นโยบายด้านการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

บริษัท ลีโอ โกลบอล โลจิสติกส์ จำกัด (มหาชน)

นโยบายด้านการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

(Information Technology & Cybersecurity Policy)

บริษัทได้จัดให้มีระบบเครือข่ายและคอมพิวเตอร์เพื่อสนับสนุนประสิทธิภาพการดำเนินงานของบริษัทให้สามารถตอบสนองเป้าหมายทางธุรกิจได้ดีที่สุด ดังนั้น บริษัทจึงถือว่าระบบเครือข่ายและคอมพิวเตอร์เป็นทรัพย์สินที่สำคัญของบริษัท ซึ่งผู้ปฏิบัติงานจะต้องใช้และดูแลรักษาให้อยู่ในสภาพที่พร้อมใช้งานได้อย่างมีประสิทธิภาพอยู่ตลอดเวลา ด้วยเหตุนี้ บริษัทจึงได้ประกาศนโยบายการใช้เครือข่ายและคอมพิวเตอร์ และได้มีการปรับปรุงเนื้อหานโยบายอย่างต่อเนื่อง เพื่อเป็นแนวทางในการใช้งานที่เหมาะสมและสอดคล้องกับเจตนารมณ์ของบริษัท โดยมีสาระสำคัญดังนี้

1. ขอบเขต

นโยบายฉบับนี้มีผลใช้บังคับกับกรรมการ ผู้บริหาร พนักงาน ลูกจ้างทุกคนของบริษัท บริษัทย่อย และบุคคลอื่นที่บริษัทอนุญาตให้เข้าใช้งานระบบเครือข่ายและคอมพิวเตอร์ และระบบข้อมูลของบริษัทรวมไปถึงการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ตโดยผ่านทางเครือข่ายของบริษัท โดยนโยบายฉบับนี้ ได้รับความเห็นชอบและได้รับอนุมัติจากคณะกรรมการบริษัทแล้ว ทั้งนี้ รายละเอียดแนวทางการปฏิบัติตามนโยบายจะถูกกำหนดไว้ในเอกสารแนวปฏิบัติด้านการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

2. หน้าที่ความรับผิดชอบ

2.1 **ประธานเจ้าหน้าที่บริหาร** ทำหน้าที่อนุมัตินโยบาย และพิจารณาการดำเนินการอนุมัติโครงการเมื่อเกิดเหตุการณ์ฉุกเฉิน รวมถึงการกำกับดูแล ติดตามแผนการบริหารโครงการด้านคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศของบริษัท เพื่อให้มั่นใจว่าผลลัพธ์ตรงตามความต้องการของธุรกิจและกลยุทธ์

2.2 **ประธานเจ้าหน้าที่ฝ่ายการเงิน** ทำหน้าที่กำกับดูแล กำหนดหลักเกณฑ์และแนวทางปฏิบัติ

2.3 **ผู้จัดการฝ่าย** ทำหน้าที่ควบคุมดูแลการปฏิบัติงานในภาพรวมของแผนก

- การมอบหมายหน้าที่ความรับผิดชอบให้แก่ผู้ดูแลระบบในการดูแลรักษาคอมพิวเตอร์ เครือข่าย และระบบข้อมูล
- การตัดสินใจด้านทรัพยากรในการจัดหาอุปกรณ์ตามความเหมาะสม
- กำกับดูแลความต่อเนื่องทางธุรกิจที่เกี่ยวข้องกับการดำเนินการด้านคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศ อาทิ การขอกู้คืนระบบหรือการย้ายไปทำงานที่ DR Site ในกรณีฉุกเฉิน

2.4 **ผู้จัดการส่วน / ผู้ดูแลระบบ** ทำหน้าที่ปฏิบัติการและบังคับใช้มาตรการความปลอดภัย

- การดูแลจัดการระบบเครือข่าย และระบบข้อมูล: การควบคุม ดูแล บำรุงรักษา และปรับปรุงเครือข่ายคอมพิวเตอร์ ตามแนวทางปฏิบัติของบริษัทและข้อกำหนดกฎหมายที่เกี่ยวข้อง
- การบริหารจัดการความปลอดภัยของระบบเทคโนโลยีสารสนเทศ อาทิ ระบบ Firewall และการกำหนดสิทธิการเข้าถึงข้อมูล
- การตอบสนองต่อเหตุการณ์: ตรวจสอบปัญหาและดำเนินการกู้คืนระบบตามแผนฉุกเฉิน (IT Continuity Plan) รวมถึงจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามกฎหมาย

3. กรอบแนวทางปฏิบัติ

3.1 บริษัทดำเนินการระบบเครือข่ายและคอมพิวเตอร์ และการเชื่อมต่อทางอินเทอร์เน็ตสอดคล้องตาม พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ที่มีผลบังคับใช้ และกฎหมายอื่นๆ ที่เกี่ยวข้อง

3.2 ดำเนินงานตามแนวปฏิบัติด้านการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด

3.3 ระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์ และอุปกรณ์เชื่อมต่อเป็นทรัพย์สินของบริษัทเพื่อการดำเนินการที่เกี่ยวข้องกับกิจการของบริษัทเท่านั้น

3.4 บริษัทจะดำเนินการเข้าตรวจสอบ เก็บหลักฐาน และกำหนดบทลงโทษตามระเบียบและข้อบังคับของบริษัท หากพบว่ามีการละเมิดนโยบายและแนวปฏิบัติการใช้งานระบบเครือข่ายและคอมพิวเตอร์ และการเชื่อมต่ออินเทอร์เน็ต

3.5 การใช้งานระบบเครือข่ายและคอมพิวเตอร์ และการเชื่อมต่อทางอินเทอร์เน็ตนั้นต้องไม่เป็นสาเหตุให้องค์กร และ บุคคลผู้ที่เกี่ยวข้องกับองค์กร เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

3.6 การบริหารจัดการข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย และการเชื่อมต่อทางอินเทอร์เน็ตของบริษัทให้เป็นไปตามข้อกำหนด กฎหมายการคุ้มครองข้อมูลส่วนบุคคล นโยบายการจัดการข้อมูลส่วนบุคคล (PDPA) และแนวปฏิบัติเกี่ยวกับ พรบ. คุ้มครองข้อมูลส่วนบุคคลของบริษัท

3.7 ดำเนินการตามแนวปฏิบัติความมั่นคงปลอดภัยของสารสนเทศของบริษัททั้ง 5 ด้าน

- การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)
- การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security)
- การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management)
- การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)
- การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)

3.8 พนักงานและบุคลากรที่เกี่ยวข้องจะต้องเข้าร่วมฝึกอบรม และทบทวนองค์ความรู้ด้านเทคโนโลยีสารสนเทศตามข้อกำหนด กฎหมาย และมาตรฐานในการบริหารจัดการด้านระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

นโยบายด้านการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ มีผลบังคับใช้ตั้งแต่วันที่ 15 พฤษภาคม 2569 เป็นต้นไป และจะมีการพิจารณาทบทวนอย่างน้อยปีละ 1 ครั้ง เพื่อนำเสนอต่อคณะกรรมการบริษัทอนุมัติ

(นายเสนีย์ แดงวัง)
ประธานคณะกรรมการบริษัท
บริษัท ลีโอ โกลบอล โลจิสติกส์ จำกัด (มหาชน)