นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

บริษัท รักชัยห้องเย็น จำกัด กำหนดให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ต้องสอดคล้องกับนโยบายการบริหารความเสี่ยงองค์กร (Corporate Risk Management) และ ครอบคลุมในเรื่องดังต่อไปนี้

1. **การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

   ผู้จัดการแผนกเทคโนโลยีสารสนเทศมีหน้าที่รับผิดชอบในการศึกษา จัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่ แล้ว นำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

2. **การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ** (Information Technology Related Risk)

   2.1. ความเสี่ยงด้านกายภาพและสภาพแวดล้อม ได้แก่ ห้องศูนย์กลางข้อมูล (Data Center Room) ซึ่งเป็นที่จัดเก็บติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์เครือข่ายและอุปกรณ์อื่น ต้อง มีการควบคุมการเข้า-ออกและการใช้งาน การตรวจสอบระบบต่าง ๆ เช่น ระบบเตือนอัคคีภัย เป็นต้น

   2.2. ความเสี่ยงด้านการใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ เพื่อป้องกันการใช้งานการติดตั้งโปรแกรมที่ไม่ปลอดภัย เช่น การดาวน์โหลดโปรแกรมจากภายนอกมาติดตั้ง ซึ่งอาจมีชุดคำสั่งไม่พึงประสงค์ ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะ มัลแวร์ เช่น ไวรัสคอมพิวเตอร์ เข้าโจมตีเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องอื่นที่อยู่บนเครือข่ายเดียวกัน เป็นต้น

   2.3. ความเสี่ยงด้านการใช้งานระบบเครือข่ายคอมพิวเตอร์ ต้องมีการตรวจสอบและเฝ้าระวังการใช้งานเครือข่ายภายในและระบบอินเทอร์เน็ต ตรวจสอบและเฝ้าระวังช่องโหว่เชื่อมต่อเครือข่ายภายนอก โดยมีการจัดทำระบบป้องกันการเข้าถึงและการโจมตีจากภายนอกให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่ผู้ปฏิบัติงานใช้งาน เช่น ระบบป้องกันการเข้าออกใช้งานผ่านอินเทอร์เน็ต การติดตั้งโปรแกรมป้องกัน ชุดคำสั่งไม่พึงประสงค์ การกรองข้อมูลรับส่งอีเมล เป็นต้น

   2.4. ความเสี่ยงด้านบุคคล ต้องมีการกำหนดสิทธิ์การใช้งานและการเข้าถึงระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายต่างๆ ข้อมูล และข้อมูลส่วนบุคคล ให้เป็นไปตามสิทธิ์ที่พึงมี เพื่อป้องกันการเข้าถึง ใช้ แก้ไข เปลี่ยนแปลง ข้อมูลและข้อมูลส่วนบุคคลโดยมิชอบหรือโดยปราศจากอำนาจ

3. **การประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง โดยกำหนดความเสี่ยงไว้ 4 ประเภท ดังนี้**

   3.1. ความเสี่ยงด้านเทคนิค ที่อาจเกิดขึ้นจากคอมพิวเตอร์และอุปกรณ์ถูกโจมตี

   3.2. ความเสี่ยงจากผู้ปฏิบัติงานหรือความเสี่ยงด้านบุคคล ที่เกิดขึ้นจากการจัดการสิทธิ์ที่ไม่เหมาะสม ทำให้เกิดการเข้าถึงข้อมูลโดยมิชอบหรือปราศจากหรือนอกเหนืออำนาจหน้าที่ และอาจทำให้เกิดความเสียหายกับข้อมูลสารสนเทศได้

3.3. ความเสี่ยงจากภัยและสถานการณ์ฉุกเฉิน ที่เกิดขึ้นจากภัยพิบัติหรือธรรมชาติ รวมทั้งสถานการณ์อื่น เช่น กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง เป็นต้น

3.4. ความเสี่ยงด้านบริหารจัดการ ที่เกิดขึ้นจากนโยบายที่มีอยู่หรือการนำนโยบายไปปฏิบัติหรือการปฏิบัติงานซึ่งอาจไม่สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้น

4. **การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับยอมรับได้**

จัดทำตารางลักษณะรายละเอียดความความเสี่ยง (Description of Risk) โดยมี หัวเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง (Risk Map)

5. **กำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ** (Information Technology Risk Indicator)

กำหนดตัวชี้วัดระดับความเสี่ยงรวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

นโยบายการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) ฉบับนี้อนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1 เมื่อวันที่ 27 กุมภาพันธ์ 2566 และให้มีผลบังคับใช้ตั้งแต่วันที่ 27 กุมภาพันธ์ 2566

(.....)

ประธานกรรมการบริษัท

นายสุริยะ ประสาทบัณฑิตย์