บสก BAM บริษัทบริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (มหาชน)
Bangkok Commercial Asset Management Public Company Limited
99 ถนนสุรศักดิ์ แขวงสีลม เขตบางรัก กรุงเทพฯ 10500 โทร: 0 2267 1900 โทรสาร: 0 2266 3377
ทะเบียนเลขที่ 0107558000482 www.bam.co.th

ประกาศบริษัทบริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (มหาชน)

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์

ตามที่ ที่ประชุมคณะกรรมการบริษัท ครั้งที่ 13/2566 เมื่อวันที่ 3 พฤศจิกายน 2566 มีมติอนุมัตินโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ เพื่อให้การปฏิบัติงานสอดคล้องกับมาตรฐาน ISO/IEC 27001:2022 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมถึงบรรดาประกาศ คำสั่ง ตลอดจนกฎหมายอื่น ๆ ที่เกี่ยวข้อง อย่างถูกต้องครบถ้วน และมีประสิทธิภาพ จึงได้ออกนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ เพื่อเป็นแนวทางในการปฏิบัติงานไว้ ดังนี้

1. หลักการและเหตุผล

บริษัทบริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (มหาชน) มีการติดตั้ง ใช้งาน บำรุงรักษา ระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ ระบบจัดเก็บข้อมูล และระบบอิเล็กทรอนิกส์อื่นใดที่เกี่ยวข้อง ซึ่งเป็นโครงสร้างทางสารสนเทศที่สำคัญ (Critical Information Infrastructure) ที่ใช้ในการดำเนินงาน การให้บริการ การสร้างรายได้ ดังนั้น เพื่อสร้างความมั่นใจในการใช้งานระบบดังกล่าวว่ามีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทำให้สามารถทำงานได้อย่างต่อเนื่องไม่หยุดชะงัก ไม่มีการรั่วไหล ข้อมูลมีความถูกต้อง และสามารถตรวจสอบย้อนกลับถึงความผิดปกติที่เกิดขึ้นได้ รวมทั้งการได้รับความร่วมมือจาก กรรมการ ผู้บริหาร พนักงาน ลูกจ้าง และบุคคลภายนอกที่ปฏิบัติงานด้านสารสนเทศให้บริษัททุกคน มีความตระหนัก จิตสำนึก และเอาใส่ใจต่อการกระทำตามข้อปฏิบัติที่กำหนดไว้ในนโยบาย มาตรการและวิธีปฏิบัติต่าง ๆ โดยขอบข่ายการบังคับใช้นั้นครอบคลุมข้อมูลทั้งหมดของบริษัท บุคคลทั้งหมดที่มีส่วนเกี่ยวข้องในการใช้งานข้อมูลและระบบคอมพิวเตอร์ของบริษัท ตลอดจนทรัพย์สินทั้งหมดที่ใช้ในการประมวลผลข้อมูลของบริษัท

2. วัตถุประสงค์

2.1 เพื่อกำกับดูแลการบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของบริษัท ให้มีประสิทธิผลและเป็นไปโดยถูกต้องตามกฎหมาย และมาตรฐาน ISO/IEC 27001:2022

2.2 เพื่อบูรณาการในการจัดการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของบริษัท

2.3 เพื่อสร้างมาตรการและกลไกที่เหมาะสมเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ที่อาจสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

2.4 เพื่อกำหนดแนวทางการประสานความร่วมมือระหว่างบริษัทกับคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และหน่วยงานภายนอกที่มีความเชี่ยวชาญ

2.5 เพื่อพัฒนาผู้ดูแลระบบที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของบริษัท

2 / 2.6 เพื่อให้...

2.6 เพื่อให้กรรมการ ผู้บริหาร พนักงาน ลูกจ้าง และบุคคลภายนอกที่ปฏิบัติงานด้านสารสนเทศให้บริษัททุกคน มีความตระหนัก ความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม และการร่วมมือ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และไซเบอร์ รวมถึงการใช้ทรัพย์สินสารสนเทศอย่างระมัดระวัง เพื่อให้เกิดคุณค่า และประโยชน์สูงสุดต่อบริษัท

2.7 เพื่อการป้องกัน และลดความเสี่ยงที่อาจเกิดความเสียหาย และส่งผลกระทบต่อทรัพย์สินสารสนเทศของบริษัท

2.8 เพื่อพัฒนา นโยบาย มาตรการ และวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และไซเบอร์ของบริษัท ถูกกำหนดเป็นลายลักษณ์อักษรเพื่อให้กรรมการ ผู้บริหาร พนักงาน ลูกจ้าง และบุคคลภายนอกที่ปฏิบัติงานด้านสารสนเทศให้บริษัททุกคนได้รับทราบ และยึดถือเป็นแนวทางในการปฏิบัติสำหรับใช้งานระบบสารสนเทศ การสื่อสารภายในระบบเครือข่ายคอมพิวเตอร์ของบริษัท ทำให้มีการบริหารจัดการที่ดี มีประสิทธิภาพ และมีความมั่นคงปลอดภัย สามารถสนับสนุนงานด้านสารสนเทศของบริษัทได้อย่างต่อเนื่องโดยไม่หยุดชะงัก

3. นิยาม

"บริษัท" หมายถึง บริษัทบริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (มหาชน)

"นโยบาย" หมายถึง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ ฉบับนี้

"กรรมการ" หมายถึง กรรมการของบริษัท และกรรมการในคณะกรรมการชุดย่อยของบริษัท

"ผู้บริหาร" หมายถึง ประธานเจ้าหน้าที่บริหาร และพนักงานผู้มีตำแหน่งตั้งแต่รองผู้จัดการขึ้นไป

"พนักงาน" หมายถึง พนักงานของบริษัท ตามคำนิยามในข้อบังคับ ว่าด้วยการทำงานของพนักงานบริษัทบริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (มหาชน) พ.ศ. 2562

"ลูกจ้าง" หมายถึง ลูกจ้างของบริษัท ตลอดจนลูกจ้างที่เกี่ยวข้องของผู้รับจ้างภายนอก (Outsource)

"บุคคลภายนอกที่ปฏิบัติงานให้บริษัท" หมายถึง บุคลากรหรือหน่วยงานภายนอกที่ดำเนินธุรกิจหรือให้บริการบริษัทคู่ค้า ผู้รับจ้างปฏิบัติงานให้กับบริษัท ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ ผู้ให้บริการต่าง ๆ และที่ปรึกษาที่บริษัทว่าจ้างให้ดำเนินการต่าง ๆ ที่อาจได้รับสิทธิ์เข้าถึง ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลคอมพิวเตอร์ เช่น ลูกค้า ลูกหนี้ เป็นต้น

"ผู้ดูแลระบบ" หมายถึง พนักงาน ลูกจ้าง หรือบุคคลภายนอกที่ปฏิบัติงานให้บริษัทที่ได้รับมอบหมายให้ดูแลใช้งาน และบำรุงรักษาระบบคอมพิวเตอร์ ระบบสารสนเทศ เป็นผู้ที่ได้รับอนุญาตให้ทำการปรับเปลี่ยน เพิ่มเติม แก้ไข ปรับปรุงระบบคอมพิวเตอร์ ระบบสารสนเทศของบริษัทให้ทำงานได้อย่างถูกต้อง มีประสิทธิภาพสอดคล้องกับความต้องการทางธุรกิจและมีความปลอดภัย

"ผู้ใช้ระบบ" หมายถึง กรรมการ ผู้บริหาร พนักงาน ลูกจ้าง และบุคคลภายนอกที่ปฏิบัติงานให้บริษัท

"ระบบคอมพิวเตอร์" หมายถึง เครื่องมือ หรืออุปกรณ์คอมพิวเตอร์ทุกชนิดทั้งฮาร์ดแวร์และซอฟต์แวร์พื้นฐานที่คอมพิวเตอร์จำเป็นต้องใช้ทำงาน เช่น ระบบปฏิบัติการ เป็นต้น อุปกรณ์เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั้งชนิดมีสายและไร้สาย อุปกรณ์จัดเก็บรักษาข้อมูลและการถ่ายโอนข้อมูลชนิดต่าง ๆ ระบบอินเทอร์เน็ตและอินทราเน็ตรวมถึงอุปกรณ์ไฟฟ้า อิเล็กทรอนิกส์และสื่อสารโทรคมนาคมต่าง ๆ ที่สามารถทำงาน หรือใช้งานได้ในลักษณะเช่นเดียวกัน ทั้งที่เป็นทรัพย์สินของบริษัท ของบริษัทคู่ค้า และบริษัทอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของผู้ใช้ระบบที่ได้รับอนุญาตให้นำเข้ามาติดตั้ง หรือใช้งาน

3 / "ระบบ...

"ระบบสารสนเทศ" หมายถึง ซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ที่ใช้งานระบบคอมพิวเตอร์เพื่อการประมวลผล จัดเก็บ จัดการข้อมูลคอมพิวเตอร์ทั้งที่เป็นทรัพย์สินของบริษัท ของบริษัทคู่ค้า และบริษัทอื่นที่อยู่ระหว่างการติดตั้ง และยังไม่ได้ส่งมอบ หรือของผู้ใช้ระบบที่ได้รับอนุญาตให้นำเข้ามาติดตั้ง หรือใช้งาน

"ข้อมูลสารสนเทศ" หมายถึง ข้อเท็จจริงที่ได้จากข้อมูล ซึ่งมีการนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งประกอบด้วยข่าวสาร บันทึก ประวัติ ข้อความในเอกสาร โปรแกรมคอมพิวเตอร์รูปภาพ เสียง เครื่องหมายและสัญลักษณ์ต่าง ๆ ไม่ว่าจะเก็บในรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือหรืออุปกรณ์ใด ๆ และสามารถนำไปใช้ประโยชน์ในการบริหารจัดการ การวางแผน การตัดสินใจ และอื่น ๆ

"ข้อมูลคอมพิวเตอร์" หมายถึง ข้อมูล ข่าวสาร บันทึก ข้อความใน เอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ รูปภาพ เสียง และรหัสต่าง ๆ ที่เป็นรูปแบบที่สามารถสื่อความหมายให้บุคคลสามารถเข้าใจได้โดยตรง หรือผ่านเครื่องมือ หรืออุปกรณ์ใด ๆ

"การรักษาความมั่นคงปลอดภัย" หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางด้านสารสนเทศ และไซเบอร์ทั้งจากภายในและภายนอกบริษัท อันกระทบต่อความมั่นคงของบริษัททั้งด้านการรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล และระบบสารสนเทศ

"ภัยคุกคามทางไซเบอร์" หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้าย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง

"ไซเบอร์" หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการของระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

"ISO/IEC 27001:2022" หมายถึง มาตรฐานระดับสากลในการจัดการด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems: ISMS) ประกอบด้วยข้อกำหนดที่ครอบคลุมถึงการจัดทำ นำไปปฏิบัติ ทบทวนและเฝ้าระวัง รักษาความต่อเนื่อง รวมถึงปรับปรุงระบบให้สอดคล้องกับสถานะการณ์ โดยวิเคราะห์ความเสี่ยงจากจุดอ่อนหรือช่องโหว่ของระบบ และหาวิธีปกป้องข้อมูลจากภัยคุกคามทางด้านสารสนเทศและไซเบอร์

4. หลักการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์มีหลักการที่สำคัญดังต่อไปนี้

4.1 **ความลับ (Confidentiality)** – การรักษาข้อมูลรวมถึงข้อมูลส่วนบุคคลหรือข้อมูลอื่นใด ให้มีความลับเข้าถึงได้เฉพาะผู้มีสิทธิ์ มีการป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

4.2 **ความเชื่อถือได้ (Integrity)** – การทำให้มั่นใจว่าข้อมูลมีความถูกต้องสมบูรณ์ เชื่อถือได้ และต้องไม่มีการแก้ไข ดัดแปลง หรือถูกทำลายโดยผู้ที่ไม่ได้รับอนุญาต

4.3 **ความพร้อมใช้งาน (Availability)** – การทำให้มั่นใจว่าระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลต่าง ๆ สามารถใช้งานได้อย่างต่อเนื่อง และไม่ถูกขัดขวางการทำงานทั้งจากความตั้งใจหรือจากภัยพิบัติต่าง ๆ

4.4 **การพิสูจน์ตัวตน (Authentication)** – การทำให้มั่นใจว่าการเข้าถึงระบบและข้อมูลต่าง ๆ เป็นการเข้าถึงจากผู้ที่ได้รับอนุญาตที่แท้จริงเท่านั้นและต้องผ่านกระบวนการยืนยันตัวตนที่เชื่อถือได้

4.5 **สิทธิการเข้าถึง (Authorization)** – มีการกำหนดระดับการเข้าถึงระบบและข้อมูลต่าง ๆ ตามสิทธิขั้นต่ำ (Least privilege) สอดคล้องกับสิทธิ์มาตรฐานการใช้งานที่ได้รับ

4.6 **การตรวจสอบย้อนกลับ (Auditability)** – การตรวจสอบย้อนกลับถึงการทำงานหรือการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้น ทำให้มั่นใจว่าสามารถตรวจย้อนหาผู้รับผิดชอบที่เกี่ยวข้องได้

4.7 **การปฏิเสธไม่ได้ (Non-repudiation)** – การทำให้มั่นใจว่ามีการระบุตัวตนของผู้ที่มีส่วนสำคัญในการสร้างหรือแก้ไข หรือตัดสินใจต่าง ๆ เกี่ยวกับการทำธุรกรรมที่เกิดขึ้น และไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้อง

5. การบริหารจัดการ

บริษัทกำหนดให้มีระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022 เพื่อให้การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางด้านสารสนเทศและไซเบอร์อย่างมีประสิทธิภาพมีการประเมินความเสี่ยง ป้องกันและเฝ้าระวังตรวจสอบ สามารถจัดการการคุกคาม บุกรุก แทรกแซงในรูปแบบต่าง ๆ ได้ สามารถเผชิญเหตุและตอบสนองได้อย่างถูกต้องและรวดเร็ว และมีกระบวนการฟื้นฟูความเสียหายได้อย่างครบถ้วน รวมถึง มีมาตรการควบคุมเชิงองค์กร (Organization Control) มาตรการควบคุมบุคลากร (People Control) มาตรการควบคุมเชิงกายภาพ (Physical Control) และมาตรการควบคุมเชิงเทคโนโลยี (Technological Control) โดยไม่ทำให้การดำเนินธุรกิจของบริษัทหยุดชะงักหรือมีประสิทธิภาพลดลง รวมทั้งทำให้ผู้ใช้ระบบมีความตระหนัก ความรู้ ความเข้าใจ สามารถปฏิบัติได้อย่างถูกต้องและเหมาะสม สอดคล้องกับข้อกำหนดของกฎหมาย และมาตรฐาน ISO/IEC 27001:2022 ดังนี้

5.1 การดำเนินงาน

บริษัทกำหนดให้มีมาตรการ และวิธีปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ หรือมาตรการอื่นที่เกี่ยวข้อง เป็นแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ซึ่งมีมาตรการต่าง ๆ ที่สำคัญ ดังนี้

5.1.1 การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายบุคคล

5.1.2 มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

5.1.3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

5.1.4 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

5.1.5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

บริษัทจะกำหนดระดับภัยคุกคามประกอบด้วย ภัยคุกคามระดับที่ไม่ร้ายแรง ภัยคุกคามระดับร้ายแรง และภัยคุกคามระดับวิกฤต ให้สอดคล้องตามที่กฎหมายกำหนด นอกจากนี้ บริษัทจัดให้มีการวิเคราะห์สาเหตุ วิธีการแก้ไขความเสียหายที่เกิดขึ้น อุปสรรคและความรวดเร็วในการแก้ปัญหาจากภัยคุกคามที่เกิดขึ้นเพื่อสร้างเป็นองค์ความรู้ กำหนดเป็นแนวทางป้องกันและการจัดการภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในภายหลัง

5 / 5.2 การฝ่าฝืน...

5.2 การฝ่าฝืนไม่ปฏิบัติตามนโยบาย

5.2.1 ผู้ใช้ระบบทุกคน ที่ฝ่าฝืนข้อกำหนดนโยบายฉบับนี้ บริษัทอาจจะพิจารณาดำเนินการทางวินัย และความรับผิดทางแพ่งและทางอาญาแก่บุคคลนั้น ตามกฎหมาย ข้อบังคับ ระเบียบ หรือประกาศที่เกี่ยวข้อง

5.3 การขอยกเว้นการปฏิบัติ

5.3.1 ในกรณีที่ต้องปฏิบัติแตกต่างหรือต้องยกเว้นการปฏิบัติตามหัวข้อใด ๆ ในมาตรการและแนวปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ที่จัดทำตามนโยบายฉบับนี้ ผู้ใช้ระบบทุกคนจะต้องดำเนินการร้องขอโดยใช้แบบฟอร์มขออนุมัติยกเว้นการปฏิบัติตามมาตรการและแนวปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ (รหัสเอกสาร FM-ISMS-001) โดยระบุเหตุผลและความจำเป็นสำหรับข้อยกเว้น และเสนอต่อคณะทำงานด้านเทคโนโลยีสารสนเทศ เพื่อพิจารณาอนุมัติ

5.4 การทบทวน

5.4.1 บริษัทมีการพิจารณาตรวจสอบ ทบทวน นโยบาย และมาตรการต่าง ๆ ที่จัดทำขึ้นอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

6. หน้าที่และความรับผิดชอบ

6.1 บริษัท มีหน้าที่ความรับผิดชอบ ดังนี้

6.1.1 กำหนดมาตรการ วิธีปฏิบัติ และแผนงานต่าง ๆ ที่เป็นมาตรฐานขั้นต่ำ เพื่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ โดยให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2022 กฎหมาย กฎระเบียบ ข้อบังคับ และแนวปฏิบัติที่ดีที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์

6.1.2 ควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของบริษัท

6.1.3 จัดหาผู้ที่มีความรู้ความสามารถมาเป็นผู้ดูแลระบบ หรือจัดฝึกอบรม ส่งเสริม หรือสนับสนุนผู้ดูแลระบบรวมถึง ผู้ใช้ระบบทุกคน ให้มีความรู้ความสามารถในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และไซเบอร์

6.1.4 จัดหาอุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์

6.1.5 เผยแพร่ ชี้แจง ส่งเสริมให้ผู้ใช้ระบบทุกคน รับทราบและปฏิบัติตามนโยบาย มาตรการ และวิธีปฏิบัติต่าง ๆ ของบริษัทที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ รวมถึงการตระหนักถึงบทบาทหน้าที่ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยในการใช้ทรัพย์สินสารสนเทศ และตรวจสอบติดตามการปฏิบัติตามนโยบายฉบับนี้ให้เป็นไปอย่างสอดคล้อง และนโยบายฉบับนี้ต้องสามารถเข้าถึงได้โดยผู้ใช้ระบบ

6.1.6 จัดทำคู่มือและข้อควรระวังการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศอย่างปลอดภัย และสื่อสารให้ผู้ใช้ระบบทุกคนได้รับทราบ

6.1.7 ดูแล แนะนำ และตักเตือน รวมทั้งการพิจารณาลงโทษแก่ผู้กระทำผิดต่อนโยบาย มาตรการ และวิธีปฏิบัติต่าง ๆ ของบริษัทที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ อย่างเสมอภาค และเป็นธรรม

6.1.8 ส่งเสริมให้มีการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

6.2 ผู้ใช้ระบบทุกคนมีหน้าที่ความรับผิดชอบ ดังนี้

6.2.1 ต้องเรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบาย มาตรการ วิธีปฏิบัติของบริษัทที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และไซเบอร์โดยเคร่งครัด

6.2.2 ให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการป้องกันระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัทจากภัยคุกคามทางด้านสารสนเทศและไซเบอร์

6.2.3 เข้าร่วมอบรม พัฒนาความรู้ ความเข้าใจต่าง ๆ อันเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ที่จัดให้โดยบริษัท

6.2.4 แจ้งให้บริษัททราบทันที เมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม หรือพบเห็นภัยคุกคามทางด้านสารสนเทศและไซเบอร์ที่อาจสร้างความเสียหายต่อบริษัท

ประกาศ ณ วันที่ 23 พฤศจิกายน 2566

(นางทองอุไร ลิ้มปิติ)

ประธานกรรมการบริษัท

คณะทำงานด้านความมั่นคงปลอดภัย (ISMS Core Team)

ฝ่ายกลยุทธ์เทคโนโลยีสารสนเทศ

โทร. (02) 267-1900 ต่อ 2401