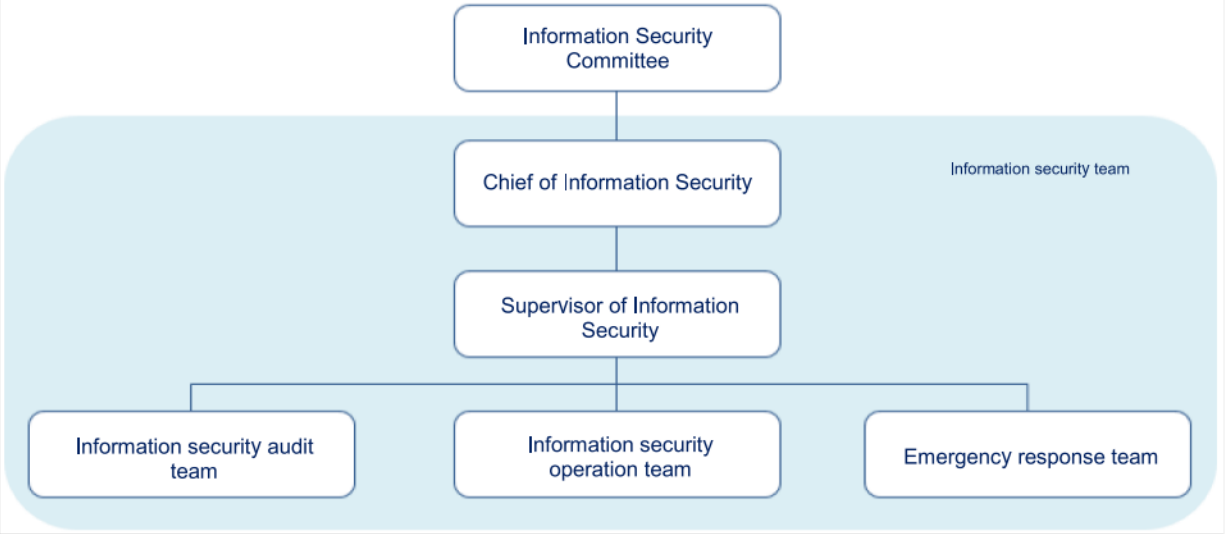
IX. Information security management

- **Management organization**

The Information Safety Management Committee was established to strengthen the company's information security management and ensure security of its data, system, and network. The chief information security officer serves as the convener of the Committee, and reports to the board of directors at least once a year. The organization of the Committee includes the information security operation team, emergency response team, and information security audit team. The information security operation team implements the building of the Information Security Management System, including network management and system management; The emergency handling team is responsible for operating continuity plan specifications and crisis handling procedures, implementing crisis response measures and reporting, and conducting post-incident analysis and prevention; The information security audit team cooperates with the company's audit unit to conduct information security auditing, including internal and external auditing.



- **Risk management mechanisms**

Execute management of the IT server room, computer information file security, network security, mail security management, information system control access, etc.

- **Information security policy**

The company's information security policy aims to "maintain the confidentiality, integrity, availability, and legality of company information, and avoid human negligence, deliberate destruction, and natural disasters, which result in improper use, leakage, tampering, damage, or disappearance of information and assets which affect the company's operations and cause damage to the company's rights and interests." The company introduced the ISO 27001 information management system in 2016, and has regularly obtained ISO 27001 certification. The current certificate is valid from August 2022 to August 2025. Through the introduction of the ISO 27001 information security management system, the ability to respond to information security incidents has been strengthened, and assets of the company and customers are more secure.

Specific information security management plan

Item	Specific management measures
Firewall protection	1. Set firewall connection rules. 2. Can only be opened with the approval of the responsible supervisor when there are special connection needs.
User Internet access control mechanism	1. Use an automatic website protection system to control users' online behavior. 2. Automatically filter users' Internet access to websites that may have links to Trojans, ransomware, or malicious programs.
Antivirus software	Use antivirus software and automatically update virus pattern files to reduce the chance of infection.
Updating of the operating system	The operating system is automatically updated. If it is not updated for some reason, the information center will assist in updating.
Email security control	1. There is automatic email threat scanning protection that prevents suspicious attachment files, phishing emails, spam emails, and expands the protection range against malicious links before users receive emails. 2. After a personal computer receives an email, the antivirus software also scans it for suspicious attachment files.
Data backup mechanism	Every important information system database is set up for daily backup.
Important file upload server	The important files of each department in the company are stored on this server, which is backed up and saved by the information center.
Information security insurance	The company's customers are mainly corporate customers, and there is no risk of consumer personal data custody. After evaluating the insurance coverage and applicable industries for IT security insurance on the market, we have not purchased capital security insurance for the time being. However, in response to the challenges faced by information security, certain software and hardware have been imported, such as firewalls, anti-virus software, intrusion prevention systems, etc., and we continue to pay attention to the changing trends of the information environment and strengthen our employees' awareness of information security crises and the ability of information security handlers to respond to such crises.

- **Emergency notification procedure**

When an information security incident occurs, the unit(s) to which it occurred will notify the information security team—emergency handling team, determine the type of the incident, find the problem point, deal with it immediately, and leave a record.

- **Losses, possible impacts, and countermeasures due to material information security incidents: None**