2.5 Cybersecurity

2.5.1 Cybersecurity risk management framework

In accordance with international cybersecurity management practices, personal data protection standards, and legal regulations, and in consideration of the "concerns of internal and external stakeholders," the Company has established the "Cybersecurity Management System" to ensure that our IT infrastructure and information systems meet the requirements for confidentiality, integrity, availability, and legality.

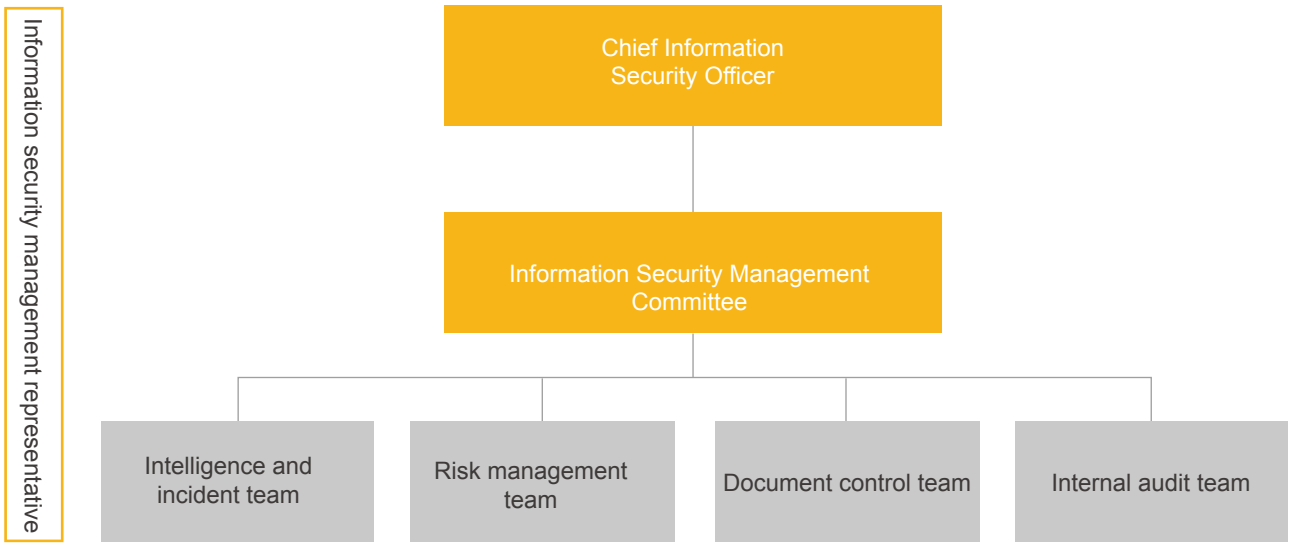
We also integrated and strengthened the cybersecurity management system based on the continuous improvement of the PDCA cycle process management model. In March 2024, the Company obtained certification for the latest and highest international standard for information security management, ISO/IEC 27001:2022, demonstrating our commitment to the highest standards of information security. We actively strive to establish a secure system environment to ensure the safety and stability of all operations, thereby supporting the Company's long-term sustainable development.

2.5.2 General Policy for Cybersecurity Management

The Chairman of the Company has appointed an Assistant Manager of the IT Department to set up an internal Cybersecurity Management Committee to be responsible for formulating the Company's cybersecurity management policy. A dedicated unit, managers, and personnel are set up to plan and implement cybersecurity operations. Based on the principles of simplicity, easy-to-remember, and compliance with cybersecurity management objectives, the Company has formulated the cybersecurity policy statement: "Cybersecurity is everyone's responsibility."

2.5.3 Cybersecurity Management Organization

In order to ensure that the operation of the Company's cybersecurity management system can meet the Company's policies and goals, and to confirm its continuous application and the effectiveness of its operation, the Company has established the "Cybersecurity Organization and Management Review Procedures" to regulate the Company's information and serve as the basis for the management's regular evaluation of the cybersecurity management system. Below is the organization chart:



- Scope of application: The Company's headquarters and plants in Taiwan.
- Goals:

  The Company's cybersecurity goal is to ensure the confidentiality, integrity, availability, and compliance of important and core systems.

  Quantitative metrics of cybersecurity performance are defined and measured according to each hierarchy and function to confirm the implementation status of the cybersecurity management system and whether the cybersecurity goals are achieved.

Confidentiality	Avoid leaking any sensitive information about the Company to the internet.
Completeness	Ensure the accuracy of the Company's sensitive data (e.g. financial information, personnel data, system information)
Usability	Ensure that important data held by the Company are backed up.
Compliance	The Company shall ensure that it does not violate the cybersecurity requirements of laws, regulations, or contractual obligations.

2.5.4 Cybersecurity management measures and implementation effectiveness

Management items	Scope of operation	Implementation measures	Execution Progress
1. Network security protection	1. Prevent hacker intrusions and damage 2. Ensure smooth network operation	1. Network infrastructure has been established in the plants, separating IT and OT networks 2. Introduced zero-trust network architecture 3. Continue to refine the management strategy of network protection equipment and optimize the control operation process	No incidents of hacking occurred in 2024
2. Email security control	1. Protect the Company's sensitive data from being leaked 2. Reduce the risk of external cybersecurity threats entering employee mailboxes	1. Established advanced email defense management system 2. An email audit system has been established	No abnormal event occurred in 2024
3. Device safety protection	1. Protect the Company's internal information equipment from virus attacks or malicious intrusion 2. Protect the Company's sensitive data from being leaked	1. Anti-virus software and endpoint protection software protection devices (PC/NB, machine computers) are in place 2. Controlled the use of NB/PC external devices and cloud space 3. The privileged account management system has been introduced to strengthen the security of system account management. 4. Continue to improve system cybersecurity vulnerability control items	No abnormal event occurred in 2024
4. System/measure education and promotion	1. Optimize cybersecurity policies and information security operating regulations 2. Cybersecurity policy/ regulation promotion and education training	1. The ISO27001 cybersecurity management system has been introduced, and management measures, specifications, and operating guidelines have been continuously updated 2. Provide training for new recruits 3. Regularly promote cybersecurity-related topics through email	100% achieved by 2024
5. Disaster recovery and response	1. Data backup integrity and compliance 2. System backup and activation capability	1. Build a cloud backup system to enhance the emergency response capability 2. Regularly implement disaster recovery system drills 3. Optimize the efficiency of backup system switching operations and shorten the operation time for emergency activation	No abnormal event occurred in 2024