1. Information Security Risk Management Framework

(1) The information security authority in our company is the Information Center, responsible for planning, executing, and promoting information security matters.
(2) The company's audit unit is responsible for information security audits. If any deficiencies are found during audits, the audited unit is required to propose relevant improvement plans and report them to the board of directors, with regular follow-ups on improvement effectiveness to reduce security risks. The organizational operation model adopts the PDCA (Plan-Do-Check-Act) cycle management to ensure goal achievement and continuous improvement.

2. Information Security Policy

Our company specifies information security policies in the information security control procedures, including network resources, hardware resources, software licensing, and data security. The main objectives are: (1) To maintain the continuous operation of information-related systems.
(2) To prevent internal misuse of software and information.
(3) To prevent external hackers and viruses from damaging equipment and stealing data, causing operational disruptions.
(4) To protect sensitive confidential data and prevent data leaks.

3. Specific Management Solutions

(1) Network Resource Security Management

- **Account/Password Management:**
  - Account Management: When there is a need for an account or changes, an application form must be filled out.
  - Password Management: Passwords must be set according to the minimum length and complexity rules announced by the information unit and must be changed quarterly.
  - Account Inventory: The information unit will conduct an inventory of idle accounts that have not been logged into for over a year in the first quarter of each year and record the results.
- **Internet and Email Usage Guidelines:**
  Usage guidelines will be established. If violated, the information personnel will issue a ticket to the user, requiring the unit to propose corrective measures.
- **Antivirus System Security Management:**
  To effectively prevent virus intrusions and strengthen information security,

and to monitor the status of personal computers throughout the company, the information unit will establish an antivirus system according to planned standards, implementing automatic protection mechanisms. The virus monitoring center will update virus definitions and set scheduled scans for all machines.

- **Network Traffic Monitoring Management:**
  To grasp the company's network usage status, the information unit will perform daily monitoring using network traffic statistics systems.
- **Personal Computer Usage Rights:**
  A. For information security considerations, general personal computers will be set to company domain and general user permissions upon purchase.
  B. Computers provided for personal use by the company are prohibited from other uses besides official business.
- **Firewall Management:**
  A. To block unknown intrusions and attacks from the internet, ensuring the security and integrity of internal company data, the information unit will establish firewalls to control internet connections based on the company's security policy.
  B. The information unit will conduct a rules inventory every six months. If there are operational abnormalities, the applicability of the rules will be confirmed, and improvements will be made accordingly, with results recorded.

(2) Hardware Resource Security Management

- Hardware resources purchased by the company will be managed by the requesting unit. If the purchased hardware resources are key equipment, the information unit will manage and register them.
- Key equipment must be installed on an uninterruptible power supply (UPS) system, with attention paid to power load and balance during installation.

(3) Copyright Software Resource Security Control

- **Software Purchase and Management:**
  A. Basic configuration software: The information unit will evaluate needs annually, propose suggestions, and budget for purchases, followed by safekeeping and registration.
  B. Non-basic configuration software: The requesting unit will purchase based on needs, followed by safekeeping and registration.

C. Software should be stored in appropriate locations and managed by designated personnel.

- **Software Installation Management:**
  A. Basic configuration software will be installed by the information unit after selecting an appropriate licensed software version based on the overall performance of new machines.
  B. For installation, addition, or change of non-basic configuration software, an application form must be filled out for the information unit to install.
  C. The information unit will audit the installation and usage of software regularly, notifying the responsible unit of any abnormalities for improvement.

(4) Information Security Education and Training

The information unit will explain the appropriate use of information resources during new employee training, ensuring users understand the threats and concerns regarding information security. In addition to new employee training, the information unit will place relevant information security materials on the company's intranet for users to access at any time.

(5) Data Security Control

- **Electronic File Data Storage:**
  A. All relevant documents used by the company must be stored on the file server. If units need to establish server folder permissions, an application must be submitted for the information unit to set them up.
  B. The information unit will conduct monthly audits of server folder permission management and record the inventory results.
- **Server Data Backup:**
  A. Systems and file data stored by the company must be backed up, retaining daily change records for potential historical data retrieval at specific points in time.
  B. Backup media and hosts must be password protected.
  C. Backup data should be stored in appropriate locations and managed by designated personnel. Backups may not be borrowed without consent.
  D. Backup data should have both local and off-site backup methods for preservation.
  E. Backup data must be retained for a minimum of one year.
- **Control of Portable Storage Devices:**
  For information security considerations, external storage device functions should be disabled based on the unit's characteristics.

(6) Outsourced Information Security

- The information unit must specify in outsourcing contracts that suppliers must keep data processing and procedures confidential, strictly prohibiting leaks, and relevant clauses or penalties must be drafted in the contract.
- Suppliers must obtain consent from the information unit before proceeding with operations, or information unit personnel must accompany them.

(7) Data Center Security Control

- Data centers should have access control, monitoring, fire protection, and temperature/humidity management configurations.
- Access control for the data center will be managed by the information unit, requiring approval for personnel entry and recording logs.
- Maintenance vendors must be accompanied by authorized personnel during data center operations and are restricted to the scope of the operation without operating unrelated equipment.
- Only items necessary for operations are allowed in the data center, aside from hardware, software, and relevant documentation.
- The information unit will conduct periodic inspections of the data center, prohibiting the storage of flammable materials, unauthorized electrical installations, eating, or smoking.

(8) Security Incident Reporting and Recovery

- **Reporting:**
  Upon occurrence of a security incident, the information unit must assess the type of disaster and immediately report to the highest information authority. If immediate repair is not possible, the head of the information unit must promptly report to the general manager and the CEO, notifying colleagues of the impact scope and potential recovery time.
- **Emergency Response:**
  A. For security threats, determine the cause, assess potential impacts and losses, and decide whether support requests are needed while preserving evidence of intrusions or damages.
  B. Solutions will be obtained through vulnerability databases, online resources, and technical support units.
- **Recovery:**
  A. Check whether hardware is functioning normally; if damaged beyond use,

substitute with backup equipment and contact vendors for repair.

B. Assess whether security risks affect normal operations; upon elimination of risks, execute system restoration or environmental reconstruction.

C. Once operations are normal, data recovery and resetting will occur.

- **Review/Drill:**

  A. After disaster recovery, the information unit must document the cause, emergency response, recovery process, and improvement proposals.

  B. The information unit will conduct practical drills on disaster recovery procedures for key equipment, implementing security incident drills annually to confirm system effectiveness and keeping records of the drill process.

4. Resources Invested in Information Security Management

Our company continues to invest resources in information security management, including improving governance and technical security infrastructure, strengthening security defense equipment, and providing education and training. Information systems will regularly perform security updates and enhance employee awareness of security issues, promoting through meetings and the company intranet to raise security consciousness. Employees are advised not to open suspicious files or emails to avoid hacker attacks, and security protective equipment will be updated in a timely manner to optimize protection effectiveness.

2024 Information Security Performance

- Information security training: 655 participants
- Security drills: 2 times
- Vulnerability scans: 1 time
- Security assessments: 3 sessions
- A report on information security risk management was presented at the 21st meeting of the 9th Board of Directors (November 13, 2024).