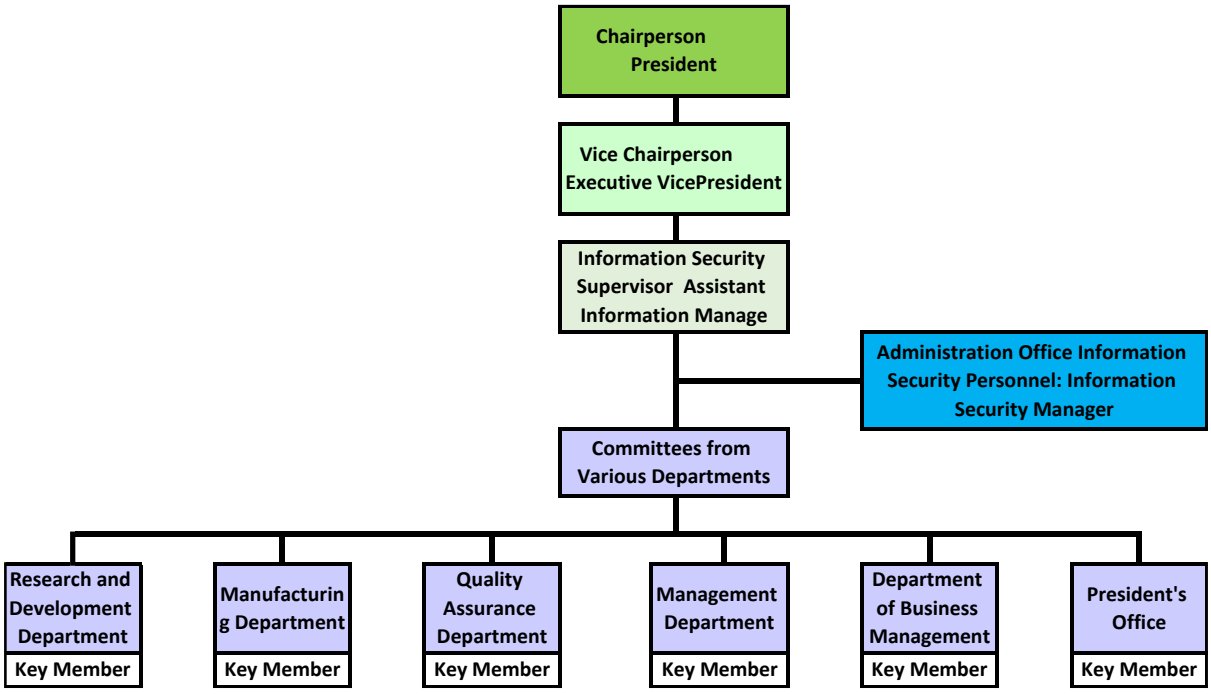
● Information Security Management

1. Information Security Risk Management Framework

The Company has established a Risk Management Committee that conducts regular risk assessments annually. Starting from August 2018, due to potential failures or intrusions in information system equipment that could increase the risk of operational disruption, we have strengthened various information security protective measures and set management objectives to enhance information management efficiency. The management objectives undergo regular performance reviews and controls.

The Company has established relevant operational standards such as "Information Operation Management Regulations," "Portable Storage Media Management Regulations," and "Email Operation," which cover: application system development and maintenance, data access, backup mechanisms, virus and network intrusion protection, data center installation of uninterruptible power supply systems, access control systems, management of portable hard drives and USB drives, and email usage authorization management. Employees execute and implement these activities according to company regulations and ensure the implementation of authorized access control to ensure information security.

The Information Security Management Committee was established in January 2022, with the President and Vice President serving as the Chairperson and Vice Chairperson, respectively. The Deputy Manager and managers of the President's Office are designated as responsible individuals for information security, leading and maintaining the execution of information security policies. The organization chart of the Information Security Management Committee is as follows:



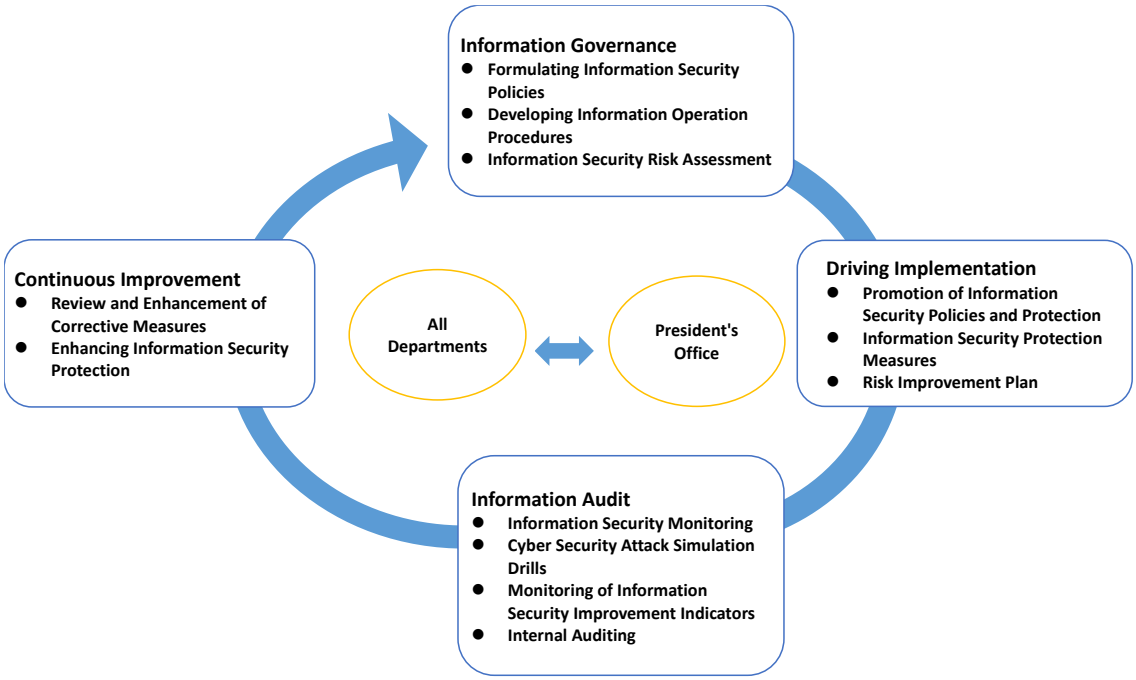
2.The Company has formulated the “Information Operation Management Regulations”, which stipulate the following information security policies:

As an enterprise engaged in the manufacture of automobile, motorcycle, and bicycle parts, in order to prevent unauthorized access, control, or other infringements of information systems and to ensure the confidentiality, integrity, and availability of information, the Company has established the following policy for all employees to follow jointly:

- Compliance with government information security-related legal requirements.
- Establishment of system and network permissions to prevent unauthorized use.
- Provision of suitable information software and hardware to maintain normal company operations.
- Establishment of a system data backup mechanism to verify the feasibility and correctness of data recovery.
- Establishment of information security protective measures to prevent viruses and hacker invasions.
- Establishment of an information security reporting mechanism to reduce the impact on company operations.
- Employee information security education and training to enhance awareness of information security.

3.Information Security Risk Management Framework and Continuous Improvement Process

Flowchart.



4.Specific Management Solutions

Management Solutions		2024 Implementation Status
Network Safety	●Strengthen network firewalls and network controls to prevent computer virus spread across machines and factories.	●Establish firewalls for real-time monitoring, promptly report and eliminate abnormalities.
Device Safety	●Conduct vulnerability detection and penetration testing at least once every two years. ●Implement endpoint antivirus measures based on computer types, and enhance malicious software behavior detection.	●Vulnerability detection and penetration testing were conducted in 2024. ●Weekly virus code updates and scans.
Enhanced Information Security	●Document and data encryption control and effective tracking.	●Access permissions set according to department roles. ●Email usage authorization management. ●Management of portable hardware and USB drives. ●Computer system host disposal, destroy the equipment to ensure it's not used by others, so that the data is not captured or leaked.
Education, Training, and	●Each unit implements information security promotion campaign at least once a year. ●Conduct at least one information security emergency response drill per year.	●In 2024, a total of 150 people participated in information security promotion activities. ●In May 2024, an intrusion response drill for information systems was conducted.

5.Resources Invested in Information Security Management

(1).Human Resources: The Company's information security operations involve a total of 23 personnel, including the Chairperson, Vice Chairperson, responsible manager for information security, responsible personnel for information security, implementation committee members from various departments, and designated key members.

(2).Security Equipment: Includes firewalls, antivirus software, network automatic defense systems, email filtering systems, application system development and maintenance data access, mobile media management, access control and password management, backup systems, and cloud storage management.

(3).Physical Environment Setup: Includes data center access control and uninterruptible power supply systems.

6.Even though the company has established the above management processes and numerous information security protective measures, it cannot guarantee the complete prevention of network attacks from any third party that could paralyze the computer systems essential for crucial business functions such as manufacturing, operations, and accounting.

The Company will continuously review and assess information-related SOPs to ensure their appropriateness and effectiveness. Internal information security training and promotion will be carried out at least once a year in each unit, such as not to open files from unknown sources, not to install unknown programs, not to link to websites arbitrarily, etc., in order to enhance the ability of users in each unit to identify information security and develop good operating habits.

Regular simulated information system intrusion disaster recovery drills are conducted, and the results are reviewed. When necessary, the original management processes are revised and necessary facilities are added to reduce the risk of unauthorized intrusion into the information system.

7.In the 2024 fiscal year 1, the Company did not experience any significant cybersecurity risks.