



นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด(มหาชน)

นโยบายฉบับนี้อนุมัติโดยคณะกรรมการบริษัทเมื่อวันที่ 15 กันยายน 2565

ทบทวนครั้งที่ 1 ฉบับลงวันที่ 29 ธันวาคม 2568

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ของบริษัท พรีเมียร์ควอลิตี้สตาร์ซ จำกัด (มหาชน) รวมถึงบริษัทย่อย ได้แก่ บริษัท พรีเมียร์ควอลิตี้สตาร์ซ (2012) จำกัด บริษัท พรีเมียร์ไบโอเอนเนอร์จี จำกัด บริษัท พรีเมียร์โมดิไฟด์สตาร์ซ จำกัด และบริษัท พรีเมียร์โลจิสติกส์ จำกัด (รวมเรียกว่า "บริษัท") ที่ใช้ระบบสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ร่วมกัน เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของบริษัทได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัท บริษัทฯ จึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ดังนี้

คำนิยาม

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้กันใน นโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

1. "บริษัท" หมายความว่า บริษัท พรีเมียร์ควอลิตี้สตาร์ซ จำกัด(มหาชน) รวมถึงบริษัทย่อย ที่ใช้ระบบสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ร่วมกัน
2. "ฝ่ายทรัพยากรบุคคล" หมายความว่า ฝ่ายทรัพยากรบุคคล ของบริษัท พรีเมียร์ควอลิตี้สตาร์ซ จำกัด(มหาชน) รวมถึงบริษัทย่อย
3. "ส่วนเทคโนโลยีสารสนเทศ" หมายความว่า ส่วนเทคโนโลยีสารสนเทศ ของบริษัท พรีเมียร์ควอลิตี้สตาร์ซ จำกัด (มหาชน) รวมถึงบริษัทย่อย
4. "ส่วนจัดการอาคารและบริเวณ" หมายความว่า ส่วนจัดการอาคารและบริเวณ ของบริษัท พรีเมียร์ควอลิตี้สตาร์ซ จำกัด(มหาชน) รวมถึงบริษัทย่อย
5. "ผู้ใช้งาน" หมายความว่า กรรมการบริษัท ผู้บริหาร ผู้ปฏิบัติงาน ผู้ใช้งานที่เกี่ยวข้อง และผู้ใช้งานภายนอกที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเครือข่ายของบริษัท
6. "ผู้ปฏิบัติงาน" หมายความว่า ผู้ปฏิบัติงาน ลูกจ้างทดลองงาน และลูกจ้างชั่วคราวของบริษัท
7. "ผู้ใช้งานที่เกี่ยวข้อง" หมายความว่า บุคคล หรือนิติบุคคลที่เป็นคู่สัญญาของบริษัท ที่เข้ามาดำเนินกิจกรรมภายในบริษัท
8. "ผู้ใช้งานภายนอก" หมายความว่า บุคคล หรือนิติบุคคลนอกเหนือจากข้อ (6) และข้อ (7)

9. "ผู้ดูแลระบบ" หมายความว่า ผู้จัดการส่วนเทคโนโลยีสารสนเทศ หรือผู้ปฏิบัติงานอื่น ที่ได้รับมอบหมายจากผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายขึ้นไป ให้มีหน้าที่รับผิดชอบในการพัฒนา แก้ไข ปรับปรุง และดูแล รักษา ระบบสารสนเทศและระบบเครือข่ายที่ใช้งานอยู่ในบริษัทหรือหน่วยงานที่มีหน้าที่ และรับผิดชอบในการดูแลระบบสารสนเทศและระบบเครือข่ายโดยตรง
10. "สารสนเทศ" หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ เอกสาร แผนผัง แผนที่ ภาพถ่าย ฟิล์ม การบันทึกภาพ การบันทึกเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
11. "ระบบสารสนเทศ" หมายความว่า ระบบงานของบริษัท ที่ใช้จัดเก็บ ประมวลผลข้อมูล และเผยแพร่สารสนเทศ ซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผล ให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร และการสนับสนุนกลไกการทำงานของบริษัท
12. "ระบบเครือข่าย" หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของบริษัท ได้ เช่น ระบบ LAN ระบบ Wireless ระบบ Intranet ระบบ Internet และระบบการสื่อสารอื่นๆ
13. "สินทรัพย์" หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับบริษัท ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี หรือซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อบริษัท
14. "ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายของบริษัท โดยอ้างไว้ซึ่งความลับ(Confidentiality) ความถูกต้องครบถ้วน(Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง(Authenticity) ความรับผิดชอบ(Accountability) การห้าม ปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
15. "สิทธิ์ของผู้ใช้งาน" หมายความว่า ระดับขั้นของการเข้าถึงข้อมูลสารสนเทศของผู้ปฏิบัติงานและผู้ใช้งานที่เกี่ยวข้อง ได้แก่ สิทธิ์ทั่วไป สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ และระบบเครือข่ายของบริษัท
16. "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

17. "บัญชีผู้ใช้งาน" หมายความว่า บัญชีรายชื่อ (Username) และรหัสผ่าน (Password) สำหรับผู้ปฏิบัติงาน ผู้ใช้งานที่เกี่ยวข้อง และผู้ใช้งานภายนอก
18. "เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือ มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความปลอดภัย
19. "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่า สถานการณ์ ซึ่งอาจทำให้ระบบของบริษัทถูกรบกวนหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
20. "การเข้ารหัส (Encryption)" หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูลผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้ จะต้องมียุทธศาสตร์เพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
21. "การยืนยันตัวตน (Authentication)" หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปแล้ว เป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
22. "SSL (Secure Socket Layer)" หมายความว่า เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน
23. "VPN (Virtual Private Network)" หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยใช้การรับส่งข้อมูลจริง ซึ่งในการรับส่งข้อมูลจะทำการเข้ารหัสเฉพาะ โดยผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

หมวดที่ 1

การกำกับดูแลและบริหารจัดการ IT ระดับองค์กรที่ดี (Governance of Enterprise IT)

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ มีจุดมุ่งหมายเพื่อให้แน่ใจว่า บริษัทสามารถบรรลุเป้าหมายที่กำหนดไว้ โดยนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุน และสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศมาใช้งานได้อย่างมีประสิทธิภาพ การบริหารจัดการด้านเทคโนโลยีสารสนเทศที่ดีนั้นต้องมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศทรัพยากรและข้อมูลที่มีประสิทธิภาพเพื่อสนับสนุนนโยบาย ยุทธศาสตร์ เป้าหมายขององค์กรและการบริหารความเสี่ยงที่เหมาะสม รวมทั้งมีการรายงานและติดตามการดำเนินงาน เพื่อให้มั่นใจว่า เทคโนโลยีที่บริษัทนำมาใช้งานสามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจและสร้างศักยภาพในการแข่งขัน รวมทั้งเพิ่มมูลค่าให้กับบริษัท โดยบริษัทต้องพิจารณาดำเนินการอย่างน้อยดังต่อไปนี้

1. นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)

1. บริษัทต้องจัดให้มีหน้าที่ดูแลให้มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และบริษัทต้องทำการสื่อสารนโยบายดังกล่าวเพื่อสร้างความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานด้านอื่นภายในบริษัท เพื่อให้มีการประสานงานและสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้
2. บริษัทต้องจัดให้มีการทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท

2. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

ต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงองค์กร (Corporate Risk Management) และครอบคลุมในเรื่องดังต่อไปนี้

1. การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ผู้จัดการส่วนเทคโนโลยีมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่ แล้วนำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ
2. การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Information Technology Related Risk)
 - ความเสี่ยงด้านกายภาพและสภาพแวดล้อม ได้แก่ ห้องศูนย์กลางข้อมูล (Data Center Room) ซึ่งเป็นที่จัดเก็บติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย(Server) อุปกรณ์เครือข่ายและอุปกรณ์อื่น ต้องมีการควบคุมการเข้า-ออกและการใช้งาน การตรวจสอบระบบต่างๆ เช่น ระบบเตือนอุณหภูมิภายในห้อง ระบบเตือนอัคคีภัย เป็นต้น
 - ความเสี่ยงด้านการใช้งาน โปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของบริษัทเพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัยหรือไม่ประสงค์ดี เช่น การดาวน์โหลดโปรแกรมจากภายนอกมาติดตั้ง ซึ่งอาจมีมัลแวร์ หรือไวรัสคอมพิวเตอร์หรือมีช่องโหว่เชื่อมต่อเครือข่ายภายนอก เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน เป็นต้น
 - ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ของบริษัท ต้องมีตรวจสอบและเฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต โดยมีการจัดทำระบบป้องกันการเข้าถึงและการโจมตีจากภายนอกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงาน

ใช้งาน เช่น ระบบป้องกันการเข้าออกใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ การกรองข้อมูลรับส่งอีเมล เป็นต้น

- ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิ์การใช้งานเข้าถึงระบบเครื่องคอมพิวเตอร์อุปกรณ์เครือข่ายต่างๆ และข้อมูล ให้เป็นไปตามสิทธิ์ที่พึงมี เพื่อป้องกันการเข้าแก้ไขหรือเปลี่ยนแปลงข้อมูล

3. การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ 4 ประเภท ดังนี้

- ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี
- ความเสี่ยงจากผู้ปฏิบัติงาน ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึง ข้อมูลเกินกว่าหน้าที่ และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้
- ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้ง สถานการณ์อื่น เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น
- ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากแนวนโยบายที่ทำการใช้งานอยู่อาจไม่ สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

4. การกำหนดวิธีการหรือเครื่องมือในการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่บริษัทยอมรับได้ จัดทำตารางลักษณะรายละเอียดความความเสี่ยง (Description of Risk) โดยมีหัวเรื่อง ชื่อความเสี่ยง ประเภท ความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนด ระดับโอกาสการเกิดเหตุการณ์ และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

5. กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk Indicator) รวมถึง จัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารจัดการความเสี่ยง ได้อย่างเหมาะสมและทันต่อเหตุการณ์ และเพื่อให้นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศมีความสมบูรณ์และสามารถวัดผลได้อย่างเป็นรูปธรรมยิ่งขึ้น ควรมีการทบทวนและกำหนดเกณฑ์ชี้วัด (Threshold) หรือ ค่าเป้าหมาย (Target Value) สำหรับตัวชี้วัดความเสี่ยง (IT Risk Indicator) แต่ละรายการให้ชัดเจน นอกเหนือจากการติดตามและรายงานผลเพียงอย่างเดียว ตัวอย่างเช่น การกำหนดระยะเวลาเฉลี่ยในการแก้ไขช่องโหว่หรือเหตุการณ์ด้านความปลอดภัย (Mean Time to Remediate) ให้อยู่ภายในจำนวนวันทำการที่ยอมรับได้ การมี เกณฑ์ที่ชัดเจนจะช่วยให้ผู้รับผิดชอบสามารถประเมินประสิทธิภาพของการจัดการความเสี่ยงและดำเนินการแก้ไขได้ อย่างทัน่วงทีเมื่อผลการดำเนินงานต่ำกว่าเป้าหมายที่กำหนดไว้

3. นโยบายความมั่นคงปลอดภัยสำหรับระบบควบคุมอุตสาหกรรม (ICS/SCADA)

เพื่อกำหนดมาตรการควบคุมขั้นพื้นฐานในการรักษาความมั่นคงปลอดภัย ความสมบูรณ์ และความพร้อมใช้งาน (Security Integrity and Availability) ของระบบควบคุมอุตสาหกรรม (ICS) ซึ่งรวมถึงระบบ SCADA PLC (Programmable Logic Controller) และ HMI (Human-Machine Interface) เพื่อป้องกันผลกระทบต่อกระบวนการผลิต ความปลอดภัยของพนักงาน และสิ่งแวดล้อม นโยบายนี้บังคับใช้กับสินทรัพย์สารสนเทศทั้งหมดที่เกี่ยวข้องกับระบบควบคุมอุตสาหกรรม รวมถึงฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย และบุคลากรที่เข้าถึงหรือบริหารจัดการระบบดังกล่าว ดังนี้

1. การแบ่งแยกเครือข่าย (Network Segmentation)

- ต้องมีการแบ่งแยกเครือข่ายของระบบควบคุมอุตสาหกรรม (OT Network) ออกจากเครือข่ายสำนักงาน (IT Network) และเครือข่ายอินเทอร์เน็ตอย่างชัดเจน
- การเชื่อมต่อระหว่างเครือข่าย IT และ OT จะต้องมีการควบคุมการเข้าถึงผ่านไฟร์วอลล์ (Firewall) อย่างรัดกุม

2. การควบคุมการเข้าถึง (Access Control)

- จำกัดการเข้าถึงระบบ SCADA ทั้งทางกายภาพและทางตรรกะ (Logical Access) ให้เฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้น
- ห้ามใช้บัญชีผู้ใช้งานร่วมกัน (Shared Accounts) และให้ใช้หลักการให้สิทธิ์น้อยที่สุด (Principle of Least Privilege)
- การเข้าถึงระบบจากระยะไกล (Remote Access) ต้องผ่านการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication - MFA) และใช้ช่องทางที่เข้ารหัส (Encrypted Channel) เช่น VPN ที่มีความปลอดภัยสูง

3. การบริหารจัดการช่องโหว่และความปลอดภัยของระบบ (System Hardening & Patch Management)

- ระบบปฏิบัติการและแอปพลิเคชันบนเครื่องแม่ข่ายและสถานีงานของ SCADA ต้องได้รับการปรับปรุงให้มีความปลอดภัย (Hardening) โดยการปิดบริการที่ไม่จำเป็น
- การติดตั้งแพตช์ (Patch) ความปลอดภัยต้องผ่านการทดสอบในสภาพแวดล้อมจำลองก่อนนำไปติดตั้งบนระบบจริง และต้องมีแผนสำรองในกรณีที่เกิดปัญหา

4. การป้องกันมัลแวร์ (Malware Protection)

- ติดตั้งโปรแกรมป้องกันมัลแวร์ที่ออกแบบมาสำหรับสภาพแวดล้อมระบบควบคุมอุตสาหกรรม โดยเฉพาะ เพื่ออนุญาตให้เฉพาะโปรแกรมที่ได้รับการอนุมัติเท่านั้นที่ทำงานได้
- ห้ามนำเข้าอุปกรณ์จัดเก็บข้อมูลแบบพกพา (เช่น USB Drive) ที่ไม่ผ่านการตรวจสอบมาเชื่อมต่อกับระบบ SCADA โดยเด็ดขาด

5. การสำรองข้อมูลและแผนฟื้นฟูระบบ (Backup and Recovery)

- ต้องมีกระบวนการสำรองข้อมูลการตั้งค่า (Configuration) โปรแกรม และข้อมูลสำคัญของระบบ SCADA อย่างสม่ำเสมอ
- ต้องมีการทดสอบกระบวนการกู้คืนระบบ (System Recovery Test) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าสามารถฟื้นฟูระบบให้กลับมาทำงานได้ตามระยะเวลาที่กำหนด (Recovery Time Objective - RTO)

หมวดที่ 2

การรักษาความมั่นคงปลอดภัยของระบบ IT (IT Security)

1. แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของ IT (Information Security Policy)

- วัตถุประสงค์

เพื่อเป็นการป้องกันการกระทำผิดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

- แนวทางปฏิบัติ

- ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น
- ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้

- ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือ คัดลอก
- ห้ามเผยแพร่ข้อมูลของผู้อื่นหรือของหน่วยงานโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูลนั้นๆ
- ห้ามก่อวินาศกรรม ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัท เกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ การบ่อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น
- ห้ามลักลอบดักจับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัท และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์
- ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนทุกครั้ง
- ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

2. การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

- วัตถุประสงค์
เพื่อกำหนดกรอบการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายในบริษัท
- แนวทางปฏิบัติ
 - ผู้บริหารระดับสูง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท
 - ผู้จัดการส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในส่วนเทคโนโลยีสารสนเทศ รับผิดชอบการดูแลระบบสารสนเทศที่บริษัทใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท

- ผู้จัดการส่วนเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแลติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท
- ผู้ปฏิบัติงานส่วนเทคโนโลยีสารสนเทศ ที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator รับผิดชอบต่อระบบที่ดูแลนั้น จะต้องทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยในการใช้งานของระบบด้วย และเมื่อมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด จะต้องดำเนินการแก้ไขและรายงานต่อผู้บังคับบัญชา
- ผู้ใช้งาน และหน่วยงานทั้งภายในและภายนอก ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัท ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

3. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

- วัตถุประสงค์
เพื่อให้ผู้ใช้งานเข้าใจนโยบาย หน้าที่และความรับผิดชอบในการใช้งานระบบสารสนเทศของบริษัท
- แนวทางปฏิบัติ
 - ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับบุคคลหรือหน่วยงานภายนอกที่จ้างมาปฏิบัติงานและจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศของบริษัท
 - ต้องมีการลงนามในสัญญาระหว่างผู้ปฏิบัติงานและหน่วยงานว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างผู้ปฏิบัติงานนั้นๆ ทั้งนี้ ต้องมีผลผูกพันทั้งในขณะทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว
 - เพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ฝ่ายทรัพยากรบุคคลหรือหน่วยงานที่เกี่ยวข้อง ต้องแจ้งให้ผู้จัดการส่วนเทคโนโลยีสารสนเทศทราบทันที เมื่อมีเหตุดังนี้
 - การว่าจ้างงาน

- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นกรรมการและผู้บริหารงานของบริษัท
- การโยกย้ายหน่วยงาน
- ต้องให้พนักงานและหน่วยงานภายนอกที่เข้าปฏิบัติงานรับทราบ นโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- ผู้ปฏิบัติงานใหม่ของบริษัทต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศหลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน หรือสิ้นสุดโครงการ ต้องยกเลิกการเข้าถึงข้อมูลในระบบสารสนเทศทันที

4. การบริหารจัดการสินทรัพย์สารสนเทศ (Asset Management)

4.1 การควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral Access Control)

- วัตถุประสงค์
เพื่อให้พนักงานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของบริษัทให้มีความปลอดภัย ถูกต้องและมีความพร้อมใช้งานอยู่เสมอ
- แนวทางปฏิบัติ
 - ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน
 - ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม
 - ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน

- ห้ามตัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม
- ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่นละออง และต้องระวังการตกกระทบ
- ไม่ใช่หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็กไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 35 องศาเซลเซียส
- ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับหรือโยน
- ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่
- หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วนหรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- ผู้ใช้งานที่พ้นสภาพหรือสิ้นสุดโครงการต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน
- การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงานให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

4.2 การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

- วัตถุประสงค์

เพื่อให้ผู้ใช้งานตระหนักถึงหน้าที่และความรับผิดชอบในการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนเข้าใจการใช้โปรแกรมที่ต้องลิขสิทธิ์และปฏิบัติตามแนวทางปฏิบัติอย่างเคร่งครัด รวมถึงการใช้งานโปรแกรมคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยและสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

- แนวทางปฏิบัติ

ข้อกำหนดสำหรับผู้ดูแลระบบ

- มีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัทตามสิทธิ์การใช้งานที่กำหนดมีหน้าที่รับผิดชอบในการติดตั้งและอัปเดตโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวันเวลาที่นัดหมาย
- ทำการถอดและยกเลิกสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์ทันที เมื่อบริษัทและ/หรือหน่วยงาน แจ้งยกเลิกและ/หรือย้ายสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์

ข้อกำหนดสำหรับผู้ใช้งาน

- ต้องใช้โปรแกรมคอมพิวเตอร์อย่างเช่นวิญญูชน พึงจะใช้ทรัพย์สินของตนเองโดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหาย
- โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน
- ห้ามคัดลอก จำหน่าย เผยแพร่ โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัดทำขึ้น โดยไม่ได้รับอนุญาต โดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย
- ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้งใช้งานบนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด กรณีผู้ใช้งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทมีอยู่ มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะ มี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้น ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
- การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณี ให้ผู้มีอำนาจพิจารณาอนุมัติ และผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี

4.3 การควบคุมสิทธิ์ด้านสารสนเทศและการใช้งานระบบคอมพิวเตอร์

- แนวทางปฏิบัติ

ต้องควบคุมไม่ให้สิทธิ์ด้านสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ และข้อมูลสารสนเทศ อยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ์ ขณะที่ไม่มีผู้ใช้งาน อุปกรณ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

- ออกจากระบบสารสนเทศ (Log out) โดยทันทีเมื่อเสร็จสิ้นงาน
- มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้การพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน
- ต้องจัดเก็บและสำรองข้อมูลสารสนเทศที่มีความสำคัญของหน่วยงานไว้ในที่ที่ปลอดภัย การจัดเก็บข้อมูลของผู้ใช้งาน จะจัดเก็บได้อยู่ในรูปแบบดังนี้
 - ในฐานข้อมูลของระบบ Application นั้นๆ ที่จัดเก็บภายใน Data Center ของบริษัท การ Export ข้อมูลออกมาจากระบบ Application ไม่สามารถทำได้
 - สามารถจัดเก็บใน Shared File (Drive กลาง) ใน Folder ตามสิทธิ์ที่ได้รับ
- ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อไม่มีการใช้งานนานเกิน 1 ชั่วโมง หรือเมื่อใช้งานประจำวันเสร็จสิ้นงาน เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์แม่ข่ายให้บริการที่ต้องใช้งานตลอด 24 ชั่วโมง
- การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ให้มีการล็อก(Lock) หน้าจอโดยอัตโนมัติหลังจากไม่ใช้งานเครื่องคอมพิวเตอร์เกินกว่า 10 นาที
- ให้มีการขออนุมัติจากผู้มีอำนาจสูงสุดของฝ่ายขึ้นไป ในกรณีที่ต้องการนำทรัพย์สินด้านสารสนเทศต่างๆ เช่น เอกสาร สื่อบันทึกข้อมูล อุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกบริษัททุกครั้ง โดยปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท
- ระมัดระวังและดูแลทรัพย์สินของบริษัท ที่ตนเองใช้งานเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาณเล็กน้อย ต้องรับผิดชอบหรือชดเชยต่อความเสียหายนั้น

4.4 การใช้งานจดหมายอิเล็กทรอนิกส์

- วัตถุประสงค์

เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ สามารถสนับสนุนการปฏิบัติงานและเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ ปลอดภัย ภายใต้ข้อกำหนดของกฎหมายระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของบริษัท ตลอดจนเพื่อให้ผู้ใช้งานเข้าใจถึงความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต โดยผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบอย่างเคร่งครัด

- แนวทางปฏิบัติ

- ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายที่เกี่ยวข้อง และนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศที่บริษัทกำหนด
- หน่วยงานหรือผู้ปฏิบัติงานผู้ให้บริการจดหมายอิเล็กทรอนิกส์ของบริษัทจะต้องใช้จดหมายอิเล็กทรอนิกส์ เพื่อผลประโยชน์ของบริษัท
- ผู้ปฏิบัติงานจะได้รับสิทธิ์ในการใช้บริการจดหมายอิเล็กทรอนิกส์ โดยทางผู้ดูแลระบบจะเป็นผู้ทำการลงทะเบียนผู้ให้บริการจดหมายอิเล็กทรอนิกส์ตามรายชื่อผู้ปฏิบัติงานที่ได้รับแจ้งมาจากฝ่ายทรัพยากรบุคคล
- ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อความ เว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ให้บริการ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน
- การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่งหรือบัญชีผู้ใช้งานอื่น
- การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของบริษัทผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทขัดข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

- การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุยง เสียดยั่ว ส่อไปในทางผิดกฎหมาย และผู้ใช้งาน ต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของบริษัท หรือก่อให้เกิดความเสียหายต่อบริษัท
- ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์ หรือกระทบต่อการดำเนินงานของบริษัท ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของบริษัท
- ห้ามผู้ให้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการงานส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีกระทำความผิดดังกล่าว ให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ หรือเจ้าของผู้ให้บริการ เป็นผู้รับผิดชอบการกระทำความผิดดังกล่าว
- ห้ามกระทำการอันที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่ (Chain mail) การส่งจดหมายจำนวนมาก (Spam mail) การส่งจดหมายต่อเนื่อง (Letter bomb) การส่งจดหมายเพื่อการแพร่กระจาย ไวรัสคอมพิวเตอร์ เป็นต้น
- ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทให้กับบุคคลอื่น หรือหน่วยงานที่ไม่เกี่ยวข้องกับการกิจของบริษัท
- การส่งข้อมูลข่าวสารที่เป็นความลับบริษัท ควรมีการเข้ารหัสข้อมูลข่าวสารนั้น และไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
- หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรออกจากระบบ (Log out) ทุกครั้ง
- กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิก หรือระงับการบริการชั่วคราวแก่ผู้ปฏิบัติงานนั้นๆ เพื่อทำการสอบสวน และตรวจสอบสาเหตุ
- หากผู้ให้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิดเกิดขึ้นในบริษัท ให้แจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของบริษัท

- การกระทำใดๆ ที่เกี่ยวข้องกับการเผยแพร่ ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์ และ โสมเพจของผู้ให้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ให้บริการ เท่านั้น ผู้ดูแลระบบและบริษัทไม่มีส่วนเกี่ยวข้องใดๆ

4.5 การใช้งานอุปกรณ์อินเทอร์เน็ตทุกสรรพสิ่งหรืออุปกรณ์อัจฉริยะที่เชื่อมต่อกับระบบเครือข่ายภายใน

- วัตถุประสงค์

เพื่อกำหนดหลักเกณฑ์การบริหารจัดการสินทรัพย์และอุปกรณ์ประเภทอินเทอร์เน็ตทุกสรรพสิ่ง (IoT) หรืออุปกรณ์อัจฉริยะที่เชื่อมต่อกับเครือข่าย ตั้งแต่การขึ้นทะเบียน การใช้งาน การดูแลรักษา การเคลื่อนย้าย จนถึงการทำนายออกจากระบบ เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ และให้เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง

- แนวทางปฏิบัติ

- ก่อนจัดหาอุปกรณ์ IoT หรืออุปกรณ์อัจฉริยะ ให้หน่วยงานผู้เข้าร่วมกับหน่วยงานด้านเทคโนโลยีสารสนเทศ พิจารณาความจำเป็น ประโยชน์ และความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- ในกรณีที่อุปกรณ์จะเชื่อมต่อกับระบบงานที่สำคัญ หรือเกี่ยวข้องกับข้อมูลส่วนบุคคล ให้พิจารณาดำเนินการประเมินความเสี่ยงตามกระบวนการบริหารความเสี่ยงของหน่วยงานก่อนอนุมัติใช้
- การขึ้นทะเบียนและกำหนดผู้รับผิดชอบของอุปกรณ์ IoT และอุปกรณ์อัจฉริยะทุกชิ้นที่เชื่อมต่อกับเครือข่ายของหน่วยงาน ต้องได้รับอนุมัติและขึ้นทะเบียนในทะเบียนสินทรัพย์เทคโนโลยีสารสนเทศ พร้อมกำหนดผู้รับผิดชอบหลักและวัตถุประสงค์การใช้งานให้ชัดเจน
- การออกแบบและแยกเครือข่ายของอุปกรณ์ดังกล่าวควรเชื่อมต่อภายในเครือข่ายที่แยกจากระบบงานหลักหรือระบบที่มีข้อมูลสำคัญ และต้องมีการกำหนดนโยบายควบคุมการเข้าถึงและการสื่อสารให้จำกัดเฉพาะที่จำเป็น
- ข้อกำหนดด้านความมั่นคงปลอดภัยขั้นต่ำ ก่อนใช้งานจริงต้องมีการตั้งค่าเริ่มต้นด้านความมั่นคงอย่างเหมาะสม อย่างน้อยให้เปลี่ยนรหัสผ่านเริ่มต้น ปิดบริการที่ไม่จำเป็น กำหนดสิทธิ์การเข้าถึงตามความจำเป็น และใช้ช่องทางการสื่อสารที่มีการเข้ารหัสตามความเหมาะสม
- การอัปเดตซอฟต์แวร์และเฟิร์มแวร์ หน่วยงานที่รับผิดชอบต้องติดตามและดำเนินการอัปเดตเฟิร์มแวร์หรือแพตช์ความปลอดภัยของอุปกรณ์อย่างสม่ำเสมอ ภายในระยะเวลาที่เหมาะสม โดยคำนึงถึงผลกระทบต่อการใช้งาน

- การเข้าถึงจากภายนอกและการควบคุมจากระยะไกล ให้การเข้าถึงอุปกรณ์จากภายนอกเครือข่าย หน่วยงาน หรือโดยผู้ให้บริการภายนอก ต้องผ่านช่องทางที่ปลอดภัยตามที่หน่วยงานกำหนด มีการจำกัดขอบเขตและระยะเวลา พร้อมบันทึกการเข้าถึงไว้เป็นหลักฐาน
- การเฝ้าระวัง บันทึก และตรวจสอบการใช้งาน ควรมีอุปกรณ์ที่รองรับการบันทึกเหตุการณ์ เปิดใช้การบันทึกและกำหนดให้นำส่งข้อมูล log ไปยังระบบกลาง เช่น Syslog หรือ SIEM (หากมี) ตามความเหมาะสม และให้มีการทบทวน log อย่างสม่ำเสมอ โดยเฉพาะเหตุการณ์การเข้าถึงจากภายนอก การเปลี่ยนแปลงค่าการตั้งค่า และเหตุผิดปกติ หากตรวจพบพฤติกรรมผิดปกติของอุปกรณ์ เช่น ส่งข้อมูลออกนอกเครือข่ายผิดปกติ ถูกสแกนพอร์ต หรือทำงานผิดปกติ ให้ดำเนินการตามขั้นตอนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของหน่วยงาน
- การเลิกใช้งานและการทำลายข้อมูล เมื่อยกเลิกการใช้งาน หรือจำหน่าย/โอนย้ายอุปกรณ์ ต้องดำเนินการลบหรือทำลายข้อมูลภายในอุปกรณ์ให้ไม่สามารถกู้คืนได้ตามมาตรฐานของหน่วยงาน และปรับปรุงทะเบียนสินทรัพย์ให้ถูกต้อง
- การฝึกอบรมและสร้างความตระหนักรู้ บุคลากรที่เกี่ยวข้องกับการจัดหา ติดตั้ง ดูแล หรือใช้งานอุปกรณ์ IoT และอุปกรณ์อัจฉริยะ ควรได้รับการอบรมหรือชี้แจงแนวปฏิบัติด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง และควรมีการประชาสัมพันธ์หรือให้ข้อมูลแก่ผู้ใช้ปลายทางอย่างสม่ำเสมอ เกี่ยวกับความเสี่ยง ข้อควรระวังในการใช้อุปกรณ์ดังกล่าว

5. การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

การใช้งานระบบเครือข่ายของบริษัท

- วัตถุประสงค์
เพื่อกำหนดมาตรการในการใช้งานระบบอินเทอร์เน็ตผ่านระบบเครือข่ายของบริษัท ให้เกิดประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้ผู้ใช้งานมีความตระหนัก ในการใช้งานเว็บไซต์ต่างๆ ผ่านระบบเครือข่ายของบริษัท
- แนวทางปฏิบัติ
 - ส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่าย เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy เป็นต้น

- เครื่องคอมพิวเตอร์ของบริษัท ก่อนทำการเชื่อมต่อระบบเครือข่าย ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการก่อน
- หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น
- ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของบริษัท
- ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของบริษัท ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของบริษัท
- ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดเพื่อปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
- ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำไปใช้งาน
- ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของบริษัท เพื่อประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมอันดี เว็บไซต์ที่มีเนื้อหาเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เว็บไซต์ที่เป็นภัยต่อสังคม เว็บไซต์ลามกอนาจาร เป็นต้น
- ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่นๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อบริษัท รวมทั้งจะต้องไม่กระทำการใด อันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่บริษัทกำหนดไว้อย่างเคร่งครัด

6. การควบคุมการเข้ารหัสข้อมูล (Cryptographic Control)

- วัตถุประสงค์

เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือการทำงานของระบบสารสนเทศในส่วนที่มีได้อำนาจหน้าที่เกี่ยวข้อง

- แนวทางปฏิบัติ

6.1 การบริหารจัดการข้อมูล

- ต้องมีการจัดลำดับชั้นความลับ ต้องมีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนดวิธีบริหารจัดการกับข้อมูลแต่ละประเภท รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญก่อนการยกเลิกหรือการนำกลับมาใช้ใหม่
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น การใช้ SSL(SecureSocket Layer) การใช้ VPN (Virtual Private Network) เป็นต้น
- ต้องมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ (Storage)นำเข้า (Input) ประมวลผล (Operate) และแสดงผล (Output) ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ (Distributed Database) หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน
- ควรมีมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม เป็นต้น หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

6.2 การควบคุมการกำหนดสิทธิ์ให้ผู้ใช้งาน (User Privilege)

- ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวข้องกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
- ต้องกำหนดสิทธิ์การใช้ข้อมูลและระบบสารสนเทศ เช่น สิทธิ์การใช้โปรแกรมระบบสารสนเทศ (Application System) สิทธิ์การใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

- ในกรณีที่มีความจำเป็นต้องใช้ User ที่มีสิทธิ์พิเศษ ต้องมีการควบคุมการใช้งานอย่างรัดกุม ทั้งนี้ ในการพิจารณาว่าการควบคุม User ที่มีสิทธิ์พิเศษมีความรัดกุมเพียงพอหรือไม่นั้น บริษัทจะใช้ปัจจัยประกอบการพิจารณาในภาพรวมดังต่อไปนี้

- ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่
- ควรควบคุมการใช้งานของผู้ใช้งานที่มีสิทธิ์พิเศษอย่างเข้มงวด เช่น จำกัดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
- ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ควรเปลี่ยนรหัสผ่านทุก 6 เดือน เป็นต้น

- ในกรณีที่ไม่มี การปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ ต้องมีมาตรการป้องกันการใช้งานโดยบุคคลอื่นที่ได้มีสิทธิ์และหน้าที่เกี่ยวข้อง เช่น กำหนดให้ผู้ใช้งานออกจากระบบงาน (Log Out) ในช่วงเวลาที่ไม่ได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์ เป็นต้น

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

- ในกรณีที่มีความจำเป็นต้องให้สิทธิ์บุคคลอื่น ให้มีสิทธิ์ใช้งานระบบสารสนเทศและระบบเครือข่ายในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

6.3 การควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน(Password)

- ต้องมีระบบตรวจสอบตัวตนจริงและสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบสารสนเทศที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมี User Account เป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้นบริษัทจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณา

พิจารณาในภาพรวม

- ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร (Alphabet + Numeric)
- ควรใช้อักขระพิเศษประกอบ เช่น : ; <> \$ @ # เป็นต้น
- สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือน ส่วนผู้ใช้งานที่มีสิทธิ์พิเศษ เช่น ผู้จัดการระบบ(System Administrator) และผู้ใช้งานที่ติดมากับระบบ(Default User) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 2 เดือน
- ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิม 3 ครั้งหลังสุด
- ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน หรือคาดเดาได้ง่าย เช่น "abcdef" "aaaaaa" "123456" "password" "P@ssword" เป็นต้น
- ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อนามสกุล วัน เดือน ปี เกิด ที่อยู่ เป็นต้น
- ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
- ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด(Logon Attempt-Retires) ซึ่งในทางปฏิบัติโดยทั่วไปให้อยู่ที่ 5 ครั้ง หากการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนดไว้ระบบงานหรือโปรแกรมจะไม่อนุญาตหรือระงับการใช้งาน

- ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (Default Password) หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที
- ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ไม่ควรจดใส่กระดาษแล้วติดไว้หน้าเครื่อง ทั้งนี้ ในกรณีที่มีการลวงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที
- สำหรับกรณีผู้ใช้งานมีการใช้งานร่วมกันลักษณะ SharedUsers Licenses เช่น ระบบ ERP เป็นต้น ทางผู้ดูแลจะมีการส่งอีเมลแจ้งเตือนผู้รับผิดชอบการใช้งานให้ทำการเปลี่ยนรหัสผ่านในการเข้าระบบงานนั้น เมื่อมีการเปลี่ยนแปลงของผู้ใช้งานในสังกัด
- ต้องมีระบบการเข้ารหัส (Encryption) ไฟล์ที่เก็บรหัสผ่านเพื่อป้องกันการลวงรู้หรือแก้ไขเปลี่ยนแปลง
- ต้องตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอและดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มีได้มีสิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของผู้ปฏิบัติงานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ (Default User) เป็นต้น พร้อมทั้งระงับการใช้งาน โดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือ เปลี่ยน รหัสผ่าน เป็นต้น

7. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

- วัตถุประสงค์

การควบคุมการเข้าออกห้องศูนย์กลางข้อมูล (Data Center Room) มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ แก้ไขเปลี่ยนแปลง หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ โดยมีเนื้อหาครอบคลุม

เกี่ยวกับแนวทางการควบคุมการเข้าออก Data Center Room และระบบป้องกันความเสียหายต่างๆ ที่บริษัทควรจัดให้มีภายใน Data Center Room

- แนวทางปฏิบัติ

- 0. การควบคุมห้องศูนย์กลางข้อมูล (Data Center Room)

- ต้องจัดเก็บอุปกรณ์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ใน Data Center Room หรือพื้นที่หวงห้าม และต้องกำหนดสิทธิ์การเข้าออก Data Center Room ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น ผู้ดูแลระบบ เป็นต้น
 - ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออก Data Center Room ในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุมเช่น กำหนดให้มีผู้ดูแลระบบ และ/หรือ ผู้ปฏิบัติงานที่เกี่ยวข้องควบคุมดูแลการทำงานตลอดเวลา เป็นต้น
 - ต้องมีระบบเก็บบันทึกการเข้าออก Data Center Room โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออกและควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
 - ควรจัด Data Center Room ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ส่วนเครื่องสำรองไฟฟ้า (UPS Zone) ส่วนแบตเตอรี่เครื่องสำรองไฟฟ้า (Battery UPS Zone) เป็นต้น เพื่อความสะดวกในการปฏิบัติงานและทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น

- 1. การป้องกันความเสียหาย

- ระบบป้องกันไฟไหม้
 - ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา
 - Data Center Room หลักต้องมีระบบดับเพลิงแบบอัตโนมัติสำหรับศูนย์คอมพิวเตอร์สำรอง อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

- ระบบป้องกันไฟฟ้าขัดข้อง
 - ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า
 - ต้องมีระบบสำรองไฟฟ้าสำหรับระบบงานคอมพิวเตอร์ที่สำคัญ และระบบเครือข่ายคอมพิวเตอร์ เพื่อให้การดำเนินงานมีความต่อเนื่อง
- ระบบควบคุมอุณหภูมิและความชื้น
 - ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม
- ระบบเตือนภัยน้ำรั่ว
 - ในกรณีที่มีการยกระดับพื้นที่ของ Data Center Room เพื่อติดตั้งระบบปรับอากาศ รวมทั้งเดินสายไฟและ/หรือ สายเครือข่ายด้านล่าง ควรติดตั้งระบบเตือนภัยน้ำรั่วบริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุ น้ำรั่วได้ทันเวลา หาก Data Center Room ตั้งอยู่ในสถานที่ ที่มีความเสี่ยงต่อภัยน้ำรั่วควรหมั่นสังเกตว่า มีน้ำรั่วหรือไม่อย่างสม่ำเสมอ

8. การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ (Operations Security)

- วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับระบบสารสนเทศของบริษัทเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย ป้องกันการสูญหายของข้อมูล และได้รับการปกป้องจากโปรแกรมไม่ประสงค์ดี
- แนวทางปฏิบัติ
 0. จัดทำคู่มือหรือขั้นตอนปฏิบัติงานเกี่ยวกับระบบสารสนเทศที่สำคัญของบริษัทเพื่อป้องกันความผิดพลาดในการปฏิบัติงานด้านสารสนเทศ
 1. กำหนดให้มีการควบคุมการเปลี่ยนแปลงสารสนเทศ เช่น ต้องมีการขออนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ เป็นต้น

2. ต้องมีการสำรองข้อมูลสารสนเทศก่อนการเปลี่ยนแปลงสารสนเทศ
3. ควรติดตั้งระบบเพื่อตรวจสอบติดตามทรัพยากรของระบบสารสนเทศ เช่น CPU Memory Hard Disk ว่าเพียงพอหรือไม่ และนำข้อมูลการตรวจสอบติดตามมาวางแผนการเพิ่มหรือลดทรัพยากรในอนาคต
4. ระบบที่มีความสำคัญสูง ควรแยกระบบการพัฒนาออกจากระบบการให้บริการจริง เพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต
5. ต้องสำรวจข้อมูล จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรองและความถี่ในการสำรองข้อมูล
6. ข้อมูลที่มีความสำคัญสูง ต้องจัดให้มีความถี่การสำรองมาก และการจัดให้มีการสำรองข้อมูลภายนอกบริษัท
7. ต้องทดสอบสภาพพร้อมใช้งานระบบสำรองของระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
8. ต้องมีมาตรการป้องกันโปรแกรมไม่ประสงค์ดี เช่น
 - เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องคอมพิวเตอร์แบบพกพาส่วนบุคคล ก่อนเชื่อมต่อระบบเครือข่ายของบริษัท ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์
 - ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการและโปรแกรมที่ใช้งานที่ได้มีการออก Patch และ/หรือ HotFix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลดจากเว็บไซต์ของเจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่
 - ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอีเมล จะต้องตรวจสอบไวรัส โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
 - ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ที่ทางบริษัทได้จัดเตรียมไว้ให้ หากต้องการติดตั้งซอฟต์แวร์อื่นนอกเหนือจากที่บริษัทเตรียมไว้ให้ ต้องแจ้งส่วนเทคโนโลยีสารสนเทศเพื่อตรวจสอบความปลอดภัยก่อนการติดตั้ง

9. การรักษาความมั่นคงปลอดภัยด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

- วัตถุประสงค์
เพื่อป้องกันข้อมูลสารสนเทศในเครือข่ายจากบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึง หรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศ
- แนวทางปฏิบัติ

0. การบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย (Network Security Management)

- กำหนดการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย
- ต้องจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้งานนอกที่ติดต่อกับบริษัท

1. การถ่ายโอนข้อมูล (Information Transfer)

- ต้องดำเนินการจัดทำข้อตกลงสำหรับการถ่ายโอนข้อมูล (Agreements on Information Transfer) โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
- ต้องมีการลงนามในสัญญาระหว่างบริษัทและหน่วยงานภายนอกว่าจะไม่เปิดเผยความลับของบริษัท (Non-Disclosure Agreement:NDA)

10. การจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ (System Acquisition, Development And Maintenance)

- วัตถุประสงค์
การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศมีวัตถุประสงค์เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity Risk โดยมีเนื้อหาครอบคลุม

กระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอจนถึงการนำระบบงานที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

- แนวทางปฏิบัติ

0. ควรมีขั้นตอนหรือวิธีปฏิบัติในการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานเป็นลายลักษณ์อักษร โดยอย่างน้อยควรมีข้อกำหนดเกี่ยวกับขั้นตอนในการร้องขอ ขั้นตอนในการพัฒนาหรือแก้ไขเปลี่ยนแปลง ขั้นตอนในการทดสอบและขั้นตอนในการโอนย้ายระบบงาน

1. ควรมีขั้นตอนหรือวิธีปฏิบัติในกรณีที่มีการแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในกรณีฉุกเฉิน (Emergency Change) และควรมีการบันทึกเหตุผลความจำเป็นและขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง

2. ควรสื่อสารเกี่ยวกับรายละเอียดของขั้นตอนดังกล่าวให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง พร้อมทั้งควบคุมให้มีการปฏิบัติตาม

3. กรณีมีการพิจารณา ทดลองใช้ และนำเทคโนโลยีเกิดใหม่มาใช้ในหน่วยงาน (Emerging Technologies) ซึ่งเป็นเทคโนโลยีใหม่หรือเทคโนโลยีที่มีการเปลี่ยนแปลงรวดเร็ว เช่น เทคโนโลยีคลาวด์ ปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง เทคโนโลยี IoT หุ่นยนต์และกระบวนการอัตโนมัติ Big Data and Analytics บล็อกเชน และเทคโนโลยีดิจิทัลอื่นๆ ที่เห็นสมควร ให้มีแนวปฏิบัติดังนี้

- การติดตามและคัดเลือกเทคโนโลยี หน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ ควรติดตามแนวโน้มเทคโนโลยีเกิดใหม่จากแหล่งข้อมูลที่เชื่อถือได้อย่างสม่ำเสมอ หากเป็นการคัดเลือกเทคโนโลยีเกิดใหม่เพื่อศึกษา หรือนำมาใช้ ต้องพิจารณาความสอดคล้องกับยุทธศาสตร์และภารกิจขององค์กร รวมทั้งประเมินความพร้อมของโครงสร้างพื้นฐานและบุคลากร

- การทดลองใช้เทคโนโลยี (Pilot / Sandbox) ก่อนนำเทคโนโลยีเกิดใหม่มาใช้ในระบบงานจริง ควรดำเนินการทดลองใช้ในสภาพแวดล้อมที่ควบคุมได้และแยกจากระบบงานหลัก และในการทดลองใช้หากเกี่ยวข้องกับข้อมูลส่วนบุคคล ควรใช้ข้อมูลสมมติ หรือดำเนินการลดทอนการระบุตัวบุคคลตามความเหมาะสม ทั้งนี้ต้องมีการประเมินผลการทดลอง ทั้งด้านประสิทธิภาพ ความปลอดภัย และผลกระทบต่อกระบวนการทำงาน ก่อนตัดสินใจนำไปใช้จริง

- การประเมินความเสี่ยงและผลกระทบของโครงการที่เกี่ยวข้องกับเทคโนโลยีเกิดใหม่ต้องผ่านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามกระบวนการบริหารความเสี่ยงที่กำหนดไว้ ผลการประเมินความเสี่ยงต้องถูกนำมาใช้กำหนดมาตรการควบคุมและเงื่อนไขการใช้งานเทคโนโลยีนั้น
- หากเทคโนโลยีที่นำมาใช้มีการประมวลผลข้อมูลส่วนบุคคลในลักษณะที่อาจมีความเสี่ยงสูง ให้พิจารณาดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้อง
- เทคโนโลยีเกิดใหม่ที่นำมาใช้ต้องมีมาตรการพื้นฐานด้านความมั่นคงปลอดภัย ได้แก่ การพิสูจน์ตัวตนและกำหนดสิทธิ์ การเข้ารหัสข้อมูล การบันทึกและติดตามเหตุการณ์ และการสำรองและกู้คืนข้อมูลตามความเหมาะสม
- กรณีใช้บริการจากผู้ให้บริการภายนอก เช่น บริการคลาวด์หรือบริการ AI ควรกำหนดเงื่อนไขด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลไว้ในสัญญาอย่างชัดเจน
- กรณีใช้เทคโนโลยีคลาวด์ ให้กำหนดประเภทและระดับของข้อมูลที่อนุญาตให้จัดเก็บบนคลาวด์ พร้อมทั้งกำหนดเงื่อนไขการย้าย เปลี่ยน หรือยกเลิกผู้ให้บริการ
- กรณีใช้เทคโนโลยีปัญญาประดิษฐ์ ให้คำนึงถึงคุณภาพของข้อมูล ความโปร่งใสในกระบวนการประมวลผล ตลอดจนที่ไม่เป็นธรรมต่อบุคคล กลุ่มบุคคล
- ในกรณีที่เทคโนโลยีอาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่น การวิเคราะห์พฤติกรรมหรือการตัดสินใจโดยอัตโนมัติ ต้องพิจารณาประเด็นด้านจริยธรรม ความเป็นธรรม และความโปร่งใสเป็นพิเศษ
- การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงาน
 0. การร้องขอ
 - การร้องขอให้มีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ ต้องจัดทำเป็นลายลักษณ์อักษร โดยอาจเป็น Electronic Transaction เช่น อีเมล

เป็นต้น และได้รับอนุมัติจากผู้มีอำนาจหน้าที่ เช่น หัวหน้าส่วนงานที่ร้องขอ หรือ ผู้รับผิดชอบระบบสารสนเทศ เป็นต้น

- ควรมีการประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และ การทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง
- ควรสอบทานกฎเกณฑ์ของทางที่เกี่ยวข้อง เนื่องจากการแก้ไขเปลี่ยนแปลง ในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของทาง

1. การปฏิบัติงานพัฒนาระบบงาน

- ต้องแบ่งแยกส่วนคอมพิวเตอร์ที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) ออกจากส่วนที่ใช้งานจริง (Production Environment) และ ควบคุมให้มีการเข้าถึงเฉพาะผู้ที่เกี่ยวข้องในแต่ละส่วนเท่านั้น ทั้งนี้ การแบ่งแยกส่วน ดังกล่าวอาจแบ่งโดยใช้เครื่องคอมพิวเตอร์คนละเครื่อง หรือแบ่งโดยการจัดเนื้อที่ไว้ ภายในเครื่องคอมพิวเตอร์เดียวกันก็ได้
- ผู้ที่ร้องขอ รวมทั้งผู้ใช้งานที่เกี่ยวข้อง ควรมีส่วนร่วมในกระบวนการพัฒนาหรือ แก้ไขเปลี่ยนแปลงเพื่อให้พัฒนาระบบงานได้ตรงกับความต้องการ
- ควรตระหนักถึงระบบรักษาความปลอดภัย (Security) และเสถียรภาพการทำงาน (Availability) ของระบบงานตั้งแต่ในช่วงเริ่มต้นของการพัฒนา หรือการ แก้ไขเปลี่ยนแปลง

2. การทดสอบ

- ผู้ที่ร้องขอและส่วนเทคโนโลยีสารสนเทศ รวมทั้งผู้ใช้งานอื่นที่เกี่ยวข้องต้องมีส่วนร่วมในการทดสอบ เพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้อง ครบถ้วน และเป็นไปตามความต้องการก่อนที่จะโอนย้ายไปใช้งานจริง

3. การโอนย้ายระบบงานเพื่อใช้งานจริง

- ต้องตรวจสอบการโอนย้ายระบบงานให้ถูกต้องครบถ้วนเสมอ

4. การจัดทำเอกสารและรายละเอียดประกอบการพัฒนาระบบงาน และจัดเก็บ Version ของระบบงานที่ได้รับการพัฒนา

- ต้องจัดให้มีการเก็บข้อมูลรายละเอียดเกี่ยวกับโปรแกรมที่ใช้อยู่ในปัจจุบัน ซึ่งมีรายละเอียดเกี่ยวกับการพัฒนา หรือแก้ไขเปลี่ยนแปลงที่ผ่านมา
- ต้องปรับปรุงเอกสารประกอบระบบงานทั้งหมดหลังจากที่ได้พัฒนาหรือแก้ไขเปลี่ยนแปลงเพื่อให้ทันสมัยอยู่เสมอ เช่น เอกสารประกอบรายละเอียดโครงสร้างข้อมูล คู่มือระบบงาน ทะเบียนรายชื่อผู้มีสิทธิ์ใช้งาน เป็นต้น และต้องจัดเก็บเอกสารดังกล่าวในที่ปลอดภัยและสะดวกต่อการใช้งาน
- ต้องจัดเก็บโปรแกรม Version ก่อนการพัฒนาไว้ใช้งานในกรณีที่ Version ปัจจุบันทำงานผิดพลาดหรือไม่สามารถใช้งานได้

5. การทดสอบหลังการใช้งาน (Post-Implementation Test)

- ควรกำหนดให้มีการทดสอบระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงหลังจากที่ได้ใช้งานระยะหนึ่ง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน

6. การสื่อสารการเปลี่ยนแปลง

- ต้องสื่อสารการเปลี่ยนแปลงให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้ถูกต้อง

11. การใช้บริการระบบสารสนเทศจากผู้รับดำเนินการ (IT Outsourcing)

• วัตถุประสงค์

เพื่อเป็นการป้องกันสินทรัพย์ของบริษัทที่มีการเข้าถึงโดย IT Outsourcing และมีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ

• แนวทางปฏิบัติ

0. ต้องจัดทำข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัทเมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท โดยสอดคล้องกับข้อกำหนดเกี่ยวกับการรักษาความลับข้อมูลของบริษัท

1. ต้องสื่อสาร และบังคับใช้ข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับข้อมูลของบริษัท เมื่อมีความจำเป็นต้องให้ IT Outsourcing เข้าถึงข้อมูลหรือสินทรัพย์ของบริษัท ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้
2. ในข้อตกลงการให้บริการ ต้องกำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการภายนอกอย่างสม่ำเสมอ
3. หากมีการเปลี่ยนแปลงข้อตกลงการให้บริการสำหรับระบบที่สำคัญ จะต้องทำการประเมินความเสี่ยงด้านความมั่นคงปลอดภัย

12. การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Incident Management)

- วัตถุประสงค์

เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ รวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศ และจุดอ่อนของความมั่นคงปลอดภัยของระบบสารสนเทศให้ได้รับทราบ

- แนวทางปฏิบัติ

0. ต้องกำหนดหน้าที่รับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของบริษัท
1. ต้องกำหนดช่องทางการติดต่อสื่อสาร เพื่อรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน
2. หากผู้ใช้งานตรวจพบเหตุอันอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ต้องแจ้งเหตุการณ์ดังกล่าวต่อส่วนเทคโนโลยีสารสนเทศ
3. กำหนดให้มีการรายงานสถานการณ์ความมั่นคงปลอดภัยของระบบสารสนเทศตามระดับความรุนแรงของเหตุการณ์ หากส่งผลกระทบรุนแรงต่อผู้ใช้งานเป็นจำนวนมาก ต้องประกาศให้ทราบโดยรวดเร็ว
4. ต้องมีการบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายที่เกิดจากความเสียหาย เพื่อที่จะได้เรียนรู้และเตรียมการป้องกัน

5. ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหมายหรือหลักเกณฑ์สำหรับอ้างอิงในกระบวนการทางศาล

13. การบริหารความต่อเนื่องทางธุรกิจในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security Aspects of Business Continuity Management)

- วัตถุประสงค์

เพื่อเป็นการป้องกันการหยุดชะงักในการดำเนินงานของบริษัท อันเกิดมาจากวิกฤตหรือภัยพิบัติ และเป็นการจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ระบบสารสนเทศของบริษัท

- แนวทางปฏิบัติ

0. ส่วนเทคโนโลยีสารสนเทศ ต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดขึ้นกับระบบสารสนเทศ ตามแผนบริหารภาวะวิกฤต (Crisis Management Plan) ของบริษัท
1. ต้องดำเนินการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้นอย่างน้อย ปีละ 1 ครั้ง
2. ต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง
3. ต้องมีการตรวจสอบสภาพความพร้อมใช้งานของระบบสารสนเทศสำรองอย่างน้อยปีละ 1 ครั้ง

นโยบายฉบับนี้อนุมัติโดยคณะกรรมการบริษัทเมื่อวันที่ 29 ธันวาคม 2568



ลงชื่อ.....

(นายมนตรี มหาพฤกษ์พงศ์)

ประธานคณะกรรมการบริษัท

บริษัท พรีเมียร์ควอลิตี้สตาร์ช จำกัด(มหาชน)