Information Security Management

(A) Describe the information security risk management structure, information security policies, specific management plans and resources invested in information security management, etc.:

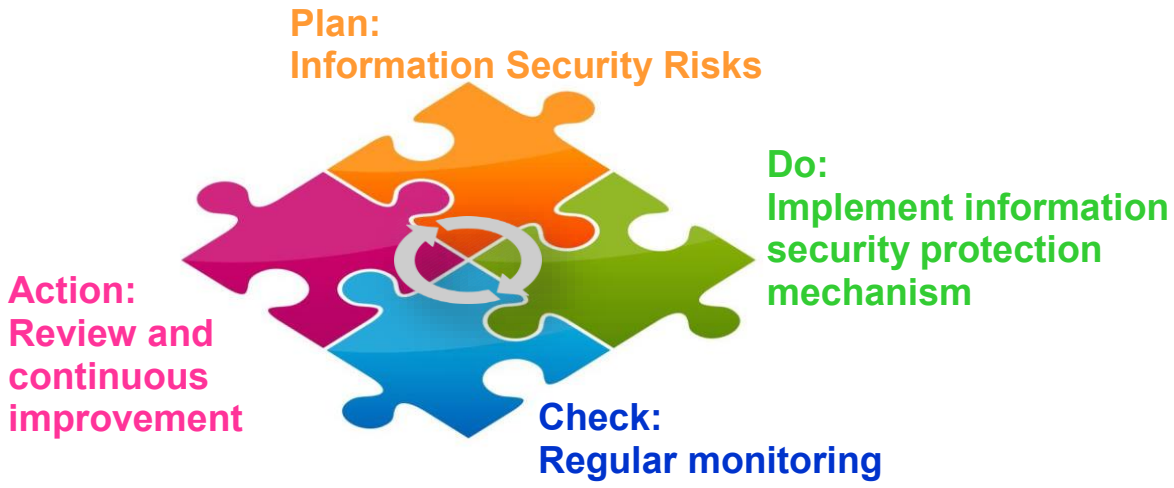
1. Information Security Organizational Structure:

The company established the "Information Security Committee" in 2022, which is responsible for implementing information security management plans, establishing and maintaining information security management systems, and coordinating the formulation, implementation, risk management and compliance assessment of information security and protection-related policies.

The Information Security Committee is composed of the Executive Vice President as the chief information security officer and the senior division director as the general convener. Each business unit appoints representatives to hold at least one information security meeting every year to discuss information security policies and other major information security-related issues to ensure information security. Management achieves confidentiality, integrity and availability, and regularly reports information security implementation status to the board of directors once a year.

2.Information Security Policy:

- The company attaches great importance to information security and is committed to protecting customer privacy and confidential information. It strictly abides by customer contracts and protects customer privacy and confidential information.
- Ensure the confidentiality, integrity and availability of the company's important assets and comply with relevant laws and regulations.
- The company has passed ISO27001 certification and follows the information security management mechanism, using the PDCA method for correction and prevention, and continues to strengthen the information security management mechanism.
- Strengthen employees' security awareness and capabilities, and conducts information security courses and information security awareness for all employees. Regularly conduct social engineering drills to strengthen employees' ability to identify and respond to phishing emails.



Specific Management Plan:

Control Plan	Control Results
Network Security	● **Next-generation firewall:** Have intrusion detection and prevention mechanisms, regularly checks firewall policies and vulnerabilities, and blocks malicious traffic in real time. ● **Network Segmentation:** Network segmentation to prevent computer viruses or malicious attacks from spreading across factories. ● **Information Security Threat Detection and Management Mechanism (SOC: Security Operation Center):** Aggregates information security information, real-timely grasps internal and external information security threats and response measures, and minimizes damage.
Device Security	● **Active E-mail filtering system.** ● **Active personal mobile device and portable media management and usage control.** ● **Active detection of unreasonable application for software installation.** ● **Dr. IP:** Before a new machine is connected to the network, it must complete a virus scan to prevent the

	risk of virus infection and spreading.
Data Security and Protection	● **USB and printing controls:** data encryption, transmission encryption, access rights control. ● **Document Control Procedures:** Establish confidentiality levels and reading permissions. Important documents are protected by encryption software to prevent the leakage of sensitive information. ● Two-factor authentication (MFA): Check user legitimacy through two step verification to prevent unauthorized users from accessing company internal information
Computer Security Management	● **Personal account password management:** Force password changes regularly and comply with password complexity rules. ● **Anti-virus Software:** Update virus codes in a timely manner, automatically send updates to users' computers, and scan the entire machine regularly every week.
External threat detection and protection	● **Penetration testing and vulnerability scanning:** Regularly outsourced to third-party information security vendors, and reinforced and repaired to reduce information security risks. ● **Third-party risk assessment system:** Monitor and analyze information security risks and vulnerabilities
Supplier Management	● **Sign a confidentiality contract:** Ensure the use of the company's information assets to prevent unauthorized access, modification, and destruction. ● **Supplier education and training:** regularly organize information security education and training for suppliers
Improve information security defense capabilities	● **Provide Security education and training for new employees and sign a confidentiality agreement** ● **All Employees:** Safety awareness education and training for all employees is conducted regularly every year and the training completion rate is 100% ● **Social engineering phishing email drills:** Conducted regularly every year to enhance employee security

	awareness ● **Information security awareness promotion:** Promote information through computer startup screens and posters from time to time
Operations continuity and security incident management	● **Perform disaster recovery drills:** Conduct drills for important systems every year ● **Establish information security incident reporting and handling procedures:** determine incident impact and damage assessment, internal and external reporting procedures

Invest resources in information security management:

Unit:NTD

Resources Invested	2022	2023	2024
Amount invested in information security project	5 Million	7 Million	10 Million
Information security project manpower allocation	Information security manager: 1 person Responsible personnel: 2 people	Chief of Information Security:1 person Information security manager: 1 person Responsible personnel: 2 people	Chief of Information Security:1 person Information security manager: 1 person Responsible personnel: 2 people Additional responsibility: 2 people
Establish information security policies and goals	V	V	V
Convene information security committee regularly	V	V	V
Obtained ISO27001	V	V	V

certification			
vulnerability scanning, penetration testing, social engineering drill	V	V	V
Information security education training and promotion	V	V	V
Join the Information Security Joint Defense	V	V	V
Report regularly to the board of directors	X	X	V
Information security incidents	**X**	**X**	**X**

- Dedicated personnel: There are two full-time information security personnel and two part-time information security personnel who are responsible for the planning and implementation of the company's information security policy, information system security management and information security technology introduction, in order to maintain and continuously strengthen information security management.
- Certification: Passed ISO27001 information security verification (the current certificate is valid from October 13, 2022 to October 31, 2025), and there are no major deficiencies in the relevant information security audit.
- Information Security Committee: The Information Security Committee is convened at least once a year to review the effectiveness of the information security policy.
- Information security education and training: All new colleagues must complete new employee information security education and training; all employees must complete online education and training once a year and pass the test, with a 100% completion rate; information units must have at least 3 hours of information security education and training every year; Security personnel participate in more than 40 hours of external seminars and professional training courses every year; they conduct a social phishing email test once a year.
- Information security promotion: Promote information security rules and

precautions from time to time through startup screens or posters at least 5 times a year.

- Our company has joined the Taiwan Computer Network Crisis Management and Coordination Center (TWCERT/CC), Taiwan Information Security Bulletin Annual Conference to collect information security information collection and analysis practices, CYBERSEC Taiwan Information Security Conference, regularly collect external threat information, and based on the information Conduct risk assessments on information content and strengthen protection against external information security threats.
- Information security implementation status is reported to the board of directors once a year, with the latest report date being November 8, 2024.

(A) **List the losses, possible impacts and response measures suffered due to major information security incidents in the most recent year and up to the date of publication of the annual report. If it cannot be reasonably estimated, the fact that it cannot be reasonably estimated should be stated:** the most recent year and as of the publication date of the annual report, the Company has not discovered any cyber-attacks that have a significant impact on the company's operations.