288/2563

12 พฤษภาคม 2563

บริษัท ศักดิ์สยามลิสซิ่ง จำกัด (มหาชน)
นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

บริษัท ศักดิ์สยามลิสซิ่ง จำกัด (มหาชน) ให้ความสำคัญและตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยของภัยคุกคามทางไซเบอร์ และเพื่อให้สามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ บริษัทจึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้น ดังต่อไปนี้

1.คำนิยาม

"การรักษาความมั่นคงปลอดภัยไซเบอร์" หมายถึง กระบวนการและการกระทำใด ๆ เช่น การป้องกันรับมือ ลดความเสี่ยง การเข้มงวดกวดขัน การระมัดระวัง การเอาใจใส่ในการใช้งาน และการดูแลรักษาระบบคอมพิวเตอร์และข้อมูลสารสนเทศที่เป็นระบบและข้อมูลสำคัญ ให้พ้นจากความพยายามใด ๆ ในการเข้าถึง เพื่อโจรกรรมทำลายหรือแทรกแซงการทำงาน จนเป็นเหตุให้การดำเนินธุรกิจได้รับความเสียหาย

"ภัยคุกคามทางไซเบอร์" หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

"ไซเบอร์" หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเตอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมกันเป็นการทั่วไป

"บริษัท" หมายถึง บริษัท ศักดิ์สยามลิสซิ่ง จำกัด (มหาชน)

"หน่วยงานภายนอก" หมายถึง บุคคลหรือนิติบุคคลที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัท เช่น ที่ปรึกษา ผู้ให้บริการ ผู้รับจ้างพัฒนาระบบหรือจัดหาวัสดุอุปกรณ์ต่าง ๆ ผู้รับจ้างปฏิบัติงานให้กับบริษัท เป็นต้น

2. วัตถุประสงค์

1. เพื่อกำหนดแนวทาง หลักการในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์

2. เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนการปฏิบัติงานคำแนะนำ รวมถึงกฎหมายที่เกี่ยวข้องได้อย่างถูกต้องและเหมาะสม

3. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลายแทรกแซงการทำงานหรือโจรกรรมในรูปแบบต่าง ๆ ที่อาจสร้างความเสียหายต่อการดำเนินธุรกิจ

3. การกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์

1. บริษัทจะกำหนดบทบาทหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ เพื่อให้บริษัทมีมาตรฐานในการรักษาความปลอดภัยที่สามารถระบุ ป้องกัน ตรวจพบ รับมือและสามารถกู้คืนเพื่อกลับสู่

สภาวะปกติได้ และสนับสนุนให้บริษัทมีขีดความสามารถที่เพียงพอและเหมาะสมกับปริมาณและความซับซ้อนของระบบงานของบริษัท

2. บริษัทจะกำหนดให้มีหน่วยงานหรือผู้รับผิดชอบมีหน้าที่รับผิดชอบในการประเมิน ติดตามดูแลป้องกัน และรับมือกับภัยคุกคามทางไซเบอร์ และรายงานข้อมูลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ให้คณะกรรมการบริหารและคณะกรรมการบริหารความเสี่ยงได้รับทราบ ทั้งนี้ บริษัทอาจพิจารณากำหนดให้มีพนักงานเฉพาะเพื่อทำหน้าที่รับผิดชอบในการรับมือและจัดการกับเหตุการณ์ผิดปกติทางไซเบอร์ได้ทันเวลาเพื่อลดผลกระทบที่เกิดขึ้น

3. บริษัทจะให้ความรู้เรื่องภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เพื่อให้พนักงานมีความรู้ความเข้าใจและตระหนักถึงความจำเป็นในการรักษาความปลอดภัยและเข้าใจถึงผลกระทบที่จะเกิดขึ้นตามมาหากเกิดเหตุการณ์ขึ้น รวมทั้งสื่อสารแนวทางการป้องกันและการรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์

4. บริษัทจะกำหนดให้มีช่องทางในการประสานงานระหว่างหน่วยงานภายในและหน่วยงานภายนอกอย่างชัดเจน เพื่อกำหนดแนวทางในการรับมือและแก้ไขเหตุการณ์ทางด้านความปลอดภัยได้อย่างมีประสิทธิภาพ

4. การบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์

บริษัทจะกำหนดนโยบายในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ที่ครอบคลุมการระบุความเสี่ยงด้านภัยคุกคามทางไซเบอร์ การป้องกัน การตรวจพบ การรับมือ และการกู้คืน รวมทั้งทบทวนและปรับปรุงข้อมูลภัยคุกคามทางไซเบอร์ตลอดเวลา เพื่อให้เท่าทันต่อการเปลี่ยนแปลงที่เกิดขึ้น ดังนี้

1. การระบุ บริษัทจะทำการระบุว่ากระบวนการดำเนินงานและทรัพย์สินสารสนเทศใดบ้างที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ และต้องได้รับการรักษาความมั่นคงปลอดภัย เพื่อบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีผลต่อระบบ ทรัพย์สิน ข้อมูล ของบริษัทได้อย่างเหมาะสม

2. การป้องกัน บริษัทจะมีมาตรการป้องกันที่เหมาะสมเพื่อจำกัดผลกระทบของเหตุการณ์ภัยคุกคามทางไซเบอร์ ซึ่งครอบคลุมถึงเรื่องการควบคุมการเข้าถึง การฝึกอบรมและการสร้างความตระหนักให้แก่พนักงานและผู้เกี่ยวข้อง ความปลอดภัยของข้อมูล และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี นอกจากนี้ บริษัทจะทำการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบอิเล็กทรอนิกส์อย่างสม่ำเสมอ เพื่อให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง

3. การตรวจจับ บริษัทจะจัดให้มีกระบวนการติดตามเฝ้าระวัง และตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง และแจ้งเตือนถึงสิ่งผิดปกติต่าง ๆ รวมถึงการติดตามเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งภายในและภายนอก วิเคราะห์จุดอ่อนหรือช่องโหว่ของภัยคุกคามที่เกิดขึ้น เพื่อเป็นข้อมูลประกอบการในพิจารณาทบทวนแนวทางการป้องกันความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคต

4. การรับมือ บริษัทจะกำหนดแผนการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์และแนวทางแก้ไขปัญหา รวมถึงจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่องให้ครอบคลุมกรณีที่ผลกระทบหรือความเสียหายจากภัยคุกคามทางไซเบอร์ทำให้การดำเนินงานหยุดชะงัก เพื่อให้สามารถรักษาระดับความปลอดภัยและการให้บริการอย่างต่อเนื่อง และจะทำการวิเคราะห์หาสาเหตุและตรวจหาหลักฐานของภัยคุกคามที่เกิดขึ้น รวมถึงมีกระบวนการสื่อสารกับลูกค้าและผู้มีส่วนได้เสีย เพื่อความเข้าใจที่ถูกต้องตรงกันต่อสถานการณ์ที่เกิดขึ้นของบริษัท

5. การกู้คืน บริษัทจะกำหนดแผนและกระบวนการในการกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติภายในระยะเวลาที่กำหนด รวมถึงทำการทบทวนปรับปรุงแผนให้เป็นปัจจุบันเพื่อทันต่อสถานการณ์และนำบทเรียนที่ได้รับจากเหตุการณ์ภัย

คุกคามที่เกิดขึ้นมาเป็นส่วนหนึ่งในการทบทวนแผนและกระบวนการกู้คืนระบบให้มีประสิทธิภาพยิ่งขึ้น เพื่อป้องกันปัญหาและผลกระทบที่จะเกิดขึ้นซ้ำให้อนาคต

5. การทบทวนนโยบาย

ให้มีการทบทวนนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์และนำเสนอต่อคณะกรรมการบริษัทพิจารณาอนุมัติอย่างน้อยปีละ 1 ครั้ง

6. การบังคับใช้

ในกรณีที่ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 (พ.ร.บ.) ได้มีการแก้ไข หรือได้มีการประกาศกำหนดรายละเอียดในส่วนใดเพิ่มเติม ซึ่งขัดหรือแย้งโดยชัดแจ้งกับนโยบายฉบับนี้ หรืออาจส่งผลให้บริษัทหรือผู้ที่เกี่ยวข้องอาจเข้าข่ายเป็นผู้ฝ่าฝืน พ.ร.บ. ดังกล่าว ให้ พ.ร.บ. ในส่วนที่มีการแก้ไข และ/หรือประกาศหรือข้อกำหนดที่เกี่ยวข้องนั้นใช้บังคับแทนที่ในส่วนที่ขัดหรือแย้งโดยชัดแจ้งดังกล่าว

โดยนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้รับการอนุมัติจากคณะกรรมการบริษัท ในการประชุมครั้งที่ 3/2563 เมื่อวันที่ 12 พฤษภาคม 2563

ประกาศ ณ วันที่ 12 พฤษภาคม 2563

(นายศิวพงศ์ บุญสาลี)
กรรมการผู้จัดการ

<u>หมายเหตุ</u>

การประชุมคณะกรรมการบริษัท ครั้งที่ 8/2568 เมื่อวันที่ 11 พฤศจิกายน 2568 ได้ทบทวนแล้วเห็นว่านโยบายยังมีความเหมาะสม โดยไม่มีการเปลี่ยนแปลงจึงให้ใช้ฉบับเดิม

<u>การนำเสนอทบทวนอย่างน้อยปีละ 1 ครั้ง</u>

1. การประชุมคณะกรรมการบริษัท ครั้งที่ 1/2565 วันที่ 22 กุมภาพันธ์ 2565
2. การประชุมคณะกรรมการบริษัท ครั้งที่ 8/2565 วันที่ 10 พฤศจิกายน 2565
3. การประชุมคณะกรรมการบริษัท ครั้งที่ 9/2566 วันที่ 9 พฤศจิกายน 2566
4. การประชุมคณะกรรมการบริษัท ครั้งที่ 9/2567 วันที่ 24 ธันวาคม 2567
5. การประชุมคณะกรรมการบริษัท ครั้งที่ 8/2568 วันที่ 11 พฤศจิกายน 2568