Information security management:

The Company has established the information security risk management team, with the IT Officer as the convener, to regularly review the information security policies and report to the Board of Directors. The latest report made to the Board of Directors was on November 4, 2022. The Company did not have any material information security incidents hazardous to computer systems in 2022.

(1) Information security risk management framework, policy, specific management plans, and resources put in Information security management:

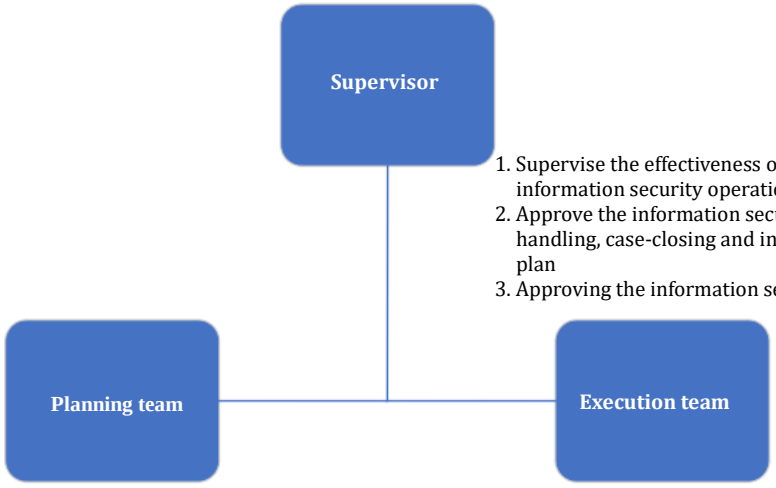
1. Information security risk management framework

The accountable unit of the Company's information security governance organization is IT Department, where a IT Officer and professional IT personnel are established to coordinate and formulate the internal information security and protection related policies, plan and implement the information security safeguard, as well as information security policy promotion and Implementation, and the top officer of the corporate information security organization regularly reports to the Board of Directors regarding the effectiveness of information security management, issues and directions related to information security.

Supervisor: the officer of the IT Department

Planning team: the personnel from the IT Department

Execution team: formed by the Planning Team according to the needs of the task



1. Understand the content and status of the reported incident, to determine whether it is an information security incident
2. Confirm the scope of impact for the information security incidents
3. Evaluate the handling capabilities for the information security incident
4. Seek external support
5. Formulate handling program of information security
6. Form and supervise the executive team
7. Review, evaluate, and report on the status of information security safeguard

1. Handling of information security incidents
2. Prevention and enhancement of information security
3. The reporting unit is required to cooperate with the execution team to handle the information security incidents

2. Information security policy

To enable the thorough implementation, effective operation, supervision and management, and continuous progress of Company's various information security policies, as well as maintain the confidentiality, integrity and availability of the Company's important information systems, the information security policy is specially formulated.

The policy aims to give employees a clear guiding principle in their daily work. All employees are obliged to actively participate in the promotion of information security management policy, to ensure the security operation and maintenance of all employees, data, information systems, devices and networks of the Company, seeking that all employees understand, implement and maintain the policy, to achieve the goal of continuous operation of information.

"Implement information security and strengthen service quality"

"Enhance information security training to ensure continuous operation"
"Good contingency response for rapid disaster recovery"

- Implement information security and strengthen service quality
  All employees implement information security. All information operation-related measures should ensure the confidentiality, integrity and availability of business data, and be free from risks of leakage, compromise or loss due to external threats or improper management of internal personnel. The appropriate protective measures are selected to lower the risk to an acceptable level for the continuous monitoring, reviewing and auditing the tasks of the information security management system, for strengthening the service quality and improving the service level.
- Enhance information security training to ensure continuous operation
  Supervise corporate employees to implement the information security management tasks, with continuous appropriate Information security education and training conducted every year, to establish the concept of “everyone is responsible for information security,” prompting employees to understand the importance of Information security, and urging them to comply with the regulations of Information security, to improve the Information security concepts and emergency response capabilities, reduce information security hazards, for achieving the goal of continuous operation.
- Good contingency response for rapid disaster recovery
  Formulate contingency plans and disaster recovery plans for important information assets and key businesses, and regularly implement drills for various emergency response processes, to ensure rapid recovery when information systems fail or major disasters occur, and ensure the key businesses continue the operation with losses minimized.

3. Specific management plans, and resources put in Information security management

① In addition to building a safe information and communication environment, the Company continues to invest in improving vulnerabilities and enhancing the system’s operation efficiency. The main Information security management programs are as below:

A. Description of network security attack risk and countermeasures

a. The Company has established network security protection management to ensure the operation of information systems related to internal corporate operations. However, when facing the ever-changing sources and approaches of network security attacks, it is impossible to guarantee that the computer system may be 100% free from the attacks.

b. The computers used in the manufacturing sites of factories are isolated from the external network or adopt a closed independent system, to avoid the shutdown of the production line caused by network security hazardous incidents.

c. For the IBM mainframes mainly used for operation, the long-term system software and hardware maintenance contract are entered with the original maker, while the internal information system maintenance personnel are also familiar with data backup and recovery operations, to ensure that the computer system meets the operational needs.

B. The Company’s information security control measures

a. Network security monitoring: including -email server system and security control of the Company’s website.

(a) The Company has leased the dedicate line service of Chunghwa Telecom Hinet Information Security Fleet 2018 series "New Generation Firewall Edition" solution. Hinet performs the network security monitoring task, to block malicious intrusion behaviors of external hackers, and provide regular statistical analysis statements.

(b) The Company use the Palo Alto global information security intelligence engine which updates the attribute codes regularly and automatically to detect and block the malicious programs and connections including the latest viruses, worms, spyware, ransomware, mining software, to achieve instant protection.
Control over sites of five major categories
"Malicious websites," such as: malware and phishing;
"Violation of good customs," such as: adults, drugs, gambling and nudity;
"Reducing productivity," such as: social networks, promotion and auctions,

stocks and investments, and recommended games;
"Video playing," such as: peer-to-peer transmission, media and streaming;
"Others," such as: web-based mail services, hosting sites that cannot be categorized.

(c) In addition to providing a network security control mechanism, Hinet also installs a firewall device on the Company's internal internet port, to monitor and record various conditions of internet usage, providing the statements of necessary statistical analysis for warnings.

(d) For the email server system security, the Company has leased the Mail Could system service provided by an external server supplier. The supplier is responsible for the maintenance of the email server hardware and control over the outward network security, including anti-virus software service for mail, to strengthen the safeguard of e-mail security.

(e) The Company's official website (www.nhjeans.com) system is commissioned to an external web hosting service. The provider is responsible for the maintenance of the website server host hardware and the control over the outward network security.

b. Computer security: including connection control, anti-virus and backup operations between personal computers and server hosts

(a) On the internal network (Intranet) or external Internet (Internet), when attempting to use the server host, the dedicated software must be installed to connect with the server host.

(b) For the PC (personal computer) to make the connection, the device name must be configured on the server host, and the users are limited to logging into the server host with a specific device name based on the necessity.

(c) Whenever a user logs into the server host, the operating system (OS) will always record the login date, time and device name, even wrong passwords. In addition, the process of the user's execution of the program and the date and time of logout from the host are also recorded.

(d) When attempting to log into the server host, if the times of wrong password entries exceed the defined value, the user ID and device name will be suspended by the OS, and it may be restored through the system administrator of permission.

(e) USB interfaces are controlled, that external USB devices cannot be used without authorization.

(f) The anti-virus software console, OfficeScan Console, monitors the updates and protection status of users' end.

(g) Perform daily backups of server files, including disk-to-disk, disk-to-tape, and multi-tape versions and store them remotely.

c. User security: application software system security control

(a) The establishment of a User ID (user account) is applied by the department of the user to IT Department, and established by the system administrator for permission.

(b) To execute the connection software, a legitimate user ID & password must be entered for the user login screen of the application system.

(c) Different user IDs are established in different application systems, depending on the department to which the user belongs and the characteristics of the job in charge, with specific divisions of permissions.

(d) The password of each user ID is established by the user; if the password is forgotten, an application for changing must be submitted to the IT Department, and reset by the system administrator with permission.

(e) For personnel changes or job changes in each department, an application for changing the user ID permission must be submitted to the Information Department, and reset by the system administrator of permission.

(f) The user's permission is determined depending on the level provided by the OS, and then adapted to the configuration files of different application systems to further manage and determine respectively.

② Resources invested in Information security management

A. The network hardware equipment such as firewalls, backup management equipment, SSL VPN private channel connection.
B. Software systems such as email anti-virus and spam filtering.
C. Information security manpower: one IT officer and two information engineers are in place, to convene the information security management meetings at least once a year, responsible for information security framework design, information security operation, maintenance and monitoring, information security event response and investigation, information security policy review and amendment.
D. Implementation: daily inspection of system status, regular weekly backup and execution of retaining the backup media in different places, annual information security promotion, annual internal audit of information cycle, and CPAs' audits.