[Translation]

Information Technology Security and Cyber Resilience Policy

Introduction

The Company extensively processes digital information and utilizes information technology in its operations. Therefore, it is essential to assess and mitigate risks associated with the use of applications and information technology systems. Appropriate Information Technology Security ("IT Security") controls must be implemented to protect the organization from threats that may adversely affect business operations and customer services.

In addition, the Company must address emerging cybersecurity threats such as ransomware and malware attacks. Cyber Resilience refers to the Company's capability to continuously deliver its intended products and services even in the event of cyberattacks.

Operating Principles

The Company's information technology and cybersecurity practices are governed by key principles and controls to achieve the following objectives:

- **Confidentiality**
  To protect the confidentiality of information by preventing unauthorized access, use, or disclosure of data, including customers' personal data and the Company's business information.
- **Integrity**
  To ensure that customers' personal data and the Company's business information are not altered, modified, or destroyed by unauthorized persons.
- **Availability**
  To ensure that customers and authorized users are able to access information and services promptly and reliably whenever required.

Information Technology and Cybersecurity Requirements

In compliance with applicable legal and regulatory requirements, the Company has established an Information Technology Security and Cyber Resilience Policy covering the following key areas:

- Information asset management
- Information security
- Security of the Company's infrastructure and communication networks
- Security monitoring and surveillance
- System development lifecycle management
- Information system access management
- Physical and environmental security
- Operational security in information technology operations
- Information technology business continuity management

- Acceptable use of information and systems
- Cyber resilience
- Use of Artificial Intelligence (“AI”) and Machine Learning (“ML”)

Key Activities Undertaken During the Past Year

- The Company has implemented ongoing monitoring, surveillance, and reporting of information technology risk status against acceptable risk levels to the Risk Management Committee or Risk Oversight Committee on a regular basis. This enables timely decision-making and implementation of key information technology risk management policies.
- The Company has assigned the Information Technology Department and the Information Security and Cybersecurity Department to manage information technology risks within acceptable risk levels. These activities are recorded in a tracking system used for monitoring actions and follow-up activities. Such action plans are discussed during Information Technology Steering Committee meetings.
- The Company regularly conducts cybersecurity awareness assessments, such as phishing email simulations, for executives and employees at all levels. Additional targeted training is also provided to high-risk employee groups as necessary.
- The Company continuously communicates cybersecurity knowledge and awareness through internal communication channels to ensure employees remain informed of emerging cyber threats.