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

- The scope and purpose of cyber security

  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.

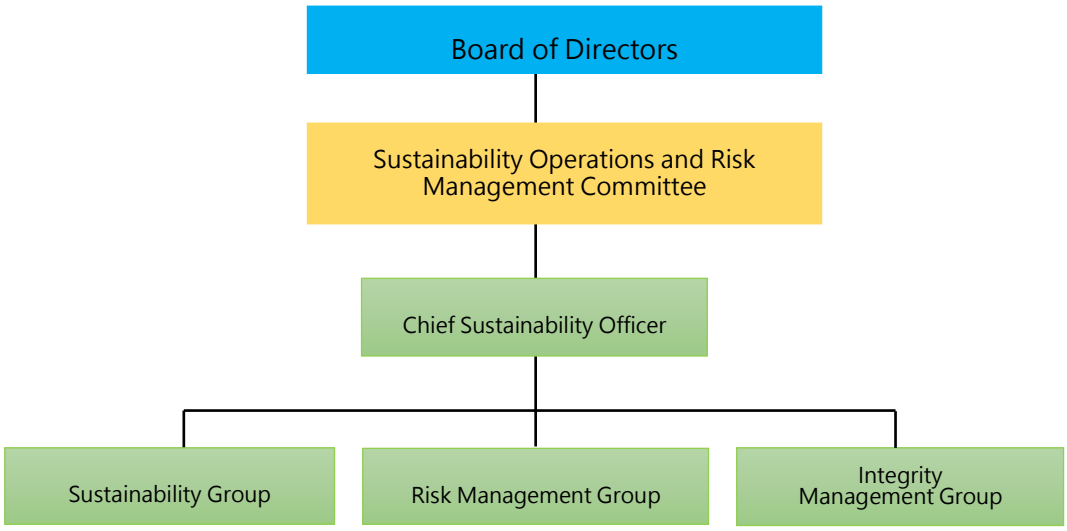
- Cyber security risk management framework

  To promote the Company's sound management and sustainable development, establish a robust risk management mechanism, and reasonably ensure the achievement of the Company's strategic objectives, the Sustainability and Risk Management Committee has been established pursuant to Article 27 of the "Code of Corporate Governance Practices for Listed and OTC Companies." This committee serves as a decision-making and executive body assisting the Board of Directors in advancing sustainable development, risk management, and integrity in business operations. It covers the three key areas of Environment (E), Social (S), Economic, and Corporate Governance (G). The Committee is responsible for formulating risk management policies, identifying risks, assessing impacts, establishing integrity management principles, and developing corresponding strategies and action plans regarding sustainability issues related to the Company's operations. Under the Sustainability and Risk Management Committee, a Chief Sustainability Officer (CSO) shall be appointed to coordinate and lead three working groups: the "Sustainability Working Group," the "Risk Management Working Group," and the "Ethical Business Practices Working Group." These groups are responsible for the operation of relevant matters and the implementation of the Committee's resolutions, and shall regularly report their implementation plans and results to the Committee, which in turn shall report to the Board of Directors. The Sustainability and Risk Management Committee shall meet at least twice a year and report to the Board of Directors at least once a year.

  The "Risk Management Team," composed of heads of various operational units or their designated representatives, serves as the Company's unit responsible for promoting and implementing risk management. It assesses the extent of both negative and positive impacts that may arise from risks affecting the Company's sustainable operations and regularly reviews the significant risks associated with various business operations in accordance with the Company's established "Risk Management Policy and Procedures." It is also responsible for overall risk management matters, including operational risks, financial risks, information security risks, environmental risks, compliance risks, and other risks not falling under the aforementioned categories.

  Regarding information security risk management, the Information Section of the Company's Administrative Management Division is responsible for overseeing the planning, execution, and management of the Company's information strategy, optimizing the information system

architecture, enhancing information management efficiency, and implementing, periodically reviewing, and revising information security systems and management practices.



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. In 2025, the Company convened two Risk Management Committee meetings and two Risk Management Staff Executive Group meetings to review the implementation of information security policies across all departments. On October 28, 2025, the Company reported to the Board of Directors that neither TTMC nor its subsidiaries had experienced any incidents that compromised information security during the current fiscal year. In accordance with the "Guidelines for the Establishment of Internal Control Systems by Publicly Traded Companies," the Company appointed one dedicated information security manager and one dedicated information security officer in November 2022, implementing these measures one year ahead of the regulatory requirement.

▼Resources invested in cyber security management

Management countermeasures	Execution instructions
Update the company's operating system to the latest version	■Strengthen information security measures by updating the environment to address potential security risks in existing systems, ensuring that the new version of the ERP and related systems have a secure and stable foundation for operation. ■The current procurement project is replacing legacy systems on-site and will gradually expand to core systems, with completion expected by mid-year.
Raise employees' awareness of information security	■Conduct monthly presentations on real-life cybersecurity incidents to raise employees' awareness of prevention measures. ■ Conduct internal penetration tests: Employees who are successfully compromised must not only submit a report on their experience but also prepare a specific cybersecurity topic to present to their colleagues, thereby strengthening their vigilance and ability to prevent hacking.

5. Information security training and awareness-raising events:

(1) In 2025, a total of 12 information security awareness campaigns were conducted monthly; two penetration tests were carried out, successfully compromising three systems. Three-day training sessions were scheduled in September and October, with a total of 112 participants, to enhance employees' information security awareness..

(2) After conducting penetration tests for several consecutive years, cybersecurity awareness has gradually become widespread among employees; however, there are still some employees who remain less vigilant. The IT department has identified these individuals as a priority for monitoring and is tracking and managing them on an ongoing basis.

Year	Number of Successful Penetrations	Total Number of Penetrations	Penetration Success Rate	Note
2022	12	140	8.57%	TTMC114 employees; subsidiaries: 26 employees
2023	2	141	1.42%	TTMC116 employees; subsidiaries: 25 employees
2024	5	116	4.31%	TTMC116 employees
2025	3	112	2.68%	TTMC112 employees

(3) Regarding courses on risk awareness and prevention, such as information security and risk management, a total of 96 participants completed training in 2025, totaling 291 hours.

▼The table below summarizes internal and external training and publicity:

Internal/External training	Category of course	Number of people	Number of hours/people
External training	D Forum 2025 Smart Factory Forum (Kaohsiung) Harnessing AI, Shaping the Future: Green and Sustainable Manufacturing	2	8
External training	CYBERSEC 2025 Taiwan Cybersecurity Conference: Cybercrime Trends and the Cybersecurity Defense Revolution in the AI Era; Sovereign AI and Resilient Nations: AI-Driven Intelligent Protection and Efficient Operations	2	24
External training	Computex Taipei	1	24
External training	Fortinet Accelerate25 Taiwan	2	4
Internal training	Software Licensing Compliance	3	1
Internal training	Cybersecurity Training	92	2

(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: The Company and its subsidiaries have not suffered any loss due to material information security incidents.