Jaymart

บริษัท เจ มาร์ท จำกัด (มหาชน)

นโยบายเทคโนโลยีสารสนเทศ

(นางสาวยุวดี พงษ์อัชฌา)	(นางมณี สุนทรวาทิน)
กรรมการ บริษัท เจ มาร์ท จำกัด (มหาชน)	กรรมการ บริษัท เจ มาร์ท จำกัด (มหาชน)

Jaymart	นโยบายเทคโนโลยีสารสนเทศ		
รหัสเอกสาร :	จัดทำครั้งที่ 1	วันที่บังคับใช้ : 1 มี.ค. 2565	21 หน้า

หมวดที่ 1 บทสรุปผู้บริหาร

บริษัทเจ มาร์ท จำกัด (มหาชน) (องค์กร) คำนึงถึงความสำคัญของการนำเทคโนโลยีสารสนเทศ เข้ามาเพิ่มศักยภาพการดำเนินการขององค์กร เพื่อให้เกิดกระบวนการการบริการจัดการที่เป็นระบบ มีระเบียบ เป็นขั้นตอน ลดความซ้ำซ้อน และตอบสนองความต้องการของผู้ใช้บริหาร และช่วยให้การดำเนินธุรกิจมีความต่อเนื่อง

องค์กรจึงได้เล็งเห็นว่าในการนำเทคโนโยลีสารสนเทศเข้ามาใช้ในการดำเนินการ จำเป็นต้องกำหนดแนวทางการพัฒนาให้สอดคล้องกับกลยุทธ์ และวิสัยทัศน์ขององค์กร รวมถึงกฎหมาย ข้อบังคับ มาตรฐานสากลต่างๆ ที่เกี่ยวข้องและการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศในปัจจุบัน เพื่อให้การให้บริหารทางด้านเทคโนโลยีสารสนเทศ เป็นไปอย่างมีประสิทธิภาพ มีประสิทธิผล มีความมั่นคงปลอดภัย และมีกรอบในการบริการจัดการเทคโนโลยีสารสนเทศที่ดี รวมถึง เพื่อให้ผู้ที่เกี่ยวข้องเกิดความเชื่อมั่นในการให้บริการระบบสารสนเทศของเจ มาร์ท กรุ๊ป

หมวดที่ 2 บททั่วไป

ส่วนที่ 2.1 วัตถุประสงค์

เพื่อให้องค์กรมีแนวนโยบายในการดำเนินงาน หรือการจัดการทางด้านเทคโนโลยีสารสนเทศ และให้ผู้ที่เกี่ยวข้องกับสารสนเทศ ทั้งผู้บริหาร บุคลากรในองค์กร หน่วยงานภายนอกและบุคลากรภายนอกที่เข้ามาเกี่ยวข้องกับสารสนเทศขององค์กรได้มีแผนงาน และกรอบการปฏิบัติที่ชัดเจน อันจะนำไปสู่การประสานงานในการให้บริการที่มีประสิทธิภาพ มีความปลอดภัยในการให้บริการสูงสุด และมีมาตรฐานยิ่งขึ้น อีกทั้งกำหนดมาตรการป้องกันที่เหมาะสมเพื่อควบคุมและลดความเสียหายต่างๆที่อาจเกิดขึ้นจากกรณีที่ทรัพย์สินไม่สามารถใช้งานได้ สูญหาย เสียหาย บกพร่อง หรือถูกคุกคามด้านความมั่นคงปลอดภัย

ส่วนที่ 2.2 กฎหมายและกฎระเบียบที่เกี่ยวข้อง

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2558 และ (ฉบับที่ 3) พ.ศ. 2558
- พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553
- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2556
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

ส่วนที่ 2.3 บทบังคับใช้และบทลงโทษ

นโยบายเทคโนโลยีสารสนเทศฉบับนี้ ให้มีผลบังคับใช้นับจากวันที่ประกาศให้มีผลบังคับใช้ต่อผู้ใช้งานระบบสารสนเทศของ บริษัท เจ มาร์ท จำกัด (มหาชน) และบริษัทย่อย ทั้งหมดโดยไม่มีการยกเว้น ผู้ฝ่าฝืนจะมีความผิดและต้องได้รับการลงโทษทางวินัยตามระเบียบที่องค์กรกำหนดไว้

ส่วนที่ 2.4 การเผยแพร่นโยบาย

ฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการประกาศและเผยแพร่นโยบายไปยังผู้ใช้งานระบบสารสนเทศขององค์กร เพื่อช่วยให้เกิดความเข้าใจในบทบาทของตนเองในการใช้งานเทคโนโลยีสารสนเทศและปกป้องทรัพย์สินขององค์กร

ส่วนที่ 2.5 การทบทวนนโยบาย

นโยบายเทคโนโลยีสารสนเทศนี้ต้องได้รับการทบทวน ปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญของสภาพแวดล้อมต่างๆ เช่น สภาพธุรกิจ กฎเกณฑ์ กฎหมายและเทคโนโลยี เป็นต้น โดยถือเป็นหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศในการทบทวนปรับปรุง โดยมีผู้บริหารฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ควบคุมให้เกิดการทบทวนและปรับปรุงตามที่ได้กำหนดไว้

หมวดที่ 3 บทบาทและความรับผิดชอบ

ส่วนที่ 3.1 ประธานกรรมการบริษัท

- อนุมัตินโยบายเทคโนโลยีสารสนเทศ รวมถึงการเปลี่ยนแปลงที่อาจจะมีขึ้น
- อนุมัติเรื่องที่คณะกรรมการนำเสนอซึ่งเกี่ยวข้องกับนโยบายเทคโนโลยีสารสนเทศ
- รับผิดชอบโดยรวมในความมั่นคงปลอดภัยด้านสารสนเทศของทรัพย์สิน เพื่อให้มั่นใจว่า
    - นโยบายเทคโนโลยีสารสนเทศที่ถูกจัดทำขึ้นครอบคลุมสารสนเทศที่มีความสำคัญ
    - การปฏิบัติสอดคล้องกับวัตถุประสงค์ทางธุรกิจขององค์กรและความต้องการของผู้ใช้งาน

ส่วนที่ 3.2 ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการ และผู้ช่วยกรรมการผู้จัดการ

- อนุมัติระเบียบปฏิบัติ รวมถึงการเปลี่ยนแปลงที่อาจจะมีขึ้น
- กำหนดทิศทาง และให้การสนับสนุนในการจัดทำนโยบายเทคโนโลยีสารสนเทศ รวมถึงระเบียบปฏิบัติที่เกี่ยวข้อง
- ตัดสินใจในการติดต่อกับหน่วยงานบังคับใช้กฎหมาย และหน่วยงานสืบสวน เมื่อมีข้อสงสัยว่ามีการกระทำผิดร้ายแรงเกิดขึ้น
- อนุมัติ และสนับสนุนกิจกรรมโครงการความมั่นคงปลอดภัยด้านสารสนเทศ และเป็นหลักในการริเริ่มให้มีการสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสรเทศ
- ทบทวน สรุป และนำเสนอต่อประธานกรรมการบริษัท เพื่อขออนุมัติประกาศใช้นโยบายเทคโนโลยีสารสนเทศ รวมถึงการเปลี่ยนแปลงที่อาจจะมีขึ้น

ส่วนที่ 3.3 ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO)

- กำหนดผู้รับผิดชอบต่อทรัพย์สินและวิเคราะห์ความเสี่ยงของทรัพย์สิน รวมถึงบริหารจัดการทรัพย์สินที่อยู่ภายใต้การดูแล ให้คงสภาพการป้องกันความลับ ความสมบูรณ์ครบถ้วน และความพร้อมใช้งานของทรัย์สินนั้นๆ
- กำหนดบทบาทหน้าที่และความรับผิดชอบ ในการปฏิบัติงานด้านความมั่นคงปลอดภัยของบุคลากร โดยยึดถือตามนโยบายเทคโนโลยีสารสนเทศที่กำหนดไว้
- กำหนดให้ให้มีการให้ความรู้ในเรื่องของนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติที่เกี่ยวข้อง ต่อบุคคลภายในองค์กรและหน่วยงานภายนอกที่เกี่ยวข้อง
- กำหนดความสำคัญ การริเริ่ม และลงมือปฏิบัติตามนโยบายสารสนเทศ เพื่อให้บุคลากรในหน่วยงานปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศ อาทิ การกำหนดวิธีการตรวจสภาพแวดล้อมของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร
- ทบทวนและอนุมัติความต้องการด้านความมั่นคงปลอดภัยของระบบ ที่จะนำไปใช้กับข้อมูลสารสนเทศที่มีความอ่อนไหว (Sensitive) หรือสำคัญมากต่อการปฏิบัติการทางธุรกิจ การเริ่มต้นพัฒนาโครงการ (Project Development)
- กำกับดูแลให้มีการทำสัญญาข้อตกลงการรักษาความลับขององค์กร (Non-Disclosure Agreement หรือ NDA) ต่อบุคลากรภายในองค์กรและหน่วยงานภายนอกที่เกี่ยวข้อง โดยระบุความต้องการเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติที่อาจส่งผลต่อการละเมิดสัญญาข้อตกลงต่างๆ
- กำกับให้มีสัญญาเกี่ยวกับการใช้หรือประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement or DPA) ระหว่างกันเพื่อปกป้องจากการที่คู่สัญญานำข้อมูลไปใช้งานหรือได้ข้อมูลมาโดยไม่ถูกต้องได้
- ชี้แจงการเปลี่ยนแปลงที่อาจจะมีขึ้น ที่ส่งผลต่อการปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติในส่วนงานที่รับผิดชอบ
- ตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นเหตุการณ์ที่มีผลกระทบด้านลบต่อหน่วยงานหรือทั้งองค์กร อาทิ เหตุการณ์ที่ส่งผลอย่างยิ่งต่อภาพพจน์ขององค์กร ความเชื่อมั่นของลูกค้า การดำเนินการขององค์กร โดยต้องรายงานต่อประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการและผู้ช่วยกรรมการผู้จัดการ
- ให้การสนับสนุนในการสืบสวน และเสนอแนวทางแก้ไขต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- วิเคราะห์ ประเมินผล และสรุปผลประเด็นซึ่งมีการกระทบอย่างยิ่งยวดต่อทั้งองค์กร อาทิ สัญญากับผู้ขาย ซึ่งผู้ฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรอย่างรุนแรง การขาย การจำหน่าย การแจก หรือการโอนถ่ายซอฟต์แวร์ขององค์กร รวมทั้งทรัพย์สินทางปัญญาไปยัง บุคคลอื่น การเปิดเผยข้อมูลสารสนเทศที่สำคัญ การเปลี่ยนแปลงที่สำคัญต่อเว็บไซต์ขององค์กร พร้อมทั้งนำเสนอต่อประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการ และผู้ช่วยกรรมการผู้จัดการ เพื่อรับทราบและพิจารณาแนวทางบริหารจัดการต่อไป
- กำกับให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นแบบแผนและมีการนำกระบวนการวิเคราะห์ผลกระทบธุรกิจมาใช้
- พิจารณาคัดเลือกบุคคลผู้ที่เกี่ยวข้องกับการกำเนินการในการติดต่อกับหน่วยงาน บังคับใช้กฎหมาย และหน่วยงานสืบสวน เมื่อมีข้อสงสัยว่ามีการกระทำผิดร้ายแรงเกิดขึ้น และการนำเสนอต่อประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการ และผู้ช่วยกรรมการผู้จัดการ

- นำเสนอนโยบายเทคโนโลยีสารสนเทศรวมถึงรายงานการเปลี่ยนแปลงนโยบายที่เกิดขึ้นต่อประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการ และผู้ช่วยกรรมการผู้จัดการ
- ให้คำแนะนำแก่กลุ่มบุคคลที่เหมาะสม ในเรื่องการวัดผล เพื่อปรับปรุงกระบวนการที่กี่ยวข้องกับการให้บริการและการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงการควบคุมให้ดีขึ้น
- ทบทวน และอนุมัติความต้องการที่จำเป็นในการให้บริการและการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่จะต้องใช้กับข้อมูลสารสนเทศที่มีความอ่อนไหวหรือสำคัญต่อการปฏิบัติงานในเชิงธุรกิจก่อนเริ่มต้นออกแบบโครงการด้านเทคโนโลยีสารสนเทศ
- ทบทวน และอนุมัติการดำเนินกิจกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศในระดับหน่วยงาน ซึ่งอาจมีผลกระทบในระดับองค์กรได้

ส่วนที่ 3.4 ผู้ดูแลระบบ

- ระบุกฎเกณฑ์การกำหนดสิทธิ์ในการเข้าถึงข้อมูลและทรัพย์สิน เช่น บทบาทของผู้ใช้งานหรือขององค์กร แนวทางในการขออนุมัติเข้าถึงทรัพย์สิน เป็นต้น พร้อมทั้งแจ้งให้กลุ่มผู้ที่เกี่ยวข้องรับทราบในการเปลี่ยนแปลงกฎเกณฑ์ที่เกิดขึ้น
- พัฒนา และจัดทำขั้นตอนการปฏิบัติงาน เพื่อให้แน่ใจว่าสอดคล้องตามนโยบายเทคโนโลยีสารสนเทศ
- ควบคุมดูแลระบบสารสนเทศให้คงสภาพการรักษาความลับ ความสมบูรณ์ครบถ้วน และความพร้อมใช้ของทรัพย์สินที่ให้บริการระบบสารสนเทศซึ่งอยู่ภายใต้การดูแล และควบคุมการเข้าถึงทรัพย์สิน เพื่อเป็นการป้องกันทรัพย์สินอย่างเหมาะสม
- เตรียมการช่วยเหลือทางด้านเทคนิคแก่ผู้เป็นเจ้าของทรัพย์สิน เพื่อนำเอาการควบคุมที่เหมาะสมมาใช้ในการดูแลทรัพย์สิน
- ให้ความช่วยเหลือในการคัดเลือกและประเมินด้านความมั่นคงปลอดภัยสารสนเทศ ในส่วนที่เกี่ยวข้องกับฮาร์ดแวร์ และ/หรือ ซอฟต์แวร์ ที่นำมาใช้งานในองค์กร
- แจ้งให้เจ้าของทรัพย์สิน และผู้ที่เกี่ยวข้องรับทราบในกรณีที่พบหรือสงสัยว่าทรัพย์สินที่ให้บริการระบบสารสนเทศขององค์กรถูกคุกคาม (Compromise) หรือสูญเสีย หรือเสียหาย รวมทั้งกรณีที่มีการละเมิดต่อนโยบายเทคโนโลยีสารสนเทศหรือระเบียบปฏิบัติที่เกี่ยวข้อง
- ตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และช่วยเหลือในการสอบสวน รวมถึงแก้ไขปัญหาในส่วนที่ทราบหรือสงสัยว่าทรัพย์สินขององค์กรถูกคุกคาม หรือเหตุการณ์ที่ต้องสงสัยว่ามีการโจมตีระบบรักษาความมั่นคงปลอดภัยสารสนเทศหรือเป็นการกระทำที่ไม่เหมาะสมและแจ้งผลลัพธ์ให้เจ้าของทรัพย์สินและผู้ที่เกี่ยวข้องทราบ

ส่วนที่ 3.5 ผู้พัฒนาระบบ

- ยึดมั่นถึงความต้องการที่ระบุไว้ในนโยบายเทคโนโลยีสารสนเทศ และกฎระเบียบ หรือมาตรฐานที่เกี่ยวข้องในการพัฒนาระบบ โดยประกอบไปด้วยการออกแบบ การพัฒนา การนำเอาระบบมาใช้งาน และการบำรุงรักษาระบบ เพื่อให้มั่นใจว่ามีการปฏิบัติที่เหมาะสมในการควบคุมการพัฒนาระบบที่เพียงพอ

ส่วนที่ 3.6 ฝ่ายเทคโนโลยีสารสนเทศ

- พัฒนาและปรับปรุงนโยบายสารสนเทศให้เป็นปัจจุบัน และสอดคล้องต่อการดำเนินงานธุรกิจรวมถึงกฎหมาย หรือข้อกำหนดที่เกี่ยวข้อง
- พัฒนาและปรับปรุงระเบียบปฏิบัติ หรือขั้นตอนการปฏิบัติงานที่มีความสอดคล้องกับนโยบายเทคโนโลยีสารสนเทศและมาตรฐานสากล
- นำเสนอการปรับปรุงนโยบายเทคโนโลยีสารสนเทศและระเบียบปฏิบัติ ต่อผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เพื่อพิจารณาเห็นชอบและนำเสนอขออนุมัติต่อไป
- เผยแพร่ให้ผู้ใช้งานทราบถึงนโยบายเทคโนโลยีสารสนเทศขององค์กร และระเบียบปฏิบัติที่เกี่ยวข้อง
- เผยแพร่ให้ผู้ใช้งานทราบถึงการตรวจสอบระบบ และการตรวจสอบกิจกรรมทางเครือข่าย
- จัดเตรียมแนวทางการติดตามการบังคับใช้นโยบายเทคโนโลยีสารสนเทศและระเบียบปฏิบัติ เพื่อให้มั่นใจว่าผู้ใช้งานระบบสารสนเทศทุกคนมีความตระหนักถึงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร กฎหมายลิขสิทธิ์และกฎหมายทรัพย์สินทางปัญญา และบทบัญญัติอื่นๆที่บังคับใช้ในปัจจุบัน

ส่วนที่ 3.7 ฝ่ายกฎหมาย

- ให้ข้อแนะนำทางกฎหมายที่เกี่ยวข้องกับระเบียบ วิธีการปฏิบัติสำหรับการตรวจสอบการใช้ระบบสารสนเทศและอุปกรณ์ประมวลผลต่างๆ รวมถึงการรวบรวม และการป้องกันสิ่งที่เป็นหลักฐานที่ต้องการสำหรับการลงโทษทางวินัยภายในองค์กร และการเอาผิดในทางแพ่งหรืออาญา

ส่วนที่ 3.8 ส่วนตรวจสอบระบบงาน

- สอบทานการนำนโยบายเทคโนโลยีสารสนเทศมาใช้ และประเมินผลการปฏิบัติตามนโยบาย ระเบียบปฏิบัติ และขั้นตอนปฏิบัติงานที่เกี่ยวข้อง รวมถึงประสิทธิภาพของนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนวัดผลการควบคุมภายใน โดยถือเป็นส่วนหนึ่งของตารางการตรวจสอบเป็นประจำและรายงานผลการตรวจสอบภายในไปยังผู้บริหารที่เกี่ยวข้องได้รับทราบเพื่อพิจารณาดำเนินการ

ส่วนที่ 3.9 ผู้ใช้งาน

- ทำความเข้าใจกับนโยบาย ระเบียบปฏิบัติ และขั้นตอนปฏิบัติบัติงานต่างๆที่องค์กร หรือหน่วยงานได้กำหนดไว้ รวมถึงให้ความร่วมมือในการใช้กฎข้อบังคับต่างๆ
- ลงนามยินยอม และปฏิบัติตามข้อตกลงไม่เปิดเผยความลับขององค์กร
- ใช้ทรัพย์สินขององค์กรอย่างมีประสิทธิภาพ มีจริยธรรม และถูกต้องตามกฎหมาย
- รายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศแก่ผู้บังคับบัญชา และฝ่ายเทคโนโลยีสารสนเทศให้ทราบโดยทันที และช่วยเหลือในการสนองตอบต่อเหตุกาณ์เหล่านั้น

ส่วนที่ 3.10 หน่วยงานภายนอก

- ลงนามและปฏิบัติตามข้อตกลงไม่เปิดเผยความลับขององค์กร
- ยึดถือการปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศขององงค์กรต่อการให้บริการของบุคคลที่สาม และกระทำการใด ตามความจำเป็นเพื่อป้องกันความลับของข้อมูลสารสนเทศ และระบบต่างๆ ที่องค์กรจัดเตรียมไว้เพื่อใช้งาน
- เข้าถึงระบบสารสนเทศเฉพาะสิทธิ์ที่ได้รับเท่านั้น
- ทำสัญญาข้อตกลงการรักษาความลับขององค์กร (NDA) ข้อมูลสารสนเทศที่ได้รับจากการเก็บรวบรวมหรือเข้าถึงในระหว่างที่มีการทำงานกับองค์กร ให้ถือเป็นความลับ ห้ามทำการใดๆ อันเกี่ยวข้องการการใช้ การเปิดเผย ส่ง หรือ แก้ไขข้อมูลสารสนเทศที่ได้มา โดยไม่มีการยินยอมอย่างชัดเจนจากหน่วยงานขององค์กรที่ทำหน้าที่กำกับดูแลดำเนินการ
- ในกรณีที่มีการใช้หรือประมวลผลข้อมูลส่วนบุคคลกับบริษัท ให้ทำสัญญาเกี่ยวกับการใช้หรือประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement or DPA) ระหว่างกัน เพื่อปกป้องการนำข้อมูลไปใช้งานหรือได้ข้อมูลมาโดยไม่ถูกต้อง
- รายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นทันที ให้แก่หน่วยงานขององค์กรที่ทำหน้าที่กำกับดูแลการดำเนินงานและฝ่ายเทคโนโลยีสารสนเทศ รวมถึงช่วยเหลือการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

หมวดที่ 4 คำจำกัดความ

นโยบายเทคโนโลยีสารสนเทศ ได้กำหนดคำนิยามของคำศัพท์ที่ใช้ในนโยบายฉบับนี้ เพื่อให้เข้าใจถึงความหมายตรงกันและอ้างอิงได้ถูกต้อง ดังต่อไปนี้

คำศัพท์	ความหมาย
	หน่วยงาน
องค์กร	บริษัท เจ มาร์ท จำกัด (มหาชน) และบริษัทย่อย
บริษัทย่อย	บริษัท เจ มาร์ท จำกัด (มหาชน) มีอำนาจควบคุมได้
ฝ่ายเทคโนโลยีสารสนเทศ	หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศขององค์กร
	บุคคล
ผู้บริหารระดับฝ่าย	ผู้บริหารสูงสุดของแต่ละฝ่ายงาน
ผู้มีอำนาจ	ผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายขึ้นไป หรือผู้ที่ได้รับมอบหมายให้มีหน้าที่ตัดสินใจ
ผู้ดูแลระบบ (Administrator)	
บุคลากร	บุคลากรของบริษัท เจ มาร์ท จำกัด (มหาชน) และบริษัทย่อย
บุคลากรภายนอก	บุคคล หรือพนักงานของหน่วยงานภายนอกที่มาติดต่อสื่อสาร และมีการเข้าถึงทรัพย์สินสารสนเทศขององค์กร

คำศัพท์	ความหมาย
ผู้ให้บริการภายนอก / หน่วยงานภายนอก (Third Party)	ผู้ค้า หุ้นส่วนการค้า ผู้ให้บริการ/จำหน่ายระบบ (Vendor) พนักงานสัญญาจ้าง (Outsource) และบุคคล หรือนิติบุคคลอื่นใดทั้งในประเทศและต่างประเทศที่ให้บริการด้านเทคโนโลยีสารสนเทศ ซึ่งเข้าทำสัญญาหรือทำข้อตกลงในการให้บริการให้กับองค์กร รวมถึงหน่วยงานผู้รับจ้างช่วงที่ผู้ให้บริการภายนอกเป็นผู้จัดจ้าง โดยได้รับอนุญาตให้มีสิทธิ์เข้าถึงสถานที่หรือทรัพย์สินสารสนเทศขององค์กร และใช้งานระบบสารสนเทศขององค์กรตามอำนาจหน้าที่ที่รับผิดชอบ
ผู้ใช้งาน (User)	บุคลากร บุคคลภายนอก และหน่วยงานภายนอก ที่ใช้งานระบบคอมพิวเตอร์ขององค์กร
เจ้าของโครงการ	หน่วยงานภายในบริษัท เจ มาร์ท จำกัด (มหาชน) และบริษัทย่อย ที่เป็นผู้รับผิดชอบในการดำเนินงานโครงการที่มีการจัดจ้างผู้ให้บริการภายนอก/หน่วยงานภายนอกเข้ามาปฏิบัติงานให้กับองค์กร
เจ้าของทรัพย์สิน / เจ้าของข้อมูล (Data Owner)	บุคคล ส่วนงาน หรือฝ่ายงานผู้เป็นเจ้าของข้อมูล หรือเป็นผู้ที่ได้รับความเสียหายสูงสุดเมื่อข้อมูลนั้นเสียหายหรือถูกเปิดเผย
	คำอื่น ๆ
ข้อมูล	ข้อความ ข่าวสาร เอกสาร เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ ที่อยู่ในรูปของตัวเลข ภาษา ภาพ สัญลักษณ์ต่างๆ ที่ยังไม่ผ่านการประมวลผล ทั้งที่อยู่ในรูปอิเล็กทรอนิกส์หรืออยู่ในรูปสื่อสิ่งพิมพ์ และให้ความหมายรวมถึงข้อมูลคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
ข้อมูลอิเล็กทรอนิกส์	ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร
ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้ความหมายรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
บัญชีผู้ใช้ (User Name หรือ Account)	กลุ่มของข้อมูลที่ใช้ในการอ้างถึงเพื่อระบุตัวตน สิทธิ์การเข้าถึง และข้อจำกัดต่างๆในการเข้าถึงระบบสารสนเทศ
รหัสผ่าน (Password)	กลุ่มอักขระที่ใช้ในการพิสูจน์ตัวตน ใช้เพื่อควบคุมการเข้าถึงระบบสารสนเทศ หรือข้อมูลสารสนเทศ
สิทธิระดับสูง (Privilege)	สิทธิ์ที่สามารถใช้งาน โดยได้รับสิทธิ์มากกว่าสิทธิ์ของผู้ดูแลระบบหรือผู้ใช้งานทั่วไปในระบบ เช่น Root หรือ Administrator
ระบบสารสนเทศ	ระบบคอมพิวเตอร์ ระบบเก็บข้อมูล ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบสื่อสารข้อมูลทุกประเภท อุปกรณ์สื่อสาร เครื่องพิมพ์ เครื่องสแกนหรืออุปกรณ์ใดๆ ที่เกี่ยวข้องที่เป็นกรรมสิทธิ์ขององค์กร และ/หรือ ที่องค์กรได้รับอนุญาตให้ใช้ได้ตามกฎหมาย
ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)	การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

คำศัพท์	ความหมาย
เหตุขัดข้อง (Incident)	เหตุขัดข้องที่ส่งผลทำให้ระบบสารสนเทศไม่สามารถให้บริการได้ตามที่กำหนดไว้หรือคุณภาพในการให้บริการลดลง เช่น ระบบอีเมลไม่สามารถใช้งานได้ เครื่องแม่ข่ายขัดข้อง หรือ ระบบงานประมวลผลช้าผิดปกติ เป็นต้น
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
การเข้ารหัสลับ (Encryption)	การเปลี่ยนแปลงรูปแบบของข้อมูลให้อยู่ในรูปแบบที่มีความมั่นคงปลอดภัย โดยใช้กุญแจในการเข้ารหัสลับ เพื่อที่ผู้เข้าถึงข้อมูลจะไม่สามารถทราบเนื้อหาที่แท้จริงของข้อมูลได้ ถ้าไม่มีการถอดรหัสลับจากกุญแจที่ใช้ในการถอดรหัสที่ถูกต้อง ทั้งนี้ขึ้นอยู่กับเทคนิคของการเข้ารหัสลับข้อมูลที่ใช้ โดยลักษณะของการเข้ารหัสลับมีด้วยกัน 2 ประเภทคือ 1. การเข้ารหัสแบบสมมาตร (Symmetric Key Encryption) เป็นการเข้ารหัสที่ใช้กุญแจรหัสเดียวในการเข้ารหัสและถอดรหัส เรียกว่า กุญแจลับ (Secret Key) 2. การเข้ารหัสแบบอสมมาตร (Asymetrix Key Encryption or Public Key Cryptography) เป็นการเข้ารหัสในลักษณะที่มีกุญแจคู่เรียกว่ากุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) โดยนโยบายฉบับนี้เรียกว่ากุญแจคู่
กุญแจ (Key)	กุญแจที่ใช้ในกระบวนการเข้ารหัสลับ หรือถอดรหัสลับ ขึ้นอยู่กับการใช้งานเทคนิค การเข้ารหัสลับข้อมูล โดยแยกเป็น 2 ประเภทคือ 1. กุญแจลับ (Secret Key) ซึ่งใช้การเข้ารหัสลับแบบสมมาตร (Symmetric Key Encryption) ตัวอย่างของอัลกอรึทึม สำกรับการเข้ารหัสแบบสมมาตรเช่น 3DES, RC5, RC6, AE5 เป็นต้น 2. กุญแจคู่ ซึ่งใช้ในการเข้ารหัสแบบอสมมาตร (Asymmetric Key Encryption or Public Key Cryptography) ประกอบไปด้วย กุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) ตัวอย่างของอัลกอรึทึมสำหรับการเข้ารหัสแบบอสมมาตร เช่น RSA (Rivest - Shamir-Adleman), Diffie - Hellman Key Exchange Protocol, Elliptic Curve Cryptography (ECC) เป็นต้น
ช่องโหว่ (Vulnerability)	สภาพหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์ของทรัพย์สินสารสนเทศ ซึ่งอาจเกิดจากความบกพร่องในการผลิต หรือการออกแบบ หรือการบริหารจัดการทำให้เกิดจุดอ่อน โดยมีความเสี่ยงที่จะเกิดภัยคุกคามจากช่องโหว่ที่เกิดขึ้น เช่น ช่องโหว่ของโปรแกรมที่ทำให้บุคคลภายนอกสามารถเข้าใช้โปรแกรมได้โดยไม่ต้องผ่านการพิสูจน์ตัวตน
การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัย (Security Awareness)	การให้ความรู้ ความเข้าใจทางด้านความมั่นคงปลอดภัยของสารสนเทศ เพื่อสร้างความตระหนักถึงภัยคุกคามและปัญหาทางด้านความมั่นคงปลอดภัยสารสนเทศแก่บุคลากร
การสำรองข้อมูล (Data Backup)	การทำสำเนาข้อมูลทั้งหมดในระบบที่ต้องการ เพื่อเป็นการสำรองข้อมูลที่อาจมีการก้ไขเปลี่ยนแปลง หรือสูญหายให้สามารถนำกลับมาใช้งานได้
แหล่งข้อมูล (Source of Data and Information)	ที่เก็บข้อมูล หรือสารสนเทศทั้งที่อยู่รูปแบบต่างๆ กัน เช่น ข้อมูลแหล่งข้อมูลเฉพาะและแหล่งข้อมูลกลาง เป็นต้น

คำศัพท์	ความหมาย
ทรัพย์สินสารสนเทศ	หมายถึง 1. อุปกรณ์เทคโนโลยีสารสนเทศ และอุปกรณ์อื่นใดที่ใช้งานร่วมกับอุปกรณ์เทคโนโลยีสารสนเทศที่เกี่ยวข้องทุกประเภท 2. ชุดคำสั่ง โปรแกรมระบบงานสารสนเทศ และโปรแกรมอื่นใดที่ใช้งานร่วมกับโปรแกรมระบบงานสารสนเทศ 3. ข้อมูล ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ และ/หรือ ทรัพย์สินทางปัญญาใดๆ
พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure Area)	คือ บริเวณที่ใช้เก็บรักษาอุปกรณ์สารสนเทศที่ใช้ในงานระบบสารสนเทศ แบ่งได้เป็น 3 ประเภท คือ 1. พื้นที่ห้อง Patching Room 2. พื้นที่ห้องปฏิบัติการคอมพิวเตอร์ 3. พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)
พื้นที่ห้องปฏิบัติการคอมพิวเตอร์ (Computer Operation)	พื้นที่ที่ใช้ในการป้อนข้อมูล ออกรายงาน และปฏิบัติงานเกี่ยวกับระบบงานสารสนเทศขององค์กร
พื้นที่ห้อง (Patching Room)	พื้นที่ที่ใช้เก็บอุปกรณ์ในการเชื่อมต่อเครือข่ายคอมพิวเตอร์ และโทรศัพท์ในแต่ละชั้น
ห้องคอมพิวเตอร์ (Data Center)	พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ที่ใช้เก็บอุปกรณ์คอมพิวเตอร์และเครื่องคอมพิวเตอร์หลักที่สำคัญในระบบงาน เช่น เครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายหลัก
บันทึกเหตุการณ์ (Logs)	บันทึกเหตุการณ์การใช้งานของระบบสารสนเทศ การเข้าใช้งานระบบงานหรือระบบสารสนเทศ การประมวลผลกิจกรรมของระบบสารสนเทศ และเหตุการณ์ทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบถึงประสิทธิภาพความปลอดภัย และความผิดปกติที่เกิดจากการประมวลผลกิจกรรมต่างๆของระบบสารสนเทศ
การเฝ้าระวัง (Monitoring)	การเฝ้าระวังด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อตรวจสอบความผิดปกติจากการประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศ จากบันทึกเหตุการณ์ (Logs) เช่น การเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต การใช้งานสารสนเทศผิดวัตถุประสงค์ และปัญหาที่เกิดจากระบบงาน
ความเสี่ยง (Risk)	โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือการกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถาณการณ์ที่ไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคตและมีผลกระทบหรือทำให้เกิดการดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายของการให้บริการ
โปรแกรมที่ไม่พึงประสงค์ (Malicious Code or Malware)	โปรแกรมหรือ Code ที่เป็นอันตรายต่อประสิทธิภาพ และความปลอดภัยของระบบสารสนเทศไม่ทางใดก็ทางหนึ่ง เช่น ไวรัส (Virus) เวิร์ม (Worm) หรือโทรจัน (Trojan) เป็นต้น
แผนการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Plan)	การสร้างความต่อเนื่องทางธุรกิจ เพื่อป้องกันการติดขัดหรือการหยุดชะงักของระบบงานธุรกรรมที่สำคัญที่อาจมีสาเหตุมาจากภัยทางด้านสิ่งแวดล้อม เหตุการณ์
แผนรองรับกรณีเหตุการณ์ฉุกเฉิน (DRP: Disaster Recovery Plan)	การเตรียมความพร้อมรองรับเหตุฉุกเฉินและแผนการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน เช่น การย้ายสถานที่ปฏิบัติงาน ไปจนถึงการใช้งานระบบสารสนเทศสำรอง

คำศัพท์	ความหมาย
แผนสำหรับย้อนกลับสู่สภาวะเดิม (Fallback Plan)	แผนการดำเนินงานเพื่อใช้ในการกลับสู่สถาณการณ์ดำเนินงานครั้งล่าสุด เพื่อใช้ในกรณีที่การแก้ไขเหตุฉุกเฉินไม่เป็นผลสำเร็จ
ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objectives: RTO	ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อส่งมอบผลิตภัณฑ์ บริการ และกิจกรรมหรือกระบวนการกลับสู่สภาวะปกติหลังจากเกิดเหตุการณ์ไม่พึงประสงค์ที่มีความเสียหายระดับรุนแรง
ระยะเวลสสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหายจากระบบได้ และเพื่อให้เป็นข้อมูลในการออกแบบวิธีการสำรองข้อมูลเพื่อให้ข้อมูลไม่สูญหายเกินกว่าที่กำหนด
ระยะเวลาหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD)	ช่วงเวลาสูงสุดที่การดำเนินงานหยุดชะงัก หากเกินกำหนดช่วงเวลานี้แล้ว จะไม่สามารถทำให้การดำเนินงานฟื้นคืนสู่สภาพปกติได้
ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)	ข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้รับบริการที่อธิบายถึงรายละเอียดการบริการ ระดับการให้บริการที่จะถูกวัดละประเมินผล เป้าหมายของระดับการให้บริการ รวมไปถึงระบุหน้าที่ความรับผิดชอบที่ชัดเจนของทั้งผู้ให้บริการและผู้รับบริการ
ข้อตกลงการให้บริการระดับปฏิบัติงาน (Operational Level Agreement: OLA)	ข้อตกลงในการให้บริการสำหรับปฏิบัติงานร่วมกันระหว่างหน่วยงานภายใน เพื่อสนับสนุนให้การบริการของผู้รับบริการเป็นไปตามข้อตกลงระดับการให้บริการ (SLA)
สัญญาการให้บริการ (Underpinning Contracts: UC)	ข้อตกลงร่วมกันระหว่างผู้ให้บริการ / ผู้จำหน่ายระบบ (Vendor) เพื่อให้บริการผู้รับบริการได้ตามข้อตกลงการให้บริการ (SLA)
ระบบงานที่สำคัญ (High Priority Application System)	หมายถึง ระบบที่ให้บริการธุรกรรมหลักที่ใช้ในการให้บริการลูกค้า หรือระบงานที่นำส่งข้อมูลรายงานแก่ทางราชการ
ระบบพัฒนา (Development Area)	ระบบสารสนเทศที่ใช้ในการพัฒนาระบบงาน โดยเป็นการจำลองทรัพยากร และสภาพแวดล้อมของระบบให้บริการจริง เพื่อใช้พัฒนาระบบงานใหม่
ระบบทดสอบ (Use Acceptance Area)	ระบบสารสนเทศที่ใช้ในการทดสอบโดยเป็นการจำลองทรัพยากร และสภาพแวดล้อมของระบบให้บริการจริงมาเพื่อทดสอบประสิทธิภาพ และความปลอดภัยของระบบที่ได้พัฒนาขึ้น
ระบบสารสนเทศสำรอง (Disaster Recovery Center: DRC)	ระบบงาน ข้อมูล และระบบเครือข่ายสำรองนอกเหนือจากระบบสารสนเทศหลัก เพื่อให้สามารถทำธุรกรรมหลักได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุกาณ์ฉุกเฉิน
ระบบให้บริหารจริง (Production Area)	ระบบสารสนเทศที่ให้บริการจริงแก่ผู้ใช้งานซึ่งต้องมีการรักษาความมั่นคงปลอดภัย และการคงบคุมการเข้าถึงจากการพัฒนาระบบและการทดสอบระบบอย่างเคร่งครัด
อุปกรณ์สื่อสารประเภทพกพา (Mobile Device)	เครื่องคอมพิวเตอร์พกพา (Laptop Computer) สมาร์ทโฟน (Smart Phone) แท็บเล็ตคอมพิวเตอร์ (Tablet Computer) ที่องค์กรอนุญาตให้เชื่อมต่อและใช้งานระบบสารสนเทศขององค์กรได้
สื่อบันทึกข้อมูล (Media)	อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Hard Drive หรือ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Drive เป็นต้น

หมวดที่ 5 นโยบายการบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ

ส่วนที่ 5.1 การบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการบริหาร จัดการกระบวนการเปลี่ยนแปลงระบบสารสนเทศ และลดความผิดพลาดในการดำเนินการเปลี่ยนแปลง รวมถึงระบบงานสามารถสนับสนุนธุรกิจขององค์กรได้อย่างต่อเนื่องและมีประสิทธภาพ

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

5.1.2 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศและให้บันทึกการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร

5.1.3 ผู้ร้องขอและผู้ดำเนินการเปลี่ยนแปลง ต้องดำเนินการวิเคราะห์ผลกระทบและความเสี่ยงในการดำเนินการเปลี่ยนแปลง เพื่อเตรียมมาตรการรองรับการเปลี่ยนแปลงในแต่ละกิจกรรม

5.1.4 ผู้ที่ร้องขอให้มีการเปลี่ยนแปลงจะต้องจัดทำแผนงานตามภาพรวม สำหรับการดำเนินการเปลี่ยนแปลง โดยกำหนดวันเวลาที่ต้องการดำเนินงาน และทรัพยากรที่จำเป็น เป็นต้น และแจ้งให้ผู้ที่เกี่ยวข้องรับทราบถึงแผนการเปลี่ยนแปลง

ส่วนที่ 5.2 การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

วัตถุประสงค์

เพื่อกำหนดแนวทางการบริหารจัดการความต่อเนื่อง ในการให้บริการระบบสารสนเทศ ในกรณีที่เกิดเหตุฉุกเฉินหรือเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศใดๆ ซึ่งอาจส่งผลกระทบให้การดำเนินธุรกิจขององค์กรหยุดชะงัก

5.2.1 องค์กร ต้องจัดให้มีศูนย์คอมพิวเตอร์สำรอง และระบบสารสนเทศสำรอง เพื่อรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเหตุการณ์ที่ส่งผลทำให้การดำเนินธุรกิจหยุดชะงัก โดยมีผู้บริหารระดับสูงสุดขององค์กร เป็นผู้มีอำนาจตัดสินใจ ในการสั่งการ

5.2.2 หน่วยงานผู้ใช้บริการ และฝ่ายเทคโนโลยีสารสนเทศ ต้องร่วมกันกำหนดกรอบมาตรฐาน (Framework) เพื่อให้เกิดความต่อเนื่อง ทางธุรกิจและครอบคลุมข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศที่ได้กำหนดไว้ รวมถึงมีความสะดวกในการจัดลำดับความสำคัญของแผนและกิจกรรมที่ต้องดำเนินการ

5.2.3 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน (Disaster Recovery Plan: DRP) โดยให้มีความสอดคล้องกับแผนการบริหารจัดการความต่อเนื่องทางธุรกิจขององค์กร

5.2.4 ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการสำรองข้อมูล เอกสาร ซอฟต์แวร์ และระบบงาน รวมถึงอุปกรณ์ต่างๆ และบุคลากรที่จำเป็น เพื่อสนับสนุนให้การกู้คืนระบบสารสนเทศให้เป็นไปอย่างรวดเร็วที่สุด หลังจากเกิดการหยุดชะงักในการให้บริการหรือเหตุภัยพิบัติ

5.2.5 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉิน (Disaster and Service Request Plan: DRP) อย่างน้อยปีละ 1 ครั้ง และให้มีการบันทึกผลการทดสอบ เพื่อให้มั่นใจได้ว่าธุรกิจสามารถดำเนินต่อไปได้เมื่อเกิดเหตุการณ์ที่กระทบกับกระบวนการทางธุรกิจขององค์กร

ส่วนที่ 5.3 การจัดการด้านงบประมาณและการควบคุมการใช้จ่ายของการให้บริการ (Budgeting and Accounting for Services Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบริหารจัดการงบประมาณและควบคุมค่าใช้จ่ายที่เกี่ยวข้องกับการสนับสนุนการให้บริการด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

5.3.1 ฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการจัดสรรงบประมาณให้ครบถ้วนและเพียงพอต่อการให้บริการและควบคุมการใช้จ่ายงบประมาณที่เกิดประสิทธิภาพสูงสุด

5.3.2 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีการจัดสรรงบประมาณเป็น 3 หมวด ดังนี้

1. หมวดค่าใช้จ่ายที่เป็นทรัพย์สินสารสนเทศ (IT Asset) แบ่งเป็น 2 ส่วน คือ
   - 1.1 ส่วนของการจัดซื้อจัดจ้างระบบ IT ใหม่ โดยแยกเป็น Hardware, Software หรือรวมทั้งหมด
   - 1.2 ส่วนของการปรับปรุงระบบ IT เดิมให้มีประสิทธิภาพเพิ่มขึ้นหรือซ่อมบำรุงให้สามารถใช้ต่อไปโดยแยก Hardware, Software หรือรวมทั้งหมด
2. หมวดค่าใช้จ่ายที่เป็นสัญญาต่าง ๆ ของระบบ IT (Agreement) ที่จำเป็นต้องใช้งานแบ่งเป็น 3 ส่วน คือ
   - 2.1 ส่วนของสัญญาเช่าวงจรสัญญานความเร็วสูงหรือบริการต่าง ๆ ของ ISP ได้แก่ Leased line, Internet, Co-location, SOC
   - 2.2 ส่วนของสัญญาซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ของสำนักงานใหญ่และห้องศูนย์คอมพิวเตอร์ ได้แก่ Server, Network, Software
   - 2.3 ส่วนของสัญญาการจัดจ้างหน่วยงานภายนอก (Outsourcing) ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ของสาขา ได้แก่ Hardware, Software, Network ภายในสาขา
3. หมวดค่าใช้จ่ายสำหรับเบี้ยเลี้ยงพนักงานในการจัดเตรียมระบบคอมพิวเตอร์สำหรับงานแสดงสินค้าหรืองานขายสินค้าราคาพิเศษนอกสถานที่

5.3.3 ฝ่ายเทคโนโลยีสารสนเทศ ต้องติดตามการใช้งบประมาณ และตรวจสอบงบประมาณคงเหลือเพื่อใช้บริการการใช้งบประมาณได้อย่างมีประสิทธิภาพ

ส่วนที่ 5.4 การบริหารข้อมูลสารสนเทศเพื่อรายงานผลการให้บริการ (Service Reporting Policy)

วัตถุประสงค์

เพื่อให้บริการด้านข้อมูลสำหรับจัดทำรายงานให้กับผู้บริหาร และสนับสนุนการดำเนินงาน ตอบสนองการแข่งขันขององค์กร รวมถึงสนับสนุนให้รายงานต่างๆ มีข้อมูลที่ถูกต้องครบถ้วนและให้ผู้ที่เกี่ยวข้องสามารถใช้งานได้ข้อมูลได้อย่างถูกต้อง

5.4.1 **การจัดหาและบำรุงรักษาแหล่งข้อมูลและรายงานผู้บริหาร**

1) ส่วนงานภายในองค์กร ต้องจัดให้มีรายงานผลการดำเนินงานและข้อมูลต่างๆที่เป็นประโยชน์ต่อการดำเนินธุรกิจแก่ผู้บริหาร เพื่อให้ผู้บริหารใช้เป็นข้อมูลในการตัดสินใจต่อการดำเนินงานได้อย่างรวดเร็วและทันเวลา

2) ส่วนงานภายในองค์กร ควรกำหนดให้ข้อมูลในแหล่งข้อมูลและรายงานผู้บริหาร มีความสำคัญระดับข้อมูลลับเฉพาะ (Highly Restricted) และห้ามเผยแพร่ให้ผู้อื่นทราบโดยไม่ได้รับอนุญาต

3) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดหาแหล่งข้อมูลเพื่อสนับสนุนให้แต่ละส่วนงานสามารถนำข้อมูลไปใช้ในการวิเคราะห์หรือวิจัย เพื่อใช้ในการแข่งขันทางธุรกิจได้อย่างรวดเร็ว

4) ฝ่ายเทคโลยีสารสนเทศ ต้องบำรุงรักษาแหล่งข้อมูลและผลดำเนินงานของข้อมูลต่างๆที่ใช้สำหรับรายงานผู้บริหารให้คงสภาพความถูกต้องและพร้อมใช้อยู่เสมอ

5) ฝ่ายเทคโนโลยีสารสนเทศ ต้องสนับสนุนการพัฒนาทักษะของผู้ใช้ข้อมูลแต่ละส่วนงานให้สามารถสร้างรายงานได้อย่างถูกต้องและมีประสิทธิภาพ

5.4.2 **การเข้าถึงข้อมูลในแหล่งข้อมูล**

1) ผู้ใช้งาน ต้องร้องขอสิทธิ์การใช้งาน/เข้าถึงข้อมูลในแหล่งข้อมูล จากส่วนงานซึ่งเป็นเจ้าของข้อมูลก่อนเข้าถึงแหล่งข้อูลต่างๆ โดยกำหนดกลุ่มของผู้มีสิทธิ์ใช้งานตามขอบเขตข้อมูลเป็น 3 ระดับ ดังนี้

1.1) เข้าถึงข้อมูลทุกคลัง/สาขา

1.2) เข้าถึงข้อมูลเฉพาะคลัง/สาขา

1.3) เข้าถึงข้อมูลเฉพาะเรื่องที่เกี่ยวข้อง

5.4.3 **การควบคุมคุณภาพของข้อมูลในแหล่งข้อมูล**

1) ผู้ใช้งานต้องรับผิดชอบในการทำข้อมูลให้มีความสมบูรณ์ (Data Cleansing) โดยต้องแจ้งขอข้อมูลเพื่อการดำเนินการผ่าน IT Job Request และส่งมายังฝ่ายเทคโนโลยีสารสนเทศ เพื่อให้เจ้าหน้าที่เทคโนโลยีสารสนเทศดำเนินการดึงข้อมูลและปรับปรุงข้อมูลเข้าระบบ

2) กรณีผู้ใช้งานต้องเปลี่ยนแปลงข้อมูลในแหล่งข้อมูล ผู้ใช้งานต้องจัดเตรียมข้อมูลตามกระบวนการทำข้อมูลให้มีความสมบูรณ์ (Data Cleansing) และแจ้งขอดำเนินการเปลี่ยนแปลงข้อมูลผ่าน IT Job Request และส่งมายังฝ่ายเทคโนโยลีสารสนเทศ เพื่อให้เจ้าหน้าที่เทคโนโลยีสารสนเทศดำเนินการปรับปรุงข้อมูลในฐานข้อมูล

ส่วนที่ 5.5 การบริหารจัดการทรัพย์สิน (Asset Management)

วัตถุประสงค์

เพื่อให้สินทรัพย์และระบบสารสนเทศขององค์กรได้รับการปกป้องในระดับที่เหมาะสม เพื่อลดความเสี่ยงต่อการถูกเปิดเผยข้อมูลขององค์กรโดยไม่ได้รับอนุญาต รวมถึงป้องกัน การนำทรัพย์สินสารสนเทศไปใช้โดยผิดวัตถุประสงค์ และเกิดความเสียหายกับทรัพย์สินสารสนเทศขององค์กร

5.5.1 หน้าที่ความรับผิดชอบต่อทรัพยสิน (Responsibility for assets)

1) การจัดทำบัญชีทรัพย์สิน (Inventory of Assets)

1.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องสนับสนุนให้หน่วยงานที่รับผิดชอบจัดทำบัญชีทรัพย์สินสารสนเทศ เพื่อบริหารจัดการและควบคุมทรัพย์สินสารสนเทศอย่างเหมาะสม และให้มีการปรับปรุงบัญชีทรัพย์สินให้เป็นปัจจุบันเสมอ

2) การใช้ทรัพย์สินสารสนเทศ (Acceptable Use of Assets)

2.1) ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำข้อกำหนดในการใช้ทรัพย์สิน เพื่อการบริหารจัดการอุปกรณ์คอมพิวเตอร์ให้เหมาะสมก่อให้เกิดประสิทธิภาพสูงสุด รวมทั้งมีความปลอดภัยจากความเสียหายที่อาจเกิดขึ้นได้ โดยต้องสื่อสารให้บุคลากรขององค์กรรับทราบและปฏิบัติตาม

3) การบ่งชี้สารสนเทศ (Labeling of Information)

3.1) องค์กร ต้องควบคุมให้ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นมีการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม ตั้งแต่เริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้บุคลากรและผู้ที่เกี่ยวข้องต้องปฏิบัติตาม เพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสม

3.2) ฝ่ายเทคโนโลยีสารสนเทศ และหน่วยงานที่กี่ยวข้อง ต้องทำป้ายชื่อตามทะเบียนบัญชีทรัพย์สินและขั้นตอนการใช้งานติดที่อุปกรณ์คอมพิวเตอร์ทุกชิ้น

4) การบริหารจัดการทรัพย์สิน (Handling of Assets)

4.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีขั้นตอนการปฏิบัติงานในการบริหารจัดการทรัพย์สินสารสนเทศ เพื่อมิให้ข้อมูลสำคัญขององค์กรรั่วไหล หรือทรัพย์สินสารสนเทศถูกนำไปใช้ผิดประเภท

หมวดที่ 6 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ส่วนที่ 6.1 การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์

เพื่อกำหนดแนวทางปฏิบัติในในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลขององค์กร

6.1.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement for Access Control)

1) นโยบายควบคุมการเข้าถึง (Access Control Policy)

1.1) องค์กรต้องกำหนดให้มีนโยบายควบคุมการเข้าถึง (Access Control Policy) อย่างเป็นลายลักษณ์อักษร และปรับปรุงนโยบายให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

2) การควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Service)

2.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการขอเข้าถึงข้อมูลและระบบสารสนเทศของผู้ใช้งานโดยต้องได้รับการอนุมัติจากผู้บังคับบัญชาเท่านั้น

2.2.) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจำกัดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายได้ เฉพาะบริการที่ผู้ใช้งานได้รับอนุญาตให้เข้าถึงเท่านั้น โดยสิทธิที่ได้รับต้องเป็นไปตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน

6.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

1) การลงทะเบียนและถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration) และการจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

1.1) ฝ่ายทรัพยากรบุคคลแจ้งการลงทะเบียน ถอดถอนสิทธิ และเปลี่ยนแปลงสิทธิผ่านระบบ IT Job Request

1.2) ฝ่ายเทคโนโลยีสารสนเทศ ทำการลงทะเบียนถอดถอนสิทธิ และดำเนินการเปลี่ยนแปลงสิทธิของผู้ใช้งานตามที่ระบุใน IT Job Request

2) การบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูง (Management of Privileged Access Right)

2.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดเก็บรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูง เช่น Administrator / root บนเครื่องแม่ข่าย หรือ Administrator ของระบบ Application และให้มีการเบิกใช้งานตามความจำเป็นเท่านั้น

2.2) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบและปฏิบัติตาม

3) การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้ (Management of Secret Authentication Information of Users)

3.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดวิธีการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้อย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานในองค์การรับทราบและปฏิบัติตาม

6.1.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

1) การใช้งานข้อมูลการพิสูจน์ตัวตน (Use of Secret Authentication Information)

1.1) ผู้ใช้งานจะต้องไม่ใช้โครงสร้างรหัสผ่านหรือคุณลักษณะที่ง่ายต่อการเดา อาทิ คำศัพท์ในพจนานุกรม หรือคัดลอกหรือผสมจากชื่อผู้ใช้ หรืออักขระเรียงลำดับ หรือข้อมูลส่วนบุคคล หรือประโยควลีใดๆที่สามารถเดาได้ง่าย

1.2) ผู้ใช้งานจะต้องไม่เขียนหรือบันทึกรหัสผ่านที่ใช้ และเก็บหรือแสดงให้เห็นไว้ใกล้กับระบบหรืออุปกรณ์ที่ใช้กับรหัสผ่านนั้น

1.3) ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำทุกอย่างที่เกิดขึ้น หากกระกระทำนั้นสามารถบ่งชี้ให้เห็นว่าเกิดจากบัญชีผู้ใช้งานนั้น และจะต้องไม่อนุญาตให้ผู้อื่นกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานของตน หรือการกระทำใดๆ โดยใช้บัญชีผู้ใช้งานอื่นที่ไม่มีสิทธิ์

1.4) ผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดการบริหารจัดการรหัสผ่านอื่นๆที่องค์กรกำหนดไว้

6.1.4 การควบคุมการเข้าถึงแอพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

1) การจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

1.1) เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดวิธีการเข้าถึงข้อมูล ระบบสารสนเทศและฟังก์ชั่นในระบบงาน โดยต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

1.2) เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดวิธีการใช้งานระบบสารสนเทศที่สำคัญ ไม่ว่าจะเป็นข้อมูลระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบ

เครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของฝ่ายงานนั้นๆเป็นลายลักษณ์อักษร

2) การเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัย (Secure Log-on Procedures)

2.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดวิธีการเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัยอย่างเป็นลายลักษณ์อักษร โดยอ้างวิธีการที่เป็นมาตรฐานสากลและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

3) ระบบสำหรับบริการจัดการรหัสผ่าน (Password Management System)

3.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีระบบสำหรับบริหารจัดการบัญชีผู้ใช้และรหัสผ่านสำหรับการเข้าถึงระบบสารสนเทศของผู้ใช้งานภายในองค์กร เพื่อให้เกิดการบริหารจัดการที่เป็นมาตรฐานเดียวกัน

4) การควบคุมการใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

4.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์ และจำกัดการใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบสารสนเทศหรือโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้

5) การควบคุมการแก้ไขซอร์สโค๊ด (Version Control)

ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการควบคุมการปรับปรุงแก้ไขซอร์สโค๊ดของโปรแกรมที่ใช้งาน เพื่อควบคุมเวอร์ชั่นในการปรับปรุง และแก้ไขโปรแกรม หากเกิดข้อผิดพลาดในการทำงานจะช่วยให้สามารถตรวจสอบ ติดตาม หรือย้อนกลับกระบวนการ ทำให้การพัฒนาโปรแกรมเป็นมาตรฐานและเกิดความสอดคล้อง

ส่วนที่ 6.2 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการป้องกัน ควบคุมการใช้งานและการบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศและอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศขององค์กร ให้อยู่นสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพยสินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

6.2.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Security Area)

1) ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security control)

1.1) องค์กรต้องพิจารณาและจัดทำพื้นที่ที่ต้องการรักษาความปลอดภัยโดยจะประกอบด้วยพื้นที่กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า – ออกหลัก และระบบรักษาความปลอดภัยอย่างเหมาะสม

2) การควบคุมทางเข้าออกทางกายภาพ (Physical Entry Control)

2.1) องค์กร ต้องควบคุมการเข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ให้เข้าถึงได้เฉพาะบุคลากรผู้ได้รับอนุญาตเท่านั้น

2.2) รายชื่อผู้ได้รับอนุญาตให้เข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ต้องได้รับการตรวจสอบ ปรับปรุง และดูแลให้เหมาะสมอย่างสม่ำเสมอ

2.3) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการเข้าออกพื้นที่ที่ต้องการรักษาความปลอดภัย (Security Area) ได้แก่ ห้องคอมพิวเตอร์ รวมถึงพื้นที่ปฏิบัติงานของผู้ดูแลระบบ โดยต้องกำหนดให้เฉพาะผู้มีสิทธิ์ที่สามารถเข้าออกได้ และมีการเก็บบันทึกการเข้าออกห้องคอมพิวเตอร์ และบันทึกการเข้าออกดังกล่าวจะต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก วัตถุแระสงค์การผ่านเข้าออก รวมถึงต้องมีการตรวจสอบบข้าออก วัตถุประสงค์การผ่านเข้าออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

3) การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing Offices, Rooms, and facilities)

3.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องออกแบบและติดตั้งระบบการรักษาความมั่นคงปลอดภัยทางกายภาพเพื่อป้องกันพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูล ห้องคอมพิวเตอร์ และพื้นที่ปฏิบัติงานของผู้ดูแลระบบหรืออุปกรณ์สารสนเทศต่างๆ ที่ใช้ในการปฏิบัติงานอันเนื่องจากการได้รับความเสียหายและถูกเข้าถึงโดยไม่ได้รับอนุญาต

4) การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting against External and Environment Threats)

4.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยคุกคามจากภายนอก ทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัยแผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

6) พื้นที่สำหรับรับส่งสิ่งของ (Delivery and Loading Area)

6.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมบริเวณผู้ที่ไม่มีสิทธิ์เข้าถึงอาจสามารถเข้าถึงได้ โดยต้องกำหนดพื้นที่การส่งมอบสินค้าและพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้องคอมพิวเตอร์ ทั้งนี้ให้แยกเป็นสัดส่วนที่ชัดเจนเพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยผู้ที่ไม่ได้รับอนุญาต

6.2.2 อุปกรณ์ (Equipment)

1) การจัดวางและป้องกันอุปกรณ์ (Equipment Setting and Protection)

1.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดวางอุปกรณ์สารสนเทศไว้ในห้องหรือบริเวณที่ปลอดภัย อุปกรณ์ที่มีตู้ ประตูของตู้วางคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารแม่ข่ายและอุปกรณ์สื่อสารเครือข่ายต้องถูกล็อคอยู่เสมอ โดยกำหนดให้มีเพียงเจ้าหน้าที่ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิ์ในการเปิดเพื่อซ่อมบำรุงหรือการปรับปรุงค่าคอนฟิเกอเรชั่น (Reconfiguration) เพื่อลดความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

2) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

2.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดให้มีให้มีการติดตั้งอุปกรณ์ป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่างๆ ภายในห้องคอมพิวเตอร์ ได้แก่ อุปกรณ์ดับเพลิง อุปกรณ์ดักจับควัน อุปกรณ์สำรองไฟฟ้า ระบบควบคุมอุณภูมิและความชื้น ระบบเตือนภัยน้ำรั่วหรือระบบแจ้ง

เตือนเมื่ออุปกรณ์สารสนเทศทำงานผิดปกติ เป็นต้น และต้องบำรุงดูแลรักษาอุปกรณ์ให้พร้อมใช้งานอยู่เสมอ

3) ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

3.1) เทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้การติดตั้งและการบำรุงรักษาสายไฟฟ้าและสายสื่อสารในพื้นที่ปฏิบัติงานและห้องคอมพิวเตอร์เป็นไปตามมาตรฐานตวามปลอดภัยอุตสาหกรรมเพื่อป้องกันไม่ให้มีการเข้าถึงหรือดักจับข้อมูล หรือเกิดความเสียหายทางด้านกายภาพ

4) การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

4.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้อุปกรณ์สารสนเทศหลักทั้งหมดซึ่งใช้ในการประมวลผลในระดับปฏิบัติการ รวมถึงอุปกรณ์สนับสนุนการทำงานที่ได้รับการบำรุงรักษาตามช่วงเวลาและตามข้อกำหนดที่ผู้ผลิตแนะนำ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้งาน

.4.2) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการบันทึกบันทึกกิจกรรมการบำรุงอุปกรณ์ รวมถึงบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ให้อยู่ในสภาพพร้อมใช้งานเสมอ

5) การนำทรัพย์สินสารสนเทศออกนอกสำนักงาน (Removal of Assets)

5.1) ผู้ทำหน้าที่กำกับดูแลพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยและอาคารสถานที่ ต้องไม่อนุญาตอให้นำอุปกรณ์สารสนเทศออกจากองค์กร ยกเว้นจะมีการอนุญาตให้นำออกโดยผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

5.2) ผู้ใช้งาน ต้องไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกนอกองค์กร ยกเว้นจะได้รับอนุญาตจากผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

5.3) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการทำทรัพย์สินออกนอกสำนักงานอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานในองค์กรรับทราบและปฏิบัติตาม

6) ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน
(Security of Equipment and Asset Off-Premises)

6.1) กำหนดให้ผู้บริหารระดับฝ่ายขึ้นไป เป็นผู้มีอำนาจในการอนุญาตให้นำอุปกรณ์สารสนเทศขององค์กรไปใช้งานภายนอกสำนักงาน และต้องกำหนดให้มีการป้องกันอุปกรณ์สารสนเทศต่างๆ ที่ใช้งานอยู่ภายนอกสำนักงาน และต้องกำหนดให้มีการป้องกันอุปกรณ์สารสนเทศต่างๆที่ใช่งานอยู่ภายนอกสำนักงานเพื่อไม่ให้เกิดความเสีย หายต่ออุปกรณ์ โดยพิจารณาจากความเสี่ยงที่อาจเกิดขึ้นกับอุปกรณ์เหล่านี้

6.2) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการความมั่นคงปลอดภัยในการควบคุมทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินขององค์กรออกไปใช้งาน

7) ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้งานซ้ำ (Secure Disposal or Re-Use of Equipment)

7.1) ผู้ใช้งาน ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำคัญหรือซอฟต์แวร์ลิขสิทธิ์ที่อยู่ภายในสื่อบันทึกข้อมูลได้มีการลบ ย้าย หรือทำลายอย่างเหมาะสมตามลำดับชั้นความลับข้อมูล ก่อนที่จะทำลายหรือจำหน่ายอุปกรณ์หรือนำอุปกรณ์กลับมาใช้ใหม่

7.2) ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดทำขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลหรือทรัพย์สินสารสนเทศและมาตรการหรือเทคนิคสำหรับการทำลายข้อมูลเพื่อนำอุปกรณ์สารสนเทศกลับมาใช้งานซ้ำ

7.3) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดผู้รับผิดชอบในการทำหน้าที่ทำลายข้อมูลสารสนเทศที่ไม่จำเป็นต่อการดำเนินกิจการขององค์กรซึ่งจัดเก็บอยู่บนสื่อบันทึกข้อมูล

8) การป้องกันอุปกรณ์ที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended User Equipment)

8.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการควบคุมการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศทิ้งไว้โดยไม่มีผู้ดูแล เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต

8.2) ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

8.3) ผู้ใช้งานต้องออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน หรือระบบคอมพิวเตอร์โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน

8.4) ผู้ใช้งาน ต้องล็อคหน้าจอคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์

9) นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

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

9.2) ผู้ใช้งาน ต้องไม่ละเลยข้อมูลสารสนเทศที่สำคัญ เช่น เอกสารกระดาษ หรือสื่อบันทึกข้อมูล ให้อยู่ในสถานที่ไม่ปลอดภัย พื้นที่สาธารณะ หรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ที่ใช้งานจะต้องจัดเก็บข้อมูลสารสนเทศในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงของผู้ไม่มีสิทธิ์

ส่วนที่ 6.3 การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ (Operations Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมให้การดำเนินงาน การจัดการด้านการสื่อสารความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร มีแนวทางปฏิบัติที่มีขั้นตอนชัดเจนและมีความมั่นคงปลอดภัย

1) การบริหารจัดการการเปลี่ยนแปลง (Change Management)

1.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุม กำกับให้มีการจัดการควบคุมการเปลี่ยนแปลงขอการเปลี่ยนแปลงโครงสร้างองค์กร ขั้นตอนการปฏิบัติงาน ระบบสารสนเทศ เพื่อควบคุมก่อนการเปลี่ยนแปลง แก้ไข หรือกระทำการใดๆ ซึ่งส่งผลต่อการดำเนินงานของระบบงานต่างๆ ทั้งนี้ให้ปฏิบัติ

ตามที่กำหนดไว้ในนโยบายส่วนที่ 5.1 การบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy)

2) การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

2.1) ผู้ดูแลระบบ ต้องติดตามประสิทธิภาพการทำงานของระบบงานและอุปกรณ์สารสนเทศที่สำคัญให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

2.2) ผู้ดูแลระบบ ต้องประเมินสมรรถภาพและความเพียงพอ (Capacity) ของทรัพยากรสารสนเทศ เช่น การใช้งานของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย เช่น หน่วยประมวลผล (CPU) หน่วยความจำ (Memory) หน่วยจัดเก็บข้อมูล (Disk) หรือปริมาณการใช้งานระบบเครือข่าย (Bandwidth) เป็นต้น และต้องวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศให้ระบบสารสนเทศมีประสิทธิภาพที่เหมาะสม และเพียงพอต่อการใช้งานในอนาคต

3) การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operation Environment)

3.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมกำกับให้มีการแยกส่วนระบบคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เพื่อทดสอบระบบงาน (Test Environment) และระบบที่ให้บริการจริง (Production Environment) ออกจากกัน

3.2) ฝ่ายเทคโนโลยีสารสนเทศ ต้องควบคุมให้มีการกำหนดสิทธิ์การเข้าถึงในแต่ละสภาพแวดล้อมและจัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบอย่างชัดเจน โดยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหา และวิธีการแก้ไขรวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ

6.3.1 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

1) มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls Against Malware)

1.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

6.3.2 การสำรองข้อมูล (Information Backup)

1.1) ฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมาตรการในการสำรองข้อมูล และรอบการสำรองข้อมูลของระบบสารสนเทศที่สำคัญไว้อย่างสม่ำเสมอ เพื่อป้องกันการสูญหายของข้อมูล

1.2) เจ้าของข้อมูลสารสนเทศ ต้องดำเนินการหรือกำหนดให้มีการสำรองข้อมูลสารสนเทศและการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าจะสามารถนำข้อมูลกลับมาใช้ใหม่ได้เมื่อต้องการ

1.3) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลที่ไม่เกี่ยวข้องกับข้อมูลส่วนบุคคลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น External Hard Disk เป็นต้น ให้เป็นปัจจุบันอย่างสม่ำเสมอ รวมถึงให้จัดเก็บไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

1.4) ผู้ใช้งานทำการสำรองข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลแบบรวมศูนย์ (Centralized, shared drives หรือ Cloud Storage) ตามที่ฝ่ายเทคโนโลยีสารสนเทศกำหนด ผู้ใช้งานต้องไม่ทำการเก็บ

ข้อมูลส่วนบุคคลของลูกค้าใดๆ ไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล (Endpoint) หรือสื่อบันทึกข้อมูลอื่นใด ฝ่ายเทคโนโลยีสารสนเทศต้องทำหน้าที่สำรองข้อมูลลงสื่อบันทึกแบบ Storage Area Network (SAN) อย่างสม่ำเสมอ

6.3.3 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

1) การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Event Logging)

1.1) ผู้ดูแลระบบ ต้องจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ซึ่งเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศให้เพียงพอต่อการตรวจสอบ

1.2) ผู้ดูแลระบบ ต้องเฝ้าติดตาม (Monitoring) การใช้งานระบบสารสนเทศ โดยผลของการเฝ้าติดตามจะต้องถูกสอบทานอย่างสม่ำเสมอ เพื่อตรวจหาความผิดปกติ

1.3) ผู้ดูแลระบบ ต้องควบคุมและกำกับให้มีการบันทึกเหตุการณ์ความผิดพลาด (Fault Logging) ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ รวมถึงวิเคราะห์ ดำเนินการแก้ไข ตลอดจนวางแนวทางป้องกันการเกิดปัญหาซ้ำอีกในอนาคต

2) การป้องกันข้อมูลล็อก (Protection of Log Information)

2.1) ผู้ดูแลระบบ ต้องจัดให้มีการป้องกันข้อมูล และระบบการบันทึกและจัดเก็บหลักฐานการใช้งานที่เกี่ยวกับระบบสารสนเทศจากการถูกเปลี่ยนแปลงแก้ไข ถูกทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต

3) การบันทึกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ระบบปฏิบัติการ (Administration and Operation Logs)

3.1) ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบและผู้ฏิบัติงานที่เกี่ยวข้องกับระบบ อาทิ เวลาเปิดและปิดระบบ การเปลี่ยนแปลงการตั้งค่าของระบบความผิดพลาดของระบบ ความผิดพลาดของระบบ และการดำเนินการแก้ไขและต้องมีการสอบทานบันทึกกิจกรรมอย่างสม่ำเสมอ

4) การตั้งเวลาระบบสารสนเทศ (Clock Synchronization)

4.1) ผู้ดูแลระบบ ต้องควบคุมกำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศขององค์กรได้รับการกำหนดเวลาให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องและตรงกับเวลาอ้างอิงสากล

4.2) ผู้ดูแลระบบ ต้องตรวจสอบเวลาของอุปกรณ์สารสนเทศและระบบสารสนเทศขององค์กร รวมถึงปรับปรุงให้เป็นปัจจุบันเสมอ เพื่อป้องกันไม่ให้เกิดการบันทึกเวลาที่ไม่ถูกต้อง