Information Technology & Cybersecurity Policy

Leo Global Logistics Public Company Limited

Information Technology & Cybersecurity Policy

The Company has established network and computer systems to enhance operational efficiency and to support achievement of business goals. The Company therefore considers the network and computer systems as vital assets, for personnel to use and maintain fully functional at all times. Consequently, the Company has announced a network and computer utilization policy called Information Technology & Cybersecurity Policy. The Policy has been continuously updated and implement as digital code of conduct or practice guidelines for employees to use appropriately in line with the Company's intentions. The key points are as follows:

1. Scope

This Policy is applicable to all directors, executives, employees, and staff of the Company, subsidiaries, and other individuals authorized by the Company to access the Company's network and computer systems, and information systems, including internet connectivity through the Company's network. This Policy has been approved by the Company's Board of Directors. Detailed practice guidelines for compliance with this Policy are specified in the IT & Cybersecurity practice guidelines documents**.**

2. Duties and Responsibilities

2.1 Chief Executive Officer, having duties to approve the Policy and consider the approval of the project in emergency situations, including the governing & overseeing and monitoring of the Company's computer and IT system project management plan to ensure the outputs according to business requirements and strategy.

2.2 Chief Financial Officer, having duties to govern & oversee in terms of specifying criteria and practice guidelines.

2.3 Department Managers, having duties to control and oversee the overall operations of their departments:

- Assigning responsibilities to system administrator(s) for the maintenance of computers, networks, and data system
- Making decisions regarding resources: equipment procurement and provision, as appropriate
- Governing & overseeing business continuity related to computer and IT system operations, such as system recovery requests or relocation to a Disaster Recovery (DR) site in case of emergency, etc.

2.4 Section Manager/System Administrator, having duties regarding operations and security measures enforcement

- Oversee and manage network and information system: control, upkeep, maintenance, and computer networks improvement in accordance with the Company’s practice guidelines and related laws and regulations
- Manage IT security systems, such as Firewalls and access control, etc.

- Incident response: Investigate problems and implement system recovery according to the IT Continuity Plan, including storing computer traffic data as required by law.

3. Practice Guidelines Framework

3.1 The Company operates the network and computer systems, and internet connections in compliance with Thailand's Computer-Related Crime Act (CCA) and other relevant laws.

3.2 The Company strictly adheres to it's IT and Cybersecurity practice guidelines.

3.3 Computer systems, computers, and connectivity devices are properties of the Company and are used solely for business-related operations.

3.4 The Company shall conduct inspections, collect evidence, and impose penalties in accordance with Company rules and regulations if any violation is found concerning Policy and practice guidelines of the network and computer systems, and internet connection.

3.5 The use of network and computer systems, and internet connections, must not cause reputational damage to the organization or individuals associated with the organization, or involve them in illegal activities. Misuse of the internet is considered a disciplinary offense and may result in legal action.

3.6 The management of personal data related to the use of the Company's IT systems, network systems, and internet connections must comply with the regulations of the Personal Data Protection Act (PDPA), the Privacy Policy, and the Company's practice guidelines on PDPA.

3.7 Adheres to the Company's five (5) areas of IT security practice guidelines:

- Control of access to the computer center and damage prevention (Physical Security)
- Security of data, computer system, and network (Information and Network Security)
- Control of computer system development or modification (Change Management)
- Backup of data and computer system, including emergency preparedness (Backup and IT Continuity Plan)
- Control of the use of IT services from other service providers (IT Outsourcing)

3.8 All employees and relevant personnel are require to regularly attend IT training and refresher courses in compliance with the regulations, laws, and IT system management standards.

The Information Technology & Cybersecurity Policy is effective as of 15 May, and shall be subject to review at least once per year, with any revisions submitted to the Board of Directors for approval.

-Signature-

(Mr. Sanee Dangwang)

Chairman of the Board of Directors

Leo Global Logistics Public Company Limited