Ablerex Electronics Co., Ltd.

Implementation of Information Security Risk Management

Date : Nov 3, 2025

Foreword:

The Company is committed to upholding the rights and interests of its investors, shareholders, customers, suppliers, employees, financial institutions, government agencies, neighboring communities, and other stakeholders, supporting sustainable growth and responsible corporate governance. Alongside robust corporate governance and a strong sense of social responsibility, the Company's operations are guided by internal control systems and management mechanisms that ensure operational effectiveness, financial reporting accuracy, and legal compliance.

With advances in technology and the increasing prevalence of the Internet, information security risks have become more complex and can impact business operations and lead to financial and operational losses. To address these risks, the Company has implemented comprehensive information security risk management mechanisms, including the "Internal Control Information Cycle", "Internal Critical Information Processing Procedures", "Insider Trading Prevention Management Procedures", "Personal Information Protection Procedures", "Computer Operations Management Measures", and the "Information Security Management System Procedures". In 2023, the Company achieved ISO 27001 certification for its information security management system, enabling all employees to adhere to these regulations and protect the interests of stakeholders and the integrity of the Company's operations.

Information security management mechanism

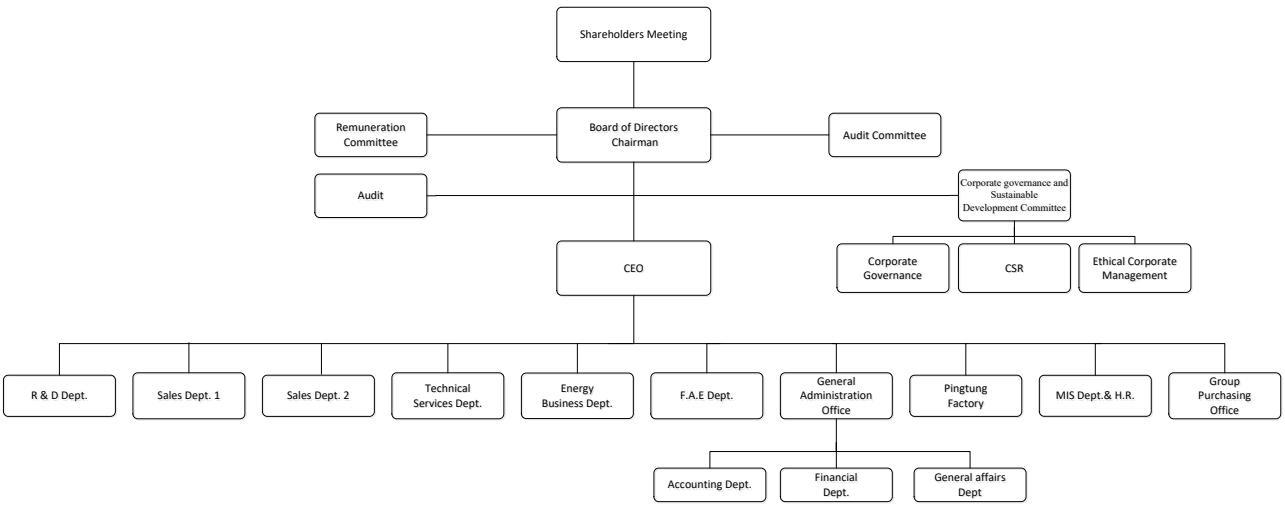
In alignment with its commitment to sustainable operations and development, the Company advances the objectives of its Information Security Risk Management Policy through three core pillars: Information Security Governance, Regulatory Compliance, and Technology Adoption. This approach strengthens information security management and promotes a "security-based information development" model. The Company prioritizes the confidentiality, integrity, and availability of data processed for customers and employees, ensuring secure data handling at every stage. By providing safe, stable, and efficient information services, the Company supports the adoption of security measures and continuous improvement within its information security management system.

Information Security Policy	
Information security governance	Physical and environmental security: ensures that the organisation's physical facilities and environment are subject to appropriate security controls. Asset Management: The management of an organisation's assets, including their identification, classification, tracking, and protection. Information Security Incident Management: Establishing policies and procedures for responding to information security incidents and incidents.

	Information assurance: ensuring adequate plans are in place to secure and recover information. Classifying, categorising, and processing information: Ensure that information is classified, categorised, and processed according to its sensitivity.
Compliance	Cybersecurity: Follow relevant regulations and standards to protect the organization's network and data transmission. Security Development Policy: Develop and implement appropriate security policies to ensure regulatory compliance. Technical Vulnerability Management: Monitor and manage system and application security vulnerabilities.
Technology application	Data transfer: Ensure data is appropriately protected during transmission. Security configuration of endpoint devices: Manage and maintain the security configuration of terminal devices. Cryptography: Using appropriate encryption techniques to protect sensitive information and communications. Technology Vulnerability Management: Integrated use of technology tools to identify, assess, and address vulnerabilities.

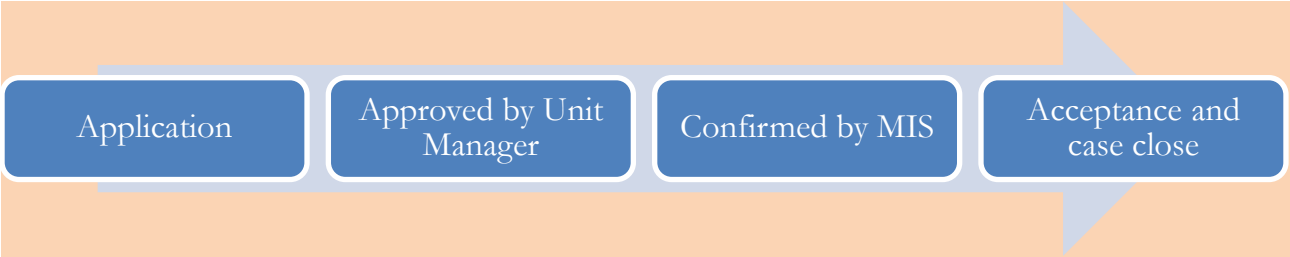
Information security management unit

The information security management unit of the company is the Information and Human Resources Department, which is responsible for reviewing the information security governance policies, planning, supervision, and information security management operations of each branch of the company, and monitoring the information security situation of each branch at any time. In case of major information security risk events, report to the general manager in a timely manner, regularly assess information security risks and report to the board of directors.



Information service process management

Applications and changes to resource permissions for information application software and hardware, systems, emails, networks, etc. required by personnel in each unit of the company shall be handled through an electronic application process, which shall be reviewed and approved by the relevant responsible person in charge, and shall be handled after confirmation of authorization.



Information Security Management Solution

The company reviews information security risks through risk identification and risk assessment, confirms the degree of adverse impact of the information security risks on corporate operations, takes corresponding management measures, and reviews information architecture, network activities, network equipment, servers and terminals Focusing on equipment detection and security settings review, we can check and evaluate whether there are vulnerabilities or old equipment problems at any time, and also respond to the challenges faced by information security, such as APT advanced persistent attacks, DDoS attacks, ransomware, and social engineering attacks. , information theft and other information issues, the planned information security management plan is as follows:

1. Risk Assessment: Conduct comprehensive risk assessments on a regular basis to identify potential threats, vulnerabilities, and risks.
2. Security policies and procedures: Implement access controls, password policies, data classification, and other requirements.
3. Access control: implement authentication and authorization mechanisms to ensure that only authorized personnel can access sensitive information.
4. Cybersecurity: protecting network infrastructure, including firewalls, intrusion detection systems, vulnerability scans and security updates to reduce cyber threats.
5. Security Training and Education: Conduct security training and education for employees to increase their awareness of information security.
6. Monitoring and alerting: Implement monitoring systems to observe network activity and detect abnormal behavior in a timely manner to respond quickly to security incidents.
7. Incident response plan: Develop a security incident response plan and data recovery strategy to mitigate losses and quickly resume operations.
8. Regular reviews and updates: Review and update security measures regularly to ensure they are responsive to new threats and vulnerabilities.

Resources in information security management

project	2023	2024	2025
Antivirus software	58,500	96,750	123,000
Maintenance costs	2,363,149	2,209,711	2,177,810
Computer room door control fee	0	0	0
Equipment and software upgrade costs	3,259,830	4,653,578	2,310,577
total	5,681,479	6,960,039	4,611,387

Information security incidents and insurance

The company's information security governance and management mechanism is implemented by all employees in accordance with regulations. No serious information security incidents have occurred. The overall information security risk management is appropriate and the expected goals can be achieved. The company has insurance on its physical assets, and adopts off-site backup of major file data, as well as an information system disaster recovery plan. If future legal regulations and information security management needs require the purchase of information security insurance, the company will evaluate and understand the relevant regulations and supporting facilities. Measures will be decided later.

Information security risk management review and improvement

implements information security internal control implementation and risk supervision and management based on the business scope of its responsibilities and operates the management mechanism process. It also conducts self-inspections on the risk internal control system on an annual basis, conducts self-inspections on information cycle internal controls, and self-assesses information security. Management implementation. The audit unit also tracks the implementation status, and the annual audit plan is included in the inspection items to ensure implementation and effectiveness review or improvement reference basis.

Implementation in 2025 is as follows:

✧ Execution of Social Engineering Simulation

To enhance employee awareness of social engineering attacks and strengthen prevention capabilities, the company conducted two social engineering simulations in 2025, from June 23 to July 28, covering 280 employees.

Simulation Method and Purpose

- Customized emails were sent to all employee accounts, with five simulation emails mimicking common social engineering tactics.
- Employee responses were quantified by tracking metrics such as email open rate, link click rate, attachment open rate, and phishing success rate, to inform follow-up training and performance evaluation.

Simulation Results

Item	Number of Employees	Percentage
Opened emails containing unsafe content	20	7.1%
Clicked on malicious links	7	2.5%
Opened/downloaded attachments	8	2.8%
Fell for phishing attempt	2	0.7%

Follow-up Actions

- Employees who failed the simulation were required to attend 1-hour cybersecurity training.
- All participants completed the course and passed the assessment, achieving a 100% training pass rate.

✧ Regular System Updates

The Kaohsiung FileServer and Taipei MailServer were recently updated to patch known vulnerabilities, ensuring systems remain secure and resilient.

✧ Annual User Permissions Review

User permissions are reviewed annually to prevent unauthorized data access, with all permissions evaluated and adjusted as necessary before year-end.

✧ Centralized Anti-Virus Monitoring

The company utilizes a centralized anti-virus system, Kaspersky, to monitor and swiftly respond to any virus incidents.

✧ Be approved by ISO 27001 Information Security Management System

✧ Ad Hoc Awareness Campaigns on Cybersecurity Threat Intelligence

Recently, it was observed that hackers are distributing malware via spoofed LINE websites to steal personal data and account credentials. Their attack methods include:

- Impersonating messaging app websites.
- Using search engine manipulation to increase exposure of fake sites.
- Distributing malicious installation files with multi-layer backdoors.
- Evading antivirus detection.

Examples of recent spoofed websites include:

- www[.]lineoe[.]com
- www[.]linerm[.]com
- www[.]linecl[.]com

- www[.]line-tww[.]com

Preventive Recommendations for All Employees:

- Download software only from official websites or authorized app stores.
- Avoid clicking on links or opening attachments from unknown sources.
- Regularly update antivirus software.
- Immediately verify suspicious messages and refrain from replying or clicking.

Reporter: Manager of Information and Human Resources Department/ T.M. Lin

(Submit the ”Information Security Risk Management Report ” to the Audit committee and Board of Directors for review on 2025.11.3)