SEVEN UTILITIES AND POWER
PUBLIC COMPANY LIMITED

นโยบาย
เทคโนโลยีสารสนเทศ
(ฉบับปรับปรุงแก้ไข ครั้งที่ 1)

บริษัท เซเว่น ยูทิลิตี้ส์ แอนด์ พาวเวอร์ จำกัด (มหาชน)

ได้รับอนุมัติตามมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2566 เมื่อวันที่ 30 มกราคม 2566

คำนำ

ปัจจุบันเทคโนโลยีสารสนเทศมีการพัฒนาอย่างต่อเนื่อง และรวดเร็ว ซึ่งการพัฒนานั้นมีทั้งการสร้างสิ่งที่อำนวยความสะดวก และสร้างคุณประโยชน์ให้เกิดแก่ผู้ใช้งานเทคโนโลยีสารสนเทศ ซึ่งการพัฒนาเทคโนโลยี จะมีประโยชน์มากยิ่งขึ้น หากได้กำหนดแนวทางการพัฒนาให้สอดคล้องกับกลยุทธ์ของบริษัท และเป็นไปในทิศทางเดียวกับวิสัยทัศน์ ประกอบกับมีการการประกาศใช้กฎหมาย และกฎข้อบังคับต่างๆ ที่เกี่ยวเนื่องกับเทคโนโลยีสารสนเทศมีเพิ่มมากขึ้น และมีการพัฒนาในแง่ลบเกิดขึ้นตามมาอย่างต่อเนื่องเช่นเดียวกัน จึงเป็นที่มาของการกำหนดนโยบายเทคโนโลยีสารสนเทศ เพื่อให้สามารถครอบคลุมกับการเปลี่ยนแปลงต่างๆ ของสารสนเทศได้อย่างทันท่วงที เป็นไปตามข้อกำหนด กฎหมาย และมีระบบควบคุมภายในที่เพียงพอ

ทั้งนี้ คณะกรรมการบริษัทจึงได้มีการทบทวนนโยบายเทคโนโลยีสารสนเทศของบริษัท โดยได้มีการปรับปรุงเพิ่มเติม และได้รับการอนุมัติตามมติที่ประชุมคณะการบริษัท ครั้งที่ 1/2566 เมื่อวันที่ 30 มกราคม 2566 เพื่อเป็นแนวทางในการดำเนินงานของบริษัทด้านเทคโนโลยีสารสนเทศต่อไป

พลตำรวจเอก

(ดร.สมยศ พุ่มพันธุ์ม่วง)

ประธานกรรมการ

สารบัญ

เรื่อง	หน้า
วัตถุประสงค์	1
คำนิยาม	2
นโยบายด้านเทคโนโลยีสารสนเทศ	6
1. การรักษาความลับของข้อมูล (Confidentiality)	6
2. การจัดหา ติดตั้งระบบงานคอมพิวเตอร์	6
3. ระบบสารสนเทศสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRC, DRP)	8
4. การให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น (IT Insourcing) และการใช้บริการด้านงานเทคโนโลยี สารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)	8
5. การบริหารข้อมูลสารสนเทศ	9
นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	11
1. นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)	11
2. แนวปฏิบัติการจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information)	12
3. แนวปฏิบัติการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resources Security)	13
4. แนวปฏิบัติการบริหารจัดการทรัพย์สิน (Asset Management)	15
5. แนวปฏิบัติการควบคุมการเข้าถึง (Access Control)	17
6. แนวปฏิบัติการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security)	21
7. แนวปฏิบัติความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)	25
8. แนวปฏิบัติความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)	27
9. แนวปฏิบัติการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition Development and Maintenance)	29
10. แนวปฏิบัติความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)	31

สารบัญ (ต่อ)

เรื่อง หน้า

11. แนวปฏิบัติการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย
(Information Security Incident Management)..... 32
12. แนวปฏิบัติประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความ
ต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity management).. 33
13. การปฏิบัติตามข้อกำหนด (Compliance)..... 34

วัตถุประสงค์

เพื่อให้บริษัทฯ มีแนวนโยบายในการดำเนินงาน หรือการจัดการทางด้านเทคโนโลยีสารสนเทศ และให้ผู้ที่เกี่ยวข้องกับสารสนเทศ ทั้งผู้บริหาร พนักงาน และบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับสารสนเทศของบริษัทฯ ได้มีแผนงาน และกรอบการปฏิบัติที่ชัดเจน อันจะนำไปสู่การประสานงานในการให้บริการที่มีประสิทธิภาพ ความปลอดภัยในการให้บริการสูงสุด และมีมาตรฐานยิ่งขึ้น

หน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับนโยบาย

- แผนกเทคโนโลยีสารสนเทศ รับทราบนโยบาย และปฏิบัติตาม รวมถึงกำกับการทำงาน ให้เป็นไปตามนโยบาย
- ฝ่ายตรวจสอบภายใน มีหน้าที่ตรวจสอบการควบคุมภายใน และสอบทานกระบวนการ

หน่วยงานที่ต้องปฏิบัติตามนโยบาย

- ทุกฝ่าย และทุกส่วนของบริษัทฯ

หน่วยงานที่กำกับดูแลให้เป็นไปตามนโยบาย

- ผู้บังคับบัญชาแผนกเทคโนโลยีสารสนเทศทุกระดับ
- ฝ่ายกำกับดูแลการปฏิบัติตามกฎเกณฑ์

คำนิยาม

นโยบายเทคโนโลยีสารสนเทศได้กำหนดคำนิยามของคำศัพท์ที่ใช้ในนโยบายฉบับนี้ เพื่อให้เข้าใจถึงความหมายตรงกันและอ้างอิงได้ถูกต้อง ดังต่อไปนี้

คำศัพท์	คำนิยาม
บริษัทฯ	บริษัท เซเว่น ยูทิลิตี้ส์ แอนด์ พาวเวอร์ จำกัด (มหาชน) และบริษัทในเครือ
แผนกเทคโนโลยีสารสนเทศ	หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศของบริษัทฯ
บุคคลภายนอก	บุคคล หรือพนักงานของหน่วยงานภายนอกที่มาติดต่อสื่อสาร และมีการเข้าถึงทรัพย์สินสารสนเทศของบริษัทฯ
ผู้ดูแลระบบ (Administrator)	เจ้าหน้าที่ฝ่ายสารสนเทศที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบ หรือเครือข่ายคอมพิวเตอร์ รวมไปถึงการแก้ไขปัญหาการใช้งานในด้านต่างๆ ซึ่งสามารถเข้าถึงโปรแกรม หรือเครือข่ายคอมพิวเตอร์เพื่อการจัดการต่างๆ ได้
ผู้บริหารฝ่าย	ผู้บริหารสูงสุดของแต่ละฝ่ายงาน
ผู้ให้บริการรายอื่น	บุคคล หรือนิติบุคคลอื่นใดทั้งในประเทศ และต่างประเทศที่ให้บริการด้านเทคโนโลยีสารสนเทศ
หน่วยงานภายนอก (Third party)	หน่วยงานที่มีความจำเป็นในการเข้ามาปฏิบัติงาน หรือเข้ามาเกี่ยวข้องกับสถานที่หรือทรัพย์สินสารสนเทศของบริษัทฯ มีหน้าที่ความรับผิดชอบในการปฏิบัติตามนโยบาย และกฎระเบียบ ตามข้อกำหนด ข้อตกลง หรือสัญญาที่ได้จัดทำกับบริษัทฯ
ผู้ใช้งาน (User)	ผู้ใช้งานระบบงานคอมพิวเตอร์
เจ้าของข้อมูล (Data Owner)	ฝ่าย หรือส่วนที่เป็นเจ้าของข้อมูล
ผู้มีอำนาจ	ผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายขึ้นไป หรือผู้ที่ได้รับมอบหมายที่มีหน้าที่ตัดสินใจ
การเข้ารหัสลับ (Cryptography or Encryption)	การเปลี่ยนแปลงรูปแบบของข้อมูลให้อยู่ในรูปแบบที่มีความมั่นคงปลอดภัย โดยใช้กุญแจในการเข้ารหัสลับ เพื่อที่ผู้เข้าถึงข้อมูลจะไม่สามารถทราบเนื้อหาที่แท้จริงของข้อมูลได้ ถ้าไม่มีการถอดรหัสลับจากกุญแจที่ใช้ในการถอดที่ถูกต้อง ทั้งนี้ขึ้นกับเทคนิคการเข้ารหัสลับข้อมูลที่ใช้
การเปลี่ยนแปลงปรับปรุงแก้ไข	การเปลี่ยนแปลง ปรับปรุงแก้ไขระบบ หรืออุปกรณ์ประมวลผลสารสนเทศ เช่น การติดตั้งหรือการปรับเปลี่ยนระบบปฏิบัติการซอฟต์แวร์ระบบ และระบบเครือข่าย
การเฝ้าระวัง (Monitoring)	การเฝ้าระวังทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบความผิดปกติจากการประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศ จากบันทึกเหตุการณ์การใช้งานของระบบ (Logs) เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานสารสนเทศผิดวัตถุประสงค์ และปัญหาที่เกิดจากระบบงาน

คำศัพท์	คำนิยาม
การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัย (Security Awareness)	การให้ความรู้ความเข้าใจทางด้านความมั่นคงปลอดภัยของสารสนเทศ เพื่อสร้างความตระหนักถึงภัยคุกคาม และปัญหาทางด้านความมั่นคงปลอดภัยสารสนเทศแก่บุคลากร
การสำรองข้อมูล (Data Backup)	การทำสำเนาข้อมูลทั้งหมดในระบบที่ต้องการ เพื่อเป็นการสำรองข้อมูลที่อาจมีการแก้ไขเปลี่ยนแปลง หรือสูญหายให้สามารถนำกลับมาใช้งานได้
กุญแจ (Key)	กุญแจที่ใช้ในกระบวนการเข้ารหัสลับ ใช้ในการเข้ารหัสลับ หรือถอดรหัสลับ ขึ้นอยู่กับการใช้งานเทคนิคการเข้ารหัสลับข้อมูล หรือแยกเป็น 2 ประเภท คือ กุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key)
ข้อมูลสารสนเทศ (Information asset and Software License)	สารสนเทศที่อยู่ในสื่อบันทึกข้อมูล และลิขสิทธิ์ซอฟต์แวร์ เช่น ฐานข้อมูลระบบงานต่างๆ ข้อมูลการทำงาน ลิขสิทธิ์ สัญญาต่างๆ
แหล่งข้อมูล (Source of Data and information)	ที่เก็บข้อมูล หรือสารสนเทศทั้งที่อยู่ในรูปแบบต่างๆ กัน เช่น ข้อมูล แหล่งข้อมูลเฉพาะ และแหล่งข้อมูลส่วนกลาง เป็นต้น
ความมั่นคงปลอดภัย (Security)	ปัจจัยด้านความมั่นคงปลอดภัยในที่นี้มี 3 ประการด้วยกัน คือ 1. การรักษาความลับ (Confidentiality) 2. ความถูกต้องครบถ้วน (Integrity) 3. ความพร้อมใช้งาน (Availability) โดยสรุปได้ใจความว่า ความมั่นคงปลอดภัยสารสนเทศ คือ การรักษาสารสนเทศจากการเข้าถึงเพื่อการขโมย เปลี่ยนแปลง ทำให้ใช้การไม่ได้ หรือการทำลายสารสนเทศโดยไม่รับอนุญาต
งานเทคโนโลยีสารสนเทศ	งานใดๆ ที่เกี่ยวกับเทคโนโลยีสารสนเทศ ได้แก่ งานประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ การจัดเก็บข้อมูล การพัฒนาระบบงาน และโปรแกรม การบำรุงรักษาความปลอดภัยทรัพยากรคอมพิวเตอร์ เช่น เครื่องคอมพิวเตอร์และอุปกรณ์ระบบงานและโปรแกรมระบบเครือข่าย และข้อมูล เป็นต้น
ช่องโหว่ (Vulnerability)	ช่องโหว่ ในทรัพย์สินสารสนเทศที่อาจเกิดจากความบกพร่องในการผลิต หรือการออกแบบทำให้เกิดจุดอ่อน และมีความเสี่ยงในการคุกคามจากช่องโหว่ที่เกิดขึ้น เช่น ช่องโหว่ของโปรแกรมที่ทำให้บุคคลภายนอกสามารถเข้าใช้โปรแกรมได้โดยไม่ต้องผ่านการพิสูจน์ตัวตน
ทรัพย์สินสารสนเทศ (IT Asset)	1. ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์และระบบสารสนเทศ 2. เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล สื่อบันทึกข้อมูล และอุปกรณ์อื่นใด 3. ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

คำศัพท์	คำนิยาม
บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Area)	คือ บริเวณที่ใช้เก็บรักษาอุปกรณ์สารสนเทศที่ใช้ในงานระบบสารสนเทศ แบ่งได้เป็น 3 ประเภท คือ 1) พื้นที่ห้อง Patching Room 2) พื้นที่ห้องปฏิบัติการคอมพิวเตอร์ 3) พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)
บริเวณปฏิบัติการคอมพิวเตอร์ (Computer Operation)	พื้นที่ที่ใช้ในการป้อนข้อมูล ออกรายงาน และปฏิบัติงานเกี่ยวกับระบบงานสารสนเทศของบริษัทฯ
บริเวณ Patching Area	พื้นที่ที่ใช้เก็บอุปกรณ์ในการเชื่อมต่อเครือข่ายคอมพิวเตอร์และโทรศัพท์ในแต่ละชั้น
บัญชีผู้ใช้ (User Name หรือ Account)	กลุ่มของข้อมูลที่ใช้ในการอ้างถึงเพื่อระบุตัวตน สิทธิการเข้าถึง และข้อจำกัดต่างๆ ในการเข้าถึงนั้น
บันทึกเหตุการณ์ (Logs)	บันทึกเหตุการณ์การใช้งานของระบบสารสนเทศ การเข้าใช้งานระบบ การประมวลผลกิจกรรมของระบบสารสนเทศ และเหตุการณ์ทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบถึงประสิทธิภาพ ความปลอดภัย และความผิดปกติที่เกิดจากการประมวลผลกิจกรรมต่างๆ ของระบบสารสนเทศ
ประมวลผล (Process)	กระบวนการทำงานทางตรรกะของคอมพิวเตอร์
ประเมินความเสี่ยง (Risk Assessment)	การประเมินความเสี่ยง หรือเหตุการณ์ที่อาจเกิดขึ้นได้ ซึ่งอาจเป็นอันตราย หรือคุกคามถึงความมั่นคงปลอดภัยสารสนเทศ
โปรแกรมที่ไม่พึงประสงค์ (Malicious Code or Malware)	โปรแกรมหรือ Code ที่เป็นอันตรายต่อประสิทธิภาพ และความปลอดภัยของระบบสารสนเทศไม่ทางใดก็ทางหนึ่ง เช่น ไวรัส (Virus) เวิร์ม (Worm) และโทรจัน (Trojan)
แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)	การสร้างความต่อเนื่องทางธุรกิจ ป้องกันการติดขัดหรือการหยุดชะงักของระบบงานธุรกรรมที่สำคัญ ซึ่งอาจมีสาเหตุมาจาก ภัยทางด้านสิ่งแวดล้อม เหตุการณ์ทางด้านความมั่นคงปลอดภัย หรือภัยคุกคามอื่นๆ
แผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRP: Disaster Recovery Plan)	การเตรียมความพร้อมรองรับเหตุฉุกเฉิน และแผนการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน เช่น การย้ายสถานที่ปฏิบัติงาน ไปจนถึงการใช้งานระบบสารสนเทศสำรอง
รหัสผ่าน (Password)	กลุ่มอักขระที่ใช้ในการพิสูจน์ตัวตน ใช้เพื่อควบคุมการเข้าถึงระบบสารสนเทศ หรือข้อมูลสารสนเทศ
ระบบงานที่สำคัญ (High Priority Application System)	หมายถึง ระบบที่ให้บริการธุรกรรมหลักที่ใช้ในการให้บริการลูกค้า หรือระบบงานที่นำส่งข้อมูลรายงานแก่ทางราชการ
ระดับของการให้บริการ Service Level Agreement (SLA)	ตัวชี้วัดถึงประสิทธิภาพของการให้บริการโดยผู้ให้บริการภายนอก

คำศัพท์	คำนิยาม
ระดับของการให้บริการ perational Level Agreement (OLA)	ตัวชี้วัดประสิทธิภาพการปฏิบัติงานโดยฝ่ายเทคโนโลยีสารสนเทศ
ระบบพัฒนา (Development Area)	ระบบสารสนเทศที่ใช้ในการพัฒนาระบบงาน โดยเป็นการจำลองทรัพยากร และสภาพแวดล้อมของระบบให้บริการจริง เพื่อใช้พัฒนาระบบงานให้มีประสิทธิภาพมากขึ้น
ระบบทดสอบ (User Acceptance Area)	ระบบสารสนเทศที่ใช้ในการทดสอบ โดยเป็นการจำลองทรัพยากร และสภาพแวดล้อมของระบบให้บริการจริง มาเพื่อทดสอบประสิทธิภาพ และความปลอดภัยของระบบที่ได้พัฒนาขึ้น
ระบบสารสนเทศสำรอง (Disaster Recovery Center: DRC)	ระบบงาน ข้อมูล และระบบเครือข่ายสำรองนอกเหนือจากระบบสารสนเทศหลัก เพื่อให้สามารถทำธุรกรรมหลักได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุการณ์ฉุกเฉิน
ระบบให้บริการจริง (Production Area)	ระบบสารสนเทศที่ให้บริการจริงแก่ผู้ใช้งาน ซึ่งต้องมีการรักษาความปลอดภัย และการควบคุมการเข้าถึงจากการพัฒนาระบบ และการทดสอบระบบอย่างเคร่งครัด
สิทธิเฉพาะ (Privilege)	สิทธิพิเศษที่ใช้ในการปฏิบัติงาน นอกเหนือจากสิทธิทั่วไป เช่น ผู้ดูแลระบบ หรือเจ้าของข้อมูลสารสนเทศ
สื่อบันทึกข้อมูล (Media)	สื่อที่ใช้ในการบันทึกข้อมูลในระบบงานสารสนเทศ โดยสามารถจำแนกเป็นสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เพื่อใช้ในการรักษาความลับของข้อมูล เช่น Tapes, Disks, Removable Hard Drives, CDs, DVDs, และ Printed Media และสื่อบันทึกข้อมูลทั่วไป เช่น กระดาษ และเครื่องคอมพิวเตอร์
ห้องคอมพิวเตอร์ (Data Center)	พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ที่ใช้เก็บอุปกรณ์คอมพิวเตอร์ และเครื่องคอมพิวเตอร์หลักที่สำคัญในระบบงาน เช่น เครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายหลัก
เหตุการณ์ทางด้านความมั่นคงปลอดภัย (Security Event and Incident)	เหตุการณ์ที่เกิดจากการเปลี่ยนแปลงระบบ สภาพแวดล้อม กระบวนการ ขั้นตอนการปฏิบัติงาน หรือจากพนักงาน ซึ่งทำให้เกิดความเสี่ยง หรือการคุกคามถึงประสิทธิภาพ และความปลอดภัยของระบบสารสนเทศ หรือทรัพย์สินสารสนเทศ รวมไปถึงการโจมตีระบบทำให้ระบบไม่สามารถทำงานได้อย่างปกติ และการถูกโจมตีโดยโปรแกรมไม่ประสงค์ดีต่างๆ
การซ่อมบำรุง	กิจกรรม หรืองานที่ทำต่ออุปกรณ์ต่างๆ เพื่อรักษาสภาพ หรือป้องกันเพื่อไม่ให้เกิดความชำรุดเสียหาย โดยให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา รวมทั้งช่วยยืดอายุการใช้งานให้ยาวนานขึ้น และเสียค่าใช้จ่ายน้อยที่สุด

นโยบายด้านเทคโนโลยีสารสนเทศ

1. การรักษาความลับของข้อมูล (Confidentiality)

เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล ให้มีการระบุความสำคัญ และการระบุการจัดการของข้อมูลที่ใช้งานในระบบสารสนเทศ และพนักงานผู้ต้องปฏิบัติงานเกี่ยวข้องกับข้อมูล เพื่อป้องกันการนำเข้าข้อมูลสารสนเทศไปใช้โดยผิดวัตถุประสงค์หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

1.1 การจัดระดับข้อมูลสารสนเทศ (Information Classification)

กำหนดให้มีการแบ่งระบบความปลอดภัยขององค์กร โดยคำนึงถึงระดับความเสี่ยงต่อความมั่นคงปลอดภัยผลกระทบต่อมูลค่า และความเสียหายที่ผู้ใช้บริการอาจได้รับ รวมถึงผลกระทบต่อความเสียหายทางทรัพย์สิน และชื่อเสียงในการดำเนินธุรกิจ โดยข้อมูลขององค์กรสามารถแบ่งออกตามระดับความสำคัญ 4 ระดับ ดังนี้

- ข้อมูลที่เผยแพร่ได้ (Public) เป็นข้อมูลที่มีเจตนาต้องการให้ลูกค้า หรือบุคคลภายนอกทราบ เช่น News Release และ Brochure ที่จัดทำออกมาเพื่อประชาสัมพันธ์ เป็นต้น

- ข้อมูลภายใน (Internal) เป็นข้อมูลสำหรับให้พนักงานของบริษัทฯ ใช้เท่านั้น และไม่มีเจตนาให้ภายนอกทราบ แต่ถ้าหากถูกนำไปเผยแพร่ จะไม่ทำให้เกิดความเสียหายมากนัก โดยมากจึงมักไม่ต้องการระบบการป้องกัน เช่น ระเบียบ บันทึกต่างๆ และจดหมายเรื่องทั่วไป เป็นต้น

- ข้อมูลลับ (Confidential) เป็นข้อมูลเฉพาะสำหรับพนักงานที่ได้รับมอบหมายเท่านั้น หากถูกเผยแพร่ออกไปสู่พนักงานอื่นที่ไม่เกี่ยวข้อง จะทำให้เกิดความเสียหายแก่บริษัทฯ ลูกค้า หรือพนักงาน จึงต้องเก็บรักษาป้องกันมิให้รั่วไหลออกไป เช่น รายงานทุกรายงานจากระบบคอมพิวเตอร์ ข้อมูลลูกค้า ข้อมูลส่วนบุคคล เงินเดือนพนักงาน โบนัสพนักงาน และงบประมาณของบริษัทฯ เป็นต้น

- ข้อมูลลับเฉพาะ (Highly Restricted) เป็นข้อมูลลับที่สำคัญที่สุด หากถูกเผยแพร่ออกไปสู่พนักงานอื่นที่ไม่เกี่ยวข้อง จะทำให้บริษัทฯ ลูกค้า หรือพนักงาน เสื่อมเสียชื่อเสียง ได้รับการกล่าวโทษ หรือฟ้องร้อง หรือเกิดความเสียหายอย่างยิ่ง จึงต้องมีการระวังรักษาป้องกันอย่างเข้มงวด เช่น ข้อมูลเกี่ยวกับบริการใหม่ที่ยังไม่ถึงเวลาประกาศ ข้อมูลงบการเงินที่ยังไม่ถึงเวลาประกาศ ข้อมูลการควบรวมกิจการ หรือการเพิ่มทุนที่ยังไม่ถึงเวลาประกาศ และรหัสผ่านของระบบงานต่างๆ เป็นต้น

1.2 การจัดการเกี่ยวกับข้อมูลข่าวสาร (Information Handling)

ข้อมูลถือเป็นทรัพย์สมบัติขององค์กร พนักงานทุกคนต้องดูแลรักษาข้อมูลที่ตนเองดูแลรับผิดชอบอยู่ โดยให้พิจารณาการจัดการตามระดับความสำคัญของข้อมูล เพื่อลดความเสี่ยงต่อความเสียหายทางทรัพย์สินและชื่อเสียงในการดำเนินธุรกิจ

2. การจัดหา ติดตั้งระบบงานคอมพิวเตอร์

เพื่อกำหนดวิธีการจัดหา และการจัดการระบบงานคอมพิวเตอร์ของบริษัทฯ ที่สามารถสนับสนุนการให้บริการธุรกิจของบริษัทฯ ได้อย่างรวดเร็ว มีความต่อเนื่อง มีความถูกต้องน่าเชื่อถือ และมีประสิทธิภาพ

2.1 การจัดหาระบบงานคอมพิวเตอร์

หมายถึง กระบวนการ หรือวิธีการให้ได้มาซึ่งระบบงานคอมพิวเตอร์ที่สามารถตอบสนองความต้องการทางธุรกิจและสอดคล้องกับกลยุทธ์ของบริษัทฯ เริ่มตั้งแต่ระบุความต้องการระบบงานคอมพิวเตอร์ของแต่ละสายงาน โดยมีการจัดทำโครงการ

และบันทึกเป็นลายลักษณ์อักษร และได้รับการอนุมัติจากผู้บริหารสายงาน หรือผู้ที่มีอำนาจ จึงได้กำหนดแนวทางในการจัดหาระบบงานคอมพิวเตอร์ โดยเรียงลำดับตามการจัดหาระบบงานดังนี้

1) จัดซื้อระบบงานคอมพิวเตอร์ (Software Package Implementation)

2) จัดหาพัฒนาระบบงานคอมพิวเตอร์ (Software Customization Implementation)

3) พัฒนาระบบงานคอมพิวเตอร์โดยหน่วยงานเทคโนโลยีสารสนเทศขององค์กร (In-house Development)

2.2 การติดตั้งระบบงานคอมพิวเตอร์

เพื่อให้การติดตั้งระบบงานคอมพิวเตอร์สำเร็จตามวัตถุประสงค์ของโครงการ จึงกำหนดกรอบในการติดตั้ง ระบบงานคอมพิวเตอร์ ดังนี้

- การกำหนดหน้าที่ของคณะทำงาน จัดให้มีการกำหนดหน้าที่ และความรับผิดชอบของคณะทำงานอย่างชัดเจน

- การควบคุมงานโครงการ จัดให้มีการควบคุมโครงการ ตามกรอบการติดตั้ง และพัฒนาระบบงาน (Software Implementation Framework) กำหนดให้มีการจัดทำแผนงานที่ชัดเจน ระบุความถี่ และขั้นตอนในการติดตาม ความคืบหน้าและการรายงานผลการดำเนินโครงการให้ผู้เกี่ยวข้องรับทราบโดยต้องปรับปรุงแผนให้เป็นปัจจุบันอย่างสม่ำเสมอ

- การตรวจรับมอบงาน จัดให้มีกระบวนการตรวจสอบความถูกต้อง และประเมินประสิทธิภาพ ของระบบงานก่อนการรับมอบระบบงาน รวมถึงจัดทำเอกสารตรวจรับมอบงาน และใช้เป็นเอกสารประกอบการเบิกจ่ายเงิน โดยยึดตาม “นโยบายเรื่องการเบิกจ่ายเงินงบประมาณโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ”

2.3 การควบคุมการเปลี่ยนแปลงระบบงานคอมพิวเตอร์

เพื่อให้ระบบงานสามารถสนับสนุนธุรกิจขององค์กรได้อย่างต่อเนื่องและมีประสิทธิภาพ หากมีการเปลี่ยนแปลงความต้องการของธุรกิจ ซึ่งกระทบกับระบบงานคอมพิวเตอร์ปัจจุบันที่จะต้องมีการปรับแก้ไขให้ทันการณ์จึงต้องกำหนดกรอบการควบคุมการเปลี่ยนแปลงระบบงาน ดังนี้

- การร้องขอให้มีการเปลี่ยนแปลง จัดให้มีการบันทึกการร้องขอให้มีการเปลี่ยนแปลงเป็นลายลักษณ์อักษร และได้รับการอนุมัติจากผู้จัดการส่วนขึ้นไป หรือผู้ที่มีอำนาจ

- การวิเคราะห์ผลกระทบ จัดให้ผู้เกี่ยวข้องจัดทำเอกสารวิเคราะห์ผลกระทบรอบด้าน เพื่อควบคุมความเสี่ยง และใช้ประกอบการตัดสินใจ

- การควบคุมการเปลี่ยนแปลง จะต้องผ่านการอนุมัติจากผู้มีอำนาจของแต่ละฝ่ายงาน ต้องมีการสื่อสาร และแจ้งให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลง

2.4 การควบคุมคุณภาพการให้บริการของระบบงานคอมพิวเตอร์

เพื่อให้ระบบงานเทคโนโลยีสารสนเทศสามารถให้บริการตอบสนองธุรกิจอย่างต่อเนื่อง และมีความถูกต้องน่าเชื่อถือ ดังนั้น จึงได้จัดกำหนดการควบคุมคุณภาพให้บริการ ดังนี้

- การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการจริง จัดให้มีการแบ่งแยกส่วนพัฒนา (Development Environment) และส่วนทดสอบ (Test Environment) ออกจากส่วนระบบที่ให้บริการจริง (Production Environment) อย่างชัดเจน

- การแบ่งแยกเครือข่าย จัดให้มีการแยกเครือข่าย และแยกบัญชีผู้ใช้งานเข้าถึงส่วนพัฒนา (Development Environment) และส่วนทดสอบ (Test Environment) ออกจากส่วนระบบที่ให้บริการจริง (Production Environment) อย่างชัดเจน

- กำหนดให้มีการจัดทำคู่มือเอกสารประกอบระบบงาน และฐานข้อมูลความรู้ เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจระบบงาน ลักษณะงาน และกระบวนการทำงาน รวมถึงปรับปรุงเอกสารให้เป็นปัจจุบันอยู่เสมอ

- การสนับสนุนการใช้ระบบงาน จัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบงานอย่างชัดเจน โดยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหา และวิธีการแก้ไขรวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ

3. ระบบสารสนเทศสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRC, DRP)

เพื่อให้ฝ่ายงานธุรกิจต่างๆ สามารถทำธุรกรรมได้อย่างต่อเนื่อง และแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว แม้ว่าจะเกิดเหตุฉุกเฉิน หรือเหตุการณ์ทางด้านความมั่นคงปลอดภัยใดๆ ซึ่งมีการจัดระบบสารสนเทศสำรอง (DRC : Disaster Recovery Center) การสำรองข้อมูล (Data Backup) และแผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRP : Disaster Recovery Plan) รวมถึงให้สอดคล้องกับการเตรียมการในเรื่องการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)

- กำหนดให้มีศูนย์คอมพิวเตอร์สำรอง และระบบสารสนเทศสำรอง เพื่อรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุการณ์ฉุกเฉิน

- กำหนดให้มีการสำรองข้อมูล (Backup) เพื่อรักษาความถูกต้องสมบูรณ์ และความพร้อมใช้ของสารสนเทศ ต้องมีการสำรองข้อมูลทั้งในส่วน System Software ส่วน Application Software และส่วนข้อมูลสารสนเทศ รวมถึงทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ โดยรูปแบบ และความถี่ในการสำรองข้อมูล ให้พิจารณาตามความจำเป็น

- กำหนดให้มีการจัดทำแผนรองรับกรณีเหตุฉุกเฉินที่สอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ การทดสอบแผนและการรายงานผลการทดสอบให้คณะกรรมการบริหารบริษัทฯ และ/หรือคณะกรรมการในบริษัทฯ รับทราบ รวมถึงต้องมีการเผยแพร่แผนรองรับเหตุฉุกเฉินให้ผู้ที่เกี่ยวข้องรับทราบโดยความถี่ในการทดสอบอย่างน้อยปีละ 1 ครั้ง

4. การให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น (IT Insourcing) และการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

เพื่อจัดทำข้อกำหนดต่างๆ และกรอบการปฏิบัติงาน ในการให้บริการ หรือการใช้บริการด้านงานเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ ความมั่นคงปลอดภัย และผลประโยชน์สูงสุดแก่บริษัทฯ

4.1 การให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น (IT Insourcing)

- การควบคุมและกำกับ บริษัทฯ มีการควบคุม และกำกับการดำเนินการด้านเทคโนโลยีสารสนเทศให้เป็นไปตามเกณฑ์ของบริษัทฯ โดยบริษัทฯ จะให้บริการทางเทคโนโลยีสารสนเทศภายในบริษัทฯ และบริษัทในเครือเท่านั้น

- การคิดค่าบริการ และค่าธรรมเนียม บริษัทฯ คิดค่าบริการ และค่าธรรมเนียม โดยเป็นที่ตกลงร่วมกันระหว่างผู้ให้บริการ และผู้ใช้บริการ สามารถอธิบายที่มาของค่าธรรมเนียม ค่าบริการ ได้ชัดเจน โปร่งใส

- การควบคุมภายใน จัดทำขั้นตอนการทำงาน (Operation Procedure Manual) แบ่งแยกอำนาจหน้าที่ของผู้ปฏิบัติงาน (Segregation of duty) ตามโครงสร้างผู้ปฏิบัติงานที่ชัดเจน และมีการบันทึกการปฏิบัติงาน

- การรักษาความปลอดภัยของข้อมูล กำหนดให้มีการสำรองข้อมูลโดยใช้สื่อบันทึกข้อมูล และการเก็บสื่อจะดำเนินการในสถานที่ที่ผู้รับบริการจัดหา และเตรียมไว้ให้เป็นการเฉพาะ รวมถึงไม่นำข้อมูลการให้บริการของผู้รับบริการไปเผยแพร่หรือนำไปใช้กับบุคคลภายนอก

- การรองรับเหตุฉุกเฉิน จัดให้มีการรองรับเหตุฉุกเฉิน และการสำรองข้อมูล ตามรายละเอียด กำหนดการ และรอบการสำรองข้อมูลตามที่ตกลงกัน

- มาตรฐานการให้บริการ ควรจัดให้มีมาตรฐานการให้บริการ (Operation Level Agreement) ตามที่ตกลงกัน

4.2 การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการอื่น (IT Outsourcing)

เพื่อจัดหาระบบงานเทคโนโลยีสารสนเทศได้รวดเร็ว สอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัทฯ โดยคำนึงถึงการให้บริการแก่ลูกค้าอย่างต่อเนื่องและมีความถูกต้องน่าเชื่อถือ การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นจึงเป็นทางเลือกที่ดีที่บริษัทฯ ได้กำหนดไว้ เพื่อให้สามารถบรรลุวัตถุประสงค์และได้รับการถ่ายทอดเทคโนโลยีที่ดีจากผู้ให้บริการรายอื่น โดยมีหลักเกณฑ์เบื้องต้นในการใช้บริการรายอื่น ดังนี้

- หลักเกณฑ์ในการพิจารณาการใช้บริการจากผู้ให้บริการรายอื่น ต้องไม่ขัดแย้งกับกฎระเบียบ หรือข้อกำหนดที่หน่วยงานราชการประกาศใช้

- การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) เพื่อให้มั่นใจว่าระบบสารสนเทศของบริษัทฯ และบริษัทสามารถดำเนินธุรกิจหรือให้บริการลูกค้าได้อย่างต่อเนื่อง

- ความน่าเชื่อถือของผู้ให้บริการ ต้องมีแนวทางในการพิจารณาคัดเลือกผู้ให้บริการ เพื่อประเมิน ถึงความน่าเชื่อถือของการให้บริการ และเพื่อให้แน่ใจว่าผู้ให้บริการมีความสามารถในการให้บริการลูกค้าได้ตามข้อตกลงการให้บริการ

- การดูแลและความรับผิดชอบต่อลูกค้า/การคุ้มครองผู้บริโภค (Customer Protection) ต้องมีแนวทางในการรักษาความปลอดภัยและความลับของข้อมูล เพื่อให้แน่ใจได้ว่าดูแลและรับผิดชอบต่อลูกค้าอย่างเหมาะสม

- การติดตาม ประเมินผล และตรวจสอบการให้บริการจากบุคคลภายนอก จัดให้มีการติดตาม ประเมิน และตรวจสอบการให้บริการจากบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้เป็นไปตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

- กำหนดให้มีแนวทางการบริหารความเสี่ยงจากการใช้บริการจากบุคคลภายนอก สำหรับความเสี่ยงด้านกลยุทธ์ด้านการเงิน และความเสี่ยงด้านกฎหมาย โดยกำหนดแนวทางการบริหารความเสี่ยงจากการใช้บริการจากบุคคลภายนอกด้านเทคโนโลยีสารสนเทศไว้อย่างชัดเจนและเป็นลายลักษณ์อักษร ให้เหมาะสมกับความสำคัญของระบบงานที่ใช้บริการจากบุคคลภายนอกและสอดคล้องกับนโยบายการบริหารความเสี่ยงโดยรวม รวมทั้งสื่อสารให้บุคคลที่เกี่ยวข้องเข้าใจและถือปฏิบัติตามแนวทางที่กำหนด

5. การบริหารข้อมูลสารสนเทศ

เพื่อให้บริการทางด้านข้อมูลเพื่อสนับสนุนในการดำเนินงาน และตอบสนองการแข่งขันของบริษัทฯ จึงต้องมีการจัดหาแหล่งข้อมูล และรายงานให้กับผู้บริหารอย่างรวดเร็ว ซึ่งข้อมูลและรายงานเหล่านี้จะต้องมีความถูกต้อง และสามารถใช้งานได้โดยผู้ที่เกี่ยวข้องเท่านั้น

5.1 การจัดหาและบำรุงรักษาแหล่งข้อมูลและรายงานผู้บริหาร

- จัดหาแหล่งข้อมูลให้แต่ละส่วนงานสามารถนำข้อมูลไปใช้ในการวิเคราะห์วิจัย เพื่อใช้ในการแข่งขันทางธุรกิจอย่างรวดเร็ว

- จัดให้มีรายงานสำหรับผู้บริหาร เพื่อเป็นข้อมูลในการตัดสินใจได้อย่างรวดเร็วและทันเวลา

- การบำรุงรักษาแหล่งข้อมูล และรายงานผู้บริหารให้สามารถใช้งานได้ตามปกติ ดำเนินการโดยฝ่ายสารสนเทศ

- ข้อมูลในแหล่งข้อมูลและรายงานผู้บริหาร มีความสำคัญระดับข้อมูลลับเฉพาะ (Highly Restricted)

- ฝ่ายสารสนเทศจะพัฒนาพนักงานผู้ใช้ข้อมูลของแต่ละส่วนงานให้สามารถสร้างรายงานเพิ่มเติมได้เอง

5.2 การเข้าถึงข้อมูลในแหล่งข้อมูล

- ผู้ที่มีสิทธิใช้งานข้อมูลในแหล่งข้อมูลจะต้องได้รับการอนุมัติจากส่วนงานซึ่งเป็นเจ้าของข้อมูลเท่านั้น
- กำหนดกลุ่มของผู้มีสิทธิใช้งานตามขอบเขตข้อมูลเป็น 3 ระดับ ดังนี้
- เข้าถึงข้อมูลทุกโครงการ/สาขา
- เข้าถึงข้อมูลเฉพาะโครงการ/สาขา
- เข้าถึงข้อมูลเฉพาะเรื่องที่เกี่ยวข้อง

5.3 การควบคุมคุณภาพของข้อมูลในแหล่งข้อมูล

- การทำ Data Cleaning จะเป็นหน้าที่ของผู้ใช้งาน โดยเจ้าหน้าที่สารสนเทศช่วยสนับสนุนในการดึงข้อมูล และการปรับปรุงข้อมูลเข้าระบบ และทางผู้ใช้งานจะทำการแจ้งขอทำ Data Cleaning ผ่านทาง IT Memo

- การเปลี่ยนแปลงข้อมูลในแหล่งข้อมูล User จะเป็นผู้จัดเตรียมข้อมูลให้ และเจ้าหน้าที่สารสนเทศ จะทำการปรับปรุงข้อมูลในฐานข้อมูล โดยใช้กระบวนการเดียวกันกับการทำ Data Cleaning และทางผู้ใช้งานจะทำการแจ้งขอเปลี่ยนแปลงข้อมูลผ่านทาง IT Memo

5.4 การจัดส่งข้อมูลให้หน่วยงานภายนอก

การจัดข้อมูลให้กับหน่วยงานภายนอก จะต้องได้รับการอนุมัติจากผู้มีอำนาจเท่านั้น และก่อนที่จะจัดส่งต้องมีการตรวจสอบความถูกต้องของข้อมูลโดยผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลก่อน โดยฝ่ายสารสนเทศจะแนะนำแหล่งข้อมูลในการดึงข้อมูลให้พิจารณาก่อนดำเนินการ

5.5 การจัดพิมพ์รายงาน

- การขอให้จัดพิมพ์รายงาน ควรได้รับความเห็นชอบจากผู้บริหารแต่ละฝ่ายที่เป็นเจ้าของข้อมูลสารสนเทศ
- ควรมีทะเบียนคุมการพิมพ์ การจัดส่งรายงาน และการจัดเก็บรายงานต่างๆ ที่ได้จัดพิมพ์แล้วอย่างรัดกุม
- กำหนดให้มีการลงลายมือชื่อเมื่อมีการรับรายงาน นอกจากนี้ควรทำลายรายงานที่ไม่ได้ใช้งานแล้ว

นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1. นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

เพื่อให้ผู้ใช้งาน และบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงต่างๆ โดยองค์กรต้องจัดให้มีนโยบาย และมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1.1 ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Directions for Information Security)

1) นโยบายสำหรับสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policy for Information Security) ต้องจัดให้มีนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรโดยได้รับการอนุมัติจากคณะกรรมการบริษัท หรือคณะกรรมการอื่นที่คณะกรรมการบริษัทมอบหมาย และจัดให้มีการทบทวน หรือปรับปรุงนโยบายดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงของสภาพแวดล้อมต่างๆ ที่มีนัยสำคัญ เช่น สภาพธุรกิจ กฎเกณฑ์ กฎหมาย และเทคโนโลยี เป็นต้น นอกจากนี้จะต้องเผยแพร่นโยบายดังกล่าวในลักษณะที่ผู้ใช้งานเข้าถึงได้ง่าย เพื่อให้บุคลากรที่เกี่ยวข้องทราบ และถือปฏิบัติเป็นไปตามที่นโยบายกำหนด

2) นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ต้องมีเนื้อหาครอบคลุมในเรื่อง

2.1) การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

1) การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ

2) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

2.2) การจัดการข้อมูลสารสนเทศและการรักษาความลับ

1) การจำแนกประเภทของข้อมูลสารสนเทศ (Information Classification) เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัย

2) การสำรองข้อมูล (Backup)

3) การควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls)

4) การป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personally IdentifiableInformation)

2.3) การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

1) การควบคุมการใช้งานของผู้ใช้งาน (End User)

2) การควบคุมดูแลผู้ให้บริการภายนอก (Supplier Relationships)

2.4) การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

1) การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์

2) การควบคุมการรับส่งข้อมูลสารสนเทศ (Information Transfer)

2.5) การป้องกันภัยคุกคามต่อระบบสารสนเทศ

1) การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

2) การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

2.6) การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

1.2 การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the Policies for Information Security) ต้องดำเนินการตรวจสอบ ทบทวน และประเมินนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และการสื่อสารตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อบริษัทฯ

2. แนวปฏิบัติการจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

เพื่อกำหนดมาตรการควบคุมการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ สำหรับส่วนงานต่างๆ ภายในบริษัทฯ ให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2.1 การจัดโครงสร้างภายในองค์กร (Internal Organization)

1) บทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities) ผู้บริหารต้องกำหนดรายละเอียดหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร ให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2) การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of Duties) ผู้บริหารต้องจัดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศออกจากกันอย่างชัดเจนเพื่อให้มีการสอบทานระหว่างกันได้

3) การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with Authorities) ต้องจัดให้มีรายชื่อและช่องทางสำหรับการติดต่อของหน่วยงานกำกับดูแล และหน่วยงานผู้ให้บริการที่สนับสนุนการทำงานของระบบสารสนเทศของบริษัท เพื่อให้สามารถติดต่อประสานงาน หรือขอความช่วยเหลือในกรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ พร้อมทั้งปรับปรุงรายชื่อ และช่องทางสำหรับติดต่อดังกล่าวให้เป็นปัจจุบัน

4) ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information Security in Project Management) การบริหารโครงการไม่ว่าจะเป็นประเภทใดของโครงการก็ตามต้องมีการระบุความมั่นคงปลอดภัยสารสนเทศของโครงการนั้น

2.2 การควบคุมอุปกรณ์สื่อสารประเภทพกพา และการปฏิบัติงานภายนอกองค์กร (Mobile Computing and Teleworking)

1) การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile Computing and Communication)

1.1) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

1.2) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

1.3) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์ และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

1.4) เจ้าหน้าที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์ และสื่อสารเคลื่อนที่ที่รับคืนด้วย

1.5) หากปรากฏความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

2) การปฏิบัติงานภายนอกสำนักงาน (Teleworking)

2.1) มีการกรอกแบบแบบฟอร์มการขอใช้งานจากภายนอก

2.2) มีการชี้แจงแผนงานและขั้นตอนปฏิบัติ

2.3) ตรวจสอบการทำงานอย่างเคร่งครัด

3. แนวปฏิบัติการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resources Security)

เพื่อควบคุมการสรรหาบุคลากรเข้ามาปฏิบัติงานภายในบริษัทฯ

3.1 ก่อนการจ้างงาน (Prior to Employment)

1) การคัดเลือก (Screening) ควรตรวจสอบ และยืนยันความถูกต้องจากเอกสาร ข้อมูล หรือบุคคลอ้างอิงของผู้สมัครงานดังนี้

1.1) เอกสารประวัติการทำงาน (Curriculum Vitae) ของผู้สมัครงาน

1.2) คุณสมบัติต่างๆ ของผู้สมัครงานตามที่ต้องการ

1.3) ข้อมูลที่เกี่ยวข้องกับผู้สมัครงานจากบุคลากรที่ได้รับการอ้างอิง

1.4) ประวัติการศึกษาของผู้สมัครงาน

1.5) ใบรับรอง หรือประกาศนียบัตรของผู้สมัครงาน

1.6) ข้อมูลหลักฐานแสดงตนของผู้สมัครงาน เช่น บัตรประชาชน หรือเอกสารระบุตัวบุคคลอื่นๆ

1.7) ประวัติหนี้สินของผู้สมัครงาน

1.8) ประวัติอาชญากรของผู้สมัครงาน

1.9) ประวัติโดยละเอียดสำหรับผู้สมัครงานที่จะทำงานกับเอกสารลับ หรือสำคัญ

1.10) กำหนดขั้นตอนปฏิบัติสำหรับการตรวจสอบประวัติของผู้สมัครงาน

2) ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) มีข้อปฏิบัติ ดังนี้

2.1) กำหนดบทบาท และหน้าที่ความรับผิดชอบของผู้รับการว่าจ้างในสัญญาจ้างงาน

2.2) สัญญาจ้างงานควรครอบคลุมประเด็นต่างๆ ดังนี้

1) กำหนดให้มีการปฏิบัติตามนโยบายความมั่นคงปลอดภัยของบริษัทฯ

2) กำหนดให้มีการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้อง

3) กำหนดหน้าที่ความรับผิดชอบในการจัดการกับข้อมูลและการบริหารจัดการทรัพย์สินขององค์กรอื่นๆ

4) กำหนดหน้าที่ความรับผิดชอบในการจัดการกับข้อมูลที่ได้รับจากองค์กรหรือหน่วยงานภายนอกอื่นๆ

5) กำหนดหน้าที่ความรับผิดชอบในการจัดการกับข้อมูลส่วนบุคคล เช่น การป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

6) กำหนดหน้าที่ความรับผิดชอบในการจัดการกับข้อมูลแม้ว่าจะอยู่ภายนอกบริษัทฯ หรือนอกเวลาทำการก็ตาม เช่น การทำงานของบริษัทฯ จากที่บ้าน

7) กำหนดให้มีการปฏิบัติตามกฎหมายลิขสิทธิ์ผลงานที่เกี่ยวข้อง

8) กล่าวถึงการดำเนินการทางวินัยและกฎหมาย รวมทั้งบทลงโทษ หากผู้รับการว่าจ้างไม่ปฏิบัติตามข้อกำหนดในสัญญาจ้าง

9) กำหนดให้มีการลงนามการรักษาความลับของบริษัทฯ

10) กล่าวถึงความเป็นเจ้าของลิขสิทธิ์ของผลงานที่เกิดขึ้นจากการปฏิบัติงานกับบริษัทฯ

11) กำหนดช่วงระยะเวลาที่ผู้รับการว่าจ้างสามารถใช้งานทรัพย์สินสารสนเทศของบริษัทฯ ได้

3.2 ระหว่างการจ้างงาน (During Employment)

1) หน้าที่ความรับผิดชอบของผู้บริหาร (Management Responsibilities)

1.1) จัดทำเอกสารซึ่งระบุถึงบทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของผู้รับการว่าจ้าง

1.2) กำหนดให้ผู้รับการว่าจ้างต้องทำความเข้าใจในบทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยก่อนที่จะอนุญาตให้เริ่มต้นปฏิบัติงานกับบริษัทฯ

1.3) หัวหน้างาน หรือผู้บังคับบัญชาควรมีหน้าที่ความรับผิดชอบในการสร้างแรงจูงใจให้ผู้รับการว่าจ้างปฏิบัติตามนโยบายความมั่นคงปลอดภัยของบริษัทฯ อย่างเคร่งครัด

1.4) หัวหน้างาน หรือผู้บังคับบัญชาควรมีหน้าที่ความรับผิดชอบในการสร้างความตระหนักให้ผู้รับการว่าจ้างเห็นความสำคัญในบทบาท และหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของตนเอง

1.5) หัวหน้างาน หรือผู้บังคับบัญชาควรมีหน้าที่ความรับผิดชอบในการสอดส่องดูแลการปฏิบัติตามนโยบายความมั่นคงปลอดภัยของผู้รับการว่าจ้าง

1.6) หัวหน้างาน หรือผู้บังคับบัญชาควรมีหน้าที่ความรับผิดชอบในการสร้างเสริมทักษะ ความรู้ และความสามารถของผู้รับการว่าจ้างอย่างต่อเนื่อง

2) การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information Security Awareness, Education, and Training)

2.1) กำหนดให้ผู้รับการว่าจ้างต้องทำการศึกษา และทำความเข้าใจในนโยบายความมั่นคงปลอดภัย บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยของตนเองก่อนที่จะอนุญาตให้เริ่มต้นปฏิบัติงานกับบริษัทฯ

2.2) บริษัทฯ ควรจัดโปรแกรมการอบรมที่เกี่ยวข้องกับการปฏิบัติงานทั่วไปเพื่อให้ผู้รับการว่าจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เช่น วิธีการใช้ระบบงาน วิธีการใช้งานซอฟต์แวร์สำเร็จรูป การแก้ปัญหาการใช้คอมพิวเตอร์เบื้องต้น การปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง เป็นต้น

2.3) จัดโปรแกรมการอบรม และสร้างความตระหนักด้านความมั่นคงปลอดภัยเพื่อให้ผู้รับการว่าจ้างได้เรียนรู้และทำความเข้าใจในหัวข้อเหล่านั้นอย่างสม่ำเสมอ เช่น นโยบายความมั่นคงปลอดภัยของบริษัทฯ ข้อกำหนดด้านความมั่นคงปลอดภัย ภัยคุกคามต่อความมั่นคงปลอดภัย ช่องทาง และวิธีการรายงานเมื่อประสบกับเหตุการณ์ความมั่นคงปลอดภัย การรู้จักการทำความเข้าใจ และการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัย กระบวนการลงโทษเมื่อมีการฝ่าฝืนนโยบายความมั่นคงปลอดภัย เป็นต้น

2.4) จัดโปรแกรมการอบรมและสร้างความตระหนักที่มีเนื้อหาช่วยให้ผู้รับการว่าจ้างสามารถปฏิบัติงานที่ตนเองรับผิดชอบได้เป็นอย่างดีและอย่างมั่นคงปลอดภัย

3) กระบวนการทางวินัย (Disciplinary Process)

3.1) กำหนดให้มีการรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัย เช่น การไม่ปฏิบัติตามนโยบายการตั้งรหัสผ่าน (การรายงานนี้จะนำไปสู่กระบวนการทางวินัยต่อไป)

3.2) กระบวนการทางวินัยควรมีความยุติธรรม เที่ยงธรรม และเหมาะสมต่อผู้ละเมิดความมั่นคงปลอดภัย

3.3) กระบวนการทางวินัยควรมีการลงโทษที่เข้มข้นมากขึ้นตามระดับความรุนแรงของการละเมิดความมั่นคงปลอดภัย

3.4) กระบวนการทางวินัยควรพิจารณาตามประเด็นเหล่านี้ของการละเมิดความมั่นคงปลอดภัย

3.5) สภาพหรือลักษณะการละเมิด เช่น ความรุนแรง ผลกระทบที่มีต่อองค์กร เป็นการกระทำผิดครั้งแรกหรือซ้ำหลายครั้งแล้ว การกระทำผิดนั้นเกิดจากการได้รับการอบรมไม่เพียงพอหรือไม่

3.6) กระบวนการทางวินัยควรจะสามารถลงโทษผู้รับการว่าจ้างที่กระทำความผิดร้ายแรงได้

3.7) กระบวนการทางวินัยควรจะสามารถยกเลิกสิทธิต่างๆ ยกเลิกการปฏิบัติงานได้โดยทันทีทันใดและ/หรือไม่อนุญาตให้เข้ามาภายในบริษัทฯ นับจากนั้น

3.8) กระบวนการทางวินัยควรมีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่บริษัทฯ ต้องปฏิบัติตาม

3.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or Change of Employment) มีข้อปฏิบัติ ดังนี้

1) กำหนดให้ผู้รับการว่าจ้างต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ เงื่อนไขการจ้างงาน และ/หรือข้อกำหนดต่างๆ ที่ได้กำหนดไว้

2) ฝ่ายบริหารทรัพยากรมนุษย์ หัวหน้างาน หรือผู้บังคับบัญชาควรเน้นย้ำให้ผู้รับการว่าจ้างทราบถึงการปฏิบัติตามเงื่อนไขในสัญญาจ้างจนกว่าจะสิ้นสุดการจ้างงาน

3) ฝ่ายบริหารทรัพยากรมนุษย์ หัวหน้างาน หรือผู้บังคับบัญชาควรเน้นย้ำให้ผู้รับการว่าจ้างทราบถึงการปฏิบัติตามข้อตกลงการรักษาความลับของบริษัทฯ

4) ฝ่ายบริหารทรัพยากรมนุษย์ หัวหน้างาน หรือผู้บังคับบัญชาควรร่วมกันกำหนดให้ผู้ที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงาน ต้องปฏิบัติตามข้อกำหนดต่างๆ ที่ได้กำหนดไว้จนกว่าจะสิ้นสุดสัญญาจ้าง

5) กรณีที่ผู้ที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานยังคงต้องปฏิบัติหน้าที่ที่ตนรับผิดชอบต่อไปอีกช่วงระยะเวลาหนึ่ง สัญญาจ้างงานควรครอบคลุมเงื่อนไข และระยะเวลาดังกล่าวด้วย ฝ่ายบริหารทรัพยากรมนุษย์ หัวหน้างาน หรือผู้บังคับบัญชาควรแจ้งให้ผู้รับการว่าจ้างทราบถึงการเปลี่ยนแปลงที่เกี่ยวข้องกับบุคลากรของบริษัทฯ สวัสดิการ เงื่อนไขการปฏิบัติงาน หรือการเปลี่ยนแปลงอื่นๆ ที่กระทบต่อผู้รับการว่าจ้าง

4. แนวปฏิบัติการบริหารจัดการทรัพย์สิน (Asset Management)

เพื่อให้สินทรัพย์ของบริษัทฯ ได้รับการป้องกัน และปกป้องอย่างเหมาะสม ทำให้แน่ใจว่าสารสนเทศขององค์กรได้รับการปกป้องในระดับที่เหมาะสม และเพื่อลดความเสี่ยงต่อการถูกเปิดเผยข้อมูลขององค์กรโดยไม่ได้รับอนุญาตป้องกันการนำทรัพย์สินสารสนเทศไปใช้โดยผิดวัตถุประสงค์ และเกิดความเสียหายกับทรัพย์สินสารสนเทศ

4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน มีข้อปฏิบัติดังนี้

1) บัญชีทรัพย์สิน (Inventory of Assets) เพื่อบริหารจัดการ และควบคุมทรัพย์สินคอมพิวเตอร์ มีข้อปฏิบัติดังนี้

1.1) ให้หน่วยงานจัดทำทะเบียนบัญชีทรัพย์สิน (อุปกรณ์คอมพิวเตอร์ เครือข่าย และ Software) ให้ครบถ้วน ระบุรายละเอียด ได้แก่ ชื่ออุปกรณ์ คุณลักษณะเฉพาะของอุปกรณ์ บริษัทที่ผลิต

1.2) ให้หน่วยงานขึ้นทะเบียนทรัพย์สินที่ได้รับจัดสรรให้ใหม่ทุกครั้ง

1.3) ควรมีการตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินอย่างน้อยปีละ 1 ครั้ง

2) ผู้ถือครองทรัพย์สิน (Ownership of Assets) เพื่อติดตาม และควบคุมทรัพย์สินคอมพิวเตอร์ มีข้อปฏิบัติดังนี้

2.1) หน่วยงานต้องระบุรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์ เครือข่ายและ Software โดยระบุชื่อ สกุล ตำแหน่งและหน่วยงาน อย่างครบถ้วน

2.2) ให้มีการปรับปรุงรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์ เครือข่าย และ Software ทุกครั้งเมื่อมีการเปลี่ยนแปลง

3) การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable Use of Assets) เพื่อการบริหารจัดการอุปกรณ์คอมพิวเตอร์ให้เหมาะสม ก่อให้เกิดประสิทธิภาพสูงสุด รวมทั้งมีความปลอดภัยจากความเสียหายที่อาจเกิดขึ้นได้ มีข้อปฏิบัติดังนี้

3.1) จัดทำกฎ ระเบียบ หลักเกณฑ์การจัดสรรอุปกรณ์คอมพิวเตอร์ให้เหมาะสมกับภารกิจ และบุคลากร และมีการทบทวนปีละ 1 ครั้ง

3.2) จัดทำคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์ เครือข่าย และ Software รวมทั้งกำหนดขั้นตอนการดูแลรักษาเป็นรายอุปกรณ์

3.3) จัดให้มีการตรวจสอบ บำรุงรักษา อุปกรณ์คอมพิวเตอร์ เครือข่าย และ Software ให้มีความพร้อมใช้งานอย่างน้อยปีละ 1 ครั้ง

3.4) ประกาศใช้ กฎ ระเบียบ หลักเกณฑ์ และคู่มือการใช้งานอุปกรณ์คอมพิวเตอร์ เครือข่าย และ Software ให้บุคลากรในหน่วยงานรับทราบ และถือปฏิบัติอย่างเคร่งครัด

4) การคืนทรัพย์สิน (Return of Assets)

4.1) กระบวนการสิ้นสุด หรือเปลี่ยนการจ้างงานควรแจ้งให้ผู้รับการว่าจ้างคืนทรัพย์สินขององค์กร ดังนี้

1) ซอฟต์แวร์

2) เอกสาร หรือคู่มือสำคัญ

3) ข้อมูล ซึ่งรวมถึงข้อมูลบนสื่อบันทึกข้อมูล

4) อุปกรณ์ ซึ่งรวมถึงอุปกรณ์ประเภทพกพา

5) บัตรเข้าห้อง บัตรผ่าน หรือบัตรอื่นๆ

4.2) กระบวนการสิ้นสุด หรือเปลี่ยนการจ้างงานควรแจ้งให้ผู้รับการว่าจ้างลบข้อมูลสำคัญขององค์กรที่เก็บไว้บนอุปกรณ์ส่วนตัวของตนเองทิ้งไป โดยที่การลบทิ้งนั้นจะต้องไม่สามารถเรียกข้อมูลกลับคืนมาได้

4.3) องค์กรควรมีกระบวนการบริหารจัดการ และจัดเก็บองค์ความรู้สำคัญของผู้รับการว่าจ้างเพื่อให้ความรู้เหล่านั้นยังคงอยู่กับบริษัทฯ ต่อไปแม้บุคคลเหล่านั้นจะลาออกไปแล้ว

4.2 การจัดชั้นความลับของสารสนเทศ (Information Classification) เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม มีข้อปฏิบัติดังนี้

1) ชั้นความลับของสารสนเทศ (Classification of Information) มีข้อปฏิบัติดังนี้

1.1) ให้หน่วยงานจัดทำรายการสารสนเทศโดยระบุชื่อระบบสารสนเทศ คุณสมบัติ การจัดเก็บ และภาษาที่ใช้ในการพัฒนา ระบุกลุ่มผู้ใช้สารสนเทศและระดับสารสนเทศ

1.2) ให้หน่วยงานกำหนดชั้นความลับสารสนเทศ ได้แก่ ไม่เป็นความลับ เป็นความลับระดับน้อย ปานกลาง มาก ไม่สามารถเผยแพร่ได้

1.3) กำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ

2) การบ่งชี้สารสนเทศ (Labeling of Information) มีข้อปฏิบัติดังนี้

2.1) จัดทำป้ายชื่อตามทะเบียนบัญชีทรัพย์สินและขั้นตอนการใช้งานติดที่อุปกรณ์คอมพิวเตอร์ทุกชิ้น

2.2) ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุม และรักษาความปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุม และรักษาความปลอดภัย

3) การจัดการทรัพย์สิน (Handing of Assets)

3.1) กำหนดมาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกบริษัทฯ เช่น กำหนดให้มีการใส่รหัสผ่านก่อนการใช้อุปกรณ์

3.2) กำหนดให้มีมาตรการในการทำลายอุปกรณ์หรือสื่อบันทึกข้อมูลที่จัดเก็บข้อมูลสำคัญ เพื่อป้องกันการรั่วไหลของข้อมูล

3.3) การควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ ควรมีการทดสอบการใช้งานระบบให้ถูกต้องเหมาะสม และมีการบันทึกการเปลี่ยนแปลงแก้ไขทุกครั้ง รวมทั้งแจ้งให้หน่วยงานที่เกี่ยวข้องทราบ

4.3 การจัดการสื่อบันทึกข้อมูล (Media Handing)

1) การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of Removable Media)

1.1) กรณีที่ไม่มีความจำเป็นต้องใช้ข้อมูล ต้องจัดให้มีกระบวนการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล และไม่ให้สามารถกู้คืนข้อมูลได้

2) การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

2.1) ต้องจัดให้มีกระบวนการทำลายสื่อบันทึกข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล ที่เป็นความลับ หรือมีความสำคัญ

2.2) กรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่

3) การขนย้ายสื่อบันทึก (Physical Media Transfer) ต้องจัดให้มีกระบวนการดูแลรักษาความปลอดภัยกรณีที่มีการเคลื่อนย้ายสื่อบันทึกข้อมูล ออกจากพื้นที่ทำการ

5. แนวปฏิบัติการควบคุมการเข้าถึง (Access Control)

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของบริษัทฯ ป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่ข้อมูล และเพื่อให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมเข้าถึงและการใช้งานระบบสารสนเทศของบริษัทฯ

5.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirement for Access Control) มีข้อปฏิบัติดังนี้

1) นโยบายควบคุมการเข้าถึง (Access Control Policy) อย่างเป็นลายลักษณ์อักษร ปรับปรุงตามระยะเวลาอันสมควร มีข้อปฏิบัติดังนี้

1.1) สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า-ออกที่รัดกุม และอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

1.2) ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

1.3) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูล และระบบข้อมูลได้

1.4) ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของบริษัทฯ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

1.5) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาต และไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

2) การเข้าถึงเครือข่าย และบริการเครือข่าย (Access to Networks and Network Service) การเข้าถึงข้อมูลและระบบสารสนเทศ จะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดยผู้บังคับบัญชา

5.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management) มีข้อปฏิบัติดังนี้

1) การลงทะเบียน และถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration)

1.1) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

1.2) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

1.3) ผู้ดูแลระบบต้องมีการตรวจสอบ และมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

1.4) ผู้ดูแลระบบต้องมอบเอกสารรับรองสิทธิการเข้าถึงแก่ผู้ใช้ และกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

1.5) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อผู้ใช้งานนั้นทำการลาออก หรือเปลี่ยนตำแหน่ง

1.6) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องตรวจสอบ หรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

2) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

2.1) มีการแสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

2.2) ผู้ดูแลระบบ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

2.3) ผู้ดูแลระบบ ต้องจัดเก็บเอกสารการมอบหมายสิทธิให้แก่ผู้ใช้งาน

2.4) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

3) การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of Privileged Access Right)

3.1) มีการแสดงกระบวนการในการมอบหมาย หรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

3.2) ผู้ดูแลระบบ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ แต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

3.3) ผู้ดูแลระบบต้องจัดเก็บเอกสารการมอบหมายสิทธิให้แก่ผู้ใช้งาน

3.4) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว หรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

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

5) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

5.1) สิทธิการเข้าถึงข้อมูลของผู้ใช้ควรได้รับการพิจารณาทบทวนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เช่น ทุกๆ 6 เดือน และทุกครั้งที่มีการปรับเปลี่ยน เช่น การย้ายหน่วยงาน การเลื่อนตำแหน่ง

5.2) สิทธิการเข้าถึงข้อมูลควรได้รับการทบทวน และจัดสรรให้ใหม่เมื่อมีการเคลื่อนย้ายบุคลากรภายในบริษัทฯ

5.3) การให้อำนาจสำหรับสิทธิการเข้าถึงพิเศษ ควรมีการทบทวนบ่อยกว่า เช่น ทำทุกๆ 3 เดือน

5.4) การจัดสรรสิทธิพิเศษควรได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อให้มั่นใจได้ว่าไม่มีสิทธิพิเศษกับผู้ใช้ที่ไม่ได้รับมอบอำนาจ

5.5) ความเปลี่ยนแปลงของผู้ใช้ที่ได้รับสิทธิพิเศษควรถูกบันทึกเพื่อการทบทวน

6) การถอดถอนสิทธิในการเข้าถึง (Removal of Access Rights)

6.1) ดำเนินการเพิกถอน หรือเปลี่ยนสิทธิการเข้าถึงระบบงานของผู้ที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

6.2) ดำเนินการเพิกถอน หรือเปลี่ยนสิทธิการเข้าถึงทางกายภาพของผู้ที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

6.3) ดำเนินการเพิกถอน ลบ หรือเปลี่ยนรหัสผ่านของผู้ที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

6.4) ดำเนินการขอคืนกุญแจ หรือบัตรสำหรับเข้าพื้นที่ต่างๆ และไม่อนุญาตให้ผู้ที่สิ้นสุดการว่าจ้างใช้งานกุญแจหรือบัตรเหล่านั้น

6.5) ดำเนินการเพิกถอนหรือยกเลิกการลงทะเบียน หรือสมัครเป็นสมาชิกต่างๆ ของผู้ที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงาน

6.6) ดำเนินการลบ หรือเปลี่ยนชื่อของผู้ที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงานออกจากเอกสารต่างๆ ขององค์กรที่มีชื่อของบุคคลดังกล่าวอยู่ในนั้น

6.7) ดำเนินการเพิกถอน ลบ สิทธิในการเข้าถึงของผู้ที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงานก่อนวันสุดท้ายของการมาทำงานหรือในสัญญาจ้าง สำหรับกรณีที่

1) การเข้าถึงระบบงาน หรือข้อมูลที่ยังสามารถเข้าถึงได้อยู่มีความเสี่ยงต่อความเสียหายต่อบริษัทฯ ในระดับสูง

2) ผู้บริหารคาดว่าอาจมีการแก้แค้น หรือตอบโต้กันเกิดขึ้นกับผู้ที่สิ้นสุดการว่าจ้าง หรือถูกเปลี่ยนการจ้างงาน

3) บทบาท และหน้าที่ความรับผิดชอบของผู้ที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงานนั้นมีความเสี่ยงต่อความเสียหายที่อาจเกิดขึ้นกับบริษัทฯ

4) ทรัพย์สินสารสนเทศที่ถูกเข้าถึงนั้นมีคุณค่า หรือมีความสำคัญสูงต่อบริษัทฯ

5.3 การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) มีข้อปฏิบัติดังนี้

1) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

1.1) การเข้าถึงสารสนเทศ และฟังก์ชั่นในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง

1.2) การใช้งานระบบสารสนเทศที่สำคัญ ไม่ว่าจะเป็นระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) ต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของฝ่ายงานนั้นๆ เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ 1 ครั้ง

2) ขั้นตอนปฏิบัติสำหรับล็อคอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure Log-on Procedures) กำหนดการเข้าถึงระบบต้องมีการควบคุมโดยผ่านขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบ ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

2.1) ต้องตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

2.2) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนสำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงานอย่างน้อย 1 วิธี

2.3) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญ หรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

2.4) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

2.5) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

2.6) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

3) ระบบบริหารจัดการรหัสผ่าน (Password Management System)

3.1) ผู้ใช้ควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อคอินเข้าสู่ระบบงาน

3.2) ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

3.3) ควรกำหนดรหัสผ่าน ให้มีตัวอักษรความยาวขั้นต่ำ 6-8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน (เช่น “#”) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

3.4) ผู้ใช้งานไม่ควรใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

3.5) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

3.6) ผู้ใช้งานควรเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือมีผู้อื่นล่วงรู้

3.7) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

3.8) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่างๆ ที่ตนใช้งาน

3.9) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

3.10) กรอบระยะเวลาในการเปลี่ยนรหัสผ่าน ต้องไม่เกิน 90 วัน

4) การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs) ควรจำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

4.1) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

4.2) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

4.3) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

4.4) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

4.5) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

5) การควบคุมการเข้าซอร์สโคดของโปรแกรมการเข้าถึงซอร์สโคดของโปรแกรมต้องมีการจำกัดและควบคุม

6. แนวปฏิบัติการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

เพื่อควบคุมทรัพย์สินสารสนเทศ และโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของบริษัทฯ ทางด้านกายภาพ ควบคุมการใช้งาน และบำรุงรักษาอุปกรณ์สารสนเทศให้ระบบสารสนเทศอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน และป้องกันการเข้าถึงทรัพย์สินสารสนเทศหรือการถูกเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

6.1 พื้นที่ที่ต้องการการรักษาความมั่นคง (Secure Area)

1) ขอบเขต หรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter) มีข้อปฏิบัติดังนี้

1.1) การจัดทำบริเวณล้อมรอบต้องมีการจัดเป็นพื้นที่ควบคุม โดยสามารถแบ่งออกได้ ดังนี้

1) พื้นที่ทำงาน

2) พื้นที่ติดตั้งและจัดการอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย

3) พื้นที่ใช้งานระบบเครือข่ายไร้สาย

1.2) มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายในบริษัทฯ

1.3) ประตู หรือทางเข้าสำนักงาน หรืออาคารออกแบบเพื่อป้องกันการบุกรุกทางกายภาพ

1.4) ประตู หรือทางเข้าของห้องควบคุมระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายต้องมีระบบที่สามารถล็อคได้ เพื่อป้องกันการบุกรุกทางกายภาพ

1.5) ต้องแยกพื้นที่สำหรับระบบเทคโนโลยีสารสนเทศของบริษัทฯ ออกจากพื้นที่ที่มีการดูแล หรือบริหารจัดการโดยผู้ให้บริการภายนอก

2) การควบคุมการเข้าออกทางกายภาพ (Physical Entry Controls) มีข้อปฏิบัติดังนี้

2.1) จัดให้มีการควบคุมการเข้าออก

2.2) อนุญาตให้ผ่านเข้าออกเฉพาะผู้ที่มีหน้าที่ปฏิบัติงานภายในพื้นที่ หรือผู้ที่ได้รับอนุญาตตามความจำเป็นเท่านั้น

2.3) มีการกำหนดสิทธิในการเข้าถึงบริเวณที่ต้องมีการรักษาความปลอดภัย

2.4) ต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาต้นสังกัด และฝ่ายสารสนเทศ

3) การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing Offices, Rooms and Facilities) มีข้อปฏิบัติดังนี้

3.1) เจ้าหน้าที่ทุกคนต้องปฏิบัติการป้องกันทรัพย์สิน

3.2) เจ้าหน้าที่ต้องออกจากระบบ เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

3.3) ต้องมีการจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย เช่น ในตู้เอกสารที่มีกุญแจล็อค และไม่ทิ้งเอกสารที่สำคัญไว้บนโต๊ะ เพื่อความปลอดภัยของข้อมูล

3.4) ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ต่างๆ เช่น เครื่องคอมพิวเตอร์ เครื่องพิมพ์เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น โดยไม่ได้รับอนุญาต

3.5) นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

4) การป้องกันภัยคุกคามจากภายนอก และสภาพแวดล้อม (Protecting Against External and Environmental Threats) มีข้อปฏิบัติดังนี้

บริเวณที่ต้องมีการรักษาความปลอดภัยที่ระดับความสำคัญสูงสุด คือ ห้องคอมพิวเตอร์ ต้องปฏิบัติตามในทุกข้อและบริเวณที่ต้องมีการรักษาความปลอดภัยอื่นๆ ควรปฏิบัติตามความจำเป็น ดังนี้

4.1) จัดให้มีผนังที่แข็งแรง ติดตั้งจากพื้นห้องถึงเพดานด้านบน เพื่อป้องกันการบุกรุก

4.2) จัดให้มีระบบป้องกันอัคคีภัย โดยใช้ระบบตรวจจับควันความไวสูงที่มีความสามารถในการตรวจจับฝุ่นควัน ผง และระบบดับเพลิงอัตโนมัติ

4.3) จัดให้มีระบบควบคุมน้ำรั่ว การยกระดับพื้น และระบบตรวจจับน้ำรั่ว เพื่อตรวจจับการกลั่นตัวของหยดน้ำภายในห้องคอมพิวเตอร์

4.4) จัดให้มีระบบควบคุมอุณหภูมิ และความชื้น เครื่องปรับอากาศที่สามารถตั้งอุณหภูมิ และควบคุมความชื้นภายในห้องให้มีสภาพแวดล้อมที่เหมาะสม

4.5) จัดให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

5) การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in Secure Areas) มีข้อปฏิบัติดังนี้

5.1) ต้องปฏิบัติงานตามคู่มือปฏิบัติงาน และคู่มือการจัดการอุปกรณ์ต่างๆ อย่างเคร่งครัด

5.2) ห้ามนำสิ่งของต่อไปนี้เข้าพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยโดยเด็ดขาด

1) อาหาร หรือเครื่องดื่ม

2) วัตถุไวไฟ หรือเชื้อเพลิง

3) กล่องบันทึกภาพ หรือเสียง

5.3) การปฏิบัติงานนอกเหนือจากเวลางานปกติ ต้องผ่านการอนุมัติจากผู้บังคับบัญชาต้นสังกัด และฝ่ายสารสนเทศ

5.4) การขนย้ายอุปกรณ์ใดๆ เข้า-ออกห้อง ต้องขออนุมัติ และได้รับความเห็นชอบจากฝ่ายสารสนเทศ

6) พื้นที่สำหรับรับส่งสิ่งของ (Delivery and Loading Areas) มีข้อปฏิบัติดังนี้

6.1) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบ หรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

6.2) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่ หรือบริเวณส่งมอบนั้น

6.3) ควรจัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในบริษัทฯ

6.4) ต้องตรวจสอบวัสดุ หรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้น ไปยังพื้นที่ที่มีการใช้งาน

6.5) กำหนดให้มีการลงทะเบียน เพื่อให้สอดคล้องกับขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของบริษัทฯ

6.2 อุปกรณ์ (Equipment)

1) การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Setting and Protection) มีข้อปฏิบัติดังนี้

1.1) ต้องจัดวางอุปกรณ์ในพื้นที่ และบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในหน่วยงานหรือองค์กรให้น้อยที่สุด

1.2) ต้องจัดวางระบบเทคโนโลยีสารสนเทศในตำแหน่งที่เหมาะสมเพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญจากบุคคลภายนอก โดยการหันหน้าจอเข้ามาภายในโดยไม่ให้บุคคลผู้ซึ่งไม่มีสิทธิสามารถมองเห็นหน้าจอนั้นได้

1.3) ต้องแยกอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่ง เพื่อดูแลความมั่นคงปลอดภัย

1.4) ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณ หรือพื้นที่ห้องควบคุมระบบเครือข่าย/ระบบคอมพิวเตอร์/ระบบเครื่องคอมพิวเตอร์แม่ข่าย

1.5) ดำเนินการตรวจสอบระดับอุณหภูมิ และดูแลสภาพแวดล้อมภายในบริเวณห้องควบคุมระบบเครือข่าย/ระบบคอมพิวเตอร์/ระบบเครื่องคอมพิวเตอร์แม่ข่าย เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว

2) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) มีข้อปฏิบัติดังนี้

2.1) ต้องมีระบบสนับสนุนการทำงานของระบบสารสนเทศของบริษัทฯ ที่เพียงพอต่อความต้องการ

2.2) จัดให้มีแหล่งกำลังไฟฟ้าสำรอง โดยแยกเครื่องปั่นไฟของสำนักงาน และเครื่องปั่นไฟของระบบคอมพิวเตอร์ออกจากกัน

2.3) จัดให้มีเครื่องสำรองไฟฟ้า และปรับแรงดันไฟฟ้าอัตโนมัติที่สามารถทำงานเมื่อเกิดปัญหาขัดข้องทางไฟฟ้าโดยไม่ทำความเสียหายให้แก่อุปกรณ์ และระบบงานสารสนเทศ

2.4) จัดให้มีระบบควบคุมอุณหภูมิ เพื่อควบคุมอุณหภูมิและความชื้นให้คงที่

2.5) จัดให้มีระบบเฝ้าดูและรายงานเมื่อพบข้อพิดพลาด

2.6) จัดให้มีการตรวจสอบหรือทดสอบ ระบบและอุปกรณ์สนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบงานทำงานได้ตามปกติ

3) ความมั่นคงปลอดภัยของการเดินสายสัญญาณ และสายสื่อสาร (Cabling Security) มีข้อปฏิบัติดังนี้

3.1) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

3.2) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหาย

3.3) ให้เดินสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

3.4) ทำป้ายชื่อสำหรับสายสัญญาณ และบนอุปกรณ์เพื่อป้องกันการตัดสัญญาณผิดเส้น

3.5) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนถูกต้อง

3.6) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

3.7) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม สำหรับระบบสารสนเทศที่สำคัญ

3.8) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

4) การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) มีข้อปฏิบัติดังนี้

4.1) ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

4.2) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

4.3) จัดเก็บบันทึกกิจกรรมการบำรุงอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินภายหลัง

4.4) จัดเก็บบันทึกปัญหาและขอบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

4.5) ควบคุม และสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในองค์กร

4.6) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

5) การนำทรัพย์สินสารสนเทศออกนอกสำนักงาน (Removal of Assets) มีข้อปฏิบัติดังนี้

5.1) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกบริษัทฯ

5.2) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกบริษัทฯ

5.3) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้นอกบริษัทฯ

5.4) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

5.5) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้นอกบริษัทฯ เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

6) ความมั่นคงปลอดภัยของอุปกรณ์ และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน มีข้อปฏิบัติดังนี้

6.1) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ หรือทรัพย์สินขององค์กรออกไปใช้งาน

6.2) ไม่ทิ้งอุปกรณ์ หรือทรัพย์สินของบริษัทฯ ไว้โดยลำพังในที่สาธารณะ

6.3) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์ หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

7) ความมั่นคงปลอดภัยสำหรับการกำจัด หรือทำลายอุปกรณ์ หรือนำอุปกรณ์ไปใช้งานอย่างอื่น มีข้อปฏิบัติดังนี้

7.1) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

7.2) มีมาตรการ หรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

8) อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended User Equipment) มีข้อปฏิบัติดังนี้

8.1) ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ ระบบงานคอมพิวเตอร์ที่ใช้งานหรือเครื่องคอมพิวเตอร์ที่พกพา โดยทันทีเมื่อเสร็จสิ้นงาน

8.2) ผู้ใช้งาน ต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน หรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

8.3) ผู้ดูแลระบบ ต้องกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

9) นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) มีข้อปฏิบัติดังนี้

9.1) ต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลต่างๆ เช่นThumb Drive และ External Hard Disk ที่มีข้อมูลสารสนเทศที่จัดเก็บ หรือบันทึกอยู่ไม่ให้วางทิ้งไว้บนโต๊ะทำงาน หรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (Clear Desk)

9.2) ต้องมีการควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (Clear Screen) เช่น การตัดออกจากระบบ (Session Time Out) และการล็อคหน้าจอ (Lock Screen) อัตโนมัติ เป็นต้น

7. แนวปฏิบัติความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

เพื่อให้การจัดการด้านการสื่อสาร และดำเนินงานต่างๆ ของเครือข่ายสารสนเทศต่างๆ ขององค์กร มีแนวทางปฏิบัติที่มีขั้นตอนชัดเจน และมีความมั่นคงปลอดภัย

7.1 ขั้นตอนการปฏิบัติงาน และหน้าที่ความรับผิดชอบ (Operations Procedures and Responsibilities) มีข้อปฏิบัติดังนี้

1) ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures) ต้องจัดให้มีวิธีปฏิบัติงานด้านระบบสารสนเทศที่สำคัญเป็นลายลักษณ์อักษร เพื่อให้พนักงานปฏิบัติการคอมพิวเตอร์ (Computer Operator) สามารถปฏิบัติงานได้อย่างถูกต้อง และเป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และต้องทบทวนวิธีปฏิบัติดังกล่าวให้เป็นปัจจุบันอยู่เสมอ รวมทั้งจัดให้วิธีปฏิบัติงานดังกล่าวอยู่ในสภาพที่พร้อมใช้งาน และเข้าถึงได้

2) การบริหารจัดการการเปลี่ยนแปลง (Change Management) ต้องจัดให้มีการควบคุมการปฏิบัติงานอย่างเคร่งครัด โดยเฉพาะในกรณีที่มีการเปลี่ยนแปลงโครงสร้างบริษัทฯ ขั้นตอนการปฏิบัติงาน หรือการทำงานของระบบงานต่างๆ

3) การบริหารจัดการขีดความสามารถของระบบ (Capacity Management) ต้องติดตามประสิทธิภาพการทำงานของระบบงาน และอุปกรณ์สารสนเทศที่สำคัญ ให้ทำงานได้อย่างต่อเนื่อง และมีประสิทธิภาพ เพื่อใช้เป็นข้อมูลในการประเมินสมรรถภาพ และความเพียงพอ (Capacity) ของระบบงาน และอุปกรณ์สารสนเทศ

4) การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) และใช้งานจริง (Production Environment) ออกจากกัน และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่แยกไว้ต่างหากภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้

7.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware) มีข้อปฏิบัติดังนี้

1) มีระบบการตรวจจับ การป้องกัน และการกู้คืนข้อมูลจากผู้ที่ไม่ประสงค์ดี

2) มีการจัดอบรมเจ้าหน้าที่ให้ทราบถึงพฤติกรรมที่พึงประสงค์ต่อการใช้งานที่ถูกต้อง ปลอดภัย และไม่มีความเสี่ยง

3) มีการติดตั้งระบบป้องกันโปรแกรมที่ไม่ประสงค์ดี

4) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัทฯ ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

5) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้ง และแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของบริษัทฯ

7.3 การสำรองข้อมูล (Back up) มีข้อปฏิบัติดังนี้

1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น External Hard Disk เป็นต้น ให้เป็นปัจจุบันอย่างสม่ำเสมอ

2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

3) กำหนดระยะเวลาการสำรองข้อมูลตามความเหมาะสมของข้อมูล

4) เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศจัดทำแผนการสำรองข้อมูลของฝ่ายผู้ใช้งานและแจ้งให้พนักงานฝ่ายที่เกี่ยวข้องรับทราบและหยุดการใช้งานข้อมูลตามเวลาดังกล่าว

7.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

1) การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event Logging)

1.1) ต้องจัดให้มีการบันทึก และจัดเก็บหลักฐาน (Logs) ของระบบงานที่มีความสำคัญประเภทต่างๆ ดังต่อไปนี้

1) หลักฐานการเข้าถึงพื้นที่หวงห้าม (Physical Access Log) โดยต้องมีรายละเอียดเกี่ยวกับบุคคลที่เข้าถึง ความพยายามในการเข้าถึง (ถ้ามี) และวัน เวลาที่ผ่านเข้า-ออก โดยจัดเก็บเป็นระยะเวลา ไม่น้อยกว่า 6 เดือน

2) หลักฐานการเข้าถึงระบบปฏิบัติการ ฐานข้อมูล ระบบเครือข่ายคอมพิวเตอร์ (Authentication Log) โดยต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน วัน เวลาที่เข้าใช้งาน และความพยายามในการเข้าใช้งาน โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 6 เดือน

3) หลักฐานการเข้าถึง และใช้งานระบบสารสนเทศ โดยต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งานหมายเลขประจำเครื่องที่ใช้งาน (Client IP Address) (ถ้ามี) วัน เวลาที่มีการใช้งาน Order ID และ Account ID โดยจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 2 ปี

4) หลักฐานการใช้งานอินเทอร์เน็ตที่เกิดขึ้นจากการใช้งานผ่านเครือข่ายสารสนเทศ โดยต้องมีรายละเอียดเกี่ยวกับบัญชีผู้ใช้งาน หมายเลขประจำเครื่องที่ใช้งาน (IP Address) หมายเลขอินเทอร์เน็ต (Organization IP Address) วัน เวลาที่มีการใช้งาน และที่อยู่ของเว็บไซต์ปลายทาง (Full URL) โดยจัดเก็บเป็นระยะเวลาไม่น้อยกวา 2 ปี

2) การป้องกันข้อมูลล็อก (Protection of Log Information) ต้องจัดให้มีการป้องกันข้อมูล และระบบการบันทึกและจัดเก็บหลักฐานการใช้งานเกี่ยวกับระบบสารสนเทศจากการถูกเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต

3) ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบ และเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and Operator Logs) กิจกรรมของผู้ดูแลระบบ และเจ้าหน้าที่ปฏิบัติการต้องมีการบันทึกไว้เป็นข้อมูลล็อก และมีการตรวจสอบอย่างสม่ำเสมอ

4) การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization) ต้องกำหนดระบบเวลาของอุปกรณ์ และระบบสารสนเทศที่มีความสำคัญให้ตรงกับเวลาอ้างอิงสากล

7.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software) มีข้อปฏิบัติคือ การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of Software on Operational Systems) ต้องจัดให้มีขั้นตอนเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบงาน รวมทั้งจัดให้มีมาตรการเพื่อจำกัดการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน

7.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management) มีข้อปฏิบัติดังนี้

1) การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

1.1) ต้องจัดให้มีการติดตามข้อมูลข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่อาจเป็นความเสี่ยงต่อระบบสารสนเทศของผู้ประกอบธุรกิจอย่างทันต่อเหตุการณ์โดยต้องกำหนดแนวทางดำเนินการดังนี้

1) กำหนดผู้มีหน้าที่รับผิดชอบในการจัดการเกี่ยวกับช่องโหว่ทางเทคนิค โดยครอบคลุมถึงการประเมินความเสี่ยงของทรัพย์สินสารสนเทศที่เกี่ยวข้อง

2) มีการทดสอบการบุกรุกระบบ (Penetration Test) กับระบบงานที่มีความสำคัญทุกระบบ โดยต้องจัดทำการทดสอบอย่างน้อยทุก 3 ปี

3) มีการบันทึก และจัดเก็บหลักฐานเพื่อการตรวจสอบในการดำเนินการต่างๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ทางเทคนิค

2) การจำกัดการติดตั้งซอฟแวร์ (Restrictions on Software Installation) ผู้ใช้งานต้องปฏิบัติตามกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์ ไม่ติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ขององค์กร

7.7 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit) มีข้อปฏิบัติดังนี้

1) ต้องจัดให้มีการวางแผนการตรวจสอบระบบสารสนเทศให้สอดคล้องกับความเสี่ยงที่ได้ประเมินไว้

2) ต้องกำหนดขอบเขตการตรวจสอบทางเทคนิค (Technical Audit Test) ให้ครอบคลุมจุดเสี่ยงที่สำคัญและต้องควบคุมการตรวจสอบดังกล่าวไม่ให้กระทบต่อการปฏิบัติงานตามปกติ

3) ในกรณีที่การตรวจสอบระบบสารสนเทศมีโอกาสกระทบต่อความพร้อมใช้งานของระบบ (SystemAvailability) ต้องจัดให้มีการทดสอบนอกเวลาทำการ

8. แนวปฏิบัติความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

เพื่อป้องกันการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายคอมพิวเตอร์เพื่อป้องกันความผิดพลาดของระบบสารสนเทศจากความถูกต้องของข้อมูล การสูญหายและการแก้ไขอย่างไม่ถูกต้อง รักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในบริษัทฯ และระหว่างระบบเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอก และเพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

8.1 การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management) มีข้อปฏิบัติดังนี้

1) มาตรการเครือข่าย (Network Controls)

1.1) ต้องจัดให้มีการบริหารจัดการ และควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคง ปลอดภัย โดยควรมีการดำเนินการดังนี้

1) แบ่งแยกหน้าที่ความรับผิดชอบระหว่าง Network Administrator และ Computer Administrator ออกจากกัน พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบ และขั้นตอนในการบริหารจัดการระบบ และอุปกรณ์เครือข่ายให้ชัดเจน

2) จำกัดการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างเครือข่าย เช่น จำกัดการใช้งานจุดเชื่อมต่อระบบเครือข่าย (Port Outlet)

3) เปิดใช้งาน Service Port ที่เชื่อมต่อตามความจำเป็น พร้อมทั้งมีวิธีการเพื่อระบุถึงอุปกรณ์ที่เชื่อมต่อ (Authenticate) อย่างชัดเจน เช่น IP Address และประเภทของอุปกรณ์ เป็นต้น

4) มีการควบคุมการเชื่อมต่อกับระบบเครือข่ายสาธารณะ (Public Network) และระบบเครือข่ายไร้สาย (Wireless Network)

5) มีการบันทึก และจัดเก็บหลักฐาน (Logs) เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้อง หรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

2) ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services) ต้องจัดทำข้อตกลงการใช้บริการระบบเครือข่ายคอมพิวเตอร์ (Network Services Agreements) กับผู้ให้บริการภายนอก

3) การแบ่งแยกเครือข่าย (Segregation in Network) ต้องจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขต (Domain) ของระบบเครือข่ายย่อยอย่างชัดเจน และจัดให้มีกระบวนการควบคุมการเข้าถึงขอบเขตดังกล่าว โดยสอดคล้องเหมาะสมกับระดับความต้องการด้านการรักษาความมั่นคงปลอดภัยของแต่ละขอบเขตที่ถูกจัดแบ่ง

8.2 การถ่ายโอนสารสนเทศ (Information Transfer)

1) นโยบาย และขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information Transfer Policies and Procedures)

1.1) ต้องจัดให้มีนโยบาย และหลักปฏิบัติเพื่อปกป้องข้อมูลสารสนเทศที่รับส่งผ่านระบบ และอุปกรณ์ในการสื่อสารทุกประเภท โดยมีเนื้อหาขั้นต่ำครอบคลุมถึง

1) แนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่างๆ

2) กระบวนการป้องกันการรับส่งข้อมูลสารสนเทศนอกเส้นทางที่ได้กำหนดไว้ (Miss-Routing)

3) กระบวนการป้องกันข้อมูลที่เป็นความลับ หรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (Attachment Files) และการส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกบริษัทฯ

4) การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารบางประเภทที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ Cloud Computing เป็นต้น

2) ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on Information Transfer) ข้อตกลงสำหรับการถ่ายโอนสารสนเทศให้มีความมั่นคงปลอดภัยต้องมีระบุระหว่างบริษัทฯ กับหน่วยงานภายนอก

3) การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging) ในการใช้งานระบบรับส่งขอความผ่านทางอิเล็กทรอนิกส์ (Electronic Messaging) ต้องคำนึงถึงความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านช่องทางดังกล่าว

4) ข้อตกลงการรักษาความลับ หรือการไม่เปิดเผยความลับ (Confidentiality or Non-Disclosure Agreements)

4.1) ต้องจัดให้พนักงาน และผู้ให้บริการภายนอก มีการทำสัญญารักษาความลับ หรือไม่เปิดเผยข้อมูลที่มีความสำคัญ โดยต้องมีเนื้อหาครอบคลุมถึง

1) การระบุความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และวิธีป้องกันการรั่วไหลของข้อมูล

2) การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ต้องจัดให้มีการลงนามโดยผู้รับผิดชอบ

3) การกำหนดขั้นตอนการขออนุญาตเข้าถึงข้อมูล หรือกำหนดสิทธิการเข้าถึงข้อมูลตามที่ได้ลงนาม

4) การกำหนดสิทธิการเข้าถึงข้อมูลเพื่อตรวจสอบ หรือติดตามการใช้งานข้อมูลที่มีความสำคัญ

5) การกำหนดกระบวนการแจ้งเตือน และรายงานผู้เกี่ยวข้องหากพบการรั่วไหล หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

6) การกำหนดมาตรการดำเนินการกรณีละเมิด หรือยกเลิกสัญญา รวมทั้งข้อกำหนดในการคืน หรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดสัญญา

9. แนวปฏิบัติการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information System Acquisition, Development and Maintenance)

เพื่อการสร้างความปลอดภัยให้กับระบบสารสนเทศ ป้องกันความผิดพลาดของระบบสารสนเทศจากความถูกต้องของข้อมูล การสูญหาย และการแก้ไขอย่างไม่ถูกต้อง ให้โครงการสารสนเทศได้รับการดำเนินการอย่างปลอดภัย และเพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วยเพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่ หรือตีพิมพ์ในสถานที่ต่างๆ

9.1 ความต้องการด้านความมั่นคงปลอดภัยระบบ (Security Requirements of Information Systems) มีข้อปฏิบัติดังนี้

1) การวิเคราะห์ และกำหนดความต้องการด้านความปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

1.1) กลุ่มงานเทคโนโลยีสารสนเทศ และการสื่อสารต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งาน

1.2) หน่วยงานดูแลระบบเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่างๆ ดังนี้

1) มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย อาทิ การสำรองข้อมูล ระบบเครือข่ายสำรอง

2) มาตรการปฏิบัติหลังจากเกิดความเสียหาย อาทิ แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล

2) ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing Application Service on Public Networks) ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการ การใช้งาน (Application Service) ทั้งในกรณีทั่วไป และกรณีที่ผ่านเครือข่ายสาธารณะ เพื่อป้องกันการกระทำผิดในลักษณะทุจริต (Fraudulent Activities) การทำธุรกรรมที่ไม่สมบูรณ์ หรือผิดพลาด (Incomplete Transmission or Miss-Routing) หรือการเปิดเผยคัดลอกหรือเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

3) การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting Application Service Transactions) สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การเปลี่ยนแปลงขอความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

9.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาระบบและสนับสนุน (Security in Development and Support Processes) มีข้อปฏิบัติดังนี้

1) นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy) กฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และระบบต้องมีการกำหนด และปฏิบัติตามสำหรับการพัฒนาระบบของบริษัทฯ

2) ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures) จัดให้มีการควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้ เช่น

2.1) มีการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง

2.2) มีการกำหนดวิธีปฏิบัติให้คำขอ แก้ไขหรือพัฒนาต้องมาจากผู้ที่มีสิทธิ และอนุมัติคำขอโดยผู้มีอำนาจอนุมัติของฝ่ายงาน หรือผู้ที่ได้รับมอบหมาย ต้องควบคุมผลข้างเคียงที่อาจเกิดขึ้นเนื่องจากมีการแก้ไข

2.3) กำหนดวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน และบันทึกเหตุผลความจำเป็น และขออนุมัติจากผู้มีอำนาจอนุมัติของฝ่ายงานทุกครั้ง

2.4) ปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้มีการแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิใช้งาน ขั้นตอนการทำงานของโปรแกรม และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัย และสะดวกต่อการใช้งาน

2.5) จัดเก็บโปรแกรม Version ก่อนการเปลี่ยนแปลงไว้ใช้งาน หรือมีกระบวนการถอยกลับสู่สภาพเดิม (Fall-Back) ของระบบงาน ในกรณีระบบงานผิดพลาด หรือไม่สามารถใช้งานได้

2.6) มีการสื่อสารให้กับบุคคลที่เกี่ยวข้องได้รับทราบ และสามารถปฏิบัติงานได้อย่างถูกต้อง

3) การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical Review of Applications after Operating Platform Changes) เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบสำคัญต้องมีการทบทวน และทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงาน หรือด้านความมั่นคงปลอดภัยของบริษัทฯ

4) การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages) การเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูปต้องไม่อนุญาตการดำเนินการ จำกัดการเปลี่ยนแปลงเท่าที่จำเป็น และต้องมีการควบคุมอย่างรัดกุม

5) หลักการวิศวะกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles) หลักการวิศวกรรมระบบให้มีความมั่นคงปลอดภัยต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร ปรับปรุงอย่างต่อเนื่อง และประยุกต์กับงานการพัฒนาระบบ

6) สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure Development Environment) การควบคุมสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ ซึ่งได้แก่ บุคลากรผู้พัฒนาระบบ ขั้นตอนการพัฒนาระบบ และเทคโนโลยีสำหรับการพัฒนาระบบให้มีความมั่นคงปลอดภัยตลอดถึงขั้นตอนในการพัฒนาระบบ โดยคำนึงถึง

6.1) การรักษาความลับของข้อมูลที่นำมาประมวลผล จัดเก็บ และส่งผ่านระบบ และการควบคุมการนำข้อมูลเข้าและออกจากระบบที่อยู่ระหว่างการพัฒนา

6.2) การควบคุมการเข้าถึงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศอย่างรัดกุมเหมาะสม

6.3) การติดตามหากมีการเปลี่ยนแปลงสภาพแวดล้อมของการพัฒนาระบบสารสนเทศ

6.4) มีการจัดเก็บข้อมูลสำรองในพื้นที่นอกองค์กรที่มีความปลอดภัย

7) การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced Development) องค์กรต้องกำกับดูแล เฝ้าระวัง และติดตามกิจกรรมการพัฒนาระบบที่หน่วยงานภายนอกเป็นผู้ดำเนินการ

8) การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing) การทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการในระหว่างที่ระบบอยู่ในช่วงการพัฒนา

9) การทดสอบเพื่อรับรองระบบ (System Acceptance Testing) แผนการทดสอบ และเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ ต้องมีการจัดทำสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชั่นใหม่

9.3 ข้อมูลสำหรับการทดสอบ (Test Data)

การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data) ข้อมูลสำหรับการทดสอบระบบต้องมีการคัดเลือกอย่างระมัดระวัง มีการป้องกัน และควบคุมการนำมาใช้งาน

10. แนวปฏิบัติความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

เพื่อจัดทำข้อกำหนดต่างๆ และกรอบการปฏิบัติงาน ในการให้บริการ หรือการใช้บริหารด้านงานเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ ความมั่นคงปลอดภัย และผลประโยชน์สูงสุดแก่บริษัทฯ

10.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationship)

1) นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information SecurityPolicy for Supplier Relationships)

1.1) ต้องจัดให้มีนโยบายในการควบคุมดูแลผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร เพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศของผู้ประกอบธุรกิจอย่างไม่เหมาะสม

2) การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

2.1) ข้อตกลงเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ต้องมีดังนี้

1) รายละเอียดของข้อมูลที่จำเป็นต้องใช้หรือเข้าถึงโดยผู้ให้บริการภายนอกรวมทั้งวิธีการเข้าถึงข้อมูลดังกล่าว

2) การจัดแบ่งประเภทข้อมูลโดยต้องสอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัย ของระบบสารสนเทศ

3) มีมาตรการดำเนินการเพื่อให้มั่นใจได้ว่าข้อมูลที่เป็นความลับ หรือมีความสำคัญ ทรัพย์สินทางปัญญา และลิขสิทธิ์ได้รับการคุ้มครองอย่างปลอดภัยตามกฎหมาย และหลักเกณฑ์ของทางการที่เกี่ยวข้อง

4) แนวทางการใช้งานข้อมูลสารสนเทศอย่างถูกต้องเหมาะสม

5) แผนรองรับกรณีเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Incident Response Policy)

6) ข้อกำหนดเพิ่มเติมเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ กรณีที่ผู้ให้บริการภายนอกมอบหมายการปฏิบัติงานให้กับบุคคลอื่นต่อ (Sub-Contracting to Another Supplier)

3) ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศ และการสื่อสารโดยผู้ให้บริการภายนอก (Information and Communication Technology Supply Chain) กำหนดข้อตกลงกับผู้ให้บริการภายนอกเกี่ยวกับเรื่องความเสี่ยงอันเกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก

10.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

1) การติดตาม และทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and Review of Supplier Services) ต้องจัดให้มีการติดตาม ทบทวน และตรวจสอบผู้ให้บริการภายนอกอย่างสม่ำเสมอ ทั้งในด้านฐานะทางการเงินกระบวนการปฏิบัติงาน และประสิทธิภาพการให้บริการ

2) การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

2.1) ในกรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน ต้องจัดให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว และกำหนดกระบวนการบริหารจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสม

11. แนวปฏิบัติการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัย (Information Security IncidentManagement)

เพื่อจัดการเหตุการณ์ทางด้านความมั่นคงปลอดภัย เรียนรู้ข้อผิดพลาดจากปัญหาที่เกิดขึ้น และปรับปรุงแก้ไข ซึ่งเป็นการป้องกันการเกิดเหตุการณ์ทางด้านความมั่นคงปลอดภัยในครั้งต่อไป

11.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of Information Security Incidents and Improvements) มีข้อปฏิบัติดังนี้

1) หน้าที่ความรับผิดชอบ และขั้นตอนปฏิบัติ (Responsibilities and Procedures)

1.1) ต้องจัดให้มีขั้นตอน และกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

1.2) กำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ ความสามารถ และประสบการณ์

2) การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

2.1) ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้ โดยปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

2.2) ผู้ใช้งาน และบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใดๆ ที่เกิดขึ้นภายในองค์กรต่อผู้บังคับบัญชา

2.3) ผู้ใช้งานที่พบ หรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อเจ้าหน้าที่สารสนเทศทันที

2.4) ผู้ใช้งานที่พบว่าฮาร์ดแวร์ หรืออุปกรณ์ใดๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อเจ้าหน้าที่สารสนเทศทันที

2.5) ผู้ใช้งาน และบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัย หรือจุดอ่อนใดๆ ในองค์กรต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้นผู้บังคับบัญชา หน่วยงานจัดการความปลอดภัย และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

3) การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย

3.1) ต้องบันทึก และรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตุพบ หรือเกิดความสงสัยในระบบ หรือบริการที่ใช้งาน

3.2) ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวัง และรักษาอุปกรณ์ตรวจจับ และป้องกันการบุกรุกระบบเหตุการณ์ผิดปกติ และการแจ้งเตือนต่างๆ ที่อุปกรณ์ตรวจพบจะถูกทำการวิเคราะห์ และหาสาเหตุ ของการบุกรุกในระบบสารสนเทศของบริษัทฯ เพื่อเป็นเครื่องมือสืบสวนหาบุคคลที่โจมตีบุกรุก หรือใช้ระบบในทางที่ผิด

3.3) ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามที่จะบุกรุก หรือโจมตีองค์กร เป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัยอื่น เช่น ไฟวอลล์ เป็นต้น และเพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตรายที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือ Hacker รวมทั้งไวรัสประเภทต่างๆ

3.4) ผู้ดูแลระบบต้องมีการบริหารจัดการ การบุกรุกระบบ โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับบริษัทฯ และจัดทำวิธีปฏิบัติที่ถูกต้องให้กับบริษัทฯ เพื่อป้องกันเหตุการณ์ที่เกิดขึ้นซ้ำ

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

5) การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to Information Security Incidents) ต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็ว และทันต่อเหตุการณ์ผ่านบุคคล หรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (Point of Contact)

6) การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from Information Security Incidents) แจ้งบุคคลที่เกี่ยวข้อง รับทราบโดยไม่ชักช้า ในกรณีที่เหตุการณ์ส่งผลกระทบต่อบุคคลดังกล่าว

7) การเก็บรวบรวมหลักฐาน (Collection of Evidence) จัดให้มีการรายงานความคืบหน้าในการบริหารจัดการสถานการณ์และผลการบริหารจัดการเป็นระยะ และเมื่อเหตุการณ์ยุติแล้ว

12. แนวปฏิบัติประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

เพื่อป้องกันการติดขัด หรือหยุดชะงักของการทำงานขององค์กร และป้องกันกระบวนการทางธุรกิจ ที่สำคัญอันเป็นผลมาจากการล้มเหลว หรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ในระยะเวลาอันเหมาะสม

12.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity)

1) การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning Information Security Continuity) ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤต หรือภัยพิบัติ

2) การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity) ต้องกำหนด จัดทำเป็นลายลักษณ์อักษร ปฏิบัติ และปรับปรุง กระบวนการ ขั้นตอนปฏิบัติ และมาตรการเพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

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

12.2 การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

1) ต้องกำหนดระยะเวลาในการกลับคืนสู่สภาพการดำเนินงานปกติของระบบสารสนเทศ

2) ต้องจัดลำดับการกู้คืนระบบงานสารสนเทศที่มีความสำคัญทุกระบบ ให้เหมาะสมกับผลกระทบที่อาจเกิดขึ้น

3) ควรจัดให้มีการสำรองระบบสารสนเทศ เพื่อให้อยู่ในสภาพพร้อมใช้งาน

13. การปฏิบัติตามข้อกำหนด (Compliance)

เพื่อให้การดำเนินงานต่างๆ ของบริษัทฯ เป็นไปตามกฎหมาย ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆ ที่ทางบริษัทฯ ต้องปฏิบัติตาม และมีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศ

13.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

1) การระบุกฎหมาย และความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of Applicable Legislation and Contractual Requirements)

1.1) ต้องระบุกฎหมาย หลักเกณฑ์ และข้อกำหนดตามสัญญาต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศ โดยจัดทำเป็นเอกสาร และปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ

1.2) ห้ามเจ้าหน้าที่ในบริษัทฯ ใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของบริษัทฯ กระทำการใดๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศไม่ว่าโดยกรณีใดก็ตาม

2) สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)

2.1) ต้องกำหนดขั้นตอนปฏิบัติงานเพื่อให้มั่นใจว่าในการใช้งานข้อมูลสารสนเทศที่อาจถือเป็นทรัพย์สินทางปัญญา หรือการใช้งานซอฟต์แวร์ที่พัฒนาโดยผู้ประกอบธุรกิจมีความสอดคล้องกับกฎหมาย และข้อกำหนดตามสัญญาต่างๆ

2.2) ห้ามผู้ใช้งานทำการใช้งานทำซ้ำ หรือเผยแพร่รูปภาพ บทความ หนังสือ หรือเอกสารใดๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของบริษัทฯ โดยเด็ดขาด

3) การป้องกันข้อมูล (Protection of Records) ต้องป้องกันมิให้ข้อมูลบันทึกหลักฐาน (Logs) ต่างๆ เกิดความเสียหาย สูญหาย เปลี่ยนแปลงแก้ไข เข้าถึง หรือเผยแพร่โดยไม่ได้รับอนุญาต โดยให้สอดคล้องกับกฎหมาย ข้อกำหนด ตามสัญญาต่างๆ และความต้องการทางธุรกิจ

4) ความเป็นส่วนตัว และการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information) ต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย หลักเกณฑ์ ของทางการ และข้อกำหนดตามสัญญาต่างๆ

5) ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Regulation of Cryptographic Controls) ต้องควบคุมการเข้ารหัสข้อมูลให้สอดคล้องกับกฎหมาย หลักเกณฑ์ของทางการ และข้อกำหนดตามสัญญาต่างๆ

13.2 การทบทวนความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Reviews)

1) การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent Review of Information Security) ต้องจัดให้มีการตรวจสอบขั้นตอน และการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2) ความสอดคล้องกับนโยบาย และมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with Security Policies and Standards) ต้องจัดให้มีการทบทวน และปรับปรุงขั้นตอน และการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และสอดคล้องกับมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

3) การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review) ต้องจัดให้มีการทบทวนระบบสารสนเทศในด้านเทคนิค เช่นการทดสอบการบุกรุก ระบบ (Penetration Test) อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และมาตรฐานสากลด้านความมั่นคงปลอดภัยของระบบสารสนเทศ