Kumwell

บริษัท คัมเวล คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทย่อย

KUMWELL CORPORATION PUBLIC COMPANY LIMITED and SUBSIDIARY

นโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

(Information and Communication Technology Security Management and Governance Policy)

หมายเลขเอกสาร (Document No.) : ICT Policy_01

แก้ไขครั้งที่ (Revision No.) : 02

วันที่อนุมัติใช้ (Effective date) : 14-08-2568

จำนวนหน้าทั้งหมด (Page No.) : 57 หน้า (รวมปก)

การดำเนินการ	ลงนาม / ตำแหน่ง	วันที่ดำเนินการ
เสนอโดย	แผนกสารสนเทศและเทคโนโลยีสื่อสาร	14-08-2568
ตรวจทานโดย	ประธานเจ้าหน้าที่สายงานธุรการ	14-08-2568
เห็นชอบโดย	ประธานเจ้าหน้าที่บริหาร / คณะกรรมการบริหาร	14-08-2568
อนุมัติโดย	คณะกรรมการบริษัท	14-08-2568

บันทึกการเปลี่ยนแปลง

Version No.	หน้าที่แก้ไข	วันที่อนุมัติใช้	รายละเอียดการแก้ไข	โดย
00	-	03-07-2560	จัดทำใหม่	นายเกรียงศักดิ์ อำนวยโชค
01	-	10-08-2561	ทบทวนใหม่ทั้งเล่ม	นายเกรียงศักดิ์ อำนวยโชค
02	-	14-08-2568	แก้ไขรายละเอียด ทั้งเล่ม - รายหมวด และขั้นตอนการปฏิบัติ	นายเกรียงศักดิ์ อำนวยโชค

สารบัญ

หน้า

ส่วนที่ 1

บทนำ

บริษัท คัมเวล คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทในเครือ (ต่อไปนี้เรียกว่า “บริษัท”) ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยของ ข้อมูลระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในองค์กร ซึ่งเป็นปัจจัยสำคัญ ที่สนับสนุนการดำเนินธุรกิจขององค์กรให้มีประสิทธิภาพและประสิทธิผล พร้อมป้องกันความเสี่ยงจากภัยคุกคาม การรั่วไหลของข้อมูลสำคัญ รวมถึงผลกระทบที่อาจเกิดขึ้นต่อการดำเนินธุรกิจและภาพลักษณ์ของบริษัท การบริหารจัดการความมั่นคงปลอดภัยจึงถือเป็นปัจจัยสำคัญในการดำเนินงานอย่างต่อเนื่องและยั่งยืน

บริษัทได้กำหนดกรอบ นโยบายบริหารจัดการและกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ระดับองค์กรที่ดี โดยอ้างอิงจากหลักเกณฑ์ และแนวปฏิบัติในการจัดการข้อกฎหมายและมาตรฐานที่เกี่ยวข้อง ได้แก่:

- พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
- ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ
- มาตรฐาน ISO/IEC 27001 ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ

เพื่อให้ครอบคลุมถึงการปกป้องข้อมูลสำคัญจากการโจมตี การรั่วไหล หรือการเข้าถึง โดยไม่ได้รับอนุญาต รวมถึงการป้องกันการใช้งานระบบเทคโนโลยีสารสนเทศการและการสื่อสาร ในลักษณะที่ไม่เหมาะสม พร้อมทั้งกำหนดแนวทางในการตอบสนองต่อภัยคุกคามทางไซเบอร์ และบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับข้อมูลทางธุรกิจ ข้อมูลทางการเงิน และข้อมูลส่วนบุคคลของผู้มีส่วนได้ส่วนเสีย

1.1 วัตถุประสงค์

วัตถุประสงค์ของนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับนี้ มีดังต่อไปนี้

1. เพื่อกำหนดแนวทางและมาตรการในการบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีประสิทธิภาพ ปลอดภัย และสอดคล้องกับแนวทางของบริษัท

2. เพื่อป้องกันความเสียหายอันอาจเกิดจากภัยคุกคามทางไซเบอร์ การรั่วไหลของข้อมูล และการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต

3. เพื่อให้การดำเนินการด้านสารสนเทศของบริษัทสอดคล้องกับข้อกฎหมาย และข้อกำหนดที่เกี่ยวข้อง ได้แก่ ISO/IEC 27001 , พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA) , พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ , พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และประกาศที่ออกโดยสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

4. เพื่อส่งเสริมวัฒนธรรมมความมั่นคงปลอดภัยสารสนเทศภายในบริษัท และสร้างความตระหนักรู้แก่พนักงานทั่วทุกระดับ

5. เพื่อสนับสนุนความต่อเนื่องทางธุรกิจ และการฟื้นฟูระบบเมื่อเกิดเหตุการ์ผิดปกติ

6. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในบริษัทได้รับทราบ และเจ้าหน้าที่ทุกคนในบริษัทต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.2 บทบังคับใช้และบทลงโทษ

นโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับนี้ ให้มีผลบังคับใช้นับจากวันที่ประกาศ และให้มีผลบังคับใช้ต่อผู้ใช้งานระบบสารสนเทศ ของบริษัทและบริษัทในเครือทั้งหมด โดยไม่มีข้อยกเว้น หากพนักงานผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายบริหารจัดการและกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร บริษัทจะพิจารณาบทลงโทษทางวินัยและดำเนินการทางกฎหมาย ทันทีตามกรณีเหตุแห่งความเสียหายที่เกิดขึ้นจริง

1.3 การเผยแพร่นโยบาย

บริษัทจะดำเนินการเผยแพร่ และอบรมนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้พนักงานทุกระดับตั้งแต่ กรรมการ ประธานเจ้าหน้าที่ ผู้บริหาร พนักงาน และผู้เกี่ยวข้องทุกระดับ ผ่านช่องทางที่เหมาะสม ระบบอินทราเน็ต การอบรมภายใน เอกสารประกอบการปฏิบัติงาน หรือประกาศภายในบริษัท ทั้งนี้ เพื่อให้ผู้ปฏิบัติงานสามารถเข้าใจบทบาทความรับผิดชอบ และแนวทางปฏิบัติที่ถูกต้องตามนโยบายดังกล่าว

1.4 การทบทวนนโยบาย

นโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับนี้ ต้องได้รับการทบทวน ปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ 2 ครั้ง หรือมีการเปลี่ยนแปลงที่มีนัยสำคัญของสภาพแวดล้อมต่าง ๆ เช่น สภาพธุรกิจ กฎเกณฑ์ กฎหมายและเทคโนโลยี เป็นต้น โดยถือเป็นหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ในการทบทวน และปรับปรุง โดยมีประธานเจ้าหน้าที่สายงานธุรการเป็นผู้ควบคุมดูแลให้เกิดการทบทวนและปรับปรุงตามที่กำหนดไว้

ส่วนที่ 2

บทบาทหน้าที่และความรับผิดชอบ

2.1 คณะกรรมการบริษัท

- อนุมัตินโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงการเปลี่ยนแปลงที่อาจเกิดขึ้น
- อนุมัติระเบียบปฏิบัติ รวมถึงการเปลี่ยนแปลงที่อาจเกิดขึ้น
- รับทราบรายงานความเสี่ยงและเหตุการณ์สำคัญที่อาจกระทบต่อการดำเนินธุรกิจ
- สนับสนุนให้มีการปฏิบัติตามกฎหมายและการของหน่วงงานกำกับดูแล เช่น ประกาศที่ออกโดยสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

2.2 ผู้บริหารระดับสูง (Executive Management (CEO / CFO / CPO / CIO / CAO))

- กำหนดเป้าหมายด้านเทคโนโลยีสารสนเทศ และสื่อสารความมั่นคงปลอดภัยให้สอดคล้องกับแผนธุรกิจ
- สนับสนุนทรัพยากร บุคลากร และงบประมาณที่จำเป็น
- กำกับให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเป็นแบบแผนและมีการนำขบวนการวิเคราะห์ผลกระทบธุรกิจมาใช้
- ต้องนำเสนอนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงรายงานการเปลี่ยนแปลงนโยบายที่เกิดขึ้นต่อคณะกรรมการบริษัท
- ต้องสื่อสาร และผลักดันให้ทุกฝ่ายในองค์กรตระหนักและปฏิบัติตามนโยบาย
- ต้องทบทวน และอนุมัติความต้องการที่จำเป็นในการให้บริการ และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จะต้องใช้กับข้อมูลสารสนเทศที่อ่อนไหวหรือสำคัญต่อการปฏิบัติงานในเชิงธุรกิจ
- ต้องทบทวนและอนุมัติการดำเนินกิจกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารในระดับหน่วยงานซึ่งอาจมีผลกระทบในระดับองค์กรได้

2.3 เจ้าของทรัพย์สิน/ เจ้าของข้อมูล

- กำหนดลำดับขั้นความลับของข้อมูลตามความสำคัญของข้อมูลต่อองค์กร พร้อมทั้งแจ้งให้ผู้เกี่ยวข้องรับทราบในการเปลี่ยนแปลงลำดับชั้นความลับข้อมูลที่เกิดขึ้น
- พัฒนาและปรับปรุงโครงสร้างการแบ่งลำดับชั้นความลับข้อมูล และข้อกำหนดในการบริหารจัดการตามลำดับชั้นความลับ
- รับผิดชอบและในการอนุญาต / จำกัดสิทธิ์ในการเข้าถึงหรือใช้ข้อมูล

- ต้องตรวจสอบให้แน่ใจว่าข้อมูลที่อยู่ภายใต้ความรับผิดชอบได้รับการปกป้องจากภัยคุกคามอย่างเหมาะสม

- ต้องประสานกับฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ในกรณีเกิดการละเมิดข้อมูล

- ต้องร่วมประเมินความเสี่ยง และหาแนวทางการควบคุมที่เป็นมาตรฐาน ในกรณีที่มีความจำเป็นทางธุรกิจไม่สอดคล้องกับนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงระเบียบปฏิบัติ หรือมาตรฐานความมั่นคงปลอดภัยสารสนเทศ และการสื่อสาร เพื่อควบคุมให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ หรือเพื่อไม่ให้ความเสี่ยงอยู่ในระดับที่สูงขึ้น

2.4 ผู้ดูแลระบบ

- พัฒนาและจัดทำเอกสารกระบวนการสนับสนุน แนวทาง และขั้นตอนการปฏิบัติงานเพื่อให้มั่นใจว่าสอดคล้องตามนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

- ควบคุมดูแลระบบสารสนเทศและการสื่อสารให้คงสภาพการรักษาความลับ ความสมบูรณ์ครบถ้วน และความพร้อมใช้ของทรัพย์สินที่ให้บริการระบบสารสนเทศซึ่งอยู่ภายใต้การดูแล และการควบคุมการเข้าถึงทรัพย์สิน เพื่อเป็นการปกป้องทรัพย์สินอย่างเหมาะสม

- กำหนดกลไกการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยตรวจสอบการเข้าถึงระบบสารสนเทศอย่างสม่ำเสมอ เพื่อป้องกันการบุกรุกสารสนเทศอย่างทันท่วงที

- ให้ความช่วยเหลือในการคัดเลือก และประเมินด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ในส่วนที่เกี่ยวข้องกับฮาร์ดแวร์ และหรือซอฟต์แวร์ที่นำมาใช้ในองค์กร

- ตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยช่วยเหลือในการสอบสวน รวมถึงแก้ไขปัญหาในส่วนที่ทราบ หรือสงสัยว่าทรัพย์สินถูกคุกคาม หรือเหตุการณ์ที่ต้องสงสัยว่ามีการโจมตีระบบรักษาความมั่นคงปลอดภัยสารสนเทศ หรือเป็นการกระทำที่ไม่เหมาะสม และแจ้งผลลัพธ์ให้เจ้าของทรัพย์สินและผู้ที่เกี่ยวข้องรับทราบ

- รับผิดชอบและบำรุงรักษาระบบคอมพิวเตอร์ เซิร์ฟเวอร์ ระบบเครือข่าย หรือฐานข้อมูลให้พร้อมใช้งานและปลอดภัย

- ดำเนินการตามนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงมาตรการความปลอดภัยที่ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้บริหารกำหนด

2.5 ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร

- พัฒนาและปรับปรุงนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นปัจจุบัน และสอดคล้องต่อการดำเนินงานธุรกิจรวมถึงกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

- พัฒนาและปรับปรุงระเบียบปฏิบัติ หรือขั้นตอนการปฏิบัติงานที่มีความสอดคล้องกับนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

- นำเสนอการปรับปรุงนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงระเบียบปฏิบัติต่อประธานเจ้าหน้าที่สายงานธุรการเพื่อพิจารณาเห็นชอบและนำเสนอขออนุมัติต่อไป

- เผยแพร่ให้พนักงานทราบถึงนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของบริษัทและระเบียบปฏิบัติที่เกี่ยวข้อง

- บริหารจัดการโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ระบบสำรองข้อมูล รวมถึงการกู้คืนเมื่อเกิดเหตุฉุกเฉิน

- กำหนดและควบคุมมาตรการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามนโยบายและมาตรฐาน ISO/IEC 27001

- ให้บริการสนับสนุนผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงส่งเสริมการใช้งานอย่างปลอดภัย และถูกต้อง

- ต้องปฏิบัติตามข้อกำหนดของกฎหมายและหน่วยงานกำกับดูแล เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA) , พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ , พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และประกาศที่ออกโดยสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

- ต้องสนับสนุนการควบคุมสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ดูแลทะเบียนทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสารให้ครบถ้วนและตรวจสอบได้

- ต้องจัดเตรียมแนวทางการติดตามการบังคับใช้นโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงระเบียบปฏิบัติ เพื่อให้มั่นใจว่าผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทุกคนมีความตระหนักถึงนนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร กฎหมายลิขสิทธิ์ทางปัญญาและบทบัญญัติอื่น ๆ ที่บังคับใช้อยู่ปัจจุบัน

2.6 คณะกรรมการตรวจสอบ (Audit Committee)

- ตรวจสอบความเพียงพอของการควบคุมภายในระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- รับทราบรายงานการตรวจสอบ (Audit Report) ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงความปลอดภัยของข้อมูล

- ต้องแนะนำการปรับปรุงหรือมาตรการเพิ่มเติมหากพบข้อบกพร่องหรือความเสี่ยงที่อาจจะเกิดขึ้น

2.7 **พนักงานและผู้ใช้งานระบบ**

- ปฏิบัติตามนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร มาตรการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของบริษัทอย่างเคร่งครัดรวมถึงข้อบังคับทางกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA) และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ต้องใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงทรัพยากรฯ ของบริษัทเพื่อวัตถุประสงค์ในการทำงานเท่านั้น ห้ามนำไปใช้ในทางส่วนตัว หรือ กิจกรรมที่อาจสร้างความเสียหายให้บริษัท

- ต้องรักษาความลับของข้อมูล และบัญชีผู้ใช้งาน ห้ามเปิดเผยชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลเข้าระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้บุคคลอื่นไม่ว่าในกรณีใด ๆ

- หลีกเลี่ยงการเปิดไฟล์แนบ หรือคลิกลิงก์จากแหล่งที่ไม่น่าเชื่อถือ เพื่อป้องกันมัลแวร์ และภัยคุกคามทางไซเบอร์

- แจ้งฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารทันทีเมื่อพบเหตุผิดปกติ เช่น การเข้าใช้งานที่ไม่ได้รับอนุญาต อีเมลต้องสงสัย หรือเหตุการณ์ที่อาจก่อให้เกิดการรั่วไหลของข้อมูล

- ห้ามกระทำการใด ๆ ที่อาจละเมิดสิทธิของบุคคลภายนอก หรือก่อให้เกิดความเสียหายทางชื่อเสียงต่อบริษัทผ่านช่องทาง ระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- ต้องลงนามยินยอม และปฏิบัติตามข้อตกลงไม่เปิดเผยความลับองค์กร (NDA)

- ต้องใช้ทรัพย์สินขององค์กรอย่างมีประสิทธิภาพ มีจริยธรรม และถูกต้องตามกฎหมาย

2.8 **หน่วยงานภายนอก**

- ต้องปฏิบัติตามนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท รวมถึงข้อตกลงที่ระบุไว้ในสัญญาหรือเอกสารที่บริษัทกำหนด

- ต้องใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเข้าถึงข้อมูลของบริษัทตามขอบเขตหน้าที่และสิทธิ์ที่ได้รับอนุญาตเท่านั้น

- ห้ามเปิดเผยหรือเผยแพร่ข้อมูลหรือทรัพย์สินทางปัญญาของบริษัทแก่บุคคลภายนอก เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษร

- ต้องแจ้งบริษัททันทีเมื่อเกิดเหตุการณ์ผิดปกติ เช่น การรั่วไหลของข้อมูล การถูกเจาะระบบหรือการเข้าถึงโดยไม่ได้รับอนุญาต

- ต้องยินยอมให้บริษัทตรวจสอบ หรือประเมินความปลอดภัยในการให้บริการตามที่บริษัทเห็นสมควร

- ต้องจัดการข้อมูลทั้งหมดตามหลักการความมั่นคงปลอดภัย และดำเนินการลบหรือส่งคืนข้อมูลหลังสิ้นสุดสัญญาตามข้อกำหนดของบริษัท

- ลงนาม และปฏิบัติตามข้อตกลงไม่เปิดเผยความลับขององค์กร

ส่วนที่ 3

ความหมายและคำจำกัดความ

คำ	คำจำกัดความ
หน่วยงาน	
บริษัท	บริษัท คัมเวล คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทในเครือ
บริษัทในเครือ	บริษัท คัมเวล คอร์ปอเรชั่น จำกัด (มหาชน) มีอำนาจควบคุมได้
หน่วยงาน	ฝ่าย / แผนกที่ตามโครงสร้างของ บริษัท คัมเวล คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทในเครือ
บุคคล	
คณะกรรมการบริษัท	ผู้ที่มีอำนาจในการตัดสินใจสูงสุด มีหน้าที่ในการบริหารงานต่าง ๆ ของบริษัท คัมเวล คอร์ปอเรชั่น จำกัด (มหาชน) ตั้งแต่ 1 คนขึ้นไป
ประธานเจ้าหน้าที่บริหาร	ผู้ที่มีอำนาจในการตัดสินใจสูงสุด มีหน้าที่ในการบริหารงานต่าง ๆ ของบริษัท คัมเวล คอร์ปอเรชั่น จำกัด (มหาชน)
ประธานเจ้าหน้าที่สายงานธุรการ	ผู้ที่ได้รับหมอบหมายให้กำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ผู้ดูแลระบบ	เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรม หรือเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์ รวมไปถึงการแก้ไขปัญหาการใช้งานระบบสารสนเทศในด้านต่าง ๆ ซึ่งสามารถเข้าถึงโปรแกรม หรือเครือข่ายคอมพิวเตอร์เพื่อการจัดการต่าง ๆ ได้
ผู้พัฒนาระบบ	ผู้ซึ่งได้รับหมอบหมายให้รับผิดชอบในการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร
ผู้ใช้งาน (User)	เจ้าหน้าที่บริษัท ผู้บริหาร เจ้าหน้าที่สารสนเทศ หรือเจ้าหน้าที่จากหน่วยงานภายนอกที่ได้รับอนุญาต ในการเข้าถึงข้อมูล และ/หรือ ระบบเครือข่าย และคอมพิวเตอร์ของบริษัท
หน่วยงานภายนอก	องค์กร หรือหน่วยงานภายนอก ที่บริษัทอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของบริษัท โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

คำ	คำจำกัดความ
เจ้าของทรัพย์สิน / เจ้าของข้อมูล	ผู้ได้รับมอบอำนาจจากผู้บริหารให้รับผิดชอบข้อมูลของระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
คำอื่น ๆ	
หน่วยงาน	ฝ่าย / แผนกที่ตามโครงสร้างของ บริษัท คัมเวล คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทในเครือ
บุคคล	
การรักษาความมั่นคงปลอดภัย	การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ข้อมูลสารสนเทศ (Information)	ข้อมูลในรูปแบบใด ๆ ที่สามารถบันทึก จัดเก็บ หรือสื่อสารผ่านระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยเฉพาะข้อมูลที่มีความสำคัญต่อการดำเนินธุรกิจ
ข้อมูลอิเล็กทรอนิกส์	ข้อความที่สร้าง ส่ง รับ เก็บรักษาหรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ เป็นต้น
ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
วิธีการปฏิบัติ (Procedure)	รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
แนวปฏิบัติ (Guideline)	แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
สิทธิของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
สินทรัพย์	ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เซิร์ฟเวอร์ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบเครือข่าย อุปกรณ์เครือข่าย เลขที่อยู่ไอพี โดเมนเนม รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อหน่วยงาน

คำ	คำจำกัดความ
เจ้าของทรัพย์สิน / เจ้าของข้อมูล	ผู้ได้รับมอบอำนาจจากผู้บริหารให้รับผิดชอบข้อมูลของระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
คำอื่น ๆ	
หน่วยงาน	ฝ่าย / แผนกที่ตามโครงสร้างของ บริษัท คัมเวล คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทในเครือ
บุคคล	
การรักษาความมั่นคงปลอดภัย	การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ข้อมูลสารสนเทศ (Information)	ข้อมูลในรูปแบบใด ๆ ที่สามารถบันทึก จัดเก็บ หรือสื่อสารผ่านระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยเฉพาะข้อมูลที่มีความสำคัญต่อการดำเนินธุรกิจ
ข้อมูลอิเล็กทรอนิกส์	ข้อความที่สร้าง ส่ง รับ เก็บรักษาหรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ เป็นต้น
ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
วิธีการปฏิบัติ (Procedure)	รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
แนวปฏิบัติ (Guideline)	แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
สิทธิของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
สินทรัพย์	ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ได้แก่ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เซิร์ฟเวอร์ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบเครือข่าย อุปกรณ์เครือข่าย เลขที่อยู่ไอพี โดเมนเนม รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อหน่วยงาน

คำ	คำจำกัดความ
ห้องควบคุมระบบ	ห้องที่ติดตั้ง และจัดวางระบบเซิร์ฟเวอร์ อุปกรณ์เชื่อต่อ และอุปกรณ์เครือข่ายของบริษัท
ระบบสารสนเทศ	ระบบงานของบริษัทที่นำเอาเทคโนโลยีสารสนเทศและการสื่อสาร ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างเทคโนโลยีสารสนเทศและการสื่อสาร ที่บริษัทสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหารการสนับสนุนให้การบริการการพัฒนาและควบคุม การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ ฯลฯ
ระบบเครือข่ายคอมพิวเตอร์	ระบบที่เชื่อมต่อคอมพิวเตอร์ เซิร์ฟเวอร์ อุปกรณ์เครือข่ายต่าง ๆ ของบริษัท
บัญชีผู้ใช้ (User Name /Account)	กลุ่มของข้อมูลที่ใช้ในการอ้างถึงเพื่อระบุตัวตน สิทธิ์การเข้าถึงและข้อจำกัดต่าง ๆ ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
รหัสผ่าน (Password)	ตัวอักษร หรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศและการสื่อสาร
การเข้าถึงหรือควบคุมการใช้งานสรสนเทศ	การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน และหน่วยงานภายนอก เข้าถึงหรือใช้งานระบบสารสนเทศ อุปกรณ์ประมวลผลสารสนเทศและระบบเครือข่าย ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ
ความมั่นคงปลอดภัยด้านสารสนเทศ	การรักษาไว้ซึ่งความลับ (confidentiality) ความครบถ้วนถูกต้อง (integrity) และความพร้อมใช้ (availability) ของเทคโนโลยีสารสนเทศและการสื่อสารระบบเครือข่าย รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)
เหตุการณ์ด้านความปลอดภัย	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่งคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

คำ	คำจำกัดความ
การพิสูจน์ยืนยันตัวตน (authentication)	ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ยืนยันตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ และรหัสผ่าน
แผนผังระบบเครือข่าย (network diagram)	แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของบริษัท

ส่วนที่ 4

นโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

หมวดที่ 1 นโยบายความมั่นคงปลอดภัยขององค์กร (Security Policy)

1.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์

เพื่อสร้างความตระหนักรู้แก่ผู้ใช้งานและบุคลากรที่เกี่ยวข้องเกี่ยวกับความสำคัญของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงกำหนดหน้าที่ ความรับผิดชอบและแนวทางปฏิบัติในการควบคุมความเสี่ยงอย่างเหมาะสม โดยบริษัทจะจัดให้มีนโยบายบริหารจัดการและกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามแนวทางดังนี้

1.1.1 การบริหารจัดการนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Security Management and Governance Policy)

- บริษัทจัดทำนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร เป็นลายลักษณ์อักษรเพื่อเสริมสร้างความเชื่อมั่นและความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบเครือข่ายของบริษัท โดยนโยบายฯ ต้องได้รับการอนุมัติคณะกรรมการบริษัทเพื่อนำไปใช้

- บริษัทจัดให้มีการเผยแพร่นโยบายฯ ดังกล่าวให้บุคลากรทุกระดับ หน่วยงานภายนอกและผู้ที่เกี่ยวข้องในขอบเขตรับทราบ และปฏิบัติตามอย่างเคร่งครัด

1.1.2 การทบทวนการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Review of the Information Security Policy)

- บริษัทดำเนินการตรวจสอบ ทบทวน และประเมินนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย 2 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

หมวดที่ 2 โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Organization of information Security)

2.1 โครงสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ภายในองค์กร (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม กำกับ และติดตามการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ในหน่วยงานภายในองค์กรอย่างมีประสิทธิภาพ

2.1.1 การกำหนดบทบาทและหน้าที่ด้านการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

- ประธานเจ้าหน้าที่บริหารต้องแต่งตั้งบุคลากร หรือคณะทำงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร พร้อมกำหนดหน้าที่ และความรับผิดชอบอย่างชัดเจน เพื่อให้สามารถกำกับดูแลและดำเนินงานให้เป็นไปตามนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของบริษัทได้อย่างต่อเนื่อง

2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

- กำหนดให้การแบ่งแยกหน้าที่การปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารย่างชัดเจน เพื่อลดความเสี่ยงจากการทุจริตหรือข้อผิดพลาด โดยต้องมีการสอบทานและควบคุมภายในระหว่างกัน

2.1.3 การประสานงานกับหน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Contact with authorities)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องจัดทำและปรับปรุงรายการช่องทางติดต่อกับหน่วยงานภาครัฐ หน่วยงานด้านความมั่นคงไซเบอร์ (เช่น ETDA , NCSA , ปอท.) รวมถึงผู้เชี่ยวชาญที่สามารถประสานงานหรือให้การสนับสนุนเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

2.1.4 ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ

- ต้องบูรณาการการควบคุมความมั่นคงปลอดภัยไว้ในกระบวนการพัฒนา และบริหารจัดการโครงการทั้งหมด ทั้งโครงการภายใน ภายนอก และโครงการจัดซื้อจัดจ้าง โดยครอบคลุมถึงการประเมินความเสี่ยง การควบคุมภายใน และการติดตามผล

2.2 การควบคุมคอมพิวเตอร์แบบพกพา และการปฏิบัติงานภายนอกองค์กร (Mobile devices and Teleworking)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร จากการใช้งานอุปกรณ์พกพา และการทำงานนอกสถานที่หรือผ่านระบบระยะไกล

2.2.1 การใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

- อุปกรณ์คอมพิวเตอร์แบบพกพา หมายถึง อุปกรณ์ที่สามารถนำออกนอกสถานที่ได้ และมีความสามารถในการจัดเก็บข้อมูล หรือเชื่อมต่อกับเครือข่ายของบริษัท เช่น โน๊ตบุ๊ค (Laptop) , แท็บเล็ต , สมาร์ตโฟน , External Hard Drive , USB Drive และอุปกรณ์พกพาอื่น ๆ

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดมาตรการในการป้องกันข้อมูล และสินทรัพย์เทคโนโลยีสารสนเทศและการสื่อสารที่จัดเก็บ หรือใช้งานผ่านอุปกรณ์เหล่านี้ โดยพิจารณาจากความเสี่ยงที่อุปกรณ์จะถูกเชื่อมต่อกับระบบเครือข่ายของบริษัท หรือถูกนำออกไปใช้งานภายนอก

- พนักงานที่นำอุปกรณ์ดังกล่าวมาเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ต้องปฏิบัติตามนโยบายฯ ของบริษัท และมีหน้าที่ในการดูแลรักษาอุปกรณ์ไม่ให้ตกอยู่ในความเสี่ยง เช่น การตั้งรหัสผ่าน การเข้ารหัสข้อมูล และการไม่เปิดเผยข้อมูลสำคัญในพื้นที่สาธารณะ

- การใช้อุปกรณ์แบบพกพาที่ไม่ใช่ของบริษัทต้องได้รับการอนุมัติจากฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ก่อนใช้งานและต้องเป็นไปตามข้อกำหนดด้านความปลอดภัยที่บริษัทกำหนด

2.2.2 การปฏิบัติงานภายนอกหน่วยงาน (Teleworking)

- พนักงานที่ปฏิบัติงานจากภายนอกบริษัท ต้องปฏิบัติตามนโยบายฯ เช่นเดียวกับผู้ปฏิบัติงานภายใน

- พนักงานที่เข้าถึงข้อมูล หรือระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทจากระยะไกล (Remote Access) ต้องได้รับอนุมัติจากเจ้าของข้อมูลและเจ้าของระบบ

- การเข้าใช้งานจากระยะไกลต้องมีการควบคุมด้วยมาตรการรักษาความปลอดภัยที่เหมาะสม เช่น VPN , MFA , และระบบบันทึกการเข้าใช้งาน (Log)

2.3 ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารกับหน่วยงานภายนอก (Information Security and Third Parties)

วัตถุประสงค์

เพื่อกำหนดแนวทางควบคุม และติดตามการเข้าถึงหรือการจัดการข้อมูลของบริษัท โดยบุคคลภายนอก เช่น ผู้ให้บริการภายนอก (Outsource) , Vendor , คู่สัญญา หรือพนักงานชั่วคราว

- บริษัทมีการทำข้อตกลงด้านการรักษาความลับ (NDA) และข้อกำหนดด้านความมั่นคงปลอดภัยกับบุคคลภายนอกที่เข้าถึงระบบหรือข้อมูล

- การอนุญาตให้หน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ภายในของบริษัท ต้องได้รับอนุมัติจากเจ้าของข้อมูลหรือผู้รับผิดชอบหลักของระบบ

- การควบคุมการเข้าถึง (Access Control) , ตรวจสอบประวัติการใช้งาน และกำหนดระยะเวลาการเข้าถึงของหน่วยงานภายนอกอย่างชัดเจน

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องจัดเก็บและทบทวนรายชื่อบุคคล / บริษัทภายนอกที่เกี่ยวข้อง พร้อมตรวจสอบให้มั่นใจว่ามีการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยตามนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

หมวดที่ 3 ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม กำกับ และติดตามการจัดการด้านทรัพยากรบุคคล ทั้งในช่วงก่อน ระหว่างและหลังการจ้างงาน เพื่อให้มั่นใจว่าบุคลากรทุกระดับตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยปฏิบัติตามข้อกำหนดขององค์กรอย่างถูกต้อง

3.1 การบริหารจัดการก่อนเริ่มจ้างงาน (Prior to Employment)

3.1.1 การตรวจสอบคุณสมบัติและความเหมาะสมของผู้สมัคร

- ดำเนินการตรวจสอบคุณสมบัติพื้นฐาน ความน่าเชื่อถือ และประวัติการทำงานของผู้สมัคร โดยเฉพาะตำแหน่งที่เกี่ยวข้องกับการเข้าถึงข้อมูลสำคัญ หรือระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- อาจรวมถึงการตรวจสอบอ้างอิงจากที่ทำงานเดิม และการตรวจสอบประวัติอาชญากรรมตามความเหมาะสม

3.1.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)

- ต้องระบุบทบาท หน้าที่ และความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนในสัญญาการจ้าง

- พนักงานและหน่วยงานภายนอกต้องลงนามในข้อตกลงไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) ซึ่งมีผลทั้งในระหว่างและอย่างน้อย 5 ปีหลังจากพ้นสภาพการจ้าง

3.1.3 การแจ้งข้อมูลการจ้างงาน (Employment Notification Process)

- ฝ่ายทรัพยากรบุคคลต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารทันทีในกรณี ต่อไปนี้

  - การเริ่มจ้าง / ลาออก / สิ้นสุดสภาพการจ้าง

  - การโยกย้าย / ปรับเปลี่ยนตำแหน่ง

  - การพักงาน หรือระงับสิทธิ์ในการเข้าถึงระบบ

3.2 การบริหารจัดการระหว่างการจ้างงาน (During employment)

3.2.1 หน้าที่ในการควบคุมและกำกับบุคลากร (Management Responsibilities)

- ผู้บริหารทุกระดับต้องควบคุม กำกับ และตรวจสอบให้บุคลากรภายในและภายนอกปฏิบัติตามนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

3.2.2 การอบรมและการสร้างความตระหนักรู้ (Information Security Awareness, Education and Training)

- พนักงานต้องได้รับการอบรมเกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารก่อนเริ่มงาน และต่อเนื่องอย่างน้อยปีละ 1 ครั้ง

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องจัดทำหลักสูตรให้เหมาะสมกับบทบาทหน้าที่ พร้อมมีการประเมินผลและบันทึกการเข้าอบรม

3.2.3 กระบวนการทางวินัย (Disciplinary Process)

- บริษัทจัดให้มีกระบวนการพิจารณาทางวินัย กรณีมีการฝ่าฝืน นโยบาย หรือกระทำการที่ส่งผลกระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

3.3 การบริหารจัดการเมื่อพ้นสภาพการจ้างงานหรือเปลี่ยนแปลงหน้าที่ (Termination or Change of Employment)

3.3.1 การจัดการสิทธิและทรัพย์สินเมื่อสิ้นสุดการจ้างงาน

- ต้องดำเนินการยกเลิกสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารทันทีเมื่อพนักงานพ้นสภาพการจ้าง

- ดำเนินการเรียกคืนอุปกรณ์ของบริษัท เช่น คอมพิวเตอร์ โทรศัพท์ USB รวมถึงให้ลบข้อมูลขององค์กรออกจากอุปกรณ์ส่วนตัว (ถ้ามี)

- ลงนามรับทราบการสิ้นสุดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร และรับทราบการคงไว้ซึ่ง NDA หลังสิ้นสุดการจ้างงาน

หมวดที่ 4 การบริหารจัดการสินทรัพย์ (Asset Management)

วัตถุประสงค์

เพื่อให้ทรัพย์สินและระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทได้รับการระบุ จัดหมวดหมู่ และได้รับการปกป้องในระดับที่เหมาะสม โดยมีมาตรการควบคุมการใช้งาน การเข้าถึง และการดูแลรักษา เพื่อลดความเสี่ยงจากการรั่วไหลของข้อมูล การใช้งานที่ผิดวัตถุประสงค์ หรือการสูญเสียข้อมูลที่อาจส่งผลกระทบต่อบริษัท

4.1 หน้าที่ความรับผิดชอบต่อสินทรัพย์ (Responsibility for Assets)

4.1.1 การจัดทำบัญชีสินทรัพย์ (Inventory of assets)

- บริษัทต้องจัดทำ ทะเบียนทรัพย์เทคโนโลยีสารสนเทศและการสื่อสาร (Asset Register) ซึ่งครอบคลุมทรัพย์สินทุกประเภท ได้แก่

- ทรัพย์สินทางกายภาพ (Physical Assets) : คอมพิวเตอร์ , เซิร์ฟเวอร์ , อุปกรณ์เครือข่าย

- ทรัพย์สินเชิงตรรกะ (Logical Assets) : ซอฟต์แวร์ , สิทธิการใช้งานระบบ , บัญชีผู้ใช้

- ข้อมูลสารสนเทศ (Information Assets) : ฐานข้อมูล , เอกสาร , รายงานภายใน

- ข้อมูลในทะเบียนต้องประกอบด้วยรายละเอียดอย่างน้อย ได้แก่ : ชื่อสินทรัพย์ , หมายเลขประจำตัว , ผู้รับผิดชอบ , ตำแหน่งการใช้งาน , ปริมาณ , สถานะการใช้งาน และระดับความสำคัญ

- ต้องมีการตรวจสอบและอัพเดทรายการทรัพย์สินอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง และจัดทำรายงานผลการตรวจสอบ

4.1.2 การระบุผู้ถือครองทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร (Ownership of assets)

- กำหนดระบุ “เจ้าของทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร (Asset Owner)” สำหรับทรัพย์สินแต่ละรายการ โดยเจ้าของมีหน้าที่รับผิดชอบในการควบคุมการเข้าถึง การจัดการความเสี่ยง และการอนุมัติการใช้งาน

- เจ้าของทรัพย์สินต้องประสานกับผู้ดูแลระบบเพื่อกำหนดมาตรการความปลอดภัยที่เหมาะสม

4.1.3 การใช้งานทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร (Acceptable user of assets)

- กำหนดจัดทำ "ระเบียบการใช้งานทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร" ครอบคลุมการใช้งานฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย อีเมล และอินเทอร์เน็ต เพื่อให้การใช้งานเป็นไปตามวัตถุประสงค์และไม่ก่อให้เกิดความเสี่ยง

- พนักงานต้องได้รับการอบรมหรือชี้แจง และลงนามรับทราบก่อนเริ่มใช้งาน

- การเข้าถึงทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร ต้องอยู่ภายใต้หลัก "Need to Know" และ "Least Privilege"

4.1.4 การคืนทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร (Return of assets)

- เมื่อมีการย้ายตำแหน่ง , สิ้นสุดสัญญาจ้าง หรือออกจากงาน พนักงานต้องคืนทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร ที่ได้รับมอบหมายทั้งหมด เช่น คอมพิวเตอร์ , อุปกรณ์สื่อสาร , เอกสาร หรือข้อมูล

- หัวหน้างานต้องร่วมกับฝ่ายทรัพยากรบุคคล ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร และฝ่ายบัญชีและการเงินตรวจสอบรายการก่อนการออกจากงาน

- ต้องมีแบบฟอร์มการตรวจสอบ / รับคืนทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร โดยต้องจัดเก็บเป็นหลักฐาน

4.2 การจัดชั้นความลับของข้อมูลด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information classification)

4.2.1 การจัดลำดับชั้นความลับของข้อมูลด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Classification of information)

- บริษัทกำหนดระดับชั้นความลับของข้อมูลด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเป็นทางการ เช่น

  - ชั้นความลับสูงสุด (Confidential) - จำกัดการเข้าถึงเฉพาะผู้มีอำนาจ

  - ใช้ภายใน (Internal Use Only) - เฉพาะพนักงานในองค์กร

  - ข้อมูลสาธารณะ (Public) – สามารถเผยแพร่ได้โดยไม่จำกัด

- การจัดระดับต้องพิจารณาตามกฎหมาย กฎระเบียบ รวมประกาศที่เกี่ยวข้องอาศัยอำนาจตามนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับนี้ สำหรับการป้องกันความเสียหายที่อาจเกิดขึ้นจากการรั่วไหล

4.2.2 การบ่งชี้สารสนเทศ (Labeling of Information)

- จัดการติดป้ายหรือระบุระดับความลับของข้อมูลอย่างชัดเจนบนเอกสาร อีเมล และระบบจัดเก็บข้อมูล เช่น Confidential , Internal และ Availability

- มีแนวทางการใช้สัญลักษณ์หรือตัวบ่งชี้ และสื่อสารให้บุคลากรเข้าใจตรงกัน

4.2.3 การบริหารจัดการสินทรัพย์ (Handling of assets)

- มีขั้นตอนชัดเจนในการจัดเก็บ แจกจ่าย เคลื่อนย้าย ใช้งาน และทำลายทรัพย์สิน หรือข้อมูลตามระดับความลับ

- ดำเนินการสำรองข้อมูลด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ และเก็บไว้ในระบบที่มีความมั่นคงปลอดภัย เช่น Backup Server หรือ Cloud ที่เชื่อถือได้

- การกู้คืนข้อมูลต้องมีแผนและทดสอบการกู้คืนเป็นระยะ

4.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)

4.3.1 การบริหารจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (Management of removable media)

- กำหนดนโยบายการใช้สื่อเคลื่อนย้ายข้อมูล (เช่น USB , CD-ROM , External HDD) โดยเฉพาะเมื่อต้องใช้งานกับข้อมูลที่มีความลับ

- มีการเข้ารหัสข้อมูล (Encryption) ก่อนจัดเก็บในอุปกรณ์ และควบคุมการใช้งานผ่านการอนุญาตจากผู้มีอำนาจ

- มีเก็บบันทึกการใช้งาน (Usage Log) สำหรับการตรวจสอบย้อนหลัง

4.3.2 การทำลายสื่อบันทึกข้อมูล (Disposal of media)

- เมื่อสื่อบันทึกข้อมูลหมดอายุหรือไม่ใช้งาน ต้องดำเนินการลบหรือทำลายด้วยวิธีที่ปลอดภัย เช่น

  - การลบแบบปลอดภัย (Secure Erase)

  - การทำลายทางกายภาพ (Shredding)

- ต้องจัดทำแบบฟอร์ม หรือบันทึกการทำลาย (Media Disposal Record) เพื่อใช้เป็นหลักฐานและตรวจสอบย้อนหลังได้อย่างน้อย 2 ปี

หมวดที่ 5 การควบคุมการเข้าถึง (Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงข้อมูลขององค์กรให้เป็นไปตามหลักการ "Need to Know (จำเป็นต้องรู้)" และ "Least Privilege (สิทธิ์น้อยที่สุด)" โดยการให้สิทธิ์เฉพาะเท่าที่จำเป็นต่อการปฏิบัติงาน รวมถึงการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การละเมิดสิทธิ หรือการใช้งานที่อาจก่อให้เกิดความเสียหายต่อข้อมูล ระบบ หรือบริษัท

5.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business requirements of Access control)

5.1.1 นโยบายควบคุมการเข้าถึง (Access control policy)

- องค์กรต้องกำหนดนโยบายควบคุมการเข้าถึงเป็นลายลักษณ์อักษร พร้อมปรับปรุงอย่างสม่ำเสมอ

- นโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารนี้ ต้องกำหนดแนวทางการให้สิทธิ์ การควบคุมการเข้าใช้งานระบบ และการยืนยันตัวตน รวมถึงแนวปฏิบัติใน กรณีเกิดเหตุผิดปกติ

5.1.2 การควบคุมการเข้าถึงเครือข่าย และบริการเครือข่าย (Access to Networks and Network Service)

- ต้องมีขั้นตอนการอนุมัติการเข้าถึงเครือข่ายและบริการเครือข่ายโดยผู้มีอำนาจ

- การให้สิทธิ์ต้องสอดคล้องกับบทบาทหน้าที่

- ต้องมีการจัดทำบันทึกการเข้าถึง (Access Logs) และทบทวนอย่างสม่ำเสมอ

5.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

5.2.1 การลงทะเบียนและถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration)

- กำหนดกระบวนการลงทะเบียนผู้ใช้งานใหม่อย่างชัดเจน โดยรวมถึงการยืนยันตัวตน การระบุบทบาทหน้าที่ และการอนุมัติจากผู้มีอำนาจก่อนสร้างบัญชี

- การเพิกถอนบัญชีต้องดำเนินการทันทีเมื่อพนักงานลาออก เปลี่ยนบทบาท หรือพ้นสภาพ เพื่อป้องกันบัญชีหลงเหลือ

- บันทึกการสร้าง และเพิกถอนบัญชีต้องเก็บไว้เป็นหลักฐานเพื่อการตรวจสอบย้อนหลัง

5.2.2 การมอบหมาย และควบคุมสิทธิ์การเข้าถึง (User Access Provisioning and Control)

- การให้สิทธิ์เข้าถึงระบบหรือข้อมูลใด ๆ ต้องผ่านการร้องขอ และอนุมัติจากเจ้าของระบบ หรือเจ้าของข้อมูล

- สิทธิ์ต้องถูกกำหนดตามหลักการ Least Privilege (ให้สิทธิ์เท่าที่จำเป็น)

- ต้องจัดทำทะเบียนควบคุมบัญชีผู้ใช้และสิทธิ์ที่ได้รับ พร้อมทั้งทบทวนและอัพเดทอย่างสม่ำเสมอ

5.2.3 การจัดการบัญชีที่มีสิทธิพิเศษ (Privileged Access Management)

- บัญชีที่มีสิทธิพิเศษ เช่น Administrator , หรือบัญชีของผู้บริหารระบบ ต้องถูกควบคุมแยกต่างหากจากบัญชีทั่วไป

- ใช้ชื่อบัญชีเฉพาะบุคคล หลีกเลี่ยงการใช้บัญชีร่วมกัน (Shared Account) และหากจำเป็นต้องใช้ต้องมีมาตรการควบคุมเข้มงวด

- จัดทำบันทึกกิจกรรมการใช้งานบัญชีสิทธิพิเศษ และมีการตรวจสอบอย่างสม่ำเสมอโดยหน่วยงานตรวจสอบภายในหรือเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร

5.2.4 การควบคุม และจัดเก็บข้อมูลพิสูจน์ตัวตน (Authentication Credentials Management)

- ผู้ใช้ต้องได้รับข้อมูลพิสูจน์ตัวตน เช่น รหัสผ่าน , Token , Certificate โดยช่องทางที่ปลอดภัย

- กำหนดนโยบายรหัสผ่านที่ปลอดภัย เช่น ความยาวไม่ต่ำกว่า 8 ตัวอักษร มีตัวอักษรพิเศษ ตัวเลข ตัวใหญ่ และต้องเปลี่ยนรหัสอย่างน้อยทุก 90 วัน

- ห้ามบันทึกรหัสผ่านในที่ที่ไม่ปลอดภัย และห้ามเปิดเผยให้ผู้อื่นทราบ

- ควรส่งเสริมการใช้การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) โดยเฉพาะในบัญชีสิทธิพิเศษ หรือระบบสำคัญ

5.2.5 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

- กำหนดรอบการทบทวนสิทธิ์ของผู้ใช้ เช่น อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงบทบาท / โครงสร้างองค์กร

- การทบทวนต้องทำโดยเจ้าของข้อมูลหรือเจ้าของระบบ และต้องมีบันทึกการดำเนินการและผลการตรวจสอบ

- หากพบสิทธิ์ที่ไม่จำเป็นหรือสิทธิ์ซ้ำซ้อน ต้องดำเนินการถอนหรือปรับลดทันที

- การทบทวนสิทธิ์การเข้าถึง ต้องพิจารณาประเด็น ดังต่อไปนี้

1. รอบการทบทวนสิทธิ์ที่กำหนดไว้

2. การพ้นสภาพการเป็นบุคลากรขององค์กร

3. การเปลี่ยนแปลงโยกย้ายหน้าที่การปฏิบัติงาน

4. การขอใช้สิทธิ์นอกเหนือจากหน้าที่ความรับผิดชอบที่กำหนดไว้

- เมื่อดำเนินการทบทวนสิทธิ์เรียบร้อยแล้ว ให้เจ้าของข้อมูล หรือผู้ดูแลระบบจัดเก็บหลักฐานการทบทวนสิทธิ์ โดยให้แยกหลักฐานตามช่วงเวลาการทบทวนสิทธิ์

5.2.6 การควบคุมบัญชีผู้ใช้ภายนอก (Third-party and Temporary Access Control)

- กรณีที่มีผู้ใช้งานจากภายนอก เช่น ที่ปรึกษา ผู้รับจ้าง หรือผู้ให้บริการระบบ ต้องมีขั้นตอนการขออนุญาตการมอบสิทธิ์แบบชั่วคราว และการเพิกถอนสิทธิ์เมื่อเสร็จสิ้นงาน

- ต้องบันทึกระยะเวลา ช่วงเวลา และขอบเขตการเข้าถึงของผู้ใช้งานเหล่านี้ พร้อมทั้งมีการควบคุมการใช้งานระบบหรือข้อมูลที่สำคัญ

- ควรใช้ระบบ VPN หรือ Jump Server เพื่อควบคุมการเข้าถึงของบุคคลภายนอก

- ระบบต้องสามารถบันทึกกิจกรรมสำคัญของผู้ใช้ได้ เช่น การเข้าสู่ระบบ การเข้าถึงข้อมูลสำคัญ หรือการเปลี่ยนแปลงค่าการกำหนดค่า

- จัดให้มีการตรวจสอบบันทึกอย่างสม่ำเสมอ โดยอัตโนมัติหรือโดยเจ้าหน้าที่ที่ได้รับมอบหมาย

- ในกรณีที่พบพฤติกรรมผิดปกติ ต้องมีแนวทางการแจ้งเตือน และตอบสนองเหตุการณ์ตามที่กำหนดไว้ในนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

5.3.1 การใช้งานข้อมูลการพิสูจน์ตัวตน (Use of Secret Authentication Information)

- ผู้ใช้งานต้องรักษาข้อมูลพิสูจน์ตัวตน เช่น รหัสผ่าน , PIN , Token , หรืออุปกรณ์ยืนยันตัวตนอื่น ๆ ไว้เป็นความลับ และต้องไม่เปิดเผยแก่บุคคลอื่นโดยเด็ดขาด

- ห้ามจดหรือบันทึกรหัสผ่านไว้ในที่เปิดเผย หรือในรูปแบบที่เสี่ยงต่อการเข้าถึงโดยผู้อื่น เช่น ใต้แป้นพิมพ์ บนโพสต์อิท หรือในไฟล์ที่ไม่มีการเข้ารหัส

- ห้ามนำรหัสผ่านที่ใช้ในระบบอื่น หรือบัญชีส่วนตัว มาใช้ในระบบขององค์กร

- ต้องเปลี่ยนรหัสผ่านในกรณีที่สงสัยว่ามีการรั่วไหลหรือถูกบุกรุกทันที

5.3.2 ความรับผิดชอบต่อบัญชีผู้ใช้ (Accountability for User Accounts)

- พนักงานต้องรับผิดชอบต่อกิจกรรมทุกอย่างที่เกิดขึ้นภายใต้บัญชีของตน หากไม่มีหลักฐานที่แสดงชัดว่าเป็นการบุกรุกจากภายนอก

- ห้ามนำบัญชีของตนไปให้ผู้อื่นใช้งาน และห้ามใช้บัญชีของผู้อื่น ไม่ว่าด้วยเหตุผลใด ๆ

- พนักงานต้องออกจากระบบ (Log off) เมื่อเลิกใช้งาน และต้องล็อกหน้าจอ (Lock screen) ทุกครั้งเมื่อไม่อยู่หน้าจอคอมพิวเตอร์

5.3.3 การแจ้งเหตุผิดปกติ (Reporting of Anomalies or Incidents)

- พนักงานต้องแจ้งเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร หรือเจ้าหน้าที่ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทันทีหากพบ

- ความผิดปกติในการทำงานของระบบ

- ข้อสงสัยว่าข้อมูลพิสูจน์ตัวตนถูกละเมิด

- การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- ความพยายามหลอกลวงทางไซเบอร์ เช่น Phishing , Social Engineering

- พนักงานไม่ควรพยายามแก้ไข หรือปิดบังเหตุการณ์ด้วยตนเองหากไม่มีอำนาจ หรือความรู้เพียงพอ

5.3.4 การใช้งานระบบและข้อมูลตามหน้าที่ (Appropriate Use of Systems and Data)

- พนักงานต้องใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงข้อมูลภายในขอบเขตของบทบาทหน้าที่ตามที่ได้รับมอบหมาย

- ห้ามใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อวัตถุประสงค์ส่วนตัว ที่ไม่ได้รับอนุญาต หรือการกระทำที่ละเมิดกฎหมาย เช่น การเข้าถึงข้อมูลส่วนบุคคลโดยไม่มีสิทธิ์ การกระทำผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA) , พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ต้องเคารพลิขสิทธิ์ของซอฟต์แวร์ ไฟล์ และข้อมูล ห้ามติดตั้งหรือใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์ในเครื่องของบริษัท

5.3.5 การปฏิบัติตามนโยบายและแนวปฏิบัติ (Compliance)

- พนักงานต้องศึกษานโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร แนวปฏิบัติ และคู่มือที่บริษัทกำหนดไว้ และลงนามรับทราบการปฏิบัติตาม

- การละเมิดข้อกำหนดใด ๆ อาจนำไปสู่การดำเนินการทางวินัย และหากเกี่ยวข้องกับกฎหมาย บริษัทอาจดำเนินคดีตามกฎหมายที่เกี่ยวข้อง

5.4 การควบคุมการเข้าถึงแอพพลิเคชั่น เทคโนโลยีสารสนเทศและการสื่อสาร (Application and Information Access Control)

5.4.1 การจำกัดการเข้าถึงเทคโนโลยีสารสนเทศและการสื่อสาร (Information Access Restriction)

- เจ้าของข้อมูล และผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูล ระบบ และฟังก์ชันการใช้งานภายในแอปพลิเคชันให้เฉพาะผู้มีหน้าที่เกี่ยวข้องตามหลักการ “Need to Know”

- การกำหนดสิทธิ์ต้องผ่านการอนุมัติจากผู้มีอำนาจ และจัดเก็บเป็นหลักฐาน

5.4.2 ขั้นตอนการเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่ปลอดภัย (Secure Log-on Procedures)

- ระบบเทคโนโลยีสารสนเทศและการสื่อสารต้องมีขั้นตอนการเข้าสู่ระบบที่ปลอดภัย โดยใช้กลไกการยืนยันตัวตนขั้นต่ำ 2 ชั้น (Two-Factor Authentication) สำหรับระบบที่มีความเสี่ยงสูง

- ต้องมีการตั้งค่าการปิดการเชื่อมต่ออัตโนมัติ (Auto-logout) เมื่อไม่มีการใช้งานตามช่วงเวลาที่กำหนด

5.4.3 ระบบสำหรับบริหารจัดการรหัสผ่าน (Password Management System)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องจัดให้มีระบบ หรือกลไกสำหรับบริหารจัดการรหัสผ่าน เช่น Active Directory หรือระบบ SSO ซึ่งสามารถกำหนดนโยบายด้านรหัสผ่าน เช่น

- ความยาวขั้นต่ำ

- ความซับซ้อน

- อายุรหัสผ่าน (Password Expiry)

- การห้ามใช้รหัสผ่านซ้ำ

- ระบบต้องสามารถบังคับเปลี่ยนรหัสผ่านเมื่อผู้ใช้งานครั้งแรก หรือเมื่อมีเหตุสงสัยด้านความปลอดภัย

5.4.4 การควบคุมการใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

- โปรแกรมอรรถประโยชน์ที่สามารถเข้าถึงหรือแก้ไขค่าระบบได้ เช่น Command-line Tools , System Utility ต้องได้รับการควบคุมการใช้งานอย่างเข้มงวด

- การใช้โปรแกรมเหล่านี้ต้องได้รับการอนุมัติล่วงหน้า และควรมีการจัดทำ Log และ Audit Trail

- ไม่อนุญาตให้พนักงานทั่วไปเข้าถึงหรือดาวน์โหลดเครื่องมือประเภทนี้จากแหล่งที่ไม่ปลอดภัย

5.4.5 การจำกัดการเข้าถึงตามอุปกรณ์ และสถานที่ (Access Based on Device and Location)

- การเข้าถึงแอปพลิเคชัน และข้อมูลสำคัญอาจกำหนดให้เข้าถึงได้เฉพาะจากอุปกรณ์ที่ลงทะเบียนไว้หรือจากเครือข่ายภายในองค์กรเท่านั้น

- การเข้าถึงจากระยะไกล (Remote Access) ต้องผ่าน VPN หรือระบบที่มีมาตรการรักษาความปลอดภัยเพียงพอ

- ต้องมีการจำกัดการเข้าถึงจากอุปกรณ์ส่วนตัว ตามข้อกำหนดขององค์กร

5.4.6 การบันทึก และติดตามการใช้งาน (Logging and Monitoring of Application Access)

- ระบบเทคโนโลยีสารสนเทศและการสื่อสารต้องสามารถบันทึกกิจกรรมของผู้ใช้ในระบบ (Application Log) ได้อย่างครบถ้วน รวมถึงข้อมูลที่เกี่ยวข้องกับ

  - การเข้าสู่ระบบ / ออกจากระบบ

  - การเปลี่ยนแปลงสิทธิ์

  - การเข้าถึงหรือแก้ไขข้อมูลสำคัญ

- บันทึกดังกล่าวต้องจัดเก็บไว้อย่างปลอดภัย และมีการกำหนดระยะเวลาการเก็บรักษาตามข้อกฎหมาย เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA) , พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ต้องมีการตรวจสอบ และทบทวน Log เป็นระยะ หากมีพฤติกรรมผิดปกติ

หมวดที่ 6 การสร้างความมั่นคงปลอดภัยทางกายภาพ และสิ่งแวดล้อม (Physical and Environment Security)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมด้านกายภาพ และสิ่งแวดล้อมสำหรับสถานที่ อุปกรณ์ และโครงสร้างพื้นฐานของสารสนเทศในองค์กร เพื่อป้องกันการเข้าถึง การใช้ การเปิดเผย การแก้ไข หรือการทำลายทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร โดยไม่ได้รับอนุญาต ตลอดจนลดผลกระทบจากเหตุการณ์ภัยคุกคามทางกายภาพหรือสิ่งแวดล้อม

6.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Physical Security Perimeter)

6.1.1 ขอบเขต หรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)

- บริษัทกำหนดพื้นที่ควบคุม (Secure Areas) เช่น ห้องศูนย์ข้อมูล ของฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร และพื้นที่ที่เก็บข้อมูลสำคัญ พร้อมติดตั้งโครงสร้างป้องกันทางกายภาพ เช่น ผนัง ประตู ระบบล็อก และระบบเฝ้าระวัง (CCTV) ให้เหมาะสม

- มีแผนผัง และรายการพื้นที่ที่จัดเป็น Secure Area พร้อมอัปเดตอย่างสม่ำเสมอ

6.1.2 การควบคุมทางเข้าออกกายภาพ (Physical Entry Controls)

- การเข้าถึง Secure Area ต้องจำกัดเฉพาะบุคคลที่ได้รับอนุญาตโดยมีระบบควบคุม เช่น ระบบสแกนลายนิ้วมือ/ใบหน้า และมีการบันทึกประวัติการเข้าออก

- มีการตรวจสอบ และทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

6.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่น ๆ

- มีการออกแบบสำนักงาน และห้องทำงานเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงมีระบบเตือนภัยและควบคุมสภาพแวดล้อม เช่น ระบบตรวจจับควันหรือความร้อน

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องออกแบบและติดตั้งระบบการรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อป้องกันพื้นที่ปฏิบัติงานและพื้นที่ ซึ่งมีข้อมูลสำคัญ ห้องคอมพิวเตอร์ และพื้นที่ปฏิบัติงานของผู้ดูแลระบบ หรืออุปกรณ์สารสนเทศต่าง ๆ ที่ใช้ในการปฏิบัติงานอันเนื่องมาจากการได้รับความเสียหายและถูกเข้าถึงโดยไม่ได้รับอนุญาต

6.1.4 การป้องกันภัยคุกคามจากภายนอก และสภาพแวดล้อม (Protecting Against External End Environmental Threats)

- มีมาตรการลดความเสี่ยงจากภัยธรรมชาติ และเหตุการณ์จากภายนอก เช่น อัคคีภัย น้ำท่วม การบุกรุก หรือความเสียหายจากสิ่งแวดล้อม โดยจัดให้มีระบบเตือนภัย อุปกรณ์ป้องกัน และการประกันความเสียหายที่เหมาะสม

6.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

- กำหนดข้อบังคับ และข้อปฏิบัติสำหรับการเข้าปฏิบัติงานใน Secure Area เช่น ห้ามใช้อุปกรณ์ส่วนตัว ห้ามนำของมีคม หรือห้ามใช้กล้องถ่ายรูป

- บุคลากรต้องผ่านการอบรม และลงนามรับทราบข้อปฏิบัติก่อนเข้าพื้นที่ดังกล่าว

6.1.6 พื้นที่สำหรับรับส่งสิ่งของ (Delivery and Loading Areas)

- กำหนดจุดรับส่งอุปกรณ์ หรือสิ่งของแยกจากพื้นที่ปฏิบัติงานหลักอย่างชัดเจน พร้อมทั้งควบคุมการเข้าถึงเพื่อลดความเสี่ยงจากการบุกรุก หรือแอบแฝงข้อมูล

6.2 อุปกรณ์ (Equipment)

6.2.1 การจัดวาง และป้องกันอุปกรณ์ (Equipment Setting and Protection)

- อุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารต้องติดตั้งในสถานที่ปลอดภัย มีระบบป้องกันการโจรกรรมหรือการรบกวนจากบุคคลภายนอก

- ตู้แร็คและอุปกรณ์เครือข่ายต้องมีระบบล็อก และเข้าถึงได้เฉพาะผู้มีอำนาจเท่านั้น

6.2.2 ระบบเทคโนโลยีสารสนเทศและการสื่อสาร และอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

- ติดตั้งอุปกรณ์สำรอง และระบบสนับสนุน เช่น UPS , ระบบดับเพลิง , ระบบปรับอากาศและควบคุมความชื้น ตลอดจนมีการบำรุงรักษาให้อยู่ในสภาพพร้อมใช้งานเสมอ

6.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)

- ต้องวางสายสัญญาณในช่องทางที่ปลอดภัยแ ละควบคุมได้ เพื่อป้องกันการดักฟัง การเข้าถึงโดยไม่ได้รับอนุญาต หรือความเสียหายจากกายภาพ

6.2.4 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องควบคุมดูแลให้อุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสารหลักทั้งหมด ซึ่งใช้ในการประมวลผลในระดับปฏิบัติการรวมถึงอุปกรณ์สนับสนุนการทำงานได้รับการบำรุงดูแลรักษา ตามช่วงเวลาและตามข้อกำหนดที่ผู้ผลิตแนะนำ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้งาน

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องควบคุมให้มีการบันทึกกิจกรรมการบำรุงอุปกรณ์รวมถึงบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ให้อยู่ในสภาพพร้อมใช้งานเสมอ

6.2.5 การนำทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสารออกนอกสำนักงาน (Removal of Assets)

- ผู้ทำหน้าที่กำกับดูแลพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยและอาคารสถานที่ ต้องไม่อนุญาตให้นำอุปกรณ์สารสนเทศออกจากบริษัท ยกเว้นจะมีการอนุญาตให้นำออกโดยผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

- ผู้ใช้งาน ต้องไม่นำอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร ข้อมูลสารสนเทศหรือซอฟต์แวร์ออกนอกบริษัท ยกเว้นจะได้รับอนุญาตจากผู้ที่ได้รับมอบหมายในการอนุญาตให้นำทรัพย์สินออก

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดขั้นตอนปฏิบัติสำหรับการนำทรัพย์สินออกนอกบริษัทอย่างเป็นลายลักษณ์อักษร และปรับปรุงให้เป็นปัจจุบันเสมอ รวมถึงสื่อสารให้ผู้ใช้งานภายในองค์กรรับทราบและปฏิบัติตาม

6.2.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of Equipment and Asset Off-Permises)

- กำหนดให้ผู้บริหารระดับฝ่ายขึ้นไป เป็นผู้มีอำนาจในการอนุญาตให้นำอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารขององค์กรไปใช้ภายนอกสำนักงาน และต้องกำหนดให้มีการป้องกันอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารต่าง ๆ ที่ใช้งานอยู่ภายนอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์โดยพิจารณาจากความเสี่ยงที่อาจเกิดขึ้นกับอุปกรณ์เหล่านั้น

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดมาตรการความมั่นคงปลอดภัยในการควบคุมทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสารที่ใช้งานอยู่ภายนอกสำนักงาน เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรออกไปใช้งาน

- ฝ่ายเทคโนโลยีและการสื่อสารต้องมีมาตรการป้องกันอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารที่ใช้ภายนอก เช่น การเข้ารหัสข้อมูล การใช้ VPN การล็อกอุปกรณ์ และต้องประเมินความเสี่ยงก่อนอนุมัติการใช้งาน

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

- ผู้ใช้งาน ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่สำคัญหรือซอฟต์แวร์ลิขสิทธิ์ที่อยู่ภายในสื่อบันทึกข้อมูลได้มีการลบ ย้าย หรือทำลายอย่างเหมาะสม ตามลำดับชั้นความลับข้อมูล ก่อนที่จะทำลายหรือจำหน่ายอุปกรณ์กลับมาใช้ใหม่

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องจัดทำขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลหรือทรัพย์สินเทคโนโลยีสารสนเทศและการสื่อสาร และมาตรการหรือเทคนิคสำหรับการทำลายข้อมูล เพื่อนำอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารกลับมาใช้งานซ้ำ โดยต้องมีความสอดคล้องกับการจัดลำดับชั้นความลับข้อมูล

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดผู้รับผิดชอบในการทำหน้าที่ทำลายข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร ที่ไม่จำเป็นต่อการดำเนินกิจการขององค์กรซึ่งจัดเก็บอยู่บนสื่อบันทึกข้อมูล

6.2.8 การป้องกันอุปกร์ที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended User Equipment)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดมาตรการควบคุมการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสารที่ทิ้งไว้โดยไม่มีผู้ดูแล เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต

- ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศและการสื่อสารของตน โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

- ผู้ใช้งานต้องออกจากระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบงานคอมพิวเตอร์ที่ใช้งานหรือเครื่องคอมพิวเตอร์โดยทันทีเมื่อไม่มีความจำเป็นต้องใช้งาน หรือเมื่อเสร็จสิ้นการปฏิบัติงาน

- ผู้ใช้งาน ต้องล็อคหน้าจอเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือเมื่อออกห่างจากเครื่องคอมพิวเตอร์

6.2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

- ผู้ดูและระบบควบคุมให้มีการล็อคหน้าจอคอมพิวเตอร์เมื่อไม่ได้ใช้งาน (Clear Screen) เช่นการตัดออกจากระบบ (Session Time Out) และการล็อคหน้าจอ (Lock Screen) อัตโนมัติ เป็นต้น

- ผู้ใช้งาน ต้องไม่ละเลยข้อมูลสารสนเทศที่สำคัญ เช่น เอกสารกระดาษหรือสื่อบันทึกข้อมูล ให้อยู่ในสถานที่ไม่ปลอดภัย พื้นที่ สาธารณะ หรือสถานที่ที่พบเห็นได้โดยง่าย ผู้ใช้งานต้องจัดเก็บข้อมูลเทคโนโลยีสารสนเทศและการสื่อสารในสถานที่ที่เหมาะสม รวมถึงมีการป้องกันเพื่อให้ยากต่อการเข้าถึงของผู้ไม่มีสิทธิ์

- ผู้ใช้งานต้องไม่จัดเก็บข้อมูลสำคัญไว้บนหน้าเดสท็อป (Desktop) ของเครื่องคอมพิวเตอร์ โดยผู้ใช้งานต้องจัดสรรพื้นที่ในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์และควบคุมการเข้าถึงอย่างเหมาะสม เพื่อป้องกันผู้อื่นเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

หมวดที่ 7 การดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ (Operations Security)

วัตถุประสงค์

เพื่อกำหนดแนวทางการควบคุมการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ให้มีความมั่นคงปลอดภัย มีประสิทธิภาพ และสามารถตรวจสอบย้อนหลังได้ โดยมีมาตรการที่ชัดเจน ครอบคลุมตั้งแต่การดำเนินงานประจำวัน การบริหารจัดการระบบ การเฝ้าระวัง และการควบคุมความเสี่ยง จากซอฟต์แวร์และช่องโหว่ทางเทคนิค

7.1 การจัดการกระบวนการปฏิบัติงาน (Operations Management)

7.1.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operations Procedures and Responsibilities)

- ฝ่ายเทคโนโลยีสารเสนเทศและการสื่อสาร ต้องจัดให้มีขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร ครอบคลุมกระบวนการดำเนินงานทั้งหมด โดยแยกหน้าที่ความรับผิดชอบให้ชัดเจน (segregation of duties)

- เอกสารประกอบ เช่น คู่มือปฏิบัติงาน เอกสารระบบ และฐานความรู้ ต้องจัดทำและทบทวน อย่างสม่ำเสมอ พร้อมจัดให้เข้าถึงได้ง่ายสำหรับผู้ที่เกี่ยวข้อง

- ต้องมีการอบรมให้กับเจ้าหน้าที่ที่เกี่ยวข้องตามหน้าที่ เพื่อให้เข้าใจแนวปฏิบัติอย่างถูกต้อง

7.1.2 การบริหารจัดการเปลี่ยนแปลง (Change Management)

- ขั้นตอนควบคุมการเปลี่ยนแปลงระบบ (เช่น software , hardware , process) เพื่อหลีกเลี่ยงผลกระทบ ด้านความมั่นคงปลอดภัย โดยมีการอนุมัติ ตรวจสอบ และบันทึกทุกขั้นตอน

- การเปลี่ยนแปลงที่สำคัญต้องมีการประเมินผลกระทบ (impact analysis) และทดสอบก่อนใช้งานจริง

7.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องมีการติดตาม วิเคราะห์ และวางแผนความสามารถ ของระบบอย่างต่อเนื่อง เพื่อให้รองรับการใช้งานในปัจจุบันและอนาคตอย่างมีประสิทธิภาพ

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

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องควบคุม กำกับให้มีการแยกส่วนระบบคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environments) การทดสอบระบบงาน (Test Environment) และระบบที่ให้บริการจริง (Production Environment) ออกจากกัน

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องควบคุม ให้มีการกำหนดสิทธิ์การเข้าถึงในแต่ละสภาพแวดล้อมและจัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบงานอย่างชัดเจน โดยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหา และวิธีการแก้ไขรวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ

7.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

7.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls Against Malware)

- ฝ่ายเทคโนโลยีสารและการสื่อสารต้องติดตั้งระบบตรวจจับและป้องกันมัลแวร์ในทุกอุปกรณ์ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร พร้อมทั้งอัปเดตฐานข้อมูลมัลแวร์เป็นประจำ

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องอบรมผู้ใช้งานเกี่ยวกับความเสี่ยงจากมัลแวร์และแนวทางการใช้งานที่ปลอดภัย

7.3 การสำรองข้อมูล (Back up)

7.3.1. การสำรองข้อมูล (Information Backup)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดมาตรการในการสำรองข้อมูล และรอบการสำรองข้อมูล ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่สำคัญไว้อย่างสม่ำเสมอ เพื่อป้องกันการสูญหายของข้อมูล

- เจ้าของข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร ต้องดำเนินการ หรือกำหนดให้มีการสำรองข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร และการทดสอบข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าจะสามารถนำข้อมูลกลับมาใช้ใหม่ได้เมื่อต้องการ

- การสำรองข้อมูลต้องได้รับการเข้ารหัสและจัดเก็บในสถานที่ที่ปลอดภัย

7.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

7.4.1 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event Logging)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีการจัดเก็บ Log ที่จำเป็นต่อการตรวจสอบความปลอดภัย เช่น login / logout , การเข้าถึงข้อมูลสำคัญ ฯลฯ

- Log ต้องเก็บในรูปแบบที่ไม่สามารถเปลี่ยนแปลงได้ง่าย และมีระยะเวลาเก็บรักษาตามกฎหมายและข้อบังคับที่เกี่ยวข้อง เช่น อย่างน้อย 90 วันตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

7.4.2 การป้องกันข้อมูล Log (Protection of Log Information)

- มีการควบคุมการเข้าถึง Log และจัดเก็บอย่างปลอดภัย โดยต้องมีการเข้ารหัสหรือแยกพื้นที่จัดเก็บ

7.4.3 การบันทึกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and Operator Logs)

- บันทึกกิจกรรมของผู้ดูแลระบบทั้งหมด และมีการทบทวนโดยผู้มีอำนาจสูงกว่าเป็นระยะ

7.4.4 การตั้งเวลาระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Clock Synchronization)

- ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีการกำหนดเวลาให้ตรงกับ NTP (Network Time Protocol) ที่น่าเชื่อถือ และใช้เวลามาตรฐานเดียวกันทั่วทั้งองค์กร

7.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software)

- ต้องมีการอนุมัติล่วงหน้าก่อนการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการจริง

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีการกำหนดรายการซอฟต์แวร์ที่ได้รับอนุญาตและอัปเดตเป็นประจำ

- ห้ามพนักงานติดตั้งซอฟต์แวร์เองโดยไม่ได้รับอนุญาต

7.6 การบริหารจัดการช่องโหว่ทางเทคนิคในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

7.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องควบคุมให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ได้รับการพิสูจน์ถึงช่องโหว่ทางเทคนิคซึ่งอาจเกิดขึ้นได้ โดยให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง

- ผู้ดูแลระบบ ต้องดูแลและบำรุงรักษาระบบ เพื่อรักษาระดับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของระบบอย่างสม่ำเสมอ ได้แก่ การตรวจสอบหาช่องโหว่ การประเมินความเสี่ยงของช่องโหว่ ที่ตรวจสอบพบ และการปรับปรุงแก้ไขช่องโหว่ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีการติดตามข่าวสารช่องโหว่จากผู้ผลิตหรือแหล่งข่าวด้านความปลอดภัย และประเมินผลกระทบต่อระบบขององค์กร

7.6.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

- ผู้ใช้งานต้องปฏิบัติตามกฎเกณฑ์การควบคุมการติดตั้งซอฟต์แวร์ และไม่ติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของบริษัท

7.7 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information System Audit Considerations)

7.7.1 มาตรการตรวจสอบประเมินระบบ (Information System Audit Controls)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องจัดทำแผนการตรวจสอบระบบเทคโนโลยีสารสนเทศและการสื่อสารให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้ เช่น แผนการตรวจสอบช่องโหว่ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Vulnerability Assessment) เป็นต้น

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องแจ้งให้หน่วยงานที่เกี่ยวข้องรับทราบก่อนดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศและการสื่อสารทุกครั้ง

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดขอบเขตการตรวจสอบทางเทคนิค (Technical Audit Test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญ และต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติตามปกติ โดยกรณีที่การตรวจสอบระบบเทคโนโลยีสารสนเทศและการสื่อสารมีโอกาสกระทบต่อความพร้อมใช้งานของระบบ (System Availability) ต้องจัดให้มีการทดสอบนอกเวลาทำการ

- การตรวจสอบต้องไม่ละเมิดสิทธิส่วนบุคคลหรือข้อมูลส่วนบุคคลโดยมิชอบตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act : PDPA)

หมวดที่ 8 การสื่อสารด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Communications Security)

วัตถุประสงค์

เพื่อกำหนดแนวทางควบคุมการจัดการระบบเครือข่าย และการแลกเปลี่ยนข้อมูลสารสนเทศทั้งภายในและภายนอกองค์กรให้มีความมั่นคงปลอดภัย เป็นไปตามมาตรฐานสากล และสอดคล้องกับข้อกำหนดด้านกฎหมายและกฎระเบียบที่เกี่ยวข้อง

8.1 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)

8.1.1 การควบคุมเครือข่าย (Network Controls)

- ผู้ดูแลระบบต้องดำเนินการควบคุมและบริหารจัดการระบบเครือข่ายอย่างเหมาะสม เพื่อป้องกันภัยคุกคามจากภายนอกและภายใน

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่ส่งผ่านเครือข่าย และของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ทำงานอยู่บนเครือข่ายดังกล่าว

8.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)

- ผู้ดูแลระบบต้องจัดทำข้อตกลงหรือสัญญาบริการเครือข่าย (Service Level Agreement - SLA) โดยกำหนดคุณสมบัติด้านความมั่นคงปลอดภัย และมาตรฐานขั้นต่ำที่ผู้ให้บริการจะต้องปฏิบัติตาม

- ข้อตกลงต้องรวมถึงมาตรการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเข้ารหัสข้อมูล และการตรวจสอบย้อนกลับ

8.1.3 การแบ่งแยกเครือข่าย (Segregation in Network)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีการแยกเครือข่ายตามระดับความเสี่ยงของระบบงาน เช่น เครือข่ายสำหรับงานภายใน เครือข่ายที่เชื่อมต่อกับภายนอก และเครือข่ายให้มีการควบคุมการเข้าถึงระหว่างเครือข่ายอย่างเหมาะสม เช่น การใช้ VLAN , Firewall , หรือ DMZ

8.2 การแลกเปลี่ยนข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร (Information Transfer)

8.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร (Information Transfer Policies and Procedures)

- บริษัทจัดทำนโยบายและขั้นตอนการแลกเปลี่ยนข้อมูลให้สอดคล้องกับระดับความลับของข้อมูล และประเภทของช่องทางที่ใช้ในการส่งผ่าน

- มีการระบุว่าใครเป็นผู้รับผิดชอบอนุมัติการแลกเปลี่ยน และวิธีการป้องกันความลับหรือความถูกต้องของข้อมูล

8.2.2 ข้อตกลงสำหรับการแลกเปลี่ยนข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร (Agreements on Information Transfer)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร จัดทำข้อตกลงเป็นลายลักษณ์อักษร สำหรับการแลกเปลี่ยนข้อมูลทั้งภายในและภายนอกองค์กร โดยเฉพาะกับผู้ให้บริการภายนอก (Third Party)

- การแลกเปลี่ยน ข้อมูลสารเทคโนโลยีสารสนเทศและการสื่อสารภายในองค์กรกับหน่วยงานภายนอกต้องได้รับการอนุมัติจากเจ้าของข้อมูลก่อนทุกครั้งและมีการควบคุมโดยการระบุข้อตกลงเป็นลายลักษณ์อักษร รวมถึงกำหนดเงื่อนไขสำหรับการแลกเปลี่ยน ตลอดจนต้องมีการป้องกันข้อมูลสารสนเทศตามลำดับชั้นความลับข้อมูลอย่างเหมาะสม

8.2.3 การส่งข้อความอิเล็กทรอนิกส์ (Electronic Messaging)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีมาตรการควบคุมการใช้งานอีเมลและช่องทางการสื่อสารอิเล็กทรอนิกส์อื่น เช่น EDI , Instant Messaging

- สำหรับข้อมูลที่มีความอ่อนไหวหรือเป็นความลับ ต้องมีการเข้ารหัสก่อนส่ง และตรวจสอบผู้รับที่ได้รับอนุญาต

8.2.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or Non-Disclosure Agreements - NDA)

- พนักงาน และบุคคลภายนอกที่เข้ามาปฏิบัติงาน ต้องลงนามในข้อตกลงการรักษาความลับ (NDA) โดยระบุข้อผูกพันในการไม่เปิดเผยข้อมูลขององค์กรทั้งระหว่างปฏิบัติงาน และหลังสิ้นสุดสัญญาจ้าง

- บริษัทจัดเก็บเอกสารดังกล่าวอย่างเป็นระบบและสามารถตรวจสอบย้อนหลังได้

8.2.5 การเข้ารหัสข้อมูลในการสื่อสาร (Encryption of Information in Transit)

- ข้อมูลที่มีการส่งผ่านเครือข่ายทั้งภายในและภายนอกองค์กร ต้องได้รับการเข้ารหัสโดยใช้มาตรฐานที่ยอมรับ เช่น TLS/SSL หรือ IPsec

- บริษัทต้องกำหนดนโยบายการใช้ใบรับรองดิจิทัล (Digital Certificates) และการจัดการกุญแจเข้ารหัสอย่างปลอดภัย

8.2.6 การควบคุมการใช้สื่อพกพา (Control of Removable Media)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ควรกำหนดนโยบายในการใช้สื่อพกพา เช่น USB Drive หรือ External HDD เพื่อป้องกันการรั่วไหลของข้อมูล

- การส่งข้อมูลผ่านสื่อพกพาต้องได้รับการอนุญาต และมีมาตรการควบคุม เช่น การเข้ารหัสข้อมูลในอุปกรณ์

8.2.7 การใช้งานสื่อสังคมออนไลน์ (Use of Social Media)

- บริษัทต้องกำหนดระเบียบการใช้สื่อสังคมออนไลน์ (Social Media Policy) เพื่อควบคุมการสื่อสารข้อมูลข่าวสารขององค์กรผ่านแพลตฟอร์มต่าง ๆ เช่น Facebook , Line , X (Twitter) , TikTok เป็นต้น

- พนักงานที่ได้รับมอบหมายในการดูแลบัญชีโซเชียลมีเดียขององค์กรต้องได้รับการฝึกอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูล และต้องปฏิบัติตามนโยบายที่กำหนดไว้อย่างเคร่งครัด

- ห้ามเผยแพร่ข้อมูลที่มีลักษณะเป็นความลับ ข้อมูลส่วนบุคคล หรือข้อมูลที่อาจก่อให้เกิดความเสียหายต่อองค์กรโดยไม่ได้รับอนุญาตล่วงหน้า

- มีการกำกับดูแลและบันทึกประวัติการเข้าถึงบัญชีโซเชียลมีเดียอย่างเหมาะสม

หมวดที่ 9 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System Acquisition , Development and Maintenance)

วัตถุประสงค์

เพื่อลดความผิดพลาดในการกำหนดความต้องการ การออกแบบ การพัฒนา และการทดสอบระบบสารสนเทศที่มีการพัฒนาขึ้นใหม่หรือปรับปรุงระบบงานเพิ่มเติม รวมถึงควบคุมให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อตกลงที่กำหนดไว้

9.1 ความต้องการด้านความมั่นคงปลอดภัยระบบ (Security Requirement of Information Systems)

9.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information Security Requirements Analysis and Specification)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารมีหน้าที่รับผิดชอบในการพัฒนา จัดหา หรือปรับปรุงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ต้องดำเนินการวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างชัดเจนในทุกระยะของโครงการ โดยครอบคลุมด้านความลับ (Confidentiality) , ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability)

- ข้อกำหนดดังกล่าวต้องถูกรวมไว้ในเอกสารข้อกำหนดผู้ใช้ (User Requirements Specification - URS) , เอกสารข้อกำหนดระบบ (System Requirements Specification - SRS) หรือเอกสารขอบเขตงาน (Terms of Reference - TOR)

- ต้องมีการติดตาม ตรวจสอบ และประเมินความสอดคล้องของระบบกับข้อกำหนดด้านความมั่นคงปลอดภัยอย่างต่อเนื่องตลอดกระบวนการพัฒนาและจัดหา

9.1.2 ความมั่นคงปลอดภัยของบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร บนเครือข่ายสาธารณะ (Securing Application Service on Public Networks)

- ให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลทคโนโลยีสารสนเทศและการสื่อสารที่ผ่านระบบให้บริการ การใช้งาน (Application Service) ทั้งในกรณีทั่วไปและกรณีที่ผ่านเครือข่ายสาธรณะ เพื่อป้องกันการกระทำผิดในลักษณะทุจริต (Fraudulent Activities) การทำธุระกรรมที่ไม่สมบูรณ์หรือผิดพลาด (Incomplete Transmission of Miss-Routing) หรือการเปิดเผยคัดลอก หรือเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

- มาตรการที่ควรนำมาใช้ ได้แก่ การเข้ารหัสข้อมูล (Data Encryption), การพิสูจน์ตัวตนแบบสองชั้น (Two-Factor Authentication), การใช้ช่องทางสื่อสารที่ปลอดภัย (เช่น HTTPS, VPN), และการใช้ไฟร์วอลล์

9.1.3 การป้องกันธุรกรรมของบริการเทคโนโลยีสารสนเทศและการสื่อสาร (Protecting Application Services Transactions)

- ธุรกรรมทางอิเล็กทรอนิกส์หรือข้อมูลที่เกี่ยวข้องกับการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารต้องได้รับการป้องกันจากการถูกดัดแปลง การสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

- ต้องใช้วิธีการรับรองความถูกต้องของข้อมูล (Data Integrity Checks) , การเข้ารหัสระหว่างการส่ง (Encryption-in-Transit) , และการตรวจสอบเส้นทางการส่งข้อมูล (Routing Validation)

- ควรมีระบบจัดเก็บบันทึกเหตุการณ์ (Audit Trail) เพื่อสามารถตรวจสอบย้อนหลังได้ในกรณีเกิดปัญหาหรือข้อผิดพลาด

9.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและสนับสนุน (Security in Development and Support Processes)

9.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดนโยบายและแนวทางสำหรับการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารให้มั่นคงปลอดภัย ครอบคลุมตลอดวงจรการพัฒนาระบบ โดยระบุข้อกำหนดและมาตรการควบคุมความมั่นคงปลอดภัยที่ชัดเจน เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากกระบวนการพัฒนา

9.2.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures)

- การเปลี่ยนแปลงที่มีผลต่อซอฟต์แวร์หรือระบบเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการตามขั้นตอนที่เป็นลายลักษณ์อักษร โดยรวมถึงการวิเคราะห์ความเสี่ยง การทดสอบผลกระทบ และการขออนุมัติอย่างเป็นทางการก่อนดำเนินการ

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

- เมื่อมีการเปลี่ยนแปลงระบบปฏิบัติการหรือโครงสร้างพื้นฐาน ต้องมีการวิเคราะห์ผลกระทบทางเทคนิค และทดสอบในสภาพแวดล้อมที่แยกจากระบบจริงก่อนดำเนินการจริง รวมถึงตรวจสอบความถูกต้องหลังการเปลี่ยนแปลง

9.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

- การใช้งานซอฟต์แวร์สำเร็จรูปควรดำเนินการตามมาตรฐานของผู้ผลิต และหลีกเลี่ยงการแก้ไขเว้นแต่มีความจำเป็น โดยต้องดำเนินการภายใต้การควบคุมการเปลี่ยนแปลงและการอนุมัติอย่างเป็นทางการ

- การเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำเร็จรูป ต้องดำเนินการเปลี่ยนแปลงตามขั้นตอนปฏิบัติการควยคุมการเปลี่ยนแปลงที่ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารกำหนดไว้

9.2.5 หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles)

- ส่วนพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร ส่วนบริหารโครงการเทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่ได้รับมอบหมายให้พัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร ต้องยึดหลักการความมั่นคงปลอดภัยในการพัฒนาระบบ ดังต่อไปนี้เป็นอย่างน้อย

- การให้สิทธิ์ต่ำที่สุด (Least Privilege) แก่ผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

- การให้สิทธิ์เฉพาะที่จำเป็นในการปฏิบัติงาน (Need to know) แก่ผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ

- การออกแบบระบบให้สามารถป้องกันได้หลายระดับชั้น (Defense In-Depth) เพื่อลดความเสี่ยงของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- การออกแบบในลักษณะเปิด (Open Design) เพื่อให้การพัฒนาระบบมีการใช้กลไกหรืออัลกอริทึม (Algorithm) ที่เป็นมาตรฐานเดียวกันและสามารถตรวจสอบการทำงานได้

9.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure Development Environment)

- กำหนดแยกสภาพแวดล้อมสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกัน และควบคุมการเข้าถึงให้เหมาะสม รวมถึงต้องมีมาตรการป้องกันข้อมูลที่ใช้ในกระบวนการพัฒนาให้ปลอดภัยจากการรั่วไหลหรือการเข้าถึงโดยไม่ได้รับอนุญาต

9.2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsource Development)

- ในกรณีที่มีการว่าจ้างหน่วยงานภายนอกพัฒนาระบบ ต้องกำหนดข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน และมีการติดตาม ตรวจสอบ และควบคุมการดำเนินการอย่างต่อเนื่อง

9.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing)

- ระบบที่พัฒนาใหม่หรือมีการเปลี่ยนแปลงต้องผ่านการทดสอบด้านความมั่นคงปลอดภัยอย่างเหมาะสม เช่น การสแกนหาช่องโหว่ หรือการทดสอบการเจาะระบบ (Penetration Testing) และต้องจัดเก็บหลักฐานการทดสอบอย่างเป็นระบบ

9.2.9 การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)

- ก่อนนำระบบไปใช้งานจริง ต้องดำเนินการทดสอบเพื่อรับรองความพร้อมในการใช้งาน (Acceptance Testing) โดยผู้ใช้งานระบบร่วมตรวจสอบ และต้องมีเกณฑ์การประเมินและอนุมัติที่ชัดเจนจากหน่วยงานที่เกี่ยวข้อง

9.3 ข้อมูลสำหรับการทดสอบ (Test Data)

9.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

- หลีกเลี่ยงการใช้ข้อมูลจริงในการทดสอบระบบ เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล

- มีมาตรการป้องกันข้อมูลที่ใช้ในการทดสอบ เช่น การเข้ารหัส การปกปิดข้อมูล (Data Masking) หรือการควบคุมสิทธิ์การเข้าถึง

- กรณีหากใช้สำเนาข้อมูลจริง ต้องควบคุมการจัดเก็บและใช้งานข้อมูลทดสอบในระดับเดียวกับระบบจริง

หมวดที่ 10 การบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอก (Supplier Relationships)

วัตถุประสงค์

เพื่อกำหนดกรอบการควบคุมและแนวปฏิบัติที่ชัดเจนสำหรับการบริหารจัดการความสัมพันธ์กับหน่วยงานภายนอกที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพ ปลอดภัย และสอดคล้องกับข้อตกลง รวมถึงการลดความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารที่อาจเกิดขึ้นจากการพึ่งพาบุคคลหรือหน่วยงานภายนอก

10.1 มั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารกับความสัมพันธ์กับหน่วยงานนอก (Information Security in Supplier Relationships)

10.1.1 นโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านความสัมพันธ์กับหน่วยงานนอก (Information Security Policy for Supplier Relationships)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารในการว่าจ้างหรือใช้บริการจากหน่วยงานภายนอก โดยพิจารณาและประเมินความเสี่ยงก่อนให้สิทธิ์ในการเข้าถึงระบบหรือข้อมูลเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร

- หน่วยงานที่รับผิดชอบในการประสานงานกับหน่วยงานภายนอกต้องควบคุมให้ผู้ให้บริการปฏิบัติตามข้อตกลงด้านความมั่นคงปลอดภัยที่ระบุไว้ในสัญญา โดยรวมถึงลักษณะบริการและระดับการให้บริการที่ตกลงกันไว้

10.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing Security Within Supplier Agreements)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องมีการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไว้ในสัญญาหรือข้อตกลงกับหน่วยงานภายนอกอย่างชัดเจน ครอบคลุมถึงสิทธิในการเข้าถึงระบบ การประมวลผล การจัดเก็บ และการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- การเข้าถึงข้อมูลขององค์กรโดยหน่วยงานภายนอกต้องดำเนินการตามหลักการ “Need-to-know” และต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล

- ต้องควบคุมให้มีการปฏิบัติตามข้อกำหนดในสัญญาตลอดระยะเวลาการให้บริการ

10.1.3 การบริหารจัดการและการสื่อสารต่อผู้รับจ้างช่วงของหน่วยงานภายนอก (Information and Communication Technology Supply Chain)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดให้สัญญาหรือข้อตกลงกับผู้ให้บริการภายนอก รวมถึงผู้รับจ้างช่วง (subcontractors) ระบุถึงความรับผิดชอบและมาตรการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างชัดเจน เพื่อให้มั่นใจได้ว่าไม่มีช่องโหว่ในห่วงโซ่อุปทาน

10.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

10.2.1 การติดตามและทบทวนการให้บริการของหน่วยงานภายนอก (Monitoring and Review of Supplier Services)

- ดำเนินการติดตาม ตรวจสอบ และทบทวนผลการให้บริการของหน่วยงานภายนอกอย่างสม่ำเสมอ เพื่อประเมินความสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัย ประสิทธิภาพในการให้บริการ สถานะทางการเงิน และการปฏิบัติงานตามสัญญา

10.2.2 การบริหารจัดการการเปลี่ยนแปลงบริการของหน่วยงานภายนอก (Managing Changes to Supplier Services)

- ในกรณีที่หน่วยงานภายนอกมีการเปลี่ยนแปลงกระบวนการให้บริการ วิธีการปฏิบัติงาน หรือมาตรการรักษาความมั่นคงปลอดภัย ต้องมีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว

- รายงานการเปลี่ยนแปลงให้ผู้บริหารที่เกี่ยวข้องรับทราบ และกำหนดแนวทางบริหารจัดการความเสี่ยงอย่างเหมาะสม

หมวดที่ 11 การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information Security Incident Management)

วัตถุประสงค์

เพื่อกำหนดแนวทางการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างเป็นระบบ รวมถึงการเรียนรู้จากเหตุการณ์ที่ผ่านมา เพื่อป้องกันมิให้เหตุการณ์ลักษณะเดียวกันเกิดขึ้นซ้ำอีก และเพื่อให้การตอบสนองเป็นไปอย่างทันท่วงที มีประสิทธิภาพ และสอดคล้องกับกฎหมายที่เกี่ยวข้อง

11.1 การบริหารจัดการเหตุขัดข้องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Management of Information Security Incidents and Improvement)

11.1.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องจัดทำแนวทางปฏิบัติและกำหนดหน้าที่ความรับผิดชอบในการจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารอย่างชัดเจน

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องแยกแยะเหตุการณ์ด้านความมั่นคงปลอดภัยออกจากปัญหาการดำเนินงานทั่วไป เพื่อดำเนินการตามแนวทางที่เหมาะสม

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดช่องทางและเกณฑ์การรายงานเหตุการณ์พร้อมประชาสัมพันธ์ให้บุคลากรภายในและหน่วยงานภายนอกที่เกี่ยวข้องรับทราบ

11.1.2 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย (Reporting Information Security Events)

- พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องต้องรายงานเหตุการณ์ต่อผู้บังคับบัญชาและฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารอย่างเร่งด่วน ผ่านช่องทางที่กำหนด

11.1.3 การรายงานจุดอ่อนด้านความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

- ผู้ใช้งาน และหน่วยงานภายนอกต้องรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรต่อผู้บังคับบัญชาและฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร โดยผ่านช่องทางการรายงานที่กำหนดไว้และจะต้องดำเนินการรายงานอย่างรวดเร็วที่สุด

- ผู้ใช้งานและหน่วยงานภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือจุดอ่อนใดๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสารในองค์กร ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้นผู้บังคับบัญชาและฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารด้วยตนเอง

11.1.4 การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Assessment of and Decision on Information Security Events)

- ผู้ดูแลระบบต้องประเมินความรุนแรงของเหตุการณ์หรือจุดอ่อน และจำแนกลำดับความสำคัญตามเกณฑ์
- แจ้งให้ผู้ที่เกี่ยวข้องรับทราบและดำเนินการแก้ไขโดยเร็ว

11.1.5 การตอบสนองต่อเหตุขัดข้องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Response to Information Security Incidents)

- บุคลากรที่ได้รับมอบหมายและผู้ให้บริการภายนอกต้องดำเนินการตอบสนองตามขั้นตอนที่กำหนด
- หากไม่สามารถดำเนินการได้ทันตามระยะเวลาที่กำหนด ต้องแจ้งให้ผู้บังคับบัญชาทราบทันที

11.1.6 การเรียนรู้จากเหตุขัดข้องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Leaning from Information Security Incidents)

- บุคลากรที่ได้รับมอบหมายให้เป็นผู้แก้ไขเหตุขัดข้องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานภายนอกที่เป็นผู้มีสัญญาทำงานให้ จะต้องจัดเตรียมรายงานผลการวิเคราะห์และการแก้ไขเหตุขัดข้องจุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร และจัดเก็บไว้เป็นองค์ความรู้ เพื่อใช้ในการเรียนรู้ในการดำเนินงานและลดโอกาสเกิดในอนาคต

11.1.7 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

- บุคลากรที่เกี่ยวข้องต้องรวบรวมหลักฐานที่เกี่ยวข้องกับเหตุการณ์เพื่อสนับสนุนการตรวจสอบภายในการตัดสินใจของผู้บริหาร และกระบวนการทางกฎหมาย หากจำเป็น

หมวดที่ 12 ความมั่นคงปลอดภัยสำหรับการบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อกำหนดมาตรการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ในกรณีที่เกิดเหตุการณ์ฉุกเฉินหรือเหตุขัดข้องทางเทคนิค ซึ่งอาจก่อให้เกิดการหยุดชะงักของกระบวนการทางธุรกิจ โดยมุ่งเน้นให้ระบบสารสนเทศและกระบวนการที่เกี่ยวข้องสามารถดำเนินการต่อไปได้อย่างมั่นคง หรือสามารถฟื้นฟูการให้บริการกลับสู่สภาวะปกติได้ภายในระยะเวลาที่เหมาะสม ทั้งนี้ เพื่อรักษาความพร้อมในการดำเนินงานอย่างต่อเนื่องและลดความเสียหายที่อาจเกิดขึ้น

12.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information Security Continuity)

12.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Planning Information Security Continuity)

- หน่วยงานเจ้าของข้อมูลและฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารต้องร่วมกันดำเนินการระบุเหตุการณ์ที่อาจส่งผลกระทบต่อกระบวนการทางธุรกิจที่สำคัญ และดำเนินการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) พร้อมกับการประเมินความเสี่ยง (Risk Assessment) ต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อกำหนดลำดับความสำคัญของระบบงานและกำหนดมาตรการป้องกันและกู้คืนที่เหมาะสม

- ข้อมูลที่ได้จากการวิเคราะห์ต้องมีความครบถ้วน ถูกต้อง และเชื่อถือได้ เพื่อใช้ประกอบการจัดทำแผนความต่อเนื่องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

12.1.2 การสร้างกระบวนการความต่อเนื่องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Implementing Information Security Continuity)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องจัดทำแผนการรองรับกรณีเกิดเหตุฉุกเฉิน โดยให้รวมมาตรการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ไว้เป็นส่วนหนึ่งของแผน และต้องสอดคล้องกับแผนบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Plan: BCP) ขององค์กร

- แผนดังกล่าวต้องได้รับการอนุมัติจากผู้มีอำนาจ และจัดเก็บไว้ในสถานที่ที่สามารถเข้าถึงได้ในกรณีฉุกเฉิน รวมถึงมีการเผยแพร่ให้บุคลากรที่เกี่ยวข้องรับทราบอย่างชัดเจน

12.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Verify, Review and Evaluate Information Security Continuity)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร ต้องทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉินอย่างน้อยปีละ 1 ครั้งและจัดให้มีการบันทึกผลการทดสอบ เพื่อให้มั่นใจว่าแผนงานที่จัดทำมีความถูกต้องและสามารถตอบสนองต่อการดำเนินงานได้เป็นอย่างดี

- บุคลากรผู้ซึ่งมีส่วนเกี่ยวข้องในการปฏิบัติงานกู้คืนระบบเทคโนโลยีสารสนเทศและการสื่อสารต้องมีความรู้ด้านเทคนิคที่จำเป็นต่อการกู้คืนระบบและเข้าร่วมการซักซ้อมแผน

- ผลการทดสอบ การทบทวน และการประเมินแผนต้องได้รับการบันทึกและนำไปปรับปรุงแผนให้เหมาะสมกับสถานการณ์และภัยคุกคามที่เปลี่ยนแปลงอยู่เสมอ

12.2 การจัดให้มีอุปกรณ์หรือระบบเทคโนโลยีสารสนเทศและการสื่อสารสำรอง (Redundancies)

12.2.1 การประเมินและติดตั้งระบบสำรอง

- บริษัทควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีความสำคัญสูง และพิจารณากำหนดระดับการให้บริการขั้นต่ำที่ยอมรับได้ (Minimum Service Level)

- บริษัทมีการกำหนด Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) สำหรับแต่ละระบบงานที่สำคัญ เพื่อใช้เป็นเกณฑ์ในการวางแผนกู้คืน

12.2.2 การจัดเตรียมและทดสอบระบบสำรอง

- ดำเนินการติดตั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารสำรอง หรืออุปกรณ์สำรองที่เพียงพอและเหมาะสม เพื่อให้สามารถดำเนินงานต่อไปได้ในกรณีที่ระบบหลักไม่สามารถใช้งานได้

- ระบบสำรอง ได้รับการทดสอบสม่ำเสมอ และผลการทดสอบต้องได้รับการจัดเก็บและประเมินผลเพื่อให้มั่นใจว่าสามารถรองรับเหตุการณ์ฉุกเฉินได้จริง

หมวดที่ 13 การปฏิบัติตามกฎระเบียบและข้อบังคับ (Compliance)

วัตถุประสงค์

เพื่อให้การดำเนินงานของบริษัทเป็นไปตามกฎหมาย ข้อกำหนด สัญญา และระเบียบข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตลอดจนการปฏิบัติตามนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงมาตรฐานภายในขององค์กรอย่างเคร่งครัด

13.1 การปฏิบัติตามกฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้อง (Compliance with legal and Contractual Requirements)

13.1.1 การระบุกฎหมายและข้อกำหนดในสัญญาจ้าง (Identification of Applicable Legislation and Contractual Requirements)

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับฝ่ายทรัพยากรบุคคลต้องจัดทำรายการกฎหมาย กฎระเบียบ และข้อกำหนดตามสัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร อย่างครบถ้วนพร้อมจัดทำเป็นเอกสารและปรับปรุงให้เป็นปัจจุบัน

- บุคลากรทุกคนมีหน้าที่ปฏิบัติตามข้อกำหนดดังกล่าวอย่างเคร่งครัด

- ห้ามใช้ทรัพยากรเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรเพื่อกระทำการใด ๆ ที่ขัดต่อกฎหมายของราชอาณาจักรไทยหรือนานาชาติ ไม่ว่าในกรณีใด

13.1.2 การป้องกันสิทธิ และทรัพย์สินทางปัญญา (Intellectual property rights)

- บริษัทมีกระบวนการควบคุมการใช้ซอฟต์แวร์และทรัพย์สินทางปัญญาให้เป็นไปตามกฎหมายลิขสิทธิ์และข้อกำหนดของผู้พัฒนา

- ห้ามผู้ใช้งานทำซ้ำหรือเผยแพร่ซอฟต์แวร์ หรือสื่ออื่นใดที่ละเมิดลิขสิทธิ์

- ซอฟต์แวร์ที่พัฒนาโดยบุคลากรในหรือโดยผู้รับจ้างภายนอกให้ถือเป็นทรัพย์สินขององค์กร ห้ามเผยแพร่หรือจำหน่ายต่อโดยไม่ได้รับอนุญาต

- การใช้ซอฟต์แวร์ต้องสอดคล้องกับนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

13.1.3 การป้องกันข้อมูลขององค์กร (Protection of Records)

- เจ้าของข้อมูลต้องจัดการและจัดเก็บข้อมูลให้สอดคล้องกับข้อบังคับทางกฎหมาย เช่น การจัดเก็บข้อมูลทางบัญชี ข้อมูลลูกค้า

- มาตรการในการควบคุมบันทึก (logs) เพื่อป้องกันการสูญหาย การถูกเปลี่ยนแปลง หรือการเข้าถึงโดยไม่ได้รับอนุญาต

13.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information)

- ข้อมูลส่วนบุคคลของลูกค้าและพนักงานถือเป็นความลับ โดยอนุญาตให้เข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตจากผู้มีอำนาจ

- มีมาตรการควบคุมและตรวจสอบการเข้าถึง แก้ไข และเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

13.2 การทบทวนความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information Security Reviews)

13.2.1 การตรวจประเมินระบบเทคโนโลยีสารสนเทศและการสื่อสารจากผู้ตรวจสอบอิสระ (Independent Review of Information Security)

- องค์กรต้องดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศและการสื่อสารเป็นระยะ โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระภายนอก เพื่อประเมินความสอดคล้องกับนโยบาย มาตรฐาน และกระบวนการที่เกี่ยวข้อง

- การตรวจสอบต้องครอบคลุมถึงประสิทธิภาพของการควบคุมและมาตรการรักษาความมั่นคงปลอดภัย

13.2.2 การปฏิบัติตามนโยบายบริหารจัดการ และกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Compliance with Security Policies and Standards)

- หัวหน้าหน่วยงานแต่ละส่วนต้องตรวจสอบการปฏิบัติงานของบุคลากรภายใต้ความรับผิดชอบให้เป็นไปตามนโยบายและมาตรฐาน

- หัวหน้าหน่วยงานหากพบการปฏิบัติที่ไม่สอดคล้อง ต้องแจ้งเตือนให้แก้ไข และหากส่งผลกระทบร้ายแรงต้องดำเนินการตามระเบียบวินัย

- ฝ่ายเทคโนโลยีสารสนเทศและการสื่อสารมีหน้าที่สนับสนุนและให้คำแนะนำเกี่ยวกับการปฏิบัติตามนโยบาย ขั้นตอน และมาตรการด้านความมั่นคงปลอดภัย