การจัดตั้งให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายและคอมพิวเตอร์ร่วมกัน เพื่อความมั่นคงปลอดภัยและสามารถสนับสนุนการดำเนินงานของบริษัทได้อย่างต่อเนื่อง มีการใช้งานระบบในลักษณะที่ถูกต้องสอดคล้องกับข้อกำหนดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัท ดังนั้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของบริษัทคงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ บริษัทจึงกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนสารสนเทศดังต่อไปนี้

1 วัตถุประสงค์

1.1 เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

1.2 เพื่อให้พนักงานในองค์กรเข้าใจระบบความปลอดภัย ขั้นตอนการปฏิบัติงานของกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม

1.3 เพื่อป้องกันการโจรกรรมในรูปแบบการโจมตีทางไซเบอร์ (**Cyber Attack**) เป็นภัยอันตรายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ เครือข่าย และข้อมูลทางอิเล็กทรอนิกส์ โดยสามารถก่อให้เกิดความเสียหายกับองค์กร

2 ขอบเขต

นโยบายฉบับนี้ครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัททั้งที่อยู่ภายในหรือภายนอกสถานที่ปฏิบัติงานของบริษัท รวมทั้งคลาวด์ที่บริษัทจัดหา ซึ่งครอบคลุมถึง

2.1 พนักงานและหน่วยงานทั้งหมดของบริษัท

2.2 บุคคลภายนอกบริษัทที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท

3 หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

3.1 ความลับ **(Confidentiality)** การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัท

3.2 ความสมบูรณ์ **(Integrity)** การทำให้มั่นใจว่าข้อมูลของบริษัท ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต

3.3 ความพร้อมใช้งาน (**Availability)** การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูล และบริการได้อย่างรวดเร็วและเชื่อถือได้

3.4 ความรับผิดชอบ (**Accountability)** การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับ ผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้นๆ

3.5 การพิสูจน์ตัวตน **(Authentication)** การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และ ข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น

3.6 การกำหนดสิทธิ **(Authorization)** การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และ ข้อมูลสารสนเทศเป็นไปตามความจำเป็น **(Least Privilege)** และสอดคล้องกับความต้องการพื้นฐาน **(Need to Know Basis)** ตามที่ได้รับอนุญาต

3.7 การห้ามปฏิเสธความรับผิดชอบ **(Non-repudiation)** การทำให้มั่นใจว่าผู้มีส่วนร่วม **(parties)** ที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น การรักษาความมั่นคงปลอดภัยอย่างได้ผล จำเป็นต้องมีข้อตกลงร่วมกันและได้รับความเอาใจใส่อย่างจริงจังในทุกเรื่องที่เกี่ยวข้อง อันประกอบไปด้วย

- การรักษาความปลอดภัยถือว่าเป็นหน้าที่ของพนักงานและบุคคลภายนอกทุกคน
- การบริหาร และการปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยเป็นกระบวนการที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา
- การมีจิตสำนึก รู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนดไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่างๆ ถือเป็นสิ่ง สำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบายให้

พนักงานและบุคคลภายนอกทราบอย่างชัดเจน เพื่อให้มีความเข้าใจในหน้าที่และความรับผิดชอบในการรักษาความปลอดภัยที่ตนเองรับผิดชอบเป็นสิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิผล

3.8 ความน่าเชื่อถือ (**Reliability)** คุณลักษณะของซอฟต์แวร์ในการรักษาสมรรถนะการทำงานภายใต้สภาวะและระยะเวลาใด ๆ ได้อย่างถูกต้อง

4 คำจำกัดความ

4.1 “บริษัท (Company)” หมายถึง บริษัท บีคอน ออฟชอร์ จำกัด

4.2 “**พนักงาน** (Employee)” **หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญา**จ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท

4.3 “**ผู้ใช้งาน** (User)” **หมายถึง พนักงานของบริษัท รวมไปถึงบุคคลภายนอกบริษัทที่ได้รับอนุญาตให้มีรหัสเข้าใช้งานในบัญชีรายชื่อ**ผู้สามารถเข้าใช้งาน หรือ/และ มีรหัสผ่านเพื่อเข้าใช้งานอุปกรณ์ประมวลผลสารสนเทศของบริษัท

4.4 “ผู้บังคับบัญชา” หมายถึง พนักงานซึ่งเป็นผู้บังคับบัญชาของหน่วยงานภายในตามโครงสร้างองค์กรของบริษัท

4.5 “**ระบบคอมพิวเตอร์** (Computer System)” **หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้ง** Hardware **และ** Software **ทุกขนาด อุปกรณ์เครือข่ายเชื่อมโยงข้อมูลทั้งชนิดมีสายและไร้สาย วัสดุ อุปกรณ์การเก็บรักษา และการถ่ายโอนข้อมูลชนิดต่าง** ๆ ระบบ Internet และระบบ **Intranet** รวมถึง อุปกรณ์ไฟฟ้า และสื่อสารโทรคมนาคมต่าง ๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน หรือ คล้ายคลึงกับคอมพิวเตอร์ ทั้งที่เป็นทรัพย์สินของบริษัท ของบริษัทคู่ค้า และบริษัทอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของพนักงานที่นำเข้ามาติดตั้งหรือใช้งานภายในสถานประกอบการของบริษัท

4.6 **“ข้อมูลสารสนเทศ (Information Technology)”** หมายถึง ข้อมูล ข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์รูปภาพ เสียง เครื่องหมาย และสัญลักษณ์ต่าง ๆ ไม่ว่า จะเก็บไว้ในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรืออุปกรณ์ใดๆ

4.7 **“ข้อมูลสำคัญ”** หรือ **“ข้อมูลที่เป็นความลับ (Sensitive Information)”** หมายถึง ข้อมูลสารสนเทศที่มีความสำคัญต่อการดำเนินธุรกิจของบริษัท หรือที่บริษัทมีพันธะผูกพันตามข้อกำหนดของกฎหมาย จรรยาบรรณในการประกอบธุรกิจ หรือสัญญา ซึ่งบริษัทไม่อาจนำไปเปิดเผยต่อบุคคลอื่น หรือนำไปใช้ประโยชน์อย่างอื่น นอกเหนือจากวัตถุประสงค์ในการดำเนินธุรกิจของบริษัท การรั่วไหลของข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับดังกล่าวอาจเป็นเหตุให้การดำเนินธุรกิจของบริษัท ต้องหยุดชะงัก ขาดประสิทธิภาพ หรือบริษัทเสื่อมเสียชื่อเสียง

4.8 **“ระบบที่มีความสำคัญ (Important System)”** หมายถึง ระบบคอมพิวเตอร์ที่บริษัทใช้ประโยชน์ เพื่อให้บริการทางธุรกิจทั้งระบบที่ก่อให้เกิดรายได้โดยตรง และระบบที่สนับสนุนให้เกิดรายได้ รวมถึงระบบอิเล็กทรอนิกส์อื่นใดที่ช่วยในการดำเนินธุรกิจของบริษัทให้เป็นปกติ และระบบที่ได้รับการกำหนดโดยหน่วยงานด้านความปลอดภัยข้อมูล และระบบสารสนเทศของบริษัท ทั้งนี้หากระบบที่มีความสำคัญดังกล่าวหยุดการทำงาน หรือมีความสามารถในการทำงานที่ลดถอยลงจะทำให้การดำเนินธุรกิจของบริษัทต้องหยุดชะงัก หรือด้อยประสิทธิภาพ

4.9 **“Remote Access”** หมายถึง การเชื่อมต่อเพื่อเข้าถึงคอมพิวเตอร์ หรือระบบเครือข่ายของบริษัท (ผ่านช่องทางการสื่อสารภายในบริษัท) หรือจากภายนอกบริษัท (ผ่าน **Internet)**

4.10 **“เจ้าของระบบ (System Owner)”** หมายถึง หน่วยงานภายในซึ่งเป็นเจ้าของระบบคอมพิวเตอร์ และมีความรับผิดชอบในระบบคอมพิวเตอร์นั้นๆ

4.11 **“ผู้อารักขา (Custodian)”** หมายถึง ผู้ที่ได้รับมอบหมายจากเจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศในการสนับสนุนงานการดูแล จัดการ และควบคุมการเข้าใช้ข้อมูลสารสนเทศให้เป็นไปตามข้อกำหนดหรือระดับสิทธิที่เจ้าของระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศกำหนด

4.12 **“ผู้ดูแลระบบ (Administrator)”** หมายถึง ผู้ที่ได้รับมอบหมายให้ดูแลใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์ทั้งอุปกรณ์ **Hardware Software** และอุปกรณ์ต่อพ่วงที่ประกอบกันขึ้นเป็นระบบคอมพิวเตอร์ ผู้ดูแลระบบจะเป็นผู้ที่ได้รับอนุญาตให้มีอำนาจในการปรับเปลี่ยน เพิ่มเติม แก้ไข ปรับปรุงให้ระบบคอมพิวเตอร์ของบริษัททำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจและมีความปลอดภัย

4.13 **“การรักษาความมั่นคงปลอดภัย”** หรือ **“ความมั่นคงปลอดภัย (Security)”** หมายถึง กระบวนการและการกระทำใด ๆ เช่น การป้องกัน การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และ การดูแลรักษาระบบคอมพิวเตอร์ และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจาก

ความพยายามใด ๆ ทั้งจากพนักงานภายใน และจากบุคคลภายนอกในการเข้าถึง เพื่อโจรกรรมทำลาย หรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินธุรกิจของบริษัท ได้รับความเสียหาย

4.14 "บุคคลภายนอก (**External Party)**" หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของบริษัทฯ เช่น

- บริษัทคู่ค้า (**Business Partner)**
- ผู้รับจ้างปฏิบัติงานให้กับบริษัทฯ (**Outsource)**
- ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ (**Supplier)**
- ผู้ให้บริการต่าง ๆ (**Service Provider)**
- ที่ปรึกษา (**Consultant)**

5 หน้าที่ความรับผิดชอบ

5.1 หน้าที่ของกรรมการผู้จัดการ (MD)

- กำหนดกลยุทธ์ในภาพรวม ควบคุมการปฏิบัติงานในบริษัท และอนุมัตินโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของบริษัท

5.2 หน้าที่ของ IT Officer (IO)

- ประเมินความต้องการใช้ทรัพยากรด้านสารสนเทศ ความคุ้มค่า รวมทั้งจัดหา และพัฒนาระบบสารสนเทศให้สอดคล้องกับกลยุทธ์ของบริษัท
- ดูแลทรัพยากรด้านสารสนเทศของบริษัทให้สามารถสนับสนุนการปฏิบัติงานภายในอย่างมีประสิทธิภาพ

5.3 หน้าที่ของพนักงาน

- พนักงานทุกคน ต้องปฏิบัติดังต่อไปนี้
  - ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติ คำแนะนำ และกระบวนการต่าง ๆ ของบริษัทที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด
  - ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท
  - แจ้งให้บริษัททราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นการบุกรุกโจรกรรม ทำลาย แทรกแซงการทำงาน หรือจารกรรมที่อาจสร้างความเสียหายต่อบริษัท
- พนักงานที่ได้รับมอบหมายให้ใช้งานเครื่องคอมพิวเตอร์ ต้องปฏิบัติดังต่อไปนี้
  - ต้องออกจากระบบ (Log-out, Log-off) ทุกระบบเมื่อไม่ได้ใช้งานเป็นเวลานาน และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นทันทีหลังเลิกงาน
  - ต้องล็อคหน้าจอ (Lock Screen) แบบกำหนดรหัสผ่าน (Password) หากไม่ใช้งานหรือไปทำกิจกรรมอย่างอื่นเป็นระยะเวลาสั้นๆ เพื่อป้องกันมิให้บุคคลอื่นลักลอบเข้าไปใช้งาน
  - ต้องตรวจสอบข้อมูลที่นำมาลงในเครื่องคอมพิวเตอร์ของตนเองทุกครั้ง โดยใช้โปรแกรมป้องกันไวรัส(Anti-virus) ที่มีข้อมูลไวรัสที่ทันสมัย
  - ต้องเก็บรักษารหัสผ่าน (Password) และรหัสอื่นใดที่บริษัทกำหนด เพื่อใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ หรือข้อมูลของบริษัทเป็นความลับส่วนตัวพนักงาน ซึ่งจะต้องเก็บ รักษาไว้มิให้ผู้อื่นล่วงรู้ และห้ามใช้ร่วมกันกับบุคคลอื่น ทั้งนี้พนักงานต้องเปลี่ยนรหัสผ่านและรหัสอื่น ใด เมื่อรหัสเก่าหมดอายุตามระยะเวลาที่กำหนดหรือเมื่อพนักงานเห็นสมควรต้องทำการเปลี่ยนรหัสผ่าน โดยตั้งรหัสผ่าน และรหัสอื่นใด ด้วยความรอบคอบ ห้ามตั้งรหัสซ้ำกับรหัสเก่า ห้ามตั้งรหัส ที่ผู้อื่นสามารถคาดเดาได้ง่าย หรือห้ามตั้งรหัสซ้ำกันในทุกระบบที่พนักงานมีสิทธิใช้งาน ทั้งนี้มาตรฐานการตั้งรหัสผ่านอย่างปลอดภัย อ้างอิงตามเอกสาร IT Security Standard
- พนักงานที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอก ต้องจัดให้มีการควบคุมดูแลบุคคลภายนอกให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัท

6 **การรักษาความมั่นคงปลอดภัยของระบบ** IT (IT Security) **แนวทางปฏิบัติเพิ่มเติมเกี่ยวกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของ** IT (Information Security Policy)

- **การใช้งานทรัพยากรที่ต้องห้าม** (Prohibited Use of Resources) - ห้ามใช้ทรัพยากรและเครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่ผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น
- **การเข้าถึงโดยไม่ได้รับอนุญาต** (Unauthorized Access) - ไม่เข้าใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้
- ห้ามเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก
- ห้ามเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูลนั้นๆ
- ห้ามก่อกวน ขัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัทเกิดความเสียหายเช่น การส่งไวรัสคอมพิวเตอร์ การป้อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน (Denial of Service) เป็นต้น
- ห้ามลักลอบดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัท และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์
- ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนทุกครั้ง
- ผู้ใช้ต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีใช้งานและรหัสผ่านของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

6.1 การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (Organization of Information Security)

- ผู้บริหารระดับสูง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท
- ผู้จัดการส่วนเทคโนโลยีสารสนเทศ ต้องกำหนดมอบหมายหน้าที่ให้กับผู้ปฏิบัติงานในส่วนเทคโนโลยีสารสนเทศ รับผิดชอบการดูแลระบบสารสนเทศที่บริษัทใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท
- ผู้จัดการส่วนเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบการบริหารจัดการ กำกับดูแล ติดตาม และทบทวนภาพรวมของนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของบริษัท
- ผู้ปฏิบัติงานส่วนเทคโนโลยีสารสนเทศ ที่ได้รับมอบหมายเป็นผู้ดูแลระบบระดับ Administrator รับผิดชอบต่อระบบที่ดูแลนั้น จะต้องทำหน้าที่ตรวจสอบดูแลระบบความปลอดภัยในการใช้งานของระบบด้วย และเมื่อมีสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด จะต้องดำเนินการแก้ไขและรายงานต่อผู้บังคับบัญชา
- ผู้ใช้งาน และหน่วยงานทั้งภายในและภายนอก ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัท ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

6.2 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (Human Resource Security)

- ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยระบบสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับบุคคลหรือหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านระบบสารสนเทศของบริษัท
- ต้องมีการลงนามในสัญญาระหว่างผู้ปฏิบัติงานและหน่วยงาน ว่าจะไม่เปิดเผยความลับของบริษัท(Non-Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างผู้ปฏิบัติงานนั้นๆ ทั้งนี้ ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า 1 ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว
- เพื่อให้การบริหารจัดการบัญชีผู้ใช้งานเป็นไปอย่างถูกต้องและเป็นปัจจุบันที่สุด ฝ่ายทรัพยากรบุคคลหรือหน่วยงานที่เกี่ยวข้อง ต้องแจ้งให้ผู้จัดการส่วนเทคโนโลยีสารสนเทศทราบทันที เมื่อมีเหตุดังนี้
  - การว่าจ้างงาน
  - การเปลี่ยนแปลงสภาพการว่าจ้างงาน
  - การลาออกจากงาน หรือการสิ้นสุดการเป็นกรรมการและผู้ปฏิบัติงานของบริษัท
  - การโยกย้ายหน่วยงาน
  - ต้องให้ผู้ใช้งานและหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงานรับทราบนโยบายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

- ผู้ปฏิบัติงานใหม่ของบริษัทต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศหลังจากเปลี่ยนแปลงหรือยกเลิกการจ้างงาน หรือสิ้นสุดโครงการ ต้องยกเลิกการเข้าถึงข้อมูลในระบบสารสนเทศทันที
- ผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing) หน่วยงานเจ้าของโครงการ หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศของ บริษัทฯ ต้องจัดทำข้อกำหนดและกรอบการปฏิบัติงานของผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย โดยข้อกำหนดและกรอบการปฏิบัติงานต้องครอบคลุมกรณีที่ผู้รับ ดำเนินการมีการให้ผู้บริการภายนอกรายอื่น (Sub-Contract) รับช่วงจัดการงานด้านเทคโนโลยีสารสนเทศ

6.3 การบริหารจัดการสินทรัพย์สารสนเทศ (Asset Management) การควบคุมการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ (Computer and Peripheral Access Control)

- ผู้ใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของบริษัท ต้องเป็นผู้รับผิดชอบสินทรัพย์ที่ใช้งาน
- ห้ามใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของบริษัทเพื่อประกอบธุรกิจการค้า หรือบริการใดๆ ที่เป็นของส่วนตัวและไม่เหมาะสม
- ไม่อนุญาตให้ผู้ใช้งาน ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรม ในเครื่องคอมพิวเตอร์ของบริษัทเว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน
- ห้ามดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง เว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบ หรือหน่วยงานที่รับผิดชอบ และผู้ใช้งานต้องรักษาสภาพของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงให้มีสภาพเดิม
- ผู้ใช้งานต้องไม่เก็บหรือใช้อุปกรณ์คอมพิวเตอร์ในสถานที่ที่มีความร้อน ชื้น มีฝุ่ นละออง และต้องระวังการตกกระทบ
- ไม่ใช้หรือวางอุปกรณ์คอมพิวเตอร์ทุกชนิดใกล้สิ่งที่เป็นของเหลว ใกล้สนามแม่เหล็ก ไฟฟ้าแรงสูง ในที่มีการสั่นสะเทือน และในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 37 องศาเซลเซียส
- ในการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ ควรทำด้วยความระมัดระวัง ไม่วางของหนักทับ หรือโยน
- ไม่เคลื่อนย้ายเครื่องขณะที่ฮาร์ดดิสก์กำลังทำงาน หรือขณะเปิดใช้งานอยู่
- หลีกเลี่ยงของแข็งกดสัมผัสหน้าจอคอมพิวเตอร์ซึ่งอาจทำให้เป็นรอยขีดข่วน หรือแตกเสียหายได้ และควรเช็ดทำความสะอาดหน้าจอคอมพิวเตอร์อย่างเบามือที่สุด และเช็ดไปในทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
- ผู้ใช้งานที่พ้นสภาพพนักงาน หรือสิ้นสุดระยะเวลาการยืมต้องคืนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่รับผิดชอบทั้งหมดต่อหน่วยงานที่รับผิดชอบในสภาพที่พร้อมใช้งาน
- การเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์เพื่อการปฏิบัติงานภายนอกสำนักงาน ให้ผู้ใช้งานปฏิบัติตามข้อกำหนดการนำทรัพย์สินของบริษัทออกนอกบริษัท
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

6.4 การควบคุมการใช้งานโปรแกรมคอมพิวเตอร์ (Software License)

- ข้อกำหนดสำหรับผู้ดูแลระบบ
  - มีหน้าที่รับผิดชอบในการควบคุม ดูแลการใช้งานโปรแกรมคอมพิวเตอร์ ตลอดจนจัดสรรการใช้งานโปรแกรมคอมพิวเตอร์ภายในบริษัทตามสทิ ธิ์การใช้งานที่กำหนด
  - มีหน้าที่รับผิดชอบในการติดตั้ง และอัพเกรดโปรแกรมคอมพิวเตอร์ให้แก่ผู้ใช้งาน ตามวันเวลาที่นัดหมาย
  - ทำการถอดและยกเลิกสิทธิ์การใช้ งานโปรแกรมคอมพิวเตอร์ทันที เมื่อบริษัท และ/หรือหน่วยงาน แจ้งยกเลิก และ/หรือย้ายสิทธิ์การใช้งานโปรแกรมคอมพิวเตอร์
- ข้อกำหนดสำหรับผู้ใช้งาน
  - ต้องใช้โปรแกรมคอมพิวเตอร์อย่างเช่นวิญญูชนพึงจะใช้ทรัพย์สินของตนเอง โดยไม่นำไปใช้ในทางที่ผิดกฎหมายหรือละเมิดกฎหมายต่อบุคคลอื่นอันเป็นต้นเหตุให้เกิดความเสียหายขึ้นกับบริษัท
  - โปรแกรมที่ถูกติดตั้งบนเครื่องคอมพิวเตอร์ของบริษัท เป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งาน
  - ห้ามคัดลอก จำหน่าย เผยแพร่โปรแกรมที่ละเมิดลิขสิทธิ์ และชุดคำสั่งที่จัด ทำขึ้น โดยไม่ได้รับอนุญาโดยเฉพาะการนำไปใช้เพื่อเป็นเครื่องมือในการกระทำความผิดทางกฎหมาย

- ห้ามนำโปรแกรมคอมพิวเตอร์ที่ไม่ชอบด้วยกฎหมายมาติดตั้ง ใช้งานบนเครื่องคอมพิวเตอร์ของบริษัทอย่างเด็ดขาด กรณีผู้ใช้ งานนำโปรแกรมคอมพิวเตอร์อื่นใดนอกเหนือไปจากโปรแกรมที่บริษัทมีอยู่ มาใช้งานบนระบบคอมพิวเตอร์ ไม่ว่าจะมี Licensed Software หรือ Freeware ก็ตาม หากมีความเสียหายหรือละเมิดเกิดขึ้นผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว
- การติดตั้งใช้งาน การยกเลิกการใช้งาน การโอนย้าย และการคืนเครื่องคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์ ให้ผู้ใช้งานขอแจ้งความประสงค์ในแต่ละกรณีให้ผู้มีอำนาจพิจารณาอนุมัติ และผู้ดูแลระบบเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามที่ได้รับอนุมัติในแต่ละกรณี

6.5 การควบคุมสินทรัพย์ด้านสารสนเทศและการเข้าใช้งานระบบคอมพิวเตอร์

ต้องควบคุมไม่ให้สินทรัพย์ด้านสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ และข้อมูลสารสนเทศอยู่ในสภาวะเสี่ยงต่อการเข้าถึงได้โดยผู้ซึ่งไม่มีสิทธิ์ ขณะที่ไม่มีผู้ใช้งานอุปกรณ์ และต้องกำหนดให้ผู้ให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้จากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังต่อไปนี้

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

6.6 การใช้งานจดหมายอิเล็กทรอนิกส์

- ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ จะต้องไม่กระทำการละเมิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายที่เกี่ยวข้องและนโยบายและข้อกำหนดเกี่ยวกับเทคโนโลยีสารสนเทศที่บริษัทกำหนด
- หน่วยงานหรือผู้ปฏิบัติงาน ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของบริษัท จะต้องใช้จดหมายอิเล็กทรอนิกส์ เพื่อผลประโยชน์ของบริษัท
- ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อความ เว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน
- การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง หรือบัญชีผู้ใช้งานอื่น
- การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการตามภารกิจของบริษัท ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของบริษัทขัดข้อง และต้องได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
- การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อศีลธรรมอันดีงาม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความคิดเห็นส่วนบุคคล โดยอ้างเป็นความเห็นของบริษัท หรือก่อให้เกิดความเสียหายต่อบริษัท
- ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของบริษัท เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรมอันดีงาม ความมั่นคงของประเทศ กฎหมาย หมิ่นต่อสถาบันพระมหากษัตริย์หรือกระทบต่อการดำเนินงานของบริษัท ตลอดจนเป็นการรบกวนผู้ใช้งานอื่นรวมทั้งผู้รับบริการของบริษัท
- ห้ามผู้ใช้บริการนำที่อยู่จดหมายอิเล็กทรอนิกส์ ไปใช้ในกิจการงานส่วนบุคคล เช่น ธุรกิจส่วนตัว ใช้สมัครเครือข่ายสังคมออนไลน์ เป็นต้น หากตรวจพบว่ามีการกระทำดังกล่าว ให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ หรือเจ้าของผู้ใช้บริการ เป็นผู้รับผิดชอบการกระทำดังกล่าว

- ห้ามกระทำการอันที่จะสร้างปัญหาในการใช้ทรัพยากรของระบบ เช่น การสร้างจดหมายลูกโซ่ (Chainmail) การส่งจดหมายจำนวนมาก (Spam mail) การส่งจดหมายต่อเนื่อง (Letter bomb) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์ เป็นต้น
- ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของบริษัทให้กับบุคคลอื่นหรือหน่วยงานที่ไม่เกี่ยวข้องกับภารกิจของบริษัท การส่งข้อมูลข่าวสารที่เป็นความลับบริษัท ควรมีการเข้ารหัสข้อมูลข่าวสารนั้น และไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
- กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมาย ขอสงวนสิทธิ์ที่จะทำการยกเลิกหรือระงับการบริการชั่วคราวแก่ผู้ปฏิบัติงานนั้นๆ เพื่อทำการสอบสวน และตรวจสอบสาเหตุ
- หากผู้ใช้บริการพบการกระทำที่ไม่เหมาะสม หรือเข้าข่ายการกระทำความผิดเกิดขึ้นในบริษัท ให้แจ้งเบาะแสไปที่ช่องทางการรับแจ้งเบาะแสของบริษัท
- การกระทำใดๆ ที่เกี่ยวข้องกับการเผยแพร่ ทั้งในรูปแบบของจดหมายอิเล็กทรอนิกส์ และโฮมเพจของผู้ใช้บริการ ให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้บริการเท่านั้น ผู้ดูแลระบบและบริษัทไม่มีส่วนเกี่ยวข้องใดๆ

6.7 การรักษาความมั่นคงปลอดภัย ด้านการสื่อสารข้อมูลสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ (Communications Security)

ความปลอดภัยเกี่ยวกับโปรแกรมอันตรายมัลแวร์ เพื่อป้องกันข้อมูลสารสนเทศในเครือข่ายจากบุคคล ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบสารสนเทศ ซึ่งมีแนวทางปฏิบัติ ดังนี้

- การบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย (Network Security Management) กำหนดการควบคุมการเข้าถึงระบบเครือข่ายให้มีความมั่นคงปลอดภัย ต้องจัดแบ่งเครือข่ายระหว่างผู้ใช้งานภายในและผู้ใช้ภายนอกที่ติดต่อกับบริษัท
- การถ่ายโอนข้อมูล (Information Transfer) ต้องดำเนินการจัดทำข้อตกลงสำหรับการถ่ายโอนข้อมูล (Agreements on Information Transfer) โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)
- บริษัทและหน่วยงานเทคโนโลยีสารสนเทศจะต้องใช้ซอฟต์แวร์ที่มีกระบวนการในการจัดการและป้องกันโปรแกรมไม่ประสงค์ดี หรือเรียกว่ามัลแวร์ที่เหมาะสมกับสภาพแวดล้อมปัจจุบัน และพนักงานทุกคนต้องให้ความร่วมมือปฏิบัติตามนโยบายดังกล่าวรวมทั้งไม่ติดตั้งซอฟต์แวร์เอง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ทำงานแทน

6.8 การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

- การควบคุมห้องศูนย์กลางข้อมูล (Data Center Room)
  - ต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย เป็นต้น ไว้ในData Center Room หรือพื้น ที่หวงห้าม และต้องกำหนดสิทธิ์การเข้ าออก Data Center Room ให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น ผู้ดูแลระบบ เป็นต้น
  - ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออก Data Center Room ในบางครั้ง ก็ต้องมีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีผู้ดูแลระบบ และ/หรือผู้ปฏิบัติงานที่เกี่ยวข้อง ควบคุมดูแลการทำงานตลอดเวลา เป็นต้น
  - ต้องมีระบบเก็บบันทึกการเข้าออก Data Center Room โดยบันทึกดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคลและเวลาผ่านเข้าออก และควรมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ
  - ควรจัด Data Center Room ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server Zone) ส่วนเครื่องสำรองไฟฟ้า (UPS Zone)ส่วนแบตเตอรี่เครื่องสำรองไฟฟ้า (Battery UPS Zone) เป็นต้น เพื่อความสะดวกในการปฏิบัติงานและทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น
- แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (IT Disaster Recovery Plan)
  - จัดตั้งห้องจัดเก็บข้อมูลภายนอก (External Data Storage)
  - เก็บข้อมูลสำคัญลงในฮาร์ดดิสก์ที่มาในรูปแบบพกพา (External Hard Disk) เช่น ข้อมูลเกี่ยวข้องโครงการของลูกค้าสำคัญ เพื่อป้องกันข้อมูลสำคัญสูญหายถ้าเกิดภัยภิบัตที่ไม่สามารควบคุมได้
  - สถานที่จัดเก็บจะต้องไม่อยู่ในบริเวณบริษัท หรือ ส่งไปเก็บที่บริษัทจัดเก็บเอกสารและข้อมูลสำหรับสถานที่มีระบบป้องกันอัคคีภัย (Fire Protection System)
  - สำรองข้อมูลสำคัญ (Data Backup) ลงบนคลาวด์เซิร์ฟเวอร์ Cloud Server ของทางบริษัท
- การป้องกันความเสียหาย

  ระบบป้องกันไฟไหม้
  - ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

- Data Center Room หลักต้องมีระบบดับเพลิงแบบอัตโนมัติ สำหรับศูนย์คอมพิวเตอร์สำรอง อย่างน้อยต้องมีถังดับเพลิงเพื่อใช้สำหรับการดับเพลิงในเบื้องต้น

ระบบป้องกันไฟฟ้าขัดข้อง

- ต้องมีระบบป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า
- ต้องมีระบบสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) สำหรับระบบงานคอมพิวเตอร์ที่สำคัญ และระบบเครือข่ายคอมพิวเตอร์ เพื่อให้การดำเนินงานมีความต่อเนื่อง
- ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

ระบบควบคุมอุณหภูมิและความชื้น

- ต้องควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยควรตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์อาจทำงานผิดปกติภายใต้สภาวะอุณหภูมิหรือความชื้นที่ไม่เหมาะสม

7 วิธีการปฏิบัติให้เป็นไปตามนโยบาย

หน่วยงานเทคโนโลยีสารสนเทศ ได้จัดทำนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศโดยอ้างอิงมาตรฐาน ISO/TEC 27001:2013 Information Security Management Systems เพื่อให้เกิดความมั่นคงปลอดภัยแก่ระบบสารสนเทศ

8 การลงโทษทางวินัย

- ตักเตือนด้วยวาจา
- ตักเตือนเป็นลายลักษณ์อักษร
- พักงานชั่วคราวโดยไม่ได้รับค่าจ้าง
- ปลดออก
- ไล่ออก
- การดำเนินทางกฎหมายอาญาหรือแพ่ง

กรณีการลงโทษพนักงาน บริษัทไม่จำเป็นต้องปฏิบัติตามลำดับดังกล่าวข้างต้น บริษัทอาจเลือกลงโทษได้โดยพิจารณาตามความรุนแรงของความผิดที่กระทำ

9 การทบทวนนโยบาย

ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการทบทวนนโยบายฉบับนี้เป็นประจำอย่างน้อยปีละ 1 ครั้ง และต้องเสนอให้คณะกรรมการบริษัทพิจารณาอนุมัติหากมีการเปลี่ยนแปลง

นโยบายฉบับนี้ได้รับการตรวจสอบและอนุมัติโดยคณะกรรมการบริษัท ในการประชุมคณะกรรมการบริษัทครั้งที่ 8/2567 ซึ่งจัดขึ้นเมื่อ 3 ธันวาคม 2567 โดยจะมีผลใช้บังคับในวันที่ 4 ธันวาคม 2567

(นายเอกพล พงศ์สถาพร)

ประธานกรรมการบริษัท

บริษัท บีคอน ออฟชอร์ จำกัด