นโยบาย

เรื่อง ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(Information Security Policy)

จัดทำโดย	ชื่อ : คุณวัชระ นันติ	ลงนาม :	วันที่ : 16/05/68
ทบทวนโดย	ชื่อ : คุณปริศนี อัจนารมย์วาท	ลงนาม :	วันที่ : 16/5/68
อนุมัติโดย	ชื่อ : อนิวรรต ศรีรุ่งธรรม	ลงนาม :	วันที่ : 19/5/68

นโยบาย

เรื่อง ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

1. **วัตถุประสงค์**

   เนื่องจากในปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญต่อการดำเนินการของบริษัท จึงต้องจัดให้มีนโยบายในการบริหารจัดการและรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ เพื่อให้เป็นไปตามข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติของหน่วยงานกำกับดูแล ดังนั้น บริษัทจึงจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ดังต่อไปนี้

2. **หน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับนโยบาย**

   - กลุ่มบริการด้านเทคโนโลยี รับทราบนโยบายและปฏิบัติตาม รวมถึงกำกับการทำงานให้เป็นไปตามนโยบายของบริษัทฯ
   - ฝ่ายกำกับการปฏิบัติงานและตรวจสอบภายใน มีหน้าที่กำกับดูแล และให้คำแนะนำ รวมทั้งตรวจสอบการควบคุมภายใน และตรวจสอบทางกระบวนการทำงานต่างๆ เพื่อให้เป็นไปตามนโยบาย

3. **หน่วยงานที่ต้องปฏิบัติตามนโยบาย**

   ทุกหน่วยงานภายในบริษัทฯ

4. **หน่วยงานที่กำกับดูแลให้เป็นไปตามนโยบาย**

   ผู้บังคับบัญชาทุกหน่วยงาน ฝ่ายกำกับดูแลการปฏิบัติงานและตรวจสอบภายใน และกลุ่มบริการด้านเทคโนโลยี

5. **วันที่มีผลบังคับใช้**

   นับตั้งแต่ประกาศใช้นโยบายฉบับนี้

6. **นิยาม**

คำศัพท์	ความหมาย
บริษัท	บริษัท ออโรร่า ดีไซน์ จำกัด (มหาชน)
ฝ่ายกำกับดูแลการปฏิบัติงานและตรวจสอบภายใน	หน่วยงานที่รับผิดชอบการกำกับดูแลด้านการปฏิบัติงานตามกฎเกณฑ์ และตรวจสอบการดำเนินงานของบริษัท และมีหน้าที่สนับสนุนผู้บริหารระดับสูง ให้สามารถบริหารความ

	เสี่ยงด้านการปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ได้อย่างมีประสิทธิภาพ
ฝ่ายบริหารทรัพยากรบุคคล	หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการทรัพยากรบุคคล การจัดหา คัดเลือก บุคลากรให้ตรงตามความต้องการของบริษัท และจัดการขั้นตอนการเข้าทำงาน การลาออกของพนักงาน รวมไปถึงการให้ความรู้ การอบรมที่เกี่ยวข้องกับการปฏิบัติงาน
กลุ่มบริการเทคโนโลยี	หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการด้านเทคโนโลยีสารสนทศของบริษัท ให้เป็นไปตามนโยบายและแนวปฏิบัติตามที่กำหนด
บุคคลภายนอก	บุคคลหรือพนักงานของหน่วยงานภายนอกที่เข้ามาติดต่อสื่อสาร และมีการเข้าถึงทรัพย์สินทางเทคโนโลยีสารสนเทศของบริษัท
ผู้ดูแลระบบ (Administrator)	พนักงานที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบ หรือเครือข่ายคอมพิวเตอร์ รวมไปถึงการแก้ไขปัญหาการใช้งานในด้านต่าง ๆ ซึ่งสามารถเข้าถึงโปรแกรมหรือเครือข่ายคอมพิวเตอร์เพื่อการจัดการและปฏิบัติงานต่างๆได้
ผู้บริหารสายงาน	ผู้บริหารสูงสุดของทุกสายงาน
ผู้ประสานงานทางด้านความมั่นคงปลอดภัย	ตัวแทนพนักงานจากสายงานต่างๆ ภายในบริษัท ซึ่งเป็นผู้ประสานงานหรือให้ความร่วมมือในการสร้างความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ มีหน้าที่ความรับผิดชอบในการกระตุ้นให้พนักงานในสายงานต่างๆ ปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ รวมทั้งการจัดการกับพนักงานในสายงานที่ไม่ปฏิบัติตามนโยบาย และการเป็นตัวแทนในการจัดการกับเหตุการณ์ทางต้านความมั่นคงปลอดภัยทางระบบเทคโนโลยีสารสนเทศและแผนความต่อเนื่องทางธุรกิจ
หน่วยงานการนอก (Third party)	องค์กรหรือหน่วยงานที่มีความจำเป็นในการเข้ามาปฏิบัติงานหรือเข้ามาเกี่ยวข้องกับสถานที่หรือทรัพย์สินสารสนเทศของบริษัท มีหน้าที่ความรับผิดชอบในการปฏิบัติตามนโยบาย

	และกฎเกณฑ์ ระเบียบ ตามข้อกำหนด ข้อตกลง หรือสัญญาที่ได้จัดทำกับบริษัท
ผู้ให้บริการรายอื่น	บุคคลหรือนิติบุคคลอื่นใด ทั้งในประเทศ และต่างประเทศที่ให้บริหารด้านเทคโนโลยีสารสนเทศแก่บริษัท
การเข้ารหัสลับ (Cryptography or Encryption)	การเปลี่ยนแปลงรูปแบบของข้อมูล ให้อยู่ในรูปแบบที่มีความมั่นคงปลอดภัย โดยใช้กุญแจในการเข้ารหัสลับ ซึ่งผู้ที่เข้าถึงข้อมูลจะไม่สามารถทราบเนื้อหาที่แท้จริงของข้อมูลได้เลย ถ้าไม่มีการถอดรหัสลับจากกุญแจที่ใช้ในการถอดที่ถูกต้องทั้งนี้ขึ้นกับเทคนิคการเข้ารหัสลับข้อมูลที่ถูกนำมาใช้งาน
การเปลี่ยนแปลง ปรับปรุง แก้ไข	การเปลี่ยนแปลง ปรับปรุงแก้ไขระบบ หรืออุปกรณ์ประมวลผลสารสนเทศ เช่น การติดตั้ง หรือ การปรับเปลี่ยนระบบปฏิบัติการ ซอฟต์แวร์ระบบ และระบบเครือข่าย
การเฝ้าระวัง (Monitoring)	การเฝ้าระวังทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบความผิดปกติจากการประมวลผลกิจกรรมต่างๆ ของระบบเทคโนโลยีสารสนเทศ บันทึกเหตุการณ์การใช้งานของระบบ (Logs) เช่น การเข้าถึงข้อมูล โดยไม่ได้รับอนุญาต การใช้งานเทคโนโลยีสารสนเทศผิดวัตถุประสงค์ และบัญหาที่เกิดขึ้นจากระบบงานในปัจจุบัน
การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัย (Security Awareness)	การให้ความรู้ความเข้าใจทางด้านความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ เพื่อสร้างความตระหนักถึงภัยคุกคามและปัญหาทางด้านความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศแก่บุคลากร
การสำรองข้อมูล (Data Backup)	การทำสำเนาข้อมูลทั้งหมดในระบบที่ต้องการ เพื่อเป็นการสำรองข้อมูลที่อาจมีการแก้ไขเปลี่ยนแปลง หรือสูญหาย ให้สามารถกลับมาใช้งานได้
กุญแจ (Key)	กุญแจที่ใช้ในระบวนการเข้าหัสลับ ใช้ในการเข้ารหัสลับหรือถอดรหัสลับ ขึ้นอยู่กับการงานเทคนิคการเข้าเข้ารหัสลับข้อมูล หรือแยกเป็น 2 ประเภท คือ กุญแจส่วนตัว (Private Key) และ กุญแจสาธารณะ (Public Key)
ข้อมูลสารสนเทศ (Information asset and Software License)	สารสนเทศที่อยู่ในสื่อบันทึกข้อมูล และลิขสิทธิ์ซอฟแวร์ เช่น ฐานชัดมูล ระบบงานต่างๆ ข้อมูลการทำงาน ลิขสิทธิ์สัญญาต่างๆ

ความมั่นคงปลอดภัยสารสนเทศ (Information Security)	ปัจจัยความมั่นคงปลอดภัยในที่นี้มี 3 ประการด้วยกันคือ 1. การรักษาความลับ (Confidentiality) 2. ความถูกต้องครบถ้วน (Integrity) 3. ความพร้อมใช้งาน (Availability) โดยสรุป ความมั่นคงปลอดภัยสารสนเทศ คือ การป้องกันรักษาสารสนเทศจากการเข้าถึง เพื่อการขโมย การเปลี่ยนแปลง ทำให้ใช้การไม่ได้ หรือการทำลายสารสนเทศโดยไม่ได้รับอนุญาต
งานเทคโนโลยีสารสนเทศ	งานใดๆ ที่เกี่ยวกับเทคโนโลยีสารสนเทศ ได้แก่ งานประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ การจัดเก็บข้อมูล การพัฒนาระบบงานและโปรแกรม การบำรุงรักษาและการรักษาความปลอดภัยทรัพยากรคอมพิวเตอร์ เช่น เครื่องคอมพิวเตอร์และอุปกรณ์ ระบบงาน และโปรแกรมระบบเครือข่ายและข้อมูล เป็นต้น
ช่องโหว่ (Vulnerability)	ช่องโหวในทรัพย์สินสารสนเทศที่อาจเกิดจากความบกพร่องในการผลิต หรือการออกแบบทำให้เกิดจุดอ่อน และมีความเสี่ยงในการคุกคามจากช่องโหว่ที่เกิดขึ้น เช่น ช่องโหว่ของโปรแกรมที่ทำให้บุคคลภายนอกสามารถเข้าใช้โปรแกรมได้โดยไม่ต้องผ่านการพิสูจนตัวตน
ทรัพย์สินสารสนเทศ (Information Asset)	หมายความถึง 1. ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์และระบบสารสนเทศ 2. ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3. ข้อมูลสารสนทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Area)	บริเวณที่ใช้เก็บรักษาอุปกรณ์สารสนเทศที่ใช้ในงานระบบสารสนเทศ แบ่งได้ 3 ประเภท คือ บริเวณ Patching, บริเวณปฏิบัติการคอมพิวเตอร์. ห้องคอมพิวเตอร์
พื้นที่ / บริเวณปฏิบัติการคอมพิวเตอร์ (Computer Operation)	พื้นที่ /บริเวณที่ใช้ในการป้อนข้อมูล ออกรายงาน และปฏิบัติงานเกี่ยวกับระบบงานสารสนเทศของบริษัทฯ

บริเวณ Patching Area	พื้นที่ที่ใช้เก็บอุปกรณ์ในการเชื่อมต่อ ระบบเครือข่ายคอมพิวเตอร์ ในแต่ละชั้นของบริษัทฯ
บัญชีผู้ใช้ (User name หรือ Account)	กลุ่มของข้อมูลที่ใช้ในการอ้างถึงเพื่อระบุตัวตน สิทธิการเข้าถึง และข้อจำกัดต่างๆ ในการเข้าถึงนั้น
บันทึกเหตุการณ์ (Logs)	บันทึกเหตุการณ์การใช้งานของระบบเทคโนโลยีสารสนเทศ การเข้าใช้งานระบบ การประมวลผล กิจกรรมของระบบสารสนเทศ และเหตุการณ์ทางด้านความมั่นคงปลอดภัยเพื่อตรวจสอบถึงประสิทธิภาพ ความปลอดภัย และความผิดปกติที่เกิดจากการประมวลผล กิจกรรมต่างๆของระบบสารสนเทศ
ประมวลผล (Process)	กระบวนการทำงานทางตรรกะของคอมพิวเตอร์
ประเมินความเสี่ยง (Risk Assessment)	การประเมินความเสี่ยง หรือ เหตุการณ์ที่อาจเกิดขึ้นได้ ซึ่งอาจเป็นอันตราย หรือคุกคามถึงความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
โปรแกรมที่ไม่พึงประสงค์ (Malicious Code or Malware)	โปรแกรม หรือ Code ที่เป็นอันตรายต่อประสิทธิภาพ และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ไม่ทางใดก็ทางหนึ่ง เช่น Virus Worm และ Trojan (ในที่นี้ขอใช้คำว่า Virus เพื่อความเข้าใจของผู้อ่าน)
แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)	การสร้างความต่อเนื่องทางธุรกิจ ป้องกันการติดขัด หรือการหยุดชะงักของระบบงานธุรกรรมที่สำคัญของบริษัท ซึ่งอาจมีสาเหตุมาจากภัยทางด้านสิ่งแวดล้อม เหตุการณ์ทางด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ หรือภัยคุกคามอื่นๆ
แผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRP: Disaster Recovery Plan)	การเตรียมความพร้อมรองรับเหตุฉุกเฉิน และแผนการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน เช่น การย้ายสถานที่ปฏิบัติงานไปจนถึงการใช้งานระบบสารสนเทศสำรอง
รหัสผ่าน (Password)	กลุ่มอักขระที่ในการพิสูจน์ตัวตนใช้เพื่อควบคุมการเข้าถึงระบบสารสนเทศ หรือข้อมูลสารสนเทศ
ระบบงานที่สำคัญ (High Priority Application System)	หมายถึง ระบบที่ให้บริการธุรกรรมหลักที่ใช้ในการให้บริการลูกค้า หรือระบบงานที่นำส่งข้อมูลรายงานแก่ทางการ (เช่น ธนาคารแห่งประเทศไทย, สำนักงาน กลต., ตลท.)

บันทึกการแก้ไข (Amendment record)

แก้ไขครั้งที่	หน้าที่	รายละเอียดการแก้ไข	วันที่แก้ไข
0	-	จัดทำครั้งแรก	28-Aug-2020
1	20-26	Data Classification Details	11-Sep-2021
2	-	ปรับปรุงประจำปี 2024	1-Jun-2024
3		เพิ่มเรื่องการทบทวนนโยบายประจำทุกปี	14-May-2025

สารบัญ

ระบบทดสอบ (User Acceptance Test Area)	ระบบสารสนเทศที่ใช้ในการทดสอบ โดยเป็นการจำลองทรัพยากรและสภาพแวดล้อมของระบบให้บริการจริงมา เพื่อทดสอบประสิทธิภาพ และความปลอดภัยของระบบที่ได้พัฒนาขึ้น
ข้อตกลงระดับของการให้บริการ (SLA - Service Level Agreement)	ข้อตกลงระหว่างบริษัท และผู้ให้บริการ ในการแสดงถึงประสิทธิภาพของการให้บริการตามที่ได้ตกลงไว้
ระบบพัฒนา (Development Area)	ระบบสารสนเทศที่ใช้ในการพัฒนาระบบงาน โดยเป็นการจำลองทรัพยากร และสภาพแวดล้อมของระบบให้บริการจริง เพื่อใช้พัฒนาระบบงานใหม่
ระบบสารสนเทศสำรอง (DRC: Disaster Recovery Center)	ระบบงาน ข้อมูล และระบบเครือข่ายสำรอง นอกเหนือจากระบบสารสนเทศหลัก เพื่อให้สามารถทำธุรกรรมหลักได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุการณ์ฉุกเฉิน
ระบบให้บริการจริง (Production Area)	ระบบสารสนเทศจริงที่ให้บริการแก่ผู้ใช้งาน ซึ่งต้องมีการรักษาความปลอดภัยและการควบคุมการเข้าถึงจากการพัฒนาระบบ และการทดสอบระบบอย่างเคร่งครัด
สิทธิ์พิเศษเฉพาะ (Privilege)	สิทธิ์พิเศษที่ใช้ในการปฏิบัติงานนอกเหนือจากสิทธิ์ทั่วไป เช่น ผู้ดูแลระบบ หรือ เจ้าของข้อมูลสารสนเทศ
สื่อบันทึกข้อมูล (Media)	สื่อที่ใช้ในการบันทึกข้อมูลในระบบงานสารสนเทศ โดยสามารถจำแนกเป็นสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เพื่อใช้ในการรักษาความลับของข้อมูล เช่น Tapes, Disks, Removable Hard Drives, CDs, DVDS, และ Printed Media และสื่อบันทึกข้อมูลทั่วไป เช่น กระดาษ และเครื่องคอมพิวเตอร์
ห้องคอมพิวเตอร์ (Data Center)	พื้นที่ที่ใช้เก็บอุปกรณ์คอมพิวเตอร์และเรื่องคอมพิวเตอร์หลักที่สำคัญในระบบงานของบริษัท เช่น เครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายหลัก
เหตุการณ์ทางด้านความมั่นคงปลอดภัย (Security Event and Incident)	เหตุการณ์ที่เกิดจากการเปลี่ยนแปลงระบบ สภาพแวดล้อม กระบวนการ ขั้นตอนปฏิบัติงาน หรือจากพนักงาน ซึ่งทำให้เกิดความเสี่ยงหรือการคุกคามถึงประสิทธิภาพ และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ หรือทรัพย์สินสารสนเทศ รวมไปถึง การโจมตีระบบและทำให้ระบบไม่สามารถทำงานได้อย่างปกติ และการถูกโจมตีโดยโปรแกรมใดๆที่ไม่ประสงค์ดี

7. นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

7.1. การสร้างนโยบายความมั่นคงปลอดภัยทางสารสนเทศ (Information Security Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยทางสารสนเทศของบริษัทเพื่อลดความเสี่ยงต่อความเสียหายทางทรัพย์สินและชื่อเสียงในการดำเนินธุรกิจของบริษัท และให้เป็นไปตามข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

- นโยบายความมั่งคงปลอดภัยทางสารสนเทศที่เป็นลายลักษณ์อักษร (Information Security Policy Documented) ต้องได้รับการอนุมัติจากคณะกรรมการบริษัทและเผยแพร่ให้พนักงานทั้งหมดได้รับทราบโดยทั่วกัน
- การทบทวนนโยบายความมั่นคงปลอดภัยทางสารสนเทศ (Review of the Information Security Policy) ต้องมีการทบทวนอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเพื่อให้สอดคล้องกับเทคโนโลยีที่ได้มีการพัฒนาหรือเปลี่ยนแปลงไป โดยกลุ่มบริการด้านเทคโนโลยีจะเป็นผู้ดำเนินการ
- นโยบายความมั่นคงปลอดภัยทางสารสนเทศฉบับที่เป็นปัจจุบัน (Current Version) ต้องมีการจัดเก็บให้ผู้ใช้งานสามารถข้าถึงได้โดยง่าย

7.2. การจัดโครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of Information Security)

วัตถุประสงค์

เพื่อให้ระบบเทคโนโลยีสารสนทศและอุปกรณ์ประมวลผลระบบสารสนเทศภายในบริษัท หรือที่ถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก ได้มีการบริหารจัดการอย่างมีความมั่นคงปลอดภัย

7.2.1. โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal Organization)

บริษัทให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัยโดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง และการเล็งเห็นความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ โดย

- **การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)** ต้องให้ความสำคัญและสนับสนุนต่อการบริหารจัดการด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นความถึงความสำคัญของหน้าที่และรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ
- **การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)** กำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆภายในบริษัท เพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศของบริษัท โดยจะต้องมีบทบาทและลักษณะงานรับผิดชอบที่แตกต่างกัน
- **การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)** จัดให้มีการกำหนดหน้าที่ความรับผิดชอบของพนักงานที่เกี่ยวข้อง ในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของบริษัทไว้อย่างชัดเจน
- **กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities)** กำหนดให้มีกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ
- **การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)** จัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับบริษัท ว่าจะไม่เปิดเผยความลับใดๆของบริษัท (โดยการลง

นามเป็นส่วนหนึ่งของการว่าจ้างพนักงาน) รวมทั้งเงื่อนไขหรือข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับ

- **การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with authorities)** กำหนดให้การติดต่อกับหน่วยงานราชการ หน่วยงานกำกับดูแล โดยผู้บริหารกลุ่มบริการด้านเทคโนโลยีต้องทำการติดต่อผ่ายฝ่ายกำกับการปฏิบัติงานและตรวจสอบภายใน ตามกฎเกณฑ์
- **การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)** จัดให้มีรายชื่อและข้อมูลสำหรับการติดต่อกับองค์กรหรือกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่มีความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ หรือหน่วยงานที่บริษัทต้องเกี่ยวข้อง
- **การทบทวนด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent review of information security)** ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการและการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบอิสระอย่างน้อยปีละ 1 ครั้งหรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อบริษัท

7.2.2. โครงสร้างทางด้านความมั่นคงปลอดภัยภายนอกองค์กร (External organization)

- **การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)** กำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงข้อมูลสารสนเทศ หรืออุปกรณ์ที่ใช้ ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้
- **การประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)** และกำหนดมาตรการรองรับหรือแก้ไขให้เหมาะสมก่อนที่จะอนุญาตให้ หน่วยงานภายนอกสามารถเข้าถึงได้
- **การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางสารสนเทศ (Addressing security when dealing with customers)** ต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับลูกค้าหรือผู้ใช้บริการ ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้
- **การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางสารสนเทศ (Addressing security when dealing with customers)** ระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยระหว่างองค์กรและหน่วยงานภายนอก ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

7.3. การบริหารจัดการทรัพย์สินสารสนเทศ (Asset management)

วัตถุประสงค์

เพื่อลดความเสี่ยงต่อการถูกเปิดเผยข้อมูลของบริษัทโดยไม่ได้รับอนุญาต ป้องกันการนำทรัพย์สินสารสนเทศไปใช้ โดยผิดวัตถุประสงค์และการเกิดความเสียหายกับทรัพย์สินสารสนเทศ ซึ่งจะทำให้บริษัทเกิดความเสียหายในการดำเนินธุรกิจได้

7.3.1. หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ (Responsibility for assets)

เพื่อให้มีการจัดทำบัญชีทรัพย์สินสารสนเทศอย่างเป็นระบบ และป้องกันการสูญหาย หรือการนำไปใช้โดยผิดวัตถุประสงค์โดยไม่มีผู้รับผิดชอบในทรัพย์สินสารสนเทศนั้น

- การจัดทำบัญชีทรัพย์สินสารสนเทศ (Inventory of assets) จัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญให้ถูกต้องอยู่เสมอ
- การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets) โดยเจ้าของบัญชีทรัพย์สินสารสนเทศที่ได้ระบุไว้ตามบัญชีทรัพย์สินสารสนเทศ มีหน้าที่ความรับผิดชอบในการดูแลรักษาทรัพย์สินสารสนเทศ
- การใช้งานทรัพย์สินสารสนเทศอย่างเหมาะสม (Acceptable use of IT Asset) การกำหนดแนวทาง และข้อห้ามในการใช้งานทรัพย์สินสารสนเทศ เพื่อให้มีการใช้งานทรัพย์สินสารสนเทศอย่างเหมาะสมเป็นไปตามข้อกำหนดทางกฎหมาย ลิขสิทธิ์ และหน่วยงานที่มีหน้าที่กำกับ รวมถึงเป็นการป้องกันการนำทรัพย์สินสารสนเทศไปใช้โดยผิดวัตถุประสงค์และป้องกันความเสียหายที่อาจเกิดขึ้น

7.3.2. การจัดหมวดหมู่สารสนเทศ (Information classification)

เพื่อให้มีการกำหนดระดับการรักษาความปลอดภัยและการจัดการของทรัพย์สินสารสนเทศได้อย่างเหมาะสม

- การจัดหมวดหมู่ (Classification guidelines) การจัดหมวดหมู่ทรัพย์สินสารสนเทศทั้งหมดของบริษัทตามระดับชั้นความสำคัญ มูลค่า และข้อกำหนดทางกฎหมาย เพื่อให้พนักงานสามารถเข้าใจถึงระดับความสำคัญของทรัพย์สินสารสนเทศ และนำไปจัดระดับการรักษาความปลอดภัยของข้อมูลต่อไป
- การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสาร

อิเล็กทรอนิกส์ และในการรักษาความปลอดภัย ของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

- 1.1) จัดแบ่งลำดับชั้นความลับของข้อมูล - ข้อมูลลับที่สุด (Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด - ข้อมูลลับมาก (Confidential) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง - ข้อมูลลับ หรือ ใช้ภายใน (Internal Use) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย - ข้อมูลทั่วไป หรือ สาธารณะ (Public) หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้
- 1.2) จัดแบ่งระดับชั้นการเข้าถึง - ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่ที่และลำดับชั้นในบังคับบัญชาในหน่วยงานนั้น - ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้หรือได้ทำการเผยแพร่ สำหรับผู้ใช้งานทั่วไป - ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิ์ที่ได้รับหมอบหมายตามอำนาจหน้าที่
- Data Classification Policy Details (แถลงนโยบาย)
  - สินทรัพย์ข้อมูล AUR ต้องได้รับการจัดประเภท ติดฉลาก และป้องกันอย่างเหมาะสม
- เหตุผลของนโยบาย/วัตถุประสงค์ นโยบายนี้จะอำนวยความสะดวกดังต่อไปนี้: -
  - ข้อมูลจะถูกแบ่งปันอย่างมีความรับผิดชอบกับพันธมิตร
  - ข้อมูลจะถูกเก็บไว้อย่างปลอดภัย
  - การรักษาความลับจะมั่นใจ
  - จะเป็นไปตามข้อกำหนดด้านกฎระเบียบและกฎหมาย
  - แผนความต่อเนื่องทางธุรกิจจะได้รับการจัดลำดับความสำคัญตามหมวดหมู่การจัดประเภทข้อมูล
  - การละเมิดการรักษาความลับทั้งหมดจะได้รับการประเมิน ตามการจัดประเภทข้อมูลที่ได้รับผลกระทบความรุนแรง
- ใครเป็นผู้อนุมัตินโยบายนี้ (CEO , VP – Information Technology)
- ใครจำเป็นต้องรู้นโยบายนี้ (AUR พนักงานทุกคน)
- นโยบาย/ขั้นตอน
  - 1. ข้อมูลทั้งหมดที่ป้อน จัดเก็บภายใน รายงานจากหรือขนส่งทางร่างกายหรือทางดิจิทัลผ่านเครือข่าย AUR, ระบบ, ระบบโฮสต์/เอาต์ซอร์ซหรือแผนกคือทรัพย์สินของ AUR

เว้นแต่จะมีข้อตกลงทางกฎหมาย/กฎหมายที่เกี่ยวข้องซึ่งจัดทำเอกสาร ความสัมพันธ์ที่แตกต่างกัน

- 2. ข้อมูล AUR ทั้งหมดแม้จะมีรูปแบบของข้อมูลจะต้องระบุและนับในสินค้าคงคลังระหว่างแต่ละหน่วยงาน/แผนก และสุดท้ายผ่านผู้ดูแลข้อมูล
- 3. ข้อมูล AUR ทั้งหมดต้องถูกจัดประเภทเป็นประเภทใดประเภทหนึ่งต่อไปนี้:
  - AUR CONFIDENTIAL – เกี่ยวข้องกับข้อมูลทั้งหมดที่มีความไวสูงสุดเนื่องจากความอ่อนไหวต่อเวลา ศักยภาพทางการเงินหรือการฉ้อโกงที่เป็นไปได้ ข้อมูลดังกล่าวรวมถึงทุกประเภทของข้อมูลที่สามารถระบุตัวตนได้ หมายเลขประกันสังคม เลขที่บัญชี เงินเดือนข้อมูลส่วนบุคคล รหัสผ่าน รหัส ลูกค้า สัมพันธ์/การมีส่วนร่วม และสัญญาที่อยู่ระหว่างการเจรจา
  - AUR Secret– เกี่ยวข้องกับข้อมูลทั้งหมดที่มีการประนีประนอมหรือแข่งขันได้ องค์ประกอบหรือความหมายโดยนัยสำหรับใช้ภายใน AUR อย่างเคร่งครัด ข้อมูลดังกล่าวรวมถึงข้อมูลทางการเงินขั้นพื้นฐาน ข้อมูลความปลอดภัยและการตรวจสอบ และข้อมูลที่เกี่ยวข้อง
  - AUR INTERNAL – เกี่ยวข้องกับข้อมูลทั้งหมดที่สร้างขึ้นโดยผู้ใช้แต่ละรายของระบบและไม่ได้หมายถึงการแบ่งปันกับผู้อื่นโดยทั่วไป ที่ไม่ได้รับอนุญาตการเปิดเผยข้อมูลนี้อย่างสมเหตุสมผลอาจคาดว่าจะทำให้ต่ำความเสียหายที่สำคัญต่อชื่อเสียงของ AUR การเงินหรือความสัมพันธ์กับลูกค้า เช่นข้อมูลและข้อมูลการสื่อสารที่ผู้สร้างตั้งใจไว้สำหรับ เฉพาะผู้ชมเท่านั้น
  - AUR PUBLIC – เกี่ยวข้องกับข้อมูลทั้งหมดที่ไม่ต้องการความรับผิดชอบเฉพาะและ/หรือเส้นทางการตรวจสอบสำหรับการใช้งาน การเปิดเผยข้อมูลนี้โดยไม่ได้รับอนุญาตจะไม่ก่อให้เกิดผลกระทบในทางลบต่อชื่อเสียง การเงิน หรือการมีส่วนร่วมของลูกค้าของ AURข้อมูลดังกล่าวรวมถึงข้อมูลที่ไม่ใช่เชิงกลยุทธ์เปิดเผยต่อสาธารณะข้อมูลหรือข้อมูลการสมัครที่ไม่เฉพาะเจาะจง
- 4. การจัดประเภทของข้อมูลเป็นอิสระจากเทคโนโลยีหรือแพลตฟอร์มที่เป็นอยู่ประมวลผล
- 5. สิทธิ์การเข้าถึงข้อมูลที่มอบให้แก่ผู้ใช้และผู้ดูแลควรมีความสอดคล้องกันในทุกกรณีพื้นที่ ควรให้ความสนใจเป็นพิเศษกับข้อมูลที่สามารถดาวน์โหลดหรือส่งออกได้

- 6. สิทธิ์ในการเข้าถึงข้อมูล การจำแนกประเภท และกลไกการรักษาความปลอดภัย/การป้องกันที่ยอมรับได้นั้นควบคุมโดยผู้ดูแลโดเมนข้อมูลและในที่สุดโดยผู้ดูแลข้อมูล ความปลอดภัยของข้อมูลบทบาทคือการประเมินและแนะนำการควบคุมที่เหมาะสม
- 7. ผู้บริหารเครื่องมือเทคโนโลยีสารสนเทศเป็นผู้ดูแลข้อมูลที่ได้รับมอบหมายแอปพลิเคชัน/บริการคอนเทนเนอร์ เว้นแต่ข้อมูลจะเกี่ยวข้องกับขอบเขตธุรกิจที่ได้รับอนุมัติ
- 8. ข้อมูลทั้งหมดต้องจัดประเภทตั้งแต่เริ่มต้นการรวบรวมข้อมูลและการพัฒนา.
- 9. ข้อมูลที่จัดระดับสูงกว่าสาธารณะจะต้อง:
  - ติดฉลากอย่างเหมาะสม
  - รูปแบบสุดท้ายออกจากระบบควรมีการติดฉลากที่เหมาะสม
  - ตรวจสอบโดยผู้จัดการที่เหมาะสม ผู้ดูแลผลประโยชน์ และความปลอดภัยของข้อมูลสำหรับ การใช้มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อควบคุมการเข้าถึงข้อมูลนี้
- 10. การทำเครื่องหมายควรสะท้อนถึงความไวของวัสดุในรูปแบบเอาต์พุตใดๆ เอาท์พุตรวมถึงรายงานที่พิมพ์ออกมา สื่อแม่เหล็ก ข้อความอิเล็กทรอนิกส์ และการถ่ายโอนไฟล์
- 11. ข้อมูลมักจะหมดความละเอียดอ่อนหลังจากช่วงระยะเวลาหนึ่ง เช่น เมื่อข้อมูลมีถูกเผยแพร่สู่สาธารณะ การจัดประเภทข้อมูลควรปรับปรุงตามความจำเป็น
- 12. การตระหนักรู้เกี่ยวกับการจัดหมวดหมู่ข้อมูลและการฝึกอบรมให้กับพนักงานและผู้ที่เกี่ยวข้องทั้งหมดหน่วยงานจะต้องดำเนินการอย่างสม่ำเสมอผ่านผู้ดูแลข้อมูล ผู้ดูแลโดเมนข้อมูล และความปลอดภัยของข้อมูล
- 13. ตามการจัดประเภทข้อมูล กลไก/กระบวนการเก็บรักษาและกำจัดที่เหมาะสมต้องพัฒนาและประยุกต์ใช้ กลไก/กระบวนการนี้ต้องได้รับอนุมัติจากสำนักงานรักษาความปลอดภัยข้อมูลและในที่สุดโดยผู้ดูแลข้อมูล

- ข้อยกเว้น
  - ข้อยกเว้นควรน้อยที่สุด หากมี ควรได้รับการอนุมัติจาก CEO และ VP-IT
- การบังคับใช้
  - ผู้ใช้รายใดที่พบว่าละเมิดนโยบายนี้ (หรือบางส่วน) อาจถูกลงโทษทางวินัยการดำเนินการจนถึงและรวมถึงการเลิกจ้าง
- การจัดป้ายชื่อและการจัดการทรัพย์สินสารสนเทศ (Information labeling and handling) การจัดทำป้ายชื่อทรัพย์สินสารสนเทศตามการจัดทำรหัสทรัพย์สินที่ระบุไว้ในบัญชีทรัพย์สิน

สารสนเทศที่อยู่ในความดูแลทั้งหมด ภายในสถานที่ที่ปฏิบัติงาน และต้องติดป้ายชื่อเพื่อแสดงถึงความเป็นทรัพย์สินของบริษัท

7.4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human resources security)

วัตถุประสงค์

เพื่อควบคุมการสรรหาบุคลากรเข้ามาปฏิบัติงานภายในบริษัท สร้างความตระหนักในการรักษาความมั่นคงปลอดภัย ป้องกันอันตรายที่อาจเกิดขึ้นจากพนักงานที่มีความไม่ประสงค์ดี ลดความเสี่ยงจากความเสียหายที่เกิดจากความรู้เท่าไม่ถึงการณ์ของพนักงาน รวมถึงการควบคุมการสิ้นสุดงานหรือเปลี่ยนตำแหน่งงาน

7.4.1. การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment)

เพื่อป้องกันอันตรายที่อาจเกิดขึ้นจากพนักงานที่มีความประสงค์ที่จะหาผลประโยชน์จากการเป็นพนักงานของบริษัทและลดความผิดพลาดเนื่องจากความรู้เท่าไม่ถึงการณ์ของพนักงาน

- การกำหนดหน้าที่รับผิดชอบของพนักงาน (Roles and responsibility) การกำหนดหน้าที่ความรับผิดชอบในการปฏิบัติงานต่างๆ และหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยซึ่งต้องแจ้งให้พนักงานทุกคนทราบ และลงนามเป็นลายลักษณ์อักษรก่อนเข้าปฏิบัติงาน ตามที่กำหนดในเงื่อนไขการจ้างงานอ้างอิงตามนโยบายฝ่ายบริหารทรัพยากรบุคคล
- การตรวจสอบคุณสมบัติ (Screening) อ้างอิงตามนโยบายฝ่าย[ริหารทรัพยากรบุคคล
- การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment) อ้างอิงตามนโยบายฝ่ายทรัพยากรบุคคล

7.4.2. การสร้างความมั่นคงปลอดภัยระหว่างการจ้างงาน (During employment)

เพื่อสร้างความตระหนักถึงภัยคุกคามและปัญหาทางด้านความมั่นคงปลอดภัยสารสนเทศ ป้องกันอันตรายที่สามารถเกิดขึ้นได้จากการไม่ปฏิบัติตามนโยบายของบริษัทหรือความรู้เท่าไม่ถึงการณ์

- หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities) การกำหนดให้มีผู้ประสานงานทางด้านความมั่นคงปลอดภัยแต่ละสายงาน มีหน้าที่ความรับผิดชอบในการรักษาความความมั่นคงปลอดภัยสารสนเทศในส่วนงานของตน
- การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education, and training) การสร้างความตระหนักใน

การรักษาความมั่นคงปลอดภัยให้บุคคลากร (Security Awareness) ให้ความรู้ทางด้านความมั่นคงปลอดภัยของสารสนเทศ โดยครอบคลุมถึงนโยบายและขั้นตอนปฏิบัติตามลักษณะงานที่พนักงานต้องรับผิดชอบ เพื่อป้องกันอันตรายที่สามารถเกิดขึ้นได้จากการไม่ปฏิบัติตามนโยบายของบริษัทหรือความรู้เท่าไม่ถึงการณ์

- กระบวนการทางวินัยเพื่อการลงโทษ (Disciplinary process) พนักงานที่ฝ่าฝืนหรือละเว้นการปฏิบัติตามนโยบายทางด้านเทคโนโลยีทางวินัย ตามลักษณะ หรือความหนักเบาของความผิดอ้างอิงตามวินัย และโทษทางวินัยของบริษัทอ้างอิงตามนโยบายของฝ่ายบริหารทรัพยากรบุคคล

7.4.3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination or change of employment)

เพื่อรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศและระบบสารสนเทศ ที่อยู่ในความครอบครองของพนักงานที่มีการสิ้นสุดหรือการเปลี่ยนตำแหน่งงาน

- การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination responsibilities) การสิ้นสุดงานหรือเปลี่ยนตำแหน่งงาน โดยผู้ที่สิ้นสุดการจ้างงาน หรือเปลี่ยนตำแหน่งนั้นต้องปฏิบัติตาม หน้าที่ความรับผิดชอบของพนักงานที่สิ้นสุดการจ้างงานหรือเปลี่ยนตำแหน่งงานในการสิ้นสุดหน้าที่ความรับผิดชอบในการทำงานของตน อ้างอิงตามนโยบายฝ่ายบริหารทรัพยากรบุคคล
- การคืนทรัพย์สิน (Return of assets) การสิ้นสุดงานหรือเปลี่ยนตำแหน่งโดยผู้ที่สิ้นสุดการจ้างงานหรือเปลี่ยนตำแหน่งนั้น ต้องปฏิบัติตามหน้าที่ความรับผิดชอบของพนักงานที่สิ้นสุดการจ้างงานหรือเปลี่ยนตำแหน่งงานในการคืนทรัพย์สินสารสนเทศของบริษัท ที่อยู่ในความครอบครองของตน เช่น บัตรพนักงานและคู่มือการปฏิบัติงานอ้างอิงตามนโยบายฝ่ายบริหารทรัพยากรบุคคล
- การถอดถอนสิทธิ์ในการเข้าถึง (Removal of access rights) การสิ้นสุดงานหรือเปลี่ยนตำแหน่งงานผู้ดูแลระบบงานสารสนเทศ ต้องทำการถอดถอนสิทธิ์ในการเข้าถึงทรัพย์สินสารสนเทศ และระบบสารสนเทศกรณีสิ้นสุดงาน หรือเปลี่ยนสิทธิการเข้าถึงกรณีเปลี่ยนตำแหน่งงาน ทันทีที่การสิ้นสุดตำแหน่งงานหรือการเปลี่ยนตำแหน่งงานนั้นมีผล

7.5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environment security)

วัตถุประสงค์

เพื่อควบคุมทรัพย์สินสารสนเทศและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนทศของบริษัททางด้านกายภาพ และการควบคุมการใช้งานและบำรุงรักษาอุปกรณ์สารสนทศ ให้ระบบสารสนเทศอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน ป้องกันการเข้าถึงทรัพย์สินสารสนเทศ หรือการถูกเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

7.5.1. บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)

การจัดทำบริเวณที่ต้องมีการรักษาความปลอดภัยของสารสนเทศ เพื่อเป็นการป้องกันการเข้าถึงทรัพย์สิน และโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศทางกายภาพ

- การจัดทำบริเวณล้อมรอบ (Physical security perimeter) การจัดทำบริเวณล้อมรอบบริเวณที่ต้องมีการรักษาความปลอดภัย (Secured Area) และจัดเป็นพื้นที่ควบคุม (Restricted Area)
- การควบคุมการเข้าออก (Physical entry controls) บริเวณที่ต้องมีการรักษาความปลอดภัยต้องมีการควบคุมการเข้าออก และอนุญาตให้ผ่านเข้าออกได้เฉพาะผู้ที่มีหน้าที่ปฏิบัติงานภายในพื้นที่หรือผู้ที่ได้รับอนุญาตตามความจำเป็นแล้วเท่านั้น สิทธิ์ในการเข้าถึงบริเวณที่ต้องมีการรักษาความปลอดภัยต้องมีการตรวจสอบความถูกต้องตามระยะเวลาที่กำหนด
- การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing offices, rooms and facilities) การสร้างความมั่นคงปลอดภัยในสำนักงาน และห้องทำงานโดยที่ฝ่ายบริหารสำนักงานเป็นผู้ควบคุมดูแลเกี่ยวกับอุปกรณ์ระบบความปลอดภัยรวมทั้งการบำรุงรักษา
- การป้องกันภัยคุกคามจากภายนอกและจากสิ่งแวดล้อม (Protecting against external and environmental threats) การป้องกันภัยคุกคามจากภายนอกและภัยจากสิ่งแวดล้อม โดยในบริเวณที่ต้องมีการรักษาความปลอดภัยที่ระดับความสำคัญสูงสุดคือ ห้องคอมพิวเตอร์ ต้องปฏิบัติตามในทุกข้อ และบริเวณที่ต้องมีการรักษาความปลอดภัยอื่นๆควรปฏิบัติ ตามความจำเป็นขึ้นอยู่กับการพิจารณา
- การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secured areas) มาตรการควบคุมการปฏิบัติงานในบริเวณที่ต้องมีการักษาความปลอดภัย และกระบวนการควบคุม

หน่วยงานภายนอกที่เข้ามาปฏิบัติงานภายในบริษัท โดยมีการกำหนดไว้ตามระเบียบปฏิบัติของบริษัทและมาตรการการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

- การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยหน่วยงานภายนอก (Public access, delivery and loading areas) การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก ให้แยกออกจากส่วนงานอื่นๆ และมีการควบคุมการทำงานโดยพนักงานของบริษัทตลอดการส่งมอบ

7.5.2. ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)

เพื่อรักษาความมั่นคงปลอดภัย ดูแลรักษาและซ่อมบำรุงให้อุปกรณ์สารสนเทศอยู่ในสภาพที่พร้อมใช้งาน ป้องกันการเสียหาย หรือการสูญหายของอุปกรณ์สารสนเทศ ซึ่งอาจนำไปถึงการรั่วไหลของข้อมูลสารสนเทศภายในบริษัท

- การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting utilities) การจัดวาง และการจัดเก็บอุปกรณ์ ของสำนักงาน หรือทรัพย์สินสารสนเทศ ให้มีความมั่นคงปลอดภัย เพื่อป้องกันภัยคุกคามทางด้านสิ่งแวดล้อม และความรู้เท่าไม่ถึงการณ์ของพนักงาน
- ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) การจัดให้มีอุปกรณ์สนับสนุนการทำงาน เพื่อป้องกันการล้มเหลวของอุปกรณ์สารสนเทศ และทุกระบบต้องมีแผนการบำรุงรักษาและตรวจสอบความพร้อมในการใช้งาน เพื่อรองรับภัยที่สามารถคิดขึ้นได้ตลอดเวลา
- การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling security) การเดินสายไฟฟ้า สายสื่อสาร และสายเคเบิลอื่นๆ ต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต
- การบำรุงรักษาอุปกรณ์ (Equipment maintenance) กำหนดแผนการบำรุงรักษา และตรวจสอบความพร้อมในการใช้งานอุปกรณ์สารสนเทศ ตามระยะเวลาที่กำหนด เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน
- การป้องกันอุปกรณ์สารสนเทศที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises) การป้องกันอุปกรณ์สารสนเทศต่างๆที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหาย โดยการสร้างความตระหนักถึงความสำคัญของการรักษาความปลอดภัยอุปกรณ์สารสนเทศ เพื่อป้องกันการเสียหายหรือการสูญหายของอุปกรณ์สารสนเทศ และการบำรุงรักษาอุปกรณ์
- การกำจัดอุปกรณ์ หรือนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or reuse of equipment) การตรวจสอบอุปกรณ์ และสื่อบันทึกข้อมูล โดยตรวจสอบถึงระดับความสำคัญของข้อมูลที่เก็บอยู่ในสื่อบันทึก เพื่อทราบวิธีการกำจัด เช่น ถูกลบทิ้งหรือถูกบันทึกทับก่อนที่จะทิ้ง

หรือนำอุปกรณ์ดังกล่าวกลับมาใช้ใหม่ เพื่อเป็นการป้องกันการรั่วไหลของข้อมูลสารสนเทศภายในบริษัท

- การนำทรัพย์สินสารสนเทศออกนอกสำนักงาน (Removal of property) การนำทรัพย์สินสารสนเทศออกนอกบริษัท ต้องเป็นพนักงานที่มีสิทธิ์ ต้องผ่านการอนุมัติจากผู้บริหารสายงานแล้วเท่านั้น และต้องทำบันทึกการนำออกโดยรวบรวมจัดทำเป็นรายงานตามรอบการจัดเก็บที่กำหนด เพื่อใช้ในการตรวจสอบย้อนหลัง

7.6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบสารสนเทศ (Communications and operations management)

วัตถุประสงค์

เพื่อให้การจัดการด้านการสื่อสารและการดำเนินงานต่างๆของเครือข่ายสารสนเทศต่างๆของบริษัทมีแนวทางปฏิบัติที่ชัดเจน และมีความมั่นคงปลอดภัยจึงให้มีวางแนวทางดำเนินการดังนี้

7.6.1. การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)

ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานสารสนเทศที่ชัดเจน เพื่อให้การดำเนินการต่างๆที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศของบริษัท เป็นไปอย่างถูกต้องและปลอดภัย รวมถึงต้องมีการกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบสารสนเทศ หรือระบบเครือข่ายอย่างชัดเจน

- กำหนดให้มีคู่มือปฏิบัติงานและขั้นตอนการทำงาน (Documented operating procedures) กลุ่มบริการด้านเทคโนโลยี มีหน้าที่จัดทำคู่มือปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศต่างๆ ของบริษัท และปรับปรุงตามระยะเวลาที่เหมาะสม
- การควบคุมการเปลี่ยนแปลง ปรับปรุงแก้ไขระบบสารสนเทศ หรืออุปกรณ์ประมวลผลสารสนเทศ (Change management) กลุ่มบริการด้านเทคโนโลยี มีหน้าที่ดูแลและควบคุมการเปลี่ยนแปลงในระบบสารสนเทศของบริษัท
- การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties) หน่วยงานเจ้าของระบบสารสนเทศและกลุ่มบริการงานเทคโนโลยี มีหน้าที่ร่วมกันกำหนดและแบ่งหน้าที่ความรับผิดชอบในการปฏิบัติงานเพื่อป้องกันการเข้าถึงสารสนเทศของบริษัท โดยไม่ได้รับอนุญาตหรือผิดวัตถุประสงค์
- การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการจริง (Separation of development, test, and operational facilities) กลุ่มบริการด้านเทคโนโลยีต้องจัดให้มีการ

แยกระบบพัฒนา (Development Area) ระบบทดสอบ (User Acceptance Area) และระบบให้บริการจริง (Production Area) ออกจากกันเพื่อลดความเสี่ยงในการเข้าถึงหรือการเปลี่ยนแปลงข้อมูลระบบสำหรับให้บริการโดยไม่ได้รับอนุญาต โดยบุคคลภายนอกหรือผู้ให้บริการใดๆ สามารถเข้าถึงได้เฉพาะระบบพัฒนาและระบบทดสอบเท่านั้นไม่มีสิทธิ์ในการเข้าถึงระบบให้บริการจริง

7.6.2. การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management)

เพื่อรักษาระดับความปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอก ให้เป็นไปตามข้อตกลงที่ได้ทำไว้ระหว่างบริษัทกับหน่วยงานภายนอก

- การให้บริการโดยหน่วยงานภายนอก (Service delivery) กลุ่มบริการด้านเทคโนโลยีต้องกำกับและดูแลให้มีการจัดทำข้อกำหนด หรือข้อตกลงในการรับบริการจากหน่วยงานภายนอก
- การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and review of third party services) กลุ่มบริการด้านเทคโนโลยี ต้องกำกับและดูแลให้มีการตรวจสอบรายงาน หรือบันทึกการให้บริการ ที่จัดทำขึ้นโดยหน่วยงานภายนอกที่ให้บริการอย่างสม่ำเสมอ เพื่อตรวจสอบความถูกต้องในการให้บริการ ให้เป็นไปตามข้อตกลง
- การบริหารจัดการการเปลี่ยนแปลงในการให้บริการของผู้ให้บริการภายนอก (Managing changes to third party services) การเปลี่ยนแปลงต่อระบบ หรือบริการที่รับผิดชอบโดยหน่วยงานภายนอก กลุ่มบริหารด้านเทคโนโลยี ต้องดูแลให้มีการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอก เมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบ หรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก

7.6.3. การวางแผนและตรวจรับทรัพย์สินสารสนเทศ (System planning and acceptance)

เพื่อให้มีแนวทางในการวางแผนจัดการทรัพยากรบนระบบสารสนเทศ และเกณฑ์ในการตรวจรับระบบสารสนเทศเพื่อลดความเสี่ยงในการล้มเหลวของระบบสารสนเทศ

- การวางแผนเพื่อกำหนดความต้องการใช้ทรัพยากร (Capacity management) ระบบสารสนเทศใดๆ ต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนทศที่คาดว่าจะต้องมี เพื่อรองรับในปัจจุบันและต่อเนื่องในอนาคต หรือใช้ในการขยายตัวของธุรกิจของบริษัท เพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งานในอนาคต อย่างสม่ำเสมอทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

- การตรวจรับระบบ (System acceptance) ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้ง ต้องดำเนินการทดสอบก่อนที่จะรับระบบเสมอ

7.6.4. การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code)

เพื่อให้มีการป้องกันระบบสารสนเทศและข้อมูลให้ปลอดภัยจากการโจมตีของโปรแกรมที่ไม่พึงประสงค์ดี(Malicious code or Malware) จึงต้องมีมาตรการป้องกันระบบสารสนเทศของบริษัทดังนี้

- การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Control against malicious code) กำหนดให้มีระบบหรือเครื่องมือสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดีรวมทั้ง ต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย
- การป้องกันโปรแกรมเคลื่อนที่ (Control against mobile code) จัดให้มีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ โปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่งเพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง)

7.6.5. การสำรองข้อมูล (Backup)

เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของระบบสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศจึงกำหนดให้มี

- การสำรองข้อมูล (Information backup) ข้อมลสารสนเทศของบริษัทต้องมีการสำรองข้อมูลและทดสอบการกู้คืนข้อมูลรวมถึงสถานที่สำรองเก็บไว้ตามนโยบายระบบสารสนเทศสำรอง และแผนรองรับกรณีเกิดเหตุฉุกเฉิน

7.6.6. การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)

กำหนดให้มีมาตรการเพื่อผ้องกันภัยคุกคามต่างๆ ทางเครือข่ายคอมพิวเตอร์ และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศที่ใช้งานเครือข่าย รวมถึงข้อมูลต่างๆที่สงผ่านทางเครือข่าย

- มาตรการทางเครือข่าย (Network controls) กำหนดให้มีมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่ายคอมพิวเตอร์ และดูแลรักษาความมั่นคงปลอดภัย สำหรับระบบสารสนเทศที่ใช้งานเครือข่ายรวมไปถึงข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่าย
- ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services) การกำหนดการรักษาความมั่นคงปลอดภัยระดับการให้บริหาร และการบริหารจัดการเครือข่ายคอมพิวเตอร์

ทั้งหมดของบริษัท รวมทั้งบริการเครือข่ายภายนอกและบริการเชื่อมต่อเครือข่ายภายในจากภายนอก (Remote Access)

7.6.7. การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling)

เพื่อควบคุมการใช้งาน และการดูแลรักษาสื่อบันทึกข้อมูลที่มีข้อมูลสารสนเทศของบริษัทจากการถูกเปิดเผยเปลี่ยนแปลงแก้ไข การลบหรือการทำลายโดยไม่ได้รับอนุญาตและป้องกันการติดขัดหรือหยุดชะงักทางธุรกิจ อันเนื่องจากข้อมูลสารสนเทศบกพร่อง

- การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media) สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable media) ให้ตระหนักถึงข้อมูลว่าถูกทำลายจริง และไม่สามารถนำกลับมากู้ข้อมูลได้อีก เพื่อลดความเสี่ยงในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- การทำลายสื่อบันทึกข้อมูล (Disposal of media) การทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานแล้วหรือหมดอายุการใช้งาน ให้ตระหนักถึงข้อมูลว่าถูกทำลายจริง และไม่สามารถนำกลับมากกู้ข้อมูลได้อีก เพื่อลดความเสี่ยงในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ขั้นตอนปฏิบัติสำหรับการจัดการข้อมูลสารสนเทศ (Information handling procedures) กำหนดให้มีขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์
- การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation) จัดใช้มีการป้องกันเอกสารระบบ หรือข้อมูลเกี่ยวกับระบบงานที่มีความสำคัญจากการเข้าถึงโดยไม่ไดรับอนุญาต

7.6.8. การแลกเปลี่ยนสารสนเทศ (Exchange of information)

การควบคุมการแลกเปลี่ยนสารสนเทศเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลที่มีการแลกเปลี่ยนกัน ทั้งภายในบริษัทและการแลกเปลี่ยนกับหน่วยงานภายนอก

- นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures) กำหนดให้ขั้นตอนปฏิบัติ และมาตรการรองรับเพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร เช่น หน่วยงานภายนอก โดยผ่านช่องทางการสื่อสารทุกชนิด
- ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreement) การแลกเปลี่ยนสารสนเทศใดๆ กับหน่วยงานภายนอกต้องมีการจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศระหว่างบริษัท และ

หน่วยงานภายนอก และมีการลงนามอย่างเป็นลายลักษณ์อักษร เช่น การลงนามไม่เผยแพร่ความลับ (Non-disclosure agreement)

- การส่งสื่อบันทึกข้อมูลออกไปนอกบริษัท (Physical media in transit) การส่งสื่อบันทึกข้อมูลสารสนเทศกับหน่วยงานภายนอกต้องกำหนดให้มีการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานผิดวัตถุประสงค์และการทำให้ข้อมูลเกิดความเสียหาย
- การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging) ให้มีมาตรการป้องกันข้อมูลในการส่งข้อความทางอิเล็กทรอนิกส์ จากการเข้าถึงโดยไม่ได้รับอนุญาต และการแก้ไขเปลี่ยนแปลงข้อมูล ตัวอย่างเช่น วิธีการใช้งาน E-mail อย่างเหมาะสมตามระเบียบการใช้งานทรัพย์สินสารสนเทศอย่างเหมาะสม
- ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems) ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน คือ การใช้งานข้อมูล หรือระบบสารสนเทศร่วมกัน ระหว่างบริษัทและหน่วยงานภายนอกผ่านการสื่อสารเส้นทางต่างๆ เช่น เอกสาร, เครือข่ายคอมพิวเตอร์ โทรศัพท์โทรสาร, การส่งทางไปรษณีย์ E-mail, Voice Mail โดยระบบสารสนทศทางธุรกิจที่เชื่อมโยงกันต้องมีการระบุกลุ่มผู้ใช้งานและสิทธิในการเข้าถึงข้อมูลของหน่วยงานภายนอกให้ชัดเจน และกำหนดวิธีการป้องกันการเข้าถึงระบบสารสนเทศ หรือข้อมูลสารสนเทศอื่นๆของบริษัทที่ไม่ต้องการให้หน่วยงานภายนอกเข้าถึงได้

7.6.9. การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)

เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) และ การทำธุรกรรมออนไลน์ (Online transactions) ส่วนใหญ่มีการส่งผ่านข้อมูลผ่านเครือข่ายสาธารณะจึงต้องมีการกำหนดการบริหารจัดการที่เหมาะสม เพื่อเป็นการรักษาความปลอดภัยของข้อมูล และลดความเสี่ยงในการเข้าถึงข้อมูลที่มีความสำคัญโดยไม่ได้รับอนุญาต

- การพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) กำหนดให้มีมาตรการในการใช้งานและป้องกันระบบพาณิชย์อิเล็กทรอนิกส์ที่มีการส่งผ่านทางเครือข่ายสาธารณะ หรืออินเทอร์เน็ต (Internet) เพื่อการป้องกันข้อมูลสารสนเทศจากการเข้าถึง หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต
- การทำธุรกรรมออนไลน์ (Online transactions) กำหนดให้มีมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่งที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศ ที่รับ-ส่งสารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่าย การเปลี่ยนแปลง

สารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาตหรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต

- สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly available information) เพื่อป้องกันการเข้าถึงและแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

7.6.10. การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

เพื่อตรวจสอบความผิดปกติจากการใช้ระบบสารสนเทศ โดยไม่ได้รับอนุญาต หรือผิดวัตถุประสงค์

- การบันทึกเหตุการณ์การใช้งานระบบ (Audit logging) กำหนดให้มีการบันทึกเหตุการณ์ (Logging) ของระบบสารสนเทศต่างๆ ครอบคลุมถึง การเข้าใช้งานระบบสารสนเทศ การปฏิเสธการให้บริการของระบบและเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้
- การตรวจสอบการใช้งานระบบ (Monitoring system use) กำหนดให้มีขั้นตอนปฏิบัติเพื่อตรวจสอบการใช้งานระบบสารสนเทศอย่างสม่ำเสมอ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่ และป้องกันการถึงโดยไม่ได้รับอนุญาต
- การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information) ระบบและข้อมูลที่ทำการบันทึก (Logging) ต้องมีการจำกัดสิทธิการเข้าถึง และป้องกันการเปลี่ยนแปลง หรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาตไม่ว่ากรณีใดๆ ทั้งสิ้น
- บันทึกการดำเนินงานของผู้ดูแลระบบ (Administrator and operator logs) การดำเนินงานใดๆ ของผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบต้องถูกบันทึกไว้ และต้องมีการป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อมูลด้วยเช่นกัน
- การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging) ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้นและติดตามดำเนินการแก้ไข
- การตั้งเวลาของอุปกรณ์คอมพิวเตอร์ให้ตรงกัน (Clock synchronization) ต้องตั้งเวลาของอุปกรณ์คอมพิวเตอร์ทุกเครื่องให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากอุปกรณ์คอมพิวเตอร์ถูกบุกรุกหรือเกิดปัญหาใดๆ ขึ้น

7.7. การควบคุมการเข้าถึงทรัพย์สินสารสนเทศ (Access control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงทรัพย์สินสารสนเทศ ครอบคลุมถึงการควบคุมการเข้าถึงระบบเครือข่ายภายในบริษัทหลัก ระบบปฏิบัติการ และ Application ต่างๆของระบบสารสนเทศโดยมีการกำหนดในเรื่องของการพิสูจน์ตัวตน และพิสูจน์สิทธิป้องกันการเข้าถึงระบบสารสนเทศ และข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

7.7.1. ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)

เพื่อให้มีรูปแบบการกำหนดสิทธิในการเข้าถึงทรัพย์สินสารสนเทศในระบบงานสารสนเทศทุกระบบ ให้ไปในทิศทางเดียวกันและเป็นไปตามข้อกำหนดในการใช้งานของธุรกิจของบริษัท

- กำหนดให้มีการควบคุมการเข้าถึงระบบ (Access control policy) อย่างเป็นลายลักษณ์อักษร (Documented operating procedures) และต้องมีการปรับปรุงตามระยะเวลาอันสมควร

7.7.2. การบริหารจัดการการเข้าถึงของผู้ใช้ (Use access management)

เพื่อควบคุมการให้สิทธิการเข้าถึงแก่พนักงาน และการจัดการรหัสผ่านที่ใช้ในการเข้าถึงของระบบสารสนเทศ ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- การลงทะเบียนพนักงาน (User registration) การกำหนดแนวทางปฏิบัติงานเรื่องการลงทะเบียนพนักงาน หรือการให้สิทธิ์ในการเข้าถึงระบบสารสนเทศ
- การบริหารจัดการสิทธิการใช้งานระบบ (privilege management) การจัดการสิทธิเฉพาะในการใช้งานระบบตามความจำเป็นในการใช้งานของผู้ใช้ในแต่ละบัญชีผู้ใช้ (User ID)
- การบริหารจัดการรหัสผ่าน (User password management) การจัดสรรรหัสผ่านสำหรับผู้ใช้งาน และการดูแลรักษารหัสผ่านให้มีความมั่นคงปลอดภัย
- การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) มีกระบวนการทบทวนสิทธิการเข้าถึงของระบบสารสนเทศระบบงานที่สำคัญอย่างเป็นทางการ เพื่อป้องกันการให้สิทธิพนักงานเกินกว่าที่จำเป็น และการเปลี่ยนแปลงสิทธิโดยไม่ได้รับอนุญาต

7.7.3. หน้าที่ความรับผิดชอบของผู้ใช้งาน (Use responsibilities)

เพื่อกำหนดความรับผิดชอบในการใช้งานสิทธิการเข้าถึงข้อมูลสารสนเทศ และระบบสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต หรือการใช้งานผิดวัตถุประสงค์

- การใช้งานรหัสผ่านสำหรับผู้ใช้งาน (Password use) พนักงานที่มีสิทธิในระบบสารสนเทศใดๆ ของบริษัท ต้องเก็บรักษารหัสผ่านเป็นความลับ และกำหนดรหัสผ่านให้ยากต่อการคาดเดา
- การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment) การป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานส่วนกลางที่ไม่มีพนักงานดูแล
- นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy) ผู้ใช้งานมีหน้าที่ควบคุมไม่ให้มีการปล่อยทรัพย์สินสารสนทศที่สำคัญอยู่ในสถานที่ที่ไม่ปลอดภัย เช่น การป้องกันไม่ให้เอกสารหรือสื่อบันทึกข้อมูลอยู่ในพื้นที่ที่สามารถเข้าถึงได้โดยบุคคลภายนอก

7.7.4. การควบคุมการเข้าถึงเครือข่าย (Network access control)

เพื่อควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ของบริษัท และป้องกันการเข้าถึงบริการทางเครือข่ายและข้อมูลสารสนเทศที่มีการส่งผ่านเครือข่ายโดยไม่ได้รับอนุญาต

- นโยบายการควบคุมการใช้งานบริการเครือข่าย (Policy on use of network services) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ รวมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ หรือบริการใดไม่สามารถใช้งานได้
- การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections) ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้
- กำหนดให้มีการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks) เป็นการบ่งบอกการเชื่อมต่อของอุปกรณ์บนเครือข่าย เพื่อให้ทราบว่าการเชื่อมต่อมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้วจริง (Automatic Equipment identification)
- กำหนดให้มีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) มาตรการการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ โดยต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย
- กำหนดให้ทำการแบ่งแยกเครือข่าย (Segregation in networks) การแบ่งแยกเครือข่ายตามกลุ่มของข้อมูลสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ตามการดำเนินงานทางธุรกิจ และกลุ่มของระบบสารสนเทศ เช่น การแบ่งแยกเครือข่ายภายใน กับเครือข่ายภายนอก การแบ่งเครือข่ายตามกลุ่มระดับความสำคัญของข้อมูล หรือเครือข่ายไร้สาย เพื่อกำหนดระดับการรักษาความปลอดภัยให้เหมาะสมกับความเสี่ยงที่เกิดขึ้นในแต่ละกลุ่ม

- กำหนดให้ควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่าย และการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นตามการควบคุมการเข้าถึง

7.7.5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

เพื่อควบคุมการเข้าถึงข้อมูลและการเปลี่ยนแปลงข้อมูลของระบบปฏิบัติการโดยไม่ได้รับอนุญาต

- ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures) สำหรับการเข้าถึงหรือการใช้งานระบบปฏิบัติการ
- การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication) เพื่อการระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ
- ระบบบริหารจัดการรหัสผ่าน (Password management system) ระบบสารสนเทศที่มีระบบการพิสูจน์ตัวตนในรูปแบบบัญชีผู้ใช้และรหัสผ่าน ต้องมีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมต่างๆ
- การใช้งานโปรแกรมประเภท Utility (Use of system utilities) การจำกัดและควบคุมการใช้งานโปรแกรมประเภท Utility ต่างๆ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้
- การหมดเวลาการใช้งานระบบสารสนเทศ (Session time out) การจำกัดเวลาในการใช้งานระบบสารสนเทศ เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่ง เช่น ระบบตัดการใช้งานอัตโนมัติ

7.7.6. การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)

เพื่อลดความเสี่ยงในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูลผ่านระบบงานสารสนเทศ โปรแกรม Utility ซอฟต์แวร์ระบบปฏิบัติการ และโปรแกรมไม่ประสงค์ดี

- การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) การจำกัดการเข้าถึงข้อมูลสารสนเทศของระบบงานต่างๆ โดยการเข้าถึงจะต้องแยกตามความจำเป็นตามหน้าที่ของผู้ใช้งาน
- การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation) การแยกระบบสารสนเทศที่มีระดับความสำคัญที่มีระดับความสำคัญสูง เพื่อกำหนดระดับการควบคุม และการรักษาความมั่นคง ปลอดภัยตามระดับความสำคัญของข้อมูล

7.7.7. การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานภายนอกองค์กร (Mobile computing and teleworking)

การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอก เพื่อลดความเสียงในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ลดการรั่วไหลของข้อมูล

- การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communication) อุปกรณ์สื่อสารประเภทพกพา คือ อุปกรณ์สื่อสารที่สามารถประมวลผล บันทึกข้อมูล และเชื่อมต่อเครือข่ายได้ เช่น Notebooks, Tablet, Smart-Phones และอุปกรณ์อื่นๆที่สามารถทำงานลักษณะคล้ายคลึงอุปกรณ์เหล่านี้ ให้พิจารนาเพิ่มขั้นตอนปฏิบัติงานที่มีความมั่นคงปลอดภัยมากกว่าอุปกรณ์สารสนเทศทั่วไป โดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์ทีใช้เชื่อมต่อ
- การปฏิบัติงานภายนอกสำนักงาน (Teleworking) คือ การปฏิบัติงานโดยเชื่อมต่อระบบเครือข่ายจากสถานที่ภายนอกบริษัทเข้าสู่ระบบเครือข่ายภายใน โดยทั่วไปแล้วจะทำผ่านอินเทอร์เน็ต โดยมีการใช้งานการเชื่อมต่อที่มีความมั่นคงปลอดภัย เช่น Virtual Private Network (VPN)

7.8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information system acquisition, development and maintenance)

วัตถุประสงค์

เพื่อควบคุมการบริหารจัดการข้อมูลภายในการประมวลผลระบบสารสนเทศ การป้องกันข้อมูลไฟล์ของระบบ และข้อมูลที่ใช้ในการทดสอบระบบ มาตรการจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ และการจัดการช่องโหวในฮาร์ดแวร์และซอฟต์แวร์เพื่อป้องกันความผิดพลาดที่เกิดจากการจัดหา พัฒนา และการประมวลผลข้อมูลสารสนเทศ

7.8.1. ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information systems)

เพื่อให้ระบบสารสนเทศมีการจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยที่เป็นมาตรฐานเดียวกันในบริษัท

- การระบุข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัย (Security requirements analysis and specification) การวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่หรือระบบที่ปรับปรุงจากระบบเดิม โดยให้ยึดปฏิบัติตามนโยบายการจัดหา ติดตั้งระบบงานคอมพิวเตอร์

7.8.2. การแก้ไขความถูกต้อง ในการประมวลผลระบบงานสารสนเทศ (Correct processing in applications)

เพื่อป้องกันความผิดพลาด การสูญหายของข้อมูลสารสนเทศ จากการทำงาน การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์

- การตรวจสอบข้อมูลนำเข้า (Input data validation) การกำหนดกลไกสำหรับตรวจสอบข้อมูลนำเข้าสู่ระบบงานสารสนเทศว่าข้อมูลนั้นมีความถูกต้องและปลอดภัยก่อนที่จะนำไปประมวลผล
- การตรวจสอบข้อมูลที่อยู่ในระหว่างประมวลผล (Control internal processing) การกำหนดกลไกสำหรับตรวจสอบข้อมูลในระหว่างการประมวลผล สถานะ การทำงาน เพื่อป้องกันความเสียหาย หรือความผิดพลาดที่อาจเกิดขึ้นได้ ลดความล้มเหลว และความคลาดเคลื่อนของข้อมูลที่อาจเกิดขึ้น
- การตรวจสอบความถูกต้องของข้อความ (Message integrity) การกำหนดกลไกสำหรับตรวจสอบความถูกต้องของข้อความในระบบงานสารสนเทศรวมถึงมาตรการเพื่อป้องกันการเปลี่ยนแปลง เพิ่มเติมหรือลบข้อความโดยไม่ได้รับอนุญาต
- การตรวจสอบข้อมูลส่งออก (Output data validation) การกำหนดกลไกสำหรับตรวจสอบข้อมูลนำออกจากระบบงานสารสนเทศ หรือผลลัพธ์ที่ได้จากการประมวลผลเสร็จสิ้น เพื่อเป็นการตรวจสอบความถูกต้องของการประมวลผล และลดความเสี่ยงในความคลาดเคลื่อนของข้อมูล

7.8.3. มาตรการการเข้ารหัสลับข้อมูล (Cryptographic controls)

ให้มีการเข้ารหัสลับ(Cryptography or Encryption) และใช้กุญแจ (Key) ที่ใช้ในกระบวนการเข้ารหัสลับเพื่อรักษาความลับของข้อมูลยืนยันตัวตนของผู้ส่งข้อมูลและรักษาความถูกต้องของข้อมูล

- นโยบายการเข้ารหัสลับข้อมูล (Policy on the use of cryptographic control) การกำหนดให้มีการเข้ารหัสลับข้อมูลในการเก็บรักษาข้อมูลและการสื่อสารผ่านเครือข่าย
- การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key management) การบริหารจัดการกุญแจที่ใช้ในการเข้ารหัสลับ หรือถอดรหัสลับในการใช้งานเทคนิคการเข้ารหัสข้อมูลต่างๆ เพื่อป้องกันการเปลี่ยนแปลง สูญหาย หรือการถูกทำลาย

7.8.4. การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files)

การสร้างความมั่นคงให้กับไฟล์ของระบบที่ให้บริการของระบบสานสนเทศ ในการปฏิบัติงานใดๆที่เกี่ยวข้อง เช่น การติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ และการใช้ข้อมูลในการทดสอบ

ระบบ เพื่อป้องกันการเข้าถึงไฟล์ของระบบที่ให้บริการโดยไม่ได้รับอนุญาต และลดความเสี่ยงในการเกิดความเสียหายจากความผิดพลาดที่อาจเกิดขึ้นได้

- การควบคุมการปฏิบัติงานที่เกี่ยวข้องกับการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software) จัดให้มีขั้นตอนปฏิบัติเพื่อควบคุมการปฏิบัติงานที่เกี่ยวข้องกับการติดตั้งซอฟต์แวร์ต่างๆลงในระบบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดความเสียหายจากความผิดพลาดที่อาจเกิดขึ้นได้
- การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of system test data) จัดให้มีการป้องกันและควบคุมการใช้งานในการทดสอบระบบ (Test) และการกำหนดมาตรการในการทดสอบระบบเพื่อป้องกันการเปลี่ยนแปลง และความเสียหายของข้อมูล
- การควบคุมการเข้าถึง Source Code สำหรับระบบ (Access control to program source code) ต้องจำกัดและควบคุมการเข้าถึง Source Code สำหรับระบบให้บริการจริง เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ซึ่งอาจนำมาสู่ความเสียหายต่อระบบสารสนเทศที่ให้บริการ

7.8.5. การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in development and support processes)

การระบุข้อกำหนดในการพัฒนาระบบสารสนเทศ และกระบวนการสนับสนุนการทำงาน เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

- ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลง ปรับปรุงแก้ไขระบบ (Change control procedures) การกำหนดขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปล ปรับปรุงแก้ไขระบบสารสนเทศ ในการพัฒนาระบบ เพื่อลดความเสี่ยงในการเกิดความเสียหายจากความผิดพลาดที่เกิดขึ้น โดยการเปลี่ยนแปลงมีขั้นตอนให้ปฏิบัติตามนโยบายการควบคุมการเปลี่ยนแปลงระบบงานคอมพิวเตอร์
- การตรวจสอบการทำงานของ Application ภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes) การกำหนดให้มีการตรวจสอบ และทดสอบ การทำงานของ Application หลังจากเปลี่ยนแปลงระบบปฏิบัติการ เพื่อตรวจสอบความสมบูรณ์ในการประมวลผลของระบบสารสนเทศ และป้องกันปัญหาที่เกิดจากการเปลี่ยนแปลง
- การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์สำเร็จรูป (Restrictions on changes to software packages) การจำกัดและการกำหนดมาตรการควบคุมการเปลี่ยนแปลงปรับปรุงแก้ไขซอฟต์แวร์สำเร็จรูปเพื่อป้องกันความเสียหายของระบบสารสนเทศ

- การป้องกันการรั่วไหลของสารสนเทศ (Information leakage) กำหนดมาตรการป้องกันการรั่วไหลของสารสนเทศ โดยให้มีการปฏิบัติในการจัดการกับข้อมูล ตามนโยบายการรักษาความปลอดภัยด้านสารสนเทศเพื่อลดความเสี่ยงจากการรั่วไหลของข้อมูลสารสนเทศที่มีความสำคัญ ซึ่งอาจทำให้เกิดความเสียหายได้
- การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development) การควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก เพื่อป้องกันการได้มาซึ่งซอฟต์แวร์ที่ไม่ได้มาตรฐาน ไม่ตรงกับความต้องการ หรือไม่มีประสิทธิภาพ และความปลอดภัยในการใช้งาน

7.8.6. การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

การจัดการช่องโหว่ (Vulnerability) ในฮาร์ดแวร์และซอฟต์แวร์ เพื่อลดความเสี่ยงจากการคุกคามของผู้ไม่ประสงค์ดีโดยอาศัยช่องโหว่ที่มีในระบบสารสนเทศของบริษัท

- มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities) การติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆที่ใช้งาน เพื่อประเมินความเสี่ยงของช่องโหว่ รวมถึงการกำหนดมาตรการเพื่อลดความเสี่ยงที่อาจเกิดขึ้น

7.9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information security incident management)

วัตถุประสงค์

เพื่อจัดการเหตุการณ์ทางด้านความมั่นคงปลอดภัย เรียนรู้ข้อผิดพลาดจากปัญหาที่เกิดขึ้น และปรับปรุงแก้ไข ซึ่งเป็นการป้องกันการเกิดเหตุการณ์ทางด้านความมั่นคงปลอดภัยในครั้งต่อไป

7.9.1. การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information on security events and weaknesses)

เพื่อให้มีการรายงานเหตุการณ์ทางด้านความมั่นคงปลอดภัย และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย ป้องกัน หรือลดผลกระทบที่เกิดจากเหตุการณ์

- การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information on security events) การรายงานเหตุการณ์ทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศและการจัดการต่อเหตุการณ์นั้นอย่างรวดเร็วและมีประสิทธิภาพ โดยผ่านช่องทางการรายงานที่กำหนดไว้

- การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting on security weakness) การรายงานจุดอ่อนทางด้านความมั่นคงปลอดภัย ที่เกี่ยวข้องกับช่องโหว่ระบบสารสนเทศ บริการที่ใช้งานอยู่และการป้องกันความเสี่ยงที่เกิดจากจุดอ่อนนั้น

7.9.2. การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องความมั่นคงปลอดภัย (Management information security incidents and improvements)

เพื่อให้มีการบริหารจัดการปรับปรุงแก้ไข และเรียนรู้เหตุการณ์ทางด้านความมั่นคงปลอดภัยสารสนเทศ ป้องกัน หรือลดผลกระทบจากเหตุการณ์ที่เกิดขึ้น

- หน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Responsibilities and procedures) กำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน เพื่อรับมือกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศได้อย่างรวดเร็ว
- การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents) การเรียนรู้จากเหตุการณ์และเตรียมการป้องกันการเกิดเหตุการณ์ในครั้งต่อไป จากบันทึกเหตุการณ์ทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ และรายงานการจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ทางด้านความมั่นคงปลอดภัย
- การเก็บรวบรวมหลักฐาน (Collection of evidence) เหตุการณ์ทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ที่เกี่ยวข้องกับการดำเนินการทางกฎหมาย กลุ่มงานบริการด้านเทคโนโลยีต้องมีการรวบรวมและจัดเก็บหลักฐาน ตามกฎหรือหลักเกณฑ์อ้างอิงในกระบวนการทางกฎหมายที่เกี่ยวข้อง

7.10. การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)

วัตถุประสงค์

เพื่อป้องกันการติดขัดหรือหยุดชะงักของการทำธุรกรรมต่างๆของบริษัท และป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถระบบกลับคืนมาได้ในระยะเวลาอันเหมาะสม

7.10.1. หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงาน (Information security aspects of business continuity management)

การกำหนดแผนบริหารความต่อเนื่องทางธุรกิจ การป้องกันการติดขัดหรือการหยุดระงักของระบบงานธุรกรรม ซึ่งอาจมีสาเหตุมาจากภัยทางด้านสิ่งแวดล้อม หรือการล้มเหลวของระบบสารสนเทศ เพื่อลดผลกระทบที่เกิดขึ้นและสามารถกู้ระบบกลับคืนได้ภายในระยะเวลาอันเหมาะสม

- กระบวนการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process) การกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องทางธุรกิจ (Business Continuity) โดยกระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ
- กระบวนการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process) การกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องทางธุรกิจ (Business Continuity) โดยกระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ
- การประเมินความเสี่ยงในการสร้างความต่อเนื่องทางธุรกิจ (Business continuity analysis and risk management) การประเมินความเสี่ยงที่เกิดจากเหตุการณ์ทางด้านความมั่นคงปลอดภัย การระบุโอกาสที่จะเกิดขึ้นและผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศของบริษัท
- การจัดทำและใช้งานแผนการสร้างความต่อเนื่องทางธุรกิจ (Developing and implementing continuity plans including information security) การจัดทำและการใช้งานแผนการสร้างความต่อเนื่องทางธุรกิจ เมื่อเกิดเหตุการณ์ทางด้านความมั่นคงปลอดภัย เพื่อให้การทำธุรกรรมสามารถดำเนินงานต่อไปได้ หรือสามารถกู้คืนให้กลับสู่สภาวะปกติได้ในระยะเวลาที่กำหนด
- การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องทางธุรกิจ (Business continuity planning framework) การกำหนดกรอบสำหรับจัดทำแผนการสร้างความต่อเนื่องทางรุกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน ครอบคลุมถึงข้อกำหนดทางด้านความมั่นคงปลอดภัยและจัดลำดับความสำคัญของงานต่างๆ ที่ต้องดำเนินการได้
- การทดสอบและการปรับปรุงแผนการสร้างความต่อเนื่องทางธุรกิจ (Testing, maintaining and re-assessing business continuity plans) การกำหนดให้มีการทดสอบ และปรับปรุงแผนการสร้างความต่อเนื่องทางธุรกิจ ตามระยะเวลาที่กำหนด เพื่อให้แผนสามารถทำงานได้เมื่อเกิดเหตุการณ์ทางด้านความมั่นคงปลอดภัยขึ้นและมีความมั่นคงปลอดภัยรับกับระบบสารสนเทศที่มีการเปลี่ยนแปลง โดยบริษัทได้มีการกำหนดให้มีการทดสอบและปรับปรุงแผนงานอย่างน้อยปีละ 1 ครั้ง

7.11. การปฏิบัติตามข้อกำหนด (Compliance)

วัตถุประสงค์

เพื่อให้การดำเนินงานต่างๆ ของบริษัทเป็นไปตาม กฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆที่ทางบริษัทต้องปฏิบัติตาม และมีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศ

7.11.1. การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)

การปฏิบัติตามข้อกำหนดทางกฎหมายนี้จำเป็นที่จะต้องได้รับความร่วมมือจากผู้เชี่ยวชาญทางด้านกฎหมาย เพื่อให้คำแนะนำการกำหนดหลักเกณฑ์ใดๆ เป็นไปอย่างถูกต้อง

- การระบุข้อกำหนดต่างๆที่มีผลทางกฎหมาย (Identification of applicable legislation) การระบุข้อกำหนดทางด้านกฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆ ให้มีการบันทึกเป็นลายลักษณ์อักษร และกำหนดแนวทางปฏิบัติต่างๆให้เป็นตามข้อกำหนดดังกล่าว ต้องมีการทบทวนความถูกต้องของการระบุข้อกำหนดทางด้านกฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร โดยฝ่ายกฎหมาย ตามระยะเวลาที่กำหนด
- การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights (IRP)) ทรัพย์สินสารสนเทศที่ต้องมีการป้องกันสิทธิและทรัพย์สินทางปัญญา คือ ซอฟต์แวร์ เอกสารที่มีการสงวน

7.11.2. การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies, standards and technical compliance)

เพื่อตรวจสอบการปฏิบัติงานให้เป็นไปตามนโยบาย และมาตรฐานความมั่นคงปลอดภัยของบริษัท

- การใช้งานมาตรการการเข้ารหัสลับข้อมูลตามข้อกำหนด (Regulation of cryptographic controls) กำหนดให้มีการใช้งานการเข้ารหัสลับข้อมูลตามกฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัย
- การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards) การให้ความสำคัญและการสนับสนุนของผู้บริหารต่อการปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค โดยต้องควบคุมการปฏิบัติงานของผู้ใต้บังคับบัญชาให้ปฏิบัติตามหน้าที่ความรับผิดชอบ
- การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิค (Technical compliance checking) กำหนดให้มีการตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคที่ได้กำหนดไว้ในนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนด
- การขอผ่อนผันการปฏิบัติตามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Policy) เพื่อให้การขอผ่อนผันการปฏิบัติตามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มีการจัดทำเอกสารเป็นลายลักษณ์อักษร และผ่านการอนุมัติจากผู้มีอำนาจและเพื่อป้องกันการยกเว้นการปฏิบัติตามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยไม่ได้รับอนุญาต

ในกรณีที่หน่วยงานใดไม่สามารถปฏิบัติตามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ หรือมีข้อจำกัดทางเทคนิคหรือในกรณีที่ธุรกิจมีความจำเป็นต้องดำเนินการแตกต่างไปจากนโยบายฉบับนี้ เพื่อสนับสนุนภารกิจ หรือการปฏิบัติงานของบริษัทที่ไม่สามารถปฏิบัติตามนโยบายโดยมีเงื่อนไขสมควร ทั้งนี้หน่วยงานที่ได้รับการผ่อนผันจะต้องรายงานความคืบหน้าต่อกลุ่มงานบริการด้านเทคโนโลยี

อนึ่ง เรื่องที่สามารถขอผ่อนผันการปฏิบัติตามนโยบายได้นั้น ต้องเป็นเรื่องที่ไม่ขัดต่อเกณฑ์บริษัทหรือเกณฑ์การกำกับดูแล หรือข้อกฎหมายต่างๆ

บริษัทฯ โดยหน่วยงานกำกับดูแลจะทำการทบทวนรายละเอียดและข้อปฏิบัติของนโยบาย อย่างน้อยปีละ 1 ครั้ง เพื่อให้นโยบายมเหมาะสมกับการดำเนินธุรกิจของบริษัที ความสอดคล้องกับแนวปฏิบัติที่ดีตลอดจนระเบียบ ข้อบังคับ กฎเกณฑ์ และกฎหมายที่เกี่ยวข้อง