1. Purpose and Scope of Information Security:

Applicability: Information security covers employees, customers, suppliers, shareholders, and operations-related hardware and software.

Scope: To ensure corporate information security, related regulations and systems are established and technology and data security standards are set under the management system to protect the privacy of and maintain information security for employees, suppliers and customers in business activities.

2. Management Framework for Information Security Risks:

- The president establishes a cross-departmental information security management team, the IT department and administration department lead and plan information security and all business-related units implement information security to ensure the effectiveness of our information security management.
- The information security team establishes and periodically reviews and revises the information security management policy.
- The information security team periodically holds meetings to review policy implementation and report the state of implementation to the Board and review the policy every year.

3. Information Security Policy Objectives:

- Ensuring business continuity and providing reliable IT services.
- Ensuring the confidentiality, integrity, and availability of information assets in our custody and protecting the privacy of personnel.
- Establishing the business continuity plan (BCP) and implementing IT activities in compliance with related laws and regulations.

4. Information Security Control Measures:

- All employees, contractors, and suppliers must sign the non-disclosure agreement (NDA) to ensure their responsibilities and obligations for protecting the information assets acquired of the Company while providing information services or implementing related information tasks with our information in order to prevent unauthorized access, alteration, damage, or inappropriate disclosure.
- Important information systems or equipment shall be equipped with appropriate backup or monitoring mechanisms and drills are implemented regularly to maintain their availability.

- Anti-virus software shall be installed on all personal computers and virus definitions shall be updated periodically, and the use of unauthorized software shall be banned.
- Employees shall properly keep and use their user IDs, passwords, and authorization and change their passwords regularly.
- Standard operating procedures for addressing and reporting information incidents (an events) shall be established to take appropriate action and prevent damage from expanding.

All employees shall comply with the laws and regulations and the requirements in the information security policy. Supervisors shall supervise the compliance with the information security policy and enhance employees' awareness and legal compliance with information security.

5. 2021 State of Implementation of Information Security Publicity:

- Education and Training:

In 2021, we arranged 1.5 hours of e-learning courses and tests on information security for 71 new employees.

After course completion, related materials were posted on the employee portal for access by all employees for the promotion of information security.