1. Information Security Risk Management Structure

(1) The Information Center serves as the information security authority unit of the Company and is responsible for the planning, execution, and promotion of information security issues.

(2) The Company's audit unit is responsible for information security audits. If the audit reveals deficiencies, the audited unit shall be required to propose relevant improvement plans and submit them to the Board of Directors, and the effectiveness of the improvements shall be tracked on a regular basis in order to minimize the risk of information security.

The PDCA (Plan-Do-Check-Act) cycle is used for the organization's operation to ensure the achievement of goals and continuous improvement.

2. Information Security Policy

The Company has formulated information security policies in its information security control procedures, including network resources, hardware resources, software copyrights, and data security, with the main purposes to

(1) Maintain the continuous operation of the information related systems.

(2) Prevent unauthorized use of software and information by insiders.

(3) Prevent external hackers and viruses from damaging equipment and stealing data that may cause operational disruptions.

(4) Protect sensitive and confidential information from being leaked.

3. Specific Management Programs

(1) Network Resource Security Management

Account/Password management:

Account management: When there is a need or change of account, an application form shall be filled out to make the application.

Password management: Passwords shall be set in accordance with the minimum length and complexity of passwords announced by the information unit, and passwords shall be mandatorily changed on a quarterly basis.

Account inventory: The information unit conducts an inventory of inactive accounts that have not been logged in for more than one year in the first quarter of each year, and records the results of the account inventory.

Internet and Email Usage Guidelines:

The guidelines for usage are set out and in case of violation of the guidelines, the information personnel shall give a ticket to the user and the unit concerned shall propose improvement measures.

Anti-virus system security management:

In order to effectively prevent viruses from attacking, strengthen information security, and monitor the status of personal computers throughout the Company, the information unit builds the Company's anti-virus system according to anti-virus system planning standards, sets up an anti-virus automatic protection mechanism, and the virus monitoring center systematically updates the virus code and sets up a schedule for scanning the entire equipment.

Network traffic monitoring and management:

In order to control the status of the Company's network usage, the information unit carries out daily monitoring based on the network traffic statistics system.

Personal computer access authorization:

A. In consideration of information security, the information unit shall set the user's domain and authorization to the Company's domain and the general user's authorization after the purchase of the general personal computers.

B. The Company prohibits the use of personal computers for any purpose other than business.

Firewall Management:

A. In order to prevent unknown intrusions and attacks from the Internet and to ensure the security and integrity of the Company's internal data, the information unit has built a firewall to control Internet connections in accordance with the Company's information security policy.

B. The information unit conducts a semiannual inventory of rules and if there are any abnormalities in the operation, the applicability of the rules is confirmed and improvements are made, and the results are recorded after the completion of the confirmed improvements.

(2) Hardware Resources Security Management

The hardware resources of the Company are managed by the requesting unit after purchase. If the purchased hardware resources are major equipment, they are managed and registered by the information unit.

The main equipment needs to be installed on the UPS (Uninterruptible Power Supply) power system device, and attention shall be paid to the load and balance of the power supply during the installation.

(3) Security Control of Copyrighted Software Resources

The purchase and management of copyrighted software:

A. Basic configuration software: The information unit evaluates the needs and makes proposals and budgets each year, and then keeps and registers the software after purchase.

B. Non-basic configuration software: The requesting unit makes the proposal according to the demand, and then keeps and registers the software after purchase.

C. Software shall be placed in appropriate storage locations and kept by specialized personnel.

Software installation management:

A. Basic configuration software: When the new equipment is purchased, the information unit shall select the appropriate copyrighted software version and install it according to the overall performance of the equipment.

B. Non-basic configuration software: When installing additional or different software, the application form shall be filled out and installed by the information unit.

C. The information unit shall audit the installation and use of software from time to time, and if there is any abnormality, the responsible unit shall be notified for improvement.

(4) Information security education and training

The information unit shall explain the appropriate use of information resources during training for new employees and make users understand the threats and concerns of information security.

In addition to training for new employees, the information unit shall place information related to information security on the corporate portal so that users can obtain it at any time.

(5) Data security control

Electronic file data storage

A. Documents used by the Company are systematically placed on file servers for access. If each unit needs to set up server folder authorization, it shall submit an application and the information unit shall set up the authorization.

B. The information unit audits the management of server folder authorization on a monthly basis and records the results of the audit.

Server data backup

A. The system and file data stored by the Company shall be backed up and a daily record of changes shall be kept so that the historical data can be accessed at a certain point in time when needed.

B. Backup media and hosts shall be password-protected.

C. Backup data shall be stored in an appropriate location and kept properly by specialized personnel. Backup data shall not be lent out without prior consent.

D. Backup data shall be stored in two or more ways: on-site backup and off-site backup.

E. The retention period of the backup data shall be at least one year.

Portable storage device control

In consideration of information security, the function of external storage device shall be deactivated according to the attributes of the unit.

(6) Outsourcing Information Security

In the outsourcing contract, the information unit shall specify that the supplier shall keep the data handling and process confidential, and strictly prohibit the leakage of the data, and shall set out the relevant terms and conditions or penalties in the contract.

The supplier shall obtain the consent of the information unit or be accompanied by the information unit's personnel before performing the operation.

(7) Server room security control

The server room shall be equipped with access control, monitoring, fire protection, temperature and humidity management, and other related facilities.

The information unit is responsible for controlling the access control of the server room, and personnel can only enter or leave the server room after obtaining the consent of the information unit, and registering the record.

Maintenance vendors entering and leaving the server room shall be accompanied by the authority unit, and shall be restricted to stay within the operation area and shall not operate any unrelated equipment.

Except for hardware and software equipment and related documents, non-operational items are not allowed to be brought into the server room.

The information unit shall inspect the server room from time to time to prevent the storage of flammable materials, unauthorized electrical equipment, and the eating, drinking, and smoking of cigarettes.

(8) Information Security Incident Notification and Recovery

Notification:

After the occurrence of an information security incident, the information unit shall determine the type of disaster and immediately notify the top management of the information unit. If immediate recovery is not possible, the head of the information unit shall immediately report to the president and chief executive officer and notify employees of the scope of the impact and the possible time of recovery.

Emergency Responses:

A. With regard to the signs of information security hazards, the information unit identifies the cause of the incident, determines the possible scope of impact, evaluates the possible loss, and determines whether or not to apply for support, and retains evidence of intrusion or damage.

B. The information unit obtains solutions through the system vulnerability database, the Internet, and technical support units.

Recovery:

A. The information unit checks whether the hardware equipment can operate normally, and if the hardware equipment is damaged and cannot be used, the information unit

may temporarily replace it with the backup equipment and contact the vendor for maintenance.
B. The information unit examines whether the security risk affects normal operation, and performs system repair or environmental reconstruction after the security risk is eliminated.
C. After normal operation, data recovery and data reset shall be carried out.
Review/Drill:
A. When the disaster is lifted and the recovery is made, the information unit shall record the cause of the incident, the disaster response, the recovery process, and the reviews and improvement plans.
B. The information unit shall conduct a real-time drill for main equipment in accordance with the disaster recovery procedures. Information security incident drills are implemented once a year to ensure the effectiveness of the system, and records of the drills shall be kept afterwards.

4. Investment Resources in Information Security Management
The Company continuously invests resources in information security management, including improving the security infrastructure in terms of governance and technology, strengthening information security defense equipment, and education and training. We regularly update the security of our information systems, enhance employees' security concepts, and raise their awareness of information security through meetings and the Company's intranet site. The Company trains its employees not to open suspicious files and e-mails to avoid cyber attacks, and to update the information security protection equipment in a timely manner to optimize the protection effect.

Information Security Implementation Achievements in the Year of 2023
Information security education and training 625 participants
Information security drill*2 times
Vulnerability scanning*1 time
Information security assessment*4 sessions