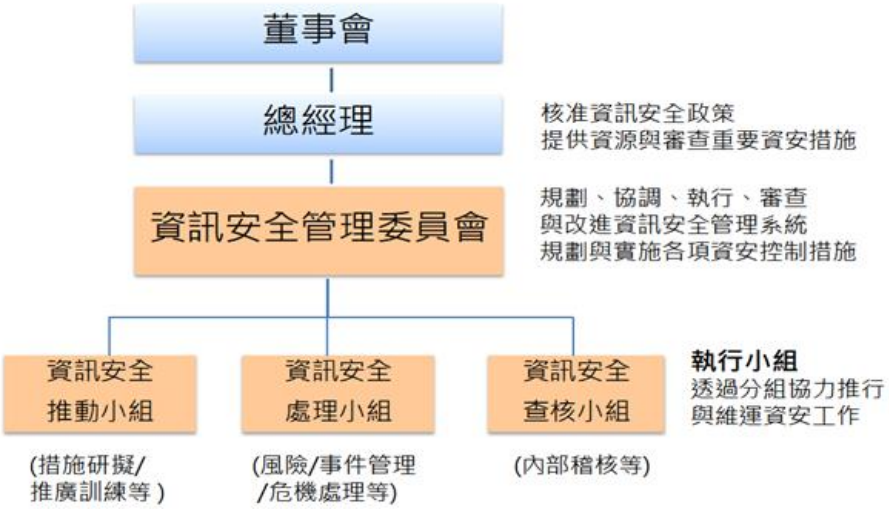
Giantplus Technology Co., Ltd.

Information security management strategy and structure

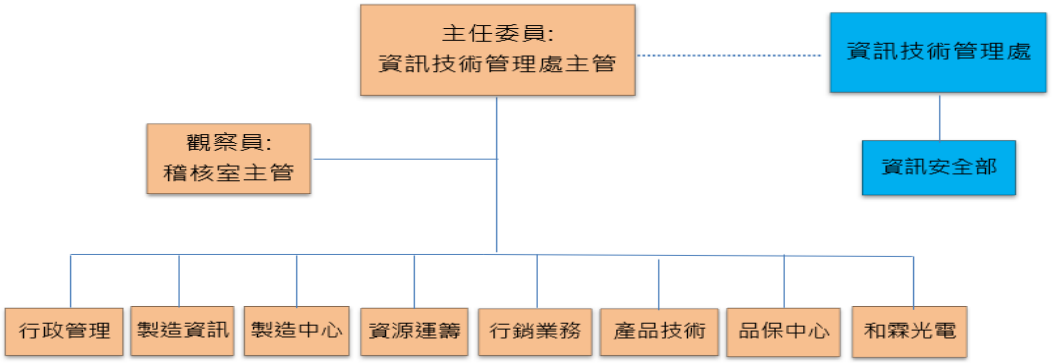
Describe the information security risk management structure, information security policies, specific management plans, and resources invested in information security management. (Regulatory basis: Article 18, Paragraph 6, Item 1, Annual Report Standards)

Information security management structure

In 2021, GP established the "Information Security Management Committee" to coordinate the formulation, implementation, risk management and compliance assessment of information security and protection-related policies, and establish a management framework to initiate and control the implementation of information security. This committee reports directly to the general manager, and the chairman reports to the board of directors regularly every year on the effectiveness of information security management, information security-related issues and future information security planning directions.



The "Information Security Management Committee" is composed of the head of the Information Technology Management Department as the chairman, and directors at the director level of administration, business, R&D, financing, manufacturing and other central plants as committee members. It also sets up the internal audit supervisor as an observer and holds meetings every month. Review and decide on information security policies and measures, discuss new major issues related to information security, and regularly review the effectiveness of information security defense. In addition, the "Information Security Department" has been established under the Information Technology Management Office, which is responsible for the company's information security planning and implementation and review of specific management measures to ensure the effectiveness of information security management.



(委員: 上列各機能中心廠處級主管)

Information security policy

GP's information security policy covers the company and its overseas subsidiaries, and follows the following guidelines:

1. Establish information security management specifications that comply with regulations and customer needs.
2. Reach a consensus that everyone is responsible for information security through awareness among all employees.
3. Provide a secure information processing, transmission and storage environment to protect the rights and interests of customers, the company and all employees.
4. Strengthen information security management, ensure the confidentiality, integrity, availability and network security of various information assets, gain customer trust, and ensure the sustainable operation of GP Group's business.

In order to effectively implement information security management, through information protection systems and management strategies, we can reduce enterprise information security threats from the system level, technical level, and procedural level, in accordance with "Plan-Do-Check-Act" (PDCA, Plan-Do-Check- Act) cycle for continuous improvement.

- Planning stage: Focus on information security risk management, establish GP Group’ s information security management specifications, regularly revise information security management plans, procedures and measures, so that information systems can operate under standard management specifications and reduce security vulnerabilities caused by human beings or abnormal.
- Execution stage: Construct a multi-layered information security defense, integrate the information security control mechanism into the daily maintenance of software and hardware, systematically monitor information security, and ensure the confidentiality, integrity, availability and network of important information assets. Safety.
- Audit stage: Actively monitor the effectiveness of information security management, measure information security indicators based on the audit results, and conduct external weak scan tests to ensure continuous improvement of information security management and defense capabilities.
- Action stage: review and continuous improvement, deal with problems immediately, and reflect the countermeasures to the revision of management rules in a timely manner. Continuously conduct information security education training and information security promotion for all employees to enhance information security awareness.

Specific management plan

Enhance information security capabilities with a multi-layered information security defense architecture:

a) Network security: Introduce next-generation defense systems IPS, APT, and WAF. In response to the digitization of attack methods, firewall network control strategies have been strengthened.

b) Email security: The group's email defense system has been upgraded and adopted the latest APT, DLP, anti-virus and anti-counterfeiting systems.

c) Device safety: Control around the device to prevent lateral infection from occurring when using the device.

d) Introduce defense systems such as EDR and MDR to automatically associate attack chains with user computers and servers to block the occurrence of horizontal attack chains.

Improve information security management procedures:

a) Application security: Continue to strengthen application security control mechanisms and integrate them into the development process.

b) Strengthen authority management: Regularly take inventory of access rights to all files in the group and administrator rights of each system platform.

c) Strengthen personnel account management and introduce a multi-factor authentication mechanism.

Review and continuous improvement:

a) Convene information security committee meetings every month to confirm the effectiveness of information security management and review and discuss information security-related issues or events.

b) Enhance employees' vigilance against email social engineering attacks and perform phishing email defense detection.

Risk control: Regularly conduct system vulnerability testing and analysis, and make enhancements and repairs.

Invest resources in information security management

Corresponding information security management matters and investment resources are as follows:

- Upgrade information security defense systems and equipment:

(a) Endpoint defense: Traditional anti-virus software has been fully upgraded to an EDR defense system in 2022.

(b) Server defense: MDR protection has been introduced in 2022 and maintained by security experts 24/7.

(c) Email protection system upgrade: The email system has been fully upgraded in 2023. The new email protection system includes new protection functions such as counterfeit identification, behavior detection, and APT defense, which can reduce the occurrence of

email security vulnerabilities.

- Dedicated manpower: There is a full-time "Information Security Department" with two information security supervisors and one information security personnel, responsible for the company's information security architecture design, information security maintenance and monitoring, information security incident response and investigation, Social engineering drills, disaster recovery drills, assisting the Information Security Committee in developing information security policies, etc.

Education and training:

(a) All new employees will complete new employee information security training within one week of arrival. Completion rate: 100%.

(b) All group employees must undergo at least one information security training course every year, with a completion score of 100.

(c) Quarterly social engineering drills and post-social engineering training, completion level: 100%.

- Information security announcement:

a) Regularly announce the key points of the Information Security Committee meeting every month to let all employees understand the company's information security defense status and effectiveness, and convey the importance of information security.

b) In response to internal and external information security incidents, information security publicity announcements will be made irregularly every month to enhance the information security alertness of colleagues.

- Customer satisfaction: There are no major information security incidents, and there are no complaints about breach of customer information and loss.

Major information security incidents

GP did not have any major information security incidents in 2012, nor did any information security incidents cause losses to the company.

Information security risks and countermeasures

In the era of rapid changes in information technology, cyber attacks occur one after another, and information security risks have become an important consideration for the operations of various enterprises. In order to pursue the sustainable development and operation of the company, GP established the "Information Security Management Committee" in 2021. The members of the organization are all senior managers of the company's various functions to promote the formulation and implementation of information security-related strategies, and regularly Hold a meeting to discuss the implementation of the information security management system, as well as related preventive and corrective measures. After the meeting, the information security implementation results and risk profile will be announced to all employees to establish the awareness that "information security is everyone's responsibility."

GP attaches great importance to the prevention of information security and network risks, so it has constructed a multi-layered information security defense network, including firewalls, intrusion detection, internal horizontal diffusion blocking EDR defense systems, and servers from the outside to the inside. Server security 7X24 hours information security expert MDR defense system, vulnerability scanning and patch

management. In the email protection part, a new defense system is introduced, including APT defense, face-changing defense, email behavior defense, email anti-virus, and spam filtering system. In order to improve the information security awareness of all employees in the company, we conduct actual social engineering drills every quarter, conduct re-education training for employees with weak information security awareness, and conduct regular information security training for all employees. The above measures are all to ensure the continuous improvement of GP's information security defense capabilities.

GP has established comprehensive network and computer-related information security protection measures. According to the existing management system and control measures, traditional malicious programs such as viruses, Trojans and worms, and traditional hacker external attacks will not easily cause damage to the company's information system. Damage, but there is no guarantee that the company will not be affected by new risks and attacks in the ever-changing information security threats. Therefore, the GP information security team always adopts a cautious and rigorous attitude, and continuously monitors the result records of all information security defense systems. Review and evaluate the information security risk coefficient. If the risk is higher or doubt arises, information security personnel will take immediate measures and respond quickly to ensure that losses are minimized when a cyber attack occurs.