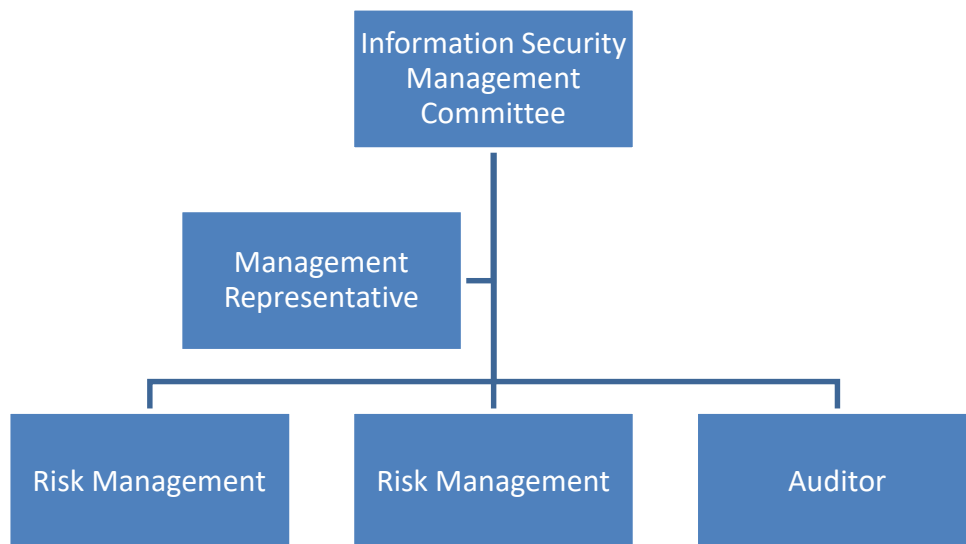


The structure of information security risk management

The company has established an "Information Security Management Committee" to be responsible for implementing information operation security management plans, establishing and maintaining information security management systems, and coordinating the formulation, implementation and risk management of information security and related policies.

The Information Security Management Committee is convened by the general manager and headed by a management representative. Directors of all units within the company (including legal affairs, human resources, materials, management, etc.) are members of the committee; the management representative is responsible for assisting the company's information security planning, Coordinate related audit matters and supervise the operation of this committee.



Information Security Policy

The company's information security policy is guided by: 1. Maintaining the continuous operation of the system; 2. Preventing intrusion and destruction by hackers, viruses, etc.; 3. Preventing improper and illegal use with human intentions; 4. Maintaining the safety of the physical operating environment. With the goal of anti-virus, anti-hacking and anti-leakage, firewalls, intrusion detection, anti-virus systems and many internal control systems are established to enhance the company's ability to defend against external attacks and ensure the protection of internal confidential information. In order to strengthen information security, our company has introduced ISO27001 information security management system certification so that all information systems can operate under standard management specifications and reduce security loopholes and abnormalities caused by human negligence. To build a multi-layer information security protection mechanism and

strengthen information security and network security protection processes to protect the company's important assets. In addition, the effectiveness of information security management is regularly monitored to ensure continuous improvement of information security management and defense capabilities, and information security education and training are reviewed and continuously improved to enhance information security awareness.

Specific management plan

In order to achieve information security policies and goals and establish comprehensive information security protection, the management matters and specific management plans implemented are as follows:

- Improve information security defense capabilities: Conduct regular drills and tests of information security systems, and strengthen and repair them to reduce information security risks.
- Improve network, endpoint and application security: Optimization of the overall information system network security area and protection of important host account authentication.
- Legal compliance, risk management and education and training: legal promotion, anti-virus, information security protection measures and risk management information security education and training for employees to enhance information security awareness so that information security operations can be implemented for every employee.

Invest resources in information security management

- Dedicated manpower: A dedicated information security management organization is established to be responsible for the company's information security planning, technology introduction and related audit matters in order to maintain and continuously strengthen information security.
- Certification: Passed ISO27001 information security certification, and there are no major deficiencies in relevant information security audits.
- Customer satisfaction: There are no major information security incidents and no complaints about breach of customer data and loss.
- Education and training: All employees (including new employees) have completed information security education and training courses: Annual information security education and training sessions totaled 11 classes and 190 participants in 2024; Conducted 2 social engineering phishing email tests and 6 operational scenario drills in 2024.
- Information security announcements and promotions: We produce information security announcements from time to time, with a total of more than 10 information security announcements produced to convey important information security protection regulations and precautions.