8.3 Information Security

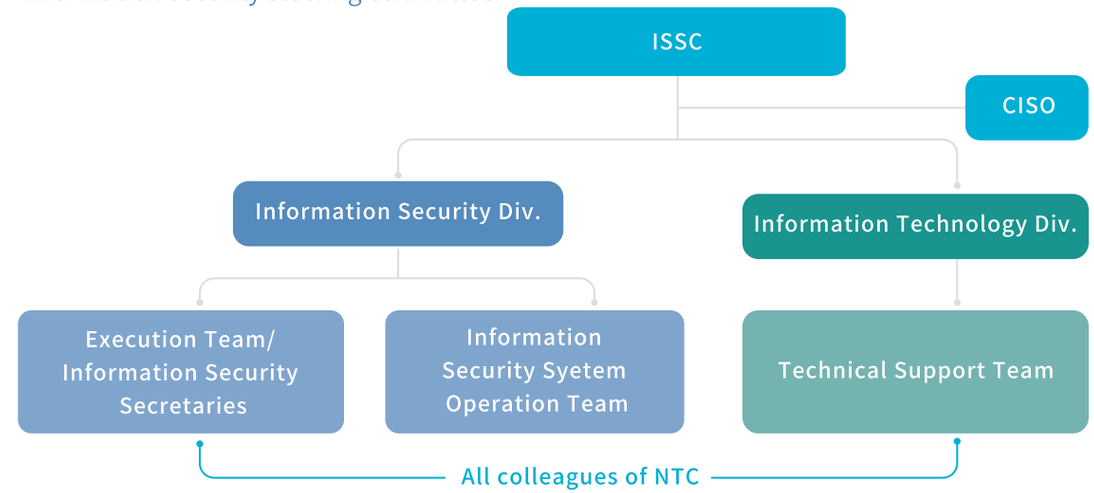
Nanya is actively implementing information security related systems to protect the interests of shareholders and customers. The Company has invested over NT$1 billion into information security over the past 6 years, and also established an Information Security Committee. Information security is personally supervised by the president and overall information security operations are already on track. We continue to make improvements in response to external threats, and ensure the Company's smooth operation to gain the trust of shareholders and customers. Information Security Policy

We have focused our efforts in the field of DRAM for several decades, and are fully aware of the challenges in developing DRAM processes and products, as well as the importance of advanced process development, production know-how, and intellectual property rights protection. This is why we take information security very seriously, and have enhanced information security measures and raised employees' information security awareness to prevent the leakage of classified and sensitive data. These efforts aim to maintain the Company's R&D capabilities and core competitiveness, which is necessary to protect the Company's long-term interests and employees' work rights.In 2022, Nanya once again passed the information security verification that is carried out for ISO 27001 every three years. The scope of verification was expanded from the six main units to 100% coverage of all fabs, and the effectiveness of the certificate was maintained in 2023, showing Nanya's emphasis on its information security management system, while meeting international standards.

Nanya established an inter-departmental Information Security Committee to advance information security management. The president serves as the convener and appoints level 1 supervisors as committee members. One of the members was appointed as the Chief Information Security Officer (executive secretary). Members include the Chief Information Security Officer (Senior Director Huang Yen-Chang), Quality Assurance Division, Legal & IP Division, Human Resources Division, and Information Technology Division. Meetings of the Information Security Committee are convened every week. The committee is mainly responsible for the planning, formulation, approval, and supervision of the information security policies, goals, and related regulations. In addition, the committee quarterly reports the results of the operations of the information security management system to the board of directors. In addition, our four executive directors (President Pei-Ing Lee, Executive Vice President Lin-Chin Su, Vice President Joseph Wu, and Vice President Rex Chuang) also actively participate in the Company's quarterly information security meetings and annual information security management review meetings to ensure the effectiveness and benefits of the management.

In accordance with the implementation of the Cyber Security Management Act, Nanya Technology Corporation is following the requirements applicable to Grade A government agencies regarding cyber security responsibilities. The company currently holds valid cyber security professional certifications, Include EC-Council CCISO (Certified Chief Information Security Officer), EC-Council ECSA (Certified Security Analyst), EC-Council CEH (Certificated Ethical Hacker), EC-Council ECIH (Certified Incident Handler), CompTIA Security+, EC-Council CND, EC-Council CPENT, and ISO/IEC 27001:2013 Information Security Management System (ISMS) Lead Auditor (ISMS chief auditor) to enhance the professional competencies and efficiency of information security personnel.

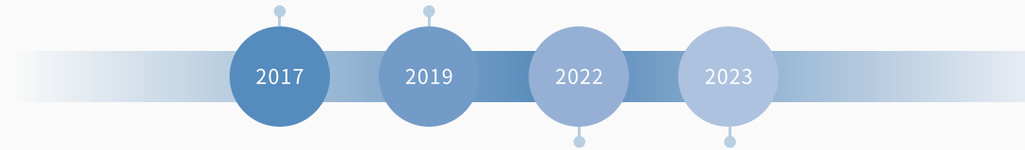
Information security steering committee



Milestones of Nanya's improvement measures for information security management

In response to risks of poaching by competitors which may cause risks of inappropriate acquisition of the Company's confidential and sensitive business information, the Company established the Information Security Section to take charge of planning, executing, auditing, and improving information security management.

- Obtained the ISO27001 Information Security Management System certificate for the first time.
- Continued to develop hacking prevention strategies and defense-in-depth plans in response to the frequent cybersecurity attacks in Taiwan and overseas, as well as the endless stream of attack methods.



- Once again passed the information security verification carried out every three years for ISO 27001 ISMS, and the scope of verification was expanded to all fabs.
- Established the OT (Facility) information security system to implement vulnerability management and establish monitoring and response mechanisms.
- Conducted ISMS information security management reviews of major downstream contractors, in order to continue improving the effectiveness of supply chain information security.

Classified suppliers and carried out risk management, audits, and improvements for key high-risk suppliers.

Main methods and implementation results of information security management

Implementation results of Nanya under the information security policy to ensure the confidentiality, integrity, and availability of information, and to protect the rights and interests of customers, shareholders, employees, and suppliers in 2023 are described below:

01 Strengthen information security and establish defense-in-depth

- Formed by sensitive data encryption, endpoint protection, and network gateway protection, which are supported by network access control, document output management, and e-mail protection mechanisms. We also installed metal detectors for controlled information security products, so as to prevent external cyberattacks and internal leaks.
- Strengthened endpoint security: Installed anti-virus software, updated security patches, controlled USB access, and established a backup mechanism to strengthen system security and lower the risk of system vulnerabilities.
- Protection from the threat of external attacks: Installed an information security system, web isolation, and file disarming mechanisms to prevent computer viruses or malware from affecting information system services or accessing confidential data, and also prevent the theft of confidential data through social engineering.
- Establish a Facility/FAB OT information security system: Improves visualized asset management, real-time monitoring of threats, and accelerates incident investigation and response.
- Establish an automated information security joint prevention and response system to improve threat detection and information security incident response capabilities.

02 Established physical security measures

- Established the Company Classified Information Management Guidelines. There are metal detectors at the entrances of office areas and plants, objects must be carried by personnel through the metal detectors, the Company's confidential information may not be disclosed to others without authorization, and the Company established related evaluation mechanisms.
- Access control, system login identity authentication, password control, access right control, and periodic vulnerability scanning.

03 Quality management and regulatory compliance

- In 2022, Nanya once again passed the information security verification that is carried out for ISO 27001 every three years. The scope of verification was expanded from the six main units to 100% coverage of all fabs, and the effectiveness of the certificate was maintained in 2023, showing Nanya's emphasis on its information security management system, while meeting international standards. ISO 27001
- Each year, we examine our information security measures and regulations, follow information security issues, formulate response plans to ensure their appropriateness and effectiveness, and give reports during ISO management review meetings.
- The Company has always attached importance to information security and personal data protection. We protect customers' rights and interests and fulfill our responsibility to personal data protection. Access rights to personal data are separated and controlled, and encryption is used for transmission protection to prevent unauthorized data leakage.

04 Training to raise information security awareness

- Phishing mail testing tools well known in the industry are used for social engineering drills. Every quarter multiple social engineering drills are carried out by mailing phishing mail and setting goals for the drills. Enhanced training is provided to employees who click on the link and open the attachment in the e-mail. We also established related evaluation mechanisms so that all employees will take the drills seriously, and to raise their information security awareness. A total of 8 drills were conducted throughout the year with over 28,000 participants and over 700 participants in overseas subsidiaries.
- We provide employees and new recruits with annual information security training to raise their awareness of information security risks.
- Professional cultivation of talents; recruit and cultivate the professional and cross-domain integration capabilities of information personnel, and obtain international professional certificates to enhance personnel's academic abilities and expand their fields.

05 Business continuity

- The Company assessed and identified risks that have the most severe impact on key business processes, and used it as the basis for the frequency of post-disaster recovery drills.
- Defined availability goals for information systems for the office area, R&D and design, and technology development, and set the annual goal for service suspension at ≤ 1 time and < 24 hours each year. Information systems were not suspended in 2023.

06 Supply chain security

- In addition to the Company, we have expanded our information security to the entire supply chain. Equipment must pass a security inspection when entering our factories before they may be used. We also signed an information security clause with vendors and their employees to prevent attacks through our supply chain.
- An ISMS inspection of main downstream contractors was carried out in 2023. Appropriate corrective and preventive measures were taken for potential non-confirming items to ensure that the supply chain meets the Company's information security requirements.
- In 2023, we classified suppliers through self-assessment questionnaire(SAQ) and SecurityScorecard(SSC) and carried out risk management, audits, and improvements for key high-risk suppliers.

07 Discuss information security incidents and methods used by hackers

- We conducted penetration inspections of external service systems for 21 external websites, and made improvements for security weaknesses that were found.
- Nanya formally joined TWCERT/CC in 2022 to more quickly learn about methods used by hackers and take preventive and response measures in advance.
- A third party is commissioned to conduct annual penetration testing and red teaming to test the Company's information security for early discovery of system loopholes and vulnerabilities, so that improvements and corrections can be carried out.
- Nanya actively participated in the 2023 TWCERT/CC enterprise information security drill to strengthen the Company's ability to respond to information security incidents, and improve overall information security capabilities.

Business Continuity Plan (BCP)

As different departments have different information system structures, we have performed risk evaluation and identification on these systems based on the severity of the impact of each system on key operation procedures so as to define the degree of severity of each system. The severity degrees are to serve as the basis for determining the frequency of post-disaster recovery exercises. The severity is classified into three degrees from important to minor (Degree 1 to 3). Description of each degree is explained below:

Degree 1	Degree 2	Degree 3
The suspension of operations of the system will suspend services provided with the primary functions.	The suspension of operations of the system will suspend services provided with the secondary functions.	The suspension of operations of the system will not affect the services provided or the system can continue operations with other remedial measures to provide services.
Recovery drill cycle **Half a year**	Recovery drill cycle **Two years**	Recovery drill cycle **No drills required**

The recovery drill cycle is also divided based on the severity degrees (semi-annually, every two years, no drills required). Each department shall register the rating of the systems they are responsible for operations and maintenance in the list in the "information system severity degree classification" document. All Degree 1 systems are provided with multiple backup mechanisms placed in different server rooms in different buildings. All production information is provided with remote backup through encryption and the Company conducts recovery exercises according to the information system disaster recovery plan, in order to ensure the normal operation of systems. The Company has a total of 17 systems that required drills in 2023. We completed drills for 17 systems and the completion rate was 100%. Each information system management unit notifies the response units in the execution of response measures in accordance with the response procedures in the "Information System Response Plan" in the event of major anomalies.

Information Security Awareness Training and Results

The Information Security Secretaries is formed by designated personnel, and members are Information Security Secretaries from each department. The members' tasks include cooperating with the Information Security in providing information security awareness training, formulating and modifying information security procedure, planning and execution of information risk assessment operations and cooperating with the Information Security Section or other units in information security-related matters. In terms of information security awareness training, Nanya has invested many resources in hopes of raising information security awareness and building a consensus among all employees. We provide information security education to our information security secretaries at monthly information security meetings. Quarterly meetings to report information security performance evaluation results to supervisors above the first level, conduct social engineering drills on a quarterly basis, and organize information security month activities each year, and in order to deepen the culture of confidential information management, all employees are required to complete the online designated reading course "Company Confidentiality Management Measures" every year. See the table below for courses and number of hours in 2023.

Type of training	Information Security Awareness Training Courses	Subjects	Number of hours
Designated reading for all employees	Company Classified Information Management Guidelines	All employees	3,629
Information security education for new employees	Proper Information Security Management (I)	New recruits (within a week)	440
	Proper Information Security Management (II)	New recruits (within six months)	570
Social engineering training	Social engineering exercises	All employees (excluding TA)	2,333
	Social engineering training	Employees who clicked on the link	14
Information security seminars (external lecturer)	AI Applications and Information Security	Information security Secretaries, Information Security Division	101
	Common hacking techniques and recommended response measures	Supervisors, Information Security Secretaries	77
Internal auditor training	ISO 27001 internal auditor training	Information Security Secretaries	90
Annual information security activities	Information security management Q&A	All employees	1,780
Total hours			9,031

Information Security Goals

The Company understands that its information systems will continue to face threats and risks, and thus comprehensively deployed suitable information security mechanisms. The Company passed the third-party audit in 2023 without any major deficiencies, and there were no customer information leakages and fines for major information security incidents as well, see the table below for details.

Item	Statistics
Violations of information security or network security incidents (number of cases)	0 cases
Data leakage incidents (number of cases)	0 cases
Number of information security violations involving customers' personal data	0 cases
Number of customers and employees affected by data leakage	0 times
Amount of fines imposed due to information security or network security incidents(NT$)	NT$0