Information Security

To protect shareholders' and customers' best interests, Nanya Technology actively implements information security-related procedures and protection systems. Over the past 7 years, we have invested over NT$1 billion in information security. An information Security Committee is also established and personally supervised by the President to optimize our information security management and ensure adherence to relevant legal requirements continuously. Working alongside all employees and supply chain partners, we collectively ensure the confidentiality, integrity and availability of our information assets. Our goal is not only to safeguard the rights of our customers, shareholders, employees and suppliers, but also to fulfill our corporate social responsibility.

Information Security Policy

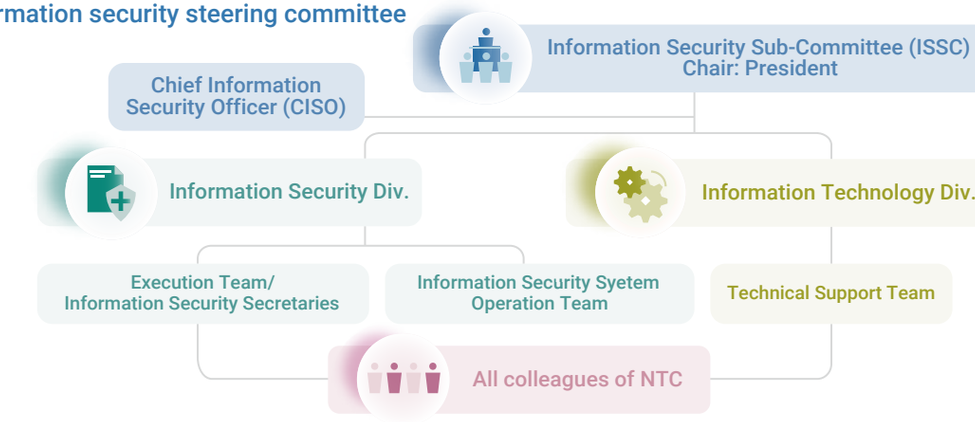
With decades of experience in the DRAM memory domain, Nanya Technology fully understands the challenges in DRAM process and product development, advanced process development, manufacturing know-how, and the importance of protecting intellectual property rights. We focus on strengthening information security measures and employee awareness to prevent sensitive technical data leaks. These efforts help preserve our R&D capabilities and core competitive advantage, thereby protecting the long-term interests of the Company and ensuring the working rights of our employees.

In 2022, Nanya Technology once again passed the triennial ISO 27001 information security certification, expanding its verification scope to cover 100% of all facilities. The certification remained valid in 2024, demonstrating our ongoing commitment to an information security management system that aligns with international standards.

To further enhance information security management, Nanya Technology established a cross-departmental Information Security Committee with the President as the convener. Several Level 1 supervisors serve as committee members, with one appointed as the Chief Information Security Officer (Executive Secretary). The committee includes Senior Division Head Yen-Chang Huang as the Chief Information Security Officer, along with representatives from the Quality Reliability Assurance Division, Legal & IP Division, Human Resources Division, and Automated Information Division. The Information Security Committee meets weekly to plan, approve, and oversee information security policies, objectives, and related regulations. It reports quarterly to the Board of Directors on the effectiveness of the information security management system and identifies opportunities for further enhancement. At the same time, four executive directors (President Pei-Ing Lee, Executive Vice President Lin-Chin Su, Vice President Joseph Wu, and Vice President Rex Chua) actively engage in the Company's quarterly information security meetings and the annual information security management review meeting. This helps make sure that our security management is working well and effectively.

Nanya Technology adheres to the Cyber Security Management Act requirements at the highest "A" level (equivalent to government agencies). We hold various cybersecurity certifications, including EC-Council Certified Chief Information Security Officer (CCISO), Certified Information Systems Security Professional (CISSP), EC-Council Certified Security Analyst (ECSA), EC-Council Certified Ethical Hacker (CEH), EC-Council CompTIA Security+, EC-Council Certified Network Defender (CND), EC-Council Certified Penetration Testing Engineer (CPENT), EC-Council Certified Application Security Engineer (CASE), and ISO/IEC 27001:2013 Information Security Management System (ISMS) Lead Auditor, enhancing the professional capabilities and efficiency of our information security team.

Information security steering committee



Milestones of Nanya Technology's Improvement Measures for Information Security Management

2017	• To deal with the risk of competitors recruiting our employees, which led to improper access to company secrets and sensitive business information, Nanya Technology set up an Information Security Division responsible for planning, implementing, auditing, and improving our information security management.
2019	• Nanya Technology obtained ISO27001 information security management system international standard certificate for the first time. • In response to the frequent cybersecurity attacks at home and abroad, and the emergence of new attack methods, Nanya Technology continued to develop external hacker protection strategies and defense in depth solutions.
2022	• Once again, Nanya Technology passed the triennial ISO27001 information security management system standard certification, with the scope of verification expanded to include the entire facility. • An OT (Facility) information security protection system has been established, incorporating vulnerability management and a monitoring and response mechanism. • Nanya Technology conducted ISMS information security management audits for major downstream subcontractors to continuously improve the effectiveness of supply chain information security.
2023	• Nanya Technology classified and graded suppliers, when conducting risk management and audit improvements for critical high-risk suppliers.
2024	• (Facility/FAB) OT information Security Protection: Nanya Technology has enhanced the visibility of industrial control equipment to monitor the normal connection behavior of facilities and machine equipment and mitigate the risk of exposure to unauthorized external equipment. • The information security automated joint defense and response system was launched to monitor more than 380,000 activities throughout the day, automatically blocking suspicious IP sources to improve threat detection and incident response capabilities. • Nanya Technology improved information security management for its supply chain by selecting 137 suppliers in 2024 for SAQ and third-party risk assessment, completing audits and improvements for critical high-risk suppliers. • Nanya Technology followed the NIST standard cybersecurity framework template and used third-party self-assessment information security risk scoring tools to analyze and evaluate multi-faceted compliance to ensure effective information security management.

1. Key Practices and Implementation Results of Information Security Management

Nanya Technology implemented information security policies to ensure the confidentiality, integrity, and availability of information. This protects the rights of our customers, shareholders, employees, and suppliers. The detailed implementation results in 2024 are explained below:

01 Strengthening Information Security and Building Defense in Depth

- Nanya Technology protects sensitive data through encryption, endpoint protection, and network gateways. We control network access, manage document outputs, and secure emails. Additionally, we employ metal detectors to check for restricted items related to information security, preventing external attacks and internal information leaks.
- Strengthening Endpoint Security: Installing antivirus software, updating official security patches, controlling USB access, and setting up backup mechanisms to enhance system security and reduce vulnerability risks.
- Protecting against External Threats: Establishing information security protection systems, isolating internet access, and implementing secure file mechanisms to prevent computer viruses or malicious programs from disrupting information system services or stealing confidential data, including through social engineering attacks.
- (Facility/FAB) OT information Security Protection: Nanya Technology has enhanced the visibility of industrial control equipment to monitor the normal connection behavior of facilities and machine equipment and mitigate the risk of exposure to unauthorized external equipment.
- The information security automated joint defense and response system was launched to monitor more than 380,000 activities annually, automatically blocking suspicious IP sources to improve threat detection and incident response capabilities.

02 Building Physical Security Protection

- Nanya Technology established the Confidential Information Management Procedure and installed metal detectors at all office and facility entrances to screen all items brought in or out. Confidential information must not be disclosed without authorization. An evaluation system is also in place to monitor the effectiveness of these measures.
- Setting up door access controls, system login identity verification, password management, access authorization, and regular vulnerability scanning audits.

03 Quality Management and Legal Compliance

- In 2022, Nanya Technology once again passed the triennial ISO 27001 information security certification, expanding the scope to cover 100% of all facilities. In 2024, we passed the certification of the third-party audit unit Taiwan Testing Technology Co., Ltd. (SGS) to maintain the validity of the certificate, demonstrating our ongoing commitment to an information security management system that aligns with international standards. ISO 27001
- Every year, Nanya Technology reviews its information security protection measures and policies, monitors security issues, and formulates response plans to ensure their adequacy and effectiveness. The implementation results are reported during ISO management review meetings.
- Nanya Technology places high importance on information security and personal data protection to safeguard customer rights and fulfill its responsibility for safeguarding personal data. Additionally, the Company isolates and controls access to personal data and employs encryption to prevent unauthorized data leaks.
- Nanya Technology followed the NIST standard cybersecurity framework template and used third-party self-assessment information security risk scoring tools to analyze and evaluate multi-faceted compliance to ensure effective information security management.

04 Security Awareness Training

- Nanya Technology conducts social engineering drills using well-known phishing email testing tools. Quarterly social engineering drills simulate realistic phishing emails with set goals, and additional training is provided to employees who click on links or open attachments. An evaluation system ensures all employees take exercises seriously, enhancing information security protection awareness. This year, we conducted 8 drills, involving over 29,000 participants locally and 1,331 from overseas subsidiaries.
- We conduct regular information security training for all employees and new hires annually to strengthen information security awareness.
- Cultivation of Professional Talent: Recruiting and nurturing IT personnel to develop both professional and cross-domain consolidated skills, supporting them in obtaining international certifications to enhance their abilities and expand their expertise.

05 Business Continuity

- Due to the constant occurrence of cybersecurity incidents, we have established Information Security Incident Report and Management Regulations. We conduct ad-hoc drills annually to practice our incident response for escalating and managing information security events.
- In accordance with the Cybersecurity Management Guidelines for TWSE/TPEx Listed Companies, we have not only defined levels of information security incident and set up internal and external reporting channels and processes, but also establish response procedures for intelligence of threat which affects stakeholders so as to prevent operational disruptions.
- Nanya Technology conducts risk assessment and identification based on the severity of impact on key business processes, using this analysis to determine the frequency of disaster recovery drills.
- Availability goals are defined for office, research and design, as well as technical development information systems. Our annual target allows no more than 1 service interruption, lasting less than 24 hours. In 2024, the Company had no system service interruptions.

06 Supply Chain Security Protection

- Nanya Technology extends its security protection to the supply chain by ensuring that all equipment undergoes security checks before use. Suppliers and their personnel are required to sign information security agreements to prevent potential attacks via supply chain relationships.
- In 2024, Nanya Technology conducted checks on its main downstream subcontractors for ISMS information security management. When potential issues were identified, the Company took appropriate measures to address and prevent them, ensuring the security of the supply chain aligns with our information security requirements.
- In 2024, Nanya Technology used Self-Assessment Questionnaires (SAQ) and Security Scorecards to classify its suppliers. The Company focused its risk management efforts and audits on critical high-risk suppliers.

07 Investigating Information Security Incidents and Hacking Methods

- Nanya Technology actively engages in information sharing with the Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC) to promptly understand hacking techniques and implement early response measures.
- Nanya Technology commissions third-party organizations to conduct annual red team exercises, testing the Company's information security by identifying system vulnerabilities and weaknesses, ensuring they are addressed and mitigated as early as possible.
- Nanya Technology participated in the 2024 enterprise information security drill organized by TWCERT/CC to enhance its ability to respond to information security incidents and further improve its overall information security protection.

2. Business Continuity Plan (BCP)

Information Security Incident Response Drills: to validate the timeliness of our information security incident report and response procedures, we conduct ad-hoc drills annually for incident response of various scenarios such as computer compromises and DDoS attacks on our official website.

Business Continuity Operations for Information System: to address the differences in information system structures across departments, Nanya Technology conducts risk assessments and identifies potential risks based on the severity of each system's impact on key operational processes. The systems are classified into three severity degrees (Degree 1 to 3), with Degree 1 being the most critical. These classifications serve as the basis for determining the frequency of disaster recovery drills. The degrees are defined as follows:

Relationship Between Severity Degree Classification and Recovery Drill Frequency

Degree 1	Degree 2	Degree 3
If this system stops working, primary functions cannot provide service.	If this system stops working, secondary functions cannot provide service.	If this system stops working, it does not affect services, or alternative measures can be in place to keep operations working.
Recovery Drill Schedule **Annually**	Recovery Drill Schedule **Biennially**	Recovery Drill Schedule **Not required**

Recovery drill schedules are aligned with severity degrees (annually, biennially, or not required). Each department is responsible for registering the severity levels of the systems they operate and maintain in the "Information System Severity Degree Classification" documentation list. All Degree 1 systems have multiple backup mechanisms located in different rooms across different buildings. Important production data is encrypted for offsite backup and tested according to the information system disaster recovery plan to ensure normal operation. In 2024, 12 systems needed drills, and all of the 12 systems completed drills, achieving a 100% completion rate. When major anomalies occur, each information system management unit follows the response procedures defined in the Information System Response Measures Plan to notify the appropriate response teams to take action.

3. Information Security Awareness Training and Implementation Results

The Information Security Division assigns dedicated personnel, with team members from each department serving as security secretaries. Their tasks include implementing information security awareness training, developing management regulations, and conducting risk assessments of information assets.

Nanya Technology invests substantial resources to enhance information security awareness and build a shared understanding among all employees through training programs. This includes monthly meetings for information security secretaries, quarterly security meetings for Level 1 and above senior supervisors to review performance evaluation outcomes, quarterly social engineering drills, annual Information Security Month initiatives, and mandatory annual online reading of the Confidential Information Management Procedure to deepen employees' understanding and strengthen the culture of confidential information management. The 2024 training courses and hours are detailed on the table below:

Training Type	Information Security Awareness Training Courses	Participants	Hours
Designated Compulsory Readings for All Employees	Confidential Information Management Procedure	All employees	1,827
	Understanding BEC (I)	All employees	1,822
	How to Prevent BEC (II)	All employees	1,832
	URL Identification Training	All employees	1,799
Information Security Training for New Recruits	Good Information Security Management (I)	New hires (within 1 week)	665
	Good Information Security Management (II)	New hires (within 6 months)	516
Social Engineering Training	Social Engineering Drills	All employees (excluding TA)	2,528
	Social Engineering Training	Employees clicking on links during drills	52
Information Security Lectures (External Speakers)	Information Security Moat: Protecting Your Digital World	Information Security Secretaries and the Information Security Division	78
	Protecting the Gateway to the Digital World: Understanding ISO 27001	Department supervisors and the Information Security Division	79
	The Functionality and Benefits of Entra ID Cloud Identity Protection	Information Security Secretaries and the Information Security Division	27
	Special Lecture on Trade Secrets	Department supervisors, the Information Security Division, and supply chain vendors	130
	Zero Trust Themed Lecture at the Information Security Seminar	Department supervisors, the Information Security Division, and supply chain vendors	112
Internal Auditor Training	ISO 27001 Internal Auditor Training	Information Security Secretaries	118
Information Security Month Events	Information Security Management Quiz	All employees	1,822
Total Annual Information Security Awareness Training Hours			13,406

4. Information Security Goal Achievement

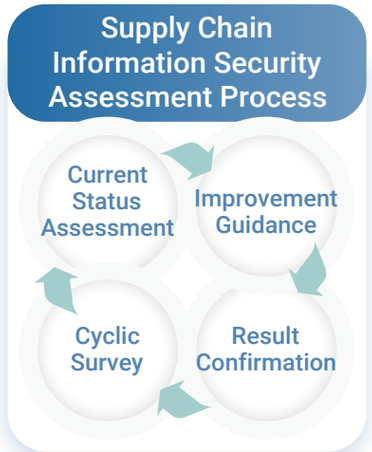
Nanya Technology recognizes the ongoing threats and risks to information security and has implemented appropriate protective measures. In 2024, the Company passed third-party audits with no significant deficiencies and reported no major security incidents such as customer information leaks and regulatory fines, as outlined below.

Item	Statistics
Number of information security violations or cybersecurity incidents	0 cases
Number of data leakage incidents	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 cybersecurity incidents	NT$0

5. Supply Chain Information Security

To promote supply chain information security, Nanya Technology evaluates significant Tier 1 suppliers, equipment vendors, subcontractors, and system integrators (140 companies in 2024) based on factors such as significance, risk level, annual procurement value, and sustainable development. The Company utilizes third-party information security risk assessments (requiring a minimum score of 80 or a B grade) and our internal security evaluations (requiring a score of 85 or above) to assess these selected companies. Those failing to meet the standards are classified as high-risk significant suppliers. Nanya Technology conducts on-site audits, provides guidance for continuous improvement, and requires such suppliers to sign information security clauses in procurement contracts and a Commitment to Comply with Information Security Policy to ensure information security.

In 2024, Nanya Technology expanded evaluations to 140 suppliers, a 164% increase compared to the previous year. Through individual information security coaching, training sessions, Security Score Card requirements, and on-site audits, we continue to help supplier partners improve their information security management. In addition, the Company is progressively requiring suppliers to obtain international certifications, such as ISO 27001, with 33% of suppliers currently certified. In 2024, to enhance supplier awareness of information security, Nanya Technology invited suppliers to participate in its Information Security Month event—Zero Trust Seminar: Never Trust, Always Verify. Through knowledge sharing and discussions with industry leaders and experts, the seminar explored how zero trust architecture can strengthen supply chain security and safeguard shared business data and assets against modern threats. A total of 37 participants from 17 suppliers attended the event.



Key Suppliers

Suppliers of concern are chosen based on factors like significance, risk level, annual purchase amount, and sustainability. The focus is on Tier 1 significant suppliers, equipment manufacturers, subcontractors, and system integrators (140 companies in total).

Third-Party Risk Assessment

Suppliers may voluntarily provide their information security score assessed using a third-party tool. The score must be at least grade B or 80 points.

Self-Assessment Questionnaire (SAQ)

Risk level is assessed based on SAQ results, information security certificates, and past major incidents (85 points and above).