นโยบายด้านความมั่นคงปลอดภัยของ ระบบเทคโนโลยีสารสนเทศ

แก้ไขครั้งที่ : 01 วันที่บังคับใช้ : 15 พฤษภาคม 2568

ลายมือชื่อ			
ชื่อ-นามสกุล	นายสุธี เหลืองรัตนเจริญ	นายประเทศ ศรีชมภู	ผศ.ดร.พัทธนันท์ เพชรเชิดชู
ตำแหน่ง	ประธานเจ้าหน้าที่บริหาร	ประธานกรรมการสรรหาและพิจารณาค่าตอบแทนและกำกับดูแลกิจการที่ดี	ประธานกรรมการ

ประวัติการแก้ไข

แก้ไขครั้งที่	วันที่บังคับใช้	รายละเอียดการแก้ไข
00		จัดทำครั้งแรก
01		ประกาศใช้งาน 15 พฤษภาคม 2568

สารบัญ

หมวดที่ 1 บทสรุปผู้บริหาร

บริษัท เวล แมเนจเม้นท์ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทในเครือ (ต่อไปเรียกว่า "บริษัทฯ") คำนึงถึงความสำคัญของการนำเทคโนโลยีสารสนเทศ เข้ามาช่วยเพิ่มศักยภาพการดำเนินงานของบริษัทฯ เพื่อก่อให้เกิดกระบวนการบริหารจัดการที่เป็นระบบ มีระเบียบ เป็นขั้นตอน ตอบสนองความต้องการของผู้มีส่วนได้ส่วยเสียของบริษัทฯ และเพื่อที่จะให้มั่นใจได้ว่าระบบสารสนเทศที่สำคัญของบริษัทฯมีการรักษาความลับ (Confidentiality) มีความครบถ้วนสมบูรณ์ถูกต้อง (Integrity) และมีความพร้อมใช้งาน (Availability) ที่เหมาะสม

บริษัทฯ จึงได้เล็งเห็นว่าในการนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินงาน จำเป็นต้องกำหนดแนวทางการพัฒนาให้สอดคล้องกับกลยุทธ์ และวิสัยทัศน์ของบริษัทฯ รวมถึงกฎหมาย ข้อบังคับ มาตรฐานสากลต่างๆ ที่เกี่ยวข้อง และการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศในปัจจุบัน เพื่อให้การให้บริการทางด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ มีประสิทธิผล มีความมั่นคงปลอดภัยและมีกรอบในการบริหารจัดการเทคโนโลยีสารสนเทศที่ดี รวมถึงเพื่อให้ผู้ที่เกี่ยวข้องเกิดความเชื่อมั่นในการให้บริการระบบสารสนเทศของบริษัทฯ

หมวดที่ 2 บททั่วไป

ส่วนที่ 2.1 วัตถุประสงค์

เพื่อให้บริษัทฯมีแนวนโยบายในการดำเนินงานหรือการจัดการทางด้านเทคโนโลยีสารสนเทศและให้ผู้ที่เกี่ยวข้องกับสารสนเทศ ทั้งผู้บริหาร บุคลากรในบริษัทฯ หน่วยงานภายนอกและบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับสารสนเทศของบริษัทฯได้มีแผนงานและกรอบการปฏิบัติที่ชัดเจน อันจะนำไปสู่การประสานงานในการให้บริการที่มีประสิทธิภาพ มีความปลอดภัยในการให้บริการสูงสุดและมีมาตรฐานยิ่งขึ้น อีกทั้งกำหนดมาตรการป้องกันที่เหมาะสมเพื่อควบคุมและลดความเสียหายต่างๆ ที่อาจเกิดขึ้นจากกรณีที่ทรัพย์สินสารสนเทศ ไม่สามารถใช้งานได้ สูญหาย เสียหาย บกพร่อง หรือถูกคุกคามด้านความมั่นคงปลอดภัย

ส่วนที่ 2.2 กฎหมายและกฎระเบียบที่เกี่ยวข้อง

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

ส่วนที่ 2.3 บทบังคับใช้และบทลงโทษ

นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศฉบับนี้ ให้มีผลบังคับใช้นับจากวันที่ประกาศให้มีผลบังคับใช้ต่อผู้ใช้งานระบบสารสนเทศของ**บริษัท เวล แมเนจเม้นท์ คอร์ปอเรชั่น จำกัด (มหาชน)และบริษัทในเครือ**โดยไม่มีการยกเว้น ผู้ฝ่าฝืนจะมีความผิดและต้องได้รับการลงโทษทางวินัยตามระเบียบที่บริษัทฯกำหนดไว้

ส่วนที่ 2.4 การเผยแพร่นโยบาย

แผนกเทคโนโลยีและสารสนเทศ มีหน้าที่รับผิดชอบในการประกาศและเผยแพร่นโยบายไปยังผู้ใช้งานระบบสารสนเทศของบริษัทฯ เพื่อช่วยให้เกิดความเข้าใจในบทบาทของตนเองในการใช้งานเทคโนโลยีสารสนเทศและปกป้องทรัพย์สินสารสนเทศของบริษัทฯ

ส่วนที่ 2.5 การทบทวนนโยบาย

นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศฉบับนี้ต้องได้รับการทบทวน ปรับปรุงให้เป็นปัจจุบัน<u>อย่างน้อยปีละ 1 ครั้ง</u> หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญของสภาพแวดล้อมต่างๆ เช่น สภาพธุรกิจ กฎเกณฑ์ กฎหมายและเทคโนโลยี เป็นต้น โดยถือเป็นหน้าที่ของแผนกเทคโนโลยีและสารสนเทศ ในการทบทวนและปรับปรุง โดยมีผู้บริหารแผนกเทคโนโลยีและสารสนเทศ เป็นผู้ควบคุมดูแลให้เกิดการทบทวนและปรับปรุงตามที่ได้กำหนดไว้

หมวดที่ 3 บทบาทและความรับผิดชอบ

ส่วนที่ 3.1 ประธานกรรมการบริษัท

- อนุมัตินโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศรวมถึงการเปลี่ยนแปลงที่อาจจะมีขึ้นในอนาคต
- อนุมัติเรื่องที่คณะกรรมการบริษัทนำเสนอซึ่งเกี่ยวข้องกับนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- กำกับดูแลโดยรวมในความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ เพื่อให้มีความมั่นใจว่า
  - นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่ถูกจัดทำขึ้นครอบคลุมสารสนเทศที่มีความสำคัญ
  - การปฏิบัติสอดคล้องกับวัตถุประสงค์ทางธุรกิจของบริษัทฯและความต้องการของผู้ใช้งาน

ส่วนที่ 3.2 ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่ และผู้ช่วยกรรมการผู้จัดการใหญ่

- อนุมัติระเบียบปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศรวมถึงการเปลี่ยนแปลงที่อาจจะมีขึ้นในอนาคต
- กำหนดทิศทางและให้การสนับสนุนในการจัดทำนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศรวมถึงระเบียบปฏิบัติที่เกี่ยวข้อง
- ตัดสินใจในการติดต่อกับหน่วยงานบังคับใช้กฎหมาย และหน่วยงานสืบสวน เมื่อมีข้อสงสัยว่ามีการกระทำผิดร้ายแรงเกิดขึ้นทางด้านเทคโนโลยีสารสนเทศ
- อนุมัติ และสนับสนุนกิจกรรมโครงการความมั่นคงปลอดภัยด้านสารสนเทศ และเป็นหลักในการริเริ่มให้มีการสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ทบทวน สรุป และนำเสนอต่อประธานกรรมการบริษัท เพื่อขออนุมัติประกาศใช้นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศรวมถึงการเปลี่ยนแปลงที่อาจจะมีขึ้น

ส่วนที่ 3.3 ผู้บริหารระดับฝ่ายทุกฝ่ายงาน

- กำหนดผู้รับผิดชอบต่อทรัพย์สินสารสนเทศและวิเคราะห์ความเสี่ยงของทรัพย์สินสารสนเทศ รวมถึงบริหารจัดการทรัพย์สินสารสนเทศที่อยู่ภายใต้การดูแลให้คงสภาพการป้องกันความลับ ความสมบูรณ์ครบถ้วน และความพร้อมใช้งานของทรัพย์สินสารสนเทศนั้นๆ
- กำหนดบทบาทหน้าที่และความรับผิดชอบ ในการปฏิบัติงานด้านความมั่นคงปลอดภัยของบุคลากรโดยยึดถือตามนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศที่กำหนดไว้
- กำหนดให้มีการให้ความรู้ในเรื่องของนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและระเบียบปฏิบัติที่เกี่ยวข้อง ต่อบุคลากรภายในบริษัทฯและหน่วยงานภายนอกที่เกี่ยวข้อง
- กำหนดความสำคัญ การริเริ่ม และลงมือปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้บุคลากรในหน่วยงานปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- ทบทวนและอนุมัติความต้องการด้านความมั่นคงปลอดภัยของระบบที่จะนำไปใช้กับข้อมูลสารสนเทศที่มีความอ่อนไหว (Sensitive) หรือสำคัญมากต่อการปฏิบัติงานทางธุรกิจก่อนเริ่มต้นพัฒนาโครงการ (Project Development)
- กำกับดูแลให้มีการจัดทำสัญญาข้อตกลงการรักษาความลับของบริษัทฯ ต่อบุคลากรภายในบริษัทฯและหน่วยงานภายนอกที่เกี่ยวข้อง โดยระบุความต้องการเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติที่อาจส่งผลต่อการละเมิดสัญญาข้อตกลงต่าง ๆ
- ตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นเหตุการณ์ที่มีผลกระทบด้านลบต่อหน่วยงานหรือทั้งบริษัทฯ อาทิ เหตุการณ์ที่มีผลอย่างยิ่งต่อภาพพจน์ของบริษัทฯ ความเชื่อมั่นของลูกค้า

การดำเนินการของบริษัทฯ โดยต้องรายงานต่อประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่และผู้ช่วยกรรมการผู้จัดการใหญ่

- ให้การสนับสนุนในการสืบสวนและเสนอแนวทางแก้ไขต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น

ส่วนที่ 3.4 เจ้าของทรัพย์สินสารสนเทศ

- กำหนดลำดับชั้นความลับข้อมูลตามความสำคัญของข้อมูลต่อบริษัทฯ พร้อมทั้งแจ้งให้ผู้เกี่ยวข้องรับทราบในการเปลี่ยนแปลงลำดับชั้นความลับข้อมูลที่เกิดขึ้น
- พัฒนาและปรับปรุงโครงสร้างการแบ่งลำดับชั้นความลับข้อมูลและข้อกำหนดในการบริหารจัดการตามลำดับชั้นความลับ
- ระบุกฎเกณฑ์การกำหนดสิทธิ์ในการเข้าถึงข้อมูลและทรัพย์สินสารสนเทศ เช่น บทบาทของผู้ใช้งานหรือของบริษัทฯ แนวทางในการขออนุมัติเข้าถึงทรัพย์สินสารสนเทศ เป็นต้น พร้อมทั้งแจ้งให้กลุ่มผู้เกี่ยวข้องรับทราบในการเปลี่ยนแปลงกฎเกณฑ์ที่เกิดขึ้น
- ประเมินความเสี่ยงและหาแนวทางการควบคุมที่เป็นมาตรฐานในกรณีที่ความจำเป็นทางธุรกิจไม่สอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและระเบียบปฏิบัติหรือมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อควบคุมให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้หรือเพื่อไม่ให้ความเสี่ยงอยู่ในระดับที่สูงขึ้น

ส่วนที่ 3.5 ผู้บริหารและเจ้าหน้าที่แผนกเทคโนโลยีและสารสนเทศ

- จัดทำและนำเสนอนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศรวมถึงรายงานการเปลี่ยนแปลงนโยบายที่เกิดขึ้น ต่อประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่ และผู้ช่วยกรรมการผู้จัดการใหญ่
- พัฒนา และจัดทำเอกสารกระบวนการสนับสนุน แนวทาง และขั้นตอนการปฏิบัติงาน เพื่อให้แน่ใจว่าสอดคล้องตามนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- ควบคุมดูแลระบบสารสนเทศให้คงสภาพการรักษาความลับ ความสมบูรณ์ครบถ้วน และความพร้อมใช้ของทรัพย์สินสารสนเทศที่ให้บริการระบบสารสนเทศซึ่งอยู่ภายใต้การดูแล และควบคุมการเข้าถึงทรัพย์สินสารสนเทศ เพื่อเป็นการปกป้องทรัพย์สินสารสนเทศอย่างเหมาะสม
- เตรียมการช่วยเหลือทางด้านเทคนิคแก่ผู้เป็นเจ้าของทรัพย์สินสารสนเทศ เพื่อนำเอาการควบคุมที่เหมาะสมมาใช้ในการดูแลทรัพย์สินสารสนเทศ

- กำหนดกลไกการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และตรวจสอบการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอเพื่อป้องกันการบุกรุกระบบสารสนเทศอย่างทันท่วงที
- ให้ความช่วยเหลือในการคัดเลือกและประเมินด้านความมั่นคงปลอดภัยสารสนเทศ ในส่วนที่เกี่ยวข้องกับฮาร์ดแวร์ และ/หรือ ซอฟต์แวร์ ที่นำมาใช้งานในบริษัทฯ
- แจ้งให้เจ้าของทรัพย์สินสารสนเทศและผู้ที่เกี่ยวข้องรับทราบในกรณีที่พบหรือสงสัยว่าทรัพย์สินสารสนเทศที่ให้บริการระบบสารสนเทศของบริษัทฯถูกคุกคาม (Compromises) หรือสูญเสีย หรือเสียหาย รวมทั้งกรณีที่มีการละเมิดต่อนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศหรือระเบียบปฏิบัติที่เกี่ยวข้อง
- ตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ และช่วยเหลือในการสอบสวน รวมถึงแก้ไขปัญหาในส่วนที่ทราบหรือสงสัยว่าทรัพย์สินสารสนเทศของบริษัทฯถูกคุกคาม หรือเหตุการณ์ที่ต้องสงสัยว่ามีการโจมตีระบบรักษาความมั่นคงปลอดภัยสารสนเทศ หรือเป็นการกระทำที่ไม่เหมาะสม และแจ้งผลลัพธ์ให้เจ้าของทรัพย์สินสารสนเทศและผู้ที่เกี่ยวข้องรับทราบ

ส่วนที่ 3.6 ส่วนกฎหมาย

- ให้ข้อแนะนำทางกฎหมายที่เกี่ยวข้องกับระเบียบ วิธีการปฏิบัติสำหรับการตรวจสอบการใช้ระบบสารสนเทศและอุปกรณ์ประมวลผลต่างๆ รวมถึงการรวบรวมและการป้องกันสิ่งที่เป็นหลักฐานที่ต้องการสำหรับการลงโทษทางวินัยภายในบริษัทฯ และการเอาผิดในทางแพ่งหรืออาญา

ส่วนที่ 3.7 ผู้ตรวจสอบระบบงาน

- สอบทานการนำนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศมาใช้ และประเมินผลการปฏิบัติตามนโยบาย ระเบียบปฏิบัติ และขั้นตอนปฏิบัติงานที่เกี่ยวข้อง รวมถึงประสิทธิภาพของนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนวัดผลการควบคุมภายใน โดยถือเป็นส่วนหนึ่งของตารางการตรวจสอบเป็นประจำและรายงานผลการตรวจสอบภายในไปยังผู้บริหารที่เกี่ยวข้องได้รับทราบเพื่อพิจารณาดำเนินการ

ส่วนที่ 3.8 ผู้ใช้งาน

- ทำความเข้าใจกับนโยบาย ระเบียบปฏิบัติ และขั้นตอนปฏิบัติงานต่างๆ ที่บริษัทฯ หรือหน่วยงานได้กำหนดไว้รวมถึงให้ความร่วมมือในการใช้กฎข้อบังคับต่างๆ
- ลงนามยินยอมและปฏิบัติตามข้อตกลงไม่เปิดเผยความลับของบริษัทฯ
- ใช้ทรัพย์สินสารสนเทศของบริษัทฯอย่างมีประสิทธิภาพ มีจริยธรรม และถูกต้องตามกฎหมาย

- รายงานเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศแก่ผู้บังคับบัญชาและแผนกเทคโนโลยีและสารสนเทศให้ทราบโดยทันทีและช่วยเหลือในการสนองตอบต่อเหตุการณ์เหล่านั้น

ส่วนที่ 3.9 หน่วยงานภายนอก

- ลงนามและปฏิบัติตามข้อตกลงไม่เปิดเผยความลับของบริษัทฯ
- ยึดถือการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯต่อการให้บริการของบุคคลที่สามและกระทำการใดตามความจำเป็นเพื่อป้องกันความลับของข้อมูลสารสนเทศและระบบต่างๆ ที่บริษัทฯจัดเตรียมไว้เพื่อใช้งาน
- เข้าถึงระบบสารสนเทศเฉพาะสิทธิ์ที่ได้รับเท่านั้น
- ข้อมูลสารสนเทศที่ได้รับจากการเก็บรวบรวมหรือเข้าถึงในระหว่างที่มีการทำงานกับบริษัทฯ ให้ถือเป็นความลับ ห้ามทำการใดๆ อันเกี่ยวข้องกับการใช้ การเปิดเผย ส่ง หรือ แก้ไขข้อมูลสารสนเทศที่ได้มาโดยไม่มีการยินยอมอย่างชัดเจนจากหน่วยงานของบริษัทฯที่ทำหน้าที่กำกับดูแลการดำเนินงาน
- รายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นทันที ให้แก่หน่วยงานของบริษัทฯที่ทำหน้าที่กำกับดูแลการดำเนินงานและฝ่ายสารสนเทศ รวมถึงช่วยเหลือการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

หมวดที่ 4 คำจำกัดความ

นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศได้กำหนดคำนิยามของคำศัพท์ที่ใช้ในนโยบายฉบับนี้ เพื่อให้เข้าใจถึงความหมายตรงกันและอ้างอิงได้ถูกต้อง ดังต่อไปนี้

คำศัพท์	ความหมาย
หน่วยงาน	
บริษัทในเครือ	บริษัท อีสเทิร์น กรีน ดีเวลลอปเมนท์ (EGD) และ บริษัท WELL TECH
แผนกเทคโนโลยีและสารสนเทศ	หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศของบริษัทฯ
บุคคล	
ผู้บริหารระดับฝ่าย	ผู้บริหารสูงสุดของแต่ละฝ่ายงาน
ผู้มีอำนาจ	ผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายขึ้นไป หรือผู้ที่ได้รับมอบหมายให้มีหน้าที่ตัดสินใจ
ผู้ดูแลระบบ (Administrator)	เจ้าหน้าที่แผนกเทคโนโลยีและสารสนเทศที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบหรือเครือข่ายคอมพิวเตอร์ รวมไปถึงการแก้ไขปัญหาการ

คำศัพท์	ความหมาย
	ใช้งานระบบสารสนเทศในด้านต่างๆ ซึ่งสามารถเข้าถึงโปรแกรม หรือเครือข่ายคอมพิวเตอร์เพื่อการจัดการต่างๆ ได้
บุคลากร	บุคลากรของบริษัทฯ
บุคคลภายนอก	บุคคล หรือพนักงานของหน่วยงานภายนอกที่มาติดต่อสื่อสารและมีการเข้าถึงทรัพย์สินสารสนเทศของบริษัทฯ
ผู้ให้บริการภายนอก /หน่วยงานภายนอก (Third party)	ผู้ค้า หุ้นส่วนการค้า ผู้ให้บริการ/จำหน่ายระบบ (Vendor) พนักงานสัญญาจ้าง (Outsource) และบุคคล หรือนิติบุคคลอื่นใดทั้งในประเทศและต่างประเทศที่ให้บริการด้านเทคโนโลยีสารสนเทศ ซึ่งเข้าทำสัญญาหรือทำข้อตกลงในการให้บริการให้กับบริษัทฯ รวมถึงหน่วยงานผู้รับจ้างช่วงที่ผู้ให้บริการภายนอกเป็นผู้จัดจ้าง โดยได้รับอนุญาตให้มีสิทธิ์เข้าถึงสถานที่หรือทรัพย์สินสารสนเทศของบริษัทฯ และใช้งานระบบสารสนเทศของบริษัทฯตามอำนาจหน้าที่ที่รับผิดชอบ
ผู้ใช้งาน (User)	บุคลากร บุคคลภายนอก และหน่วยงานภายนอก ที่ใช้งานระบบงานคอมพิวเตอร์ของบริษัทฯ
เจ้าของโครงการ	หน่วยงานภายในบริษัทฯที่เป็นผู้รับผิดชอบในการดำเนินงานโครงการที่มีการจัดจ้างผู้ให้บริการภายนอก / หน่วยงานภายนอกเข้ามาปฏิบัติงานให้กับบริษัทฯ
เจ้าของทรัพย์สินสารสนเทศ / เจ้าของข้อมูล (Data Owner)	บุคคล ส่วนงาน หรือฝ่ายงานผู้เป็นเจ้าของข้อมูล หรือเป็นผู้ที่ได้รับความเสียหายสูงสุดเมื่อข้อมูลนั้นเสียหายหรือถูกเปิดเผย
คำอื่นๆ	
ข้อมูล	ข้อความ ข่าวสาร เอกสาร เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ ที่อยู่ในรูปของตัวเลข ภาษา ภาพ สัญลักษณ์ต่างๆ ที่ยังไม่ผ่านการประมวลผล ทั้งที่อยู่ในรูปอิเล็กทรอนิกส์หรือที่อยู่ ในรูปสื่อสิ่งพิมพ์ และให้ความหมายรวมถึงข้อมูลคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
ข้อมูลอิเล็กทรอนิกส์	ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร
ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
บัญชีผู้ใช้งาน (User Name หรือ User ID)	รหัสประจำตัวของผู้ใช้งานที่ใช้ในการระบุตัวตนในระบบคอมพิวเตอร์มักจะใช้ร่วมกับ รหัสผ่าน (Password) เพื่อเข้าสู่ระบบ

คำศัพท์	ความหมาย
รหัสผ่าน (Password)	รหัสลับที่ใช้ในการยืนยันตัวตนเพื่อเข้าถึงระบบคอมพิวเตอร์ บัญชีออนไลน์ หรือข้อมูลที่ต้องการความปลอดภัย
สิทธิระดับสูง (Privilege)	สิทธิ์ที่สามารถใช้งาน โดยได้รับสิทธิ์ที่มากกว่าสิทธิ์ของผู้ดูแลระบบหรือผู้ใช้งานทั่วไปในระบบ เช่น Root หรือ Administrator
ระบบสารสนเทศ	ระบบคอมพิวเตอร์ ระบบเก็บข้อมูล ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบสื่อสารข้อมูลทุกประเภท อุปกรณ์สื่อสาร เครื่องพิมพ์ เครื่องสแกนหรืออุปกรณ์ใดๆ ที่ เกี่ยวข้องที่เป็นกรรมสิทธิ์ของบริษัทฯ และ/หรือ ที่บริษัทฯได้รับอนุญาตให้ใช้ได้ตามกฎหมาย
ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)	การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)
เหตุขัดข้อง (Incident)	เหตุขัดข้องที่ส่งผลทำให้ระบบสารสนเทศไม่สามารถให้บริการได้ตามที่กำหนดไว้ หรือคุณภาพในการให้บริการลดลง เช่น ระบบอีเมลไม่สามารถใช้งานได้ เครื่องแม่ข่ายขัดข้อง หรือ ระบบงานประมวลช้าผิดปกติ เป็นต้น
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของบริษัทฯถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
การเข้ารหัสลับ (Encryption)	การเปลี่ยนแปลงรูปแบบของข้อมูลให้อยู่ในรูปแบบที่มีความมั่นคงปลอดภัย โดยใช้กุญแจในการเข้ารหัสลับ เพื่อที่ผู้เข้าถึงข้อมูลจะไม่สามารถทราบเนื้อหาที่แท้จริงของข้อมูลได้ ถ้าไม่มีการถอดรหัสลับจากกุญแจที่ใช้ในการถอดรหัสที่ถูกต้อง ทั้งนี้ขึ้นอยู่กับเทคนิคการเข้ารหัสลับข้อมูลที่ใช้ โดยลักษณะของการเข้ารหัสลับมีด้วยกัน 2 ประเภท คือ ■ การเข้ารหัสแบบสมมาตร (Symmetric Key Encryption) เป็นการเข้ารหัสที่ใช้กุญแจรหัสเดียวในการเข้ารหัสและถอดรหัส เรียกว่า กุญแจลับ (Secret Key) ■ การเข้ารหัสแบบอสมมาตร(Asymmetric Key Encryption or Public Key Cryptography) เป็นการเข้ารหัสในลักษณะที่มีกุญแจคู่เรียกว่ากุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) โดยในนโยบายฉบับนี้เรียกว่ากุญแจคู่

คำศัพท์	ความหมาย
กุญแจ (Key)	กุญแจที่ใช้ในกระบวนการเข้ารหัสลับ หรือถอดรหัสลับ ขึ้นอยู่กับการใช้งานเทคนิคการเข้ารหัสลับข้อมูล โดยแยกเป็น 2 ประเภท คือ ■ กุญแจลับ (Secret Key) ซึ่งใช้ในการเข้ารหัสลับแบบสมมาตร (Symmetric Key Encryption) ตัวอย่างของอัลกอริทึมสำหรับการเข้ารหัสแบบสมมาตร เช่น 3DES, RC5, RC6, AES เป็นต้น ■ กุญแจคู่ ซึ่งใช้ในการเข้ารหัสแบบอสมมาตร (Asymmetric Key Encryption or Public Key Cryptography) ประกอบไปด้วย กุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) ตัวอย่างของอัลกอริทึมสำหรับการเข้ารหัสแบบอสมมาตร 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 เพื่อเป็นการสำรองข้อมูลที่อาจมีการแก้ไข เปลี่ยนแปลง หรือสูญหายให้สามารถนำกลับมาใช้งานได้
ทรัพย์สินสารสนเทศ	หมายถึง ■ อุปกรณ์เทคโนโลยีสารสนเทศ และอุปกรณ์อื่นใดที่ใช้งานร่วมกับอุปกรณ์เทคโนโลยีสารสนเทศที่เกี่ยวข้องทุกประเภท ■ ชุดคำสั่ง โปรแกรมระบบงานสารสนเทศ และโปรแกรมอื่นใดที่ใช้งานร่วมกับโปรแกรมระบบงานสารสนเทศ ■ ข้อมูล ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ และ/หรือ ทรัพย์สินทางปัญญาใดๆ
พื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure Area)	บริเวณที่ใช้เก็บรักษาอุปกรณ์สารสนเทศที่ใช้ในงานระบบสารสนเทศ ได้แก่ พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

คำศัพท์	ความหมาย
ห้องคอมพิวเตอร์ (Data Center)	พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ที่ใช้เก็บอุปกรณ์คอมพิวเตอร์และเครื่องคอมพิวเตอร์หลักที่สำคัญในระบบงาน เช่น เครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายหลัก
บันทึกเหตุการณ์ (Logs)	บันทึกเหตุการณ์การใช้งานของระบบสารสนเทศ การเข้าใช้งานระบบงานหรือระบบสารสนเทศ การประมวลผลกิจกรรมของระบบสารสนเทศ และเหตุการณ์ทางด้านความมั่นคงปลอดภัยเพื่อตรวจสอบถึงประสิทธิภาพความปลอดภัย และความผิดปกติที่เกิดจากการประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศ
การเฝ้าระวัง (Monitoring)	การเฝ้าระวังทางด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อตรวจสอบความผิดปกติจากการประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศ จากบันทึกเหตุการณ์ (Logs) เช่น การเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต การใช้งานสารสนเทศผิดวัตถุประสงค์ และปัญหาที่เกิดจากระบบงาน
ความเสี่ยง (Risk)	โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคตและมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายของการให้บริการ
โปรแกรมที่ไม่พึงประสงค์ (Malicious Code or Malware)	โปรแกรมหรือ Code ที่เป็นอันตรายต่อประสิทธิภาพ และความปลอดภัยของระบบสารสนเทศไม่ทางใดก็ทางหนึ่ง เช่น ไวรัส (Virus) เวิร์ม (Worm) หรือโทรจัน (Trojan) เป็นต้น
แผนการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Plan)	การสร้างความต่อเนื่องทางธุรกิจ เพื่อป้องกันการติดขัดหรือการหยุดชะงักของระบบงานธุรกรรมที่สำคัญซึ่งอาจมีสาเหตุมาจากภัยทางด้านสิ่งแวดล้อม เหตุการณ์ทางด้านความมั่นคงปลอดภัยหรือภัยคุกคามอื่นๆ
แผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRP: Disaster Recovery Plan)	การเตรียมความพร้อมรองรับเหตุฉุกเฉินและแผนการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน เช่น การย้ายสถานที่ปฏิบัติงาน ไปจนถึงการใช้งานระบบสารสนเทศสำรอง
ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective: RTO)	ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อส่งมอบผลิตภัณฑ์ บริการ และกิจกรรม หรือกระบวนการกลับสู่สภาวะปกติหลังจากเกิดสถานการณ์ไม่พึงประสงค์ที่มีความเสียหายระดับรุนแรง
ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลสูญหายจากระบบได้ และเพื่อเป็นข้อมูลในการออกแบบวิธีการสำรองข้อมูลเพื่อให้ข้อมูลไม่สูญหายเกินกว่าที่กำหนดไว้

คำศัพท์	ความหมาย
ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD)	ช่วงเวลาสูงสุดที่การดำเนินงานหยุดชะงัก หากเกินกำหนดช่วงเวลานี้แล้ว จะไม่สามารถทำให้การดำเนินงานฟื้นคืนสู่สภาพปกติได้
ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA)	ข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้รับบริการที่อธิบายถึงรายละเอียดการบริการ ระดับการให้บริการที่จะถูกวัดและประเมินผล เป้าหมายของระดับการให้บริการ รวมไปถึงระบุหน้าที่ความรับผิดชอบที่ชัดเจนของทั้งผู้ให้บริการและผู้รับบริการ
ข้อตกลงการให้บริการระดับปฏิบัติงาน (Operational Level Agreement: OLA)	ข้อตกลงในการให้บริการการสำหรับปฏิบัติงานร่วมกันระหว่างหน่วยงานภายในเพื่อสนับสนุนให้การบริการของผู้รับบริการเป็นไปตามข้อตกลงระดับการให้บริการ (SLA)
สัญญาการให้บริการ (Underpinning Contracts: UC)	ข้อตกลงร่วมกันระหว่างผู้ให้บริการและผู้ให้บริการ/ผู้จำหน่ายระบบ (Vendor) เพื่อให้บริการผู้รับบริการได้ตามข้อตกลงการให้บริการ (SLA)
อุปกรณ์สื่อสารประเภทพกพา (Mobile Device)	เครื่องคอมพิวเตอร์พกพา (Laptop Computer) สมาร์ทโฟน (Smartphone) แท็บเล็ตคอมพิวเตอร์ (Tablet Computer) ที่บริษัทฯอนุญาตให้เชื่อมต่อและใช้งานระบบสารสนเทศของบริษัทฯ ได้
สื่อบันทึกข้อมูล (Media)	อุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น Hard Drive หรือ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard Drive เป็นต้น

หมวดที่ 5 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ส่วนที่ 5.1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและได้รับทราบถึงหน้าที่ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงต่างๆ โดยต้องจัดให้มีนโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีแนวทางปฏิบัติดังนี้

5.1.1 ทิศทางการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Management Directions for Information Security)

1) นโยบายสำหรับความมั่นคงปลอดภัยด้านสารสนเทศ (Policy for Information Security)

1.1) บริษัทฯต้องจัดให้มีนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร โดยได้รับการอนุมัติจากประธานกรรมการบริษัท หรือผู้บริหารระดับสูงที่ประธานกรรมการบริษัทมอบหมายให้เป็นผู้อนุมัติ

1.2) บริษัทฯต้องเผยแพร่นโยบายดังกล่าวให้ผู้ใช้งานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบ และถือปฏิบัติเป็นไปตามที่นโยบายกำหนด โดยการเผยแพร่ต้องดำเนินการในลักษณะที่ผู้ใช้งานเข้าถึงได้ง่าย

2) การทบทวนนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Review of the Policies for Information Security)

2.1) แผนกเทคโนโลยีและสารสนเทศต้องดำเนินการตรวจสอบและทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามเงื่อนไขที่กำหนดไว้ในส่วนที่ 2.5 การทบทวนนโยบาย

ส่วนที่ 5.2 การจัดโครงสร้างความมั่นคงปลอดภัยด้านสารสนเทศ (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม กำกับ และติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับส่วนงานต่างๆ ภายในบริษัทฯ และเพื่อเป็นแนวทางควบคุมการใช้งานอุปกรณ์สื่อสารประเภทพกพา ให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

5.2.1 การจัดโครงสร้างภายในองค์กร (Internal Organization)

1) การกำหนดบทบาทและหน้าที่ความรับผิดชอบความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Roles and Responsibilities)

1.1) ผู้บริหารระดับฝ่ายต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศสำหรับบุคลากรในหน่วยงานอย่างเป็นลายลักษณ์อักษรและให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่กำหนดไว้

2) การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties)

2.1) ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบในการปฏิบัติงานด้านต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศออกจากกันอย่างชัดเจนเพื่อให้มีการสอบทานระหว่างกันได้

3) การประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้องด้านความมั่นคงปลอดภัย(Contact with authorities)

3.1) แผนกเทคโนโลยีและสารสนเทศต้องรวบรวมรายชื่อและช่องทางการติดต่อของหน่วยงานที่จำเป็น เช่น หน่วยงานด้านกฎหมาย โรงพยาบาล สถานีตำรวจ สถานีดับเพลิง หรือหน่วยกู้ภัย เป็นต้น สำหรับติดต่อเมื่อเกิดเหตุฉุกเฉิน พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

4) การประสานงานกับกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Contact with special interest groups)

4.1) แผนกเทคโนโลยีและสารสนเทศต้องรวบรวมรายชื่อกลุ่มผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และเพิ่มช่องทางการรับข่าวสารจากกลุ่มผู้เชี่ยวชาญ เพื่อให้สามารถติดต่อประสานงาน หรือรับข้อมูลข่าวสาร หรือขอความช่วยเหลือในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศได้ทันท่วงที พร้อมทั้งปรับปรุงรายชื่อและช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

5) การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศในการบริหารจัดการโครงการ (Information Security in Project Management)

5.1) ผู้บริหารระดับฝ่ายต้องกำหนดให้มีการควบคุมความเสี่ยง การติดตามการดำเนินงานโครงการ รวมถึงการประเมินภาพรวมในการดำเนินงานโครงการ ทั้งโครงการที่เป็นโครงการภายในและโครงการที่จัดซื้อจัดจ้างจากหน่วยงานภายนอก

ส่วนที่ 5.3 การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศของบริษัทฯและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูลของบริษัทฯ

5.3.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง

(Business Requirement for Access Control)

1) การควบคุมการเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Service)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดให้มีการขอเข้าถึงข้อมูลและระบบสารสนเทศของผู้ใช้งานโดยต้องได้รับการอนุมัติจากผู้บังคับบัญชาเท่านั้น

1.2) แผนกเทคโนโลยีและสารสนเทศต้องจำกัดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายได้ เฉพาะบริการที่ผู้ใช้งานได้รับอนุญาตให้เข้าถึงเท่านั้น โดยสิทธิที่ได้รับต้องเป็นไปตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน

5.3.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

1) การลงทะเบียนและถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration)

1.1) แผนกเทคโนโลยีและสารสนเทศและเจ้าของข้อมูล ต้องร่วมกันกำหนดวิธีการบริหารจัดการการลงทะเบียนและถอดถอนสิทธิผู้ใช้งานอย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทฯรับทราบและปฏิบัติตาม

2) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

2.1) แผนกเทคโนโลยีและสารสนเทศและเจ้าของข้อมูล ต้องกำหนดให้มีการมอบหมายหรือกำหนดสิทธิ์การใช้งานให้แก่ผู้ใช้งานในการเข้าถึงข้อมูลหรือระบบสารสนเทศตามหน้าที่ความรับผิดชอบ

2.2) แผนกเทคโนโลยีและสารสนเทศและเจ้าของข้อมูล ต้องจัดทำเอกสารการมอบหมายสิทธิ์การเข้าถึงข้อมูลหรือระบบสารสนเทศ และจัดเก็บไว้เป็นหลักฐานในการดำเนินงาน

2.3) แผนกเทคโนโลยีและสารสนเทศและเจ้าของข้อมูล ต้องกำหนดกระบวนการในการบริหารจัดการสิทธิ์การเข้าถึง ในกรณีที่ผู้ใช้งานมีความจำเป็นต้องใช้งานข้อมูลหรือระบบสารสนเทศเกินสิทธิ์ที่ได้รับมอบหมาย

3) การบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูง (Management of Privileged Access Right)

3.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดเก็บรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูง เช่น Administrator/ root บนเครื่องแม่ข่าย หรือ Administrator ของระบบ Application และให้มีการเบิกใช้งานตามความจำเป็นเท่านั้น

3.2) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการรหัสผู้ใช้งานที่มีสิทธิ์ระดับสูงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบและปฏิบัติตาม

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

4.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดวิธีการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้อย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทฯรับทราบและปฏิบัติตาม

5) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

5.1) แผนกเทคโนโลยีและสารสนเทศและเจ้าของข้อมูล ต้องจัดทำขั้นตอนปฏิบัติการทบทวนสิทธิ์การเข้าถึงข้อมูล ระบบสารสนเทศ และโปรแกรมประยุกต์ (Application) อย่างเป็นลายลักษณ์อักษรและปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทฯรับทราบและปฏิบัติตาม

5.2) แผนกเทคโนโลยีและสารสนเทศและเจ้าของข้อมูล ต้องกำหนดรอบในการทบทวนสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศอย่างชัดเจนและแจ้งให้ผู้ที่เกี่ยวข้องรับทราบ

5.3) การทบทวนสิทธิ์การเข้าถึง ต้องพิจารณาประเด็นดังต่อไปนี้

1. รอบการทบทวนสิทธิ์ที่กำหนดไว้
2. การพ้นสภาพการเป็นบุคลากรของบริษัทฯ
3. การเปลี่ยนแปลงโยกย้ายหน้าที่การปฏิบัติงาน
4. การขอใช้สิทธิ์นอกเหนือจากหน้าที่ความรับผิดขอบที่กำหนดไว้

5.4) เมื่อดำเนินการทบทวนสิทธิ์เรียบร้อยแล้วให้เจ้าของข้อมูลหรือผู้ดูแลระบบจัดเก็บหลักฐานการทบทวนสิทธิ์ โดยให้แยกหลักฐานตามช่วงเวลาการทบทวนสิทธิ์

6) การถอดถอนสิทธิ์ในการเข้าถึง (Removal of Access Rights)

6.1) เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดเกณฑ์การพิจารณาการถอดถอนสิทธิ์การเข้าถึงและวิธีการถอดถอนสิทธิ์ในการเข้าถึงอย่างเป็นลายลักษณ์อักษร รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทฯรับทราบและปฏิบัติตาม

5.3.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

1) การใช้งานข้อมูลการพิสูจน์ตัวตน (Use of Secret Authentication Information)

1.1) ผู้ใช้งานจะต้องไม่ใช้โครงสร้างรหัสผ่านหรือคุณลักษณะที่ง่ายต่อการเดา อาทิ คำศัพท์ในพจนานุกรม (Dictionary) หรือคัดลอกหรือผสมจากชื่อผู้ใช้ หรืออักขระเรียงลำดับ หรือข้อมูลส่วนบุคคล หรือประโยควลีใดๆ ที่สามารถคาดเดาได้ง่าย

1.2) ผู้ใช้งานจะต้องไม่เขียนหรือบันทึกรหัสผ่านที่ใช้ และเก็บหรือแสดงให้เห็นไว้ใกล้กับระบบหรืออุปกรณ์ที่ใช้กับรหัสผ่านนั้น

1.3) ผู้ใช้งานจะต้องรับผิดชอบต่อการกระทำทุกอย่างที่เกิดขึ้นหากการกระทำนั้นสามารถบ่งชี้ให้เห็นว่าเกิดจากบัญชีผู้ใช้งานนั้น และจะต้องไม่อนุญาตให้ผู้อื่นกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานของตน หรือกระทำการใดๆ โดยใช้บัญชีผู้ใช้งานอื่นที่ไม่มีสิทธิ์

1.4) ผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดการบริหารจัดการรหัสผ่านอื่นๆ ที่บริษัทฯกำหนดไว้

5.3.4 การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ

(Application and Information Access Control)

1) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

1.1) เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดวิธีการเข้าถึงข้อมูล ระบบสารสนเทศและฟังก์ชั่นในระบบงาน โดยต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

1.2) เจ้าของข้อมูลและผู้ดูแลระบบ ต้องกำหนดวิธีการใช้งานระบบสารสนเทศที่สำคัญ ไม่ว่าจะเป็นข้อมูล ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของฝ่ายงานนั้นๆ เป็นลายลักษณ์อักษร

2) การเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัย (Secure Log-on Procedures)

2.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดวิธีการเข้าสู่ระบบสารสนเทศที่มีความมั่นคงปลอดภัย อย่างเป็นลายลักษณ์อักษร โดยอ้างอิงวิธีการที่เป็นมาตรฐานสากลและปรับปรุงให้เป็นปัจจุบันเสมอรวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทฯรับทราบและปฏิบัติตาม

3) ระบบสำหรับบริหารจัดการรหัสผ่าน (Password Management System)

3.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดให้มีระบบสำหรับบริหารจัดการบัญชีผู้ใช้และรหัสผ่านสำหรับการเข้าถึงระบบสารสนเทศของผู้ใช้งานภายในบริษัทฯ เพื่อให้เกิดการบริหารจัดการที่เป็นมาตรฐานเดียวกัน

4) การควบคุมการใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

4.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดให้มีการควบคุมการใช้โปรแกรมอรรถประโยชน์และจำกัดการใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบสารสนเทศหรือโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้

5) การเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)

5.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดมาตรการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม และการนำซอร์สโค้ดของโปรแกรมไปใช้ในการพัฒนา เพื่อป้องกันการเกิดข้อผิดพลาดในการพัฒนาระบบสารสนเทศ และระบบงานของบริษัทฯ

ส่วนที่ 5.4 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการป้องกัน ควบคุมการใช้งานและการบำรุงรักษาด้านกายภาพของ ทรัพย์สินสารสนเทศ และอุปกรณ์สารสนเทศซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของบริษัทฯ ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

5.4.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure Area)

1) ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องพิจารณาและจัดทำพื้นที่ที่ต้องการรักษาความปลอดภัย (Data Center) โดยจะประกอบด้วยพื้นที่กั้น บริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกหลัก และระบบรักษาความปลอดภัยอย่างเหมาะสม

2) การควบคุมการเข้าออกทางกายภาพ (Physical Entry Controls)

2.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมการเข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ (Data Center) ให้เข้าถึงได้เฉพาะบุคลากรผู้ได้รับอนุญาตเท่านั้น

2.2) รายชื่อผู้ได้รับอนุญาตให้เข้าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ต้องได้รับการตรวจสอบ ปรับปรุง และดูแลให้เหมาะสมอย่างสม่ำเสมอ

2.3) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดให้มีการควบคุมการเข้าออกพื้นที่ที่ต้องการรักษาความปลอดภัย (Secure Area) ได้แก่ ห้องคอมพิวเตอร์ โดยต้องกำหนดให้เฉพาะผู้มีสิทธิ์ที่สามารถเข้าออกได้ และมีการเก็บบันทึกการเข้าออกห้องคอมพิวเตอร์ และบันทึกการเข้าออกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก วัตถุประสงค์การผ่านเข้าออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

3) การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินสารสนเทศอื่นๆ ทางด้านระบบเทคโนโลยีสารสนเทศ (Securing Offices, Rooms, and Facilities for Information Technology Systems)

3.1) แผนกเทคโนโลยีและสารสนเทศ ต้องออกแบบและติดตั้งระบบการรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อป้องกันพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีข้อมูลสำคัญ ห้องคอมพิวเตอร์ หรืออุปกรณ์สารสนเทศต่างๆ ที่ใช้ในการปฏิบัติงานอันเนื่องจากการได้รับความเสียหายและถูกเข้าถึงโดยไม่ได้รับอนุญาต

4) การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting Against External end Environmental Threats)

4.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุม กำกับให้มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยคุกคามจากภายนอก ทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

5) การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

5.1) แผนกเทคโนโลยีและสารสนเทศต้องกำกับให้มีการกำหนดแนวปฏิบัติของการป้องกันทางกายภาพสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure Area) ได้แก่ ห้องคอมพิวเตอร์ และกำหนดให้มีการนำแนวปฏิบัติไปใช้งานอย่างเคร่งครัด

6) พื้นที่สำหรับรับส่งสิ่งของ (Delivery and Loading Areas)

6.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดให้มีการควบคุมบริเวณที่ผู้ไม่มีสิทธิ์เข้าถึงอาจสามารถเข้าถึงได้ ในกรณีที่ต้องมีการส่งหรือรับมอบสินค้าอุปกรณ์ที่ต้องเข้าถึงห้องคอมพิวเตอร์ แผนกเทคโนโลยีและสารสนเทศจะต้องจัดสรรพื้นที่แยกสำหรับการดำเนินการเพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยผู้ที่ไม่ได้รับอนุญาต

5.4.2 อุปกรณ์ (Equipment)

1) การจัดวางและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดวางอุปกรณ์สารสนเทศไว้ในห้องหรือบริเวณที่ปลอดภัย อุปกรณ์ที่มีตู้ ประตูของตู้วางคอมพิวเตอร์แม่ข่ายและอุปกรณ์สื่อสารเครือข่ายต้องถูกล็อคอยู่เสมอ โดยกำหนดให้มีเพียงเจ้าหน้าที่ผู้ที่ได้รับอนุญาตเท่านั้นที่มีสิทธิ์ในการเปิดเพื่อซ่อมบำรุง หรือการปรับปรุงค่าคอนฟิเกอเรชัน (Reconfiguration) เพื่อลดความเสี่ยงจากการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

2) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

2.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมดูแลให้มีการติดตั้งอุปกรณ์ป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่างๆ ภายในห้องคอมพิวเตอร์ เช่น อุปกรณ์ดับเพลิง อุปกรณ์ดักจับควันไฟ อุปกรณ์สำรองไฟฟ้า ระบบควบคุมอุณหภูมิ หรือระบบแจ้งเตือนเมื่ออุปกรณ์สารสนเทศทำงานผิดปกติ เป็นต้น และต้องบำรุงดูแลรักษาอุปกรณ์ให้พร้อมใช้งานอยู่เสมอ

3) ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

3.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมดูแลให้การติดตั้งและการบำรุงรักษาสายไฟฟ้าและสายสื่อสารในพื้นที่ปฏิบัติงานและห้องคอมพิวเตอร์เป็นไปตามมาตรฐานความปลอดภัยอุตสาหกรรม เพื่อป้องกันไม่ให้มีการเข้าถึงหรือดักจับข้อมูล หรือเกิดความเสียหายทางด้านกายภาพ

4) การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

4.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมดูแลให้อุปกรณ์ระบบสารสนเทศหลักทั้งหมดซึ่งใช้ในการประมวลผลในระดับปฏิบัติการ รวมถึงอุปกรณ์สนับสนุนการทำงานได้รับการบำรุงดูแลรักษาตามช่วงเวลาและตามข้อกำหนดที่ผู้ผลิตแนะนำ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้งาน

4.2) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมให้มีการบันทึกบันทึกกิจกรรมการบำรุงอุปกรณ์ รวมถึงบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ให้อยู่ในสภาพพร้อมใช้งานเสมอ

5) การนำทรัพย์สินสารสนเทศออกนอกสำนักงาน (Removal of Assets)

5.1) ผู้ทำหน้าที่กำกับดูแลพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยและอาคารสถานที่ ต้องไม่อนุญาตให้นำอุปกรณ์สารสนเทศออกจากบริษัทฯ ยกเว้นจะมีการอนุญาตให้นำออกโดยผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินสารสนเทศออก

5.2) ผู้ใช้งาน ต้องไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกนอกบริษัทฯ ยกเว้นจะได้รับอนุญาตจากผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินสารสนเทศออก

6) ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินสารสนเทศที่ใช้งานอยู่ภายนอกสำนักงาน (Security of Equipment and Asset Off-Permises)

6.1) กำหนดให้ผู้บริหารระดับฝ่ายขึ้นไป เป็นผู้มีอำนาจในการอนุญาตให้นำอุปกรณ์สารสนเทศของบริษัทฯไปใช้งานภายนอกบริษัทฯและต้องกำหนดให้มีการป้องกันอุปกรณ์สารสนเทศต่างๆ ที่ใช้งานอยู่ภายนอกบริษัทฯเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์ โดยพิจารณาจากความเสี่ยงที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

6.2) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดมาตรการความมั่นคงปลอดภัยในการควบคุมทรัพย์สินสารสนเทศใช้งานอยู่ภายนอกบริษัทฯ เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินสารสนเทศของบริษัทฯออกไปใช้งาน

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

7.1) ผู้ใช้งาน ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำคัญหรือซอฟต์แวร์ลิขสิทธิ์ที่อยู่ภายในสื่อบันทึกข้อมูลได้มีการลบ ย้าย หรือทำลายอย่างเหมาะสมตามลำดับชั้นความลับข้อมูล ก่อนที่จะทำลายหรือจำหน่ายอุปกรณ์หรือนำอุปกรณ์กลับมาใช้ใหม่

7.2) แผนกเทคโนโลยีและสารสนเทศต้องจัดทำขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลหรือทรัพย์สินสารสนเทศ และมาตรการหรือเทคนิคสำหรับการทำลายข้อมูลเพื่อนำอุปกรณ์สารสนเทศกลับมาใช้งานซ้ำ โดยต้องมีความสอดคล้องกับการจัดลำดับชั้นความลับข้อมูล

7.3) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดผู้รับผิดชอบในการทำหน้าที่ทำลายข้อมูลสารสนเทศที่ไม่จำเป็นต่อการดำเนินกิจการของบริษัทฯซึ่งจัดเก็บอยู่บนสื่อบันทึกข้อมูล

8) การป้องกันอุปกรณ์ที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended User Equipment)

8.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดมาตรการควบคุมการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศที่ทิ้งไว้โดยไม่มีผู้ดูแล เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต

8.2) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

8.3) ผู้ใช้งานต้องออกจากระบบสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์ โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน

8.4) ผู้ใช้งาน ต้องล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์

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 หรือสื่อบันทึกข้อมูลให้อยู่ในสถานที่ไม่ปลอดภัย พื้นที่สาธารณะ หรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ใช้งานต้องจัดเก็บข้อมูลสารสนเทศในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงของผู้ไม่มีสิทธิ์

9.3) ผู้ใช้งานต้องไม่จัดเก็บข้อมูลสำคัญไว้บนหน้าเดสท็อป (Desktop) ของเครื่องคอมพิวเตอร์ โดยผู้ใช้งานต้องจัดสรรพื้นที่ในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์และควบคุมการเข้าถึงอย่างเหมาะสม เพื่อป้องกันผู้อื่นเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

ส่วนที่ 5.5 การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ (Operations Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมให้การดำเนินงาน การจัดการด้านการสื่อสารความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ มีแนวทางปฏิบัติที่มีขั้นตอนชัดเจนและมีความมั่นคงปลอดภัย

5.5.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operations Procedures and Responsibilities)

1) ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดให้มีขั้นตอนปฏิบัติงานด้านระบบสารสนเทศที่สำคัญเป็นลายลักษณ์อักษร โดยต้องแบ่งแยกอำนาจหน้าที่ของบุคลากรตามโครงสร้างการปฏิบัติหน้าที่ที่ชัดเจนเพื่อให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทฯ

1.2) หน่วยงานในแผนกเทคโนโลยีและสารสนเทศต้องจัดทำคู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจระบบงาน ลักษณะงาน และกระบวนการทำงาน

1.3) หน่วยงานในแผนกเทคโนโลยีและสารสนเทศต้องทบทวนวิธีปฏิบัติ คู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ดังกล่าวให้เป็นปัจจุบันอยู่เสมอรวมทั้งจัดให้ขั้นตอนปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งานและเข้าถึงได้ และต้องสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบและปฏิบัติตาม

2) การบริหารจัดการการเปลี่ยนแปลง (Change Management)

2.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุม กำกับให้มีการจัดการควบคุมการเปลี่ยนแปลงของการเปลี่ยนแปลงโครงสร้างบริษัทฯขั้นตอนการปฏิบัติงาน ระบบสารสนเทศ เพื่อควบคุมก่อนการเปลี่ยนแปลง แก้ไข หรือกระทำการใดๆ ซึ่งส่งผลต่อการดำเนินงานของระบบงานต่างๆ ทั้งนี้ให้ปฏิบัติตามที่กำหนดไว้

3) การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

3.1) ผู้ดูแลระบบ ต้องติดตามประสิทธิภาพการทำงานของระบบงานและอุปกรณ์สารสนเทศที่สำคัญ ให้ทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

3.2) ผู้ดูแลระบบ ต้องประเมินสมรรถภาพและความเพียงพอ (Capacity) ของทรัพยากรสารสนเทศ เช่น หน่วยประมวลผล (CPU) หน่วยความจำ (Memory) หน่วยจัดเก็บข้อมูล (Disk) หรือปริมาณการใช้งานระบบเครือข่าย (Bandwidth) เป็นต้น และต้องวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศให้ระบบสารสนเทศมี ประสิทธิภาพที่เหมาะสม และเพียงพอต่อการใช้งานในอนาคต

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

4.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุม กำกับให้มีการแยกส่วนระบบคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) การทดสอบระบบงาน (Test Enviroment) และระบบที่ให้บริการจริง (Production Environment) ออกจากกัน

4.2) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมให้มีการกำหนดสิทธิ์การเข้าถึงในแต่ละสภาพแวดล้อม และจัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบงานอย่างชัดเจน โดยต้องรายงาน

ผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหา และวิธีการแก้ไข รวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ

5.5.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

1) มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls Against Malware)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้คืนระบบเพื่อป้องกันทรัพย์สินสารสนเทศจากซอฟต์แวร์ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานอย่างเหมาะสม

5.5.3 การสำรองข้อมูล (Back up)

1) การสำรองข้อมูล (Information Backup)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดมาตรการในการสำรองข้อมูล และรอบการสำรองข้อมูลของระบบสารสนเทศที่สำคัญไว้อย่างสม่ำเสมอ เพื่อป้องกันการสูญหายของข้อมูล

1.2) เจ้าของข้อมูลสารสนเทศ ต้องดำเนินการหรือกำหนดให้มีการสำรองข้อมูลสารสนเทศและการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าจะสามารถนำข้อมูลกลับมาใช้ใหม่ได้เมื่อต้องการ

1.3) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น External Hard Disk , Share Drive ของบริษัทฯ เป็นต้น ให้เป็นปัจจุบันอย่างสม่ำเสมอ รวมถึงให้จัดเก็บไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

5.5.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

1) การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event Logging)

1.1) ผู้ดูแลระบบ ต้องจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log) ซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศให้เพียงพอต่อการตรวจสอบ

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 ต้องจัดให้มีการป้องกันข้อมูลและระบบการบันทึกและจัดเก็บหลักฐานการใช้งาน เกี่ยวกับระบบสารสนเทศจากการถูกเปลี่ยนแปลงแก้ไข ถูกทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต

3) การบันทึกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and Operator Logs)

3.1) ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบและผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบ อาทิ เวลาเปิดและปิดระบบ การเปลี่ยนแปลงการตั้งค่าของระบบ ความผิดพลาดของระบบ และการดำเนินการแก้ไข และต้องมีการสอบทานบันทึกกิจกรรมอย่างสม่ำเสมอ

4) การตั้งเวลาระบบสารสนเทศ (Clock Synchronization)

4.1) ผู้ดูแลระบบ ต้องควบคุม กำกับให้อุปกรณ์สารสนเทศ และระบบสารสนเทศของบริษัทฯ ได้รับการกำหนดเวลาให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องและตรงกับเวลาอ้างอิงสากล

4.2) ผู้ดูแลระบบ ต้องตรวจสอบเวลาของอุปกรณ์สารสนเทศและระบบสารสนเทศของบริษัทฯ รวมถึงปรับปรุงให้เป็นปัจจุบันเสมอ เพื่อป้องกันไม่ให้เกิดการบันทึกเวลาที่ไม่ถูกต้อง

5.5.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software)

1) การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of Software on Operational Systems)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดทำขั้นตอนปฏิบัติงานและมาตรการควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง เพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งานและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน

1.2) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดรายการซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัทฯอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในบริษัทฯรับทราบและปฏิบัติตาม

5.5.6 การบริหารจัดการช่องโหว่ทางเทคนิคในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

1) การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมให้ระบบสารสนเทศของบริษัทฯ ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้ดำเนินการตามความเหมาะสมและความเสี่ยง

1.2) ผู้ดูแลระบบ ต้องดูแลและบำรุงรักษาระบบ เพื่อรักษาระดับความมั่นคงปลอดภัยด้านสารสนเทศของระบบอย่างสม่ำเสมอ ได้แก่ การประเมินความเสี่ยงของช่องโหว่ที่ตรวจสอบพบ และการปรับปรุงแก้ไขช่องโหว่ของระบบสารสนเทศ

2) การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

2.1) ผู้ใช้งานต้องปฏิบัติตามกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์ และไม่ติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของบริษัทฯ

5.5.7 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)

1) มาตรการการตรวจประเมินระบบ (Information System Audit Controls)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดให้มีการตรวจสอบทางด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

ส่วนที่ 5.6 การสื่อสารด้านความมั่นคงปลอดภัยสารสนเทศ (Communications Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการบริหารจัดการเครือข่าย และการส่งข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอกบริษัทฯให้มีความมั่นคงปลอดภัย

5.6.1 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)

1) การควบคุมเครือข่าย (Network Controls)

1.1) ผู้ดูแลระบบ ต้องควบคุม กำกับให้มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชั่นที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย

2) ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)

2.1) ผู้ดูแลระบบ ต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมด ลงในข้อตกลงหรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายในหรือภายนอก

3) การแบ่งแยกเครือข่าย (Segregation in Network)

3.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยต้องพิจารณาถึงความต้องการของผู้ใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่ายนั้น

ส่วนที่ 5.7 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

วัตถุประสงค์

เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

5.7.1 ความต้องการด้านความมั่นคงปลอดภัยระบบ (Security Requirements of Information Systems)

1) การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

1.1) แผนกเทคโนโลยีและสารสนเทศและหน่วยงานที่ได้รับมอบหมายให้พัฒนาหรือจัดหาระบบสารสนเทศเพื่อนำมาใช้งานในบริษัทฯ กำหนดคุณลักษณะความต้องการด้านความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือระบบที่จัดหามาใช้งาน

1.2) แผนกเทคโนโลยีและสารสนเทศและหน่วยงานที่ได้รับมอบหมายให้พัฒนาหรือจัดหาระบบสารสนเทศ ต้องติดตามการพัฒนาระบบสารสนเทศ เพื่อตรวจสอบว่าการพัฒนาระบบสารสนเทศตรงตามความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงความต้องการด้านการใช้งานที่กำหนดไว้

2) ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing Application Service on Public Networks)

2.1) ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการ การใช้งาน (Application Service) ทั้งในกรณีทั่วไปและกรณีที่ผ่านเครือข่ายสาธารณะ เพื่อป้องกันการกระทำผิดในลักษณะทุจริต (Fraudulent Activities) การทำธุรกรรมที่ไม่สมบูรณ์หรือผิดพลาด (Incomplete Transmission or Miss-Routing) หรือการเปิดเผยคัดลอก หรือเปลี่ยนแปลงแก้ไขข้อมูล โดยไม่ได้รับอนุญาต

3) การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting Application Services Transactions)

3.1) ข้อมูลสารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง (Miss-Routing) การเปลี่ยนแปลงโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการสำเนาข้อมูลโดยไม่ได้รับอนุญาต

5.7.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและสนับสนุน (Security in Development and Support Processes)

1) นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดกฎระเบียบสำหรับการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย และครอบคลุมตลอดทั้งวงจรการพัฒนาระบบสารสนเทศ

2) ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures)

2.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร โดยให้ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ

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

3.1) ผู้ดูแลระบบ จะต้องทำการตรวจสอบทางเทคนิคเพื่อวิเคราะห์ถึงผลกระทบทบที่อาจเกิดขึ้นเมื่อต้องการที่จะเปลี่ยนแปลงหรือปรับปรุงระบบปฏิบัติการ เช่น การเปลี่ยนเวอร์ชัน และการแก้ไข ข้อบกพร่องด้านความมั่นคงปลอดภัย เป็นต้น โดยจะต้องมีการทดสอบบนเครื่องทดสอบ (Test Environment) จนมั่นใจว่าระบบงานต่างๆ ที่ประมวลผลบนเครื่องดังกล่าวสามารถทำงานได้ตามปกติและมีความมั่นคงปลอดภัย จึงจะทำการเปลี่ยนแปลงหรือปรับปรุงบนเครื่องที่ใช้งานจริง (Production Environment)

3.2) ผู้ดูแลระบบ จะต้องทำการตรวจสอบทางเทคนิคภายหลังการเปลี่ยนแปลงระบบปฏิบัติการบนระบบจริง เพื่อตรวจสอบว่าการเปลี่ยนแปลงไม่มีผลกระทบต่อการทำงานของระบบ และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยระบบสารสนเทศ

4) การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

4.1) ซอฟต์แวร์สำเร็จรูปที่นำมาใช้งานในบริษัทฯควรใช้งานโดยปราศจากการแก้ไข หากในกรณีที่มีความจำเป็นต้องดำเนินการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป หน่วยงานที่ได้รับมอบหมายให้ดำเนินการต้องพิจารณาการควบคุมการแก้ไขอย่างเข้มงวด

4.2) การเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป ต้องดำเนินการเปลี่ยนแปลงตามขั้นตอนปฏิบัติการควบคุมการเปลี่ยนแปลงที่ฝ่ายสารสนเทศกำหนดไว้

5) หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles)

5.1) แผนกเทคโนโลยีและสารสนเทศและหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบ ดังต่อไปนี้เป็นอย่างน้อย

1. การให้สิทธิ์ต่ำที่สุด (Least Privilege) แก่ผู้ใช้งานระบบสารสนเทศ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
2. การให้สิทธิ์เฉพาะที่จำเป็นในการปฏิบัติงาน (Need to Know) แก่ผู้ใช้งานระบบสารสนเทศ เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ

6) สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure Development Environment)

6.1) แผนกเทคโนโลยีและสารสนเทศและหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบสารสนเทศต้องมีการควบคุมสภาพแวดล้อมของการพัฒนาและบูรณาการระบบให้มีความมั่นคงปลอดภัย โดยต้องป้องกันข้อมูลของระบบที่เกิดขึ้นในระหว่างการพัฒนา การรับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบสารสนเทศ

7) การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced Development)

7.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดข้อตกลงในการพัฒนาระบบสำหรับหน่วยงานภายนอกที่ทำหน้าที่พัฒนาซอฟต์แวร์เพื่อใช้งานภายในบริษัทฯอย่างเป็นลายลักษณ์อักษร

7.2) หน่วยงานที่ได้รับมอบหมายให้ดำเนินการจัดจ้างหน่วยงานภายนอกเข้ามาพัฒนาระบบสารสนเทศให้บริษัทฯ ต้องกำกับดูแล เฝ้าระวัง และติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการอย่างสม่ำเสมอ เพื่อป้องกันไม่ให้เกิดความเสียหายใดๆ ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ

8) การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing)

8.1) แผนกเทคโนโลยีและสารสนเทศหน่วยงานที่ได้รับมอบหมาย และผู้ใช้งาน ต้องร่วมกันทดสอบฟังก์ชันการทำงานของระบบสารสนเทศ และฟังก์ชันการทำงานด้านความมั่นคงปลอดภัยสารสนเทศในระบบที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงทุกครั้ง

8.2) การทดสอบการพัฒนาระบบสารสนเทศ ต้องดำเนินการทดสอบระหว่างการพัฒนา และก่อนนำระบบขึ้นใช้งานจริง โดยต้องจัดเก็บหลักฐานในการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาขึ้นใหม่ หรือระบบที่มีการเปลี่ยนแปลงอย่างเป็นทางการ

9) การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)

9.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่หรือที่ปรับปรุงเพิ่มเติม ทั้งที่มาจากส่วนพัฒนาระบบโนโลยีสารสนเทศพัฒนาขึ้น หรือที่มีการจัดหาจากหน่วยงานภายนอก และต้องทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้งานจริง

5.7.3 ข้อมูลสำหรับการทดสอบ (Test Data)

1) การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

1.1) แผนกเทคโนโลยีและสารสนเทศหน่วยงานที่ได้รับมอบหมาย และผู้ใช้งานต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่มีอยู่บนระบบให้บริการมาใช้ในการทดสอบ ในกรณีที่มีการนำสำเนาข้อมูลจากระบบใช้งานจริงเพื่อใช้ในการทดสอบต้องมีการ ควบคุมข้อมูลที่ใช้ทดสอบเหมือนกับการควบคุมข้อมูลที่อยู่ในระบบใช้งานจริง

ส่วนที่ 5.8 การบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอก (Supplier Relationships)

วัตถุประสงค์

เพื่อจัดทำข้อกำหนดต่างๆ และกรอบการปฏิบัติงานของหน่วยงานภายนอกในการให้บริการหรือการใช้บริการด้านงานเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย และได้รับผลประโยชน์สูงสุดแก่บริษัทฯ

5.8.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับหน่วยงานภายนอก (Information Security in Supplier Relationships)

1) นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับหน่วยงานภายนอก (Information Security Policy for Supplier Relationships)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดนโยบายหรือระเบียบปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับหน่วยงานภายนอก โดยผู้ที่เกี่ยวข้องต้องพิจารณาหรือประเมินความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนที่จะอนุญาตให้หน่วยงานภายนอกหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของบริษัทฯ

1.2) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุม กำกับให้มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้าง ปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ

2) การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

2.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมให้มีการกำหนดข้อตกลงเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับการอนุญาตให้หน่วยงานภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศ เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร

2.2) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมให้หน่วยงานภายนอกสามารถเข้าถึงสารสนเทศของบริษัทฯเฉพาะส่วนที่มีความจำเป็นต้องรู้ และต้องได้รับการยินยอมจากเจ้าของข้อมูลสารสนเทศ อย่างเป็นลายลักษณ์อักษรเท่านั้น

2.3) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องควบคุมดูแลให้หน่วยงานภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างบริษัทฯและหน่วยงานภายนอก

3) การบริหารจัดการและการสื่อสารต่อผู้รับจ้างช่วงของหน่วยงานภายนอก (Information and Communication Technology Supply Chain)

3.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับหน่วยงานภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมถึงผู้รับจ้างช่วงที่หน่วยงานภายนอกเป็นผู้จัดหา

5.8.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

1) การติดตามและทบทวนการให้บริการของหน่วยงานภายนอก (Monitoring and Review of Supplier Services)

1.1) ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องติดตามและตรวจทานการดำเนินงานของหน่วยงานภายนอกซึ่งมีหน้าที่ในการบริหารจัดการระบบประมวลผลข้อมูลสารสนเทศให้กับบริษัทฯ ทั้งในด้านฐานะทางการเงิน กระบวนการปฏิบัติงาน และประสิทธิภาพการให้บริการอย่างสม่ำเสมอ

2) การบริหารจัดการการเปลี่ยนแปลงบริการของหน่วยงานภายนอก (Managing Changes to Supplier Services)

2.1) กรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ผู้ดูแลระบบ และหน่วยงานที่ได้รับมอบหมายให้ประสานงานกับหน่วยงานภายนอก ต้องจัดให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว โดยต้องรายงานให้ผู้บริหารและผู้ที่เกี่ยวข้องรับทราบ รวมถึงให้กำหนดกระบวนการบริหารจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสม

ส่วนที่ 5.9 การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ การเรียนรู้ข้อผิดพลาดจากปัญหาที่เกิดขึ้นและการปรับปรุงแก้ไข ซึ่งเป็นการป้องกันไม่ให้เกิดเหตุการณ์ทางด้านความมั่นคงปลอดภัยสารสนเทศซ้ำขึ้นอีก

5.9.1 การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Management of Information Security Incidents and Improvements)

1) หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดหน้าที่ในการบริหารจัดการสถานการด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และมอบหมายสิทธิการดำเนินงานอย่างชัดเจนให้บุคลากรภายในฝ่าย

1.2) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดให้มีการจำแนกสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิดออกจากเหตุขัดข้องด้านการปฏิบัติงานทั่วไป เพื่อกำหนดแนวทางการแก้ไขที่ถูกต้องเหมาะสม

1.3) แผนกเทคโนโลยีและสารสนเทศต้องกำหนดช่องทางและเกณฑ์ในการรายงานเหตุการณ์ หรือจุดอ่อน หรือเหตุขัดข้องที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ และสื่อสารให้บุคลากรในบริษัทฯและหน่วยงานภายนอกรับทราบ

2) การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events)

2.1) ผู้ใช้งาน และหน่วยงานภายนอกต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของบริษัทฯต่อผู้บังคับบัญชาและแผนกเทคโนโลยีและสารสนเทศโดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด

3) การรายงานจุดอ่อนด้านความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

3.1) ผู้ใช้งาน และหน่วยงานภายนอกต้องรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของบริษัทฯต่อผู้บังคับบัญชาและแผนกเทคโนโลยีและสารสนเทศโดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด

3.2) ผู้ใช้งานและหน่วยงานภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศหรือจุดอ่อนใดๆ ของระบบสารสนเทศในบริษัทฯ ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้นผู้บังคับบัญชาและแผนกเทคโนโลยีและสารสนเทศและห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศนั้นด้วยตนเอง

4) การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and Decision on Information Security Events)

4.1) ผู้ดูแลระบบ ต้องประเมินเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ ทำการจัดแยกกลุ่มเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัยและจัดลำดับความสำคัญตามเกณฑ์ที่กำหนดไว้ และแจ้งผู้ที่เกี่ยวข้องรับทราบเพื่อแก้ไขในกรณีที่พบว่าเหตุการณ์หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ที่ส่งผลกระทบด้านความมั่นคงปลอดภัยสารสนเทศ

5) การตอบสนองต่อเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Response to Information Security Incidents)

5.1) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศและหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ ต้องดำเนินการตามขั้นตอนการปฏิบัติงานสำหรับการแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดไว้

5.2) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศและหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ ต้องดำเนินการตอบสนองและแก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้ หากไม่สามารถแก้ไขได้ตามเวลาที่กำหนดต้องแจ้งให้ผู้บังคับบัญชารับทราบโดยเร็วที่สุด

6) การเรียนรู้จากเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from Information Security Incidents)

6.1) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศและหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ จะต้องจัดเตรียมรายงานผลการวิเคราะห์และการแก้ไขเหตุขัดข้อง จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและจัดเก็บไว้เป็นองค์ความรู้ เพื่อใช้ในการเรียนรู้ในการดำเนินงานและลดโอกาสเกิดในอนาคต

7) การเก็บรวบรวมหลักฐาน (Collection of Evidence)

7.1) บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศและหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ จะต้องดำเนินการเก็บรวบรวมหลักฐานที่เกี่ยวข้องกับเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น เพื่อรวบรวมหลักฐานให้เพียงพอต่อการนำเสนอผู้บริหารหน่วยงานที่เกี่ยวข้อง และใช้ในการดำเนินการด้านกฎหมายต่อไป

ส่วนที่ 5.10 ความมั่นคงปลอดภัยสำหรับการบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ Business Continuity Plan

วัตถุประสงค์

เพื่อป้องกันการติดขัด หรือหยุดชะงักของการดำเนินธุรกิจของบริษัทฯและป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวของระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบสารสนเทศกลับคืนมาได้ในระยะเวลาอันเหมาะสม

5.10.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity)

1) การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

1.1) เจ้าของข้อมูลและแผนกเทคโนโลยีและสารสนเทศต้องร่วมกันระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการทางธุรกิจ ประเมินความเสี่ยงเหตุการณ์และระบบงานสำคัญ เพื่อให้ได้มาซึ่งข้อมูลที่มีความถูกต้อง และครบถ้วน เพื่อใช้ในการจัดทำแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

2) การสร้างกระบวนการความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity)

2.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน โดยให้กำหนดมาตรการด้านความมั่นคงปลอดภัยสารสนเทศไว้เป็นส่วนหนึ่งของแผน และให้มีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจของบริษัทฯ

3) การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, Review and Evaluate Information Security Continuity)

3.1) แผนกเทคโนโลยีและสารสนเทศต้องทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉิน**อย่างน้อยปีละ 1 ครั้ง** และจัดให้มีการบันทึกผลการทดสอบ เพื่อให้มั่นใจว่าแผนงานที่จัดทำมีความถูกต้องและสามารถตอบสนองต่อการดำเนินงานได้เป็นอย่างดี

3.2) บุคลากรผู้ซึ่งมีส่วนเกี่ยวข้องในการปฏิบัติงานกู้คืนระบบสารสนเทศ ต้องมีความรู้ด้านเทคนิคที่จำเป็นต่อการกู้คืนระบบและเข้าร่วมการซักซ้อมแผน

3.3) เจ้าของข้อมูลและผู้ใช้งานระบบที่เกี่ยวข้องกับแผนรองรับการดำเนินการทางธุรกิจอย่างต่อเนื่อง ต้องเข้าร่วมการทดสอบแผน และดำเนินงานตามแผนที่กำหนดไว้

5.10.2 การจัดให้มีอุปกรณ์หรือระบบสารสนเทศสำรอง (Redundancies)

1) สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศที่มีความสำคัญสูง

1.2) แผนกเทคโนโลยีและสารสนเทศ ต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม

ส่วนที่ 5.11 การปฏิบัติตามกฎระเบียบและข้อบังคับ (Compliance)

วัตถุประสงค์

เพื่อให้การดำเนินงานต่างๆ ของบริษัทฯเป็นไปตามกฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆ ที่บริษัทฯและบุคลากรของบริษัทฯต้องปฏิบัติตาม รวมถึงให้มีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้

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

1) การระบุกฎหมายและข้อกำหนดในสัญญาจ้าง (Identification of Applicable Legislation and Contractual Requirements)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องร่วมกับส่วนกฎหมาย และฝ่ายบริหารทรัพยากรบุคคลในการรวบรวมกฎหมาย กฎระเบียบ หลักเกณฑ์ และข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.2) บุคลากรทั้งหมดต้องรับผิดชอบในการปฏิบัติตามข้อกำหนดที่ได้มีการระบุไว้อย่างเคร่งครัด

1.3) ห้ามเจ้าหน้าที่ในบริษัทฯใช้งานทรัพย์สินสารสนเทศและระบบเทคโนโลยีสารสนเทศของบริษัทฯกระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทยและกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม

2) การป้องกันสิทธิ และทรัพย์สินทางปัญญา (Intellectual Property Rights)

2.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดทำกระบวนการสำหรับการบริหารจัดการการใช้ซอฟต์แวร์ลิขสิทธิ์และทรัพย์สินทางปัญญา เพื่อให้มั่นใจว่าการใช้งานข้อมูลสารสนเทศที่อาจถือเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ที่พัฒนาโดยผู้ประกอบธุรกิจมีความสอดคล้องกับ กฎหมายและข้อกำหนดตามสัญญาต่างๆ

2.2) ผู้ใช้งานต้องไม่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่บริษัทฯ ได้จัดซื้อลิขสิทธิ์เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

2.3) ห้ามผู้ใช้งานทำการใช้งานทำซ้ำ หรือ เผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบสารสนเทศของบริษัทฯ โดยเด็ดขาด

2.4) ซอฟต์แวร์ที่พัฒนาเพื่อบริษัทฯ ทั้งโดยหน่วยงานภายนอกหรือบุคลากรในหน่วยงานของบริษัทฯถือว่าเป็นทรัพย์สินสารสนเทศของบริษัทฯ ไม่อนุญาตให้หน่วยงานภายนอกหรือบุคลากรในหน่วยงานของบริษัทฯทำสำเนา หรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินสารสนเทศของบริษัทฯ โดยไม่ได้รับอนุญาต

2.5) ผู้ใช้งานที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศของบริษัทฯต้องยึดถือและปฏิบัติตามกฎหมายลิขสิทธิ์ นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

3) การป้องกันข้อมูลขององค์กร (Protection of Records)

3.1) เจ้าของข้อมูล ต้องปฏิบัติตามข้อบังคับทางกฎหมายที่เกี่ยวกับข้อมูลสารสนเทศบางประเภท เช่น ด้านบัญชี ด้านลูกค้า และต้องจัดทำข้อกำหนดในการจัดการข้อมูลสารสนเทศ ระยะเวลาในการจัดเก็บ ให้สอดคล้องกับข้อบังคับดังกล่าว

3.2) เจ้าของข้อมูลต้องควบคุม ป้องกันมิให้ข้อมูลบันทึกหลักฐาน (Logs) ต่างๆ เกิดความเสียหาย สูญหาย ถูกเปลี่ยนแปลงแก้ไข ถูกเข้าถึงหรือเผยแพร่โดยไม่ได้รับอนุญาต โดยการควบคุมต้องให้สอดคล้องกับกฎหมาย ข้อกำหนด และความต้องการทางธุรกิจ

4) ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information)

4.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย ประกาศ หลักเกณฑ์ที่รัฐบาลได้ประกาศไว้ รวมถึงข้อบังคับต่างๆ ที่มีผลบังคับใช้กับบริษัทฯ

4.2) ข้อมูลสารสนเทศรายละเอียดที่เกี่ยวกับลูกค้าถือว่ามีความสำคัญ หน่วยงานผู้รับผิดชอบในการดูแลข้อมูลต้องกำหนดให้บุคลากรและลูกจ้างที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บังคับบัญชาเท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลสารสนเทศดังกล่าวได้

4.3) ข้อมูลส่วนบุคคลของบุคลากร ลูกจ้าง และลูกค้า ถือว่าเป็นความลับ และ สามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิ์ ตามที่บริษัทฯกำหนดเท่านั้น

4.4) แผนกเทคโนโลยีและสารสนเทศจะดำเนินงานโดยการปฏิบัติตาม นโยบายการคุ้มครองข้อมูลส่วนบุคคล(Pivacy Policy) ตามประกาศของบริษัทฯ

5) ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสลับข้อมูล (Regulation of Cryptographic Controls)

5.1) แผนกเทคโนโลยีและสารสนเทศต้องควบคุมการเข้ารหัสลับข้อมูลให้มีความสอดคล้องกับกฎหมาย ประกาศ หลักเกณฑ์ที่รัฐบาลได้ประกาศไว้ รวมถึงข้อบังคับต่างๆ ที่มีผลบังคับใช้กับบริษัทฯ

5.11.2 การทบทวนความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Reviews)

1) การตรวจประเมินระบบสารสนเทศจากผู้ตรวจสอบอิสระ (Independent Review of Information Security)

1.1) แผนกเทคโนโลยีและสารสนเทศต้องจัดให้มีการตรวจประเมินความมั่นคงปลอดภัยสารสนเทศ โดยส่วนตรวจสอบระบบงานหรือผู้ตรวจสอบอิสระภายนอก เพื่อตรวจสอบการปฏิบัติตามนโยบายมาตรฐาน และขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนทบทวนถึงความพอเพียงของการควบคุมระบบสารสนเทศ และการปฏิบัติตามการควบคุมต่างๆ

2) การปฏิบัติตามนโยบายและมาตรฐานความปลอดภัยสารสนเทศ (Compliance with Security Policies and Standards)

2.1) ผู้บังคับบัญชาของแต่ละแผนกต้องรับผิดชอบในการสอบทานการปฏิบัติตามนโยบาย มาตรฐาน และขั้นตอนปฏิบัติงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยสารสนเทศ ของบุคลากรใต้บังคับบัญชาอย่างสม่ำเสมอ

2.2) กรณีที่ผู้บังคับบัญชาของแต่ละแผนกตรวจพบการปฏิบัติงานที่ไม่สอดคล้องกับนโยบาย มาตรฐาน และขั้นตอนปฏิบัติซึ่งยังไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ ผู้บังคับบัญชาต้องชี้แจงให้บุคลากรใต้บังคับบัญชารับทราบและทำความเข้าใจ แต่หากความไม่สอดคล้องที่พบส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯผู้บังคับบัญชาต้องดำเนินการลงโทษทางวินัยตามกฎระเบียบที่บริษัทฯกำหนดไว้

2.3) แผนกเทคโนโลยีและสารสนเทศต้องให้การสนับสนุนด้านการให้คำแนะนำในการใช้งานหรือการปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนปฏิบัติ และข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศต่อหน่วยงานอื่นเมื่อได้รับคำร้องขอ

3) การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

3.1) ต้องจัดให้มีการทบทวนระบบสารสนเทศในด้านเทคนิค อย่างสม่ำเสมอตามความเหมาะสมและความเสี่ยง เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

3.2) ผู้ดูแลระบบ ต้องจัดให้มีการทดสอบระดับมาตรฐานความมั่นคงปลอดภัยของระบบสารสนเทศอย่าง อย่างสม่ำเสมอตามความเหมาะสมและความเสี่ยง เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

.....