Information Security Implementation Report

VII. Cyber security management

(I) Cyber security risk management framework, policy, specific management plans, and resources put in cyber security management

1. Cyber security risk and management

■ Object:

Parties/Entities concerned: Employees, clients, suppliers and shareholders, as well as operation-related information software and hardware equipment.

■ Scope: To ensure the Company's information security, we formulated rules and regulations, adopted technology and data security standards, and incorporated them into the management and operations system to protect employees', suppliers', and clients' privacy and information security during business dealings.

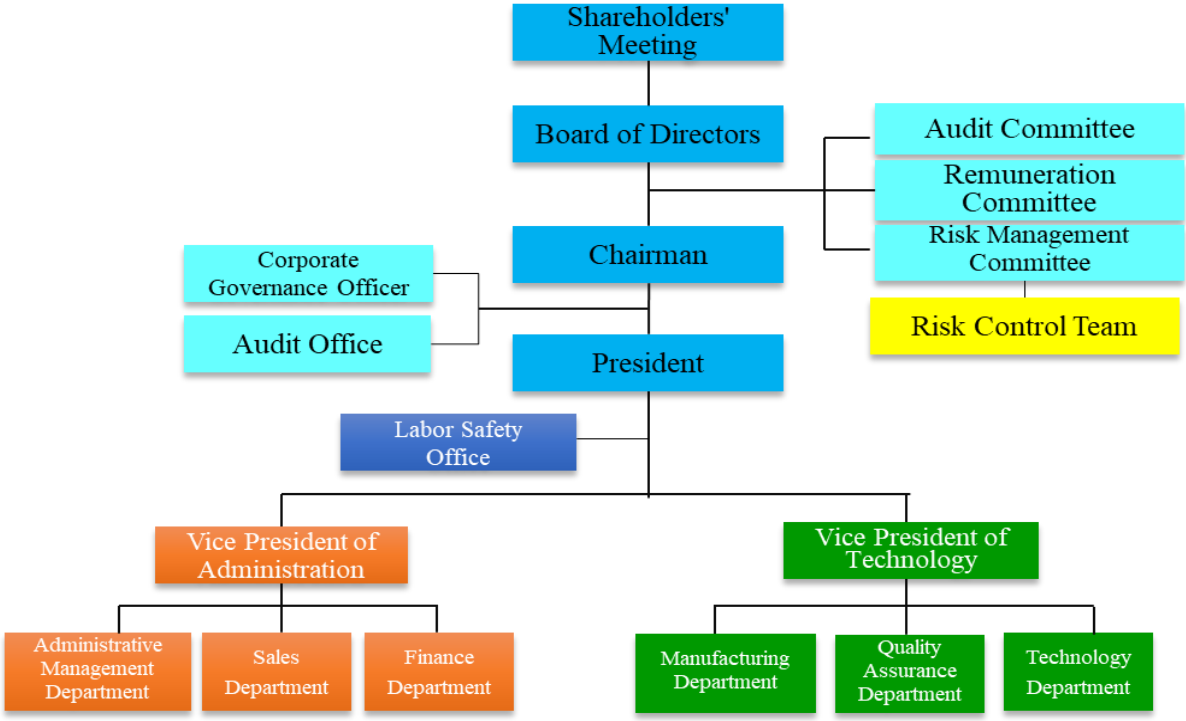
■ Cyber security risk management framework

To enhance the Company's stable operation and sustainable development, establish a complete risk management mechanism, and reasonably ensure that we achieve the Company's strategic goals, we have established a Risk Management Committee and formulated risk management policies and procedures in accordance with Article 27 of the Corporate Governance Best Practice Principles for TWSE/TPEX Listed Companies.

The Risk Management Committee assists the board in fulfilling its risk management responsibilities and is responsible for reviewing various risk management issues. A Risk Management Task Force is set up under the Risk Management Committee to assist the committee in fulfilling its risk management responsibilities. The Risk Management Committee meets at least twice per year and reports to the board at least once a year.

The executive secretary of the task force is served by a first-line manager at the Administrative Management Department, and the members of the task force are the middle managers or above from various departments. The task force is responsible for the overall risk management, including operational, financial, information security, environmental, compliance, and other risks.

Among them, information security risk management is conducted by the Information Section, Administrative Management Department. The section comprehensively manages the Company's information strategy planning, implementation, and management, optimizes the information system structure, enhances information management efficiency, and implements and regularly reviews and modifies information security systems and management measures.



2. Cyber security policy objectives

- Control information security risks, strengthen prevention, reinforce the information security structure and internal control, and ensure proper protection of information assets.
- Establish a complete management system to ensure the confidentiality and integrity of information assets.
- Establish an up-to-standard information security mechanism and regularly review and amend relevant operating regulations to comply with cyber security standards.
- Be commitment to integrating and managing all potential risks that may affect information security in proactive and cost-effective methods.

3. Specific cyber security management plans

- Regularly assess the impact of man-made and natural disasters on the Company's information assets and formulate a recovery plan to ensure business continuity.
- All employees of the Company as well as clients and suppliers who use or link with the Company's domain or computer systems should abide by the Company's information security regulations as required.
- Regularly offer internal information security and information system training courses and require information personnel to actively participate in information security seminars to enhance their professional skills.
- Regularly raise personnel' s awareness of information security policies and offer information security education and training to increase employees' awareness of information security.
- Announce any external major information security incidents by email and on the homepage of the Company's website, to remind employees of various types of information security threats and new threats to enhance their awareness of information security.
- Enhance information security, prevent the leaks of trade secrets, and manage permissions for user accounts, changes of VPN firewall connection rules, USB/storage devices, and

visitors' use of domains.

- Regularly carry out relevant backup protection measures for the information system structure, such as off-site host backup, cloud, and on-premises data backup, and power backup; test the restoration of backup data and the backup power system per month; inspect and update the operating systems in real time to ensure the normal operations of the information systems and the reliability of data retained.
- In accordance with the above policies, we regularly monitor subsidiaries' potential information security risks timely and take active measures to reduce potential harms.

4. Implementation of information security risk management

The company held two Risk Management Committee meetings and one meeting of the Risk Management Task Force during 2024 to review each department's implementation of the information security policies; they reported to the Board of Directors on October 30, 2024. No incident that undermined information security occurred during the year. According to the "Guidelines Governing the Establishment of Internal Control Systems in TWSE/TPEx Listed Companies", on November, 2022, a dedicated information security supervisor and qualified personnel were put in place, thus being implemented one year earlier than required.

▼Resources invested in cyber security management

Management countermeasures	Execution instructions
Develop information security management system	■As there are a certain number of systems and devices that need to be managed and they are scattered on different systems, management becomes more difficult. In order to achieve effective management, this system was developed to improve visibility and prevent in advance through a single platform and interface · Completion of development by the end of 2024.
Strengthen colleagues' information security awareness	■Promote information case examples every month to enhance colleagues' prevention awareness. ■Conduct internal penetration testing: In addition to reporting on their experiences, colleagues who have been successfully penetrated need to prepare a specific information security topic for company colleagues to teach colleagues to increase their vigilance and prevent being hacked.

5. Information security training and awareness-raising events:

- In 2024, the cumulative number of monthly information security awareness-raising sessions reached 12. This year, there were 2 information security infiltration sessions, with a total of 5 people (including subsidiaries) successfully infiltrated, and 3 sessions of education and training were arranged for 3 days and 3 times in September and October, respectively, with a total of 86 participants, in order to enhance the information security awareness of our colleagues.
- After several consecutive years of organizing penetration tests, the information security awareness of colleagues has gradually spread, but there are still some less alert colleagues, the information unit has been listed as a key target of concern, tracking and management at any time.

year	111	112	113
Number of Persons	9	2	5
Percentage of successful penetration	4.1%	1.8%	3.8%

- Courses related to risk awareness and prevention, such as information security and risk management113 The number of trainees in the year amounted to 142 with a total of 474 hours.

▼In 2024, a total of 142 person-times and 474 hours were spent on internal and external education and training：

Internal/External training	Category of course	Number of people	Number of hours/people
External training	Proactive Information Security Seminar	1	8
External training	Smart Factory Forum Spring Tour (Kaohsiung): Digital, Net-Zero, Dual-Axis Manufacturing Transformation	1	8
External training	cybersec 2024 Taiwan Information Security Conference	2	24
External training	5G+AIot join hands with ecological chain	2	16
External training	Proactive Information Security Seminar	2	4
External training	Secure Operational Technology Summit 2024	1	8
External training	TeamT5	2	3
Internal training	2024 Internal training-1	80	240
Internal training	2024 Internal training-2	6	18
Internal training	2024 Internal training-3	38	114
External training	DevDays Asia 2024	2	8
External training	TeamT5	2	3
External training	D Forum 2024 Smart Factory Forum	1	8
External training	025 CIO Insight Survey Presentation	1	8

(II) Specify the losses incurred due to major cyber security incidents, potential impacts, and countermeasures in the most recent year and up to the publication date of this annual report. If the amount cannot be reasonably estimated, please specify the fact that it cannot be reasonably estimated: N/A.