8-3 Information Security

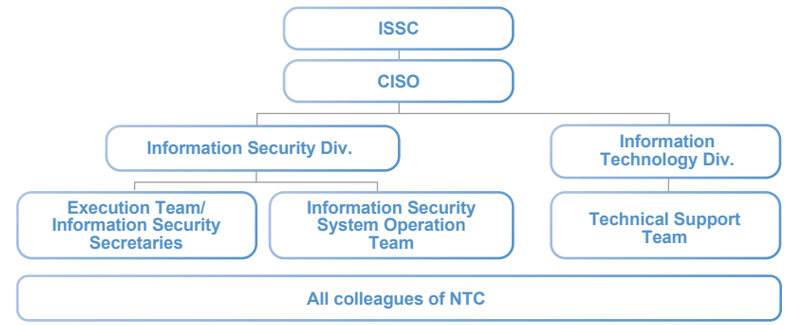
Nanya Technology Corporation is actively implementing information security related systems to protect the interests of shareholders and customers. The Company has invested over NT$1 billion into information security over the past 5 years, and also established an Information Security Committee. Information 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.

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.

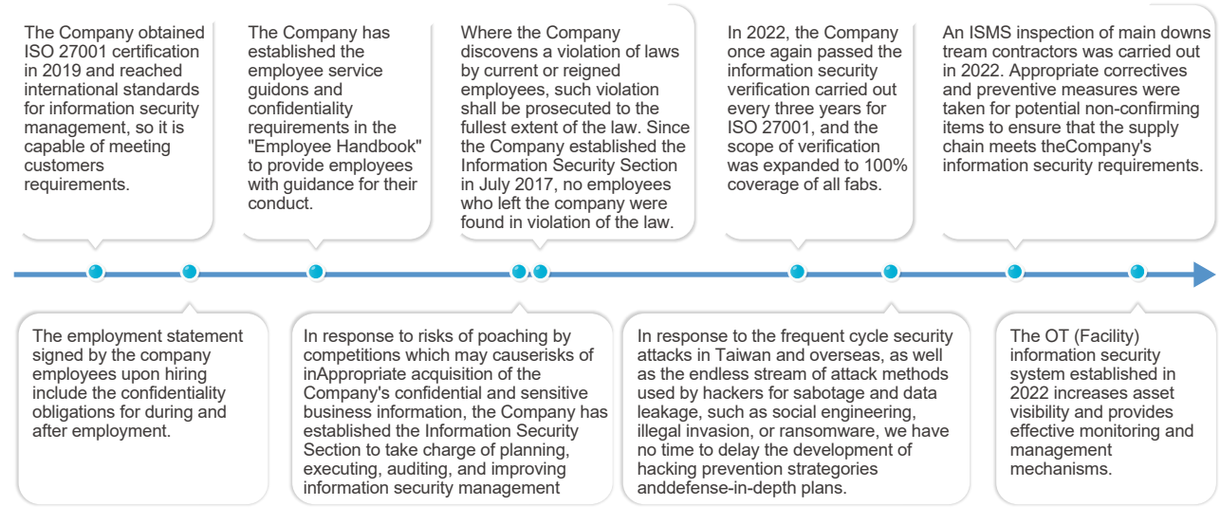
In 2022, Nanya Technology Corporation once again passed the information security verification that is carried out for ISO 27001 every three years. The scope of verification was expanded from the six main units to 100% coverage of all fabs, showing Nanya Technology Corporation's emphasis on its information security management system, while meeting international standards.

Nanya Technology Corporation established an inter-departmental Information Security Committee to advance information security management. The President serves as the convener and five level 1 supervisors were appointed as committee members. They include the Information Security Officer (Special Assistant Shin-An Niu) and heads of the Quality Assurance Division, Legal & IP Division, Human Resources Division, and Automated Information 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 coordination with the enactment of the Cyber Security Management Act, Nanya Technology Corporation obtains effective cyber security certificates the same as government agencies with Grade A information security responsibilities. We have already obtained 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, 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.



Nanya's improvement measures for information security management



Nanya's main measures for information security management

Comprehensive defense-in-depth architecture:
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.

Established physical security measures:
Access control, system login identity authentication, password control, access right control, and periodic vulnerability scanning.

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.

Enhanced training to raise information security awareness:
We provide employees with annual information security education, training, social engineering exercises, and testing to raise their awareness of information security risks.

Regulatory compliance:
Each year, we examine our information security measures and regulations, follow information security issues, and formulate response plans to ensure their appropriateness and effectiveness.

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.

Specialist cultivation:
We recruit and develop the expertise and interdisciplinary integration ability of IT personnel, who obtain international certifications to enhance their core competencies and broaden their expertise.

Discuss information security incidents and methods used by hackers:
Nanya Technology Corporation formally joined TWCERT/CC in 2022 to more quickly learn about methods used by hackers and take preventive and response measures in advance, so that we will be able to anticipate developments and trends in emerging information security threats.

Complete third party penetration testing:
Commission a third party to test the Company's information security for early discovery of system loopholes and vulnerabilities, so that improvements and corrections can be carried out.

Establish an OT (Facility) information security system:
Increases asset visibility and provides effective monitoring and management mechanisms.

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.

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 of severity and recovery cycle table

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 each year 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 2022. 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

In terms of information security awareness training, Nanya Technology Corporation has invested many resources in hopes of raising information security awareness and building a consensus among all employees. We raise awareness among information security officers during monthly information security meetings, compare the performance of reports from supervisors ranked level 1 or above in quarterly information security meetings. conduct social engineering drills on a quarterly basis, and organize information security month activities each year. To develop a culture for the management of confidential information, all employees must complete reading courses of the “Company Confidential Information Management Regulations” each year. See the table below for courses and number of hours in 2022

Information Security Awareness Training Courses	Subjects	Number of hours
Information Security Month Online Q&A	All employees	1,827 hours
Information Security Seminar (Virtual Artillery Fire in the Russo-Ukrainian War – Modern Cyber Warfare)	Information security officers, Information Security Divisio	100 hours
Information Security Seminar (Sharing of Trade Secret Cases)	Supervisors, Information Security Section	104 hours
Social engineering exercises	All employees (excluding TA)	2,373 hours
Social engineering training	Employees who clicked on the link	198 hours
[Reading for all employees] Company Classified Information Management Guidelines	All employees	1,489 hours
[Reading for all employees] Sharing of Trade Secret Cases and Exchanges	All employees	775 hours
Total		6,866 hours

Information security month activities are organized every year to raise employees’ information security awareness, and all employees participated in the production of the information security promotion clip. Implementation results are as follows

Item	Implementation results
Promote the participation of all employees and presentation in the form of short clips, and have share their own experiences of encountering fraud.	35 units submitted at least one short clip
Organized two physical information security seminars "Virtual Artillery Fire in the Russo-Ukrainian War – Modern Cyber Warfare" and "Sharing of Trade Secret Cases (Ministry of Justice Investigation Bureau)."	Unit supervisors and information security officers participated over **120** times.
All employees participate in Q&A on information security policy and rules.	**99.9**% of employees answered all questions correctly

Information security implementation results

Implementation results of Nanya Technology Corporation 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 2022 are shown in the table below:

Company Classified Information Management

Implementation measures

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.

Implementation results

There were no confidential information leakage incidents.

Social engineering exercises

Implementation measures

Every quarter 2 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.

Implementation results

There were over 28,000 participants in the 8 drills during the year.

Information security and monitoring

Implementation measures

Company's internal statistics, the number of hacking attempts has significantly increased since 2021. To lower the probability of hacking or data leakage and prevent data from being exploited or used make threats, the Company established a complete defense-in-depth system, analyzed hacking methods, continued to patch system loopholes, and appointed dedicated personnel for monitoring.

Implementation results

conduct penetration testing and red team assessments.

Business continuity

Implementation measures

1. 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.
2. 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.

Implementation results

1. Exercises were 100% completed for all 17 of the systems that required exercises to be performed in 2022.
2. Services of information systems were not suspended.

Information Security Risk Protection

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 2022 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 cases
Amount of fines due to information security or network security incidents (NTD)	NT$0