MEDEZE

นโยบาย : เทคโนโลยีสารสนเทศและการใช้อุปกรณ์ไอที

เลขที่เอกสาร : MG-E-037

วันที่มีผลบังคับใช้ : 11 สิงหาคม 2565

นโยบายบริษัท

เรื่อง เทคโนโลยีสารสนเทศและการใช้อุปกรณ์ไอที

---

1. บทนำ

บริษัท เมดีซ กรุ๊ป จำกัด (มหาชน) (“บริษัท”) และบริษัทย่อย กำหนดให้เทคโนโลยีสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญที่ช่วยส่งเสริมการดำเนินธุรกิจและเพิ่มประสิทธิภาพการทำงาน ฉะนั้น จึงเป็นความรับผิดชอบร่วมกันของพนักงานทุกคน ที่จะต้องใช้เทคโนโลยีสารสนเทศและการสื่อสารภายใต้ข้อบังคับของกฎหมาย คำสั่งบริษัทและตามมาตรฐานที่บริษัทกำหนด และบริษัทได้จัดให้มีการบริหารความปลอดภัยของระบบสารสนเทศ ซึ่งหมายถึง ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ตามมาตรฐานสากล (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือกฎหมายอื่นที่เกี่ยวข้อง) ทั้งนี้ พนักงานบริษัททุกคนมีหน้าที่และข้อปฏิบัติตามนโยบายฉบับนี้

2. บททั่วไปของนโยบายด้านเทคโนโลยีสารสนเทศ มีดังนี้

2.1 การรักษาความลับของข้อมูล เป็นการกำหนดชนิดและจัดลำดับความสำคัญของข้อมูลสารสนเทศ แบ่งออกเป็นประเภทต่าง ๆ ได้แก่ ข้อมูลที่เผยแพร่ได้ ข้อมูลภายใน ข้อมูลลับ และข้อมูลลับเฉพาะ เพื่อป้องกันการนำข้อมูลสารสนเทศไปใช้โดยผิดวัตถุประสงค์ หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

2.2 การจัดหา และติดตั้งระบบงานคอมพิวเตอร์รวมถึงการควบคุมการเปลี่ยนแปลง และการควบคุมคุณภาพของการให้บริการ ระบบงาน เพื่อให้ระบบที่ทำการจัดหานั้นมีรูปแบบที่ชัดเจน และสามารถให้การสนับสนุนธุรกิจได้อย่างรวดเร็ว ถูกต้องตามขอบเขตงานให้บริการที่ต่อเนื่อง และมีประสิทธิภาพ

2.3 นโยบายระบบสารสนเทศสำรอง และแผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRC, DRP) เป็นการจัดกระบวนการปฏิบัติงาน การจัดทำระบบสารสนเทศสำรอง การจัดสำรองข้อมูล การจัดการสถานที่สำรองเพื่อให้ธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง เมื่อเกิดเหตุสุดวิสัย

2.4 การใช้บริการทางด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการอื่น (IT Outsourcing) เป็นหลักเกณฑ์ในการป้องกันไม่ให้มีการนำข้อมูลสารสนเทศออกเปิดเผยต่อบุคคลภายนอก อันเนื่องจากการใช้บริการจากผู้ให้บริการอื่น หลักเกณฑ์ในการตรวจสอบคุณสมบัติต่าง ๆ ของผู้ให้บริการ ได้แก่ ความสามารถในการ ให้บริการอย่างต่อเนื่อง ความน่าเชื่อถือ รวมถึงการกำหนดแนวทางการติดตามประเมินผล การตรวจสอบ และบริหารความเสี่ยงในการใช้บริการจากผู้ให้บริการอื่น

3. บทที่เกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

ว่าด้วยการกำหนดให้มีการเขียนนโยบายเป็นลายลักษณ์อักษร มีหน่วยงานอนุมัติ และกำกับอย่างชัดเจน กำหนดให้มีกรอบการทบทวนปรับปรุงนโยบาย ระเบียบ ประกาศ และคู่มือปฏิบัติงานทุกปี

3.1 การบริหารจัดการทรัพย์สินสารสนเทศ เป็นการกำหนดหน้าที่ ความรับผิดชอบต่อทรัพย์สินสารสนเทศ เช่น จัดให้มีการจัดทำบัญชีทรัพย์สิน การระบุผู้มีหน้าที่ดูแลรับผิดชอบทรัพย์สิน

3.2 การสร้างความมั่นคงปลอดภัยทางกายภาพ และสิ่งแวดล้อมของระบบสารสนเทศ เพื่อให้ระบบสารสนเทศมีความสามารถ ให้บริการได้อย่างมีประสิทธิภาพ มั่นคงปลอดภัย สามารถให้บริการได้อย่างต่อเนื่อง จึงได้มีการกำหนดพื้นที่หรือบริเวณที่ต้องมี มาตรการควบคุมความปลอดภัย

3.3 การบริหารจัดการด้านการสื่อสาร และการดำเนินงานของเครือข่ายสารสนเทศ เนื่องจากระบบเครือข่ายสื่อสารมีความสำคัญอย่างยิ่งในการดำเนินธุรกิจในปัจจุบัน หากไม่มีการบริหารจัดการที่ดี จะส่งผลกระทบต่อการดำเนินธุรกิจ จำเป็นต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบ การเฝ้าระวังทั้งที่เป็นการทำงานของอุปกรณ์ การเฝ้าระวังการบุกรุก และการกำหนด ขั้นตอนการปฏิบัติงาน ตลอดจนสร้างกระบวนการบริหารจัดการการให้บริการของผู้ให้บริการภายนอก

3.4 การควบคุมการเข้าถึงระบบสารสนเทศ และข้อมูลสารสนเทศ เพื่อให้ผู้ที่มีหน้าที่รับผิดชอบในข้อมูลนั้นเท่านั้นจึงจะสามารถเข้าถึงได้ เพื่อให้ครอบคลุมการเข้าถึงข้อมูลสารสนเทศอย่างมีประสิทธิภาพ จึงได้มีการกำหนดให้มีการควบคุมต่าง ๆ ดังนี้ หน้าที่ ความรับผิดชอบของผู้ใช้งาน การควบคุมการเข้าถึงเครือข่าย การเข้าถึงระบบปฏิบัติการ การควบคุมการใช้อุปกรณ์สื่อสารประเภท พกพา และการปฏิบัติงานภายนอกองค์กร

4. วัตถุประสงค์

เพื่อให้องค์กรมีแนวนโยบายในการดำเนินงาน หรือการจัดการทางด้านเทคโนโลยีสารสนเทศ และให้ผู้ที่เกี่ยวข้องกับสารสนเทศ ทั้งผู้บริหาร พนักงาน และบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับสารสนเทศขององค์กรได้มีแผนงาน และกรอบการปฏิบัติ ที่ชัดเจน อันจะนำไปสู่การประสานงานในการให้บริการที่มีประสิทธิภาพ ความปลอดภัยในการให้บริการสูงสุด และมีมาตรฐานยิ่งขึ้น

5. หน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้องกับนโยบาย

5.1 ฝ่ายเทคโนโลยีสารสนเทศ รับทราบนโยบาย และปฏิบัติตาม รวมถึงกำกับการทำงาน ให้เป็นไปตามนโยบาย

5.2 ฝ่ายตรวจสอบภายใน มีหน้าที่ตรวจสอบการควบคุมภายใน และสอบทานกระบวนการ

6. หน่วยงานที่ต้องปฏิบัติตามนโยบาย

ทุกฝ่าย, ทุกส่วนขององค์กร

7. หน่วยงานที่กำกับดูแลให้เป็นไปตามนโยบาย

ฝ่ายเทคโนโลยีสารสนเทศและการจัดการ

8. นิยามที่เกี่ยวข้อง

องค์กร	หมายถึง	บริษัท เมดีซ กรุ๊ป จำกัด (มหาชน) และบริษัทย่อย
ฝ่ายเทคโนโลยีสารสนเทศ	หมายถึง	หน่วยงานที่รับผิดชอบในการดำเนินงานด้านบริหารจัดการเทคโนโลยีสารสนเทศขององค์กร
บุคคลภายนอก	หมายถึง	บุคคลหรือพนักงานของหน่วยงานภายนอกที่มาติดต่อสื่อสาร และมีการเข้าถึงทรัพย์สิน สารสนเทศขององค์กร
ผู้ดูแลระบบ (Administrator)	หมายถึง	เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษา ระบบ หรือเครือข่ายคอมพิวเตอร์ รวมไปถึงการแก้ไขปัญหาการใช้งานในด้านต่าง ๆ ซึ่งสามารถเข้าถึงโปรแกรม หรือเครือข่ายคอมพิวเตอร์เพื่อการจัดการต่าง ๆ ได้
ผู้บริหาร	หมายถึง	ผู้บริหารสูงสุดของแต่ละสายงาน
ผู้ให้บริการรายอื่น	หมายถึง	บุคคล หรือนิติบุคคลอื่นใดทั้งในประเทศ และต่างประเทศที่ให้บริการด้านเทคโนโลยีสารสนเทศ
หน่วยงานภายนอก (Third party)	หมายถึง	หน่วยงานที่มีความจำเป็นในการเข้ามาปฏิบัติงาน หรือเข้ามาเกี่ยวข้องกับสถานที่ หรือ ทรัพย์สินสารสนเทศขององค์กร มีหน้าที่ความรับผิดชอบในการปฏิบัติตามนโยบาย และ กฎระเบียบ ตามข้อกำหนด ข้อตกลง หรือสัญญาที่ได้จัดทำกับองค์กร
ผู้ใช้งาน (User)	หมายถึง	ผู้ใช้งานระบบงานคอมพิวเตอร์
เจ้าของข้อมูล (Data Owner)	หมายถึง	ฝ่าย หรือส่วนที่เป็นเจ้าของข้อมูล
ผู้มีอำนาจ	หมายถึง	ผู้บังคับบัญชาระดับผู้จัดการฝ่ายขึ้นไป หรือผู้ที่ได้รับมอบหมายที่มีหน้าที่ตัดสินใจ
การเข้ารหัสลับ (Cryptography Encryption)	หมายถึง	การเปลี่ยนแปลงรูปแบบของข้อมูลให้อยู่ในรูปแบบที่มีความมั่นคงปลอดภัย โดยใช้กุญแจในการเข้ารหัสลับ เพื่อที่ผู้เข้าถึงข้อมูลจะไม่สามารถทราบเนื้อหาที่แท้จริงของข้อมูลได้ ถ้าไม่มีการถอดรหัสลับจากกุญแจที่ใช้ในการถอดที่ถูกต้อง ทั้งนี้ขึ้นกับเทคนิคการเข้ารหัสลับข้อมูลที่ใช้

การเปลี่ยนแปลงปรับปรุงแก้ไข	หมายถึง	การเปลี่ยนแปลง ปรับปรุงแก้ไขระบบ หรืออุปกรณ์ประมวลผลสารสนเทศ เช่น การติดตั้ง หรือการปรับเปลี่ยนระบบปฏิบัติการซอฟต์แวร์ระบบ และระบบเครือข่าย
การเฝ้าระวัง (Monitoring)	หมายถึง	การเฝ้าระวังทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบความผิดปกติจากการประมวลผล กิจกรรมต่าง ๆ ของระบบสารสนเทศ จากบันทึกเหตุการณ์การใช้งานของระบบ (Logs) เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานสารสนเทศผิดวัตถุประสงค์ และปัญหาที่เกิดจาก ระบบงาน
การสร้างความตระหนักในการรักษา ความมั่นคงปลอดภัย (Security Awareness)	หมายถึง	การให้ความรู้ความเข้าใจทางด้านความมั่นคงปลอดภัยของสารสนเทศ เพื่อสร้างความตระหนักถึงภัยคุกคาม และปัญหาทางด้านความมั่นคงปลอดภัยสารสนเทศแก่บุคลากร
การสำรองข้อมูล (Data Backup)	หมายถึง	การทำสำเนาข้อมูลทั้งหมดในระบบที่ต้องการ เพื่อเป็นการสำรองข้อมูลที่อาจมีการแก้ไขเปลี่ยนแปลง หรือสูญหายให้สามารถนำกลับมาใช้งานได้
กุญแจ (Key)	หมายถึง	กุญแจที่ใช้ในกระบวนการเข้ารหัสลับ ใช้ในการเข้ารหัสลับ หรือถอดรหัสลับขึ้นอยู่กับการ ใช้งานเทคนิคการเข้ารหัสลับข้อมูล หรือแยกเป็น 2 ประเภท คือ กุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key)
ข้อมูลสารสนเทศ (Information asset and Software License)	หมายถึง	สารสนเทศที่อยู่ในสื่อบันทึกข้อมูล และลิขสิทธิ์ซอฟต์แวร์ เช่น ฐานข้อมูลระบบงานต่าง ๆ ข้อมูลการทำงาน ลิขสิทธิ์ สัญญาต่าง ๆ
แหล่งข้อมูล (Source of Data and information)	หมายถึง	ที่เก็บข้อมูล หรือสารสนเทศทั้งที่อยู่ในรูปแบบต่าง ๆ กัน เช่น ข้อมูลแหล่งข้อมูลเฉพาะ และแหล่งข้อมูลส่วนกลาง เป็นต้น
ความมั่นคงปลอดภัย (Security)	หมายถึง	ปัจจัยด้านความมั่นคงปลอดภัยในที่นี้ มี 3 ประการด้วยกัน คือ 1. การรักษาความลับ (Confidentiality) 2. ความถูกต้องครบถ้วน (Integrity) 3. ความพร้อมใช้งาน (Availability) โดยสรุปได้ใจความว่า ความมั่นคงปลอดภัยสารสนเทศ คือ การรักษาสารสนเทศจากการ เข้าถึงเพื่อการขโมย เปลี่ยนแปลง ทำให้ใช้การไม่ได้ หรือการทำลายสารสนเทศ โดยไม่รับอนุญาต
งานเทคโนโลยีสารสนเทศ	หมายถึง	งานใด ๆ ที่เกี่ยวกับเทคโนโลยีสารสนเทศ ได้แก่ งานประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ การจัดเก็บข้อมูล การพัฒนาระบบงาน และโปรแกรม การบำรุงรักษาความปลอดภัย ทรัพยากรคอมพิวเตอร์ เช่น เครื่องคอมพิวเตอร์และอุปกรณ์ระบบงานและโปรแกรมระบบ เครือข่าย และข้อมูล เป็นต้น

ช่องโหว่ (Vulnerability)	หมายถึง	ช่องโหว่ในทรัพย์สินสารสนเทศที่อาจเกิดจากความบกพร่องในการผลิต หรือการออกแบบ ทำให้เกิดจุดอ่อน และมีความเสี่ยงในการคุกคามจากช่องโหว่ที่เกิดขึ้น เช่น ช่องโหว่ของ โปรแกรมที่ทำให้บุคคลภายนอกสามารถเข้าใช้โปรแกรมได้โดยไม่ต้องผ่านการพิสูจน์ตัวตน
ทรัพย์สินสารสนเทศ	หมายถึง	1. ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 2. เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล สื่อบันทึกข้อมูล และอุปกรณ์อื่นใด 3. ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
บริเวณที่ต้องมีการรักษาความมั่นคง ปลอดภัย (Secure Area)	หมายถึง	บริเวณที่ใช้เก็บรักษาอุปกรณ์สารสนเทศที่ใช้ในงานระบบสารสนเทศ แบ่งได้เป็น 2 ประเภท คือ 1) พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) 2) พื้นที่ห้อง Patching Area
บริเวณปฏิบัติการคอมพิวเตอร์ (Computer Operation)	หมายถึง	พื้นที่ที่ใช้ในการป้อนข้อมูล ออกรายงาน และปฏิบัติงานเกี่ยวกับระบบงานสารสนเทศของ องค์กร
บริเวณ Patching Area	หมายถึง	พื้นที่ที่ใช้เก็บอุปกรณ์ในการเชื่อมต่อเครือข่ายคอมพิวเตอร์ และโทรศัพท์ในแต่ละชั้น
บัญชีผู้ใช้ (User Name หรือ Account)	หมายถึง	กลุ่มของข้อมูลที่ใช้ในการอ้างถึงเพื่อระบุตัวตน สิทธิการเข้าถึง และข้อจำกัดต่าง ๆ ในการเข้าถึงนั้น
บันทึกเหตุการณ์ (Logs)	หมายถึง	บันทึกเหตุการณ์การใช้งานของระบบสารสนเทศ การเข้าใช้งานระบบ การประมวลผล กิจกรรมของระบบสารสนเทศ และเหตุการณ์ทางด้านความมั่นคงปลอดภัย เพื่อตรวจสอบถึง ประสิทธิภาพ ความปลอดภัย และความผิดปกติที่เกิดจากการประมวลผลกิจกรรมต่าง ๆ ของระบบสารสนเทศ
ประมวลผล (Process)	หมายถึง	กระบวนการทำงานทางตรรกะของคอมพิวเตอร์
ประเมินความเสี่ยง (Risk Assessment)	หมายถึง	การประเมินความเสี่ยง หรือเหตุการณ์ที่อาจเกิดขึ้นได้ ซึ่งอาจเป็นอันตราย หรือคุกคามถึงความมั่นคงปลอดภัยสารสนเทศ
โปรแกรมที่ไม่พึงประสงค์ (Malicious Code or Malware)	หมายถึง	โปรแกรมหรือ Code ที่เป็นอันตรายต่อประสิทธิภาพ และความปลอดภัยของระบบสารสนเทศไม่ทางใดก็ทางหนึ่ง เช่น ไวรัส (Virus) เวิร์ม (Worm) และโทรจัน (Trojan)
แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)	หมายถึง	การสร้างความต่อเนื่องทางธุรกิจ ป้องการการติดขัดหรือการหยุดชะงักของระบบงานธุรกรรม ที่สำคัญ ซึ่งอาจมีสาเหตุมาจาก ภัยทางด้านสิ่งแวดล้อม เหตุการณ์ทางด้านความมั่นคง ปลอดภัย หรือภัยคุกคามอื่น ๆ

แผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRP: Disaster Recovery Plan)	หมายถึง	การเตรียมความพร้อมรองรับเหตุฉุกเฉิน และแผนการปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน เช่น การย้ายสถานที่ปฏิบัติงาน ไปจนถึงการใช้งานระบบสารสนเทศสำรอง
รหัสผ่าน (Password)	หมายถึง	กลุ่มอักขระที่ใช้ในการพิสูจน์ตัวตน ใช้เพื่อควบคุมการเข้าถึงระบบสารสนเทศ หรือข้อมูลสารสนเทศ
ระบบงานที่สำคัญ (Enterprise Resource Planning)	หมายถึง	ระบบที่ให้บริการธุรกรรมหลักที่ใช้ในการให้บริการลูกค้า
ระดับของการให้บริการ Service Level Agreement (SLA)	หมายถึง	ตัวชี้วัดถึงประสิทธิภาพของการให้บริการโดยผู้ให้บริการภายนอก
Operational Level Agreement (OLA)	หมายถึง	ตัวชี้วัดประสิทธิภาพการให้บริการโดยฝ่ายเทคโนโลยีสารสนเทศ
ระบบพัฒนา (Development Area)	หมายถึง	ระบบสารสนเทศที่ใช้ในการพัฒนาระบบงาน โดยเป็นการจำลองทรัพยากร และสภาพแวดล้อมของระบบให้บริการจริง เพื่อใช้พัฒนาระบบงานใหม่
ระบบทดสอบ (User Acceptance Area)	หมายถึง	ระบบสารสนเทศที่ใช้ในการทดสอบ โดยเป็นการจำลองทรัพยากร และสภาพแวดล้อมของระบบให้บริการจริง มาเพื่อทดสอบประสิทธิภาพ และความปลอดภัยของระบบที่ได้พัฒนาขึ้น
ระบบสารสนเทศสำรอง (Disaster Recovery Center: DRC)	หมายถึง	ระบบงาน ข้อมูล และระบบเครือข่ายสำรองนอกเหนือจากระบบสารสนเทศหลัก เพื่อให้สามารถทำธุรกรรมหลักได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุการณ์ฉุกเฉิน
ระบบให้บริการจริง (Production Area)	หมายถึง	ระบบสารสนเทศที่ให้บริการจริงแก่ผู้ใช้งาน ซึ่งต้องมีการรักษาความปลอดภัย และการควบคุมการเข้าถึงจากการพัฒนาระบบ และการทดสอบระบบอย่างเคร่งครัด
สิทธิเฉพาะ (Privilege)	หมายถึง	สิทธิพิเศษที่ใช้ในการปฏิบัติงาน นอกเหนือจากสิทธิทั่วไป เช่น ผู้ดูแลระบบ หรือเจ้าของข้อมูลสารสนเทศ
สื่อบันทึกข้อมูล (Media)	หมายถึง	สื่อที่ใช้ในการบันทึกข้อมูลในระบบงานสารสนเทศ โดยสามารถจำแนกเป็นสื่อบันทึกข้อมูล ที่สามารถเคลื่อนย้ายได้ เพื่อใช้ในการรักษาความลับของข้อมูล เช่น Tapes, Disks, Removable Hard Drives, CDs, DVDs, และ Printed Media และสื่อบันทึกข้อมูลทั่วไป เช่น กระดาษ และเครื่องคอมพิวเตอร์

ห้องคอมพิวเตอร์ (Data Center)	หมายถึง	พื้นที่ห้องศูนย์ข้อมูลคอมพิวเตอร์ที่ใช้เก็บอุปกรณ์คอมพิวเตอร์ และเครื่องคอมพิวเตอร์หลักที่สำคัญในระบบงาน เช่น เครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายหลัก
เหตุการณ์ทางด้านความมั่นคงปลอดภัย (Security Event and Incident)	หมายถึง	เหตุการณ์ที่เกิดจากการเปลี่ยนแปลงระบบ สภาพแวดล้อม กระบวนการ ขั้นตอนการ ปฏิบัติงาน หรือจากพนักงาน ซึ่งทำให้เกิดความเสี่ยง หรือการคุกคามถึงประสิทธิภาพ และความปลอดภัยของระบบสารสนเทศ หรือทรัพย์สินสารสนเทศ รวมไปถึงการโจมตีระบบ ทำให้ระบบไม่สามารถทำงานได้อย่างปกติ และการถูกโจมตีโดยโปรแกรมไม่ประสงค์ดีต่าง ๆ
IT Asset	หมายถึง	ประกอบด้วยอุปกรณ์ทางด้าน Hardware, Software, Database Hardware ประกอบด้วย Server, คอมพิวเตอร์ (PC), All in one, Notebook, Printer, UPS, อุปกรณ์ Network และอุปกรณ์เครือข่ายไร้สาย Software ประกอบด้วย Software License, OS, Window, Database, MS Office, Application ต่าง ๆ
การซ่อมบำรุง	หมายถึง	กิจกรรม หรืองานที่ทำต่ออุปกรณ์ต่าง ๆ เพื่อรักษาสภาพ หรือป้องกันเพื่อไม่ให้เกิดความชำรุด เสียหาย โดยให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา รวมทั้งช่วยยืดอายุการใช้งานให้ยาวนานขึ้น และเสียค่าใช้จ่ายน้อยที่สุด

9. นโยบายด้านเทคโนโลยีสารสนเทศ

9.1 การรักษาความลับของข้อมูล (Confidentiality)

เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล ให้มีการระบุความสำคัญ และการระบุการจัดการของข้อมูลที่ใช้งานในระบบ สารสนเทศ แก่พนักงานผู้ต้องปฏิบัติงานเกี่ยวข้องกับข้อมูล เพื่อป้องกันการนำเข้าข้อมูลสารสนเทศไปใช้โดยผิดวัตถุประสงค์ หรือ เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

9.1.1 การจัดระดับข้อมูลสารสนเทศ (Information Classification)

กำหนดให้มีการแบ่งระบบความปลอดภัยขององค์กร โดยคำนึงถึงระดับความเสี่ยงต่อความมั่นคงปลอดภัย ผลกระทบต่อมูลค่า และความเสียหายที่ผู้ใช้บริการอาจได้รับ รวมถึงผลกระทบต่อความเสียหายทางทรัพย์สิน และชื่อเสียงในการดำเนินธุรกิจ

ข้อมูลขององค์กรสามารถแบ่งออกตามระดับความสำคัญ 4 ระดับ ดังนี้

1. ข้อมูลที่เผยแพร่ได้ (Public) เป็นข้อมูลที่มีเจตนาต้องการให้ลูกค้า หรือบุคคลภายนอกทราบ เช่น News Release และ Brochure ที่จัดทำออกมาเพื่อประชาสัมพันธ์ เป็นต้น
2. ข้อมูลภายใน (Internal) เป็นข้อมูลสำหรับให้พนักงานขององค์กรใช้เท่านั้น และไม่มีเจตนาให้ ภายนอกทราบ แต่ถ้าหากถูกนำไปเผยแพร่ จะไม่ทำให้เกิดความเสียหายมากนัก โดยมากจึงมักไม่ต้องการระบบการป้องกัน เช่น ระเบียบ บันทึกต่าง ๆ และจดหมายเรื่องทั่วไป เป็นต้น

3. ข้อมูลลับ (Confidential) เป็นข้อมูลเฉพาะสำหรับพนักงานที่ได้รับมอบหมายเท่านั้น หากถูกเผยแพร่ออกไปสู่พนักงานอื่นที่ไม่เกี่ยวข้อง จะทำให้เกิดความเสียหายแก่องค์กร ลูกค้า หรือพนักงาน จึงต้องเก็บรักษาป้องกันมิให้รั่วไหลออกไป เช่น รายงานทุกรายงานจากระบบคอมพิวเตอร์ ข้อมูลลูกค้า ข้อมูลส่วนบุคคล เงินเดือนพนักงาน โบนัสพนักงาน และงบประมาณของ องค์กร เป็นต้น
4. ข้อมูลลับเฉพาะ (Highly Restricted) เป็นข้อมูลลับที่สำคัญที่สุด หากถูกเผยแพร่ออกไปสู่พนักงานอื่นที่ไม่เกี่ยวข้อง จะทำให้องค์กร ลูกค้า หรือพนักงาน เสื่อมเสียชื่อเสียง ได้รับการกล่าวโทษ หรือฟ้องร้อง หรือเกิดความเสียหายอย่างยิ่ง จึงต้องมีการระวังรักษาป้องกันอย่างเข้มงวด เช่น ข้อมูลเกี่ยวกับบริการใหม่ที่ยังไม่ถึงเวลาประกาศ ข้อมูลงบการเงินที่ยังไม่ถึงเวลาประกาศ ข้อมูลการควบรวมกิจการ หรือการเพิ่มทุนที่ยังไม่ถึงเวลาประกาศ และรหัสผ่านของระบบงานต่าง ๆ เป็นต้น

9.1.2 การจัดการเกี่ยวกับข้อมูลข่าวสาร (Information Handling)

ข้อมูลถือเป็นทรัพย์สมบัติขององค์กร พนักงานทุกคนต้องดูแลรักษาข้อมูลที่ตนเองดูแลรับผิดชอบอยู่ โดยให้พิจารณาการจัดการตามระดับความสำคัญของข้อมูล เพื่อลดความเสี่ยงต่อความเสียหายทางทรัพย์สินและชื่อเสียงในการดำเนินธุรกิจ

10. นโยบายการจัดหา ติดตั้งระบบงานคอมพิวเตอร์

เพื่อกำหนดวิธีการจัดหาและการจัดการระบบงานคอมพิวเตอร์ขององค์กร ที่สามารถสนับสนุนการให้บริการธุรกิจขององค์กร ได้อย่างรวดเร็ว มีความต่อเนื่อง มีความถูกต้องน่าเชื่อถือ และมีประสิทธิภาพ

10.1 การจัดหาระบบงานคอมพิวเตอร์

หมายถึง กระบวนการหรือวิธีการให้ได้มาซึ่งระบบงานคอมพิวเตอร์ที่สามารถตอบสนองความต้องการทางธุรกิจ และสอดคล้องกับกลยุทธ์ขององค์กร เริ่มตั้งแต่ระบุความต้องการระบบงานคอมพิวเตอร์ของแต่ละสายงาน โดยมีการจัดทำโครงการ และบันทึกเป็นลายลักษณ์อักษร และได้รับการอนุมัติจากผู้บริหารสายงาน หรือผู้ที่มีอำนาจ

10.2 การติดตั้งระบบงานคอมพิวเตอร์

เพื่อให้การติดตั้งระบบงานคอมพิวเตอร์สำเร็จตามวัตถุประสงค์ของโครงการ จึงกำหนดกรอบในการติดตั้งระบบงานคอมพิวเตอร์ ดังนี้

10.2.1 การกำหนดหน้าที่ของคณะทำงาน จัดให้มีการกำหนดหน้าที่ และความรับผิดชอบของคณะทำงานอย่างชัดเจน

10.2.2 การควบคุมงานโครงการ จัดให้มีการควบคุมโครงการ ตามกรอบการติดตั้ง และพัฒนาระบบงาน (Software Implementation Framework) กำหนดให้มีการจัดทำแผนงานที่ชัดเจน ระบุความถี่ และขั้นตอนในการติดตาม ความคืบหน้า และการรายงานผลการดำเนินโครงการให้ผู้เกี่ยวข้องรับทราบ โดยต้องปรับปรุงแผนให้เป็นปัจจุบันอย่างสม่ำเสมอ

10.2.3 การตรวจรับมอบงาน จัดให้มีกระบวนการตรวจสอบความถูกต้อง และประเมินประสิทธิภาพของระบบงานก่อนการรับมอบระบบงาน รวมถึงจัดทำเอกสารตรวจรับมอบงาน และใช้เป็นเอกสารประกอบการเบิกจ่ายเงิน โดยยึดตาม “นโยบายเรื่องการเบิกจ่ายเงินงบประมาณโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ”

10.3 การควบคุมการเปลี่ยนแปลงระบบงานคอมพิวเตอร์

เพื่อให้ระบบงานสามารถสนับสนุนธุรกิจขององค์กรได้อย่างต่อเนื่องและมีประสิทธิภาพ หากมีการเปลี่ยนแปลง ความต้องการของธุรกิจ ซึ่งกระทบกับระบบงานคอมพิวเตอร์ปัจจุบันที่จะต้องมีการปรับแก้ไขให้ทันการณ์ จึงต้องกำหนดกรอบการ ควบคุมการเปลี่ยนแปลงระบบงาน ดังนี้

10.3.1 การร้องขอให้มีการเปลี่ยนแปลง จัดให้มีการบันทึกการร้องขอให้มีการเปลี่ยนแปลงเป็นลายลักษณ์อักษร หรือ IT Request และได้รับการอนุมัติจากผู้ที่มีอำนาจ

10.3.2 การวิเคราะห์ผลกระทบ จัดให้ผู้เกี่ยวข้องจัดทำเอกสารวิเคราะห์ผลกระทบรอบด้าน เพื่อควบคุมความเสี่ยง และใช้ประกอบการตัดสินใจ

10.3.3 การควบคุมการเปลี่ยนแปลง จะต้องผ่านการอนุมัติจากผู้มีอำนาจของแต่ละฝ่ายงาน ต้องมีการสื่อสารและแจ้งให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลง

10.4 การควบคุมคุณภาพการให้บริการของระบบงานคอมพิวเตอร์

เพื่อให้ระบบงานเทคโนโลยีสารสนเทศสามารถให้บริการตอบสนองธุรกิจอย่างต่อเนื่อง และมีความถูกต้องน่าเชื่อถือ ดังนั้น จึงได้จัดกำหนดการควบคุมคุณภาพให้บริการ ดังนี้

10.4.1 การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการจริง จัดให้มีการแบ่งแยกส่วนพัฒนา (Development Environment) และส่วนทดสอบ (Test Environment) ออกจากส่วนระบบที่ให้บริการจริง (Production Environment) อย่างชัดเจน ยกเว้นโปรแกรมบัญชี MAC-5 Legacy เนื่องจากต้องดำเนินการทดสอบในส่วนระบบที่ให้บริการจริงเท่านั้น

10.4.2 การแบ่งแยกเครือข่าย จัดให้มีการแยกเครือข่าย และแยกบัญชีผู้ใช้งานเข้าถึงส่วนพัฒนา (Development Environment) และส่วนทดสอบ (Test Environment) ออกจากส่วนระบบที่ให้บริการจริง (Production Environment) อย่างชัดเจน ยกเว้นโปรแกรมบัญชี MAC-5 Legacy เนื่องจากต้องดำเนินการทดสอบในส่วนระบบที่ให้บริการจริงเท่านั้น

10.4.3 กำหนดให้มีการจัดทำคู่มือ เอกสารประกอบระบบงาน และฐานข้อมูลความรู้ เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจระบบงาน ลักษณะงาน และกระบวนการทำงาน รวมถึงปรับปรุงเอกสารให้เป็นปัจจุบันอยู่เสมอ

10.4.4 การสนับสนุนการใช้ระบบงาน จัดให้มีเจ้าหน้าที่รับผิดชอบการปิดระบบงานอย่างชัดเจน โดยต้องรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา กรณีที่พบปัญหาต้องมีการบันทึกปัญหา และวิธีการแก้ไข รวมถึงรายงานต่อผู้บังคับบัญชาให้ทราบ

11. นโยบายระบบสารสนเทศสำรองและแผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRC, DRP)

เพื่อให้ฝ่ายงานธุรกิจต่าง ๆ สามารถทำธุรกรรมได้อย่างต่อเนื่อง และแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว แม้ว่าจะเกิดเหตุฉุกเฉิน หรือเหตุการณ์ทางด้านความมั่นคงปลอดภัยใด ๆ ซึ่งมีการจัดระบบสารสนเทศสำรอง (DRC : Disaster Recovery Center) การสำรองข้อมูล (Data Backup) และแผนรองรับกรณีเกิดเหตุฉุกเฉิน (DRP : Disaster Recovery Plan) ขึ้น รวมถึงให้สอดคล้องกับการเตรียมการในเรื่องการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)

11.1 กำหนดให้มีศูนย์คอมพิวเตอร์สำรอง และระบบสารสนเทศสำรอง เพื่อรองรับการดำเนินธุรกิจได้อย่างต่อเนื่องและลดผลกระทบเมื่อเกิดเหตุการณ์ฉุกเฉิน

11.2 กำหนดให้มีการสำรองข้อมูล (Backup) เพื่อรักษาความถูกต้องสมบูรณ์ และความพร้อมใช้ของสารสนเทศ ต้องมีการสำรอง ข้อมูลทั้งในส่วน System Software ส่วน Application Software และส่วนข้อมูลสารสนเทศ รวมถึงทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ โดยรูปแบบและความถี่ในการสำรองข้อมูล ให้พิจารณาตามความจำเป็น

11.3 กำหนดให้มีการจัดทำแผนรองรับกรณีเหตุฉุกเฉินที่สอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ การทดสอบแผน และการรายงานผลการทดสอบให้คณะกรรมการบริหารองค์กร และ/หรือคณะกรรมการในองค์กรรับทราบ รวมถึงต้องมีการเผยแพร่ แผนรองรับเหตุฉุกเฉินให้ผู้ที่เกี่ยวข้องรับทราบโดยความถี่ในการทดสอบอย่างน้อยปีละ 1 ครั้ง

12. การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

เพื่อจัดหาระบบงานเทคโนโลยีสารสนเทศได้รวดเร็ว สอดคล้องกับกลยุทธ์ทางธุรกิจขององค์กร โดยคำนึงถึงการให้บริการแก่ลูกค้าอย่างต่อเนื่องและมีความถูกต้องน่าเชื่อถือ การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น จึงเป็นทางเลือกที่ดีที่องค์กรได้กำหนดไว้ เพื่อให้สามารถบรรลุวัตถุประสงค์และได้รับการถ่ายทอดเทคโนโลยีที่ดีจากผู้ให้บริการรายอื่น โดยมีหลักเกณฑ์เบื้องต้นในการใช้บริการรายอื่น ดังนี้

12.1 หลักเกณฑ์ในการพิจารณาการใช้บริการจากผู้ให้บริการรายอื่น ต้องไม่ขัดแย้งกับกฎระเบียบ หรือข้อกำหนดที่ หน่วยงานราชการประกาศใช้

12.2 การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) เพื่อให้มั่นใจว่าระบบสารสนเทศขององค์กรและบริษัทสามารถดำเนินธุรกิจหรือให้บริการลูกค้าได้อย่างต่อเนื่อง

12.3 ความน่าเชื่อถือของผู้ให้บริการ ต้องมีแนวทางในการพิจารณาคัดเลือกผู้ให้บริการ เพื่อประเมินถึงความน่าเชื่อถือของการให้บริการ และเพื่อให้แน่ใจว่าผู้ให้บริการมีความสามารถในการให้บริการลูกค้าได้ตามข้อตกลงการให้บริการ

12.4 การดูแลและความรับผิดชอบต่อลูกค้า/การคุ้มครองผู้บริโภค (Customer Protection) ต้องมีแนวทางในการรักษาความปลอดภัยและความลับของข้อมูล เพื่อให้แน่ใจว่าได้ดูแลและรับผิดชอบต่อลูกค้าอย่างเหมาะสม

12.5 การติดตาม ประเมินผล และตรวจสอบการให้บริการจากบุคคลภายนอก จัดให้มีการติดตาม ประเมิน และตรวจสอบการให้บริการจากบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้เป็นไปตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

12.6 กำหนดให้มีแนวทางการบริหารความเสี่ยงจากการใช้บริการจากบุคคลภายนอก สำหรับความเสี่ยงด้านกลยุทธ์ ด้านการเงิน และความเสี่ยงด้านกฎหมาย โดยกำหนดแนวทางการบริหารความเสี่ยงจากการใช้บริการจากบุคคลภายนอกด้านเทคโนโลยีสารสนเทศไว้อย่างชัดเจนและเป็นลายลักษณ์อักษร ให้เหมาะสมกับความสำคัญของระบบงานที่ใช้บริการจากบุคคลภายนอก และสอดคล้องกับนโยบายการบริหารความเสี่ยงโดยรวม รวมทั้งสื่อสารให้บุคคลที่เกี่ยวข้องเข้าใจและถือปฏิบัติตามแนวทางที่กำหนด

13. นโยบายการบริหารข้อมูลสารสนเทศ

เพื่อให้บริการทางด้านข้อมูลเพื่อสนับสนุนในการดำเนินงาน และตอบสนองการแข่งขันขององค์กร จึงต้องมีการจัดหาแหล่งข้อมูล และรายงานให้กับผู้บริหารอย่างรวดเร็ว ซึ่งข้อมูลและรายงานเหล่านี้จะต้องมีความถูกต้องและสามารถใช้งานได้โดยผู้ที่เกี่ยวข้องเท่านั้น

13.1 การจัดหาและบำรุงรักษาแหล่งข้อมูลและรายงานผู้บริหาร

13.1.1 จัดหาแหล่งข้อมูลให้แต่ละส่วนงานสามารถนำข้อมูลไปใช้ในการวิเคราะห์วิจัย เพื่อใช้ในการแข่งขันทางธุรกิจอย่างรวดเร็ว

13.1.2 จัดให้มีรายงานสำหรับผู้บริหาร เพื่อเป็นข้อมูลในการตัดสินใจได้อย่างรวดเร็วและทันเวลา

13.1.3 การบำรุงรักษาแหล่งข้อมูล และรายงานผู้บริหารให้สามารถใช้งานได้ตามปกติ ดำเนินการโดยหน่วยงานเทคโนโลยีสารสนเทศ

13.1.4 ข้อมูลในแหล่งข้อมูลและรายงานผู้บริหาร มีความสำคัญระดับข้อมูลลับเฉพาะ (Highly Restricted)

13.1.5 ฝ่ายเทคโนโลยีสารสนเทศจะพัฒนาพนักงานผู้ใช้ข้อมูลของแต่ละส่วนงานให้สามารถสร้างรายงานเพิ่มเติมได้เอง

13.2 การเข้าถึงข้อมูลในแหล่งข้อมูล

13.2.1 ผู้ที่มีสิทธิใช้งานข้อมูลในแหล่งข้อมูลจะต้องได้รับการอนุมัติจากส่วนงานซึ่งเป็นเจ้าของข้อมูลเท่านั้น

13.2.2 กำหนดกลุ่มของผู้มีสิทธิใช้งานตามขอบเขตข้อมูลเป็น 3 ระดับ ดังนี้

1. เข้าถึงข้อมูลทุกฝ่าย
2. เข้าถึงข้อมูลเฉพาะฝ่าย
3. เข้าถึงข้อมูลเฉพาะเรื่องที่เกี่ยวข้อง

13.3 การควบคุมคุณภาพของข้อมูลในแหล่งข้อมูล

13.3.1 การทำ Data Cleaning จะเป็นหน้าที่ของผู้ใช้งาน โดยเจ้าหน้าที่เทคโนโลยีสารสนเทศช่วยสนับสนุนในการดึงข้อมูล และการปรับปรุงข้อมูลเข้าระบบ และทางผู้ใช้งานจะทำการแจ้งขอทำ Data Cleaning ผ่านทาง IT Request

13.3.2 การเปลี่ยนแปลงข้อมูลในแหล่งข้อมูล User จะเป็นผู้จัดเตรียมข้อมูลให้ และเจ้าหน้าที่เทคโนโลยีสารสนเทศ จะทำการปรับปรุงข้อมูลในฐานข้อมูล โดยใช้กระบวนการเดียวกันกับการทำ Data Cleaning และทางผู้ใช้งานจะทำการแจ้งขอเปลี่ยนแปลงข้อมูลผ่านทาง IT Request

13.4 การจัดส่งข้อมูลให้หน่วยงานภายนอก

การจัดข้อมูลให้กับหน่วยงานภายนอก จะต้องได้รับการอนุมัติจากผู้มีอำนาจเท่านั้น และก่อนที่จะจัดส่งต้องมีการตรวจสอบความถูกต้องของข้อมูลโดยผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลก่อน โดยฝ่ายเทคโนโลยีสารสนเทศจะแนะนำแหล่งข้อมูลในการดึงข้อมูลให้พิจารณาก่อนดำเนินการ

13.5 การร้องขอข้อมูล หรือจัดพิมพ์รายงาน

การร้องขอเพื่อดึงข้อมูล หรือจัดพิมพ์รายงาน ตามความต้องการของผู้ใช้งาน ควรได้รับความเห็นชอบจากประธานเจ้าหน้าที่บริหาร เป็นลายลักษณ์อักษร หรือผ่านทาง IT Request

14. นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Policy)

เพื่อให้ผู้ใช้งาน และบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้รับทราบถึงหน้าที่ความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงต่าง ๆ และมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศจึงกำหนดนโยบายดังต่อไปนี้

14.1 การรักษาความปลอดภัยต่อทรัพย์สินสารสนเทศ

ทรัพย์สินด้านสารสนเทศ ได้แก่ ฐานข้อมูล ไฟล์ข้อมูล ซอฟต์แวร์ เครื่องมือในการพัฒนาอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย อุปกรณ์สื่อสาร สื่อบันทึกข้อมูลภายนอก และอุปกรณ์ต่อพ่วงทุกชนิด ต้องมีการจัดทำบัญชีทรัพย์สิน ระบุผู้ถือครองทรัพย์สิน กำหนดวิธีการใช้งานทรัพย์สิน หรือการเข้าถึงข้อมูลสารสนเทศที่เหมาะสม ต้องมีการจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรเพื่อป้องกันความเสียหายด้านสารสนเทศ รวมถึงกรณีการคืนทรัพย์สินต้องมีกระบวนการบริหารจัดการ และจัดเก็บองค์ความรู้สำคัญของผู้รับการว่าจ้างเพื่อให้ความรู้ เหล่านั้นยังคงอยู่กับองค์กรต่อไปแม้บุคคลนั้นจะลาออกไปแล้ว

14.2 การจัดการข้อมูลสารสนเทศและการรักษาความลับ

ต้องมีการกำหนดชั้นความลับ การควบคุมการเข้าถึง และกำหนดระดับความสำคัญของเอกสาร (Classification Guidelines) เพื่อป้องกันทรัพย์สินด้านสารสนเทศ ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดยดำเนินการดังต่อไปนี้

14.2.1 จำแนกประเภทของข้อมูลสารสนเทศ/การจัดการชั้นความลับของสารสนเทศ (Information Classification) เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัย

14.2.2 ควบคุมการเข้ารหัสข้อมูล (Cryptographic Controls) กำหนดให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

14.2.3 ป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personally Identifiable Information)

14.2.4 สำรองข้อมูล (Backup)

14.3 การควบคุมดูแลบุคลากรผู้ปฏิบัติงาน

14.3.1 การตรวจสอบคุณสมบัติของผู้สมัครเข้าทำงานทุกกรณีโดยละเอียด เช่น ตรวจสอบจากจดหมายรับรองประวัติการทำงาน วุฒิการศึกษา หรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น

14.3.2 การกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงความปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับผู้ใช้งาน (End User) หรือที่ว่าจ้างหน่วยงานภายนอก (Supplier Relationships) มาปฏิบัติงานรวมทั้งกำหนดมาตรการป้องกันและดูแลรักษาความปลอดภัยสำหรับสารสนเทศของบริษัท

14.3.3 จัดฝึกอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยเพื่อให้พนักงานหรือผู้รับการว่าจ้างได้เรียนรู้ และทำความเข้าใจอย่างสม่ำเสมอ

14.3.4 กำหนดให้มีการถอดถอนสิทธิ์ในการเข้าถึงข้อมูล การคืนกุญแจหรือบัตรสำหรับการเข้าพื้นที่ต่าง ๆ กรณีที่สิ้นสุดหรือการเปลี่ยนการจ้างงานก่อนวันสุดท้ายของการมาทำงานหรือในสัญญาจ้าง

14.3.5 กำหนดกระบวนการทางวินัยให้มีการรายงานเหตุการณ์การละเมิดความมั่นคงปลอดภัย เช่น การไม่ปฏิบัติตามนโยบาย การละเมิดต่อความมั่นคงปลอดภัย เป็นต้น โดยกระบวนการดังกล่าวควรมีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่าง ๆ ที่องค์กรต้องปฏิบัติตาม

14.4 การจัดการระบบเครือข่ายคอมพิวเตอร์และการรับส่งข้อมูลสารสนเทศ

14.4.1 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ โดยกำหนดให้มีการบริหารจัดการต่อการเปลี่ยนแปลง, การบริหารจัดการขีดความสามารถของระบบ, การแยกสภาพแวดล้อมสำหรับการพัฒนา, การทดสอบและการให้บริการออกจากกัน, การป้องกันโปรแกรมไม่ประสงค์ดี, การสำรองข้อมูล, การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ, การตรวจประเมินระบบ และจัดให้มีขั้นตอนการปฏิบัติงานอย่างเป็นลายลักษณ์อักษร เป็นต้น

14.4.2 การควบคุมการรับส่งข้อมูลสารสนเทศ (Information Transfer) โดยกำหนดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบระหว่าง Network Administrator และ Computer Administrator ออกจากกัน, มีการควบคุมการเชื่อมต่อกับระบบเครือข่ายสาธารณะและระบบเครือข่ายไร้สาย, มีการบันทึก และจัดเก็บหลักฐาน (Log) เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้อง, การควบคุมการถ่ายโอนสารสนเทศ, ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ เป็นต้น

14.5 การป้องกันภัยคุกคามต่อระบบสารสนเทศ

14.5.1 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

14.5.2 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

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

14.6.1 วิเคราะห์และกำหนดความต้องการด้านความปลอดภัยสารสนเทศ

14.6.2 จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ผ่านระบบให้บริการ การใช้งานทั่วไป และกรณีที่ผ่านเครือข่ายสาธารณะ

14.6.3 กำหนดให้มีขั้นตอนสำหรับการควบคุมการเปลี่ยนแปลงระบบ การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศตลอดทุกขั้นตอนตามการควบคุมที่ได้กำหนดไว้

14.6.4 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ ระบบสำคัญต้องมีการทบทวน และทดสอบเพื่อมั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงาน หรือด้านความมั่นคงปลอดภัยต่อองค์กร

14.6.5 การทดสอบด้านความมั่นคงปลอดภัยของระบบ และการทดสอบเพื่อรับรองระบบ

15. นโยบายด้านการใช้ข้อมูลระหว่างองค์กร

เพื่อให้บรรลุวัตถุประสงค์ภายใต้การบริหารงานและทิศทางกลยุทธ์ขององค์กร ที่มีความจำเป็นต้องแบ่งปัน โอนแลกเปลี่ยน ใช้ หรือเปิดเผย (รวมเรียกว่า “**แบ่งปัน**”) ข้อมูลสารสนเทศและข้อมูลส่วนบุคคลระหว่างองค์กร (รวมเรียกว่า “**ข้อมูล**”) โดยข้อมูลที่มีการแบ่งปันระหว่างกัน

15.1 ก่อนการแบ่งปันข้อมูล ต้องดำเนินการแจ้งข้อมูลที่จำเป็นเกี่ยวกับการแบ่งปันข้อมูลและขอความยินยอมจากเจ้าของข้อมูล และ/หรือ มีฐานกฎหมายหรืออำนาจหน้าที่โดยชอบด้วยกฎหมายให้สามารถเปิดเผยข้อมูลให้อีกฝ่าย และให้อีกฝ่ายสามารถนำข้อมูลที่ได้รับนั้นไปใช้ตามวัตถุประสงค์ที่ได้ตกลงกันอย่างถูกต้องตามกฎหมายแล้ว

15.2 ควบคุมดูแลให้เจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ปฏิบัติหน้าที่ มีการรักษาความลับและปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลตามนโยบายและทิศทางกลยุทธ์ขององค์กร เว้นแต่เป็นไปตามเงื่อนไขหรือกฎหมายที่เกี่ยวข้อง

15.3 มีกำหนดให้การเข้าถึงข้อมูลเฉพาะเจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมายมีหน้าที่เกี่ยวข้องหรือมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้นโยบายและทิศทางกลยุทธ์ขององค์กร

15.4 บริษัท และบริษัทย่อย ที่รับข้อมูลจะไม่เปิดเผยข้อมูลภายในองค์กรแก่ผู้ที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องในการประมวลผล หรือบุคคลภายนอกใด ๆ เว้นแต่ที่มีความจำเป็นต้องกระทำตามหน้าที่ กฎหมายที่ใช้บังคับ หรือที่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้เป็นเจ้าของข้อมูล

15.5 องค์กรจัดให้มีและคงไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิคตามที่มีการประกาศ กำหนดและ/หรือตามมาตรฐานสากล โดยคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูล เพื่อคุ้มครองข้อมูลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ ลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผย หรือโอนข้อมูลโดยไม่ชอบด้วยกฎหมาย

15.6 กรณีที่องค์กรพบพฤติการณ์ที่มีลักษณะที่กระทบต่อการรักษาความปลอดภัยของข้อมูลที่แบ่งปันกันภายใต้นโยบายฉบับนี้ ซึ่งอาจก่อให้เกิดความเสียหายจากการละเมิด อุบัติเหตุ ลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลโดยไม่ชอบด้วยกฎหมาย ผู้ที่พบเหตุดังกล่าวจะดำเนินการแจ้งอีกฝ่ายทราบโดยทันที

15.7 การแจ้งถึงเหตุการละเมิดข้อมูลที่เกิดขึ้นภายใต้นโยบายนี้ ใช้มาตรการตามที่เห็นสมควรในการระบุถึงสาเหตุของการละเมิด และป้องกันปัญหาดังกล่าวมิให้เกิดซ้ำ และจะให้ข้อมูลแก่อีกฝ่ายภายใต้ขอบเขตที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนด ดังต่อไปนี้

15.7.1 รายละเอียดของลักษณะและผลกระทบที่อาจเกิดขึ้นของการละเมิด

15.7.2 มาตรการที่ถูกใช้เพื่อลดผลกระทบของการละเมิด

15.7.3 ประเภทของข้อมูลและเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิด หากมีปรากฏ

15.7.4 ข้อมูลอื่น ๆ เกี่ยวข้องกับการละเมิด

15.8 องค์กรจะให้ความช่วยเหลืออย่างสมเหตุสมผลแก่อีกฝ่าย เพื่อปฏิบัติตามกฎหมายคุ้มครองข้อมูลที่ใช้บังคับในการตอบสนองต่อข้อเรียกร้องใด ๆ ที่สมเหตุสมผลจากการใช้สิทธิต่าง ๆ ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเจ้าของข้อมูลส่วนบุคคล โดยพิจารณาถึงลักษณะการประมวลผล ภาระหน้าที่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ใช้บังคับ และข้อมูลส่วนบุคคลที่แต่ละฝ่ายประมวลผล

นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ต้องจัดให้มีการทบทวน หรือ ปรับปรุงนโยบายดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงของสภาพแวดล้อมต่าง ๆ ที่มีนัยสำคัญ เช่น สภาพธุรกิจ กฎเกณฑ์กฎหมาย และเทคโนโลยี เป็นต้น โดยต้องได้รับการอนุมัติจากคณะกรรมการบริหาร นอกจากนี้จะต้องเผยแพร่นโยบายดังกล่าวในลักษณะที่ผู้ใช้งานเข้าถึงได้ง่าย เพื่อให้บุคลากรที่เกี่ยวข้องทราบ และถือปฏิบัติเป็นไปตามที่นโยบายกำหนด