The specific management plan for the company's information security management and the resources invested in information security management are as follows:

In order to fully protect the data of the company and its employees, customers, suppliers, shareholders and other stakeholders, the company continues to strengthen measures such as (1) data encryption management: all company-wide documents, archives, images, and software programs are encrypted. Management, if there is a need for reporting data related to customers and suppliers, an application and decryption procedure is required. Only external customers and suppliers can read the report to carry out business activities and provide relevant services to suppliers. (2) Establishment of internal antivirus software and external firewalls to prevent virus and hacking attacks: Recently, lots of companies have frequently been attacked by malicious software and computer viruses. Therefore, it is necessary to continuously strengthen information security awareness and, through training and real-time assistance from cybersecurity vendors, reduce the risks to the company's commitments to customers and shareholders, as well as mitigate the risks of significant adverse impacts on operating results, finances, and other areas.

(3) Summary of the 2024 Annual Information Security Monthly Report:

- Explanation of information security management items and management of abnormal event incidents. There were zero major incidents in the 2024 year. The company also strengthened key information security management measures, including endpoint virus attack and blocking records, network and host abnormal records, and external attack detection and blocking records. Additionally, plans for upgrading relevant network equipment were implemented.
- In response to the need for strengthening information security for sustainable development operations, the company established the "Information Business Sustainability Operation Management Guidelines" to ensure the proper management of company data. Data will be regularly backed up and disaster recovery plans will be formulated to support the sustainable development of the company's business.
- Continued monthly internal information security awareness campaigns and training for all employees.
- Enhanced protection against spam, phishing websites, and email attacks, and strengthened proactive management of information security messages, as well as high-risk and high-severity attack management. For example, unannounced social engineering (phishing) drills and social engineering awareness training were conducted irregularly. These activities included sending "bait phishing emails" to at least 300 recipients to improve internal recognition of phishing emails. Furthermore, regular information security awareness campaigns and external audits were conducted to enhance the overall information security awareness within the company.

(4) Resources Invested in Information Security Management

- Dedicated Personnel: The company has one dedicated supervisor and two full-time information security personnel responsible for planning and implementing the company’s information security policies, managing information system security, and introducing information security technologies to ensure continuous information security management.

- Information Security Awareness: To facilitate the company’s development and build a group-wide information integration system while effectively preventing the company’s critical information from being hacked or lost, the company regularly announces "online information security education and awareness campaigns" and establishes a computer information database (Information Security Endpoint Control System). These efforts aim to balance the implementation of group policies while protecting personal information privacy and security. Additionally, to prevent major information security incidents, the company strictly prohibits employees from executing, transmitting, or using non-company approved software programs for personal use or job-related activities.

- In 2024, produced more than four information security announcement awareness campaigns, covering topics such as「computer security updates, email security enhancement, legal software use for intellectual property, and phishing email awareness.」These campaigns communicated essential information security rules and precautions to all employees.