นโยบาย
เรื่อง การบริหารจัดการและความปลอดภัยของ
ระบบเทคโนโลยีสารสนเทศ

PC01-PCE-021

Rev.01

Petchsrivichai Enterprise Public Co., Ltd.
บริษัท เพชรศรีวิชัย เอ็นเตอร์ไพรส์ จำกัด (มหาชน)

สารบัญ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

1.หลักการและเหตุผล

บริษัทได้ตระหนักและให้ความสำคัญของการนำเทคโนโลยีสารสนเทศ และการสื่อสารซึ่งเป็นปัจจัยสำคัญที่ช่วยส่งเสริมการดำเนินธุรกิจ และเพิ่มประสิทธิภาพการทำงานให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกนปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ จึงได้กำหนดนโยบายฉบับนี้ขึ้นมาเพื่อให้บริษัทมีกรอบการบริหารจัดการระบบเทคโนโลยีสารสนเทศ

2. วัตถุประสงค์

เพื่อให้บริษัทมีนโยบายในการดำเนินงาน มาตรฐาน และแนวทางปฏิบัติด้านเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของบริษัท ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและวัตถุประสงค์ที่กำหนดไว้ และยังเพื่อป้องกันไม่ให้ระบบสารสนเทศ และสารสนเทศของบริษัท ถูกบุกรุก เปลี่ยนแปลง ขโมย ทำลาย หรือการกระทำอื่นๆ ซึ่งเป็นการคุกคามด้านความมั่นคงปลอดภัย ที่อาจส่งผลกระทบและสร้างความเสียหายต่อบริษัท

2.1. กฎหมายที่เกี่ยวข้อง

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560
3. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
4. พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537
5. พระราชบัญญัติเครื่องหมายการค้า
6. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.2 ขอบเขต

นโยบายฉบับนี้ใช้กับบริษัท เพชรศรีวิชัย เอ็นเตอร์ไพรส์ จำกัด *(มหาชน)* ประกอบด้วย บริษัท นิว ไบโอดีเซล จำกัด, บริษัท พี.ซี. มารีน (1992) จำกัด, บริษัท พี.เค.มารีน เทรดดิ้ง จำกัด, บริษัท เพชรศรีวิชัย จำกัด และ บริษัท ปาโก้เทรดดิ้ง จำกัด และบุคคลภายนอก (“ผู้ใช้งาน”) ที่ได้รับอนุญาตให้ ใช้ระบบเครือข่าย ระบบคอมพิวเตอร์เครื่องคอมพิวเตอร์ คอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสาร แบบพกพา หรืออุปกรณ์สื่อสารโทรคมนาคม เพื่อเข้าถึงสารสนเทศของบริษัท ทั้งที่อยู่ภายในหรือภายนอกสถานที่ปฏิบัติงานของบริษัท รวมทั้งคลาวด์ที่บริษัทจัดหา ซึ่งครอบคลุมถึง พนักงานและหน่วยงานทั้งหมดของบริษัท และบุคคลภายนอกบริษัทที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัทฯ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

3.บทบาทและความรับผิดชอบ

3.1 หน้าที่ของประธานเจ้าหน้าที่บริหาร

3.1.1 กำหนดกลยุทธ์ในภาพรวม ควบคุมการปฏิบัติงานในบริษัทฯ

3.1.2 อนุมัติระเบียบปฏิบัติ สนับสนุนนโยบายด้านสารสนเทศรวมถึงการเปลี่ยนแปลงที่อาจจะมีขึ้นของบริษัทฯ

3.1.3 กำหนดทิศทางและให้การสนับสนุนในการจัดทำนโยบายเทคโนโลยีสารสนเทศ รวมถึงระเบียบปฏิบัติที่เกี่ยวข้อง

3.1.4 ตัดสินใจในการติดต่อกับหน่วยงานบังคับใช้กฎหมาย และหน่วยงานสืบสวน เมื่อมีข้อสงสัยเกี่ยวกับการกระทำผิดร้ายแรงที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

3.2 หน้าที่ของผู้บริหาร

3.2.1 กำหนดให้มีการให้ความรู้เรื่องของนโยบายเทคโนโลยีสารสนเทศ ระเบียบปฏิบัติที่เกี่ยวข้องต่อพนักงานในบริษัทและหน่วยงานภายนอกที่เกี่ยวข้อง

3.2.2 ให้การสนับสนุนในการสืบสวน และเสนอแนวทางแก้ไขต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น

3.3 หน้าที่ของผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

3.3.1 กำหนดเป้าหมาย นโยบายด้านสารสนเทศของบริษัท โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนกลยุทธ์ของบริษัท

3.3.2 จัดการพัฒนานโยบายด้านสารสนเทศ Policy, Standard, Procedure และ Guideline เพื่อให้บริษัท ได้มาซึ่งการรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และเสถียรภาพความมั่นคง ของระบบ (Availability)

3.3.3 ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้งจัดหา และพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท

3.3.4 ดูแลทรัพยากรด้านสารสนเทศของบริษัทให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

3.3.5 จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่างๆ ที่อาจเกิดขึ้นกับระบบ รวมทั้งวางแผนบริหารความต่อเนื่องทางธุรกิจเพื่อกู้ระบบในยามฉุกเฉิน เพื่อสนับสนุนให้ธุรกิจสามารถดำเนินงานต่อไปได้อย่างต่อเนื่อง และเตรียมพร้อมรับสถานการณ์ และเพิ่มความสามารถด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

3.3.6 มีการบริหารความเสี่ยง และการวิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหา กระทบกับการดำเนินธุรกิจของบริษัท

3.3.7 ทบทวนและอนุมัติการดำเนินกิจกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

3.3.8 มีการบริหารความเสี่ยง วิเคราะห์ความเสี่ยงที่อาจทำให้ระบบเกิดปัญหาซึ่งอาจจะกระทบกับการดำเนินธุรกิจของบริษัท

3.4 หน้าที่ของผู้ดูแลระบบ

3.4.1 พัฒนาและจัดทำเอกสารกระบวนการสนับสนุนแนวทาง และขั้นตอนการปฏิบัติงาน เพื่อให้สอดคล้องตามนโยบายเทคโนโลยีสารสนเทศ

3.4.2 แจ้งให้ผู้เกี่ยวข้องรับทราบในกรณีที่พบหรือสงสัยว่าระบบสารสนเทศของบริษัทถูกคุกคาม สูญเสียหรือเสียหาย รวมทั้งกรณีที่มีการละเมิดต่อนโยบายเทคโนโลยีสารสนเทศ หรือระเบียบปฏิบัติที่เกี่ยวข้อง

3.4.3 ควบคุมระบบสารสนเทศให้คงสภาพ มีความสมบูรณ์ และความพร้อมใช้งาน และให้การช่วยเหลือด้านเทคนิคเกี่ยวกับปัญหาที่เกิดขึ้นเกี่ยวกับระบบเทคโนโลยีสารสนเทศ

3.5 หน้าที่ของผู้ใช้งาน

3.5.1 ต้องเรียนรู้ทำความเข้าใจกับนโยบาย ระเบียบปฏิบัติ และขั้นตอนปฏิบัติต่างๆ ตามนโยบายเทคโนโลยีสารสนเทศของบริษัทโดยเคร่งครัด รวมถึงให้ความร่วมมือในการใช้กฎข้อบังคับต่างๆ

3.5.2 ให้ความร่วมมือกับบริษัทอย่างเต็มที่ ในการป้องกันระบบคอมพิวเตอร์ และข้อมูลสารสนเทศของบริษัท สอดส่องดูแล ปกป้องข้อมูลและสารสนเทศของบริษัท ให้มีความมั่นคงปลอดภัย

3.5.3 รายงานต่อผู้บังคับบัญชา และฝ่ายเทคโนโลยีสารสนเทศโดยทันที เมื่อพบเห็นการบุกรุก ขโมย ทำลาย หรือโจรกรรม ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ ที่อาจสร้างความเสียหายต่อบริษัท

3.5.4 ใช้ทรัพย์สินของบริษัทอย่างมีจริยธรรม มีประสิทธิภาพ และไม่ละเมิดต่อกฎระเบียบและกฎหมาย

3.6 หน้าที่ของพนักงานหรือผู้ใช้งานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์

3.6.1 ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยต้องใช้โปรแกรมป้องกันไวรัส (Anti-virus) ที่มีฐานข้อมูลไวรัสที่มีการอัพเดทเป็นปัจจุบันและทันสมัย

3.6.2 ต้องมีการล็อคหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หรือระบบลายนิ้วมือ (Finger Scan) หากไม่ใช้งานเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งานคอมพิวเตอร์ได้

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

3.6.3 ต้องมีการออกจากระบบ (Log-out, Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังจากที่เลิกงาน

3.6.4 ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่บริษัทกำหนด เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ หรือข้อมูลของบริษัทเป็นความลับส่วนตัวพนักงาน ซึ่งจะต้องเก็บรักษาไว้มิให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น ทั้งนี้พนักงานต้องเปลี่ยนรหัสผ่านและรหัสอื่นใด เมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนดหรือเมื่อพนักงานเห็นสมควรต้องทำการเปลี่ยนรหัสผ่าน โดยตั้งรหัสผ่าน และรหัสอื่นใด ด้วยความรอบคอบ ทั้งนี้มาตรฐานการตั้งรหัสผ่านอย่างปลอดภัย

3.7 หน้าที่ของฝ่ายกฎหมาย

3.7.1 ให้ข้อแนะนำทางกฎหมายที่เกี่ยวข้องกับระเบียบ วิธีการปฏิบัติสำหรับการตรวจสอบการใช้ระบบสารสนเทศและอุปกรณ์ประมวลผลต่างๆ

3.8 หน้าที่ของหน่วยงานและผู้ใช้งานภายนอก

3.8.1 ปฏิบัติตามขั้นตอนตามนโยบายเทคโนโลยีสารสนเทศและเข้าถึงระบบสารสนเทศเฉพาะสิทธิ์ที่ได้รับเท่านั้น

3.8.2 รายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศให้กับฝ่ายเทคโนโลยีสารสนเทศที่เกิดขึ้นโดยทันที รวมถึงช่วยเหลือการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

4.ความหมายและคำจำกัดความ

นโยบายเทคโนโลยีสารสนเทศ ได้กำหนดความหมายและคำจำกัดความ เพื่อให้เกิดการเข้าใจที่ตรงกัน ดังนี้

1. "บริษัท (Company)" หมายถึง บริษัท เพชรศรีวิชัย เอ็นเตอร์ไพรส์ จำกัด *(มหาชน)* และบริษัทย่อย
2. "บริษัทย่อย และบริษัทในเครือ" หมายถึง บริษัท เพชรศรีวิชัยเอ็นเตอร์ไพรส์ มีอำนาจควบคุมในการบริหารจัดการ มีดังนี้
   - บริษัท เพชรศรีวิชัย จำกัด
   - บริษัท พี.เค. มารีน เทรดดิ้ง จำกัด
   - บริษัท พีซี มารีน (1992) จำกัด
   - บริษัท ปาโก้เทรดดิ้ง จำกัด
   - บริษัท นิว ไบโอดีเซล จำกัด
3. "พนักงาน (Employee)" หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

4. "ผู้ใช้งาน (User)" หมายถึง กรรมการบริษัท ผู้บริหาร พนักงานของบริษัท รวมไปถึงผู้ใช้งานภายนอกบริษัทที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งาน หรือ/และ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของบริษัท
5. "ผู้ปฏิบัติงาน" หมายถึง ผู้ปฏิบัติงาน ลูกจ้างทดลองงาน และลูกจ้างชั่วคราวของบริษัท
6. "ผู้ใช้งานที่เกี่ยวข้อง" หมายถึง บุคคล หรือนิติบุคคลที่เป็นคู่สัญญาของบริษัท ที่เข้ามาดำเนินกิจกรรมภายในบริษัท
7. "ผู้ใช้งานภายนอก" หมายถึง บุคคลที่นอกเหนือจากข้อ (5) และข้อ (6) ที่มาติดต่อสื่อสาร หรืออาจได้รับสิทธิ์การเข้าถึงทรัพย์สินสารสนเทศของบริษัท
8. ผู้ให้บริการภายนอก (External Party) หมายถึง หน่วยงานภายนอกที่อาจได้รับสิทธิเข้าถึงระบบสารสนเทศของบริษัท เช่น
   - ผู้ให้บริการ (Vendor)
   - ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource)
   - ผู้ให้บริการต่างๆ (Service Provider)
   - ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่างๆ (Supplier)
   - ที่ปรึกษา (Consultant)
9. "ผู้บังคับบัญชา" หมายถึง พนักงานซึ่งเป็นผู้บังคับบัญชาของหน่วยงานภายในตามโครงสร้างองค์กรของบริษัท
10. "ส่วนเทคโนโลยีสารสนเทศ" หมายถึง ส่วนเทคโนโลยีสารสนเทศ ของ บริษัท เพชรศรีวิชัย เอ็นเตอร์ไพรส์ จำกัด *(มหาชน)* และบริษัทย่อย
11. "สารสนเทศ" หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ เอกสาร แผนผัง แผนที่ ภาพถ่าย ฟิล์ม การบันทึกภาพ การบันทึกเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
12. "ระบบสารสนเทศ" หมายถึง ระบบงานของบริษัท ที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผล ให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร และการสนับสนุนกลไกการทำงานของบริษัท
13. "ข้อมูลสารสนเทศ (Information Technology)" หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่างๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรืออุปกรณ์ใดๆ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

14. "ข้อมูลสำคัญ" หรือ "ข้อมูลที่เป็นความลับ (Sensitive Information)" หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัท มีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัท ไม่อาจนำ ไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง
15. “สินทรัพย์” หมายถึง ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับบริษัท ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี หรือซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อบริษัท
16. "ระบบคอมพิวเตอร์ (Computer System)" หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุอุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่างๆ ระบบ Internet และระบบ Intranet รวมถึงอุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่างๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือคล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัท ของบริษัทย่อย และบริษัทอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของพนักงานที่นำเข้ามาติดตั้ง หรือใช้งานภายในสถานประกอบการของบริษัท
17. “ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัท ได้ เช่น ระบบ LAN ระบบ Wireless ระบบ Intranet ระบบ Internet และระบบการสื่อสารอื่นๆ
18. “ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ” หมายถึง ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายของบริษัท โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้าม ปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
19. เหตุขัดข้อง (Incident) หมายถึง เหตุขัดข้องที่ส่งผลทำให้ระบบสารสนเทศไม่สามารถให้บริการได้ตามที่กำหนดไว้ หรือคุณภาพในการให้บริการลดลง
20. “สิทธิ์ของผู้ใช้งาน” หมายถึง ระดับชั้นของการเข้าถึงข้อมูลสารสนเทศของผู้ปฏิบัติงาน และผู้ใช้งานที่เกี่ยวข้อง ได้แก่ สิทธิ์ทั่วไป สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ และระบบเครือข่ายของบริษัท

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

21. “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ
22. “บัญชีผู้ใช้งาน” หมายถึง บัญชีรายชื่อ (Username) และรหัสผ่าน (Password) สำหรับผู้ปฏิบัติงานผู้ใช้งานที่เกี่ยวข้อง และผู้ใช้งานภายนอก
23. รหัสผ่าน (Password) หมายถึง กลุ่มอักขระที่ใช้ในการพิสูจน์ตัวตน ใช้เพื่อควบคุมการเข้าถึงระบบสารสนเทศหรือข้อมูลสารสนเทศ
24. “การเข้ารหัส (Encryption)” หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ ข้อมูลผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้ จะต้องมี โปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
25. “การยืนยันตัวตน (Authentication)” หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปแล้ว เป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
26. สิทธิระดับสูง หมายถึง สิทธิ์ที่สามารถใช้งาน โดยได้รับสิทธิ์ที่ได้มากกว่าสิทธิ์ของผู้ดูแลระบบหรือผู้ใช้งานทั่วไป
27. "Remote Access" หมายถึง การเชื่อมต่อเพื่อเข้าถึงคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท (ผ่านช่องทางการสื่อสารภายในบริษัท) หรือ จากภายนอกบริษัท (ผ่าน Internet)
28. "ผู้ดูแลระบบ (Administrator)" หมายถึง เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศที่ได้รับมอบหมายให้ดูแลใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์ทั้งอุปกรณ์ Hardware Software และอุปกรณ์ต่อพ่วงที่ประกอบกันขึ้นเป็นระบบคอมพิวเตอร์ ผู้ดูแลระบบจะเป็นผู้ที่ได้รับอนุญาตให้มีอำนาจในการปรับเปลี่ยน เพิ่มเติม แก้ไข ปรับปรุงให้ระบบคอมพิวเตอร์ของบริษัททำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจและมีความปลอดภัย
29. "การรักษาความมั่นคงปลอดภัย" หรือ "ความมั่นคงปลอดภัย (Security)" หมายถึง กระบวนการ และการกระทำใดๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจากความพยายามใดๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอก ในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินธุรกิจของบริษัท ได้รับความเสียหาย
30. การสำรองข้อมูล (Data Backup) หมายถึง การทำสำเนาข้อมูลทั้งหมดในระบบที่ต้องการ เพื่อเป็นการสำรองข้อมูลที่อาจมีการแก้ไข เปลี่ยนแปลง หรือสูญหายให้สามารถนำกลับมาใช้งานได้ตามปกติ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

5. นโยบายการบริหารจัดการ บริการด้านเทคโนโลยีสารสนเทศ

5.1 การบริการจัดการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางการกำหนดขั้นตอนและข้อปฏิบัติก่อนการดำเนินการเปลี่ยนแปลงระบบสารสนเทศ เพื่อลดความเสี่ยงและข้อผิดพลาดในการหยุดให้บริการ เพื่อสนับสนุนธุรกิจของบริษัทได้อย่างต่อเนื่องและมีประสิทธิภาพ

5.1.1 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการเปลี่ยนแปลงระบบสารสนเทศและให้บันทึกการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร และต้องได้รับการอนุมัติจากผู้ที่เกี่ยวข้องและผู้บังคับบัญชาทุกครั้ง

5.1.2 ผู้ร้องขอให้มีการเปลี่ยนแปลงจะต้องจัดทำแผนภาพรวม รายละเอียดสำหรับการดำเนินการเปลี่ยนแปลง โดยกำหนดวันเวลาที่ต้องการดำเนินงาน และแจ้งให้ผู้เกี่ยวข้องรับทราบถึงแผนการเปลี่ยนแปลง

5.1.3 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดประเภทของการเปลี่ยนแปลงและกำหนดผู้ที่มีอำนาจอนุมัติ

5.2 การบริหารจัดการเหตุขัดข้อง และการบริหารจัดการเกี่ยวกับคำร้องขอ (Incident and Service Request Management Policy)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการแก้ไขเหตุขัดข้อง การจัดการระบบส่วนงานคอมพิวเตอร์ของบริษัทเพื่อสนับสนุนการให้บริการธุรกิจของบริษัทได้อย่างรวดเร็ว มีความต่อเนื่อง และมีประสิทธิภาพ

5.2.1 ฝ่ายเทคโนโลยีสารสนเทศต้องมีการกำหนดเกณฑ์ในการวัดความเร่งด่วน (Urgency) ผลกระทบ (Impact) และลำดับความสำคัญ (Priority) ของเหตุขัดข้อง

5.2.2 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบในการแก้ไขเหตุขัดข้องพร้อมทั้งจัดทำขั้นตอนปฏิบัติในการแก้ไขปัญหา เพื่อเป็นแนวทางในการแก้ไขปัญหาต่อไป พร้อมทั้งมีการบันทึกรายละเอียดของเหตุขัดข้อง เพื่อใช้ประกอบการวิเคราะห์ปัญหาที่เกิดขึ้น

5.2.3 ฝ่ายเทคโนโลยีสารสนเทศต้องมีการกำหนดขั้นตอนหรือวิธีปฏิบัติในการณีที่ไม่สามารถแก้ไขเหตุขัดข้องได้ด้วยตนเอง โดยจะต้องมีการยกระดับการให้บริการ (Escalation) ไปยังผู้เกี่ยวข้องตามลำดับ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

5.3 การบริหารจัดการควบคุมจากภายนอกหรือการควบคุมระยะไกล (Remote Access)

วัตถุประสงค์

เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัย สำหรับการปฏิบัติงานขององค์กรจากระยะไกล เฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต โดยมีแนวทางปฏิบัติดังต่อไปนี้

5.3.1 ก่อนการเข้าสู่ระบบจากระยะไกล ต้องได้รับอนุญาตจากหัวหน้างานและหัวหน้าฝ่ายเทคโนโลยีสารสนเทอย่างเป็นทางการ และผู้ใช้งานต้องปฏิบัติตามกฎระเบียบอย่างเคร่งครัด

5.3.2 ในการเข้าสู่ระบบจากระยะไกลต้องมีการยืนยันตัวตนทุกครั้ง เช่น มีการใส่รหัสผ่าน หรือวิธีการเข้ารหัส

5.3.3 ต้องมีการควบคุม Port และกำหนดระยะเวลาสำหรับเข้าใช้งานระบบ รวมไปถึงกรณีให้ตัดการเชื่อมต่อทุก 15 นาที เมื่อไม่มีการใช้งาน

5.3.4 การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น

5.4 การสอบทานสิทธิ์การเข้าถึงของผู้ใช้งานทางด้านเทคโนโลยีสารสนเทศของบริษัท

วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับระบบสารสนเทศของบริษัทเป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และเป็นไปตามสิทธิ์ที่พึงมี โดยมีแนวทางปฏิบัติดังต่อไปนี้

5.4.1 ต้องมีการดำเนินการตรวจสอบสิทธิ์การเข้าถึงของผู้ใช้งานด้านระบบสารสนเทศ อย่างน้อยทุกๆ 6 เดือน

5.4.2 หลังจากดำเนินการตรวจสอบสิทธิ์การเข้าถึงของผู้ใช้งานด้านระบบสารสนเทศแล้วต้องมีการรายงานข้อมูลต่อทางผู้บังคับบัญชาหรือผู้จัดการแผนกเทคโนโลยีสารสนเทศทุกครั้ง

5.5 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

วัตถุประสงค์

เพื่อกำหนดให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องสอดคล้องกบนโยบายการบริหารความเสี่ยงองค์กร (Corporate Risk Management) และครอบคลุมในเรื่องดังต่อไปนี้

5.5.1 การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ผู้จัดการฝ่ายเทคโนโลยีมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่ แล้วนำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

5.5.2 การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk)

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

- ความเสี่ยงด้านกายภาพและสภาพแวดล้อม ได้แก่ ห้องศูนย์กลางข้อมูล (Data Center Room) ซึ่งเป็นที่จัดเก็บติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย(Server) อุปกรณ์เครือข่ายและอุปกรณ์อื่น ต้องมีการควบคุมการเข้า-ออก และการใช้งาน การตรวจสอบระบบต่างๆ เช่นระบบเตือนอุณหภูมิภายในห้อง ระบบเตือนอัคคีภัย เป็นต้น

- ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของบริษัท เพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัยหรือไม่ประสงค์ดี เช่น การดาวน์โหลดโปรแกรมจากภายนอกมาติดตั้ง ซึ่งอาจมีมัลแวร์ หรือไวรัสคอมพิวเตอร์ หรือมีช่องโหว่เชื่อมต่อเครือข่ายภายนอก เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน เป็นต้น

- ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ของบริษัท ต้องมีตรวจสอบและ เฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต โดยมีการจัดทำระบบป้องกัน การเข้าถึงและการโจมตีจากภายนอกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงานใช้งาน เช่น ระบบป้องกันการเข้าออก ใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ การกรองข้อมูลรับส่ง อีเมล เป็นต้น

- ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิ์การใช้งานเข้าถึงระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายต่างๆ และข้อมูล ให้เป็นไปตามสิทธิ์ที่พึงมี เพื่อป้องกันการเข้าแก้ไขหรือ เปลี่ยนแปลงข้อมูล

5.5.3 การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ 4 ประเภท ดังนี้

1. ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี
2. ความเสี่ยงจากผู้ปฏิบัติงาน ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลเกินกว่าหน้าที่ และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้
3. ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้งสถานการณ์อื่นๆ เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น
4. ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากแนวนโยบายที่ทำการใช้งานอยู่อาจไม่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

5.5.4 การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่บริษัทยอมรับได้ โดยจัดทำตารางลักษณะรายละเอียดความความเสี่ยง (Description of Risk) โดยมีหัวเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

5.5.5 กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6. นโยบายความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยมีแนวทางปฏิบัติดังนี้

6.1 นโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ IT (Information Security Policy)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศของบริษัท โดยบริษัทต้องจัดให้มีหน้าที่ดูแลให้มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรจากประธานเจ้าหน้าที่บริหารหรือเจ้าหน้าที่บริหาร และบริษัทต้องทำการสื่อสารนโยบายดังกล่าวเพื่อสร้างความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานด้านอื่นภายในบริษัท เพื่อให้มีการประสานงานและสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้ และต้องดำเนินการตรวจสอบ ทบทวน และประเมินนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.1.1 ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมายหรือขัดต่อศีลธรรมอันดี เป็นต้น

6.1.2 ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้

6.1.3 ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่นที่กลุ่มบริษัท เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก หรือกระทำการอื่นใดที่ปราศจากอำนาจหรือเกินขอบเขตอำนาจ

6.1.4 ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูลนั้นๆ โดยไม่ได้รับอนุญาตจากทางบริษัท

6.1.5 ห้ามก่อกวน ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัทเกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น

6.1.6 ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัท และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์

6.1.7 ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ หรือเปิดไฟล์ที่แนบมากับ Email หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนทุกครั้ง

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.1.8 ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

6.2 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

วัตถุประสงค์

เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายในบริษัท และเพื่อกำหนดมาตรการควบคุม จำกัด กรอบการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายในบริษัท และเพื่อเป็นแนวทางควบคุมอุปกรณ์สื่อสาร ให้เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.2.1 ผู้บริหารระดับสูง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท

6.2.2 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในส่วนเทคโนโลยีสารสนเทศ รับผิดชอบการดูแลระบบสารสนเทศที่บริษัทใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัทผู้จัดการส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในส่วนเทคโนโลยีสารสนเทศ รับผิดชอบการดูแลระบบสารสนเทศที่บริษัทใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท

6.2.3 ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท

6.2.4 ผู้ปฏิบัติงานส่วนเทคโนโลยีสารสนเทศ ที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator รับผิดชอบต่อระบบที่ดูแลนั้น จะต้องทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยในการใช้งานของระบบด้วย และเมื่อมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด จะต้องดำเนินการแก้ไขและรายงานต่อผู้บังคับบัญชา

6.2.5 ผู้ใช้งานและหน่วยงานทั้งภายในและภายนอก ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัท ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

6.3 การสร้างความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร (Human Resource Security)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศของบริษัท
โดยมีแนวทางปฏิบัติดังต่อไปนี้

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.3.1 ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับบุคคลหรือหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศของบริษัท

6.3.2 ต้องมีการลงนามในสัญญาระหว่างผู้ปฏิบัติงานและหน่วยงาน ว่าจะไม่เปิดเผยความลับของบริษัท(Non-Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างผู้ปฏิบัติงานนั้นๆ ทั้งนี้ ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

6.3.3 ในกรณีที่ผู้ปฏิบัติงานซึ่งเป็นบุคคลหรือหน่วยงานภายนอกดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลในระบบสารสนเทศของบริษัท โดยมีลักษณะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องมีการลงนามในสัญญาประมวลผลข้อมูลส่วนบุคคล (Personal data processing agreement) กับผู้ปฏิบัติงานซึ่งข้อสัญญาต้องกำหนดให้ผู้ปฏิบัติงานทำการเฉพาะตามคำสั่งของบริษัทและมีหน้าที่จัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่าง เหมาะสมตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

6.3.4 เพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ฝ่ายทรัพยากรบุคคลหรือหน่วยงานที่เกี่ยวข้อง ต้องแจ้งให้ผู้จัดการส่วนเทคโนโลยีสารสนเทศทราบทันที เมื่อมีเหตุดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นกรรมการและผู้ปฏิบัติงานของบริษัท
- การโยกย้ายหน่วยงาน
- การพักงาน การลงโทษวินัย หรือระงับการปฏิบัติหน้าที่

6.3.5 ต้องให้ผู้ใช้งานและหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และนโยบายอื่นๆ ที่เกี่ยวข้อง เช่น นโยบายคุ้มครองข้อมูลส่วนบุคคล

6.3.6 ผู้ปฏิบัติงานใหม่ของบริษัทต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ

6.3.7 หลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน หรือสิ้นสุดโครงการ ต้องยกเลิกการเข้าถึงข้อมูลในระบบสารสนเทศทันที

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.4 การบริหารจัดการสินทรัพย์สารสนเทศ (Asset Management)

6.4.1 การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral Access Control)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ โดยมีแนวทางปฏิบัติดังต่อไปนี้

1. ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน
2. ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม
3. ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบฝ่ายเทคโนโลยีสารสนเทศ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน
4. ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบฝ่ายเทคโนโลยีสารสนเทศ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม
5. ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ
6. ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
7. ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน
8. ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่
9. หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
10. ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน
11. การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

12. ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

6.4.2 การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนเข้าใจการใช้โปรแกรมที่ถูกต้องลิขสิทธิ์และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง โดยมีแนวทางปฏิบัติดังต่อไปนี้

ข้อกำหนดสำหรับผู้ดูแลระบบ

1. มีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัทตามสิทธิ์การใช้งานที่กำหนด

2. มีหน้าที่รับผิดชอบในการติดตั้ง และอัพเกรดโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวันเวลาที่นัดหมาย

3. ทำการถอดและยกเลิกสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ทันที เมื่อบริษัท และ/หรือหน่วยงาน แจ้งยกเลิกและ/หรือย้ายสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์

ข้อกำหนดสำหรับผู้ใช้งาน

1. ต้องใช้โปรแกรมคอมพิวเตอร์โดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับบริษัท

2. โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน

3. ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้นโดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย

4. ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทมีอยู่ มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะมี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้นผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว นอกจากนี้ หากโปรแกรมที่ไม่ชอบด้วยกฎหมายดังกล่าวส่งผลกระทบให้เกิดการสูญหาย แก้ไขเปลี่ยนแปลง ข้อมูลส่วนบุคคล ผู้ใช้งานอาจต้องมีความรับผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอีกด้วย

5. การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติ และผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6. ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท

7. แจ้งให้บริษัททราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นการบุกรุก โจรกรรม ทำลาย แทรกแซงการทำงาน หรือจารกรรมที่อาจสร้างความเสียหายต่อบริษัท

6.4.3 การควบคุมสินทรัพย์ด้านสารสนเทศและการเข้าใช้งานระบบคอมพิวเตอร์

วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนกถึงหน้าที่และความรับผิดชอบในการไม่ให้สินทรัพย์ด้านสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ และข้อมูลสารสนเทศอยู่ในสภาวะเสี่ยงต่อการเขาถึงได้โดยผู้ซึ่งไม่มีสิทธิ์ขณะที่ไม่มีผู้ใช้งานอุปกรณ์

6.4.3.1 ต้องออกจากระบบ (Log-out, Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน

6.4.3.2 ต้องล็อคหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือไปทำกิจกรรมอย่างอื่นเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน หรือมีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้การพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

6.4.3.3 ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส (Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย

6.4.3.4 ต้องจัดเก็บและสำรองข้อมูลสารสนเทศที่มีความสำคัญของหน่วยงานไว้ในที่ที่ปลอดภัย การจัดเก็บข้อมูลของผู้ใช้งาน จะจัดเก็บได้อยู่ในรูปแบบดังนี้

- ในฐานข้อมูลของระบบ Application นั้นๆ ที่จัดเก็บภายใน Data Center ของบริษัทหรือจัดเก็บในพื้นที่ตามที่บริษัทกำหนด โดยการ Export ข้อมูลออกมาจากระบบ Application ไม่สามารถทำได้
- สามารถจัดเก็บใน Shared File (Drive กลาง) ใน Folder ตามสิทธิ์ที่ได้รับ

6.4.3.5 ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อไม่มีการใช้งานนานเกิน 1 ชั่วโมง หรือเมื่อใช้งานประจำวันเสร็จสิ้นงาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง

6.4.3.6 ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่บริษัทกำหนด เพื่อใช้ในการเข้าถึงระคอมพิวเตอร์ข้อมูลสารสนเทศ หรือข้อมูลของบริษัทเป็นความลับส่วนตัวพนักงาน ซึ่งจะต้องเก็บรักษาไว้มิให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น ทั้งนี้พนักงานต้องเปลี่ยนรหัสผ่านและรหัสอื่นใด เมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนดหรือเมื่อพนักงานเห็นสมควรต้องทำการเปลี่ยนรหัสผ่าน โดยตั้งรหัสผ่าน และรหัสอื่นใด ด้วยความรอบคอบ ห้ามตั้งรหัสซ้ำกับรหัสเก่า ห้ามตั้งรหัสที่ผู้อื่นสามารถคาดเดาได้ง่าย หรือห้ามตั้งรหัสซ้ำกันในทุกระบบที่พนักงานมีสิทธิใช้งาน ทั้งนี้มาตรฐานการตั้งรหัสผ่านอย่างปลอดภัย

6.4.3.7 การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากไม่ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 15 นาที

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.4.3.8 ให้มีการขออนุมัติจากผู้มีอำนาจสูงสุดของฝ่ายขึ้นไป ในกรณีที่ต้องการนำทรัพย์สินด้านสารสนเทศต่างๆ เช่น เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกบริษัททุกครั้ง โดยปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท

6.4.3.9 ระมัดระวังและดูแลทรัพย์สินของบริษัท ที่ตนเองใช้งานเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเลินเล่อ ต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

6.5 การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สามารถสนับสนุนการปฏิบัติงานและเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ ปลอดภัย ภายใต้ข้อกำหนดของกฎหมาย ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของบริษัท ตลอดจนเพื่อให้ผู้ใช้งานเข้าใจถึงความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ์ หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.5.1 ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายที่เกี่ยวข้อง และนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศที่บริษัทกำหนด

6.5.2 หน่วยงานหรือผู้ปฏิบัติงานผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท จะต้องใช้จดหมายอิเล็กทรอนิกส์เพื่อผลประโยชน์ของบริษัท

6.5.3 ผู้ปฏิบัติงานจะได้รับสิทธิ์ในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียนผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ ตามรายชื่อผู้ปฏิบัติงานที่ได้รับแจ้งมาจากฝ่ายทรัพยากรบุคคล

6.5.4 ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อความ เว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

6.5.5 การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น

6.5.6 การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของบริษัท ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทขัดข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.5.7 การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของบริษัท หรือก่อให้เกิดความเสียหายต่อบริษัท

6.5.8 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์ หรือกระทบต่อการดำเนินงานของบริษัท ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของบริษัท

6.5.9 ห้ามผู้ใช้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการงานส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีการกระทำดังกล่าว ให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ หรือเจ้าของผู้ใช้บริการเป็นผู้รับผิดชอบการกระทำดังกล่าวแต่ผู้เดียว

6.5.10 ห้ามกระทำการอันที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่ (Chain mail) การส่งจดหมายจำนวนมาก (Spam mail) การส่งจดหมายต่อเนื่อง (Letter bomb) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์ เป็นต้น

6.5.11 ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของบริษัท

6.5.12 การส่งข้อมูลข่าวสารที่เป็นความลับบริษัท ควรมีการเข้ารหัสข้อมูลข่าวสารนั้น และไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

6.5.13 ในการใช้ระบบจดหมายอิเล็กทรอนิกส์ส่งข้อมูลใดที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ผู้ใช้จะต้องตรวจสอบการดำเนินการให้สอดคล้องกับนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทด้วย

6.5.14 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง

6.5.15 กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมายที่เกี่ยวข้องกับการใช้ระบบจดหมายอิเล็กทรอนิกส์อันมีความเสี่ยงต่อความไม่ปลอดภัยต่อระบบเครือข่ายและระบบคอมพิวเตอร์ หรือความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล หรือความเสี่ยงต่อการกระทำใดๆ อันฝ่าฝืนกฎหมาย ทางบริษัท ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับการบริการชั่วคราวแก่ผู้ปฏิบัติงานนั้นๆ เพื่อทำการสอบสวน และตรวจสอบสาเหตุ

6.5.16 หากผู้ใช้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิด เกิดขึ้นในบริษัท ให้แจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของบริษัท

6.5.17 การกระทำใดๆ ที่เกี่ยวข้องกับการเผยแพร่ ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์ และโฮมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการเท่านั้น ผู้ดูแลระบบและบริษัทไม่มีส่วนเกี่ยวข้องใดๆ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.6 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรการในการใช้งานระบบอินเทอร์เน็ตผ่านระบบเครือข่ายของบริษัท เพื่อให้เกิดประสิทธิภาพและมีความมั่นคงปลอดภัย และเพื่อให้ผู้ใช้งานมีความตระหนักในการใช้งานเว็บไซต์ต่างๆ ผ่านระบบเครือข่ายของบริษัท โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.6.1 ส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่ายเพื่อการเข้าใช้งานระบบอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy เป็นต้น

6.6.2 เครื่องคอมพิวเตอร์ของบริษัท ก่อนทำการเชื่อมต่อระบบเครือข่าย ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการก่อน

6.6.3 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

6.6.4 ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของบริษัท

6.6.5 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของบริษัท ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของบริษัท

6.6.6 ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดเพื่อปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

6.6.7 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำไปใช้งาน

6.6.8 ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ลามกอนาจาร เป็นต้น

6.6.9 ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่นๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อบริษัท รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่บริษัทกำหนดไว้อย่างเคร่งครัด

6.6.10 กำหนดให้มีการทบทวนปรับปรุงสิทธิการใช้งานตามรอบระยะเวลาที่กำหนด โดยจัดให้มีการทบทวนสิทธิการเข้าถึงอยู่เสมอ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.6.11 การเข้าถึงจะต้องใช้วิธีการพิสูจน์ตัวตนที่มีความปลอดภัย และสามารถตรวจสอบข้อมูลย้อนหลังได้ เช่น การใช้ Username และ Password เป็นต้น

6.7 การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

วัตถุประสงค์

เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ หรือแก้ไขเปลี่ยนแปลง ข้อมูลหรือการทำงานของระบบสารสนเทศในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.7.1 การบริหารจัดการข้อมูล

6.7.1.1 ต้องมีการจัดลำดับชั้นความลับ ต้องมีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนดวิธีบริหารจัดการกับข้อมูลแต่ละประเภท รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการยกเลิกหรือการนำกลับมาใช้ใหม่

6.7.1.2 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส(Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL(Secure Socket Layer) การใช้ VPN (Virtual Private Network) เป็นต้น

6.7.1.3 ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage) นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้อง ครบถ้วนตรงกัน

6.7.1.4 ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม เป็นต้น หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

6.7.2 การบริหารจัดการการเข้าถึงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศของบริษัท กรณีลบ/ยกเลิกสิทธิ์/เปลี่ยนแปลงสิทธิ์ ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศของบริษัทเฉพาะผู้ใช้งานที่รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจในเรื่องการบริหารจัดการสิทธิ์ให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางปฏิบัติดังนี้

6.7.2.1 ฝ่ายเทคโนโลยีสารสนเทศกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และสารสนเทศ ในกรณีที่ต้องการลบ ยกเลิกสิทธิ์ หรือเปลี่ยนแปลงสิทธิ์ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

6.7.2.2 ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ต้องให้หัวหน้าแผนกหรือผู้จัดการของแผนกนั้นแจ้งฝ่ายเทคโนโลยีสารสนเทศ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

6.7.2.3 ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือพนักงานในแผนกที่พนักงานสังกัดลาออก ต้องให้ทางฝ่ายทรัพยากรบุคคลแจ้งฝ่ายเทคโนโลยีสารสนเทศ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิและทำการลบและยกเลิกสิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.7.3 การควบคุมการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Privilege)

เนื่องจากบัญชีผู้มีสิทธิ์สูงมีผลกระทบต่อระบบมาก จึงต้องมีการควบคุมบางอย่างเพื่อจำกัด หรือตรวจสอบการเข้าใจงานบัญชีเหล่านี้ ดังนั้นแนวทางปฏิบัติเบื้องต้นที่ใช้ควบคุมบัญชีผู้มีสิทธิ์สูง มีดังนี้

6.7.3.1 ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

6.7.3.2 ต้องกำหนดสิทธิ์การใช้ข้อมูลและระบบสารสนเทศ เช่น สิทธิ์การใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิ์การใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

6.7.3.3 ในกรณีมีความจำเป็นต้องใช้ User ที่มีสิทธิ์พิเศษ (High privilege User ID) ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิ์พิเศษมีความรัดกุมเพียงพอหรือไม่นั้น บริษัทจะใช้ปัจจัยประกอบการพิจารณาในภาพรวมดังต่อไปนี้

- ควรได้รับความเห็นชอบและอนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง
- ควรควบคุมการใช้งานของผู้ใช้งานที่มีสิทธิ์พิเศษอย่างเข้มงวด เช่น จำกัด การใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- จำกัดจำนวนบัญชีผู้มีสิทธิ์สูงให้น้อยที่สุด ผู้ดูแลระบบแต่ละคนควรมีบัญชีที่มี สิทธิ์สูงบัญชีเดียวสำหรับการทำงานทุกระบบ
- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นใน การใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ควรเปลี่ยน รหัสผ่านทุก 6 เดือน เป็นต้น
- ไม่อนุญาตให้ผู้ดูแลระบบทำการแชร์บัญชีผู้มีสิทธิ์สูง โดยใช้บัญชีของผู้ที่ได้รับมอบหมายโดยให้สิทธิ์สูง เพื่อทำให้ผู้ใช้งานไม่สามารถปฏิเสธความรับผิดชอบต่อ การกระทำของผู้ใช้นั้นๆ
- หากผู้ใช้งานต้องการเข้าถึงบัญชีผู้มีสิทธิ์สูง ต้องทำตามขั้นตอนการร้องขอ และการอนุมัติเอกสารไม่ว่าจะเป็นทางกระดาษ หรือระบบที่องค์กรได้จัดทำขึ้น และเข้าใช้งาน เฉพาะในช่วงเวลาที่ได้ระบุไว้

6.7.3.4 ในกรณีที่ไม่มีการปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่มิได้มีสิทธิ์และหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.7.3.5 ในกรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิ์ผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share Files เป็นต้น จะต้องเป็นการให้สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิ์ดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิ์ดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

6.7.3.6 ในกรณีที่มีความจำเป็นต้องให้สิทธิ์บุคคลอื่น ให้มีสิทธิ์ใช้งานระบบสารสนเทศและระบบเครือข่ายในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

6.7.4 การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password)

6.7.4.1 ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบสารสนเทศที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น บริษัทจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม โดย Password policy สำหรับเข้าใช้งานระบบ Microsoft Azure และนโยบายรหัสผ่านถูกนำไปใช้กับบัญชีผู้ใช้ทั้งหมดที่สร้างและจัดการโดยตรงใน Azure AD ซึ่งจะไม่สามารถเปลี่ยนแปลง Setting ได้ โดยค่าเริ่มต้น บัญชีจะถูกล็อคหลังจากพยายามลงชื่อเข้าใช้ไม่สำเร็จ 10 ครั้งด้วยรหัสผ่านที่ไม่ถูกต้อง และผู้ใช้ถูกล็อคออกเป็นเวลาหนึ่งนาที การพยายามลงชื่อเข้าใช้ที่ไม่ถูกต้องอีกจะล็อกอีกโดยมีการเพิ่มระยะเวลาขึ้น โดย Azure Password policy นี้จะเป็นการล็อกแบบอัจฉริยะ โดยจะติดตามรหัสผ่านที่ไม่เหมาะสม 3 รายการสุดท้ายเพื่อหลีกเลี่ยงการเพิ่มตัวนับการล็อกสำหรับรหัสผ่านเดียวกัน หากมีคนป้อนรหัสผ่านที่ผิดซ้ำกันหลายครั้ง สำหรับ Azure AD password policy มีรายละเอียดดังนี้

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

Property	Requirements
Characters allowed	• A – Z • a - z • 0 – 9 • @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > • blank space
Characters not allowed	Unicode characters.

Password restrictions	• A minimum of 8 characters and a maximum of 256 characters.
	• Requires three out of four of the following:
	  ◦ Lowercase characters.
	  ◦ Uppercase characters.
	  ◦ Numbers (0-9).
	  ◦ Symbols (see the previous password restrictions).

Password expiry duration (Maximum password age)	• Default value: **90** days. • The value is configurable by using the `Set-MsolPasswordPolicy` cmdlet from the Azure Active Directory Module for Windows PowerShell.
Password expiry notification (When users are notified of password expiration)	• Default value: **14** days (before password expires). • The value is configurable by using the `Set-MsolPasswordPolicy` cmdlet.
Password expiry (Let passwords never expire)	• Default value: **false** (indicates that password's have an expiration date). • The value can be configured for individual user accounts by using the `Set-MsolUser` cmdlet.
Password change history	The last password *can't* be used again when the user changes a password.
Password reset history	The last password *can* be used again when the user resets a forgotten password.

- สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือน ส่วนผู้ใช้งานที่มีสิทธิ์พิเศษ เช่น ผู้จัดการระบบ (System Administrator) และผู้ใช้งานที่ติดมากับระบบ (Default

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

User) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 3 เดือน

- ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิม 3 ครั้งหลังสุด
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที
- ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ไม่ควรจดใส่กระดาษแล้วติดไว้หน้าเครื่อง ทั้งนี้ ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที
- สำหรับกรณีผู้ใช้งานมีการใช้งานร่วมกันลักษณะ Shared Users Licenses ทางผู้ดูแลจะมีการส่งอีเมลแจ้งเตือนผู้รับผิดชอบการใช้งานให้ทำการเปลี่ยนรหัสผ่านในการเข้าระบบงานนั้น เมื่อมีการเปลี่ยนแปลงของผู้ใช้งานในสังกัด

6.7.4.2 ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง

6.7.4.3 ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มิได้มีสิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของผู้ปฏิบัติงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยน รหัสผ่าน เป็นต้น

6.8 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

วัตถุประสงค์

การควบคุมการเข้าออกห้องศูนย์กลางข้อมูล (Data Center Room) มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออก Data Center Room และระบบป้องกันความเสียหายต่างๆ ที่บริษัทควรจัดให้มีภายใน Data Center Room โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.8.1 การควบคุมห้องศูนย์กลางข้อมูล (Data Center Room)

6.8.1.1 ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ ใน Data Center Room หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิ์การเข้าออก Data Center Room ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น ผู้ดูแลระบบ เป็นต้น

6.8.1.2 ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออก Data Center Room ในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีผู้ดูแลระบบ และ/หรือ ผู้ปฏิบัติงานที่เกี่ยวข้อง ควบคุมดูแลการทำงานตลอดเวลา

6.8.1.3 ต้องมีระบบเก็บบันทึกการเข้าออก Data Center Room โดยบันทึกดังกล่าวต้องมี รายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.8.1.4 ควรจัด Data Center Room ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ส่วนเครื่องสำรองไฟฟ้า (UPS Zone) ส่วนแบตเตอรี่เครื่องสำรองไฟฟ้า (Battery UPS Zone) เป็นต้น เพื่อความสะดวกในการปฏิบัติงานและทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น

6.8.2 การป้องกันความเสียหาย

6.8.2.1 ระบบป้องกันไฟไหม้

- ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา
- Data Center Room หลักต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับศูนย์คอมพิวเตอร์สำรองอย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

6.8.3 ระบบป้องกันไฟฟ้าขัดข้อง

- ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า
- ต้องมีระบบสำรองไฟฟ้าสำหรับระบบงานคอมพิวเตอร์ที่สำคัญ และระบบเครือข่ายคอมพิวเตอร์ เพื่อให้การดำเนินงานมีความต่อเนื่อง

6.8.4 ระบบควบคุมอุณหภูมิและความชื้น

- ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

6.8.5 ระบบเตือนภัยน้ำรั่ว

- ในกรณีที่มีการยกระดับพื้นของ Data Center Room เพื่อติดตั้งระบบปรับอากาศ รวมทั้งเดินสายไฟและ/หรือ สายเครือข่ายด้านล่าง ควรติดตั้งระบบเตือนภัยน้ำรั่วบริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่วได้ทันเวลา หาก Data Center Room ตั้งอยู่ในสถานที่ที่มีความเสี่ยงต่อภัยน้ำรั่ว ควรหมั่นสังเกตว่ามีน้ำรั่วหรือไม่ อย่างสม่ำเสมอ

6.9 การรักษาความมั่นคงปลอดภัยในการดำเนินงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับระบบสารสนเทศของบริษัทเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ป้องกันการสูญหายของข้อมูล และได้รับการปกป้องจากโปรแกรมไม่ประสงค์ดี โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.9.1 จัดทำคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับระบบสารสนเทศที่สำคัญของบริษัท เพื่อป้องกันความผิดพลาดในการปฏิบัติงานด้านสารสนเทศ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.9.2 กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศ เช่น ต้องมีการขออนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ เป็นต้น

6.9.3 ต้องมีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ

6.9.4 ควรติดตั้งระบบเพื่อตรวจสอบติดตามทรัพยากรของระบบสารสนเทศ เช่น CPU, Memory, Hard Disk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต

6.9.5 ระบบที่มีความสำคัญสูง ควรแยกระบบการพัฒนาออกจากระบบการให้บริการจริง เพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

6.9.6 ต้องสำรวจข้อมูล จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรองและความถี่ในการสำรองข้อมูล

6.9.7 ข้อมูลที่มีความสำคัญสูง ต้องจัดให้มีความถี่การสำรองมาก และควรจัดให้มีการสำรองข้อมูลภายนอกบริษัท

6.9.8 ต้องทดสอบสภาพพร้อมใช้งานระบบสำรองของระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

6.9.9 ต้องมีมาตรการป้องกันโปรแกรมไม่ประสงค์ดี เช่น

- เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แบบพกพาส่วนบุคคล ก่อนเชื่อมต่อระบบเครือข่ายของบริษัท ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราเซอร์
- ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการและโปรแกรมที่ใช้งาน ที่ได้มีการออก Patch และ/หรือ HotFix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลดจากเว็บไซต์ของเจ้าของ ผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่
- ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอีเมล จะต้องตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ที่ทางบริษัทได้จัดเตรียมไว้ให้ หากต้องการติดตั้งซอฟต์แวร์อื่น นอกเหนือจากที่บริษัทเตรียมไว้ให้ ต้องแจ้งส่วนเทคโนโลยีสารสนเทศเพื่อตรวจสอบความปลอดภัยก่อนการติดตั้ง

<u>6.10 การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)</u>

วัตถุประสงค์

เพื่อป้องกันข้อมูลสารสนเทศในเครือข่ายจากบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศ โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.10.1 การบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย (Network Security Management)

- กำหนดการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย
- ต้องจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับบริษัท

6.10.2 การบริหารจัดการเข้าถึงระบบเครือข่าย

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

เพื่อกำหนดมาตรการในการบริหารจัดการเข้าถึงระบบเครือข่ายของบริษัท เพื่อให้เกิดประสิทธิภาพและมีความมั่นคงปลอดภัย โดยมีแนวทางปฏิบัติดังนี้

6.10.2.1 จัดให้มีการแยกโซนเครือข่ายสื่อสาร โดยมีการจัดแบ่งเครือข่ายอย่างเหมาะสม โดยแยกระบบสารสนเทศที่มีความสำคัญสูงออกจากระบบเครือข่ายที่ใช้ทำงานทั่วไป และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่างๆ มายังระบบที่มีความสำคัญอย่างเข้มงวด6.10.2.2 ก่อนเข้าถึงระบบเครือข่ายและบริการเครือข่ายจะต้องพิสูจน์ตัวตนก่อนทุกครั้ง

6.10.2.3 การอนุญาตให้เข้าถึงบริการเครือข่ายด้วยวิธีการรีโมท จะต้องดำเนินการผ่าน Protocol ที่มีความปลอดภัย

6.10.2.4 การอนุญาตให้เข้าถึงระบบเครือข่ายด้วยวิธีการรีโมทจะต้องอยู่ในโซน หรืออุปกรณ์ที่ได้รับอนุญาตเท่านั้น

6.10.2.5 จำกัดเวลารีโมท (Session) โดยให้ตัดการเชื่อมต่อทุก 15 นาที เมื่อไม่มีการใช้งาน

6.10.2.6 ต้องมีการควบคุมและจำกัดสิทธิการเข้าถึงระบบเครือข่าย และระบบสารสนเทศระยะไกล โดยมีการควบคุมความปลอดภัยต่อระบบเครือข่ายจากภายนอก และต้องได้รับการอนุมัติให้มีการเข้าถึงอย่างเหมาะสม

6.10.3 การถ่ายโอนข้อมูล (Information Transfer)

- ต้องดำเนินการจัดทำข้อตกลงสำหรับการถ่ายโอนข้อมูล (Agreements on Information Transfer) โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุมการ ปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

- ต้องมีการลงนามในสัญญาระหว่างบริษัทและหน่วยงานภายนอกว่าจะไม่เปิดเผย ความลับของบริษัท (Non-Disclosure Agreement: NDA)

- ในกรณี ที่มีการถ่ายโอนข้อมูลสารสนเทศที่เป็นข้อมูลส่วนบุคคลจากบริษัทไปยังหน่วยงาน หรือบุคคลภายนอก จะต้องมีการลงนามในสัญญาประมวลผลข้อมูลส่วนบุคคล (Personal data processing agreement) ระหว่างบริษัทและหน่วยงานหรือบุคคลภายนอก ซึ่งการหนดให้หน่วยงานหรือบุคคลภายนอกต้องทำการเฉพาะตามคำสั่งของบริษัทและมีหน้าที่รักษาความปลอดภัยของข้อมูลส่วนบุคคลด้วย

6.11 การใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

วัตถุประสงค์

เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศของบริษัท โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.11.1 บริษัทมีนโยบายให้ผู้ใช้งาน ใช้อุปกรณ์พกพาเฉพาะที่เป็นของบริษัทในการเข้าถึงหรือจัดเก็บ ข้อมูลและสารสนเทศของบริษัทเท่านั้น หากมีความจำเป็นต้องใช้อุปกรณ์พกพาส่วนตัวในการเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของ

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

บริษัท บริษัทอนุญาตให้ใช้ได้ไม่เกิน 1 เครื่อง หากจำเป็นต้องใช้ มากกว่าที่กำหนดต้องได้ รับการอนุมัติจากผู้จัดการ/ฝ่ายเทคโนโลยีสารสนเทศ

6.11.2 อุปกรณ์พกพาส่วนตัวที่ผู้ใช้งานนำมาเข้าถึงหรือจัดเก็บข้อมูลและสารสนเทศของบริษัท จะต้องเป็นอุปกรณ์พกพาที่ไม่ปรับแต่งให้มีการละเมิดความปลอดภัย เช่น “Jail breaking” หรือ “Rooting” ไม่ติดตั้ง Software ที่ละเมิดลิขสิทธิ์ รวมทั้งต้องกำหนดค่ารหัสผ่านและ เข้ารหัสข้อมูลหรืออุปกรณ์พกพาตามนโยบายที่ส่วนงานเทคโนโลยีสารสนเทศกำหนด

6.11.3 บริษัทขอสงวนสิทธิ์ในการตรวจสอบ ระงับเพิกถอนการใช้งาน และลบข้อมูลทั้งหมด (Wipe) บนอุปกรณ์พกพาทั้งที่เป็นของบริษัทและของส่วนตัวบุคคล ที่ใช้ในการเข้าถึงหรือจัดเก็บ ข้อมูลและสารสนเทศของบริษัท หากเห็นว่าการใช้งานมีความเสี่ยงต่อโครงสร้างพื้นฐานหรือข้อมูลและสารสนเทศของบริษัท

6.12 การควบคุมการนำคอมพิวเตอร์ออกนอกบริษัท

วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และ อุปกรณ์คอมพิวเตอร์ของบริษัทรวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัท โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.12.1 ให้มีการขออนุมัติจากผู้จัดการขึ้นไป หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ และผู้จัดการ/หัวหน้าแผนกเทคโนโลยีสารสนเทศในกรณีที่ต้องการนำทรัพย์สิน สารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึกข้อมูลข้อมูลอุปกรณ์คอมพิวเตอร์ต่าง ๆ ออกนอกบริษัท ทุกครั้ง

6.12.2 บริษัทมีมาตรการรักษาความปลอดภัยข้อมูลและข้อมูลสำคัญ ซึ่งรวมถึงข้อมูลส่วนบุคคล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัทเช่น ส่งซ่อม โดยมาตรการรักษาความปลอดภัยดังกล่าวรวมถึงการทำลายหรือทำให้ข้อมูลส่วนบุคคลที่เก็บอยู่ในสื่อบันทึก อยู่ในรูปแบบที่ไม่สามารถระบุตัวตนบุคคลได้

6.12.3 การเคลื่อนย้ายเครื่องหรืออุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของออกนอกบริษัท รวมทั้งต้องปฏิบัติตามข้อกำหนดหรือระเบียบหรือแนวปฏิบัติเกี่ยวกบการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มบริษัท

6.13 การจัดหา พัฒนา และการดูแลรักษาระบบสารสนเทศ (System Acquisition, Development and Maintenance)

วัตถุประสงค์

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศมีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

Integrity Risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอจนถึงการนำระบบงานที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.13.1 ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบ และขั้นตอนในการโอนย้ายระบบงาน

6.13.2 ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

6.13.3 ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน

6.13.4 การร้องขอ

- การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำให้เป็นลายลักษณ์อักษร โดยอาจเป็น Electronic Transaction เช่น อีเมล เป็นต้น และได้รับอนุมัติ จากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หรือผู้รับผิดชอบระบบสารสนเทศ เป็นต้น
- ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้าน การปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน(Functionality) ของระบบงานที่เกี่ยวข้อง
- ควรสอบทานกฎเกณฑ์ของทางการที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลงในหลาย กรณี อาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทางการ

6.13.5 การปฏิบัติงานพัฒนาระบบงาน

- ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และควบคุมให้มีการเข้าถึงเฉพาะผู้ที่ เกี่ยวข้องในแต่ละส่วน เท่านั้น ทั้งนี้ การแบ่งแยกส่วนดังกล่าวอาจแบ่งโดยใช้เครื่อง คอมพิวเตอร์ คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ภายในเครื่องคอมพิวเตอร์เดียวกัน ก็ได้
- ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้อง ควรมีส่วนร่วมในกระบวนการพัฒนาหรือแก้ไข เปลี่ยนแปลง เพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ
- ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการแก้ไขเปลี่ยนแปลง

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.13.6 การทดสอบ

- ผู้ที่ร้องขอและส่วนเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการ ทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมี การทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตาม ความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

6.13.7 การโอนย้ายระบบงานเพื่อใช้งานจริง

- ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

6.13.8 การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ Version ของระบบงานที่ได้รับการพัฒนา

- ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงที่ผ่านมา

- ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้ทันสมัย อยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิ์ใช้งาน และขั้นตอนการทำงานของโปรแกรม และ Program Specification เป็นต้น และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน

- ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

6.13.9 การทดสอบหลังการใช้งาน (Post-Implementation Test)

- ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้อง ครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

6.13.10 การสื่อสารการเปลี่ยนแปลง

- ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

6.14 การใช้บริการระบบสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)

วัตถุประสงค์

เพื่อกำหนดแนวทางการจัดหาผู้ให้บริการภายนอกสำหรับงานด้านเทคโนโลยีสารสนเทศ โดยต้องพิจารณาให้มีความสอดคล้องกับกลยุทธ์ของบริษัท โดยจะต้องคำนึงถึงการให้บริการอย่างต่อเนื่องและมีความถูกต้องน่าเชื่อถือ มีการตรวจสอบความพร้อมและพิจารณาความเหมาะสมของผู้ให้บริการภายนอก และเพื่อเป็นการป้องกันสินทรัพย์ของบริษัทที่มีการเข้าถึงโดย IT Outsourcing และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ โดยมีหลักเกณฑ์และแนวทางปฏิบัติดังต่อไปนี้

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.14.1 ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัท เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท โดยสอดคล้องกับข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูลของบริษัท

6.14.2 ต้องสื่อสาร และบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัท เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้โดยในข้อตกลงการให้บริการ ต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการภายนอกอย่างสม่ำเสมอ

6.14.3 หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญ จะต้องทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

6.14.4 ด้านแนวทางในการพิจารณาคัดเลือกผู้ให้บริการ ประเมินถึงความน่าเชื่อถือของการให้บริการเพื่อให้แน่ใจว่าผู้ให้บริการมีความสามารถในการให้บริการได้ตามข้อตกลงการให้บริการ

6.14.5 ศักยภาพและความสามารถในการให้บริการทั้งในภาวะปกติและไม่ปกติ

6.14.6 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและรักษาความลับข้อมูล โดยต้องมั่นใจได้ว่าผู้ให้บริการภายนอกมีกระบวนการ ขั้นตอนในการประเมินและการควบคุมความเสี่ยงอย่างน้อย 3 ข้อ คือ 1.การรักษาความลับ (Confidentiality) 2.ความถูกต้องเชื่อถือได้ (Integrity) 3.ความพร้อมใช้งาน (Availability)

6.14.7 ติดตาม ประเมินผล และตรวจสอบการให้บริการจากบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้

6.14.8 กำหนดให้มีการบริหารความเสี่ยงจากการใช้บริการบุคคลภายนอก ในความเสี่ยงด้านต่างๆดังต่อไปนี้

- ความเสี่ยงดานกลยุทธ์ (Strategic Risk)
- ความเสี่ยงด้านปฏิบัติการ (Operational Risk)
- ความเสี่ยงด้านชื่อเสียง (Reputational Risk)
- ความเสี่ยงด้านกฎหมาย (Legal Risk)

6.15 การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

วัตถุประสงค์

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ และจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศให้ได้รับทราบ และเพื่อเป็นการป้องกันการหยุดชะงักในการดำเนินงานของบริษัท อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของบริษัท โดยมีแนวทางปฏิบัติดังต่อไปนี้

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.15.1 ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท

6.15.2 ต้องกำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน

6.15.3 หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศต้องแจ้งเหตุการณ์ดังกล่าวต่อฝ่ายเทคโนโลยีสารสนเทศ

6.15.4 บริษัทจัดให้มีอุปกรณ์คอมพิวเตอร์สำรอง และระบบสารสนเทศสำรองเพื่อรองรับการทำงานได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลให้การดำเนินธุรกิจหยุดชะงัก

6.15.5. จัดให้มีการประเมินความเสี่ยงและบันทึกความเสี่ยงที่อาจส่งผลให้การให้บริการระบบสารสนเทศขาดความต่อเนื่อง และทำเงื่อนไขความต้องการ โดยจะต้องได้รับการประเมินและอนุมัติจากผู้บริหารอย่างเป็นลายลักษณ์อักษร เช่น

- ระยะเวลาเป้าหมายที่บริษัทยอมรับได้ในการกู้คืนระบบให้กลับสู่สภาวะปกติ ในกรณีเกิดเหตุฉุกเฉิน (RTO : Recovery Time Objective)

- ปริมาณข้อมูลสูญหายที่องค์กรยอมรับได้ในช่วงเวลาหนึ่ง (RPO : Recovery Point Objective)

- ระยะเวลาสูงสุดที่บริษัทยอมรับได้ในการกู้คืนระบบ เมื่อเกิดเหตุขัดข้อง โดยหากพ้นระยะนี้ แล้วจะมีผลต่อการดำเนินงานในระดับสูงสุด (MTPoD : Maximum Time Period of Disruption)

6.15.6 กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใชงานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว

6.15.7 ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อที่จะได้เรียนรู้และเตรียมการป้องกัน

6.15.8 ต้องมีการประเมินความเสี่ยง ตรวจสอบ และแจ้งเหตุการณ์ภัยคุกคามหรือความเสี่ยงอัน อาจส่งผลกระทบต่อข้อมูลส่วนบุคคลที่เกี่ยวข้องกับระบบสารสนเทศของบริษัทตามลำดับขั้นและจัดทำรายงานผลกระทบ รวมทั้งแจ้งรายงานตามเงื่อนไขของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

6.15.9 ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

6.15.10 ส่วนเทคโนโลยีสารสนเทศ ต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ ตามแผนบริหารภาวะวิกฤต (Crisis Management Plan) ของบริษัท

6.15.11 ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้น อย่างน้อย ปีละ 1 ครั้ง

6.15.12 ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

6.15.13 ต้องมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรอง อย่างน้อย ปีละ 1 ครั้ง

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.16 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษ ของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน (Compliance)

6.16.1 การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

วัตถุประสงค์

เพื่อให้การดำเนินงานต่างๆ ของบริษัทเป็นไปตามกฎหมาย ข้อตกลง สัญญา และข้อกำหนดด้านความมั่นคงปลอดภัยต่างๆ ที่บริษัทและพนักงานต้องปฏิบัติตาม รวมถึงให้มีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับ รวมทั้งสัญญาต่าง ๆ โดยมีแนวทางปฏิบัติดังต่อไปนี้

6.16.1.1 การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

6.16.1.1.1 ผู้ใช้งานทุกคนมีหน้าที่ต้องทำความเข้าใจ และปฏิบัติตามนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด ทั้งนี้รวมถึงแต่ไม่จำกัดเฉพาะ

- นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ 2550
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์
- พ.ร.บ. ลิขสิทธิ์
- พ.ร.บ. เครื่องหมายการค้า

6.16.1.1.2 ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบสารสนเทศของบริษัท ถือเป็นทรัพย์สินของบริษัท ยกเว้นข้อมูลที่เป็นทรัพย์สินของลูกค้าหรือบุคคลภายนอก ซอฟต์แวร์หรือวัสดุอื่นๆ ที่ ได้รับการคุ้มครองโดยสิทธิบัตรหรือลิขสิทธิ์ของบุคคลภายนอก

6.16.1.1.3 ต้องกำหนดให้มีการป้องกันข้อมูล ที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและแนวปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ รวมถึงต้องมีมาตรการป้องกันข้อมูลส่วนตัวตามที่ระบุไว้ในกฎหมาย แนวปฏิบัติและสัญญาที่เกี่ยวข้อง

6.16.1.1.4 ต้องกำหนดให้มีการป้องกัน สารสนเทศ ระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย และคอมพิวเตอร์แม่ข่าย ไม่ให้ใช้งานไปในทางที่ผิดหรือโดยไม่มีสิทธิ์และต้องกำหนดให้ใช้มาตรการเข้ารหัสข้อมูลโดยให้ยึดถือตามหรือสอดคล้องกับข้อตกลงทางกฎหมาย

6.16.1.1.5 การทบทวน ตรวจสอบการใช้งานระบบทุกระบบเป็นสิทธิ์ที่บริษัทสามารถกระทำได้หาก บริษัทเห็นว่าจำเป็น โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่

6.16.1.1.6 ต้องมีการตรวจสอบระบบว่ามีความมั่นคงปลอดภัยเพียงพอหรือไม่โดยใช้ซอฟต์แวร์ค้นหา ช่องโหว่และทดสอบการโจมตีระบบเพื่อตรวจข้อบกพร่องของระบบด้วย

6.16.1.1.7 ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ เพื่อให้มี ผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ และต้องมีการป้องกันซอฟต์แวร์ที่ใช้ในการ ตรวจสอบระบบ ไม่ให้มีการนำซอฟต์แวร์ไปใช้ในทางที่ผิด โดยกำหนดให้มีการแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบระบบสารสนเทศ

6.16.2 วิธีการปฏิบัติให้เป็นไปตามนโยบายฝ่ายเทคโนโลยีสารสนเทศ ได้จัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยอ้างอิง เพื่อให้เกิดความมั่นคงปลอดภัยแก่สารสนเทศ

6.16.3 บทลงโทษ

ผู้ใช้งานคนใดที่ฝ่าฝืนนโยบายฉบับนี้ บริษัทพิจารณาลงโทษทางวินัยตามระเบียบบริหารงานบุคคลรวมทั้งอาจมีความรับผิดทั้งทางอาญาและทางแพ่ง

6.16.4 การทบทวนนโยบาย

ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำ อย่างน้อยปีละ 1 ครั้งและต้องเสนอให้ประธานเจ้าหน้าที่บริหารอนุมัติหากมีการเปลี่ยนแปลง

7. ประวัติการแก้ไข

Revision No.	Approved date	สาเหตุการแก้ไข
0	14 กันยายน 2565	ออกเอกสารใหม่
01	*12 มิถุนายน 2566*	*แปรสภาพ จาก บริษัท เพชรศรีวิชัย เอ็นเตอร์ไพรส์ จำกัดเป็นบริษัท เพชรศรีวิชัย เอ็นเตอร์ไพรส์ จำกัด (มหาชน)*

(.....)

(นายประกิต ประสิทธิ์ศุภผล)

ประธานเจ้าหน้าที่บริหาร/กรรมการผู้จัดการใหญ่