เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้ บริษัท อินฟราเซท จำกัด (มหาชน) สามารถบริหารงานได้อย่างมีประสิทธิภาพสอดคล้องกับนโยบายด้านเทคโนโลยีสารสนเทศของบริษัท และการให้ความสำคัญและตระหนักถึงการบริหารจัดการความเสี่ยง ด้านความมั่นคงปลอดภัยของภัยคุกคามทางไซเบอร์ และเพื่อให้สามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นได้ อย่างมีประสิทธิภาพ บริษัทจึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้น ดังต่อไปนี้

1.คำนิยาม

"การรักษาความมั่นคงปลอดภัยไซเบอร์" (Cybersecurity) หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกบริษัท

"ภัยคุกคามทางไซเบอร์" (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของ คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

"ไซเบอร์" หมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่าย คอมพิวเตอร์ ระบบอินเตอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและ ระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมกันเป็นการทั่วไป

"บริษัท" หมายถึง บริษัทอินฟราเซท จำกัด (มหาชน)

“พนักงาน (Employee)” หมายถึง พนักงานที่ได้รับการว่าจ้างให้ทำงานเป็นพนักงานทดลองงาน พนักงานประจำ พนักงานสัญญาจ้างพิเศษ และผู้บริหารทุกระดับที่อยู่ภายใต้การจ้างงานของบริษัท

“หน่วยงานภายนอก” หมายถึง บุคคลหรือนิติบุคคลที่ดำเนินธุรกิจหรือให้บริการที่อาจได้รับสิทธิเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของบริษัท เช่น ที่ปรึกษา ผู้ให้บริการ ผู้รับจ้างพัฒนาระบบหรือ จัดหาวัสดุอุปกรณ์ต่าง ๆ ผู้รับจ้างปฏิบัติงานให้กับบริษัท เป็นต้น

2. วัตถุประสงค์

1. เพื่อกำหนดทิศทาง หลักการ และรายละเอียดของข้อกำหนดในการบริหารจัดการและการกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์โดยสอดคล้องกับกฎหมาย กฎระเบียบข้อบังคับ กรอบมาตรฐาน มาตรฐาน และข้อกำหนดต่างๆ ที่เกี่ยวข้องกับบริษัท

2. เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน ขั้นตอนการปฏิบัติงาน คำแนะนำ รวมถึงกฎหมายที่เกี่ยวข้องได้อย่างถูกต้องและเหมาะสม

3. เพื่อให้พนักงานและผู้ที่ต้องใช้หรือเชื่อมต่อระบบคอมพิวเตอร์ของบริษัท ให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม

4. เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่าง ๆ ที่อาจสร้างความเสียหายต่อการดำเนินธุรกิจ

3. การกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์

1. บริษัทจะกำหนดบทบาทหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการกำกับดูแลความเสี่ยงด้านภัย คุกคามทางไซเบอร์ เพื่อให้บริษัทมีมาตรฐานในการรักษาความปลอดภัยที่สามารถระบุ ป้องกัน ตรวจพบ รับมือ และสามารถกู้คืน เพื่อกลับสู่สภาวะปกติได้ และสนับสนุนให้บริษัทมีขีดความสามารถที่เพียงพอและเหมาะสม กับปริมาณและความซับซ้อนของระบบงานของบริษัท

2. บริษัทจะกำหนดให้มีหน่วยงานหรือผู้รับผิดชอบมีหน้าที่รับผิดชอบในการประเมิน ติดตามดูแล ป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ และรายงานข้อมูลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ให้คณะ กรรมการบริหารและคณะกรรมการบริหารความเสี่ยงได้รับทราบ ทั้งนี้ บริษัทอาจพิจารณากำหนดให้มีพนักงาน เฉพาะเพื่อทำหน้าที่รับผิดชอบในการรับมือและจัดการกับเหตุการณ์ผิดปกติทางไซเบอร์ได้ทันเวลาเพื่อลด ผลกระทบที่เกิดขึ้น

3. บริษัทจะให้ความรู้เรื่องภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เพื่อให้พนักงานมีความรู้ความเข้าใจและตระหนักถึงความจำเป็นในการรักษาความปลอดภัยและเข้าใจถึงผลกระทบที่จะเกิดขึ้นตามมาหากเกิดเหตุการณ์ ขึ้น รวมทั้งสื่อสารแนวทางการป้องกันและการรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์

4. บริษัทจะกำหนดให้มีช่องทางในการประสานงานระหว่างหน่วยงานภายในและหน่วยงานภายนอก อย่างชัดเจน เพื่อกำหนดแนวทางในการรับมือและแก้ไขเหตุการณ์ทางด้านความปลอดภัยได้อย่างมีประสิทธิภาพ

4. การบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์

บริษัทจะกำหนดนโยบายในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ที่ครอบคลุมการระบุความเสี่ยงด้านภัยคุกคามทางไซเบอร์ การป้องกัน การตรวจพบ การรับมือ และการกู้คืน รวมทั้งทบทวน และปรับปรุงข้อมูลภัยคุกคามทางไซเบอร์ตลอดเวลา เพื่อให้เท่าทันต่อการเปลี่ยนแปลงที่เกิดขึ้น ดังนี้

1. บริษัทจะทำการระบุว่ากระบวนการดำเนินงานและทรัพย์สินสารสนเทศใดบ้างที่มีความ เสี่ยงต่อการถูกโจมตีทางไซเบอร์ และต้องได้รับการรักษาความมั่นคงปลอดภัย เพื่อบริหารจัดการความเสี่ยงด้าน ภัยคุกคามทางไซเบอร์ที่มีผลต่อระบบ ทรัพย์สิน ข้อมูล ของบริษัทได้อย่างเหมาะสม

2. บริษัทจะมีมาตรการป้องกันที่เหมาะสมเพื่อจำกัดผลกระทบของเหตุการณ์ภัยคุกคาม ทางไซเบอร์ ซึ่งครอบคลุมถึงเรื่องการควบคุมการเข้าถึง การฝึกอบรมและการสร้างความตระหนักให้แก่พนักงาน และผู้เกี่ยวข้อง ความปลอดภัยของข้อมูล และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธี ปฏิบัติ ตลอดจนเทคโนโลยี นอกจากนี้ บริษัทจะทำการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบ อิเล็กทรอนิกส์อย่างสม่ำเสมอ เพื่อให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง

3. บริษัทจะจัดให้มีกระบวนการติดตามเฝ้าระวัง และตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง และแจ้งเตือนถึงสิ่งผิดปกติต่าง ๆ รวมถึงการติดตามเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ เกิดขึ้นทั้งภายในและภายนอก วิเคราะห์จุดอ่อนหรือช่องโหว่ของภัยคุกคามที่เกิดขึ้น เพื่อเป็นข้อมูลประกอบการ ในพิจารณาทบทวนแนวทางการป้องกันความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคต

4. บริษัทจะกำหนดแผนการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์และแนวทางแก้ไข ปัญหา รวมถึงจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่องให้ครอบคลุมกรณีที่ผลกระทบหรือความเสียหายจากภัย คุกคามทางไซเบอร์ทำให้การดำเนินงานหยุดชะงัก เพื่อให้สามารถรักษาระดับความปลอดภัยและการให้บริการอย่างต่อเนื่อง และจะทำการวิเคราะห์หาสาเหตุและตรวจหาหลักฐานของภัยคุกคามที่เกิดขึ้น รวมถึงมี กระบวนการสื่อสารกับลูกค้าและผู้มีส่วนได้เสีย เพื่อความเข้าใจที่ถูกต้องตรงกันต่อสถานการณ์ที่เกิดขึ้นของ บริษัท

5. บริษัทจะกำหนดแผนและกระบวนการในการกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ ภายในระยะเวลาที่กำหนด รวมถึงทำการทบทวนปรับปรุงแผนให้เป็นปัจจุบันเพื่อทันต่อสถานการณ์และนำ บทเรียนที่ได้รับจากเหตุการณ์ภัยคุกคามที่เกิดขึ้นมาเป็นส่วนหนึ่งในการทบทวนแผนและกระบวนการกู้คืนระบบ ให้มีประสิทธิภาพยิ่งขึ้น เพื่อป้องกันปัญหาและผลกระทบที่จะเกิดขึ้นซ้ำให้อนาคต

5. การทบทวนนโยบาย

บริษัทอาจให้มีการทบทวนนโยบายนี้เป็นครั้งคราวเพื่อให้สอดคล้องต่อข้อกำหนดตามกฎหมาย การเปลี่ยนแปลงการดำเนินงานของบริษัท รวมถึงข้อเสนอแนะจากหน่วยงานต่างๆ และนำเสนอต่อคณะกรรมการบริษัทพิจารณา

ทั้งนี้ มีผลบังคับใช้ตั้งแต่วันที่ 7 เดือน พฤศจิกายน พ.ศ. 2566 เป็นต้นไป