บริษัท ผลิตไฟฟ้า จำกัด (มหาชน)

นโยบายด้านความมั่นคงปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์

รหัสเอกสาร :	SP-0123-0001
หมายเลขปรับปรุงเอกสาร :	1.0
วันที่เอกสารมีผลบังคับใช้ :	1 ตุลาคม 2564
เจ้าของเอกสาร :	ฝ่ายเทคโนโลยีสารสนเทศ
ผู้อนุมัติเอกสาร :	กุลิศ สมบัติศิริ

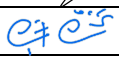
ประวัติการปรับปรุงเอกสาร

เวอร์ชั่น	คำอธิบายและเหตุผลในการแก้ไข	ผู้แก้ไข	วันที่
1.0	เอกสารเผยแพร่ฉบับแรก		

หมายเลขข้อปฏิบัติสอดคล้องตามมาตรฐาน ISO/IEC 27001:2013

ขั้นตอนปฏิบัติในเอกสารฉบับนี้ได้รับการจัดทำขึ้นเพื่อให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2013 ข้อ 5.2 และ ข้อ A.5 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ สอดคล้องตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ	ลายเซ็น	ตำแหน่ง	วันที่
จัดทำโดย	บุญโชติ บุญเกื้อ		ผู้จัดการส่วนพัฒนาระบบคอมพิวเตอร์	20 กันยายน 64
ตรวจทาน	วุฒิรัฐ จึงแสงสถิตย์พร		ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ	22 กันยายน 64
อนุมัติโดย	กุลิศ สมบัติศิริ	ท้ายเอกสาร	ประธานกรรมการ	24 กันยายน 64

1. บทนำ

บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) และบริษัทย่อยที่จดทะเบียนในประเทศไทยซึ่งอยู่ภายใต้การควบคุมของบริษัท ผลิตไฟฟ้า จำกัด (มหาชน) (รวมเรียกว่า “บริษัท”) ได้จัดให้มีระบบเทคโนโลยีสารสนเทศ ขึ้นเพื่อสนับสนุนให้บุคลากรสามารถปฏิบัติงานได้บรรลุวัตถุประสงค์ เป้าหมายในการดำเนินธุรกิจและสอดคล้องกับหลักการกำกับดูแลกิจการที่ดี มีการใช้งาน จัดทำข้อมูล จัดเก็บข้อมูล และการบริหารจัดการระบบเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ เพื่อให้เกิดประโยชน์สูงสุด เป็นธรรม และสอดคล้องกับกฎหมายที่เกี่ยวข้อง โดยตระหนักว่าข้อมูลสารสนเทศเป็นทรัพยากรที่มีความสำคัญ เราจึงมุ่งมั่นที่จะปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล รวมถึงการทบทวนเพื่อพัฒนาการปฏิบัติตามข้อกำหนดการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างสม่ำเสมอ

1.1. วัตถุประสงค์

นโยบายความมั่นคงปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์จัดทำขึ้นตามกรอบของมาตรฐาน ISO/IEC 27001:2013 และสอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีวัตถุประสงค์ดังนี้

1. เพื่อกำหนดทิศทางและให้การสนับสนุนการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนเป็นแนวทางการเข้าถึงข้อมูลสารสนเทศ และระบบเทคโนโลยีสารสนเทศของบริษัทให้เป็นไปอย่างเหมาะสมและมีการพัฒนาอย่างต่อเนื่อง โดยสอดคล้องกับกฎหมาย และข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง
2. เพื่อให้บุคลากรในบริษัท ตลอดจนบุคคลอื่นใดที่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศรับทราบ เข้าใจและปฏิบัติตามนโยบาย ได้อย่างถูกต้อง เหมาะสม และปลอดภัย
3. เพื่อปกป้องสารสนเทศให้ปลอดภัยจากความสูญเสียในรูปแบบต่างๆ เช่น การสูญหาย การถูกทำลาย การแก้ไขโดยไม่ได้รับอนุญาต การลักลอบนำข้อมูลไปใช้หรือเปิดเผย ตลอดจนสร้างความมั่นใจว่าระบบสารสนเทศมีความมั่นคงปลอดภัย น่าเชื่อถือ และสามารถให้บริการได้อย่างต่อเนื่อง

1.2. ขอบเขตของเอกสาร

บริษัทกำหนดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท และต้องมีการประกาศใช้สำหรับคณะกรรมการบริษัท พนักงาน ลูกจ้าง เจ้าหน้าที่ หรือหน่วยงานภายนอก ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัท เพื่อให้มีความเข้าใจและปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้

1.3. ระยะเวลาทบทวน

บริษัทจัดให้มีการปรับปรุงและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูล (Review of the policies for information security) อย่างสม่ำเสมอ เพื่อให้การรักษาความมั่นคงปลอดภัยสารสนเทศคงความถูกต้อง สมบูรณ์ และความพร้อมใช้งาน โดยสอดคล้องเหมาะสมกับการเปลี่ยนแปลงและความต้องการทางธุรกิจของบริษัทให้เป็นปัจจุบัน อย่างน้อยปีละ 1 ครั้ง

1.4. นิยามหรือคำจำกัดความ

1) “บริษัท/องค์กร” หมายถึง บริษัท ผลิตไฟฟ้า จำกัด (มหาชน) และบริษัทย่อยที่จดทะเบียนในประเทศไทย ซึ่งอยู่ภายใต้การควบคุมของบริษัท ผลิตไฟฟ้า จำกัด (มหาชน)

2) “ผู้บังคับบัญชา/ผู้บริหาร” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของบริษัท
3) “พนักงาน (Employee)” หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท
4) “ผู้ใช้งาน (User)” หมายถึง พนักงานของบริษัท รวมไปถึงบุคคลภายนอกบริษัทที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งาน หรือ/และ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของบริษัท
5) “หน่วยงานภายนอก (External Party)” หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ เช่น
   – บริษัทคู่ค้า (Business Partner)
   – ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource)
   – ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ (Supplier)
   – ผู้ให้บริการต่าง ๆ (Service Provider)
   – ที่ปรึกษา (Consultant)
6) “ข้อมูลสารสนเทศ” ซึ่งต่อไปนี้เรียกว่า “ข้อมูล” หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่างๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
7) “สื่อบันทึกข้อมูล” หมายถึง ข้อมูลอิเล็กทรอนิกส์ที่เก็บอยู่ในสื่อบันทึก เช่น แผ่นซีดี เทปแม่เหล็ก แฟลชไดร์ฟ ฮาร์ดิส เป็นต้น
8) “เครื่องผู้ใช้งาน (Endpoint Devices)” หมายถึง อุปกรณ์ประมวลผลปลายทางที่ผู้ใช้งานใช้ในการเข้าถึงระบบสารสนเทศ เช่น เครื่องคอมพิวเตอร์ แท็บเล็ต สมาร์ทโฟน หรือเครื่องคอมพิวเตอร์แบบพกพา
9) “ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายถึง ระบบงานของบริษัท ที่นำเอาเทคโนโลยีสารสนเทศ ระบบสารสนเทศ เครื่องคอมพิวเตอร์ เครื่องแม่ข่ายและระบบเครือข่ายมาช่วยในการสร้างข้อมูลสารสนเทศ
10) “สิทธิของผู้ใช้งาน” หมายถึง ระดับสิทธิที่ได้รับในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร เช่น สิทธิผู้ใช้งานระดับสูงสำหรับใช้ในการจัดการระบบต่างๆ (Admin Access right) สิทธิของผู้ใช้งานทั่วไป (User Access right) เป็นสิทธิพื้นฐานสำหรับใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร และสิทธิเฉพาะกลุ่ม (Special access right) เป็นสิทธิที่กำหนดการใช้งานแบบเฉพาะเจาะจงของแต่ละผู้ใช้งานตามความจำเป็นในการเข้าถึงระบบนั้นๆ เป็นต้น
11) “ข้อตกลงระดับบริการ” หมายถึง ข้อตกลงระดับในการให้บริการ ระหว่างผู้ให้บริการ และ ผู้รับบริการ ประกอบไปด้วย หน้าที่และข้อจำกัดของการบริการ ระยะเวลาในการให้บริการ เงื่อนไขการยกเลิกข้อตกลง เพื่อให้มั่นใจได้ว่าทั้งสองฝ่ายจะได้รับการปฏิบัติตามข้อตกลงอย่างสม่ำเสมอ
12) “การรักษาความมั่นคงปลอดภัย” หรือ “ความมั่นคงปลอดภัย (Security)” หมายถึง กระบวนการ และการกระทำใดๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจากความพยายามใดๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอก ในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินธุรกิจของบริษัท ได้รับความเสียหาย

13) “ภัยคุกคาม” หมายถึง ภัยที่ก่อให้เกิดผลเสียหายต่อบริษัท ซึ่งอาจเกิดจากธรรมชาติหรือมนุษย์ทั้งที่มาจากความตั้งใจหรือไม่ตั้งใจก็ตาม

14) “ช่องโหว่” หมายถึง จุดอ่อนของระบบเทคโนโลยีสารสนเทศ หรือสินทรัพย์ขององค์กร หรือจุดอ่อนจากมาตรการควบคุมหรือกระบวนการที่ไม่มีประสิทธิภาพเพียงพอ ทำให้สามารถใช้เป็นประโยชน์ในการทำให้เกิดความเสียหายต่อบริษัทได้

15) “ช่องโหว่ทางเทคนิค” หมายถึง จุดอ่อนของระบบเทคโนโลยีสารสนเทศ ที่มิจฉาชีพใช้คุกคามเพื่อทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศของบริษัท

16) “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบสารสนเทศ ทั้งทางการเข้าถึงระบบเทคโนโลยีสารสนเทศและทางกายภาพ รวมทั้งการอนุญาตตามที่กล่าวมาข้างต้น สำหรับบุคคลภายนอก รวมถึงการกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงระบบโดยมิชอบเอาไว้ด้วย

17) “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิด หรือ เหตุละเมิดด้านความมั่นคงปลอดภัย (Security Incident)” ซึ่งต่อไปนี้เรียกว่า “เหตุละเมิด”หมายถึง เหตุการณ์หนึ่งหรือหลายๆ เหตุการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่คาดคิดว่าจะเกิดขึ้น (Unwanted/Unexpected) โดยเหตุการณ์ดังกล่าวมีความเป็นไปได้ที่เกิดจากการบุกรุกหรือโจมตีการดำเนินการ และคุกคามต่อความมั่นคงปลอดภัยสารสนเทศหรือความมั่นคงปลอดภัยไซเบอร์

18) “ความเสี่ยงเกี่ยวกับการรักษาความปลอดภัยสารสนเทศ” หมายถึง เหตุการณ์ใดที่อาจเกิดขึ้นในอนาคต และมีผลกระทบต่อการรักษาความลับ (Confidentiality) ความครบถ้วนถูกต้อง (Integrity) หรือความพร้อมใช้งาน (Availability) ของระบบสารสนเทศของบริษัท

19) “ไซเบอร์” (Cyber) หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการ หรือ การประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเตอร์เน็ต หรือโครงข่ายสารสนเทศของบริษัท ที่เชื่อมต่อใช้ภายในองค์กรและติดต่อกับบุคคลภายนอก

20) “ความเสี่ยงเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์” หมายถึงเหตุการณ์ใดที่อาจเกิดขึ้นในอนาคต อันเนื่องมาจากภัยคุกคามทางไซเบอร์ ที่อาศัยจุดอ่อนและช่องโหว่ต่างๆ ที่มีเพื่อใช้เป็นประโยชน์ในการช่องทางเข้าโจมตีระบบงาน อุปกรณ์ด้านเทคโนโลยี และระบบเครือข่ายส่งผลกระทบต่อระบบบริการและระบบสารสนเทศของบริษัท

21) “การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ

2. กลยุทธ์การป้องกันความปลอดภัยของข้อมูล (Information Security Protection Strategy)

2.1. หลักการรักษาความมั่นคงปลอดภัยของข้อมูล (Security Principles)

การรักษาความมั่นคงปลอดภัยของข้อมูลนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

- ความลับ (Confidentiality) คือ การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัท
- ความถูกต้องสมบูรณ์ (Integrity) คือ การทำให้มั่นใจว่าข้อมูลสารสนเทศ ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต

- ความพร้อมใช้งาน (Availability) คือ การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้
- ความรับผิดชอบ (Accountability) คือ การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้นๆ
- การพิสูจน์ตัวตน (Authentication) คือ การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น
- การกำหนดสิทธิ (Authorization) คือ การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต

2.2. การบริหารจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ (Information Security and Cybersecurity Risk Management)

การบริหารความเสี่ยงเป็นความรับผิดชอบร่วมกันของผู้บริหารและพนักงานทุกระดับ และต้องมีการปฏิบัติอย่างต่อเนื่อง
โดยกระบวนการบริหารความเสี่ยงต้องประกอบด้วยขั้นตอนหลัก ดังนี้

- การกำหนดเป้าหมายด้านความปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์
- การระบุความเสี่ยงที่อาจเกิดขึ้นและมีผลกระทบต่อการรักษาความปลอดภัยข้อมูล
- การประเมินความเสี่ยง
- การจัดการและการบรรเทาความเสี่ยง
- การติดตามผลและการรายงาน

3. การบังคับใช้นโยบายด้านความมั่นคงปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์

นโยบายนี้มีผลบังคับใช้ภายในบริษัท โดยคลอบคลุมประเด็นด้านมั่นคงความปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัท

3.1. การบังคับใช้นโยบาย

การประกาศใช้นโยบายด้านความมั่นคงปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีการประกาศให้ผู้เกี่ยวข้องทราบเพื่อปฏิบัติได้อย่างเหมาะสม โดยผู้บังคับบัญชาตามสายงานตั้งแต่ระดับฝ่ายขึ้นไป มีหน้าที่รับผิดชอบในการจัดทำมาตรการควบคุมที่เหมาะสมเพื่อให้สอดคล้องกับนโยบายด้านความปลอดภัยสารสนเทศ ภายใต้ขอบเขตความรับผิดชอบของตน และให้มีการตรวจสอบมาตการควบคุมความปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบอิสระ

3.2. การจัดการมาตรการควบคุมด้านเทคนิคที่ล้าสมัย (Handling of Technical Controls Obsolescence)

ในกรณีที่มีการใช้มาตรการควบคุมด้านเทคนิคที่ล้าสมัยหรือกำลังจะล้าสมัย เนื่องจากข้อจำกัดของระบบหรืออุปกรณ์ บริษัทต้องกำหนดระยะเวลาที่อนุญาตให้ใช้งานเทคนิคที่ล้าสมัยหรือกำลังจะล้าสมัย ก่อนการปรับปรุงหรือเปลี่ยนแปลงเพื่อให้มีการควบคุมการใช้งานมาตรการทางเทคนิคที่ล้าสมัยหรือกำลังจะล้าสมัยอย่างเหมาะสม

3.3. การจัดการมาตรการที่ได้รับการยกเว้น (Handling of Policy Deviations)

หากมีความจำเป็นที่ต้องใช้บางมาตรการควบคุมที่ไม่เป็นไปตามนโยบายการรักษาความปลอดภัยข้อมูลและการรักษาความมั่นคงปลอดภัยไซเบอร์ ผู้บังคับบัญชาตามสายงานที่เกี่ยวข้องกับมาตรการควบคุมที่ได้รับการยกเว้นนั้น ต้องทบทวนและพิจารณาความเสี่ยงในการใช้มาตรการควบคุมดังกล่าวเป็นประจำทุกปี

4. แนวนโยบายความมั่นคงปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ (Policy Directives)

แนวนโยบายหรือมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ มีดังนี้

4.1. การจัดการด้านความปลอดภัย (General Security Management)

วัตถุประสงค์: เพื่อให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องด้านความปลอดภัยสารสนเทศ การยอมรับนโยบายในการใช้ข้อมูลสารสนเทศ และสร้างความตระหนักถึงการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานอย่างเหมาะสม

- บริษัทต้องระบุข้อกำหนดและหน้าที่รับผิดชอบด้านความปลอดภัยสารสนเทศ โดยสอดคล้องกับระเบียบ คำสั่ง หรือกฎหมายที่เกี่ยวข้อง
- บริษัทต้องมีการจัดระดับชั้นของข้อมูลแต่ละประเภท ตามวัตถุประสงค์ในการใช้งาน การเก็บรวบรวม การเปิดเผยข้อมูลนั้น โดยต้องกำหนดมาตรการที่เหมาะสมในการจัดเก็บและป้องกันข้อมูลดังกล่าว
- ผู้ใช้งานที่สามารถเข้าถึงข้อมูลและระบบสารสนเทศของบริษัท จะต้องรับทราบและยอมรับ นโยบายการใช้งานด้านความมั่นคงปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ และข้อกำหนดอื่นๆ ของบริษัทที่เกี่ยวข้อง
- ผู้ใช้งานต้องปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ และควรทำความเข้าใจหรือได้รับการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความปลอดภัยของข้อมูลอย่างสม่ำเสมอ
- การแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก ต้องจัดทำและทบทวนข้อตกลงการรักษาความลับและการไม่เปิดเผยข้อมูลให้เป็นปัจจุบัน ทั้งนี้ต้องกำหนดมาตรการควบคุมการเข้าถึงข้อมูลให้เหมาะสม
- ผู้ใช้งานต้องตระหนักถึงหน้าที่ในการปกป้องทรัพย์สินทางปัญญา และเมื่อพบเหตุการณ์ด้านความปลอดภัยของข้อมูลของบริษัทต้องรายงานไปยังผู้เกี่ยวข้องโดยเร็วที่สุด

4.2. การจัดการเครื่องผู้ใช้งาน (Endpoint Management)

วัตถุประสงค์: เพื่อให้มีมาตรการควบคุมที่เหมาะสม ในการเข้าใช้งานระบบสารสนเทศผ่านเครื่องผู้ใช้งาน

บริษัทต้อง

- กำหนดมาตรการควบคุมด้านความปลอดภัยของข้อมูล และความปลอดภัยทางไซเบอร์สำหรับอุปกรณ์ที่ใช้ในการดำเนินงานของบริษัทอย่างเหมาะสม ทั้งนี้มีผลบังคับใช้คลอบคลุมถึงอุปกรณ์ที่ทำงานจากระยะไกลด้วย เพื่อป้องกันการโจมตีจากภายนอก
- กำหนดวิธีการพิสูจน์ตัวตนก่อนเข้าสู่ระบบสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- มีการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ใช้งานที่เหมาะสม เพื่อช่วยให้ผู้ใช้งานระมัดระวัง และหลีกเลี่ยงความเสี่ยงจากการใช้งานที่ไม่ถูกต้อง

- กำหนดมาตรการควบคุมความปลอดภัย ซึ่งบังคับใช้กับการใช้อุปกรณ์ของบริษัทและอุปกรณ์ส่วนบุคคลที่นำมาลงทะเบียนเพื่อใช้ในการดำเนินงานของบริษัท เพื่อป้องกันไม่ให้ข้อมูลที่เก็บอยู่ในอุปกรณ์เหล่านี้ถูกนำไปใช้ในทางที่ผิด หรือเพื่อผลประโยชน์ส่วนตัว
- กำหนดให้มีการสำรองข้อมูลของบริษัทให้เหมาะสม เพื่อป้องกันไม่ให้ข้อมูลสูญหายอันเนื่องมาจากภัยพิบัติที่มนุษย์สร้างขึ้นหรือภัยธรรมชาติ

4.3. ความมั่นคงปลอดภัยของทรัพยากรบุคคล (Human Resource Security)

วัตถุประสงค์: เพื่อกำหนดวิธีการให้มั่นใจว่าพนักงานที่ปฏิบัติงาน เข้าใจหน้าที่และความรับผิดชอบของตน รวมถึงการสรรหาบุคลากรที่มีความเหมาะสมกับบทบาทที่ได้รับมอบหมาย

บริษัทต้องกำหนด

- ให้พนักงานทุกคนต้องผ่านกระบวนการกลั่นกรองเพื่อพิจารณาความเหมาะสมของตำแหน่งก่อนการจ้างงาน
- ให้พนักงานที่ปฏิบัติงานภายในบริษัท มีความตระหนักรู้ และปฏิบัติงานโดยคำนึงถึงการรักษาความมั่งคงปลอดภัยของข้อมูล
- หากพนักงานละเมิดด้านความปลอดภัยของข้อมูล จะถูกลงโทษทางวินัยตามแนวปฏิบัติของบริษัท
- ให้มีการปรับปรุงสิทธิให้ถูกต้องทันที เมื่อมีการปรับเปลี่ยนหน้าที่ภายในบริษัท หรือเมื่อพนักงานพ้นสภาพ โดยสอดคล้องกับการเปลี่ยนแปลงหน้าที่ที่เกี่ยวข้อง เช่น ยกเลิกสิทธิการเข้าถึงระบบทันทีเมื่อพนักงานพ้นสภาพ หรือปรับปรุงสิทธิการเข้าถึงระบบตามหน้าที่ที่ได้รับมอบหมาย

4.4. การจัดการความปลอดภัยทางกายภาพ (Physical Security and Environmental Management)

วัตถุประสงค์: เพื่อป้องกันการเข้าถึงทางกายภาพโดยมิได้รับอนุญาต ความเสียหาย การแทรกแซงการทำงานของข้อมูลและอุปกรณ์

บริษัทต้อง

- กำหนดบริเวณพื้นที่ที่มีความเสี่ยงที่แตกต่างกันอย่างชัดเจน โดยพิจารณาจากการเข้าถึงของผู้ใช้งาน ทั้งในระบบสารสนเทศทั่วไปและระบบเทคโนโยลีสารสนเทศที่มีความสำคัญสูง และกำหนดมาตรการป้องกันบริเวณที่เหมาะสมตามความสำคัญของพื้นที่นั้นๆ
- กำหนดมาตรการควบคุมความปลอดภัยทางกายภาพ รวมถึงการป้องกันการเข้าออกทางกายภาพ และจำกัดการเข้าออกภายในพื้นที่ที่สำคัญ เพื่อป้องกันการเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต ซึ่งอาจสร้างความเสียหายหรือเกิดการแทรกแซงข้อมูลของบริษัทและอุปกรณ์ประมวลผลข้อมูลได้
- ตรวจสอบกระบวนการควบคุมเพื่อบริหารจัดการพนักงาน และหน่วยงานภายนอกที่ได้รับอนุญาตให้เข้ามาปฏิบัติงานภายในพื้นที่ได้อย่างเหมาะสม
- มีการบำรุงรักษาระบบควบคุมและป้องกันพื้นที่เป็นประจำ เพื่อปกป้องชีวิตและทรัพย์สินภายในพื้นที่ดังกล่าว โดยดำเนินมาตรการป้องกันพื้นที่อย่างเหมาะสมและเพียงพอจากอุบัติเหตุ และลดการหยุดชะงักของบริการและระบบสาธารณูปโภคที่จำเป็นสำหรับการดำเนินงานของบริษัท

4.5. ความปลอดภัยและการบำรุงรักษาอุปกรณ์ (Equipment Security and Maintenance)

วัตถุประสงค์: เพื่อป้องกันการสูญหาย ความเสียหาย การขโมยหรือเป็นอันตรายต่อทรัพย์สิน และการป้องกันการหยุดชะงักต่อการปฏิบัติงานของบริษัท

บริษัทต้อง

- กำหนดกระบวนการควบคุม ดูแลและรักษาทรัพย์สินที่สามารถจัดเก็บข้อมูลหรือการประมวลผลได้ โดยกำหนดความเป็นเจ้าของและติดตามสถานะของทรัพย์สิน รวมถึงการนำออกนอกพื้นที่จะต้องได้รับอนุญาตก่อนนำทรัพย์สินหรืออุปกรณ์นั้นออกจากตำแหน่งที่ตั้งอย่างเป็นทางการ
- กำหนดมาตรการควบคุมเพื่อป้องกันอุปกรณ์ของบริษัทในการปฏิบัติงานทั้งในสถานที่และนอกสถานที่
- กำหนดกระบวนการทำลายสื่อบันทึกข้อมูลอย่างเหมาะสม เพื่อป้องกันการรั่วไหลของข้อมูลจากสื่อบันทึกที่ไม่ใช้งานเหล่านั้น

4.6. การจัดการการเข้าถึง (Logical Access Management)

วัตถุประสงค์: เพื่อควบคุมการเข้าถึงข้อมูลและสิทธิการใช้งานระบบสารสนเทศอย่างเหมาะสม

- ผู้ใช้งานที่ได้รับอนุญาตในการเข้าถึงทรัพย์สิน ข้อมูลและระบบสารสนเทศของบริษัท จะต้องผ่านกระบวนการจัดการการเข้าถึงของผู้ใช้อย่างเป็นทางการ ตามพื้นฐานความจำเป็นในการใช้งาน
- ผู้ใช้งานที่ไม่จำเป็นต้องเข้าถึงระบบเทคโนโลยีสารสนเทศหรือมีความประสงค์ยกเลิกการใช้งาน จะถูกลบออกโดยเร็วที่สุด
- บริษัทต้องมีการตรวจสอบสิทธิการเข้าถึงของผู้ใช้งานเป็นประจำ รวมถึงพนักงานและหน่วยงานภายนอกที่ได้รับอนุญาตให้เข้าถึงได้
- ผู้ดูแลระบบจะต้องมีมาตรการควบคุมบัญชีผู้ใช้งาน (User account) อย่างเหมาะสม
- บริษัทต้องมีการกำหนดวิธีการพิสูจน์ตัวตนให้สอดคล้องกับระดับความเสี่ยงในการเข้าถึงทรัพยากรของบริษัทอย่างเหมาะสม รวมถึงวิธีการเข้าถึงข้อมูลภายหลังการพิสูจน์ตัวตนสำเร็จ

4.7. การจัดการเครือข่าย (Network Management)

วัตถุประสงค์: เพื่อป้องกันการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายอย่างเหมาะสม

บริษัทต้อง

- ระบุและแบ่งแยกเครือข่ายอย่างชัดเจน ให้สอดคล้องตามความเสี่ยงในการปฏิบัติงานที่แตกต่างกัน รวมถึงการกำหนดกระบวนการควบคุมการเข้าใช้งานระบบเครือข่ายและบริการเครือข่ายที่เหมาะสม
- กำหนดมาตรการควบคุมเพื่อรักษาความปลอดภัยในการรับส่งข้อมูลระหว่างปฏิบัติงานจากระยะไกล หรือการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่ได้รับอนุญาต
- กำหนดมาตรการการรักษาความปลอดภัยในการให้บริการเครือข่าย และข้อตกลงระดับบริการของเครือข่ายทั้งหมด จะต้องระบุและรวบรวมไว้ในข้อตกลงบริการเครือข่ายทั้งภายในและภายนอกองค์กร
- กำหนดกระบวนการควบคุมสำหรับการตรวจสอบเครือข่ายเพื่อตรวจจับการบุกรุกเครือข่ายโดยไม่ได้รับอนุญาต รวมทั้งความพร้อมใช้งานของเครือข่าย

4.8. การบริหารจัดการในการปฏิบัติงาน (Operations Management)

วัตถุประสงค์: เพื่อให้การปฏิบัติงานด้านระบบสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

บริษัทต้อง

- มีมาตรการกำหนดการตั้งค่าและการจัดเก็บข้อมูลเพื่อการปฏิบัติงานที่มีประสิทธิภาพ
- จัดทำเอกสารขั้นตอนการปฏิบัติงานตามมาตรฐานที่เหมาะสม สอดคล้องกับความต้องการในการปฏิบัติงานและมีความพร้อมใช้
- มีกระบวนการเฝ้าระวังการใช้งานระบบสารสนเทศ เพื่อให้สามารถตอบสนองต่อเหตุการณ์และการจัดการทรัพยากรคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ
- มีการบันทึกและจัดเก็บหลักฐาน (logs) เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้อง หรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
- มีกระบวนการสำรองข้อมูลและการทดสอบการกู้คืนข้อมูล ต้องดำเนินการอย่างเหมาะสมกับ~~ความ~~ความสำคัญของข้อมูล
- มีระบบประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดภายในบริษัทเชื่อมต่อกับแหล่งเวลาอ้างอิงเดียว
- มีการปรับปรุงหรือการเปลี่ยนแปลงซอฟต์แวร์และแอปพลิเคชันที่ใช้งาน ได้รับการทดสอบก่อนดำเนินการ และตรวจสอบให้แน่ใจว่ามีการปฏิบัติตามแนวทางการควบคุมการเปลี่ยนแปลงที่ดี

4.9. การดูแลระบบ (System Administration)

วัตถุประสงค์: เพื่อกำหนดแนวทางในการปฏิบัติงานด้านระบบสารสนเทศให้มีความถูกต้องและปลอดภัย

บริษัทต้อง

- กำหนดมาตรการและกระบวนการควบคุม เพื่อดูแลระบบและอุปกรณ์เครือข่ายอย่างปลอดภัยและมีประสิทธิภาพ
- จัดทำกระบวนการจัดการการเปลี่ยนแปลงเพื่อดำเนินการกับการเปลี่ยนแปลงทั้งหมดที่เกิดขึ้นกับระบบและอุปกรณ์เครือข่าย
- มีมาตรการเฝ้าระวังการใช้ทรัพยากรของระบบเทคโนโลยีสารสนเทศ เพื่อคำนึงถึงขีดความสามารถในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร และพิจารณาแนวทางการรองรับ การเติบโตของการใช้ทรัพยากรระบบเทคโนโลยีสารสนเทศได้อย่างเหมาะสม
- กำหนดมาตรฐานขั้นต่ำ (Hardening) สำหรับระบบและอุปกรณ์เครือข่ายทั้งหมดที่ใช้ในระบบสารสนเทศของบริษัท
- มีการวางแผนการตรวจสอบระบบสารสนเทศอย่างเพียงพอและเหมาะสม โดยการตรวจสอบต้องส่งผลกระทบต่อการปฏิบัติงานน้อยที่สุด

4.10 การจัดการการเข้ารหัส (Cryptographic Management)

วัตถุประสงค์: เพื่อให้การใช้งานระบบการเข้ารหัสข้อมูลมีความเหมาะสม มีประสิทธิภาพ และสามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลที่มีความสำคัญ

บริษัทต้อง

- กำหนดมาตรการควบคุมและกระบวนการเข้ารหัส สอดคล้องตามความสำคัญของข้อมูล

- มีการควบคุมการเข้ารหัสจะต้องจัดตั้งขึ้นให้สอดคล้องตามข้อตกลง กฎหมายและข้อบังคับที่เกี่ยวข้อง และต้องตรวจสอบให้แน่ใจว่าคอมพิวเตอร์และซอฟต์แวร์ที่ใช้ในการทำหน้าที่เข้ารหัส รวมถึงวิธีการเข้าถึงข้อมูลที่เข้ารหัสนั้นเป็นไปตามข้อกำหนดของหน่วยงานที่กำกับดูแลของแต่ละประเทศ

4.11 การจัดหา พัฒนาและบำรุงรักษาระบบสารสนสนเทศ (Information System Acquisition, Development and Maintenance)

วัตถุประสงค์: เพื่อกำหนดให้กระบวนการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นส่วนหนึ่งของระบบสารสนเทศของทั้งภายในบริษัท และที่เกี่ยวข้องกับการให้บริการภายนอกผ่านเครือข่ายสาธารณะ ตลอดช่วงอายุการใช้งานระบบสารสนเทศ ได้แก่ กระบวนการจัดหา กระบวนการพัฒนาระบบ (system development life cycle) การใช้งานและการดูแลรักษา

บริษัทต้อง

- กำหนดวัตถุประสงค์ กระบวนการควบคุมการพัฒนาระบบสารสนเทศ และจัดเตรียมสภาพแวดล้อมสำหรับการพัฒนาและการทดสอบที่เหมาะสม และคงไว้ซึ่งความพร้อมใช้ของระบบสารสนเทศที่ใช้งานปัจจุบัน
- จัดให้มีการดูแล ติดตาม และควบคุมการปฏิบัติงานของผู้ให้บริการพัฒนาระบบงานจากภายนอก (outsourced system development) ให้เป็นไปตามนโยบายการพัฒนาระบบสารสนเทศของบริษัท ภายใต้ข้อตกลง สัญญา หรือข้อกำหนด กฎหมายที่เกี่ยวข้อง
- มีการทดสอบระบบสารสนเทศที่ได้รับการพัฒนาหรือเปลี่ยนแปลง เพื่อให้มั่นใจว่าการทำงานมีประสิทธิภาพ การประมวลผลถูกต้องครบถ้วน ข้อมูลบนระบบสารสนเทศจะได้รับการปกป้อง เพื่อป้องกันการรับส่งข้อมูลที่ไม่สมบูรณ์ การเปลี่ยนแปลงหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การทำซ้ำและการกำหนดเส้นทางที่ไม่ถูกต้อง รวมถึงการควบคุมการใช้ข้อมูลในการทดสอบระบบอย่างระมัดระวัง
- กำหนดมาตรการการป้องกันระบบสารสนเทศที่เพียงพอ ระหว่างการดำเนินการพัฒนาระบบและบริการทั้งภายในบริษัท และที่เกี่ยวข้องกับการให้บริการภายนอกผ่านเครือข่ายสาธารณะ เพื่อป้องกันการถูกบุกรุกหรือโจมตี
- มีการทดสอบการทำงานของระบบที่ได้รับการพัฒนาโดยผู้ใช้งาน หรือผู้ทดสอบอื่นที่เป็นอิสระจากผู้พัฒนาระบบสารสนเทศดังกล่าว เพื่อให้แน่ใจว่าระบบได้รับการพัฒนาตรงตามความต้องการของผู้ใช้งาน และเป็นไปตามนโยบายความปลอดภัยของข้อมูลและความปลอดภัยทางไซเบอร์ พร้อมทั้งปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจให้สอดคล้องกับการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศดังกล่าว

4.12 การบริหารจัดการผู้ให้บริการภายนอก (Supplier Security Management)

วัตถุประสงค์: เพื่อให้แน่ใจว่ามีมาตรการควบคุมการปฏิบัติงานของผู้ให้บริการภายนอกอย่างเหมาะสม

บริษัทต้อง

- กำหนดมาตรการควบคุม ติดตาม ทบทวน และตรวจสอบหน่วยงานภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการส่งมอบบริการมีประสิทธิภาพ เป็นไปตามข้อตกลง สัญญาและหน่วยงานภายนอก ได้ปฏิบัติงานสอดคล้องตามความปลอดภัยของข้อมูลและความปลอดภัยทางไซเบอร์
- สร้างความตระหนักรู้ด้านความปลอดภัยข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของผู้ให้บริการภายนอก เพื่อให้รับทราบและปฏิบัติตามข้อกำหนดด้านความปลอดภัยของข้อมูลและความปลอดภัยไซเบอร์ที่จำเป็น
- มีการประเมินความเสี่ยงและกำหนดมาตรการควบคุมที่เหมาะสม หากหน่วยงานภายนอกมีการเปลี่ยนแปลงกระบวนการ วิธีการปฏิบัติงาน มาตรการด้านความปลอดภัย รวมถึงการเปลี่ยนแปลงผู้รับจ้างช่วงต่อของหน่วยงานภายนอก

4.13 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์: เพื่อป้องกันภัยคุกคามจากช่องโหว่ทางเทคนิค

บริษัทต้อง

- กำหนดบทบาทและความรับผิดชอบสำหรับการจัดการช่องโหว่ทางเทคนิค การตรวจสอบ การประเมินความเสี่ยงและการแก้ไขเพื่อปิดช่องโหว่ทางเทคนิคนั้น
- กำหนดให้มีการติดต่อสื่อสารที่เหมาะสมกับผู้เชี่ยวชาญด้านความปลอดภัย หรือสมาคมวิชาชีพที่เกี่ยวข้อง เพื่อปรับปรุงความรู้และรับคำแนะนำด้านความปลอดภัยต่างๆ
- กำหนดมาตรการหรือกระบวนการควบคุม เพื่อดำเนินการตรวจสอบและการจัดการช่องโหว่ทางเทคนิคที่ตรวจพบ

4.14 การจัดการเหตุการณ์ด้านความปลอดภัยของข้อมูลและความปลอดภัยไซเบอร์ (Information Security and Cyber Incident Management)

วัตถุประสงค์: เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพ ในช่วงระยะเวลาที่เหมาะสม

บริษัทต้อง

- กำหนดบทบาทและความรับผิดชอบในการจัดการเหตุการณ์ด้านความปลอดภัยของข้อมูลและความปลอดภัยไซเบอร์
- กำหนดช่องทางการรายงานที่ชัดเจนสำหรับการรายงานเหตุการณ์และจุดอ่อนด้านความปลอดภัยของข้อมูลและความปลอดภัยไซเบอร์
- กำหนดวัตถุประสงค์และกระบวนการควบคุมเพื่อจัดการเหตุการณ์หรือจุดอ่อนด้านความปลอดภัยของข้อมูลและความปลอดภัยไซเบอร์ ตลอดจนการรวบรวมหลักฐานเพื่อใช้เป็นหลักฐานในการพิจารณาคดีความได้
- ดำเนินการฝึกซ้อมอย่างสม่ำเสมอเพื่อให้คุ้นเคยกับแผนการรับมือเหตุฉุกเฉิน

4.15 การจัดการความต่อเนื่องทางธุรกิจ (Business Continuity and Availability Management)

วัตถุประสงค์: เพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญ จากผลกระทบของความล้มเหลวที่สำคัญของระบบเทคโนโลยีสารสนเทศ จากภัยพิบัติหรือความตั้งใจของมนุษย์

บริษัทต้อง

- ระบุข้อกำหนดความพร้อมใช้งานและการกู้คืน เช่น ระยะของเวลาในการกู้คืนและระบบสำคัญในการกู้คืนที่ได้มาจากการประเมินผลกระทบทางธุรกิจ เพื่อเป็นการกำหนดลำดับความสำคัญของบริการในกู้คืน สำหรับแผนบริหารความต่อเนื่องทางธุรกิจ
- จัดทำขั้นตอนการตอบสนองและแผนการกู้คืนข้อมูลและระบบบริการ ที่สอดคล้องกับความพร้อมใช้งาน โดยต้องคำนึงถึงความมั่นคงปลอดภัยของระบบสารสนเทศ
- จัดให้มีการสำรองระบบสารสนเทศ หรือเทคโนโลยีที่จำเป็น เพื่อให้อยู่ในสภาพพร้อมใช้งานและสอดคล้องตามข้อกำหนดในการกู้คืนที่กำหนดไว้
- ทำการทดสอบและปรับปรุงแผน (update) ให้เป็นปัจจุบัน เพื่อช่วยให้ทีมกู้คืนมีความคุ้นเคยกับขั้นตอนการกู้คืน ตลอดจนกำหนดความเพียงพอของทรัพยากรต่างๆ ทั้งบุคคลากร งบประมาณและอุปกรณ์สารสนเทศที่จำเป็นให้สอดคล้องตามแผนที่กำหนดไว้

4.16 การจัดการข้อมูลส่วนบุคคล (Personal Data Management)

วัตถุประสงค์: เพื่อป้องกันการใช้ข้อมูลส่วนบุคคลอย่างไม่เหมาะสม

- บริษัทจะกำหนดนโยบายความเป็นส่วนตัวเพื่อให้ผู้มีส่วนได้ส่วนเสีย เข้าใจเกี่ยวกับมาตรการด้านความปลอดภัยที่บริษัทใช้ในการจัดเก็บข้อมูลส่วนบุคคล
- บริษัทต้องกำหนดกระบวนการควบคุมเพื่อป้องกันข้อมูลส่วนบุคคลและใช้ตามความต้องการทางธุรกิจที่ถูกต้องตามกฎหมายเท่านั้น
- บริษัทจะลบหรือทำลายข้อมูลส่วนบุคคลหลังจากการใช้งานส่วนบุคคลหมดอายุแล้ว
- บุคคลที่เกี่ยวข้องที่ได้รับมอบหมายให้เป็นผู้รับเรื่องเกี่ยวข้องกับข้อมูลส่วนบุคคลจากเจ้าของข้อมูล และแนวปฏิบัติให้การจัดการข้อมูลส่วนบุคคลให้อ้างอิง นโยบายการจัดการข้อมูลส่วนบุคคล

5 การปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการรักษาความมั่งคงปลอดภัยไซเบอร์

ให้ปฏิบัติตามเอกสารแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศสำหรับผู้ใช้งานตามเอกสารแนบท้ายประกาศนี้

ทั้งนี้ ให้มีผลตั้งแต่วันที่ 1 ตุลาคม 2564 เป็นต้นไป

ประกาศ ณ วันที่

(นายกุลิศ สมบัติศิริ)