

Information Security Management System

In order to cope with the rapid changes in the technological environment and the diversified development of business, effectively protect the company and customers' operational information and provide good information security governance, so as to protect the information assets of customers, companies and individuals from internal and external intentional or accidental damage, and to fulfill the responsibility of protection and management of the information processed, stored or transmitted, Nafco has started the international information security management system standard ISO27001:2013 in 2021, with six phases of introduction and verification in the second quarter of 2021.

In order to continuously align with international security standards and respond to emerging threats, Nafco continuously reviews and revises relevant information security policies, management procedures and operating methods every year. From time to time, education, training and publicity are used to enable each unit to truly understand the information security policy, follow the relevant control operation procedures and continuously improve the confidentiality, integrity and availability of all operations of each information service system, so as to maintain the information security and sustainable business philosophy of all businesses of the company.

Information security management organization

In order to improve the company's overall information service management performance, ensure the consistency of information and business needs, and effectively manage information security work, the company will cooperate with the ISO 27001 introduction schedule plan and propose to set up an information development promotion committee to implement the implementation.

Protection against emerging malicious threats

In order to raise staff's awareness of information safety to combat malicious email or commercial email fraud, in addition to implementing security education and training for new employees, we also continue to

conduct security publicity through e-newsletters; For system vulnerability patching and protection, the system and equipment are updated to the latest version before and during the launch to maintain basic security protection requirements.

Vulnerability scans are also performed regularly to detect and verify the security status of each system. And pay attention to the security situation at any time, and immediately investigate and formulate repair or improvement countermeasures for newly exposed security vulnerabilities. For threats such as new viruses and malicious programs, such as ransomware and mining software, a variety of security protection mechanisms have also been established to cooperate with the security management procedures and take timely countermeasures.

Information Services Continuing Operation Plan

In order to ensure that in the event of a sudden major disaster, the information service can minimize the impact on the business and resume operation in the shortest possible time by taking the correct response measures, Nafco has formulated a disaster recovery plan and conducted annual drills and reviews to maintain resilience and the continuous operation of the company..