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศ อาทิ การกำหนดวิธีการตรวจสภาพแวดล้อมของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

4.3.5 ทบทวน และอนุมัติความต้องการด้านความมั่นคงปลอดภัยของระบบ ที่จะนำไปใช้กับข้อมูลสารสนเทศที่มีความอ่อนไหว (Sensitive) หรือสำคัญมากต่อการปฏิบัติงานทางธุรกิจ ก่อนเริ่มต้นพัฒนาโครงการ (Project Development)

4.3.6 กำกับดูแลให้มีการจัดทำสัญญาข้อตกลงการรักษาความลับขององค์กร ต่อบุคลากรภายในองค์กร และหน่วยงานภายนอกที่เกี่ยวข้อง โดยระบุความต้องการเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติที่อาจส่งผลต่อการละเมิดสัญญาข้อตกลงต่างๆ

4.3.7 ชี้แจงการเปลี่ยนแปลงที่อาจจะมีขึ้น ที่ส่งผลต่อการปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติในส่วนงานที่รับผิดชอบ

4.3.8 ตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นเหตุการณ์ที่มีผลกระทบด้านลบต่อหน่วยงาน หรือทั้งองค์กร อาทิ เหตุการณ์ที่มีผลอย่างยิ่งต่อภาพพจน์ขององค์กร ความเชื่อมั่นของลูกค้า การดำเนินการขององค์กร โดยต้องรายงานต่อ กรรมการผู้จัดการใหญ่ ผู้ช่วยกรรมการผู้จัดการใหญ่ และประธานเจ้าหน้าที่บริหาร

4.3.9 ให้การสนับสนุนในการสืบสวน และเสนอแนวทางแก้ไขต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น

4.4 ส่วนเพิ่มเติมเฉพาะผู้บริหารระดับฝ่ายเทคโนโลยีสารสนเทศ

4.4.1 วิเคราะห์ ประเมินผล และสรุปผลประเด็นที่มีการกระทบขั้นรุนแรงต่อองค์กร อาทิ สัญญากับผู้ขาย หรือผู้ให้บริการ ผู้ซึ่งฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร การขาย จำหน่าย จ่าย แจก หรือการถ่ายโอนซอฟต์แวร์ขององค์กร รวมทั้งทรัพย์สินทางปัญญาไปยังบุคคลอื่น การเปิดเผยข้อมูลสารสนเทศที่สำคัญ การเปลี่ยนแปลงที่สำคัญต่อเว็บไซต์ขององค์กร เป็นต้น พร้อมทั้งนำเสนอต่อประธานเจ้าหน้าที่บริหาร และกรรมการผู้จัดการใหญ่ และผู้ช่วยกรรมการผู้จัดการใหญ่ เพื่อรับทราบและพิจารณาแนวทางบริหารจัดการต่อไป

4.4.2 กำกับให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารเทศอย่างเป็นแบบแผน และมีการนำกระบวนการวิเคราะห์ผลกระทบธุรกิจมาใช้

4.4.3 พิจารณาคัดเลือกบุคคลผู้ที่เกี่ยวข้องกับการดำเนินการในการติดต่อกับหน่วยงาน บังคับใช้กฎหมาย และหน่วยงานสอบสวน เมื่อมีข้อสงสัยว่ามีการกระทำผิดร้ายแรงเกิดขึ้น และนำเสนอต่อประธานเจ้าหน้าที่บริหาร กรรมการผู้จัดการใหญ่ และผู้ช่วยกรรมการผู้จัดการใหญ่

4.4.4 นำเสนอนโยบายเทคโนโลยีสารสนเทศรวมถึงรายงานการเปลี่ยนแปลงนโยบายที่เกิดขึ้น ต่อประธานเจ้าหน้าที่บริหาร กรรมการผู้จัดการใหญ่ และผู้ช่วยกรรมการผู้จัดการใหญ่

4.4.5 ให้คำแนะนำแก่กลุ่มบุคคลที่เหมาะสม ในเรื่องการวัดผล เพื่อปรับปรุงกระบวนการที่เกี่ยวข้องกับการให้บริการ และการรักษาด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงการควบคุมให้ดีขึ้น

4.4.6 ทบทวน และอนุมัติความต้องการที่จำเป็นในการใช้ซอฟต์แวร์ขององค์กร และการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่จะต้องใช้กับข้อมูลสารสนเทศ ที่มีความอ่อนไหว หรือสำคัญต่อการปฏิบัติงานในเชิงธุรกิจ ก่อนเริ่มต้นออกแบบโครงการด้านเทคโนโลยีสารสนเทศ

4.4.7 ทบทวน และอนุมัติการดำเนินกิจกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศในระดับหน่วยงาน ซึ่งอาจมีผลกระทบในระดับองค์กรได้

4.5 เจ้าของทรัพย์สิน

4.5.1 กำหนดลำดับชั้นความลับของข้อมูลตามความสำคัญของข้อมูลต่อองค์กร พร้อมทั้งแจ้งให้ผู้เกี่ยวข้องรับทราบ ในการเปลี่ยนแปลงลำดับชั้นความลับข้อมูลที่เกิดขึ้น

4.5.2 พัฒนา และปรับปรุงโครงสร้างการแบ่งลำดับชั้นความลับข้อมูล และข้อกำหนดในการบริหารจัดการตามลำดับชั้นความลับ

4.5.3 ระบุกฎเกณฑ์การกำหนดสิทธิในการเข้าถึงข้อมูล และทรัพย์สิน เช่น บทบาทของผู้ใช้งาน แนวทางในการขออนุมัติเข้าถึงทรัพย์สิน เป็นต้น พร้อมทั้งแจ้งให้กลุ่มผู้เกี่ยวข้องรับทราบในการเปลี่ยนแปลงกฎเกณฑ์ที่เกิดขึ้น

4.5.4 ประเมินความเสี่ยง และหาแนวทางการควบคุมที่เป็นมาตรฐาน ในกรณีที่ความจำเป็นทางธุรกิจไม่สอดคล้องกับนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติ หรือมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อควบคุมให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ หรือเพื่อไม่ให้ความเสี่ยงอยู่ในระดับที่สูงขึ้น

4.6 ผู้ดูแลระบบ

4.6.1 พัฒนา และจัดทำเอกสารกระบวนการสนับสนุนแนวทาง และขั้นตอนการปฏิบัติงาน เพื่อให้แน่ใจว่าสอดคล้องตามนโยบายเทคโนโลยีสารสนเทศ

4.6.2 ควบคุม ดูแลระบบสารสนเทศให้คงสภาพการรักษาความลับ ความสมบูรณ์ครบถ้วน และความพร้อมใช้ของทรัพย์สินที่ให้บริการระบบสารสนเทศ ซึ่งอยู่ภายใต้การดูแล และควบคุมการเข้าถึงทรัพย์สิน เพื่อเป็นการปกป้องทรัพย์สินอย่างเหมาะสม

4.6.3 เตรียมการช่วยเหลือทางด้านเทคนิคแก่ผู้เป็นเจ้าของทรัพย์สิน เพื่อนำเอาการควบคุมที่เหมาะสมมาใช้ในการดูแลทรัพย์สิน

4.6.4 กำหนดกลไกการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และตรวจสอบการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอเพื่อป้องกันการบุกรุกระบบสารสนเทศอย่างทันท่วงที

4.6.5 ให้ความช่วยเหลือในการคัดเลือก และประเมินด้านความมั่นคงปลอดภัยสารสนเทศ ในส่วนที่เกี่ยวข้องกับฮาร์ดแวร์ และ/หรือซอฟต์แวร์ที่นำมาใช้งานในองค์กร

4.6.6 แจ้งให้เจ้าของทรัพย์สิน และผู้ที่เกี่ยวข้องรับทราบในกรณีที่พบ หรือสงสัยว่าทรัพย์สินที่ให้บริการระบบสารสนเทศขององค์กรถูกคุกคาม สูญเสีย หรือเสียหาย รวมทั้งกรณีที่มีการละเมิดต่อนโยบายเทคโนโลยีสารสนเทศ หรือระเบียบปฏิบัติที่เกี่ยวข้อง

4.6.7 ตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และช่วยเหลือในการสอบสวน รวมถึงแก้ไขปัญหาในส่วนที่ทราบ หรือสงสัยว่าทรัพย์สินขององค์กรถูกคุกคาม หรือเหตุการณ์ที่ต้องสงสัยว่ามีการโจมตีระบบรักษาความมั่นคงปลอดภัยสารสนเทศ หรือเป็นการกระทำที่ไม่เหมาะสม และแจ้งผลลัพธ์ให้เจ้าของทรัพย์สิน และผู้ที่เกี่ยวข้องรับทราบ

4.7 ผู้พัฒนาระบบ

4.7.1 ยึดมั่นถึงความต้องการที่ระบุไว้ในนโยบายเทคโนโลยีสารสนเทศ และกฎระเบียบ หรือมาตรฐานที่เกี่ยวข้องในการพัฒนาระบบ โดยประกอบไปด้วยการออกแบบ การพัฒนา การนำเอาระบบมาใช้งาน และการบำรุงรักษาระบบ เพื่อให้มั่นใจว่ามีการปฏิบัติที่เหมาะสมในการควบคุมการพัฒนาระบบที่เพียงพอ

4.8 ส่วนบริหารกลยุทธ์เทคโนโลยีสารสนเทศ

4.8.1 พัฒนา และปรับปรุงนโยบายเทคโนโลยีสารสนเทศให้เป็นปัจจุบัน และสอดคล้องต่อการดำเนินงานธุรกิจ รวมถึงกฎหมาย หรือข้อกำหนดที่เกี่ยวข้อง

4.8.2 พัฒนา และปรับปรุงระเบียบปฏิบัติ หรือขั้นตอนการปฏิบัติงานที่มีความสอดคล้องกับนโยบายเทคโนโลยีสารสนเทศ และมาตรฐานสากล

4.8.3 นำเสนอการปรับปรุงนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติต่อผู้บริหารระดับฝ่ายเทคโนโลยีสารสนเทศ เพื่อพิจารณาเห็นชอบ และนำเสนอขออนุมัติต่อไป

4.8.4 เผยแพร่ให้ผู้ใช้งานทราบถึงนโยบายเทคโนโลยีสารสนเทศขององค์กร และระเบียบปฏิบัติที่เกี่ยวข้อง

4.8.5 เผยแพร่ให้ผู้ใช้งานทราบถึงการตรวจสอบระบบ และการตรวจสอบกิจกรรมทางเครือข่าย

4.8.6 จัดเตรียมแนวทางการติดตามการบังคับใช้นโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติ เพื่อให้มั่นใจว่าผู้ใช้งานระบบสารสนเทศทุกคนมีความตระหนักถึงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร กฎหมายทรัพย์สินทางปัญญา และบทบัญญัติอื่นๆ ที่บังคับใช้อยู่ในปัจจุบัน

4.9 ส่วนกฎหมาย

4.9.1 ให้ข้อแนะนำทางกฎหมายที่เกี่ยวข้องกับระเบียบ วิธีการปฏิบัติสำหรับการตรวจสอบการใช้ระบบสารสนเทศ ให้ข้อแนะนำทางกฎหมายที่เกี่ยวข้องกับระเบียบ วิธีการปฏิบัติสำหรับการตรวจสอบการใช้ระบบสารสนเทศ

4.10 ส่วนตรวจสอบระบบงาน

4.10.1 สอบทานการนำนโยบายเทคโนโลยีสารสนเทศมาใช้ และประเมินผลการปฏิบัติตามนโยบาย ระเบียบปฏิบัติ และขั้นตอนปฏิบัติงานที่เกี่ยวข้อง รวมถึงประสิทธิภาพของนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนวัดผลการควบคุมภายใน โดยถือเป็นส่วนหนึ่งของตารางการตรวจสอบเป็นประจำ และรายงานผลการตรวจสอบภายในไปยังผู้บริหารที่เกี่ยวข้องได้รับทราบเพื่อพิจารณาดำเนินการ

4.11 ผู้ใช้งาน

4.11.1 ทำความเข้าใจกับนโยบาย ระเบียบปฏิบัติ และขั้นตอนปฏิบัติงานต่างๆ ที่องค์กร หรือหน่วยงานได้กำหนดไว้ รวมถึงให้ความร่วมมือในการใช้กฎข้อบังคับต่างๆ

4.11.2 ลงนามยินยอม และปฏิบัติตามข้อตกลงไม่เปิดเผยความลับขององค์กร

4.11.3 ใช้ทรัพย์สินขององค์กรอย่างทะนุถนอม ดูแลให้คงสภาพสมบูรณ์ มีประสิทธิภาพ มีจริยธรรม และถูกต้องตามกฎหมาย

4.11.4 รายงานเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศแก่ผู้บังคับบัญชา และฝ่ายเทคโนโลยีสารสนเทศ ให้ทราบโดยทันที และช่วยเหลือในการสนองตอบต่อเหตุการณ์เหล่านั้น

4.12 หน่วยงานภายนอก

4.12.1 ลงนาม และปฏิบัติตามข้อตกลง ไม่เปิดเผยความลับขององค์กร

4.12.2 ยึดถือการปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศขององค์กรต่อการให้บริการของบุคคลที่สาม และกระทำการใดตามความจำเป็นเพื่อป้องกันความลับของข้อมูลสารสนเทศ และระบบต่างๆ ที่องค์กรจัดเตรียมไว้เพื่อใช้งาน

4.12.3 เข้าถึงระบบสารสนเทศเฉพาะสิทธิที่ได้รับเท่านั้น

4.12.4 ข้อมูลสารสนเทศที่ได้รับจากการเก็บรวบรวม หรือเข้าถึงในระหว่างที่มีการทำงานกับองค์กร ให้ถือเป็นความลับ ห้ามทำการใดๆ อันเกี่ยวข้องกับการใช้การเปิดเผย ส่ง หรือแก้ไขข้อมูลสารสนเทศที่ได้มา โดยไม่มีการยินยอมอย่างชัดเจนจากหน่วยงานขององค์กรที่ทำหน้าที่กำกับดูแลการดำเนินงาน

4.12.5 รายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นทันที ให้แก่หน่วยงานขององค์กรที่ทำหน้าที่กำกับดูแลการดำเนินงาน และฝ่ายเทคโนโลยีสารสนเทศ รวมถึงช่วยเหลือการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

หมวดที่ 5 นโยบายการบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ

5.1 การบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ และลดความผิดพลาดในการดำเนินการเปลี่ยนแปลง รวมถึงระบบงานสามารถสนับสนุนธุรกิจขององค์กรได้อย่างต่อเนื่อง และมีประสิทธิภาพ

5.1.1 ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการกำหนดประเภทของการเปลี่ยนแปลง (Change Type) เพื่อใช้ในการดำเนินการบันทึก จำแนกประเภท ประเมิน และกำหนดผู้อนุมัติสำหรับคำร้องขอการเปลี่ยนแปลง โดยผู้มีอำนาจอนุมัตินั้นให้หมายถึง ผู้บริหารระดับฝ่ายขึ้นไป หรือผู้ที่ได้รับมอบหมายให้มีอำนาจอนุมัติ

5.1.2 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ และให้บันทึกการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร

5.1.3 ผู้ใช้งาน ผู้ที่ร้องขอ และผู้ดำเนินการเปลี่ยนแปลง ต้องดำเนินการวิเคราะห์ผลกระทบ และความเสี่ยงในการดำเนินการเปลี่ยนแปลง เพื่อเตรียมมาตรการรองรับการเปลี่ยนแปลงในแต่ละกิจกรรม

5.1.4 ผู้ใช้งาน และผู้ที่ร้องขอให้มีการเปลี่ยนแปลงจะต้องดำเนินการจัดทำเอกสารรายละเอียดความต้องการเปลี่ยนแปลง ส่วนผู้ดำเนินการเปลี่ยนแปลงจะต้องจัดทำแผนงานภาพรวม สำหรับการดำเนินการการเปลี่ยนแปลง โดยกำหนดวันเวลาที่ต้องการดำเนินงาน และทรัพยากรที่จำเป็น เป็นต้น และแจ้งให้ผู้ที่เกี่ยวข้องรับทราบถึงแผนการเปลี่ยนแปลง

5.1.5 ผู้ดำเนินการเปลี่ยนแปลงต้องจัดทำแผนสำหรับย้อนกลับสู่สภาวะเดิม (Fallback Plan) เพื่อใช้สำหรับแก้ไขการเปลี่ยนแปลง เมื่อต้องการให้กลับสู่สภาวะเดิม หากการเปลี่ยนแปลงไม่สามารถทำได้สำเร็จตามวัตถุประสงค์ที่ต้องการ

5.2 การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

วัตถุประสงค์

เพื่อกำหนดแนวทางการบริหารจัดการความต่อเนื่องในการให้บริการระบบสารสนเทศ ในกรณีที่เกิดเหตุฉุกเฉิน หรือเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศใดๆ ซึ่งอาจส่งผลกระทบให้การดำเนินธุรกิจขององค์กรหยุดชะงัก

5.2.1 องค์กรต้องจัดให้มีเครื่องคอมพิวเตอร์สำรอง และระบบสารสนเทศสำรอง เพื่อรองรับการดำเนินธุรกิจ ได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลให้การดำเนินธุรกิจหยุดชะงัก โดยมีผู้บริหารระดับสูงสุดขององค์กรเป็นผู้มีอำนาจตัดสินใจในการสั่งการ

5.2.2 หน่วยงานผู้ใช้บริการ และฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยง และบันทึกความเสี่ยงที่อาจส่งผลให้การให้บริการระบบสารสนเทศขาดความต่อเนื่อง และทำข้อตกลงเงื่อนไขความต้องการ ได้แก่ ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD) หรือระยะเวลาเป้าหมายในการคืนสภาพ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery point objective: RPO) อย่างเป็นลายลักษณ์อักษร

5.2.3 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน (Disaster Recovery Plan: DRP) โดยให้มีความสอดคล้องกับแผนการบริหารจัดการความต่อเนื่องทางธุรกิจขององค์กร

5.2.4 ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการสำรองข้อมูล เอกสาร ซอฟต์แวร์ และระบบงาน รวมถึงอุปกรณ์ต่างๆ และบุคลากรที่จำเป็น เพื่อสนับสนุนให้การกู้คืนระบบสารสนเทศให้เป็นไปอย่างรวดเร็วที่สุด หลังจากเกิดการหยุดชะงักในการให้บริการ หรือเกิดเหตุจากภัยพิบัติ

5.3 การบริหารจัดการเหตุขัดข้อง และการบริหารจัดการคำร้องขอ (Incident and Service Request Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางจัดการกับสิ่งผิดปกติที่เกิดขึ้น แก้ไขเหตุขัดข้อง การจัดหา และการจัดการระบบงานคอมพิวเตอร์ขององค์กรให้สามารถสนับสนุนการให้ให้สามารถกลับคืนสู่สภาวะปกติให้ได้เร็วที่สุด ทั้งนี้การแก้ไขปัญหาต้องอยู่ในขอบเขตของความถูกต้อง และมีประสิทธิภาพ

5.3.1 การบริหารจัดการเหตุขัดข้อง

5.3.1.1 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการกำหนดเกณฑ์ในการวัดระดับผลกระทบ (Impact) ความเร่งด่วน (Urgency) และลำดับความสำคัญ (Priority) ของเหตุขัดข้อง

5.3.1.2 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบในการแก้ไขเหตุขัดข้อง และบริหารจัดการความสำคัญของคำร้องขอ เพื่อให้การดำเนินงานเป็นไปได้อย่างต่อเนื่อง

5.3.1.3 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการบันทึกรายละเอียดของเหตุขัดข้อง และคำร้องขอให้ครบถ้วนตามขั้นตอนปฏิบัติงานที่ระบุไว้ เพื่อใช้เป็นหลักฐาน และใช้ประกอบการวิเคราะห์ หาวิธีการแก้ไข และรายงานผลการดำเนินงานต่อไป

5.3.1.4 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการแก้ไขเหตุขัดข้อง และคำร้องขอที่ได้รับแจ้งมาอย่างรวดเร็ว เต็มความสามารถ ให้สอดคล้องกับข้อตกลงการให้บริการที่ได้กำหนดไว้

5.3.1.5 กรณีที่ผู้รับเรื่องไม่สามารถแก้ไขเหตุขัดข้อง และคำร้องขอได้ด้วยตนเองจะต้องยกระดับการให้บริการ (Escalation) ไปยังผู้เกี่ยวข้องตามลำดับ เพื่อเพิ่มประสิทธิภาพ และความรวดเร็วในการดำเนินงาน

5.3.2 การบริหารจัดการคำร้องขอ

5.3.2.1 หน่วยงานที่ต้องการให้มีการจัดหาคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือโปรแกรมสำเร็จรูป เช่น โปรแกรม Microsoft Office จะต้องระบุรายละเอียดที่ต้องการ ลักษณะงานที่นำไปใช้ โดยให้มีการบันทึกเป็นลายลักษณ์อักษรลงในเอกสารแบบฟอร์ม หรือระบบของหน่วยงานเทคโนโลยีสารสนเทศเพื่อขออนุมัติงบประมาณของหน่วยงานในการจัดหา และได้รับการอนุมัติเบื้องต้นจากผู้บริหารระดับแผนกขึ้นไป และอ้างอิงการอนุมัติตามประกาศตารางอนุมัติของแต่ละบริษัท รวมทั้งฝ่ายเทคโนโลยีสารสนเทศด้วย

5.3.2.2 หน่วยงานที่ต้องการให้มีการจัดหา หรือพัฒนาระบบงานคอมพิวเตอร์ ต้องระบุความต้องการระบบงานคอมพิวเตอร์ของแต่ละหน่วยงาน รวมทั้งจัดทำเป็นโครงการ และขออนุมัติงบประมาณในการจัดทำโครงการ โดยให้มีการบันทึกเป็นลายลักษณ์อักษร และได้รับการอนุมัติจากผู้บริหารระดับฝ่ายขึ้นไป รวมทั้งฝ่ายเทคโนโลยีสารสนเทศด้วย

5.3.2.3 ฝ่ายเทคโนโลยีสารสนเทศต้องให้การสนับสนุนด้านข้อมูลที่เกี่ยวข้องกับการจัดหาระบบงานคอมพิวเตอร์ เช่น คุณสมบัติของเครื่องคอมพิวเตอร์ หน่วยงานภายนอก ข้อมูลความมั่นคงปลอดภัยด้านสารสนเทศ หรือข้อมูลอื่นใดที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศตามที่ได้รับการร้องขอ

5.4 การจัดการระดับการให้บริการ (Service Level Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการจัดทำข้อตกลงสำหรับระดับการให้บริการด้านเทคโนโลยีสารสนเทศ ระหว่างฝ่ายเทคโนโลยีสารสนเทศ และผู้ใช้งานระบบสารสนเทศขององค์กร ให้อยู่ในเกณฑ์ที่สามารถยอมรับได้

5.4.1 องค์กรต้องกำหนดให้มีการจัดทำสัญญาที่ระบุถึงข้อตกลงระดับการให้บริการดังต่อไปนี้

5.4.1.1 ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ระหว่างหน่วยงานผู้ให้บริการ และผู้ใช้งาน

5.4.1.2 สัญญาการให้บริการ (Underpinning Contracts: UC) ระหว่างหน่วยงานผู้ให้บริการ และหน่วยงานภายนอก

5.4.2 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำข้อตกลงการให้บริการระหว่างฝ่ายเทคโนโลยีสารสนเทศ และผู้ใช้งาน ทั้งนี้ข้อตกลงการให้บริการต้องได้รับการอนุมัติอย่างเป็นทางการจากผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ และตัวแทนผู้บริหารจากหน่วยงานต่างๆ ภายในองค์กร

5.4.3 ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ ให้สอดคล้องกับสัญญาข้อตกลงการให้บริการ

5.4.4 ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการตรวจสอบวิเคราะห์ประสิทธิภาพการทำงาน แนวโน้มของการให้บริการเป็นระยะตามความเหมาะสม และนำมาแก้ไขปรับปรุงเพื่อเพิ่มประสิทธิภาพในการดำเนินงานต่อไป

5.4.5 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำเอกสาร หรือรายงานการให้บริการ (Service Catalogue) ที่ให้บริการอยู่ในปัจจุบัน โดยครอบคลุมทุกๆ การให้บริการที่อยู่ในข้อตกลงการให้บริการ ซึ่งได้รับการยอมรับเงื่อนไขการให้บริการจากตัวแทนผู้บริหารของหน่วยงานต่างๆ ภายในองค์กร

5.4.6 การแก้ไขเอกสารใดๆ ที่เกี่ยวข้องกับความต้องการด้านการให้บริการ (Service Requirement) ระดับการให้บริการ (Service Level Agreement) หรือรายละเอียดการให้บริการ (Service Catalogue) ต้องถูกดำเนินการผ่านการบริหารจัดการการเปลี่ยนแปลง (Change Management) ที่องค์กรกำหนดไว้

5.5 การจัดการด้านงบประมาณ และการควบคุมการใช้จ่ายของการให้บริการ (Budgeting and Accounting for Services Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบริหารจัดการงบประมาณ และควบคุมค่าใช้จ่ายที่เกี่ยวข้องกับการสนับสนุนการให้บริการด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

5.5.1 ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการจัดสรรงบประมาณให้ครบถ้วน และเพียงพอต่อการให้บริการและควบคุมการใช้จ่ายงบประมาณให้เกิดประสิทธิภาพสูงสุด

5.5.2 ฝ่ายเทคโนโลยีสารสนเทศ และผู้ที่เกี่ยวข้อง ต้องจัดให้มีการจัดสรรงบประมาณจะต้องพิจารณาต้นทุนทางตรง (Direct Cost) ต้นทุนทางอ้อม (Indirect Cost) ค่าใช้จ่ายของการจัดซื้อทรัพย์สินสารสนเทศ (IT Asset) ค่าใช้จ่ายจากการใช้ทรัพยากรร่วมกัน (Shared Resource Cost) ค่าใช้จ่ายประจำสำนักงาน (General and Administrative Expense) ค่าใช้จ่ายในการจัดจ้างหน่วยงานภายนอก (Externally Supplied Service Cost) ค่าใช้จ่ายของการจัดจ้างบุคลากร (People) ค่าใช้จ่ายของการทำประกัน (Insurance Expense) ค่าใช้จ่ายในการบำรุงรักษา (Maintenance Expense) และค่าใช้จ่ายด้านลิขสิทธิ์ต่างๆ (License Expense) รวมถึงค่าใช้จ่ายอื่นๆ ที่เกี่ยวข้องในการให้บริการ

5.6 การบริหารข้อมูลสารสนเทศเพื่อรายงานผลการให้บริการ (Service Reporting Policy)

วัตถุประสงค์

เพื่อให้บริการด้านข้อมูลสำหรับจัดทำรายงานให้กับผู้บริหาร รวมถึงสนับสนุนให้รายงานต่างๆ มีข้อมูลที่ถูกต้องครบถ้วน และให้ผู้ที่เกี่ยวข้องสามารถใช้งานได้ข้อมูลได้อย่างถูกต้อง

5.6.1 การจัดหา และบำรุงรักษาแหล่งข้อมูลเพื่อรายงานผู้บริหาร

5.6.1.1 ส่วนงานภายในองค์กร ต้องจัดให้มีรายงานผลการดำเนินงาน และข้อมูลต่างๆ ที่เป็นประโยชน์ต่อการดำเนินธุรกิจแก่ผู้บริหาร เพื่อให้ผู้บริหารใช้เป็นข้อมูลในการตัดสินใจต่อการดำเนินงานได้อย่างรวดเร็วและทันเวลา

5.6.1.2 ฝ่ายเทคโนโลยีสารสนเทศ ต้องบำรุงรักษาแหล่งข้อมูล และผลการดำเนินงาน และข้อมูลต่างๆ ที่ใช้สำหรับรายงานผู้บริหารให้คงสภาพความถูกต้อง และพร้อมใช้อยู่เสมอ

5.6.2 การจัดพิมพ์รายงาน

5.6.2.1 มีการระบุชื่อผู้จัดพิมพ์, วันที่และเวลาในการพิมพ์รายงาน พร้อมทั้งเก็บ Log การจัดพิมพ์ และ Export ข้อมูล นอกจากนี้ควรทำลายรายงานที่ไม่ได้ใช้งานแล้ว

5.6.3 การเข้าถึงข้อมูลในแหล่งข้อมูล

5.6.3.1 ผู้ใช้งานต้องร้องขอสิทธิ์การใช้งานข้อมูลในแหล่งข้อมูล จากส่วนงานซึ่งเป็นเจ้าของข้อมูลก่อนเข้าถึงแหล่งข้อมูลต่างๆ โดยกำหนดกลุ่มของผู้มีสิทธิ์ใช้งานตามขอบเขตข้อมูลเป็น 3 ระดับ ดังนี้

ก.) เข้าถึงข้อมูลทุกฝ่าย/แผนก

ข.) เข้าถึงข้อมูลเฉพาะฝ่าย/แผนก

ค.) เข้าถึงข้อมูลเฉพาะเรื่องที่เกี่ยวข้อง

5.6.4 การควบคุมคุณภาพของข้อมูลในแหล่งข้อมูล

5.6.4.1 กรณีที่ผู้ใช้งานต้องการเปลี่ยนแปลงข้อมูลในแหล่งข้อมูล ผู้ใช้งานต้องจัดเตรียมข้อมูลตามกระบวนการทำข้อมูลให้มีความสมบูรณ์ (Data Cleaning) และแจ้งขอดำเนินการเปลี่ยนแปลงข้อมูลเป็นลายลักษณ์อักษร และส่งมายังฝ่ายเทคโนโลยีสารสนเทศ เพื่อให้เจ้าหน้าที่เทคโนโลยีสารสนเทศดำเนินการปรับปรุงข้อมูลในฐานข้อมูล

5.7 การให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น (IT Insourcing) และการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)

วัตถุประสงค์

เพื่อจัดทำข้อกำหนดต่างๆ และกรอบการปฏิบัติงานในการให้บริการ หรือการใช้บริการด้านงานเทคโนโลยีสารสนเทศขององค์กรให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเกิดผลประโยชน์สูงสุดแก่องค์กร

5.7.1 การให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น (IT Insourcing)

5.7.1.1 ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุม และกำกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจขององค์กร โดยฝ่ายเทคโนโลยีสารสนเทศจะให้บริการทางเทคโนโลยีสารสนเทศภายในองค์กร และบริษัทย่อยเท่านั้น

5.7.1.2 ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการคิดค่าบริการ และค่าธรรมเนียม โดยการคิดค่าบริการและค่าธรรมเนียม ต้องได้รับการตกลงร่วมกันระหว่างผู้ให้บริการ และผู้ใช้บริการ และสามารถอธิบายที่มาของค่าธรรมเนียม รวมถึงค่าบริการได้ชัดเจน และโปร่งใส

5.7.1.3 ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมภายใน และจัดทำขั้นตอนการปฏิบัติงาน (Operation Procedure Manual) โดยให้มีการแบ่งแยกอำนาจหน้าที่ของผู้ปฏิบัติงาน (Segregation of Duty) ตามโครงสร้างผู้ปฏิบัติงานที่ชัดเจน

5.7.1.4 ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีมาตรการรองรับเหตุฉุกเฉิน โดยจัดให้มีแผนการรองรับเหตุฉุกเฉิน และการสำรองข้อมูล รวมถึงกำหนดรอบการสำรองข้อมูลตามที่ตกลงกันไว้กับผู้รับบริการ

5.7.1.5 ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการสำรองข้อมูลโดยใช้สื่อบันทึกข้อมูล และเก็บสื่อบันทึกข้อมูลในสถานที่ที่ผู้รับบริการจัดหา และเตรียมไว้ให้เป็นการเฉพาะ หรือสถานที่ที่ได้ตกลงไว้ร่วมกัน รวมถึงไม่นำข้อมูลการให้บริการของผู้รับบริการไปเผยแพร่ หรือนำไปใช้กับบุคคลภายนอก

5.7.1.6 องค์กร ต้องกำหนดให้ผู้ให้บริการมีการบริหารการจัดการระดับการให้บริการตามนโยบายที่กำหนดไว้ในข้อ 5.4 การจัดการระดับการให้บริการ (Service Level Management Policy)

5.7.2 การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing) การจัดหาผู้ให้บริการภายนอกเพื่อให้บริการงานด้านเทคโนโลยีสารสนเทศ ต้องพิจารณาให้มีความสอดคล้องกับกลยุทธ์ทางธุรกิจขององค์กร และคำนึงถึงการให้บริการแก่ลูกค้าอย่างต่อเนื่อง และมีความถูกต้องน่าเชื่อถือ โดยมีหลักเกณฑ์เบื้องต้นในการใช้บริการจากผู้ให้บริการภายนอก ดังนี้

5.7.2.1 หลักเกณฑ์ในการพิจารณาการใช้บริการจากผู้ให้บริการภายนอก ต้องไม่ขัดแย้งกับกฎระเบียบ หรือข้อกำหนดที่หน่วยงานราชการประกาศใช้

5.7.2.2 แนวทางในการพิจารณาคัดเลือกผู้ให้บริการเพื่อประเมินถึงความน่าเชื่อถือของการให้บริการ และเพื่อให้แน่ใจว่าผู้ให้บริการมีความสามารถในการให้บริการลูกค้าได้ตามข้อตกลงการให้บริการ

5.7.2.3 แนวทางในการรักษาความมั่นคงปลอดภัย และรักษาความลับของข้อมูล เพื่อให้แน่ใจว่าได้ดูแล และรับผิดชอบต่อลูกค้า และมีการคุ้มครองผู้บริโภค (Customer Protection) อย่างเหมาะสม

5.7.2.4 การติดตาม การประเมินผล และการตรวจสอบการให้บริการจากบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้เป็นไปตามวัตถุประสงค์ และเป้าหมายที่กำหนดไว้

5.7.2.5 กำหนดให้มีแนวทางการบริหารความเสี่ยงจากการใช้บริการจากบุคคลภายนอก สำหรับความเสี่ยงด้านปฏิบัติการ (Operational risk) ความเสี่ยงด้านกลยุทธ์ (Strategic risk) ความเสี่ยงด้านชื่อเสียง (Reputational risk) และความเสี่ยงด้านกฎหมาย (Legal risk) โดยกำหนดแนวทางการบริหารความ

เสี่ยงจากการใช้บริการบุคคลภายนอก เพื่อใช้บริการด้านเทคโนโลยีสารสนเทศไว้อย่างชัดเจน และเป็นลายลักษณ์อักษร ให้เหมาะสมกับความสำคัญของระบบงานที่ใช้บริการจากบุคคลภายนอก และสอดคล้องกับนโยบายการบริหารความเสี่ยงโดยรวม รวมทั้งสื่อสารให้บุคคลที่เกี่ยวข้องเข้าใจ และถือปฏิบัติตามแนวทางที่กำหนดไว้

5.7.2.6 ห้ามผู้ให้บริการภายนอกใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์มาใช้ในการดำเนินงานของบริษัท และให้ทางผู้ให้บริการภายนอกลงนามเป็นลายลักษณ์อักษรเพื่อเป็นการยืนยันว่าจะไม่ใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ให้กับทางบริษัท

หมวดที่ 6 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

6.1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

(Information Security Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางไว้เป็นกรอบ และเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐาน สร้างความมั่นใจถึงความมีประสิทธิผล และประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศขององค์กร รวมถึงการดำเนินการที่สอดคล้องตามข้อกำหนดด้านระบบความมั่นคงปลอดภัยของทั้งองค์กร ข้อกฎหมาย และระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้องด้วย อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว เป็นแนวทางปฏิบัติของผู้ใช้งานระบบสารสนเทศขององค์กร โดยมีแนวทางปฏิบัติดังนี้

6.1.1 ทิศทางการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Management Directions for Information Security)

6.1.1.1 นโยบายสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Policy for Information Security)

ก.) องค์กรต้องจัดให้มีนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากประธานกรรมการบริษัท หรือผู้บริหารระดับสูง ที่ประธานกรรมการบริษัทมอบหมายให้เป็นผู้อนุมัติ

ข.) องค์กรต้องเผยแพร่นโยบายดังกล่าวให้ผู้ใช้งาน และหน่วยงานที่เกี่ยวข้องได้รับทราบ และถือปฏิบัติเป็นไปตามที่นโยบายกำหนด โดยการเผยแพร่ต้องดำเนินการในลักษณะที่ผู้ใช้งานเข้าถึงได้ง่าย

6.1.1.2 การทบทวนนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Review of the Policies for Information Security)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการตรวจสอบ และทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามเงื่อนไขที่กำหนดไว้ในข้อที่ 2.5 การทบทวนนโยบาย

6.2 การจัดโครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม กำกับ และติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับส่วนงานต่างๆ ภายในองค์กร และเพื่อเป็นแนวทางควบคุมการใช้งานอุปกรณ์สื่อสารประเภทพกพา ให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

6.2.1 การจัดโครงสร้างภายในองค์กร (Internal Organization)

6.2.1.1 การกำหนดบทบาท และหน้าที่ความรับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Roles and Responsibilities)

ก.) ผู้บริหารระดับฝ่ายต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ สำหรับบุคลากรในหน่วยงานอย่างเป็นลายลักษณ์อักษร และให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่กำหนดไว้

6.2.1.2 การประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้องด้านความมั่นคงปลอดภัย (Contact with Authorities)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องรวบรวมรายชื่อ และช่องทางการติดต่อของหน่วยงานที่จำเป็น เช่น สถานีตำรวจ สถานีดับเพลิง หรือหน่วยกู้ภัย เป็นต้น สำหรับติดต่อเมื่อเกิดเหตุฉุกเฉิน พร้อมทั้งปรับปรุงรายชื่อ และช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

6.2.1.3 การประสานงานกับกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Contact with special interest groups)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องรวบรวมรายชื่อกลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และเพิ่มช่องทางการรับข่าวสารจากกลุ่มผู้เชี่ยวชาญ เพื่อให้สามารถติดต่อประสานงาน หรือรับข้อมูลข่าวสาร หรือขอความช่วยเหลือในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศได้ทันท่วงที พร้อมทั้งปรับปรุงรายชื่อ และช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

6.2.2 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานภายนอกองค์กร (Mobile Computing and Teleworking)

6.2.2.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communication)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีมาตรการที่เหมาะสมเพื่อรับรองความปลอดภัยของอุปกรณ์สื่อสารประเภทพกพา โดยพิจารณาจากความเสี่ยงที่มีการนำอุปกรณ์เข้ามาเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ขององค์กร และเมื่อนำอุปกรณ์ออกไปใช้งานนอกสถานที่

ข.) ผู้ใช้งานที่มีการใช้งานอุปกรณ์สื่อสารประเภทพกพาเพื่อเชื่อมต่อกับระบบสารสนเทศขององค์กร ทั้งหมดต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และตระหนักถึงการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

6.2.2.2 การปฏิบัติงานภายนอกสำนักงาน (Teleworking)

ก.) ผู้ใช้งานที่มีการทำงานจากภายนอกสำนักงานทั้งหมด จะต้องปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กรเช่นเดียวกันกับการทำงานภายในสำนักงาน

ข.) ผู้ใช้งานที่มีการใช้ข้อมูลสารสนเทศขององค์กรในการทำงานนอกสำนักงาน หรือการเข้าสู่ระบบผ่าน VPN (Virtual Private Network) ต้องได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ ผู้ดูแลระบบ เจ้าของข้อมูลสารสนเทศ และหน่วยงานต้นสังกัดโดยต้องมีเหตุผลอันควร

ค.) ผู้ใช้งานที่ต้องการเข้าสู่ระบบผ่านทางไกล (Remote Access) ต้องได้รับการอนุญาตจากผู้ดูแลระบบก่อน

6.2.3 การทดสอบการโจมตีทางไซเบอร์

ก) ฝ่ายเทคโนโลยีสารสนเทศ จะต้องมีการประเมินความเสี่ยงด้วยการทดสอบโจมตีทางไซเบอร์ในทุกรูปแบบของอาชญากรทางไซเบอร์ พร้อมแจ้งผลการทดสอบ และวิเคราะห์ประเมินความเสี่ยงเพื่อเตรียมป้องกัน ซึ่งการทดสอบนี้เป็นหนึ่งในมาตรการป้องกันภัยคุกคามทางไซเบอร์ (Cyber Security)

6.3 การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resources Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม การกำกับ และติดตามการสรรหาบุคลากรเข้ามาปฏิบัติงานภายในองค์กร การบริหารจัดการบุคลากรระหว่างการจ้างงาน และการบริหารจัดการบุคลากรเมื่อพ้นสภาพการเป็นลูกจ้าง หรือเมื่อมีการเปลี่ยนแปลงหน้าที่การปฏิบัติงาน

6.3.1 การบริหารจัดการบุคลากรก่อนการจ้างงาน (Prior to Employment)

6.3.1.1 การตรวจสอบประวัติ (Screening)

ก.) องค์กรต้องกำหนดให้มีการตรวจสอบประวัติของผู้สมัครงาน และหน่วยงานภายนอกที่ต้องเข้ามาให้บริการภายในหน่วยงาน

6.3.1.2 ข้อตกลง และเงื่อนไขการจ้างงาน (Terms and Conditions of Employment)

ก.) ฝ่ายบริหารทรัพยากรบุคคล ต้องกำกับให้มีการลงนามในสัญญาจ้าง หรือข้อตกลงการปฏิบัติงานของบุคลากร หรือสัญญาว่าจ้างหน่วยงาน หรือบุคคลภายนอก ซึ่งได้มีการระบุหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญา หรือข้อตกลงการปฏิบัติงาน ซึ่งผู้ใช้งานต้องรับทราบ และยอมรับระเบียบปฏิบัติขององค์กร โดยจะต้องอ่านทำความเข้าใจ และปฏิบัติตามนโยบาย กฎ ระเบียบที่องค์กรได้กำหนดไว้

6.3.2 การบริหารจัดการบุคลากรระหว่างการจ้างงาน (During employment)

6.3.2.1 หน้าที่ในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (Management Responsibilities)

ก.) ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการควบคุม และกำกับให้บุคลากร หรือหน่วยงานภายนอก ที่ได้รับการว่าจ้างเพื่อปฏิบัติงาน หรือให้บริการกับองค์กร ปฏิบัติงานตามนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่องค์กรได้ประกาศใช้

6.3.2.2 การอบรม การสร้างความตระหนัก การให้ความรู้ในเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ (Information security awareness, education and training)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดช่องทางให้ผู้ว่าจ้างสามารถทำการศึกษา และทำความเข้าใจในนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ บทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของตนเองก่อนที่จะอนุญาตให้เริ่มต้นปฏิบัติงานกับองค์กร

ข.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการอบรมที่เกี่ยวข้องกับการปฏิบัติงานทั่วไปโดยหน่วยงานผู้รับผิดชอบ เพื่อให้ผู้ว่าจ้างได้เรียนรู้ และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เช่น วิธีการใช้ระบบงาน วิธีการใช้งานซอฟต์แวร์สำเร็จรูป การแก้ปัญหาการใช้คอมพิวเตอร์เบื้องต้น การปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง เป็นต้น

ค.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดการอบรม และสร้างความตระหนักด้านความมั่นคงปลอดภัยให้ผู้ว่าจ้างได้เรียนรู้ และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เพื่อช่วยให้ผู้ว่าจ้างสามารถปฏิบัติงานที่ตนเองรับผิดชอบได้เป็นอย่างดี และอย่างมั่นคงปลอดภัย

6.3.2.3 กระบวนการลงโทษทางวินัย (Disciplinary Process)

ก.) องค์กรต้องจัดให้มีกระบวนการลงโทษทางวินัย เพื่อลงโทษผู้ใช้งานที่ฝ่าฝืน หรือละเมิดนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หรือขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

6.3.3 การสิ้นสุดการจ้างงาน หรือโยกย้ายตำแหน่งงาน (Termination or Change of Employment)

6.3.3.1 การบริหารจัดการบุคลากรพ้นสภาพ หรือเปลี่ยนหน้าที่ความรับผิดชอบในการปฏิบัติงาน (Termination or Change of Employment Responsibilities)

ก.) ฝ่ายบริหารทรัพยากรบุคคล ต้องกำหนดกฎระเบียบ และความรับผิดชอบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากร และหน่วยงานภายนอกภายหลังจากที่พ้นสภาพการจ้างงาน หรือมีการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงานอย่างเป็นลายลักษณ์อักษร

ข.) ฝ่ายบริหารทรัพยากรบุคคล ต้องควบคุมดูแลให้บุคลากร และหน่วยงานภายนอก ปฏิบัติตามกฎระเบียบที่กำหนดไว้อย่างเคร่งครัด

6.4 การบริหารจัดการทรัพย์สิน (Asset Management)

วัตถุประสงค์

เพื่อให้สินทรัพย์ และระบบสารสนเทศขององค์กรได้รับการปกป้องในระดับที่เหมาะสม เพื่อลดความเสี่ยงต่อการถูกเปิดเผยข้อมูลขององค์กรโดยไม่ได้รับอนุญาต รวมถึงป้องกันการนำทรัพย์สินสารสนเทศไปใช้โดยผิดวัตถุประสงค์ และเกิดความเสียหายกับทรัพย์สินสารสนเทศขององค์กร

6.4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for assets)

6.4.1.1 การจัดทำบัญชีทรัพย์สิน (Inventory of Assets)

ก.) ฝ่ายเทคโนโลยีสารสนเทศต้องควบคุมให้หน่วยงานภายในฝ่ายต้องจัดทำบัญชีทรัพย์สินสารสนเทศ เพื่อบริหารจัดการ และควบคุมทรัพย์สินสารสนเทศอย่างเหมาะสม และให้มีการปรับปรุงบัญชีทรัพย์สินให้เป็นปัจจุบันอยู่เสมอ

6.4.1.2 การระบุผู้ถือครองทรัพย์สิน (Ownership of Assets)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการระบุผู้ถือครองทรัพย์สิน ผู้มีหน้าที่ดูแลควบคุมการใช้งานทรัพย์สินสารสนเทศ และผู้มีหน้าที่รับผิดชอบทรัพย์สินสารสนเทศอย่างเหมาะสม

6.4.1.3 การใช้ทรัพย์สินสารสนเทศ (Acceptable Use of Assets)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำข้อกำหนดในการใช้ทรัพย์สิน เพื่อการบริหารจัดการอุปกรณ์คอมพิวเตอร์ให้เหมาะสมก่อให้เกิดประสิทธิภาพสูงสุด รวมทั้งมีความปลอดภัยจากความเสียหายที่อาจเกิดขึ้นได้ โดยต้องสื่อสารให้บุคลากรขององค์กรรับทราบ และปฏิบัติตาม

6.4.1.4 การคืนทรัพย์สิน (Return of Assets)

ก.) ฝ่ายบริหารทรัพยากรบุคคล หัวหน้างาน หรือผู้บังคับบัญชา ต้องกำกับ และติดตามให้บุคลากรในหน่วยงาน หรือหน่วยงานภายนอกที่เข้ามาให้บริการดำเนินการคืนทรัพย์สิน (Return of Assets) อาทิ เครื่องคอมพิวเตอร์พกพา เอกสาร กุญแจ บัตรพนักงานที่เป็นทรัพย์สินขององค์กรให้กับหน่วยงานที่เกี่ยวข้อง

6.5 การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์

เพื่อกำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับควบคุมการเข้าถึง และการใช้งานระบบสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลขององค์กร

6.5.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement for Access Control)

6.5.1.1 นโยบายควบคุมการเข้าถึง (Access Control Policy)

ก.) องค์กรต้องกำหนดให้มีนโยบายควบคุมการเข้าถึง (Access Control Policy) อย่างเป็นลายลักษณ์อักษร และปรับปรุงนโยบายให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบ และปฏิบัติตาม

6.5.1.2 การควบคุมการเข้าถึงเครือข่าย และบริการเครือข่าย (Access to Networks and Network Service)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการขอเข้าถึงข้อมูล และระบบสารสนเทศของผู้ใช้งาน โดยต้องได้รับการอนุมัติจากผู้บริหารระดับฝ่ายขึ้นไป

ข.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจำกัดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายได้เฉพาะบริการที่ผู้ใช้งานได้รับอนุญาตจากผู้บริหารระดับฝ่ายขึ้นไป โดยสิทธิที่ได้รับต้องเป็นไปตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน

ค.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องมีการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ขององค์กรตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์กำหนดไว้

6.5.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

6.5.2.1 การลงทะเบียน และถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ และเจ้าของข้อมูล ต้องร่วมกันกำหนดวิธีการบริหารจัดการ การลงทะเบียน และถอดถอนสิทธิผู้ใช้งานอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบ และปฏิบัติตาม

6.5.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ และเจ้าของข้อมูล ต้องกำหนดให้มีการมอบหมาย หรือกำหนดสิทธิ์การใช้งานให้แก่ผู้ใช้งานในการเข้าถึงข้อมูล หรือระบบสารสนเทศตามหน้าที่ความรับผิดชอบ

ข.) ฝ่ายเทคโนโลยีสารสนเทศ และเจ้าของข้อมูล ต้องจัดทำเอกสารการมอบหมายสิทธิการเข้าถึงข้อมูล หรือระบบสารสนเทศ และจัดเก็บไว้เป็นหลักฐานในการดำเนินงาน

ค.) ฝ่ายเทคโนโลยีสารสนเทศ และเจ้าของข้อมูล ต้องกำหนดกระบวนการในการบริหารจัดการสิทธิ์การเข้าถึง ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องใช้งานข้อมูล หรือระบบสารสนเทศเกินสิทธิ์ที่ได้รับมอบหมาย

6.5.2.3 การบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูง (Management of Privileged Access Right)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดเก็บรหัสผู้ใช้งานที่มีสิทธิระดับสูง เช่น Administrator/root บนเครื่องแม่ข่าย หรือ Administrator ของระบบ Application และให้มีการเบิกใช้งานตาม ความจำเป็นเท่านั้น

ข.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ และปฏิบัติตาม

6.5.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ และเจ้าของข้อมูล ต้องจัดทำขั้นตอนปฏิบัติการทบทวนสิทธิ์การเข้าถึงข้อมูลระบบสารสนเทศ และโปรแกรมประยุกต์ (Application) อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบ และปฏิบัติตาม

ข.) ฝ่ายเทคโนโลยีสารสนเทศ และเจ้าของข้อมูล ต้องกำหนดรอบในการทบทวนสิทธิการเข้าถึงข้อมูล และระบบสารสนเทศอย่างชัดเจน และแจ้งให้ผู้ที่เกี่ยวข้องรับทราบ

ค.) การทบทวนสิทธิการเข้าถึง ต้องพิจารณาประเด็นดังต่อไปนี้

- รอบการทบทวนสิทธิที่กำหนดไว้
- การพ้นสภาพการเป็นบุคลากรขององค์กร
- การเปลี่ยนแปลงโยกย้ายหน้าที่การปฏิบัติงาน

ง.) เมื่อดำเนินการทบทวนสิทธิเรียบร้อยแล้ว ให้เจ้าของข้อมูล หรือผู้ดูแลระบบจัดเก็บหลักฐานการทบทวนสิทธิ โดยให้แยกหลักฐานตามช่วงเวลาการทบทวนสิทธิ

6.5.2.5 การถอดถอนสิทธิในการเข้าถึง (Removal of Access Rights)

ก.) เจ้าของข้อมูล และผู้ดูแลระบบ ต้องกำหนดเกณฑ์การพิจารณาการถอดถอนสิทธิการเข้าถึง และวิธีการถอดถอนสิทธิในการเข้าถึงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบ และปฏิบัติตาม

6.5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

6.5.3.1 การใช้งานข้อมูลการพิสูจน์ตัวตน (Use of Secret Authentication Information)

ก.) ผู้ใช้งานจะต้องไม่ใช้รูปแบบรหัสผ่าน หรือคุณลักษณะที่ง่ายต่อการเดา อาทิ คำศัพท์ในพจนานุกรม หรือผสมจากชื่อผู้ใช้ หรืออักขระเรียงลำดับ หรือข้อมูลส่วนบุคคล หรือประโยควลีใดๆ ที่สามารถคาดเดาได้ง่าย เช่น nan12345 เป็นต้น

ข.) ผู้ใช้งานจะต้องไม่เขียน หรือบันทึกรหัสผ่านที่ใช้ และเก็บ หรือแสดงให้เห็นไว้ใกล้กับระบบ หรืออุปกรณ์ที่ใช้กับรหัสผ่านนั้น

ค.) ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำทุกอย่างที่เกิดขึ้นหากการกระทำนั้นสามารถบ่งชี้ให้เห็นว่าเกิดจากบัญชีผู้ใช้งานนั้น และจะต้องไม่อนุญาตให้ผู้อื่นกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานของตน หรือกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานอื่นที่ไม่มีสิทธิ

ง.) ผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดการบริหารจัดการรหัสผ่านอื่นๆ ที่ฝ่ายสารสนเทศได้กำหนดไว้

6.5.4 การควบคุมการเข้าถึงแอปพลิเคชัน และสารสนเทศ (Application and Information Access Control)

6.5.4.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ก.) เจ้าของข้อมูล และผู้ดูแลระบบ ต้องกำหนดวิธีการเข้าถึงข้อมูลระบบสารสนเทศ และฟังก์ชันในระบบงาน โดยต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

6.5.4.2 การเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัย (Secure Log-on Procedures)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดวิธีการเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษร โดยอ้างอิงวิธีการที่เป็นมาตรฐานสากล และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบ และปฏิบัติตาม

6.4.5.3 การควบคุมการใช้โปรแกรมอรรถประโยชน์ (Use of Privileged utility Programs)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์ และจำกัดการใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบสารสนเทศ หรือโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้

6.5.5.4 การเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม และการนำซอร์สโค้ดของโปรแกรมไปใช้ในการพัฒนา เพื่อป้องกันการเกิดข้อผิดพลาดในการพัฒนาระบบสารสนเทศ และระบบงานขององค์กร

6.6 การสร้างความมั่นคงปลอดภัยทางกายภาพ และสิ่งแวดล้อม (Physical and Environment Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการป้องกัน ควบคุมการใช้งาน และการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศ และอุปกรณ์สารสนเทศ ซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศขององค์กร ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

6.6.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure Area)

6.6.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)

ก.) องค์กรต้องพิจารณา และจัดทำพื้นที่ที่ต้องการรักษาความปลอดภัย เช่น พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) โดยจะประกอบด้วย พื้นที่กั้น บริเวณ จัดทำผนัง หรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกหลัก และระบบรักษาความปลอดภัยอย่างเหมาะสม

6.1.1.2 การควบคุมการเข้าออกทางกายภาพ (Physical Entry Controls)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการเข้าออกพื้นที่ที่ต้องการรักษาความปลอดภัย (Secure Area) ได้แก่ ห้องศูนย์ข้อมูลคอมพิวเตอร์ รวมถึงพื้นที่ปฏิบัติงานของผู้ดูแล

ระบบ โดยต้องกำหนดให้เฉพาะผู้มีสิทธิ์ที่สามารถเข้า-ออกได้ และมีการเก็บบันทึกการเข้า-ออกห้องศูนย์ข้อมูลคอมพิวเตอร์ และบันทึกการเข้า-ออกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่าน เข้า-ออก วัตถุประสงค์การผ่านเข้า-ออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

6.6.2 อุปกรณ์ (Equipment)

6.6.2.1 การจัดวาง และการป้องกันอุปกรณ์ (Equipment Setting and Protection)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดวางอุปกรณ์สารสนเทศไว้ในห้อง หรือบริเวณที่ปลอดภัย อุปกรณ์ที่มีตู้ ประตูของตู้วางคอมพิวเตอร์แม่ข่าย และอุปกรณ์สื่อสารเครือข่ายต้องถูกล็อคอยู่เสมอ โดยกำหนดให้มีเพียงเจ้าหน้าที่ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิในการเปิดเพื่อซ่อมบำรุง หรือการปรับปรุงค่ารีคอนฟิเกอเรชัน (Reconfiguration) เพื่อลดความเสี่ยงจากการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

6.6.2.2 ระบบ และอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ และหน่วยงานที่เกี่ยวข้อง ต้องควบคุมดูแลให้มีการติดตั้งอุปกรณ์ป้องกันการล้มเหลวของระบบ และอุปกรณ์สนับสนุนการทำงานต่างๆ ภายในห้องคอมพิวเตอร์ ได้แก่ อุปกรณ์ดับเพลิง อุปกรณ์ดักจับควันไฟ อุปกรณ์สำรองไฟฟ้า ระบบควบคุมอุณหภูมิ และความชื้น ระบบเตือนภัยน้ำรั่ว หรือระบบแจ้งเตือนเมื่ออุปกรณ์สารสนเทศทำงานผิดปกติ เป็นต้น และต้องบำรุงดูแลรักษาอุปกรณ์ให้พร้อมใช้งานอยู่เสมอ

6.6.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ และหน่วยงานที่เกี่ยวข้อง ต้องควบคุมดูแลให้การติดตั้ง และการบำรุงรักษาสายไฟฟ้า และสายสื่อสารในพื้นที่ปฏิบัติงาน และห้องคอมพิวเตอร์เป็นไปตามมาตรฐานความปลอดภัยอุตสาหกรรมเพื่อป้องกันไม่ให้มีการเข้าถึง หรือดักจับข้อมูล หรือเกิดความเสียหายทางด้านกายภาพ

6.6.2.4 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้อุปกรณ์ระบบสารสนเทศหลักทั้งหมด ซึ่งใช้ในการประมวลผลในระดับปฏิบัติการ รวมถึงอุปกรณ์สนับสนุนการทำงานได้รับการบำรุงดูแลรักษาตามช่วงเวลา และตามข้อกำหนดที่ผู้ผลิตแนะนำ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้งาน

ข.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการบันทึกกิจกรรมการบำรุงอุปกรณ์ รวมถึงบันทึกปัญหา และข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมิน และปรับปรุงอุปกรณ์ให้อยู่ในสภาพพร้อมใช้งานเสมอ

6.6.2.5 การนำทรัพย์สินสารสนเทศออกนอกสำนักงาน (Removal of Assets)

ก.) ผู้ใช้งาน ต้องไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกนอกองค์กร ยกเว้นจะได้รับอนุญาตจากผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

6.6.2.6 การป้องกันอุปกรณ์ที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended User Equipment)

ก.) ผู้ใช้งาน ต้องล็อคหน้าจอเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน หรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์

6.6.2.7 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

ก.) ผู้ดูแลระบบ ต้องควบคุมให้มีการล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งาน (Clear Screen) เช่น การตัดออกจากระบบ (Session Time Out) และการล็อคหน้าจอ (Lock Screen) อัตโนมัติ เป็นต้น

ข.) ผู้ใช้งาน ต้องไม่ละเลยข้อมูลสารสนเทศที่สำคัญ เช่น เอกสารกระดาษ หรือสื่อบันทึกข้อมูล ให้อยู่ในสถานที่ไม่ปลอดภัย พื้นที่สาธารณะ หรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ใช้งานต้องจัดเก็บข้อมูลสารสนเทศในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงของ ผู้ไม่มีสิทธิ

ค.) ผู้ใช้งานต้องต้องจัดเก็บข้อมูลสำคัญไว้บนพื้นที่ที่ทางบริษัทจัดเตรียมไว้ให้ ไม่ควรเก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลเพื่อป้องกันผู้อื่นเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

6.7 การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ (Operations Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมให้การดำเนินงาน การจัดการด้านการสื่อสารความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร มีแนวทางปฏิบัติที่มีขั้นตอนชัดเจน และมีความมั่นคงปลอดภัย

6.7.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operations Procedures and Responsibilities)

6.7.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีขั้นตอนปฏิบัติงานด้านระบบสารสนเทศที่สำคัญเป็นลายลักษณ์อักษร โดยต้องแบ่งแยกอำนาจหน้าที่ของบุคลากรตามโครงสร้างการปฏิบัติหน้าที่ที่

ชัดเจนเพื่อให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้อง และเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร

ข.) หน่วยงานในฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำคู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจระบบงาน ลักษณะงาน และกระบวนการทำงาน

ค.) หน่วยงานในฝ่ายเทคโนโลยีสารสนเทศ ต้องทบทวนวิธีปฏิบัติคู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ดังกล่าวให้เป็นปัจจุบันอยู่เสมอรวมทั้งจัดให้ขั้นตอนปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งาน และเข้าถึงได้ และต้องสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ และปฏิบัติตาม

6.7.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการจัดการควบคุมการเปลี่ยนแปลงของระบบสารสนเทศ เพื่อควบคุมก่อนการเปลี่ยนแปลง แก้ไข หรือกระทำการใดๆ ซึ่งส่งผลต่อการดำเนินงานของระบบงานต่างๆ ทั้งนี้ ให้ปฏิบัติตามที่กำหนดไว้ในนโยบายส่วนที่ 5.1 การบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy)

6.7.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

ก.) ผู้ดูแลระบบ ต้องติดตามประสิทธิภาพการทำงานของระบบงาน และอุปกรณ์สารสนเทศที่สำคัญให้ทำงานได้อย่างต่อเนื่อง และมีประสิทธิภาพ

ข.) ผู้ดูแลระบบ ต้องประเมินสมรรถภาพและความเพียงพอ (Capacity) ของทรัพยากรสารสนเทศ เช่น การใช้งานของเครื่องแม่ข่าย และอุปกรณ์เครือข่าย หน่วยประมวลผล (CPU) หน่วยความจำ (Memory) หน่วยจัดเก็บข้อมูล (Disk) หรือปริมาณการใช้งานระบบเครือข่าย (Bandwidth) เป็นต้น และต้องวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศให้ระบบสารสนเทศมีประสิทธิภาพที่เหมาะสม และเพียงพอต่อการใช้งานในอนาคต

6.7.1.4 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development Testing and Operational Environments)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการแยกส่วนระบบคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) การทดสอบระบบงาน (Test Environment) และระบบที่ให้บริการจริง (Production Environment) ออกจากกัน

ข.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดสิทธิการเข้าถึงในแต่ละสภาพแวดล้อม และจัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบงานอย่างชัดเจนโดยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหา และวิธีการแก้ไข รวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ

6.7.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

6.7.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls Against Malware)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

ข.) ฝ่ายเทคโนโลยีสารสนเทศต้องมีการแจ้งข่าวเกี่ยวกับโปรแกรมไม่ประสงค์ดีทันที หากมีการระบาดของโปรแกรมไม่ประสงค์ดีตัวใหม่ และหากผู้ใช้งานพบเหตุไม่พึงประสงค์ซึ่งอาจสร้างความเสี่ยงหรืออาจมีผลกระทบต่อการดำเนินธุรกิจและระบบสารสนเทศ จะต้องแจ้งมายังฝ่ายเทคโนโลยีสารสนเทศรับทราบโดยเร็ว

ค.) ผู้ใช้งานต้องระมัดระวังที่จะป้องกันโปรแกรมไม่ประสงค์ดีเข้ามาสู่เครื่องคอมพิวเตอร์ขององค์กร ซึ่งรวมถึงการสแกนตรวจสอบสื่อนำข้อมูลคอมพิวเตอร์ทั้งหมดที่นำมาจากแหล่งข้อมูลภายนอก และการสแกนตรวจสอบข้อมูลที่ดาวน์โหลดมาจากระบบคอมพิวเตอร์ภายนอก รวมถึงไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (Email) หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ต ก่อนการใช้งานด้วย

ง.) หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ที่ใช้งานติดโปรแกรมไม่ประสงค์ดี ให้ทำการตัดการเชื่อมต่อกับระบบเครือข่ายโดยทันที และห้ามมิให้ผู้ใช้งานใช้งานใด ๆ รวมถึงเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายใด ๆ เพื่อป้องกันการแพร่กระจายของโปรแกรมไม่ประสงค์ดีไปยังเครื่องอื่น ๆ และให้แจ้งฝ่ายเทคโนโลยีสารสนเทศทันที

6.7.3 การสำรองข้อมูล (Backup)

6.7.3.1 การสำรองข้อมูล (Information Backup)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการ รอบการสำรองข้อมูล และดำเนินการสำรองข้อมูลระบบสารสนเทศที่สำคัญไว้อย่างสม่ำเสมอ เพื่อป้องกันการสูญหายของข้อมูล

ข.) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลสำคัญจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ ที่บริษัทจัดเตรียมไว้ให้ และอัพเดทให้ข้อมูลเป็นปัจจุบันอย่างสม่ำเสมอ รวมถึงให้จัดเก็บไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

6.7.4 การบันทึกข้อมูลล็อก และการเฝ้าระวัง (Logging and Monitoring)

6.7.4.1 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event Logging)

ก.) ผู้ดูแลระบบ ต้องจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศให้เพียงพอต่อการตรวจสอบ

ข.) ผู้ดูแลระบบ ต้องเฝ้าติดตาม (Monitoring) การใช้งานระบบสารสนเทศ โดยผลของการเฝ้าติดตามจะต้องถูกสอบทานอย่างสม่ำเสมอ เพื่อตรวจหาความผิดปกติ รวมถึงวิเคราะห์ดำเนินการแก้ไข ตลอดจนวางแนวทางป้องกันการเกิดปัญหาซ้ำอีกในอนาคต

6.7.4.2 การป้องกันข้อมูลล็อก (Protection of Log Information)

ก.) ผู้ดูแลระบบ ต้องจัดให้มีการป้องกันข้อมูล และระบบการบันทึก และจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศจากการถูกเปลี่ยนแปลงแก้ไข ถูกทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต

6.7.4.3 การบันทึกกิจกรรมของผู้ดูแลระบบ และเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and Operator Logs)

ก.) ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ และผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบ เช่น เวลาเข้าใช้งานระบบ การเปลี่ยนแปลงการตั้งค่าของระบบ ความผิดพลาดของระบบ และการดำเนินการแก้ไข และต้องมีการสอบทานบันทึกกิจกรรมอย่างสม่ำเสมอ

6.7.4.4 การตั้งเวลาระบบสารสนเทศ (Clock Synchronization)

ก.) ผู้ดูแลระบบ ต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศขององค์กรได้รับการกำหนดเวลาให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง และตรงกับเวลาอ้างอิงสากล

ข.) ผู้ดูแลระบบ ต้องตรวจสอบเวลาของอุปกรณ์สารสนเทศ และระบบสารสนเทศขององค์กร รวมถึงปรับปรุงให้เป็นปัจจุบันเสมอ เพื่อป้องกันไม่ให้เกิดการบันทึกเวลาที่ไม่ถูกต้อง

6.7.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software)

6.7.5.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of Software on Operational Systems)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติงาน และมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน และป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน

ข.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดรายการซอฟต์แวร์มาตรฐาน (Software standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ขององค์กรอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบ และปฏิบัติตาม

6.7.6 การบริหารจัดการช่องโหว่ทางเทคนิคในฮาร์ดแวร์ และซอฟต์แวร์ (Technical Vulnerability Management)

6.7.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมให้ระบบสารสนเทศขององค์กร ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้โดยให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง

ข.) ผู้ดูแลระบบ ต้องดูแล และบำรุงรักษาระบบ เพื่อรักษาระดับความมั่นคงปลอดภัยด้านสารสนเทศของระบบอย่างสม่ำเสมอ ได้แก่ การตรวจสอบหาช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ ที่ตรวจสอบพบ และการปรับปรุงแก้ไขช่องโหว่ของระบบสารสนเทศ เช่น การจัดการบัญชีรายชื่อผู้ใช้ (User Account) การอัพเดทโปรแกรม Antivirus อย่างสม่ำเสมอ

6.7.6.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

ก.) ผู้ใช้งานต้องปฏิบัติตามกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์ และไม่ติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ขององค์กร

6.7.7 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)

6.7.7.1 มาตรการการตรวจประเมินระบบ (Information System Audit Controls)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้ เช่น แผนการตรวจสอบช่องโหว่ของระบบสารสนเทศ (Vulnerability Assessment) เป็นต้น

ข.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องแจ้งให้หน่วยงานที่เกี่ยวข้องรับทราบก่อนดำเนินการตรวจสอบระบบสารสนเทศทุกครั้ง

ค.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดขอบเขตการตรวจสอบทางเทคนิค (Technical Audit Test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญ และต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการ

ปฏิบัติงานตามปกติ โดยกรณีที่การตรวจสอบระบบสารสนเทศมีโอกาสกระทบต่อความพร้อมใช้งานของระบบต้องจัดให้มีการทดสอบนอกเวลาทำงาน

6.8 การสื่อสารด้านความมั่นคงปลอดภัยสารสนเทศ (Communications Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการบริหารจัดการเครือข่าย และการส่งข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ทั้งภายใน และภายนอกองค์กรให้มีความมั่นคงปลอดภัย

6.8.1 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)

6.8.1.1 การควบคุมเครือข่าย (Network Controls)

ก.) ผู้ดูแลระบบ ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และ แอปพลิเคชันที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย

6.8.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)

ก.) ผู้ดูแลระบบ ต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมด ลงในข้อตกลง หรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายใน หรือภายนอก

6.8.1.3 การแบ่งแยกเครือข่าย (Segregation in Network)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

6.8.2 การแลกเปลี่ยนข้อมูลสารสนเทศ (Information Transfer)

6.8.2.1 ข้อตกลงสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศ (Agreements on Information Transfer)

ก.) การแลกเปลี่ยนข้อมูลสารสนเทศภายในองค์กรกับหน่วยงานภายนอก ต้องได้รับการอนุมัติจากเจ้าของข้อมูลก่อนทุกครั้ง และมีการควบคุมโดยการระบุข้อตกลงเป็นลายลักษณ์อักษร

6.8.2.2 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการควบคุมการรับส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ EDI (Electronic Data Interchange) หรือ Instant Messaging เป็นต้น โดยข้อความทางอิเล็กทรอนิกส์ที่สำคัญจะต้องได้รับการป้องกันอย่างเหมาะสมจากการพยายามเข้าถึง การแก้ไข การรบกวนทำให้ระบบหยุดให้บริการจากผู้ไม่มีสิทธิ

6.8.2.3 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or Non-Disclosure Agreements)

ก.) ผู้บริหารระดับฝ่ายต้องจัดให้บุคลากร และหน่วยงานภายนอกที่ปฏิบัติงานให้องค์กร มีการทำสัญญารักษาความลับ หรือไม่เปิดเผยข้อมูลขององค์กรอย่างเป็นลายลักษณ์อักษร

6.9 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศ ที่มีการพัฒนาขึ้นใหม่ หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนา หรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

6.9.1 ความต้องการด้านความมั่นคงปลอดภัยระบบ (Security Requirements of Information Systems)

6.9.1.1 การวิเคราะห์ และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

ก.) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนา หรือจัดหาระบบสารสนเทศเพื่อนำมาใช้งานในองค์กร กำหนดคุณลักษณะความต้องการด้านความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือระบบที่จัดหามาใช้งาน

ข.) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนา หรือจัดหาระบบสารสนเทศ ต้องติดตามการพัฒนาระบบ

สารสนเทศ เพื่อตรวจสอบว่าการพัฒนาระบบสารสนเทศตรงตามความต้องการด้านความมั่นคงปลอดภัย สารสนเทศ รวมถึงความต้องการด้านการใช้งานที่กำหนดไว้

6.9.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบ และสนับสนุน (Security in Development and Support Processes)

6.9.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดกฎระเบียบสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย และครอบคลุมตลอดทั้งวงจรการพัฒนาระบบสารสนเทศ

6.9.2.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลง อย่างเป็นลายลักษณ์อักษรโดยให้ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ

6.9.2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical Review of Applications after Operating Platform Changes)

ก.) ผู้ดูแลระบบ จะต้องทำการตรวจสอบทางเทคนิคเพื่อวิเคราะห์ถึงผลกระทบที่อาจเกิดขึ้น เมื่อต้องการที่จะเปลี่ยนแปลง หรือปรับปรุงระบบปฏิบัติการ เช่น การเปลี่ยนเวอร์ชัน เป็นต้น โดยจะต้องมีการทดสอบบนเครื่องทดสอบ (Test Environment) จนมั่นใจว่าระบบงานต่างๆ ที่ประมวลผลบนเครื่องดังกล่าวสามารถทำงานได้ตามปกติ และมีความมั่นคงปลอดภัย จึงจะทำการเปลี่ยนแปลง หรือปรับปรุงบนเครื่องที่ใช้งานจริง (Production Environment)

ข.) ผู้ดูแลระบบ จะต้องทำการตรวจสอบทางเทคนิคภายหลังการเปลี่ยนแปลงระบบปฏิบัติการบนระบบจริง เพื่อตรวจสอบว่าการเปลี่ยนแปลงไม่มีผลกระทบต่อการทำงานของระบบ และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยระบบสารสนเทศ

6.9.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

ก.) ซอฟต์แวร์สำเร็จรูปที่นำมาใช้งานในองค์กรควรใช้งานโดยปราศจากการแก้ไข หากในกรณีที่มีความจำเป็นต้องดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป หน่วยงานที่ได้รับมอบหมายให้ดำเนินการ ต้องพิจารณาการควบคุมการแก้ไขอย่างเข้มงวด

ข.) การเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป ต้องดำเนินการเปลี่ยนแปลงตามขั้นตอนปฏิบัติการควบคุมการเปลี่ยนแปลงที่ฝ่ายเทคโนโลยีสารสนเทศกำหนดไว้

6.9.2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles)

ก.) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศ ต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบดังต่อไปนี้เป็นอย่างน้อย

- การให้สิทธิต่ำที่สุด (Least Privilege) แก่ผู้ใช้งานระบบสารสนเทศ เพื่อป้องกันการแก้ไข เปลี่ยนแปลงข้อมูล หรือระบบโดยไม่ได้รับอนุญาต
- การให้สิทธิเฉพาะที่จำเป็นในการปฏิบัติงาน (Need to Know) แก่ผู้ใช้งานระบบสารสนเทศ เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ
- การออกแบบระบบให้สามารถป้องกันได้หลายระดับขั้น (Defense In-Depth) เพื่อลดความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- การออกแบบในลักษณะเปิด (Open Design) เพื่อให้การพัฒนาระบบมีการใช้กลไกหรืออัลกอริทึม (Algorithm) ที่เป็นมาตรฐานเดียวกัน และสามารถตรวจสอบการทำงานได้

6.9.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure Development Environment)

ก.) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ และหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศ ต้องมีการควบคุมสภาพแวดล้อมของการพัฒนา และบูรณาการระบบให้มีความมั่นคงปลอดภัย โดยต้องป้องกันข้อมูลของระบบที่เกิดขึ้นในระหว่างการพัฒนา การรับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบสารสนเทศ

6.9.2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced Development)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดข้อตกลงในการพัฒนาระบบสำหรับหน่วยงานภายนอก ที่ทำหน้าที่พัฒนาซอฟต์แวร์เพื่อใช้งานภายในองค์กรอย่างเป็นลายลักษณ์อักษร

ข.) หน่วยงานที่ได้รับมอบหมายให้ดำเนินการจัดจ้างหน่วยงานภายนอกเข้ามาพัฒนาระบบสารสนเทศให้องค์กร ต้องกำกับดูแล เฝ้าระวัง และติดตามกิจกรรมการพัฒนาระบบที่จ้างอย่างสม่ำเสมอ เพื่อป้องกันไม่ให้เกิดความเสียหายใดๆ ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ

6.9.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing)

ก.) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ หน่วยงานที่ได้รับมอบหมาย และผู้ใช้งานต้องร่วมกันทดสอบฟังก์ชันการทำงานของระบบสารสนเทศ และ

ฟังก์ชันการทำงานด้านความมั่นคงปลอดภัยสารสนเทศในระบบที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงทุกครั้ง

ข.) การทดสอบการพัฒนาระบบสารสนเทศ ต้องดำเนินการทดสอบระหว่างการพัฒนา และก่อนนำระบบขึ้นใช้งานจริง โดยต้องจัดเก็บหลักฐานในการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงอย่างเป็นทางการ

6.9.2.9 การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ หรือที่ปรับปรุงเพิ่มเติม ทั้งที่มาจากส่วนพัฒนาระบบเทคโนโลยีสารสนเทศพัฒนาขึ้น หรือที่มีการจัดหาจากหน่วยงานภายนอก และต้องทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้งานจริง

6.9.3 ข้อมูลสำหรับการทดสอบ (Test Data)

6.9.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

ก.) ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศ ส่วนบริหารโครงการเทคโนโลยีสารสนเทศ หน่วยงานที่ได้รับมอบหมาย และผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง

6.10 การบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอก (Supplier Relationships)

วัตถุประสงค์

เพื่อจัดทำข้อกำหนดต่างๆ และกรอบการปฏิบัติงานของหน่วยงานภายนอกในการให้บริการ หรือการใช้บริการด้านงานเทคโนโลยีสารสนเทศ ให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย และได้รับผลประโยชน์สูงสุดแก่องค์กร

6.10.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับหน่วยงานภายนอก (Information Security in Supplier Relationships)

6.10.1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับหน่วยงานภายนอก (Information Security Policy for Supplier Relationships)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน่วยงานภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณา หรือประเมินความเสี่ยงที่อาจเกิดขึ้น และกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้หน่วยงานภายนอก หรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศขององค์กร

ข.) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมกำกับให้มีการดูแลให้บุคคล หรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญา หรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

6.10.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับการอนุญาตให้หน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศ เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร

ข.) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมให้หน่วยงานภายนอกสามารถเข้าถึงสารสนเทศขององค์กรเฉพาะส่วนที่มีความจำเป็นต้องรู้ และต้องได้รับการยินยอมจากเจ้าของข้อมูลสารสนเทศอย่างเป็นลายลักษณ์อักษรเท่านั้น

ค.) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมดูแลให้หน่วยงานภายนอกปฏิบัติตามข้อกำหนด หรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและหน่วยงานภายนอก

6.10.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

6.10.2.1 การติดตาม และทบทวนการให้บริการของหน่วยงานภายนอก (Monitoring and Review of Supplier Services)

ก.) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องติดตามและตรวจทานการดำเนินงานของหน่วยงานภายนอกซึ่งมีหน้าที่ในการบริหารจัดการระบบประมวลผลข้อมูลสารสนเทศให้กับองค์กร ทั้งในด้านฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการให้บริการอย่างสม่ำเสมอ

6.10.2.2 การบริหารจัดการการเปลี่ยนแปลงบริการของหน่วยงานภายนอก (Managing Changes to Supplier Services)

ก.) กรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องจัดให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลง

ดังกล่าวโดยต้องรายงานให้ผู้บริหาร และผู้ที่เกี่ยวข้องรับทราบ รวมถึงให้กำหนดกระบวนการบริหารจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสม

6.11 การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ การเรียนรู้ข้อผิดพลาดจากปัญหาที่เกิดขึ้น และการปรับปรุงแก้ไข ซึ่งเป็นการป้องกันไม่ให้เกิดเหตุการณ์ทางด้านความมั่นคงปลอดภัยสารสนเทศซ้ำขึ้นอีก

6.11.1 การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Management of Information Security Incidents and Improvements)

6.11.1.1 หน้าที่ความรับผิดชอบ และขั้นตอนปฏิบัติ (Responsibilities and Procedures)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดหน้าที่ในการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด และมอบหมายสิทธิการดำเนินงานอย่างชัดเจนให้บุคลากรภายในฝ่าย

ข.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการจำแนกสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดออกจากเหตุขัดข้องด้านการปฏิบัติงานทั่วไป เพื่อกำหนดแนวทางการแก้ไขที่ถูกต้องเหมาะสม

6.11.1.2 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events)

ก.) ผู้ใช้งาน และหน่วยงานภายนอกต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศขององค์กรต่อผู้บังคับบัญชา และฝ่ายเทคโนโลยีสารสนเทศ โดยผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด

6.11.1.3 การประเมิน และตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and Decision on Information Security Events)

ก.) ผู้ดูแลระบบ ต้องประเมินเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ทำการจัดแยกกลุ่มเหตุการณ์ และจัดลำดับความสำคัญตามเกณฑ์ที่กำหนดไว้ และแจ้งผู้ที่เกี่ยวข้องรับทราบเพื่อแก้ไขในกรณีที่พบว่าเหตุการณ์ที่ส่งผลกระทบด้านความมั่นคงปลอดภัยสารสนเทศ

6.11.1.4 การตอบสนองต่อเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Response to Information Security Incidents)

ก.) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ ต้องดำเนินการตามขั้นตอนการปฏิบัติงานสำหรับการแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดไว้

ข.) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ ต้องดำเนินการตอบสนอง และแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้ หากไม่สามารถแก้ไขได้ตามเวลาที่กำหนดต้องแจ้งให้ผู้บังคับบัญชารับทราบโดยเร็วที่สุด

6.11.1.5 การเรียนรู้จากเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from Information Security Incidents)

ก.) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ จะต้องจัดเตรียมรายงานผลการวิเคราะห์ และการแก้ไขเหตุขัดข้อง จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และจัดเก็บไว้เป็นองค์ความรู้ เพื่อใช้ในการเรียนรู้ในการดำเนินงาน และลดโอกาสเกิดในอนาคต

6.11.1.6 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

ก.) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้จะต้องดำเนินการเก็บรวบรวมหลักฐานที่เกี่ยวข้องกับเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น เพื่อรวบรวมหลักฐานให้เพียงพอต่อการนำเสนอผู้บริหารหน่วยงานที่เกี่ยวข้อง และใช้ในการดำเนินการด้านกฎหมายต่อไป

6.12 ความมั่นคงปลอดภัยสำหรับการบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อป้องกันการติดขัด หรือหยุดชะงักของการดำเนินธุรกิจขององค์กร และป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวของระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบสารสนเทศกลับคืนมาได้ในระยะเวลาอันเหมาะสม

6.12.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity)

6.12.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity)

ก.) เจ้าของข้อมูล และฝ่ายเทคโนโลยีสารสนเทศ ต้องร่วมกันระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการทางธุรกิจ ประเมินความเสี่ยงเหตุการณ์ และระบบงานสำคัญ เพื่อให้ได้มาซึ่งข้อมูลที่มีความถูกต้อง และครบถ้วน เพื่อใช้ในการจัดทำแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

6.12.1.2 การสร้างกระบวนการความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน โดยให้กำหนดมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้เป็นส่วนหนึ่งของแผน และให้มีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจขององค์กร

6.12.2 การจัดให้มีอุปกรณ์ หรือระบบสารสนเทศสำรอง (Redundancies)

6.12.2.1 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)

ก.) องค์กร ต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศที่มีความสำคัญสูง

ข.) องค์กร ต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม

6.13 การปฏิบัติตามกฎระเบียบ และข้อบังคับ (Compliance)

วัตถุประสงค์

เพื่อให้การดำเนินงานต่างๆ ขององค์กรเป็นไปตามกฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆ ที่องค์กร และบุคลากรขององค์กรต้องปฏิบัติตาม รวมถึงให้มีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้

6.13.1 การปฏิบัติตามกฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้อง (Compliance with Legal and Contractual Requirements)

6.13.1.1 การระบุกฎหมาย และข้อกำหนดในสัญญาจ้าง (Identification of Applicable Legislation and Contractual Requirements)

ก.) บุคลากรทั้งหมดต้องรับผิดชอบในการปฏิบัติตามข้อกำหนดที่ได้มีการระบุไว้อย่างเคร่งครัด

ข.) ห้ามเจ้าหน้าที่ในองค์กรใช้งานทรัพย์สิน และระบบเทคโนโลยีสารสนเทศขององค์กรกระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม รวมถึงศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานต้องรับรองว่าหากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบขององค์กร

ค.) ห้ามเจ้าหน้าที่ในองค์กรใช้งานทรัพย์สิน และระบบเทคโนโลยีสารสนเทศขององค์กรกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือแสวงหาผลกำไร หรือเพื่อพิจารใด ๆ ที่ไม่มีส่วนเกี่ยวข้องกับองค์กร ผ่านคอมพิวเตอร์และเครือข่ายขององค์กร

ง.) ห้ามเจ้าหน้าที่ในองค์กรใช้งานทรัพย์สิน และระบบเทคโนโลยีสารสนเทศขององค์กรกระทำการใดๆ ในลักษณะที่เป็นการละเมิดต่อบุคคลอื่น เช่น การเข้าถึงและแก้ไขเปลี่ยนแปลงใด ๆ ในส่วนที่มิใช่จองตนเองโดยมิได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆที่จะทำลายกลไกรักษาความปลอดภัย การเข้าสู่เครื่องคอมพิวเตอร์ขององค์กร หรือหน่วยงานอื่น ๆ รวมถึง การเผยแพร่ข้อมูล เนื้อหา หรือข้อความใด ๆ ที่ก่อให้เกิดการเสียหายเสื่อมเสียแก่บุคคลอื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของบุคคลอื่นทั้งสิ้น หากมีการกระทำการใด ๆ ดังกล่าว ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว องค์กรไม่มีส่วนรับผิดชอบต่อความเสียหายดังกล่าว

6.13.1.2 การป้องกันสิทธิ และทรัพย์สินทางปัญญา (Intellectual Property Rights)

ก.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำกระบวนการสำหรับการบริหารจัดการการใช้ซอฟต์แวร์ลิขสิทธิ์ และทรัพย์สินทางปัญญา เพื่อให้มั่นใจว่าการใช้งานข้อมูลสารสนเทศที่อาจถือเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ที่พัฒนาโดยผู้ประกอบธุรกิจมีความสอดคล้องกับกฎหมาย และข้อกำหนดตามสัญญาต่างๆ

ข.) ผู้ใช้งานต้องไม่ทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่องค์กรได้จัดซื้อลิขสิทธิ์ เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉิน หรือเพื่อเป็นสำเนาไว้ ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

ค.) ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบสารสนเทศขององค์กรโดยเด็ดขาด

ง.) ซอฟต์แวร์ที่พัฒนาเพื่อองค์กร ทั้งโดยหน่วยงานภายนอก หรือบุคลากรในหน่วยงานขององค์กร ถือว่าเป็นทรัพย์สินขององค์กร องค์กรไม่อนุญาตให้หน่วยงานภายนอก หรือบุคลากรในหน่วยงานขององค์กรทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินขององค์กรโดยไม่ได้รับอนุญาต

จ.) ผู้ใช้งานที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศขององค์กรต้องยึดถือ และปฏิบัติตามกฎหมายลิขสิทธิ์ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

ฉ.) ห้ามมิให้พนักงานจัดเก็บ หรือบันทึกไฟล์เพลง ไฟล์วีดิโอที่ไม่มีใบอนุญาตทางลิขสิทธิ์ ลงบนทรัพย์สินสารสนเทศขององค์กร เนื่องจากการกระทำดังกล่าว ถือว่าเป็นการกระทำที่ไม่ได้รับการอนุญาตจากเจ้าของลิขสิทธิ์

6.13.1.3 การป้องกันข้อมูลขององค์กร (Protection of Records)

ก.) เจ้าของข้อมูล ต้องปฏิบัติตามข้อบังคับทางกฎหมายที่เกี่ยวกับข้อมูลสารสนเทศบางประเภท เช่น ด้านบัญชี ด้านลูกค้า และต้องจัดทำข้อกำหนดในการจัดการข้อมูลสารสนเทศ ระยะเวลาในการจัดเก็บให้สอดคล้องกับข้อบังคับดังกล่าว

ข.) ฝ่ายเทคโนโลยีสารสนเทศต้องป้องกันมิให้ข้อมูลบันทึกหลักฐาน (Logs) ต่างๆ เกิดความเสียหาย สูญหาย ถูกเปลี่ยนแปลงแก้ไข ถูกเข้าถึง หรือเผยแพร่โดยไม่ได้รับอนุญาต โดยการควบคุมต้องให้สอดคล้องกับกฎหมาย ข้อกำหนด และความต้องการทางธุรกิจ

6.13.1.4 ความเป็นส่วนตัว และการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information)

ก.) องค์กร ต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย ประกาศหลักเกณฑ์ที่รัฐบาลได้ประกาศไว้ รวมถึงข้อบังคับต่างๆ ที่มีผลบังคับใช้กับองค์กร ตลอดจนนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กร

ข.) ข้อมูลสารสนเทศรายละเอียดที่เกี่ยวกับลูกค้าถือว่ามีความสำคัญ หน่วยงานผู้รับผิดชอบในการดูแลข้อมูลต้องกำหนดให้บุคลากร และลูกจ้างที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บังคับบัญชาเท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลสารสนเทศดังกล่าวได้

ค.) ข้อมูลสารสนเทศส่วนบุคคลของบุคลากร ลูกจ้าง และลูกค้า ถือว่าเป็นความลับ และสามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิ์ ตามที่องค์กรกำหนดเท่านั้น

6.13.2 การทบทวนความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Reviews)

6.13.2.1 การตรวจประเมินระบบสารสนเทศจากผู้ตรวจสอบอิสระ (Independent Review of Information Security)

ก.) องค์กรต้องจัดให้มีการตรวจประเมินความมั่นคงปลอดภัยสารสนเทศ โดยส่วนตรวจสอบระบบงาน หรือผู้ตรวจสอบอิสระภายนอก เพื่อตรวจสอบการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนทบทวนถึงความพอเพียงของการควบคุมระบบสารสนเทศ และการปฏิบัติตามการควบคุมต่างๆ

6.13.2.2 การปฏิบัติตามนโยบาย และมาตรฐานความปลอดภัยสารสนเทศ (Compliance with Security Policies and Standards)

ก.) ผู้บังคับบัญชาของแต่ละแผนกต้องรับผิดชอบในการสอบทานการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนปฏิบัติงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ ของบุคลากรใต้บังคับบัญชาอย่างสม่ำเสมอ

ข.) กรณีที่ผู้บังคับบัญชาของแต่ละแผนกตรวจพบการปฏิบัติงานที่ไม่สอดคล้องกับนโยบาย มาตรฐาน และขั้นตอนปฏิบัติซึ่งยังไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ผู้บังคับบัญชาต้องชี้แจงให้บุคลากรใต้บังคับบัญชารับทราบ และทำความเข้าใจ แต่หากความไม่สอดคล้องที่พบส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ผู้บังคับบัญชาต้องดำเนินการลงโทษทางวินัยตามกฎระเบียบที่องค์กรกำหนดไว้

ค.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องให้การสนับสนุนด้านการให้คำแนะนำในการใช้งาน หรือการปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนปฏิบัติ และข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศต่อหน่วยงานอื่นเมื่อได้รับคำร้องขอ

6.13.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

ก.) ส่วนตรวจสอบระบบงาน ต้องตรวจสอบการควบคุมทางเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอเหมาะสม และมีการปฏิบัติตามการควบคุมเหล่านั้น

ข.) ผู้ดูแลระบบ ต้องจัดให้มีการทดสอบระดับมาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เช่น การตรวจหาช่องโหว่ของระบบสารเทศ (Vulnerability Assessment) หรือการทดสอบการบุกรุกระบบ (Penetration Test) เพื่อให้สอดคล้องกับ นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

หมวดที่ 7 การบริหารจัดการข้อมูล (Data Management)

7.1 การบริหารจัดการข้อมูล

วัตถุประสงค์

เพื่อให้การบริหารจัดการข้อมูลของบริษัท พรีไซซ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทในเครือ “(บริษัท ฯ)” สอดคล้องกับกฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง ในการใช้เป็นกรอบและแนวทางในการบริหารจัดการข้อมูลของหน่วยงาน สำหรับผู้บริหาร พนักงาน และผู้ที่เกี่ยวข้อง

7.2 ข้อกำหนดทั่วไปของการบริหารจัดการข้อมูล

7.2.1 กำหนดบทบาท หน้าที่ และความรับผิดชอบของแต่ละบุคคลตามโครงสร้างองค์กร โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร พร้อมทั้งกำหนดหน่วยงานเป็นเจ้าของข้อมูล เพื่อทำหน้าที่ในการบริหารจัดการข้อมูลนั้น ๆ

7.2.1.1 หัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายต้องควบคุมและกำกับดูแลให้บุคลากรในหน่วยงาน และผู้ที่เกี่ยวข้องดำเนินการตามนโยบายการบริหารจัดการข้อมูลอย่างเคร่งครัด

7.2.1.2 ผู้บังคับบัญชาต้องตรวจสอบให้แน่ใจว่าบุคลากรในหน่วยงานและบุคคลอื่น ๆ เช่น บริษัทหรือ ผู้รับจ้าง ที่ได้รับมอบหมายจากหน่วยงานให้ทำหน้าที่บริหารจัดการข้อมูลได้รับความรู้เกี่ยวกับนโยบายนี้อย่างเหมาะสม และนำนโยบายไปปฏิบัติตามอย่างมีประสิทธิภาพและประสิทธิผล

7.2.1.3 บุคลากรในหน่วยงานและบุคคลอื่น ๆ เช่น บริษัทหรือผู้รับจ้าง ที่ได้รับมอบหมายจากหน่วยงานให้ทำหน้าที่บริหารจัดการข้อมูลต้องปฏิบัติตามนโยบาย มาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับ ข้อมูลและระบบข้อมูลสารสนเทศที่หน่วยงานกำหนด

7.2.1.4 หน่วยงานพัฒนาสถาปัตยกรรมและทุนทางปัญญาองค์กร (Intellectual Capital & Digital Organization Development Management), หน่วยงาน Data Governance (PDE102), ผู้สร้างข้อมูล ผู้บริหารจัดการข้อมูล เจ้าของข้อมูล และผู้ดูแลข้อมูล ต้องปฏิบัติ หน้าที่ที่ได้รับมอบหมาย ตัวอย่างการกำหนดบทบาทและความรับผิดชอบของผู้มีส่วนเกี่ยวข้องดังตัวอย่างต่อไปนี้

บทบาท	ความรับผิดชอบ

หน่วยงานพัฒนาสถาปัตยกรรมและทุนทางปัญญาองค์กร (Intellectual Capital & Digital Business Organization Development Management)	• ประกอบไปด้วย รองกรรมการผู้จัดการใหญ่ (Vice President – Intellectual Capital & Digital Business Organization Development Management) • มีอำนาจสูงสุดในธรรมาภิบาลข้อมูลภายในหน่วยงาน ทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการข้อมูลของหน่วยงาน ทั้งนี้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงอาจจะทำหน้าที่แทนผู้บริหารข้อมูลระดับสูง
หน่วยงานทุนทางข้อมูล (Infotmation Capital)	• นิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัย • นิยามเมทาดาตา • ร่างนโยบายข้อมูล มาตรฐาน และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูล • ตรวจสอบการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ
หน่วยงาน Data Governance (PDE102)	• ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูล • รักษา และดูแลข้อมูลที่อยู่บนระบบเทคโนโลยีสารสนเทศต่าง ๆ ในหน่วยงาน

7.2.2 จัดทำแนวปฏิบัติและมาตรฐานที่เกี่ยวกับข้อมูลเพื่อสนับสนุนการ ปฏิบัติงานให้สอดคล้องตามนโยบายฉบับนี้

7.2.3 กำหนดมาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการ ละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบหรือโดย มิได้รับอนุญาต

7.2.4 กำหนดมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติของหน่วยงาน (อ้างอิงตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) และเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

7.2.5 ตรวจสอบความมีอยู่และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล การจัดชั้นความลับข้อมูล และรายงานผลให้แก่ผู้รับผิดชอบ

7.2.6 ตรวจสอบ ติดตาม และประเมินผลการปฏิบัติตามนโยบายการบริหารจัดการข้อมูล พร้อมทั้งกำหนดให้มีการทบทวนนโยบาย รวมถึง มาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ เกี่ยวกับข้อมูล อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่ สำคัญตามความเหมาะสม

7.2.7 ตรวจสอบ ติดตาม และประเมินผลการดำเนินงานธรรมาภิบาลข้อมูลของบริษัทย่างน้อยปีละ 1 ครั้ง ในเรื่อง (1) การประเมินความพร้อมธรรมาภิบาลข้อมูล (2) การประเมินคุณภาพข้อมูล และ (3) การประเมินความมั่นคงปลอดภัยของข้อมูลเป็นอย่างน้อย

7.2.8 จัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล

7.2.9 ข้อกำหนดอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

7.3 คุณภาพข้อมูล

7.3.1 กำหนดนโยบายการจัดการคุณภาพข้อมูล เพื่อใช้เป็นกรอบแนวทางในการจัดการข้อมูลของ หน่วยงานให้มีคุณภาพเป็นตามเกณฑ์หรือคุณสมบัติที่กำหนด ได้แก่

(1) ความถูกต้อง (Accuracy)

(2) ความครบถ้วน (Completeness)

(3) ความสอดคล้อง (Consistency)

(4) ความเป็นปัจจุบัน (Timeliness)

(5) ตรงตามความต้องการของผู้ใช้ (Relevance)

(6) ความพร้อมใช้ (Availability)

โดยผู้ดูแลข้อมูลมีหน้าที่จัดการและกำกับดูแลข้อมูลให้มีคุณภาพเพื่อสร้างความมั่นใจให้กับผู้ใช้ข้อมูล ในขณะที่ผู้ใช้ข้อมูลมีบทบาทในการให้ข้อเสนอแนะแก่ผู้ดูแลข้อมูลเพื่อการปรับปรุงคุณภาพให้ดียิ่งขึ้น

7.3.2 จัดทำเกณฑ์คุณภาพข้อมูลที่สามารถวัดผลได้ พร้อมทั้งจัดทำแผนพัฒนาคุณภาพข้อมูลที่สามารถ ระบุตัวชี้วัดคุณภาพและแผนปฏิบัติการเพื่อจัดการคุณภาพข้อมูลได้อย่างมีประสิทธิภาพ โดยออกแบบการเก็บ รวบรวมข้อมูลเพื่อให้ได้ข้อมูลสำหรับประเมินคุณภาพตามเกณฑ์ดังกล่าวให้รวมอยู่ในระบบเทคโนโลยี สารสนเทศและกระบวนการทำงาน (Quality by design) เพื่อลดข้อผิดพลาดและปรับปรุงคุณภาพตั้งแต่จุด การป้อนข้อมูลหรือการสร้างข้อมูลไปจนถึงการประมวลผลข้อมูล

7.3.3 ประเมินผลและจัดการคุณภาพข้อมูลอย่างสม่ำเสมอตลอดวงจรชีวิตของข้อมูล โดยเจ้าของข้อมูลและบริกรข้อมูลควรกำหนดกรอบคุณภาพข้อมูลเฉพาะหมวดหมู่ข้อมูลหรือโดเมน (Domain) เช่น Quality Assurance Framework of the European Statistical System (ESS. QAF) ที่เป็นกรอบคุณภาพข้อมูล สถิติของ the European Statistical System ที่สามารถนำมาใช้อ้างอิงได้

7.3.4 พัฒนากระบวนการหรือกลไกให้ผู้ใช้สามารถให้ข้อเสนอแนะหรือ Feedback เพื่อรายงานปัญหาให้กับ เจ้าของข้อมูลโดยเฉพาะข้อมูลสำคัญ เช่น ข้อมูลหลัก (Master data) และข้อมูลอ้างอิง (Reference data)

7.3.5 แนวทางอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

7.4 การจัดหมวดหมู่และชั้นความลับของข้อมูล

7.4.1 กำหนดหมวดหมู่และประเภทชั้นความลับของข้อมูลที่ใช้กับข้อมูลทุกรูปแบบของหน่วยงาน ทั้งเอกสาร กระดาษ และข้อมูลดิจิทัล ด้วยการประเมินผลกระทบของข้อมูลหน่วยงาน เพื่อระบุหมวดหมู่และประเภทชั้น ความลับของข้อมูล รวมทั้งกำหนดระดับความปลอดภัยที่เหมาะสมสำหรับการสร้าง/จัดเก็บ การใช้ และการ เข้าถึงชุดข้อมูล และเพื่อใช้กับบุคลากรรวมถึงตัวแทนบุคคลที่สามที่ได้รับอนุญาตให้เข้าถึงข้อมูลในหน่วยงาน พร้อมทั้งกำหนดบทบาทหน้าที่ของบุคลากรในการจัดหมวดหมู่และชั้นความลับ เพื่อป้องกัน จัดการ และกำกับ ดูแลข้อมูลให้เหมาะสม

7.4.2 ติดป้ายกำกับชุดข้อมูล (Labeling/Tagging Dataset) ตามผลประเมินและระบุหมวดหมู่และ ประเภทชั้นความลับอย่างเหมาะสม และป้ายกำกับสำรองชั้นความลับข้อมูล (ถ้ามี) เช่น เปิดเผยสาธารณะ ใช้ภายใน ลับ ลับมาก หรือ ลับที่สุด เพื่อจำแนกความแตกต่างของชุดข้อมูลภายในหน่วยงานหรือแนวปฏิบัติตามข้อกำหนดอื่น ๆ

‘	คำนิยาม
เปิดเผยสาธารณะ	เป็นข้อมูลที่สามารถเปิดเผยให้บุคคลภายนอกได้รับรู้ รับทราบ โดยไม่จำเป็นต้องร้องขอ
เผยแพร่ในองค์กร	เป็นข้อมูลที่องค์กรไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปจะเกี่ยวข้องกับข้อมูลที่มีลักษณะเป็นส่วนตัว (Private) ไม่ว่าจะกับข้อมูลบุคคลหรือองค์กร และแม้ว่าการสูญเสียหรือการเปิดเผยข้อมูลอาจไม่ส่งผลให้เกิดผลกระทบที่สำคัญ แต่ก็ไม่พึงประสงค์ที่ให้เปิดเผยโดยไม่ได้รับอนุญาต
ลับ	เป็นข้อมูลที่มีระดับ Confidential หรือ Sensitive จะก่อให้เกิดความสูญเสีย หากมีการเปิดเผยต่อบุคคล/องค์กรที่ไม่ได้รับอนุญาตและส่งผลให้เกิดความอับอายอย่างมากต่อบุคคล/องค์กร และอาจเป็นผลทางกฎหมาย หรือจะก่อให้เกิดความเสียหายแก่ผลประโยชน์แก่เจ้าของข้อมูล
ลับมาก	เป็นข้อมูลที่จัดระดับ Secret หรือ Medium Sensitive สงวนไว้สำหรับข้อมูลที่จะก่อให้เกิดความสูญเสีย/ผลกระทบร้ายแรง อาจทำให้ชื่อเสียง และการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรง หรือ ที่มีนัยสำคัญ (Importance) หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม
ลับที่สุด	เปิดเผยไม่ได้/เป็นเอกสารปกปิด เป็นข้อมูลที่จัดระดับ Top Secret หรือ Highly Sensitive จำกัดการใช้/ไม่เปิดเผยสำหรับข้อมูลที่จะก่อให้เกิดความสูญเสีย/ผลกระทบ ร้ายแรงที่สุด อาจทำให้ชื่อเสียงและการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและผลประโยชน์ขององค์กรอย่างร้ายแรง หรือที่สำคัญยิ่งยวด (Vital) หากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม

7.4.3 กำกับดูแลและติดตามอย่างต่อเนื่อง โดยตรวจสอบความปลอดภัยการใช้งานและรูปแบบการเข้าถึง ของระบบและข้อมูล ทั้งผ่านกระบวนการอัตโนมัติหรือโดยบุคคล เพื่อระบุภัยคุกคามภายนอก การบำรุงรักษา การทำงานของระบบตามปกติ และการติดตั้งโปรแกรมเพื่อปรับปรุงและติดตามการเปลี่ยนแปลงของสภาพ แวดล้อมของระบบและข้อมูล

7.5 การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล

7.5.1 กำหนดนโยบาย แนวปฏิบัติ และสภาพแวดล้อมการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ที่เอื้อต่อการรักษาความมั่นคงปลอดภัย คุ้มครองความเป็นส่วนตัวของข้อมูล และเพื่อให้ได้ข้อมูลที่มี คุณภาพ

7.5.2 จัดทำแนวปฏิบัติการจัดการชุดข้อมูล รวมถึงการรักษาความปลอดภัยตามหมวดหมู่และประเภท ชั้นความลับตามแนวทางที่เหมาะสม และปรับปรุงอย่างต่อเนื่องให้สอดคล้องกับสถานการณ์

7.5.3 จัดเก็บข้อมูลให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ โดย ข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน พร้อมทั้งกำหนดสิทธิและจัดหาระบบ/เครื่องมือ ที่ใช้ในการเข้าถึงข้อมูล เพื่อรักษาความมั่นคงปลอดภัยและคุณภาพข้อมูล และทำลายข้อมูลตาม แนวปฏิบัติและกฎหมายที่เกี่ยวข้อง

7.5.4 จัดทำแนวปฏิบัติและมาตรฐานการประมวลผลและใช้ข้อมูล เพื่อผู้ใช้นำข้อมูลไปใช้อย่างถูกต้องตามวัตถุประสงค์ที่ต้องการเพื่อให้เกิดประโยชน์สูงสุด

7.5.5 ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย และแนวปฏิบัติ ไม่ว่าข้อมูลจะ อยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม และต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของ ข้อมูลก่อนการเปิดเผยข้อมูล รวมทั้งจัดให้มีช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

7.5.6 กำหนดกระบวนการ เทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล และจัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

7.5.7 จัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย ด้านคุณภาพข้อมูล และด้านคุ้มครองความ เป็นส่วนตัวของข้อมูล รวมถึงแนวปฏิบัติให้กับผู้ประสานงาน และตรวจสอบให้แน่ใจว่าได้บริหารจัดการข้อมูลอย่างเหมาะสมตามแนวทางหรือแนวปฏิบัติที่ กำหนดไว้

7.5.8 สร้างความรู้ความเข้าใจในการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ให้แก่ผู้เกี่ยวข้องทั้ง ภายในและภายนอกหน่วยงาน

7.6 การทำลายข้อมูล

7.6.1 เจ้าของข้อมูล (Data Owner) มีหน้าที่ปฏิบัติดังนี้

7.6.1.1 ให้ทำลายข้อมูลสำคัญหรือข้อมูลส่วนบุคคลในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

7.6.1.2 มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญหรือข้อมูลส่วนบุคคลในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลนั้นได้

7.6.1.3 เมื่อมีความจำเป็นต้องทำลายข้อมูลที่มีความสำคัญหรือข้อมูลส่วนบุคคลบนสื่อบันทึกข้อมูล ให้ทำลายข้อมูลในสื่อบันทึกข้อมูล เพื่อป้องกันการกู้คืน โดยใช้วิธีการปฏิบัติดังนี้

- ประเภท Flash Drive ใช้วิธีการทุบหรือบดให้เสียหาย
- ประเภทกระดาษ ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
- ประเภทแผ่น CD/DVD ใช้การหั่นด้วยเครื่องหั่นทำลายแผ่น CD/DVD หรือเจาะ หรือทุบทิ้งทำลาย

- ประเภทฮาร์ดดิสก์ ใช้วิธีการทุบ บดให้เสียหาย หรือเจาะ หรือทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) หรือการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ
- ประเภทฮาร์ดดิส SSD ทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) หรือการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ

ทั้งนี้ บริษัทฯ สามารถใช้การจ้างหน่วยงานภายนอกเพื่อทำลายสื่อบันทึกข้อมูล โดยต้องเก็บสื่อบันทึกข้อมูลไว้ในสถานที่ที่ล็อคไว้ เพื่อให้หน่วยงานภายนอกมาที่บริษัทฯ และทำลายข้อมูล โดยมีบุคลากรของบริษัทฯ ติดตามและควบคุมการดำเนินงานตลอดกระบวนการทั้งหมด และเก็บบันทึกไว้เป็นหลักฐานด้วย

รอบการทำลายข้อมูลปีละ 1 ครั้ง เดือน มกราคม-กุมภาพันธ์