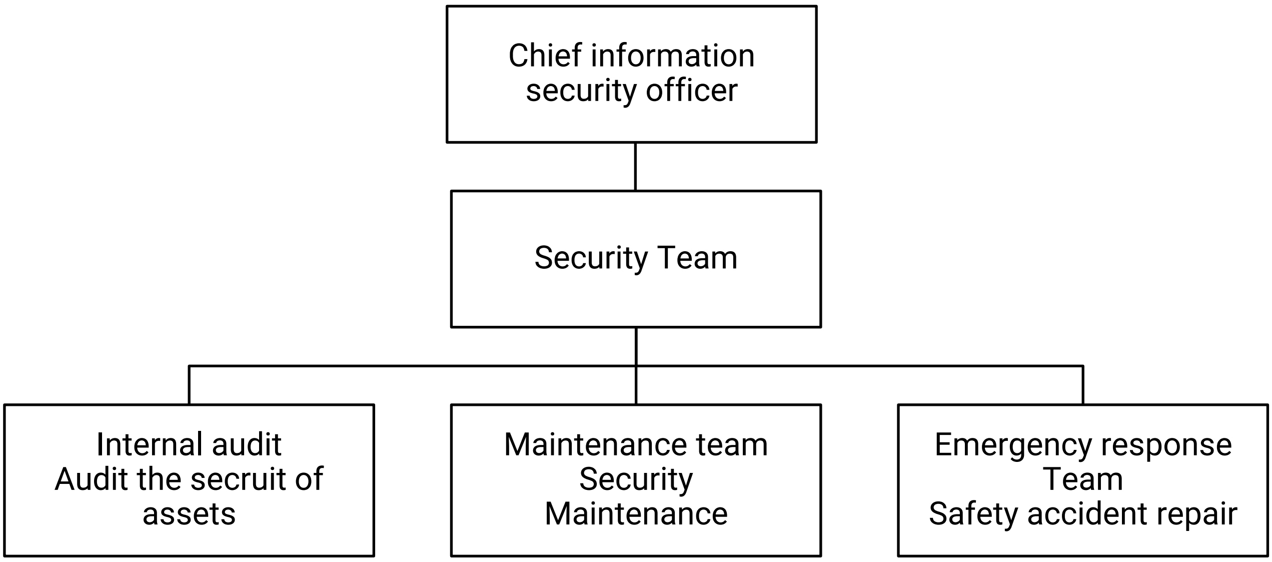
Kwong Fong Industries Corporation

Information Security Management

I. Information security risk management framework



The Company and its merged subsidiaries set up a security team (such as the above organizational chart) to integrate and implement information security policies, promote information security information, raise employee awareness of information security. Auditors conduct annual information security checks on the internal control system to assess the effectiveness of internal control in the company's information operations. Annual information security management operations checks are performed by internal audit units, audit reports are issued, and audit results are regularly reported to audit committees and boards of directors.

II. Information Security Policy

1. Objectives

   In order to improve the safety and stability of the Group's information operations, provide reliable communication services, ensure the confidentiality, integrity and availability of information assets, and carry out business smoothly.

2. Range

   This policy applies to our colleagues and related enterprises, manufacturers and third-party personnel who have access to our business information or services.

3. Aim

   To ensure the confidentiality of the Company's business-related information and to protect the Company's business secrets and personal data.

   (1) To ensure the integrity and availability of information related to the Company's business, and to improve the efficiency and quality of its work.

   (2) Improve the company's financial security protection capabilities.

   (3) to achieve the company's business continuity objectives.

4. Strategy

(1) To assess the security requirements of communications operations and establish procedures to ensure confidentiality, integrity and availability of information assets.
(2) Establish the company's financial security organization and set up a division of responsibilities to facilitate the implementation of financial security operations.
(3) To carry out the duties according to the regulations of the classification of financial security responsibilities.
(4) To establish a contingency mechanism to ensure proper response, control and handling of financial security incidents.
(5) To carry out security audit regularly to ensure the implementation of security management of information security management.

5. Censorship

This Policy shall be approved by the Chairman and assessed by the Information Office at least once a year, or re-evaluated in the event of major changes in the organization (such as reorganization, major business changes, etc.).Revise according to the results of the assessment, relevant laws, technology and business developments.

III. Information security management plan

Projects	Specific management measures
Firewall Protection	• Firewalls set up connection rules.
	• Additional applications are required for special connection requirements.
User Internet control Control mechanism	• Use automated web site protection systems to control users' online behavior.
	• Automatic filtering of links to websites with Trojan, ransomware or malicious programs.
Anti-virus software	• Use anti-virus software and automatically update virus code to reduce the risk of virus infection.
Operating System Update	• If the operating system is updated automatically, the information department will help to update it.
Email Security Control	• There is automatic email scanning threat protection, before users receive mail, prevent unsafe attachment files, phishing, spamming, and extending protection against malicious links.
	• When a personal computer receives an email, antivirus software also scans for unsafe attachment files.
Data Backup Mechanism	• The database of critical information systems is backed up daily.
Important File Upload Server	• The important files of all departments in the company are stored on the server. The information department will backup and save them.

IV. Information Security Management Operations

1. Purpose

   To establish the relevant standards to maintain the information system security and strengthen the information security protection mechanism, and to provide the basis for the basis.

2. Scope of control

   Computer host systems, computer equipment, computer programs, database files, computer output screens, reports and media.

3. management operating procedure

   A. Machine room specification

      (1) Non-information processing personnel are not allowed to enter the computer room without approval. The entry and exit register must be completed.

      (2) No easy items should be placed in the machine room, and the manufacturers should be regularly asked to check fire prevention facilities.

   B. Please purchase and install the computer equipment

      (1) Update and purchase equipment need to fill in the requisition form, will sign the supervisor approval, by the information department to purchase and install.

      (2) Installation of computer equipment should be carried out by information personnel. Illegal software should not be installed. Anti-virus software should be installed to scan and update virus code regularly.

      (3) Upon separation, the transfer of portable computer equipment is required.

      (4) Host SERVER sets up a firewall to access jobs from outside the company through the firewall.

   C. Operation control

      (1) Users must be offline when using up the computer and shutdown when not in use.

      (2) Unauthorized use of information center equipment is prohibited to handle tasks unrelated to one's own business.

      (3) To use the mainframe during non-office hours or holidays, the purpose and time of use shall be approved by the responsible supervisor, and the information department shall be notified for corresponding measures.

      (4) The information department should review the system anomaly JOBLOG at all times and take necessary action.

      (5) The information department should regularly back up the data, store it in another place, and conduct regular response tests.

   D. Password control

      Each user has their own usage code and password.

      (1) A person authorizing the use of a password shall make a list of it. Personal passwords may not be borrowed from others.

      (2) When a staff member leaves or changes jobs, his or her code of use shall be cancelled or updated immediately.

      (3) All files that are online should be maintained by the application, and the application should be subject to permission.

      (4) Password change is required every 3 months. The password must be at least 6 digits long and the first digit must be in English.

      (5) The first user's account and permissions should be approved by the head of the department and then executed by the information department's system security administrator.

E. Authority control

(1) The user shall have the relevant usage function in accordance with the authorized authority.

(2) Data usage rights should be hierarchical authorization system, audit and management have no authority to update the database.

(3) Non-designated financial personnel are not authorized to use the financial statements system.

(4) Users of general applications should not have access to host system utilities, tools and instructions other than executing the application system.

(5) System Development/Programmer should not have access to the programs and data files of the online system.

(6) Set the user code used by the manufacturer for soft and hard maintenance. Unauthorized access (disabled) should be restricted.

(7) Set up a computer logbook for the system operator to record the status of the system and review by the supervisor.

(8) The system shall record the user's use of the system, and the system administrator shall periodically review and track users who have not logged in to the system for a long time.

(9) Information personnel should not have access to officially launched applications.

(10) Passwords should not be displayed on the computer screen or printed on any report without scrambling.

(11) The information officer must fill out the application form before leaving the office. The transfer procedure must be signed by the transferor before the operation is officially completed.

V. Investing in financial security management resources

1. Network hardware device

Item	Number
Firewall	1
Computer anti-virus host	1
Garbage Software Filtering	1

2. Software system

Item	Number
Computer anti-virus software	1
Backup Management Software	1

3. Investingmanpowerincapitalsecurity

Maintenance Project	Manpower
Daily system status check	1
Weekly regular backups	1
Backup media off-site execution	1
Annual Safety Promotion	1
Annual System Disaster Recovery Simulation Exercise	2
Annual Internal Audit of the Information Cycle	2

4. Conference and Conference Program

Projects	Number/Year	Total number of participants
Staff safety education and training in 2024	2	40
Information Security Conference 2024	4	80
Information security incident case sharing in 2024	2	40

VI. Information Security Incident

1. The company currently has no major information security incidents that have caused business damage.
2. Continue to implement information security management policy objectives and conduct regular recovery plan drills to ensure the security of the company's important systems and data