วัตถุประสงค์

1. เพื่อให้การดำเนินงานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทมีความมั่นคงปลอดภัยสามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพอันจะทำให้การดำเนินธุรกรรมมีความถูกต้องเชื่อถือได้ตามมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์
2. เพื่อกำหนดแนวทางปฏิบัติให้ผู้บริหาร ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ใช้งานระบบ ตระหนักถึงความสำคัญของการรักษา ความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
3. เพื่อป้องกันเจ้าหน้าที่ผู้ใช้งานและผู้เกี่ยวข้องไม่ให้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
4. เพื่อกำหนดมาตรฐาน แนวทางและวิธีปฏิบัติ ให้ผู้บริหาร ผู้ใช้ ผู้ดูแลระบบ และหน่วยงานภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

บริษัทได้เล็งเห็นถึงความสำคัญของการบริหารความเสี่ยงทั้งจากมุมมองของ Holding Company และจากธุรกิจผลิตและจำหน่ายไฟฟ้า ซึ่งกระบวนการบริหารความเสี่ยงเป็นองค์ประกอบที่สำคัญที่ช่วยให้บริษัทสามารถเตรียมพร้อมและตอบสนองต่อการเปลี่ยนแปลงของสภาพธุรกิจได้อย่างเหมาะสมและทันเวลา รวมถึงรองรับโอกาสในการเติบโตทางธุรกิจอย่างยั่งยืน

ขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ บริษัท ซีเค เพาเวอร์ จำกัด (มหาชน) เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ

คำนิยาม

"บริษัท" หมายถึง บริษัท ซีเค เพาเวอร์ จำกัด (มหาชน)

"ผู้ใช้งาน" หมายถึง บุคคลที่ได้รับอนุญาต ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

"ผู้ดูแลระบบ" หมายถึง ผู้อำนวยการแผนกเทคโนโลยีสารสนเทศ หรือผู้ได้รับมอบหมายให้ควบคุมดูแลบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

"เจ้าหน้าที่" หมายถึง บุคลากรในสังกัดบริษัท และรวมถึงบุคคลภายนอกซึ่งได้รับอนุญาตให้เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

"สิทธิของผู้ใช้งาน" หมายถึง อำนาจอันชอบธรรมที่ผู้ใช้งานได้รับมอบหมายในการเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

"สินทรัพย์" หมายถึง ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การควบคุมและจำกัดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ที่เกี่ยวกับการให้บริการและข้อมูลตามความจำเป็นในการใช้งาน มีการป้องกันการลักลอบการเข้าถึงระบบโดยผู้ที่ไม่มีสิทธิทั้งจากภายในและภายนอกบริษัท

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การคงไว้ซึ่งความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งานของข้อมูลในระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท

"เหตุการณ์ด้านความมั่นคงปลอดภัย" (Security incidents) หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบเทคโนโลยี สารสนเทศ และการสื่อสารของบริษัทหรือเหตุการณ์ที่สงสัยว่า จะเป็นจุดอ่อนหรือสร้างความเสียหาย ได้ในที่สุด ซึ่งส่งผลให้เป็นการละเมิดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท เช่น การอนุญาตให้ผู้อื่นเข้าใช้งานระบบ การไม่กำหนดรหัสผ่านในการเข้าใช้งานระบบการเปิดเผยเอกสารสำคัญให้บุคคลภายนอกล่วงรู้ โปรแกรมไม่พึงประสงค์ ระบบถูกบุกรุกทางเครือข่าย หรือการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายถึง สถานการณ์ที่ผู้ดูแลระบบไม่ต้องการให้เกิดขึ้นหรือสร้างความเสียหายกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท โดยผู้ดูแลระบบไม่ได้คาดการณ์ไว้ว่าจะเกิดขึ้น เช่นโปรแกรมไม่พึงประสงค์ โปรแกรมทำงานผิดพลาดหรือไม่ถูกต้อง ระบบถูกบุกรุกทางเครือข่าย ข้อมูลสำคัญถูกเปลี่ยนแปลงหรือสูญหาย หน้าเว็บไซต์

ถูกเปลี่ยนแปลง การเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต ระบบถูกโจมตีจนไม่สามารถให้บริการได้ การหยุดชะงักของระบบคอมพิวเตอร์และเครือข่าย หรือเหตุการณ์อื่น ๆ ที่เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของบริษัท

“แผนกเทคโนโลยีสารสนเทศ” หมายถึง หน่วยงานที่ดำเนินการเกี่ยวกับระบบสารสนเทศและระบบงานคอมพิวเตอร์และเป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศของบริษัท โดยมีหน้าที่ศึกษาวิเคราะห์เพื่อพัฒนาระบบสารสนเทศและระบบงานคอมพิวเตอร์ของบริษัท และปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่ายสื่อสาร” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการเชื่อมโยง หรือการส่งข้อมูลสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัท ซึ่งการเชื่อมโยงเป็นได้ทั้งในรูปแบบใช้สายและแบบไร้สาย โดยระบบเครือข่ายสื่อสาร ได้แก่ ระบบเครือข่ายระยะใกล้ (Local Area Network: LAN) ระบบเครือข่ายระยะไกล (Wide Area Network: WAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet)

“ระบบอินทราเน็ต” หมายถึง ระบบเครือข่ายสื่อสารภายในที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในบริษัท

“ระบบอินเทอร์เน็ต” หมายถึง ระบบเครือข่ายสื่อสารที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ของบริษัทเข้ากับระบบเครือข่ายสื่อสารอินเทอร์เน็ตทั่วโลก

“สารสนเทศ” หมายถึง ข้อมูลที่ผ่านการประมวลผล การจัดระเบียบ ซึ่งอาจอยู่ในรูปของตัวเลขข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และนำไปใช้ประโยชน์ในการบริหารการวางแผน การตัดสินใจ และอื่น ๆ

“ระบบเทคโนโลยีสารสนเทศและการสื่อสาร” หมายถึง ระบบงานของบริษัทที่ประกอบด้วยระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร เจ้าหน้าที่ผู้ใช้ระบบ เจ้าหน้าที่ผู้พัฒนาระบบ เจ้าหน้าที่ผู้จัดการดูแลระบบ และผู้บริหารของบริษัท นำมาทำงานร่วมกันเพื่อกำหนดวัตถุประสงค์ รวบรวมจัดเก็บข้อมูล ประมวลผลข้อมูล และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้ระบบและผู้บริหารของบริษัทสามารถนำมาใช้ประโยชน์ในการวางแผนเพื่อช่วยสนับสนุนการปฏิบัติงาน การตัดสินใจ การบริหาร การวิเคราะห์และติดตามผลการดำเนินงานของหน่วยงานระดับต่าง ๆ ของบริษัท

“รหัสผ่าน (Password)” หมายถึงตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศและการสื่อสาร

“การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การดำเนินการรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท ประกอบด้วยคุณสมบัติพื้นฐาน 3 ประการ ดังนี้

1. การรักษาความลับ (Confidentiality) คือ การเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้
2. บูรณภาพ (Integrity) คือ การรับรองว่าข้อมูลจะไม่ถูกกระทำการใด ๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม
3. ความพร้อมใช้งาน (Availability) คือ การรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศและการสื่อสารทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

“วิธีการปฏิบัติ” หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวปฏิบัติ” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

“ชุดคำสั่งไม่พึงประสงค์” (Malware) หมายถึง ชุดคำสั่งที่มีผลทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

“จดหมายอิเล็กทรอนิกส์ (e-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายสื่อสารที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่ายภาพ

กราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ เช่น SMTP, POP3 หรือ IMAP

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศบริษัท

1 การรักษาความมั่นคงปลอดภัยของการเข้าถึงและการควบคุมการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร

1.1 การควบคุมการเข้าถึงสิทธิของผู้ใช้งาน

- มีการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบ โดยพิจารณาจากหน้าที่ความรับผิดชอบในข้อมูลของผู้ใช้งานแต่ละกลุ่มงาน
- ผู้ใช้งานต้องทำคำใช้สิทธิเป็นลายลักษณ์อักษรหรือผ่านทางระบบ “IT service request” ให้กับแผนกเทคโนโลยีสารสนเทศ
- ผู้อำนวยการแผนกเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายเป็นผู้พิจารณาอนุญาต

1.2 การบริหารการจัดการสิทธิผู้ใช้งาน

- ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ได้กำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารนั้นๆ ให้เหมาะสมกับการเข้าใช้บริหารของผู้ใช้งาน และหน้าที่ความรับผิดชอบของผู้ใช้งานเป็นไปตามระเบียบที่บริษัทกำหนด รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานเมื่อผู้ใช้มีการย้าย/เปลี่ยนตำแหน่งงานใหม่ หรือลาออก หรือเกษียณ ภายในบริษัทอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง
- ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- เมื่อมีเจ้าหน้าที่เข้าปฏิบัติงานใหม่ แผนกทรัพยากรบุคคล/ หน่วยงานต้นสังกัดต้องทำคำขอใช้สิทธิเป็นลายลักษณ์อักษรหรือผ่านระบบ “IT Service Request” แจ้งแผนกเทคโนโลยีสารสนเทศทันที เพื่อสร้างบัญชีและกำหนดสิทธิ์ผู้ใช้งานตามที่ร้องขอ
- เมื่อเจ้าหน้าที่ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน แผนกทรัพยากรบุคคล/ หน่วยงานต้นสังกัดต้องทำคำขอยกเลิกใช้สิทธิเป็นลายลักษณ์อักษรหรือผ่านระบบ “IT Service Request” แจ้งแผนกเทคโนโลยีสารสนเทศทันที เพื่อ

ถอดถอนสิทธิของผู้ที่ลาออกหรือเปลี่ยนสิทธิในระบบหรือปิดใช้งานบัญชีผู้ใช้ดังกล่าวเป็นการชั่วคราว จากนั้นจะดำเนินการลบข้อมูลทั้งหมดของเจ้าหน้าที่ดังกล่าวออกภายใน 7 วัน หลังจากวันที่ได้รับแจ้ง

- ห้ามผู้ใช้งานซึ่งไม่ได้รับสิทธิให้เข้าใช้งานบุกรุกเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ไม่ว่าด้วยวิธีการใดๆ

1.3 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

- ผู้ดูแลระบบมีการกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ และระบบต้องไม่แสดงรหัสผ่านให้เห็นบนหน้าจอ
- ระบบต้องกำหนดให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเมื่อเข้าระบบครั้งแรก
- ระบบมีการกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน 6 ครั้ง (ระบบบัญชีและการเงิน)
- ผู้ดูแลระบบการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยพิจารณาจาก ลำดับชั้นความลับของข้อมูล หรือความสำคัญตามภารกิจ โดยกำหนดให้ระบบมีการบันทึกประวัติการเปลี่ยนรหัสผ่าน เพื่อป้องกันการใช้รหัสซ้ำเช่น ระบบงานด้านการเงินและบัญชีต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 90 วัน
- การแจ้งปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ผู้ใช้งานติดต่อผู้ดูแล ระบบ เช่น ลืมชื่อผู้ใช้งานหรือรหัสผ่าน โดยแจ้งเป็นลายลักษณ์อักษรหรือผ่านระบบ “IT Service Request”
- การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย และส่งไปยังผู้ใช้งานพร้อม “แนวปฏิบัติสำหรับการใช้งานรหัสผ่าน” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามแนวปฏิบัติโดยเคร่งครัด

1.4 การใช้งานรหัสผ่านสำหรับผู้ใช้งาน

- ผู้ใช้ต้องใช้ชื่อผู้ใช้งาน และรหัสผ่านของตนเองในการใช้งานระบบ เพื่อป้องกัน การปฏิเสธความรับผิดชอบ
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ต้องเปลี่ยนรหัสผ่าน ที่ได้รับโดยทันที

- ผู้ใช้งานต้องกำหนดรหัสผ่าน และเปลี่ยนรหัสผ่านของตนเองในการใช้งานอย่างสม่ำเสมออย่างน้อยทุก ๆ 90 วัน หรือตามหลักเกณฑ์ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ และระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใด ๆ ทั้งสิ้น เว้นแต่กรณีผู้ใช้งานที่มีอำนาจอนุมัติใด ๆ ในระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถปฏิบัติหน้าที่อันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าว เพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้ว ให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที
- กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
- ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “12345”
- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่นชื่อสกุล วัน เดือน ปีเกิด ที่อยู่
- ไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
- ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์
- ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- ผู้ใช้งานต้องไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงาน และในกรณีใช้งานส่วนตัว
- ผู้ใช้งานต้องออกจากระบบ (Log off) ทันที เมื่อไม่ใช้งาน เพื่อป้องกันผู้ใช้งานอื่นลักลอบใช้สิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารและ
- ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหากสงสัยว่ารหัสผ่านเกิดการรั่วไหล

1.5 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

- ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงาน

- เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่เหมาะสมกับหน้าที่และความรับผิดชอบ
- ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติ และกำหนดสิทธิในการผ่าน เข้าสู่ระบบให้แก่ผู้ใช้งาน ในการขออนุญาตเข้าระบบงานนั้น ต้องทำบันทึกและกรอกแบบข้อมูลคำขอลงในฟอร์ม “IT service request”ตามที่แผนกเทคโนโลยีสารสนเทศกำหนด และให้มีการลงนามอนุมัติเอกสารดังกล่าวโดยผู้มีอำนาจที่เป็นเจ้าของข้อมูลและ/หรือเจ้าของระบบงาน เพื่อเก็บไว้เป็นหลักฐาน
- การลงทะเบียนเจ้าหน้าที่ กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ หรือเมื่อย้าย/เปลี่ยนตำแหน่งงานใหม่/ลาออก/เกษียณ ภายในบริษัท หน่วยงาน/ผู้ใช้งานต้องทำบันทึก และกรอกแบบฟอร์ม“IT service request”ตามที่แผนกเทคโนโลยีสารสนเทศกำหนด เพื่อให้มีสิทธิหรือยกเลิกสิทธิต่าง ๆ ในการใช้งาน
- ผู้ใช้งานรายใหม่หรือส่วนงานต้นสังกัด ต้องทำการกรอกข้อมูลเพื่อขอลงทะเบียนในแบบ “IT service request” และได้รับอนุมัติจะหัวหน้าส่วนงานต้นสังกัด จากนั้นส่งคำขอให้แผนกเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบจะกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เหมาะสมกับการใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งาน โดยได้รับความเห็นชอบจากผู้มีอำนาจเป็นลายลักษณ์อักษร และจะมีการทบทวนสิทธิอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง หรือในกรณีที่มีคำสั่งย้าย/เปลี่ยนตำแหน่งงานใหม่/ลาออก/เกษียณ หรือในกรณีที่หน่วยงานต้นสังกัด มีบันทึกถึงผู้อำนวยการแผนกเทคโนโลยีสารสนเทศ หรือผู้ได้รับมอบหมาย เพื่อให้มีสิทธิหรือยกเลิกสิทธิต่าง ๆ ในการใช้งาน

1.6 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

- ดูแลระบบ มีการกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ รวมทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
- เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

- วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบมีการกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล
- การรับส่งข้อมูลระดับชั้นความลับ ตั้งแต่ชั้น “ลับ” ขึ้นไปผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN , HTTPS
- มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของแผนกงาน หรือกรณีส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมเจ้าของข้อมูลต้องสำรองข้อมูลไว้ในสื่อบันทึกข้อมูล และลบข้อมูลสำคัญที่เก็บอยู่ในเครื่องคอมพิวเตอร์ออกก่อน

1.7 การควบคุมการเข้าถึงระบบเครือข่ายสื่อสาร

เป็นการควบคุมบุคคลที่เข้าสู่ระบบเครือข่ายสื่อสาร รวมถึงการควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ และให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น โดยผู้ดูแลระบบจะต้องทำการออกแบบระบบเครือข่ายสื่อสารตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ ได้แก่ Internal Zone, External Zone และ DMZ Zone เป็นต้น จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย ดังนี้

- ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาต ให้เข้าถึงเท่านั้น
- ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายสื่อสาร จะต้องขอใช้งานกับผู้ดูแลระบบ โดยกรอกข้อมูลลงในระบบ “IT service request” และต้องได้รับ พิจารณาอนุญาตจากผู้อำนวยการแผนกเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษร
- ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบ เครือข่ายสื่อสารให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างน้อยปีละ 1 ครั้ง
- ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายสื่อสารจากแบบคำขอขึ้นทะเบียนอุปกรณ์คอมพิวเตอร์และเครือข่ายสื่อสาร โดยกรอกข้อมูลลงในระบบ “IT service request”

- ผู้ดูแลระบบ จัดให้มีซอฟท์แวร์สำหรับบริหารจัดการและควบคุมระบบเครือข่าย (Network Management System) ซึ่งสามารถระบุอุปกรณ์บนเครือข่าย (Equipment Identification) ถึงระดับ IP address, Computer name, MAC address
- มีการจัดทำผังการเชื่อมโยงเครือข่าย และมีการปรับปรุงให้เป็นปัจจุบันเสมอ
- มีการจัดแบ่งแยกส่วนเครือข่ายสื่อสาร /กลุ่ม เพื่อป้องกันและควบคุมการเข้าถึงได้แก่ ส่วนที่เป็นสาธารณะ ส่วนที่เชื่อมต่อภายใน ส่วนที่เกี่ยวข้องกับสินทรัพย์สำคัญหรือที่เป็นอันตรายกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ
- มีการใช้ VLAN ในแต่ละส่วนเครือข่ายสื่อสาร /กลุ่ม เช่น กลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ
- มีการติดตั้งอุปกรณ์ Gateway กั้นไว้ระหว่างเครือข่ายสื่อสาร เพื่อเป็นตัวควบคุมข้อมูลที่สื่อสารกันระหว่างเครือข่ายสื่อสาร
- อุปกรณ์ในเครือข่ายสื่อสารมีการปรับแต่งให้สามารถควบคุมหรือกรองข้อมูลที่สื่อสารกันระหว่างเครือข่าย
- มีการควบคุมและป้องกันให้ปลอดภัย เช่น การใช้การตรวจสอบตัวตน การเข้ารหัสผ่านการเลือกกำหนดความถี่ช่องสัญญาณเอง
- มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- มีการตรวจสอบการทำงานของระบบเครือข่ายสื่อสารและอุปกรณ์เครือข่าย สื่อสารอย่างสม่ำเสมอเป็นประจำทุกวัน
- มีการตั้งค่า และการปรับแต่งค่า (Configuration) ที่ถูกต้องเหมาะสม และ เป็นปัจจุบัน
- มีการเฝ้าระวังระบบเครือข่ายสื่อสาร
- มีการสำรองข้อมูลการตั้งค่าของอุปกรณ์เครือข่ายสื่อสาร
- มีการ Update patch หรือ Release ของซอฟต์แวร์ระบบหรือ Firmware
- มีการตรวจสอบช่องโหว่ของอุปกรณ์และเครื่องคอมพิวเตอร์แม่ข่าย ที่ให้บริการในระบบเครือข่ายสื่อสารของบริษัท
- มีการทดสอบการบุกรุกเครือข่ายสื่อสาร

- มีการควบคุมการเข้าถึงระบบเครือข่ายสื่อสารจากภายใน และการควบคุมการเชื่อมต่อทางเครือข่าย
- การขอติดตั้งจุดเพื่อเชื่อมต่อเข้าเครือข่ายของห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายต้องทำเป็นหนังสือและได้รับอนุญาตจากผู้อำนวยการแผนกเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมาย
- ดูแลและปรับปรุงสิทธิการเข้าถึงและใช้งานเครือข่ายของผู้ใช้งานอยู่เสมอ
- มีอุปกรณ์ในการกรองการรับส่งข้อมูล เช่น อีเมล์ การรับส่งแฟ้มข้อมูลการเข้าถึงแบบโต้ตอบหรือการแช็ท การเข้าถึงโปรแกรมประยุกต์
- จำกัดช่วงวันหรือช่วงเวลาในการอนุญาตให้เชื่อมต่อตามความจำเป็น

1.8 การควบคุมการกำหนดเส้นทางบนเครือข่าย

- มีการควบคุมการกำหนดเส้นทางบนเครือข่ายบนอุปกรณ์เครือข่าย ได้แก่ Core switch, Edge Switch, Router เป็นต้น
- มีอุปกรณ์ Gateway ในการตรวจสอบต้นทางและปลายทาง ณ จุดควบคุมที่อยู่ระหว่างเครือข่ายภายใน โดยการใช้ Proxy Server หรือ Network Access Controller (NAC)
- มีการกำหนดโปรโตคอล สิทธิ IP Address ในการเชื่อมโยงเครือข่าย ของอุปกรณ์และผู้ใช้งานเครือข่ายให้เหมาะสม
- มีการกำหนดโปรโตคอล และพอร์ตการใช้งานของแต่ละกลุ่มผู้ใช้งาน เช่น HTTP, FTP, SMTP, TELNET
- มีการกำหนด VLAN เพื่อควบคุมและกำหนดสิทธิการใช้งาน

1.9 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน

- มีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน โดยต้องแสดงตัวตนด้วยชื่อผู้ใช้งาน พิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านในการเข้าสู่เครือข่าย

1.10 การติดตั้งอุปกรณ์ Firewall เพื่อรักษาความปลอดภัยของระบบเครือข่าย

- ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่า ของ Firewall ทั้งหมด

การ เปลี่ยนแปลงค่าต่าง ๆ ของอุปกรณ์ Firewall ในแต่ละครั้ง ได้แก่ ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการกำหนดระบบเครือข่ายสื่อสารต่าง ๆ ให้สามารถเชื่อมต่อกับระบบเครือข่ายสื่อสารของบริษัท โดยได้รับอนุญาตจากผู้อำนวยการแผนกเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมาย

- การกำหนดค่าเริ่มต้นพื้นฐานของทุกระบบเครือข่ายสื่อสาร จะต้อง เป็นการปฏิเสธทั้งหมด
- การเชื่อมต่อระบบอินเทอร์เน็ตและบริการระบบอินเทอร์เน็ตที่ไม่ได้ รับการอนุญาตตามนโยบาย ทุกเส้นทางจะต้องถูกบล็อก (Block) โดย Firewall
- การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น
- ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้อง จัดเก็บไว้ที่อุปกรณ์
- จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่น่าเชื่อถือและมีการเข้ารหัสข้อมูลเพื่อป้องกันการแก้ไขหรือเปลี่ยนแปลง และต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า 90 วัน
- ผู้ดูแลระบบต้องตรวจสอบเหตุการณ์ ข้อมูลจราจรทางคอมพิวเตอร์พฤติกรรมการใช้งานกิจกรรม และบันทึกปริมาณข้อมูลการเข้าใช้งานระบบเครือข่ายเป็นประจำทุกวัน
- การกำหนดการให้บริการระบบอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตใน Firewall สำหรับการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานนอกเหนือจากที่กำหนดไว้จะต้องมีการเปิดพอร์ตให้เป็นกรณีพิเศษต้องทำหนังสือและได้รับอนุญาตจากผู้อำนวยการแผนกเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมายการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละ ส่วนของระบบเครือข่ายสื่อสาร จะต้องกำหนดค่าอนุญาตใน Firewall เฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อ การให้บริการเท่านั้น โดยจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง
- เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานระบบอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนด เป็นกรณีไป
- การสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ Firewall จะต้องสำรองข้อมูลเป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงการกำหนดค่าในอุปกรณ์ Firewall

- ผู้ดูแลระบบมีสิทธิที่จะระงับการใช้งานของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข
- การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกผ่านระบบเครือข่ายสื่อสารมายังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์ระบบเครือข่ายสื่อสารภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบคำขออนุญาตเปิดบริการใน Firewall และจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบก่อน
- ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานระบบอินเทอร์เน็ตหรือการเชื่อมต่อระบบเครือข่ายสื่อสารภายในโดยทันที

1.11 การติดตั้งอุปกรณ์ตรวจจับและป้องกันการบุกรุก (IDS/IPS)

- การติดตั้งระบบ IDS/IPS เพื่อตรวจสอบหรือเฝ้าระวัง หรือมอนิเตอร์เหตุการณ์ต่าง ๆ ที่เกิดขึ้นจากการใช้งานของบุคคลที่เข้าใช้งานระบบคอมพิวเตอร์หรือระบบเครือข่ายสื่อสารของหน่วยงานในลักษณะที่ผิดปกติ เช่นการพยายามที่จะทำลายความลับ (Confidentiality) ความคงสภาพ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล หรือการหลีกเลี่ยงระบบการรักษาความ ปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยการบุกรุกดังกล่าวเกิดจากการที่ผู้บุกรุกเข้าถึง ระบบจากอินเทอร์เน็ต หรือการที่ผู้ใช้ภายในพยายามเข้าถึงหรือกระทำในสิ่งที่ไม่ได้รับอนุญาต หรือการที่ผู้ใช้พยายามใช้สิทธิพิเศษของตนในทางที่ผิด
- การติดตั้งระบบ IDS/IPS ให้ครอบคลุมระบบคอมพิวเตอร์และระบบ เครือข่ายสื่อสารของบริษัททั้งหมด รวมถึงเส้นทางข้อมูลจราจร ทั้งที่เชื่อมต่อสู่ระบบเครือข่ายสื่อสารภายนอกและภายในทุกเส้นทาง
- ระบบคอมพิวเตอร์ทั้งหมดที่สามารถเข้าถึงได้จากระบบเครือข่ายสื่อสาร ภายนอกหรือเครือข่ายอินเทอร์เน็ต จะต้องผ่านการตรวจสอบจากระบบ IDS/IPS
- ข้อมูลจราจรทางคอมพิวเตอร์ที่ผ่านเข้าออกระบบ IDS/IPS จะต้องมีการบันทึกไม่น้อยกว่า 90 วัน
- ผู้ดูแลระบบต้องตรวจสอบ และ Update Patch / Signature ของระบบ IDS /IPS เป็นประจำอย่างน้อยเดือนละ 1 ครั้ง หรือทุกครั้งที่มี Signature เวอร์ชั่นใหม่ให้อัพเดท

- ผู้ดูแลระบบต้องตรวจสอบเหตุการณ์ ข้อมูลจราจรทางคอมพิวเตอร์พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลการเข้าใช้งานระบบเครือข่ายเป็นประจำทุกวัน
- ระบบ IDS/IPS ทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ต้องรายงานให้ผู้บังคับบัญชาทราบตามลำดับชั้นทันทีที่ตรวจพบ
- ผู้ดูแลระบบมีสิทธิในการยุติการเชื่อมต่อระบบเครือข่ายสื่อสารของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า และรายงานให้ผู้บังคับบัญชาทราบ

1.12 การควบคุมการเข้าถึงระบบเครือข่ายสื่อสารจากภายนอก

- การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือคอมพิวเตอร์ระยะไกลจากภายนอก (Remote) ผ่านเครือข่ายสื่อสาร ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดพอร์ตใน Firewall หรืออุปกรณ์สื่อสารที่ใช้ตลอดเวลาโดยไม่จำเป็น และตัดช่องทางการเชื่อมต่อเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารจากภายนอกทันทีเมื่อไม่ได้ใช้งานแล้ว
- วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบคอมพิวเตอร์ระยะไกลจากภายนอก ต้องได้รับการอนุญาตจากผู้อำนวยการแผนกเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายก่อน ตามแบบคำขออนุญาตเปิดบริการใน Firewall และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบอย่างเคร่งครัด
- การให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบคอมพิวเตอร์ระยะไกลจากภายนอก ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการปฏิบัติงาน และต้องได้รับอนุมัติจากผู้อำนวยการแผนกเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย
- การเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบคอมพิวเตอร์ระยะไกลจากภายนอก โดยเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แบบพกพา อุปกรณ์คอมพิวเตอร์

แบบพกพา รวมถึงอุปกรณ์สื่อสารเคลื่อนที่ ต้องมีการควบคุมพอร์ตใน Firewall ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการแบ่งช่องสัญญาณอย่างชัดเจน

- มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก โดยต้องแสดงตัวตนด้วยชื่อผู้ใช้ การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน และการเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบคอมพิวเตอร์จากอินเทอร์เน็ตนั้น จะมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานด้วย
- มีการใช้อุปกรณ์พิเศษเพื่อยืนยันตัวตนอย่างเข้มข้นในการเข้าสู่ระบบสารสนเทศที่เกี่ยวกับข้อมูลที่เป็นชั้นข้อมูลที่ใช้ภายในบริษัท และชั้นข้อมูลตั้งแต่ชั้น “ลับ” แทนการใช้รหัสผ่าน เช่นการใช้อุปกรณ์ Token เมื่อต้องปฏิบัติงานภายนอกองค์กร

1.13 การควบคุมการเข้าถึงระบบเครือข่ายสื่อสารแบบไร้สาย

- ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
- ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและทำการสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่
- ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ชื่อผู้ใช้งานและรหัสผ่าน ที่ถูกกำหนดเป็นค่าตั้งต้นจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน
- ผู้ดูแลระบบต้องกำหนดค่า ในการเข้ารหัสข้อมูลระหว่างอุปกรณ์รับและอุปกรณ์กระจายสัญญาณเพื่อให้ยากต่อการดักจับ และปลอดภัยอย่างน้อยคือWPA (Wi-Fi Protected Access)
- ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุม MAC Address หรือชื่อผู้ใช้และรหัสผ่านของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายสื่อสารแบบไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้ และรหัสผ่านตามที่กำหนดไว้เท่านั้น
- ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างระบบเครือข่ายสื่อสารแบบไร้สาย กับเครือข่ายสื่อสารภายในบริษัท

- ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ / อุปกรณ์ที่อนุญาตให้เชื่อมต่อเครือข่ายสื่อสารแบบไร้สายได้ และบันทึกข้อมูลจราจรทางคอมพิวเตอร์ที่ใช้งานระบบเครือข่ายไร้สายไว้ไม่น้อยกว่า 90 วัน

1.14 การควบคุมการเข้าถึงระบบปฏิบัติการ

เป็นการควบคุมบุคคลเข้าสู่ระบบปฏิบัติการที่อยู่ภายใต้ระบบเครือข่ายสื่อสารของบริษัท เพื่อรักษาความปลอดภัยของข้อมูล และทรัพยากร จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย ดังนี้

- มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานโดยต้องแสดงตัวตนด้วยชื่อผู้ใช้งาน
- การเข้าสู่ระบบปฏิบัติการจะมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานโดยอัตโนมัติจากระบบ Active Directory (AD) หรือ Radius Server

1.15 การติดตั้งโปรแกรมอรรถประโยชน์เพื่อใช้งานร่วมกับระบบปฏิบัติการ

- ต้องไม่ติดตั้งโปรแกรมซอฟแวร์ที่ละเมิดลิขสิทธิ์
- ต้องติดตั้งโปรแกรมตามภารกิจและไม่ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน
- แผนกเทคโนโลยีสารสนเทศ กำหนดมาตรการการควบคุมการหมดเวลาใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Session time-out) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งเพื่อยุติการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารนั้น
- กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร มีการยุติการใช้งานรวมถึงปิดการใช้งานในกรณีที่ไม่มีกิจกรรมการใช้งานภายในช่วงระยะเวลา 3600 วินาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- มีกลไกในการยกเลิกการใช้โปรแกรมประยุกต์ และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติเมื่อไม่มีการใช้งานตามระยะเวลาที่กำหนด

1.16 แผนกเทคโนโลยีสารสนเทศ กำหนดมาตรการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Limitation of connection time) สำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือแอพพลิเคชันที่มีความเสี่ยง หรือมีความสำคัญสูง เพื่อให้มีความมั่นคงปลอดภัย ดังนี้

- กำหนดระยะเวลาในการเชื่อมต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ใช้ในการปฏิบัติงานต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเกินกว่า 3600 วินาที กำหนดให้ระบบยุติการใช้งานของผู้ใช้งาน

1.17 การควบคุมการเข้าถึงระบบเทคโนโลยี โปรแกรมประยุกต์และแอพพลิเคชั่น

เป็นการเข้าสู่ระบบเทคโนโลยีสารสนเทศ โปรแกรมประยุกต์ และแอพพลิเคชั่นของบริษัท เพื่อความปลอดภัยของข้อมูล จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย ดังนี้

- มีการแบ่งแยกสภาพแวดล้อมการใช้งานโดยกำหนดให้ เครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งระบบงานที่สำคัญกำหนดให้อยู่ใน Server Zone ส่วนเครื่องแม่ข่ายระบบงานที่ให้บริการบุคคลทั่วไปซึ่งมีความไวต่อการถูกรบกวนและมีความเสี่ยงสูง จำเป็นต้องเฝ้าระวังเป็นพิเศษ กำหนดให้อยู่ใน Demilitarized Zone (DMZ)
- มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานก่อนเข้าใช้งานระบบ เป็นไปตาม “แนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน” และ “แนวปฏิบัติการบริหารจัดการสิทธิผู้ใช้งาน”
- การป้อนรหัสผ่าน ระบบต้องทำการเข้ารหัสเพื่อป้องกันมิให้ผู้อื่น ทราบรหัสผ่าน
- มีการตัดการใช้งานออกจากระบบอัตโนมัติ เมื่อผู้ใช้งานไม่ตอบสนองเป็นเวลาเกิน 3600 วินาที
- มีการเข้ารหัสข้อมูลที่อยู่ในชั้นความลับในระบบฐานข้อมูล

2 แนวทางปฏิบัติการบริหารจัดการห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

2.1 การจัดการบริเวณพื้นที่โดยรอบ (Physical Security Management)

พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ภายใน (Data Center) มีการแบ่งพื้นที่สำคัญเป็นส่วนๆ ดังนี้

- ส่วนเครื่องแม่ข่ายและอุปกรณ์ระบบเครือข่าย
- ส่วนระบบปรับอากาศ

2.2 การควบคุมการเข้า-ออก (Physical entry controls) ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

- มีขั้นตอนการขออนุญาต การกำหนดสิทธิ และควบคุมการเข้าห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

- มีระบบการบันทึกวันและเวลาการเข้า-ออกพื้นที่โดยอัตโนมัติ เกี่ยวกับตัวบุคคลและเวลาที่ผ่าน เข้า-ออก เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น
- มีการควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์และเครือข่ายด้วยการใช้บัตรประจำตัวหรือลายนิ้วมือ หรือใช้บัตรประจำตัวและรหัสผ่าน เพื่อพิสูจน์ตัวตนของผู้มีสิทธิ
- มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย จนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สิน หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต
- บุคคลภายนอกต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในห้องควบคุม
- ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญในห้องควบคุม
- สร้างความเข้าใจและตระหนักในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในห้องควบคุม
- จัดให้มีการทบทวนสิทธิอย่างสม่ำเสมอ และยกเลิกสิทธิการเข้าห้องควบคุมฯ ทันทีในกรณีที่มีการเปลี่ยนแปลงสิทธิ

2.3 การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)ในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

- จัดวางอุปกรณ์แต่ละประเภทตามพื้นที่ที่กำหนด
- ห้ามนำอาหาร เครื่องดื่ม เข้าไปในบริเวณห้องควบคุมฯ
- ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในห้องควบคุมฯ เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้นให้อยู่ในระดับปกติ

2.4 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities) ในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

- มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัทที่เพียงพอต่อความต้องการใช้งานโดยมีระบบดังต่อไปนี้ ระบบไฟฟ้าและ ระบบสำรองไฟฟ้า ระบบปรับอากาศแบบควบคุมความชื้น ระบบควบคุมการเข้า-ออกประตูอัตโนมัติ ระบบเฝ้าดูแลแจ้งเตือนความผิดปกติของสภาวะแวดล้อมอัตโนมัติ ระบบกล้องโทรทัศน์วงจรปิด ระบบสายสัญญาณและอุปกรณ์เครือข่ายคอมพิวเตอร์ อุปกรณ์ในการสลับใช้งานแป้นพิมพ์ จอภาพและเมาส์ของเครื่องคอมพิวเตอร์แม่ข่าย (KVM: Keyboard Video Mouse) และระบบไฟฟ้าฉุกเฉิน
- มีการตรวจสอบหรือทดสอบระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้ระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงาน

2.5 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ ในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

- มีการร้อยสายท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย
- มีการเดินสายสัญญาณสื่อสาร และสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน
- มีป้ายชื่อสำหรับสายสัญญาณบนอุปกรณ์ เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น
- มีการจัดทำผังสายสัญญาณสื่อสารต่างๆครบถ้วนถูกต้องและเป็นปัจจุบัน
- ตู้ Rack ที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

2.6 การบำรุงรักษาอุปกรณ์ (Equipment maintenance) ในห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

- มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนดทุก 3 เดือน
- ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ
- มีการจัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินผลในภายหลัง

- จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- มีการควบคุมและดูแลการปฏิบัติงานของบริษัทผู้รับจ้างบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของบริษัทผู้รับจ้างที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

3 การรักษาความมั่นคงปลอดภัยการใช้งานเครื่องคอมพิวเตอร์

3.1 การใช้งานของผู้ใช้งาน

- ให้มีการกำหนดรหัสผ่าน เปลี่ยนรหัสผ่านและเก็บรักษารหัสผ่าน เป็นไปตามข้อ 1.4 การใช้งานรหัสผ่านสำหรับผู้ใช้งาน
- ให้ผู้ใช้งานออกจากระบบ (Log off) ทันทีในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันบุคคลอื่นมาใช้ระบบต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหล ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที
- ผู้ไม่ได้รับสิทธิให้เข้าใช้งาน ห้ามบุกรุกเข้าใช้งานระบบเทคโนโลยีสารสนเทศไม่ว่าด้วยวิธีการใด ๆ
- ห้ามติดตั้งซอฟต์แวร์ หรือ โปรแกรมอื่นใดลงบนเครื่องคอมพิวเตอร์ ที่ใช้ปฏิบัติงาน หรือติดตั้งอุปกรณ์เชื่อมโยงเครือข่ายเพิ่มเติม หรือเชื่อมโยงเครือข่ายคอมพิวเตอร์ที่ใช้ปฏิบัติงานกับเครือข่ายอื่นนอกจากเครือข่ายของบริษัท หรือนำเครื่องคอมพิวเตอร์ส่วนตัวมาใช้งานกับระบบเทคโนโลยีสารสนเทศ เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ
- ไม่เปิดให้มีการแชร์ไฟล์ในเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงาน เว้นแต่ในกรณีที่เป็นระบบงานที่บริษัทกำหนดไว้ หากมีความจำเป็นให้กำหนดระยะเวลาเท่าที่ใช้งานและยกเลิกการแชร์ไฟล์ทันทีที่ใช้งานเสร็จเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และข้อมูล
- ไม่ดาวน์โหลด (Download) ข้อมูลหรือโปรแกรมที่ไม่เกี่ยวข้องกับการปฏิบัติงาน หรือ จากเว็บไซต์ซึ่งไม่น่าเชื่อถือ หรือไม่มั่นใจว่าจะปลอดภัย

3.2 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

- เครื่องคอมพิวเตอร์ส่วนบุคคลที่อนุญาตให้ใช้ เป็นทรัพย์สินของบริษัท จึงต้องใช้งานอย่างระมัดระวัง และให้มีประสิทธิภาพ
- โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ส่วนบุคคล ต้องเป็นโปรแกรมที่บริษัทเห็นชอบให้ใช้งาน หรือได้ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคลที่มิใช่ทรัพย์สินของบริษัท หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- ไม่นำสื่อข้อมูล เช่น แผ่นซีดี ดีวีดี แฟลชไดร์ฟ ที่ใช้งานจากเครื่องคอมพิวเตอร์ส่วนบุคคลอื่น ๆ นอกระบบเทคโนโลยีสารสนเทศ หรือมาจากแหล่งข้อมูลที่น่าสงสัย มาใช้งานกับเครื่องคอมพิวเตอร์ ส่วนบุคคลที่ใช้ปฏิบัติงานในระบบเทคโนโลยีสารสนเทศ โดยไม่ได้ตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ก่อน
- ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้ปฏิบัติงานในระบบเทคโนโลยีสารสนเทศ
- ให้ติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุงฐานข้อมูลไวรัสในเครื่องคอมพิวเตอร์ส่วนบุคคลให้เป็นปัจจุบัน อย่างสม่ำเสมอ
- ผู้ใช้งานต้องปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองใช้งาน เมื่อปฏิบัติงานเสร็จสิ้น
- ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์ส่วนบุคคลที่ไม่ใช่ทรัพย์สินของบริษัทมาใช้กับระบบเครือข่ายสื่อสาร ของบริษัท ยกเว้นได้รับการอนุญาตจากผู้ดูแลระบบก่อนการใช้งาน
- ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน
- ผู้ใช้งานต้องตรวจสอบข้อมูลใด ๆ ที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วยซึ่งมีผลทำให้ข้อมูล หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
- ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ส่วนบุคคลไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

- เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ และสื่อสำรองข้อมูลที่ไม่ใช้งานแล้วต้องทำลายข้อมูลที่สำรองไว้ ไม่ให้สามารถนำไปใช้งานได้อีก
- ให้มีการกำหนดรหัสผ่าน เปลี่ยนรหัสผ่านและเก็บรักษารหัสผ่าน เป็นไปตามข้อ 1.4 การใช้งานรหัสผ่านสำหรับผู้ใช้งาน

3.3 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

- เครื่องคอมแบบพกพาที่อนุญาตให้ใช้เป็นทรัพย์สินของบริษัท จึงต้องใช้งานอย่างระมัดระวัง และให้มีประสิทธิภาพ
- โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพา ต้องเป็นโปรแกรมที่บริษัทเห็นชอบให้ใช้งาน หรือได้ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาที่ไม่ใช่ทรัพย์สินของบริษัท หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์แบบพกพาและรักษาสภาพของเครื่องคอมพิวเตอร์พกพาให้มีสภาพเดิมและพร้อมใช้งาน
- ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่นการตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
- กรณีที่หน้าจอคอมพิวเตอร์ไม่ใช่แบบ Touch Screen ให้หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปากกากดสัมผัสหน้าจอ เพราะอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้
- ไม่วางของทับบนหน้าจอและแป้นพิมพ์
- การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

- ไม่เก็บหรือใช้งานเครื่องคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ
- ต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา
- ให้มีการกำหนดรหัสผ่าน เปลี่ยนรหัสผ่านและเก็บรักษารหัสผ่าน เป็นไปตามข้อ 1.4 การใช้งานรหัสผ่านสำหรับผู้ใช้งาน
- ปิดเครื่องคอมพิวเตอร์แบบพกพาที่ตนเองใช้งาน เมื่อปฏิบัติงานเสร็จสิ้น หรือ เมื่อมีการหยุดใช้งาน
- ทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาไว้บนสื่อบันทึกอื่น ๆเช่น CD, DVD, External Hard Disk
- เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ และสื่อสำรองข้อมูลที่ไม่ใช้งานแล้วควรทำลายข้อมูลที่สำรองไว้ ไม่ให้สามารถนำไปใช้งานได้อีก

4 การรักษาความมั่นคงปลอดภัยการใช้งานอินเตอร์เน็ตและจดหมายอิเล็กทรอนิกส์

4.1 การใช้งานอินเตอร์เน็ต

- ผู้ดูแลระบบต้องลงทะเบียนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบอินเทอร์เน็ตของบริษัท ซึ่งทำให้สามารถพิสูจน์ทราบได้ว่าเป็นเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงานที่ตั้งอยู่ที่หน่วยงานใดของบริษัท
- ผู้ใช้งาน / แผนกทรัพยากรส่วนบุคคลต้องยื่นเรื่องขอสิทธิการใช้งานเป็นลายลักษณ์อักษรเพื่อให้ขอรับสิทธิการใช้งาน และรหัสผ่าน เพื่อเป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลในการเข้าถึงระบบอินเทอร์เน็ตของบริษัท ซึ่งผู้ใช้งานแต่ละคนจะต้องดูแลรักษาสิทธิการใช้งานและรหัสผ่านของตนเองไม่ให้ผู้อื่นนำไปใช้งานได้ หากมีการกระทำใดซึ่งเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เจ้าของสิทธิต้องรับผิดชอบผลจากความเสียหายที่เกิดขึ้นโดยไม่อาจปฏิเสธได้
- ผู้ใช้งานต้องไม่ใช้ระบบอินเทอร์เน็ตในการใช้งานข้อมูลมัลติมีเดีย หรือดาวน์โหลดข้อมูลที่ไม่เกี่ยวกับการปฏิบัติงานและยึดครองช่องสัญญาณการสื่อสารข้อมูล

- ให้ผู้ดูแลระบบ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย เช่น Proxy, Firewall, IPS, IDS
- เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และอุปกรณ์คอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่
- ผู้ใช้งานต้องไม่ใช้งานอินเทอร์เน็ตของบริษัท เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม
- ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของบริษัท โดยผ่านความเห็นชอบจากผู้ดูแลระบบ
- ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของบริษัท ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต
- ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ตต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
- ให้ออกจากระบบอินเทอร์เน็ตทันทีหลังจากเลิกใช้งาน เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น
- ผู้ใช้งานต้องปฏิบัติตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

4.2 การใช้งานจดหมายอิเล็กทรอนิกส์

- ผู้ดูแลระบบต้องลงทะเบียนเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบอินเทอร์เน็ตของบริษัท ซึ่งทำให้สามารถพิสูจน์ทราบได้ว่าเป็นเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงานที่ตั้งอยู่ที่หน่วยงานใดของบริษัท
- ผู้ใช้งานต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทในการรับ-ส่งจดหมายอิเล็กทรอนิกส์ซึ่งเกี่ยวกับการใช้งานของบริษัทเท่านั้น

- ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อบริษัท สร้างความน่ารำคาญต่อผู้อื่น หรือขัดต่อศีลธรรม และไม่แสวงหาประโยชน์จากการใช้จดหมายอิเล็กทรอนิกส์ของบริษัท
- ผู้ใช้งานต้องออกจากระบบจดหมายอิเล็กทรอนิกส์ทันทีหลังจากการเลิกใช้งานเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น
- ก่อนเปิดเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องใช้โปรแกรมป้องกันไวรัสตรวจสอบเอกสารแนบเสมอ
- ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
- ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
- ผู้ใช้งานต้องสำรองข้อมูลที่มีความสำคัญในจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ

5 การรักษาความมั่นคงปลอดภัยการบริหารจัดการสินทรัพย์และเครือข่าย

5.1 การบริหารจัดการข้อมูลคอมพิวเตอร์

5.1.1 กำหนดประเภทของข้อมูล

- ข้อมูลที่เป็นตัวอักขระ คือข้อมูลที่ประกอบด้วยตัวอักษร และตัวเลขที่ไม่ใช้ในการคำนวณ เช่นข้อมูลเลขที่ของเอกสาร
- ข้อมูลที่เป็นตัวเลข คือข้อมูลที่ประกอบด้วยตัวเลข 0-9 ที่ใช้ในการคำนวณได้เช่น จำนวนสินค้าที่สั่งซื้อ
- ข้อมูลที่เป็นรูปภาพคือข้อมูลที่เป็นภาพนิ่งภาพเคลื่อนไหว ภาพลายเส้น ภาพถ่าย ภาพจากวิดิทัศน์ เช่นภาพสแกนเอกสาร
- ข้อมูลที่เป็นเสียง คือข้อมูลที่ประสาทสัมผัสทางหูรับรู้ได้ เช่น เสียงบันทึกการประชุม

5.1.2 กำหนดชั้นความลับข้อมูล

- ชั้นที่ 1 ข้อมูลเปิดเผยได้ ได้แก่

  ข้อมูลที่บุคคลทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น เป็นข้อมูลที่ไม่มีผลต่อการปฏิบัติงานของบริษัท สามารถนำเสนอต่อสาธารณชน หรือเป็นข้อมูลที่กฎหมายระบุว่า

ต้องเปิดเผย การเปิดเผยข้อมูลทั้งหมดหรือบางส่วน จะไม่เกิดผลเสียหายต่อบริษัท เช่น ข้อมูลที่เผยแพร่บนเว็บไซต์บริษัท

- ชั้นที่ 2 ข้อมูลใช้ภายในบริษัท ได้แก่

ข้อมูลที่เจ้าของข้อมูลพิจารณาแล้วว่า สามารถเปิดเผยให้ผู้ใช้งานภายในบริษัทรับทราบได้ แต่ไม่สมควรเปิดเผยต่อบุคคลภายนอก เพราะอาจจะสร้างความเสียหายให้กับบริษัทได้การเปิดเผยข้อมูล เจ้าของข้อมูลต้องใช้ดุลยพินิจในการอนุญาตหรือได้รับความเห็นชอบจากเจ้าของข้อมูล หรือการบังคับตามกฎหมาย เช่น ข้อมูลระบบบุคลากรบริษัท ข้อมูลระบบจดทะเบียนสิทธิและนิติกรรม

- ชั้นที่ 3 ข้อมูลลับ

ข้อมูลที่บริษัทพิจารณาแล้วว่าไม่สามารถเปิดเผยให้ผู้ใช้งานทุกคนทราบได้กำหนดให้เฉพาะผู้ที่เกี่ยวข้อง และจำเป็นต้องใช้ในการปฏิบัติงานทราบเท่านั้น และเป็นการใช้งานตามสิทธิความจำเป็นที่ควรทราบเพื่อให้เพียงพอต่อการปฏิบัติงาน ข้อมูลมีความสำคัญต่อการดำเนินการของบริษัทเป็นข้อมูลภายใน และไม่สามารถเปิดเผยต่อบุคคลภายนอกบริษัทที่ไม่เกี่ยวข้องตามกฎหมายได้ เนื่องจากข้อมูลนี้จะสร้างความเสียหายให้กับบริษัทได้ การเปิดเผยข้อมูลจะต้องได้รับความเห็นชอบจากเจ้าของข้อมูล หรือการบังคับตามกฎหมาย เช่นข้อมูลเงินเดือน ข้อมูลการลงโทษทางวินัย

- ชั้นที่ 4 ข้อมูลลับมาก

ข้อมูลที่ใช้ภายในบริษัทแต่เป็นข้อมูลลับใช้งานโดยผู้ใช้งานบางกลุ่มของบริษัท ซึ่งมีรหัสพิเศษในการเข้าใช้งานและไม่สามารถเปิดเผยต่อบุคคลภายนอกได้ เนื่องจากข้อมูล มีความจำเป็นต่อการปฏิบัติงานของบริษัท จะทำให้เกิดผลเสียหายร้ายแรงต่อบริษัท การเปิดเผยข้อมูล จะต้องได้รับการเห็นชอบจากเจ้าของข้อมูล หรือ หรือการบังคับตามกฎหมาย เช่น ข้อมูล การจราจรทางคอมพิวเตอร์ ข้อมูลจดหมายอิเล็กทรอนิกส์

- ชั้นที่ 5 ข้อมูลลับที่สุด

ข้อมูลที่ใช้ภายในบริษัทแต่เป็นข้อมูลลับ ใช้งานโดยผู้บริหารระดับสูง ของบริษัทเท่านั้น ซึ่งมีรหัสพิเศษในการเข้าใช้งาน และเป็นการใช้เพื่อการวินิจฉัย และตัดสินใจที่สำคัญ ของบริษัท ไม่สามารถเปิดเผยต่อบุคคลภายนอกบริษัทได้ เนื่องจากข้อมูลมีความจำเป็นต่อการ

ปฏิบัติงานของบริษัท ทำให้เกิดผลเสียหายร้ายแรงต่อบริษัทการเปิดเผยข้อมูล ไม่สามารถทำได้ เว้นแต่การบังคับตามกฎหมาย

5.1.3 การควบคุมการขอข้อมูล ขอใช้ ตรวจสอบ หรือขอเข้าดูข้อมูล

- เจ้าหน้าที่ของแผนกเทคโนโลยีสารสนเทศไม่มีสิทธิที่จะให้ข้อมูลแก่ผู้ขอข้อมูล ใด ๆ โดยที่ไม่ได้รับอนุญาตจากผู้อำนวยการแผนกเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย เว้นแต่ในการพัฒนาระบบ ซึ่งเจ้าหน้าที่ของแผนกเทคโนโลยีสารสนเทศและบริษัทผู้รับจ้างรับผิดชอบในการถ่ายโอนข้อมูลเข้าสู่ระบบใหม่
- กรณีหน่วยงานภายในบริษัทเป็นผู้ขอข้อมูลซึ่งหน่วยงานภายในบริษัทอื่น ๆ เป็นเจ้าของข้อมูลให้หน่วยงานผู้ขอทำบันทึกขออนุญาตจากหน่วยงานเจ้าของข้อมูล โดยเจ้าหน้าที่ของแผนกเทคโนโลยีสารสนเทศจะให้บริการเกี่ยวกับข้อมูลเมื่อได้รับทราบการได้รับอนุญาตนั้นแล้วเท่านั้น
- กรณีหน่วยงานภายนอกบริษัทไม่ว่าจะเป็นหน่วยงานราชการหรือหน่วยงานเอกชนเป็นผู้ขอ โดยไม่มีการทำบันทึกข้อตกลงระหว่างหน่วยงานกันไว้ก่อน ต้องทำหนังสือขออนุญาตจากบริษัททุกครั้งที่ขอ หากมีการทำบันทึกข้อตกลงกันไว้ ต้องควบคุมดูแลให้ขอบเขตของข้อมูลที่ขอเป็นไปตามบันทึกข้อตกลง
- กรณีบุคคลหรือนิติบุคคลเป็นผู้ขอข้อมูลกับบริษัท ซึ่งมีแนวทางหรือระเบียบปฏิบัติที่บริษัทได้กำหนดไว้แล้ว ให้ดำเนินการตามแนวทางหรือระเบียบปฏิบัติที่กำหนด

5.1.4 การกำหนดเวลาและช่องทางการเข้าถึงข้อมูล

- การกำหนดช่องทางการเข้าถึงข้อมูล ผู้ใช้งานภายในบริษัท ใช้ผ่านช่องทางอินทราเน็ตและอินเทอร์เน็ตสำหรับผู้ใช้งานภายนอกบริษัทใช้ผ่านช่องทางอินเทอร์เน็ตและตามบันทึกข้อตกลงระหว่างหน่วยงาน ส่วนข้อมูลที่เผยแพร่ด้วยช่องทาง อินเทอร์เน็ต สามารถเข้าถึงได้ตลอด 24 ชั่วโมง

5.2 การบริหารจัดการระบบคอมพิวเตอร์

- จัดทำทะเบียนคุมสินทรัพย์ในระบบคอมพิวเตอร์
- มีการกำหนดชื่อและ IP Address ในระบบคอมพิวเตอร์

- กำหนดบุคคลรับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของโปรแกรมระบบอย่างชัดเจน
- ในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานผู้ดูแลรับผิดชอบโดยทันที
- เปิดใช้บริการ (Service) เท่าที่จำเป็น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบการรักษาความปลอดภัย ต้องมีมาตรการเพิ่มเติม
- มีการติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่าง ๆของโปรแกรมระบบ (System Software) เช่น ระบบปฏิบัติการ DBMS และ Web server อย่างสม่ำเสมอ
- ทดสอบ System Software เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา
- บำรุงรักษาอุปกรณ์ ในระบบคอมพิวเตอร์ให้สามารถทำงานได้อย่างมีประสิทธิภาพ โดยควบคุมดูแลให้มีการบำรุงรักษาอุปกรณ์ในระบบคอมพิวเตอร์ตามระยะเวลาที่กำหนดในสัญญาจ้างบำรุงรักษา

5.3 การบริหารจัดการโปรแกรม

- จัดทำทะเบียนคุมโปรแกรม
- ลงทะเบียนขอให้ใช้โปรแกรมจากเจ้าของลิขสิทธิ์
- ปรับปรุงโปรแกรมเมื่อมีการเปลี่ยนแปลงรุ่นของโปรแกรม
- มีการควบคุมเวอร์ชั่นของโปแกรมประยุกต์ (Application)
- มีการติดตั้งโปรแกรมที่ถูกต้องตามลิขสิทธิ์หรือโปรแกรมสำหรับใช้ฟรี (Freeware, Open Source) และติดตั้งเท่าที่จำเป็นต่อการใช้งาน

5.4 การบริหารจัดการเครือข่ายสื่อสาร

- มีการจัดแบ่งแยกส่วนเครือข่าย/กลุ่ม (VLAN/ Zone)
  จัดทำทะเบียนคุมการใช้งานเครือข่ายสื่อสาร
- จัดทำแผนผังและขอบเขตของระบบเครือข่ายสื่อสาร
- ตรวจสอบการใช้งานเครือข่ายสื่อสารให้สามารถใช้งานได้อย่างมีประสิทธิภาพ
- ควบคุมการจัดเส้นทางบนเครือข่ายสื่อสารและกำหนดวิธีการเข้าถึงเครือข่ายสื่อสารบริษัท

- จัดทำระบบป้องกันการบุกรุกและการใช้งานที่ผิดปกติผ่านระบบเครือข่ายสื่อสาร
- ทดสอบการบุกรุกโจมตีเครือข่ายสื่อสาร และจัดทำรายงานการโจมตี
- กำหนดผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ของระบบเครือข่ายสื่อสารและอุปกรณ์ที่เชื่อมต่อ
- ทบทวนการกำหนดค่า Parameter อย่างน้อยปีละ 1 ครั้ง
- ทำการบำรุงรักษาระบบเครือข่ายสื่อสารเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ โดยควบคุมดูแลให้มีการบำรุงรักษาระบบเครือข่ายตามระยะเวลาที่กำหนดในสัญญาจ้างบำรุงรักษา

5.5 การบริหารจัดการสินทรัพย์

- จัดทำทะเบียนคุมสินทรัพย์ มีการกำหนดดังนี้
- กำหนดผู้รับผิดชอบต่อทรัพย์สิน
- จัดหมวดหมู่สินทรัพย์

5.6 การเบิกใช้อุปกรณ์คอมพิวเตอร์และเครือข่าย

- ผู้ใช้ที่ต้องการขอเบิกใช้อุปกรณ์ต้องกรอกข้อมูลคำขอลงในระบบ IT Service Request หรือแบบฟอร์มการขอเบิกใช้อุปกรณ์คอมพิวเตอร์และเครือข่าย โดยระบุรายการคที่ต้องการเบิกใช้รวมถึงสถานที่จัดเก็บหรือติดตั้ง และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการพิจารณาอนุมัติ
- เจ้าหน้าที่ผู้รับผิดชอบพิจารณาตามขั้นตอนและความเหมาะสมในการขอเบิกใช้งานอุปกรณ์ดังกล่าวโดยขอความเห็นชอบจากผู้บริหารหน่วยงานเจ้าของสินทรัพย์ หรือผู้ที่ได้รับมอบหมาย
- เมื่อมีการอนุมัติให้เบิกใช้อุปกรณ์ เจ้าหน้าที่ผู้รับผิดชอบต้องบันทึกข้อมูลสถานที่จัดเก็บหรือติดตั้งใหม่ของอุปกรณ์ดังกล่าวลงในแบบคำขอลงในระบบ IT Service Request หรือระบุลงในแบบฟอร์มการขอเบิกใช้อุปกรณ์คอมพิวเตอร์และเครือข่ายเพื่อจัดเก็บเป็นประวัติอุปกรณ์

5.7 การแจ้งซ่อมอุปกรณ์คอมพิวเตอร์และเครือข่าย

- เมื่อผู้ใช้งานพบการทำงานที่ผิดไปจากปกติของอุปกรณ์ หรือไม่สามารถใช้งานอุปกรณ์ในการดำเนินงานได้ ผู้ใช้งานต้องแจ้ง ให้ดำเนินการซ่อมบำรุง โดยกรอกข้อมูลที่ต้องการแจ้งลงในระบบ IT Service Request และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการซ่อม
- เจ้าหน้าที่ผู้รับผิดชอบวิเคราะห์อาการเสียหายของอุปกรณ์ จากข้อมูลใน ระบบ IT Service Request และจากการทดสอบการทำงานด้วยตนเอง รวมถึงพิจารณาข้อมูลประกอบโดยเฉพาะในส่วนของระยะเวลาประกันของอุปกรณ์ดังกล่าว ซึ่งหากอยู่ในระยะเวลาประกันเจ้าหน้าที่สามารถส่งอุปกรณ์ข้ารับการซ่อมบำรุงที่ศูนย์บริการของบริษัทผู้ผลิตอุปกรณ์ได้ โดยไม่เสียค่าใช้จ่ายในส่วนที่ระบุในประกัน หากอุปกรณ์ดังกล่าวไม่อยู่ในระยะเวลาประกัน เจ้าหน้าที่ผู้รับผิดชอบต้องพิจารณาจากความเสียหายของอุปกรณ์หากเสียหายมากอาจจำเป็นจะต้องจำหน่ายอุปกรณ์ดังกล่าว หรือหากความเสียหายของอุปกรณ์สามารถแก้ไขได้ให้เนินการแก้ไข
- ในระหว่างที่เจ้าหน้าที่ผู้รับผิดชอบส่งอุปกรณ์เข้ารับการซ่อมบำรุงนั้น หากมีอุปกรณ์อื่นที่สามารถใช้งานทดแทนอุปกรณ์ดังกล่าวได้ ให้เจ้าหน้าที่ดำเนินการแจ้งแก่ผู้ใช้ โดยให้ผู้ใช้ทำเรื่องเบิกใช้งานอุปกรณ์ โดยกรอกข้อมูลลงในแบบฟอร์มการขอเบิกใช้อุปกรณ์คอมพิวเตอร์และเครือข่ายโดยระบุรายการอุปกรณ์ที่ต้องการเบิกใช้รวมถึงสถานที่จัดเก็บหรือติดตั้ง และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการพิจารณาอนุมัติ และเจ้าหน้าที่ผู้ดูแลทะเบียนอุปกรณ์ทำการบันทึกข้อมูลอุปกรณ์ใหม่ลงใน “ระบบ IT Service Request” หรือแบบฟอร์มการขอเบิกใช้อุปกรณ์คอมพิวเตอร์และเครือข่าย เพื่อจัดเก็บเป็นประวัติอุปกรณ์ของบริษัท
- หลังจากที่เจ้าหน้าที่ผู้รับผิดชอบส่งอุปกรณ์ที่พบความเสียหายเข้ารับการแก้ไขเรียบร้อยแล้ว ต้องดำเนินการทดสอบในส่วนที่พบความเสียหายอีกครั้ง ก่อนจัดส่งอุปกรณ์คืนผู้ใช้ โดยเจ้าหน้าที่ผู้รับผิดชอบกรอกข้อมูลรายละเอียดการซ่อมบำรุง และการทดสอบอุปกรณ์ลงใน “ระบบ IT Service Request” หรือแบบฟอร์มการขอเบิกใช้อุปกรณ์คอมพิวเตอร์และเครือข่ายและส่งคืนอุปกรณ์พร้อมเอกสารดังกล่าวให้กับผู้ใช้

5.8 การนำสินทรัพย์ของบริษัทออกนอกสถานที่

- ให้มีการบันทึกขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์ออกนอกสถานที่เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน
- ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

5.9 การจำหน่ายอุปกรณ์คอมพิวเตอร์และเครือข่าย

- กรณีที่อุปกรณ์เสียหายเกินกว่าที่จะแก้ไขได้ รวมถึงไม่อยู่ในระยะเวลาประกันประกอบกับเมื่อพิจารณาถึงมูลค่าของอุปกรณ์กับค่าใช้จ่ายในการซ่อมบำรุงแล้ว จำเป็นต้องดำเนินการจำหน่ายอุปกรณ์ดังกล่าว ให้เจ้าหน้าที่ผู้รับผิดชอบกรอกรายละเอียดอุปกรณ์ลงใน “แบบฟอร์มการส่งคืนอุปกรณ์คอมพิวเตอร์และเครือข่าย” ให้เจ้าหน้าที่ผู้เป็นเจ้าของงาน/โครงการ ซึ่งเป็นผู้ใช้หรือผู้จัดหาอุปกรณ์รับทราบและพิจารณาเห็นชอบ
- เจ้าหน้าที่ผู้เป็นเจ้าของงาน/โครงการ พิจารณาเรื่องการส่งคืนอุปกรณ์ หากเห็นชอบให้ลงลายมือชื่อใน “แบบฟอร์มการส่งคืนอุปกรณ์คอมพิวเตอร์และเครือข่าย” หากไม่เห็นชอบให้ระบุเหตุผลและส่งเรื่องคืนเจ้าหน้าที่ผู้รับผิดชอบ
- ส่งเรื่องให้หน่วยงานที่มีอำนาจอนุมัติการจำหน่ายอุปกรณ์พิจารณาดำเนินการต่อไป

5.10 การควบคุมเอกสาร (Print out) ที่พิมพ์ออกจากระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- มีการกำหนดสิทธิการพิมพ์เอกสาร
- กำหนดให้มีเจ้าหน้าที่ควบคุมการเข้าถึงเอกสาร (Print out)
- จัดเก็บเอกสารที่เกี่ยวข้องกับระบบไว้ในสถานที่มั่นคงปลอดภัย
- เอกสารที่ไม่ใช้งานหรือมีความผิดพลาดจากการพิมพ์ ให้ทำลาย
- มีการบันทึกขออนุญาตก่อนนำเอกสารออกนอกสถานที่เพื่อเป็นหลักฐานป้องกันการสูญหาย

6 การรักษาความมั่นคงปลอดภัยการสำรองข้อมูลและกู้คืนข้อมูล

6.1 มีระบบจัดเก็บและสำรองข้อมูล ตามประเภทของข้อมูล ได้แก่ โปรแกรมระบบปฏิบัติการ โปรแกรมประยุกต์หรือแอพลิเคชั่น ชุดคำสั่ง และข้อมูล อย่างน้อยหนึ่งชุดแยกสถานที่จากกัน เพื่อความมั่นคงปลอดภัยและใช้งานได้อย่างต่อเนื่อง

6.2 กำหนดผู้รับผิดชอบในการสำรองข้อมูล ตรวจสอบความมีอยู่อย่างถูกต้อง ครบถ้วน ของข้อมูลอย่างน้อยปีละ1 ครั้ง และมีการบันทึกรายละเอียดการตรวจสอบ ในกรณีตรวจพบข้อมูลสูญหาย ไม่ถูกต้องครบถ้วน ให้ดำเนินการปรับปรุง แก้ไขข้อมูลให้มีความสมบูรณ์ครบถ้วนในทันที

6.3 กำหนดความถี่ในการสำรองข้อมูลของระบบงาน และทำการสำรองข้อมูลตามความถี่ ที่กำหนดไว้ (ระบบงานที่มีการเปลี่ยนแปลงบ่อย ควรจะมีความถี่ในการสำรองข้อมูลมากขึ้น) และมีการนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย 1 ชุด

- กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งซอฟต์แวร์
- ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วน หรือไม่
- ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ อย่างน้อยปีละ 1 ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้ หรือไม่

6.4 จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ ภายในระยะเวลาที่กำหนด โดยมีแนวทางปฏิบัติสำหรับการกู้คืนข้อมูลจากภัยพิบัติ โดย

- มีการกำหนดระบบงานที่มีความสำคัญทั้งหมดของบริษัท และจัดทำเป็นบัญชี รายชื่อของระบบงาน ดังกล่าว รวมทั้งปรับปรุงบัญชีรายชื่อนี้ให้มีความทันสมัยอยู่เสมอตามระบบงานที่มีความสำคัญที่เกิดขึ้นใหม่
- ประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงที่พบให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง
- กำาหนดชนิดของข้อมูล เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบงาน หรือข้อมูล ในฐานข้อมูล
- กำหนดความถี่ในการสำรองข้อมูล และวิธีการสำรอง เช่น แบบ Full Backup หรือ Incremental Backup ของระบบงานที่มีความสำคัญเหล่านั้น

6.5 จัดทำแผนกู้คืนเพื่อรับมือกับภัยพิบัติที่อาจเกิดขึ้นได้ แผนกู้คืนต้องมีรายละเอียด ดังต่อไปนี้

- การกำหนดหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด
- การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้

- การกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบงาน
- การกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้
- การทดสอบตามแผนเตรียมความพร้อมฯ อย่างน้อยปีละ 1 ครั้ง

6.6 การสร้างความตะหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

6.7 ให้ปรับปรุงแผนกู้คืนอย่างน้อยปีละ 1 ครั้ง

6.8 ให้ทำการสำรองข้อมูลตามชนิด ความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลที่สำรองไปนั้นมีความครบถ้วน

6.9 ให้ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้นั้น ว่าสามารถกู้คืนได้อย่างครบถ้วนหรือไม่ อย่างน้อยปีละ 1 ครั้ง ถ้าพบว่ามีปัญหาเกิดขึ้นในระหว่างการทดสอบกู้คืน ให้ดำเนินการแก้ไข และบันทึกข้อมูลปัญหานั้นไว้ พร้อมทั้งวิธีการแก้ไขอย่างเป็นลายลักษณ์อักษร

6.10 ให้จัดประชุมและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนกู้คืน รวมทั้งมีการปรับปรุงแผนกู้คืนใหม่จะต้องจัดประชุมใหม่ และแจ้งให้ผู้เกี่ยวข้องทราบเช่นเดียวกัน

6.11 จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ เพื่อให้การปฏิบัติงานเป็นไปอย่างต่อเนื่อง

- ให้เตรียมแบบฟอร์ม/ แบบพิมพ์ที่สามารถใช้ทดแทนแบบฟอร์ม / แบบพิมพ์ ที่พิมพ์ได้จากระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- ให้ปฏิบัติงานตามกระบวนงานเดิมก่อนที่จะนำระบบเทคโนโลยีสารสนเทศและ การสื่อสารปัจจุบันมาใช้ เช่น การใช้ระบบมือ (Manual System)
- เมื่อระบบเทคโนโลยีสารสนเทศและการสื่อสารสามารถใช้งานได้ตามปกติ ให้นำข้อมูลที่เกิดขึ้นระหว่างที่เกิดเหตุฉุกเฉินฯ เข้าระบบ

7 การรักษาความมั่นคงปลอดภัยด้านการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

7.1 มีการแต่งตั้งคณะทำงานบริหารความเสี่ยงของแผนกเทคโนโลยีสารสนเทศ เพื่อดำเนินการ
- จัดลำดับความสำคัญของความเสี่ยง
- จัดทำแผนบริหารความเสี่ยง
- ดำเนินการตามแผนบริหารความเสี่ยง

7.2 มีการตรวจสอบและประเมินความเสี่ยงในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์อย่างน้อยปีละ 1 ครั้ง

8 การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

8.1 มีการเผยแพร่ประชาสัมพันธ์และฝึกอบรม ให้เจ้าหน้าที่บริษัทรับทราบ เข้าใจและไม่กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และกฎหมายอื่น ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ รวมถึงมีความรับผิดชอบในการใช้ทรัพยากรทางด้านเทคโนโลยีสารสนเทศของบริษัทอย่างเหมาะสม

8.2 ให้ผู้มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ ทางเว็บไซต์บริษัทจะต้องดำเนินการด้วยตนเอง โดยห้ามมิให้ผู้อื่นดำเนินการแทน

8.3 มีการทบทวนปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศให้มีความทันสมัย และเป็นมาตรฐานที่ยอมรับอย่างน้อยปีละ 1 ครั้ง

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

- ลายมือชื่อ -

(นายธนวัฒน์ ตรีวิศวเวทย์)

กรรมการผู้จัดการ