

# นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์



บริษัท ไอร่า แพลตฟอร์ม จำกัด (มหาชน)

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5/2566 เมื่อวันที่ 14 พฤศจิกายน 2566

## นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

### วัตถุประสงค์

1. เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์
2. เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ รวมถึงกฎหมายที่เกี่ยวข้องกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม
3. เพื่อให้พนักงานและผู้ที่ต้องใช้หรือเชื่อมต่อบริษัทคอมพิวเตอร์ของบริษัท ให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม
4. เพื่อป้องกันไม่ให้อุปกรณ์คอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่าง ๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

### ขอบเขต

นโยบายฉบับนี้ครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัท ทั้งที่อยู่ภายในหรือ ภายนอกสถานที่ปฏิบัติงานของบริษัท รวมทั้งคลาวด์ที่บริษัทจัดหา ซึ่งครอบคลุมถึง

1. พนักงานและหน่วยงานทั้งหมดของบริษัท
2. บุคคลภายนอกบริษัทที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท

### แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

- **ความลับ (Confidentiality)** – การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัท
- **ความสมบูรณ์ (Integrity)** – การทำให้มั่นใจว่าข้อมูลของบริษัท ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- **ความพร้อมใช้งาน (Availability)** – การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูล และบริการได้อย่างรวดเร็วและเชื่อถือได้
- **ความรับผิดชอบ (Accountability)** – การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับ ผิดและรับผิดชอบต่อผลของกระทำตามบทบาทหน้าที่นั้นๆ
- **การพิสูจน์ตัวตน (Authentication)** – การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และ ข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น
- **การกำหนดสิทธิ (Authorization)** – การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และ ข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต

- การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) – การทำให้มั่นใจว่าผู้มีส่วนร่วม (parties) ที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น
- การรักษาความมั่นคงปลอดภัยอย่างได้ผล จำเป็นต้องมีข้อตกลงร่วมกันและได้รับความเอาใจใส่อย่างจริงจังในทุกเรื่องที่เกี่ยวข้อง อันประกอบไปด้วย
  1. การรักษาความปลอดภัยถือว่าเป็นหน้าที่ของพนักงานและบุคคลภายนอกทุกคน
  2. การบริหาร และการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา
  3. การมีจิตสำนึก รู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนดไว้ในนโยบายมาตรฐาน การอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่างๆ ถือเป็นสิ่งสำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบายให้พนักงานและบุคคลภายนอกทราบอย่างชัดเจนเพื่อให้มีความเข้าใจในหน้าที่และความรับผิดชอบในการรักษาความปลอดภัยที่ตนเองรับผิดชอบเป็นสิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิภาพ

#### คำจำกัดความ

1. “บริษัท (Company)” หมายถึง บริษัท ไอรา แฟคตอริง จำกัด (มหาชน)
2. “พนักงาน (Employee)” หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้าง และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท
3. “ผู้ใช้งาน (User)” หมายถึง พนักงานของบริษัท รวมไปถึงบุคคลภายนอกบริษัทที่ได้รับอนุญาตให้มิดรหัส เข้าใช้งานในบัญชีรายชื่อผู้สามารถเข้าใช้งาน หรือ/และ มีรหัสผ่านเพื่อเข้าใช้งานระบบประมวลผลสารสนเทศของบริษัท
4. “ผู้บังคับบัญชา” หมายถึง พนักงานซึ่งเป็นผู้บังคับบัญชาของหน่วยงานภายในตามโครงสร้างองค์กรของบริษัท
5. “ระบบคอมพิวเตอร์ (Computer System)” หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง Hardware และ Software ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุ อุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่าง ๆ ระบบ Internet และระบบ Intranet รวมถึง อุปกรณ์ไฟฟ้า และสื่อสาร โทรคมนาคมต่าง ๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือ คล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัทหรือของพนักงานที่นำเข้ามาติดตั้ง หรือใช้งานภายในสถานประกอบการของบริษัท
6. “ข้อมูลสารสนเทศ (Information Technology)” หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ไม่ว่าจะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรืออุปกรณ์ใด ๆ
7. “ข้อมูลสำคัญ” หรือ “ข้อมูลที่เป็นความลับ (Sensitive Information)” หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัท มีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญาซึ่งบริษัท ไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น

- นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง
8. “ระบบที่มีความสำคัญ (Important System)” หมายถึง ระบบคอมพิวเตอร์ที่บริษัทใช้ประโยชน์ เพื่อให้บริการทางธุรกิจทั้งระบบที่ก่อให้เกิดรายได้โดยตรง และระบบที่สนับสนุนให้เกิดรายได้ รวมถึงระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยในการดำเนินธุรกิจของบริษัท ให้เป็นปกติ และระบบที่ได้รับการกำหนดโดย หน่วยงานด้านความปลอดภัยข้อมูล และระบบสารสนเทศของบริษัท ทั้งนี้หากระบบที่มีความสำคัญ ดังกล่าวหยุดการทำงาน หรือมีความสามารถในการทำงานที่ลดถอยลงจะทำให้การดำเนินธุรกิจของบริษัทต้องหยุดชะงัก หรือด้อยประสิทธิภาพ
  9. “Remote Access” หมายถึง การเชื่อมต่อเพื่อเข้าถึงคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท (ผ่านช่องทางการสื่อสารภายในบริษัท) หรือ จากภายนอกบริษัท (ผ่าน Internet)
  10. “เจ้าของระบบ (System Owner)” หมายถึง หน่วยงานภายในซึ่งเป็นเจ้าของระบบคอมพิวเตอร์ และมีความรับผิดชอบในระบบคอมพิวเตอร์นั้น ๆ
  11. “ผู้ดูแลระบบ (Administrator)” หมายถึง ผู้ที่ได้รับมอบหมายให้ดูแลใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์ทั้งอุปกรณ์ Hardware Software และอุปกรณ์ต่อพ่วงที่ประกอบกันขึ้นเป็นระบบคอมพิวเตอร์ ผู้ดูแลระบบจะเป็นผู้ที่ได้รับอนุญาตให้มีอำนาจในการปรับเปลี่ยน เพิ่มเติม แก้ไข ปรับปรุงให้ระบบ คอมพิวเตอร์ของบริษัท ทำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจและมีความปลอดภัย
  12. “การรักษาความมั่นคงปลอดภัย” หรือ “ความมั่นคงปลอดภัย (Security)” หมายถึง กระบวนการและการกระทำใด ๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษา ระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจากความ พยายามใด ๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอก ในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินธุรกิจของบริษัท ได้รับความเสียหาย
  13. “บุคคลภายนอก (External Party)” หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ เช่น
    - บริษัทคู่ค้า (Business Partner)
    - ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (Outsource)
    - ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ (Supplier)
    - ผู้ให้บริการต่าง ๆ (Service Provider)
    - ที่ปรึกษา (Consultant)

## หน้าที่และความรับผิดชอบ

### 1 หน้าที่ของผู้บังคับบัญชา

- ชี้แจงให้พนักงานทราบถึงนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่าง ๆ ของบริษัทที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- ดูแล แนะนำ และตักเตือน กรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม
- พิจารณาลงโทษทางวินัยแก่ผู้กระทำผิดอย่างเสมอภาค และเป็นธรรม

### 2 หน้าที่ของพนักงาน

#### 2.1 พนักงานทุกคน ต้องปฏิบัติดังต่อไปนี้

- ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่าง ๆ ของบริษัทที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด
- ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท
- แจ้งให้บริษัททราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นการบุกรุกโจรกรรม ทำลาย แทรกแซงการทำงาน หรือกิจกรรมที่อาจสร้างความเสียหายต่อบริษัท

#### 2.2 พนักงานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์ ต้องปฏิบัติดังต่อไปนี้

- ต้องออกจากระบบ (Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน
- ต้องล็อกหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือไปทำกิจกรรมอย่างอื่นเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน
- ต้องตรวจสอบข้อมูลที่นำมาจากในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส (Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย
- ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่บริษัทกำหนด เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ หรือข้อมูลของบริษัทเป็นความลับส่วนตัวพนักงาน ซึ่งจะต้องเก็บ รักษาไว้มิให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น ทั้งนี้พนักงานต้องเปลี่ยนรหัสผ่านและรหัสอื่น ใด เมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนด

#### 2.3 พนักงานที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอก ต้องจัดให้มีการควบคุมดูแลบุคคลภายนอกให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัท

### 3.การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Risk Management)

เพื่อแสดงถึงการยอมรับความเสี่ยงและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยบริษัทใช้วิธีการที่สอดคล้องกันในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Management) รวมถึงมีมาตรการรักษาความมั่นคงปลอดภัยเพื่อปกป้องข้อมูลซึ่งสอดคล้องกับกระบวนการในการระบุและประเมิน ความเสี่ยง (Risk Identification and Assessment)

#### รายละเอียด

- 3.1 วิธีการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Management Methodology)
- 3.2 การจัดโครงสร้างองค์กร (Internal Organization)
- 3.3 การบริหารความเสี่ยงภายนอก (Risk Management with External Parties)

### 4.การบริหารจัดการระบบ (System Management)

เพื่อให้มีมาตรการในการปกป้องทรัพย์สินของบริษัทอย่างเหมาะสม

#### รายละเอียด

- 4.1 บัญชีทรัพย์สินและความเป็นเจ้าของ (Inventory and Ownership)
- 4.2 การจัดชั้นความลับและการควบคุม (Security Classification and Handling)
- 4.3 การบริหารจัดการซอฟต์แวร์ลิขสิทธิ์ (Software Licensing)

### 5.การบริหารจัดการหน่วยงานและบุคลากร (Human Resource Management)

เพื่อให้พนักงานและบุคคลภายนอกที่ทำงานอยู่กับบริษัทเข้าใจในหน้าที่ความรับผิดชอบของตนเอง รวมถึงตระหนักถึงการรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน

#### รายละเอียด

- 5.1 ก่อนการจ้างงาน (Prior to Employment)
- 5.2 ระหว่างการจ้างงาน (During Employment)
- 5.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and Change of Employment)

### 6. การรักษาความมั่นคงปลอดภัยสถานที่และอุปกรณ์ (Physical and Equipment Security)

เพื่อป้องกันการเข้าถึงสถานที่และอุปกรณ์โดยไม่ได้รับอนุญาต ซึ่งอาจทำให้เกิดความเสียหายและ การแทรกแซงการทำงานของระบบคอมพิวเตอร์ของบริษัท

#### รายละเอียด

- 6.1 การรักษาความมั่นคงปลอดภัยสถานที่ (Physical Security)
- 6.2 การรักษาความมั่นคงปลอดภัยอุปกรณ์ (Equipment Security)

## 7. การบริหารจัดการการสื่อสารและการดำเนินงาน (Communications and Operation Management)

เพื่อให้มั่นใจว่ามีการดำเนินงานบนระบบคอมพิวเตอร์อย่างปลอดภัยและดำเนินการ (Implement) การรักษา (Maintain) ระดับความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสมในการลดความเสี่ยงจากการล้มเหลวของระบบคอมพิวเตอร์ รวมทั้งปกป้องรักษาความถูกต้องของข้อมูล ซอฟต์แวร์ และระบบคอมพิวเตอร์ให้มีสภาพพร้อมใช้งานให้มั่นใจว่ามีการปกป้องข้อมูลในเครือข่ายโครงสร้างพื้นฐานสนับสนุนอื่นๆ ไม่ให้มีการเปิดเผย การแก้ไข การลบ หรือการทำลายทรัพย์สิน รวมถึงการหยุดชะงักของกิจกรรมทางธุรกิจและทำการเฝ้าระวังการประมวลผลข้อมูลที่ไม่ได้รับอนุญาต

### รายละเอียด

- 7.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedure and Responsibilities)
- 7.2 การบริหารจัดการการส่งมอบบริการของบุคคลภายนอก (External Party Service Delivery Management)
- 7.3 การบริหารจัดการปริมาณความจุของระบบ (Capacity Management)
- 7.4 การป้องกันซอฟต์แวร์ไม่ประสงค์ดี (Protection Against Malicious Software)
- 7.5 การสำรองและการกู้คืนข้อมูล (Back Up and Restoration)
- 7.6 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)
- 7.7 การควบคุมสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Removable Media Handling)
- 7.8 การจัดการข้อมูลแบบคลาวด์ (Cloud Storage)
- 7.9 การรับส่งข้อมูล (Information Transfer)
- 7.10 การเฝ้าระวัง (Monitoring)
- 7.11 การบริหารจัดการแพทช์ (Patch Management)

## 8. การบริหารจัดการการควบคุมการเข้าถึง (Access Control Management)

เพื่อควบคุมการเข้าถึงข้อมูลและระบบคอมพิวเตอร์เฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึง ระบบและบริการโดยไม่ได้รับอนุญาต

### รายละเอียด

- 8.1 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
- 8.2 การบริหารจัดการรหัสผ่าน (Password Management)
- 8.3 การควบคุมการเข้าถึง (Access Control)
- 8.4 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกบริษัท (Mobile Computing and Teleworking)

## 9. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

เพื่อให้การจัดหา การพัฒนา และการบำรุงรักษาระบบ คำนึงถึงความมั่นคงปลอดภัยเป็นองค์ประกอบสำคัญ  
รายละเอียด

- 9.1 ข้อกำหนดการรักษาความมั่นคงปลอดภัยสำหรับระบบ (Security Requirements for Systems)
- 9.2 การประมวลผลบนแอปพลิเคชัน (Correct Processing in Applications)
- 9.3 การควบคุมการเข้ารหัส (Cryptographic Controls)
- 9.4 การรักษาความมั่นคงปลอดภัย System File (Security of System Files)
- 9.5 การรักษาความมั่นคงปลอดภัยในการพัฒนา และกระบวนการสนับสนุน (Security in Development and Support Processes)
- 9.6 การบริหารจัดการช่องโหว่ (Vulnerability Management)

## 10. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Management)

เพื่อลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้น และทำให้มั่นใจว่าเหตุการณ์ด้านความมั่นคง ปลอดภัยทางไซเบอร์ รวมถึงจุดอ่อนที่เกี่ยวข้องกับระบบได้รับการสื่อสารและสามารถดำเนินการแก้ไขได้ทันเวลา

รายละเอียด

- 10.1 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Management of Cyber Security Incident)

## 11. การจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

เพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญ จากผลกระทบของความล้มเหลวที่สำคัญของระบบคอมพิวเตอร์หรือจากภัยพิบัติ

รายละเอียด

- 11.1 การจัดการความมั่นคงปลอดภัยไซเบอร์ในแผนความต่อเนื่องทางธุรกิจ

## 12. กฎหมายและข้อบังคับที่เกี่ยวข้อง (Regulatory and Compliance)

เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับหรือสัญญาจ้างที่เกี่ยวข้องกับ ความมั่นคง ปลอดภัย พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติการรักษา ความมั่นคงปลอดภัย ไซเบอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมาย ระเบียบข้อบังคับอื่นที่เกี่ยวข้องซึ่งใช้บังคับอยู่แล้วในขณะนี้และที่จะได้ออกใช้บังคับ ต่อไปภายหน้า

รายละเอียด

- 12.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with Legal Requirement)
- 12.2 การพิจารณาการตรวจสอบระบบ (System Audit Considerations)



นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท  
ครั้งที่ 5/2566 เมื่อวันที่ 14 พฤศจิกายน 2566 โดยมีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2567 เป็นต้นไป

*สรสิทธิ์ สุนทรเกศ*  
(นายสรสิทธิ์ สุนทรเกศ)  
ประธานกรรมการบริษัท