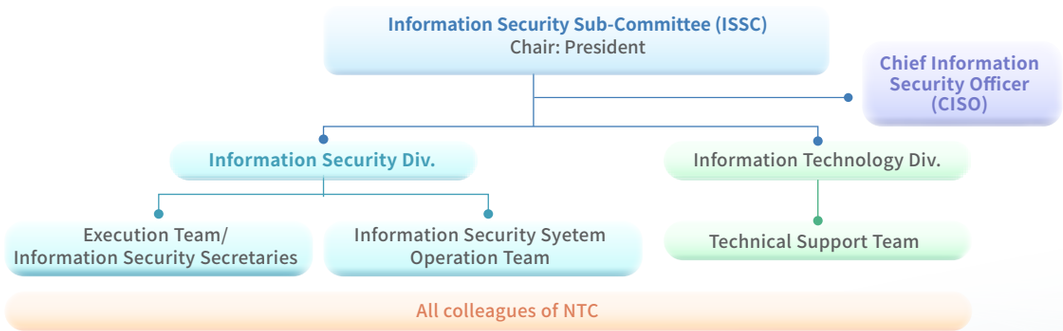
8.3 Information Security

To safeguard the maximum interests of shareholders and customers, Nanya Technology actively promotes the implementation of information security management systems and protection mechanisms. Over the past eight years, the Company has invested more than NT$1 billion in information security, and has established an Information Security Committee, personally overseen by the President, to continuously enhance its information security management practices. The Company strictly complies with relevant regulations and works in collaboration with all employees and supply chain partners to ensure the confidentiality, integrity, and availability of information assets. It safeguards the rights and interests of customers, shareholders, employees, and suppliers, and fulfills its corporate social responsibility. Information Security Policy

With decades of expertise in the DRAM sector, Nanya Technology fully understands the critical importance of protecting process know-how and intellectual property across advanced process development, product research and development, and mass production. Therefore, the Company places great emphasis on information security. It strengthens its information security protection measures and enhances employees' security awareness to mitigate the risk of sensitive technical information leakage. This helps sustain its research and development capabilities and core competitiveness and protect its long-term interests as well as employees' rights and interests.

To further strengthen information security governance, Nanya Technology has established a cross-Departmental Information Security Committee, chaired by the President. The committee comprises several senior executives as members, and one member is additionally appointed as the Chief Information Security Officer and serves as the Executive Secretary. The committee comprises the Chief Information Security Officer, Associate Vice President Yan-Chang Huang, the Quality Reliability Assurance Division, the Legal & IP Division, the Human Resources Division, and the Information Technology Division. The Information Security Committee meets on a weekly basis and is primarily responsible for the planning, formulation, approval, and supervision of Information Security Policy, objectives, and related standards. It also reports quarterly to the Board of Directors on the effectiveness of the information security management system and opportunities for continuous improvement.

In addition, four executive directors (President Pei-Ing Lee, Executive Vice President Lin-Chin Su, Vice President Joseph Wu, and Vice President Rex Chuang) actively engage in the Company's quarterly information security meetings and the annual information security management review meeting. This helps make sure that our information security management is valid and effective.



Key Practices and Implementation Results of Information Security Management

Nanya Technology implemented the Information Security Policy 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 2025 are explained below:

01 Information Security Quality Management and Legal Compliance

(1) In 2025, Nanya Technology once again passed the triennial ISO 27001 information security certification conducted by SGS Taiwan Limited., a third-party auditing organization, expanding the scope to cover 100% of all facilities. The certification demonstrated our ongoing commitment to an information security management system that aligns with international standards.
ISO 27001 Certificate

(2) In accordance with ISO 27001, Nanya Technology has established information security objectives with a total of 13 quantitative indicators.

(3) 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.

(4) 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.

02 Strengthening Information Security and Defense in Depth

(1) 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.

(2) 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.

(3) 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.

(4) (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.

(5) The information security automated joint defense and response system was launched to monitor more than 520,000 activities annually, automatically blocking suspicious IP sources to improve threat detection and incident response capabilities.

03 Strengthening the protection and resilience of information assets

Nanya Technology regards information assets as a core competitive strength. Through stringent asset classification, access control, and operational maintenance technology, it has established a highly resilient defense system to ensure business continuity and safeguard customer trust.

(1) Nanya Technology has established a comprehensive information asset management process and regularly conducts inventories and risk assessments of hardware and software assets. For critical data and personal information, encryption technologies are applied for both storage and transmission. In addition, the data loss prevention system is implemented to prevent unauthorized data leakage, ensuring the security of customer privacy and the Company's intellectual property rights.

(2) Employees are granted only the minimum level of access rights required to perform their duties, in strict accordance with the principle of least privilege. Access rights of employees who resign or change positions are promptly revoked. In addition, privileged accounts are reviewed semi-annually to eliminate the risk of unauthorized access.

(3) In terms of application security, Nanya Technology ensures that servers and operating systems are regularly updated with security patches and implements off-site backups to safeguard business continuity. For in-house developed applications, Secure Software Development Life Cycle (SSDLC) is adopted. All applications must pass vulnerability scanning and penetration testing prior to deployment to ensure no critical security vulnerabilities exist.

04 Building Physical Security Protection

(1) 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.

(2) Setting up door access controls, system login identity verification, password management, access authorization, and regular vulnerability scanning audits.

05 Business Continuity and Information Security Incident Response Measures

(1) Due to the constant occurrence of cybersecurity incidents, we have established Information Security Incident Report and Management Regulations. Moreover, 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.

(2) Nanya Technology conducts information security incident response drills covering various scenarios on an irregular basis. In 2025, the Company collaborated with downstream outsourcing partners to conduct data breach reporting procedures and established emergency response procedures for cyberattacks involving stakeholders, to validate the timeliness and effectiveness of its response procedures.

(3) 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.

(4) 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 2025, the Company had no system service interruptions.

06 Investigating Information Security Incidents and Hacking Methods

(1) 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.

(2) Nanya Technology continues to strengthen both internal and external information security defenses and maintains close cooperation with the Investigation Bureau to facilitate intelligence sharing.

(3) Nanya Technology conducts annual red team exercises. In 2025, no major deficiencies were identified and all findings were duly addressed. To promote information security, we also inspected our systems for vulnerabilities and weaknesses to ensure they are addressed and mitigated at an early stage.

(4) To ensure information security and the integrity of corporate confidentiality, Nanya Technology explicitly prohibits the use of unauthorized cloud-based generative AI tools. At the same time, the Company has introduced a systematic risk assessment mechanism for large language models, establishing comprehensive protection measures. In addition, the CNDCI-0568 Generative AI Development and Management Guidelines have been formally issued to implement structured governance over technology development and applications, strengthening its responsibility in digital governance.

07 Security Awareness Training

(1) 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.

(2) Nanya Technology conducts information security training for all employees and new hires on an irregular basis to strengthen information security awareness.

(3) Nanya Technology places emphasis on talent professional development. The Company recruits and develops information personnel with specialized expertise and cross-functional integration capabilities, while encouraging the attainment of international certifications to enhance competencies and expand professional scope. In addition, Nanya Technology adheres to the requirements at the highest "A" level under information security responsibility classification framework (equivalent to government agencies). We hold various cybersecurity certifications, including EC-Council Certified Chief Information Security Officer (CCISO), ISC2 Certified Information Systems Security Professional (CISSP), EC-Council Certificated Penetration Test Professional (CPENT), EC-Council Certified Network Defender (CND), EC-Council Certified Application Security Engineer.NET (CASE.NET), and ISO/IEC 27001:2022 Information Security Management System (ISMS) Lead Auditor, enhancing the professional capabilities and efficiency of our information security team.

08 Supply Chain Information Security (Policies and Principles)

(1) Nanya Technology adopts a risk-based management approach and has established relevant information security management standards for suppliers, requiring its partners to comply with protection standards equivalent to the Company's standards. For core systems and data service providers, the Company explicitly incorporates the right to conduct information security audits in its procurement contracts.

(2) Nanya Technology strengthens its supply chain information security management by establishing a Supplier Self-Assessment Questionnaire (SAQ). This allows suppliers to assess their own compliance status and serves as a basis for preliminary screening and classification. In addition, independent third-party SSC (Social/Security Compliance) audits are conducted to ensure that suppliers' responses in the SAQ are consistent with their actual practices.

(3) 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.

(4) In 2025, 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.

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, 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 2025 training courses and hours are detailed on the table below:

Training Type	Information Security Awareness Training Courses	Participants	Hours
Information Security Awareness Campaign for All Employees	Information Security Policy Reading	All employees	911
	Confidential Information Management Procedure	All employees	1,866
New Employee Training	Good Information Security Management (I)	New Employee	894
	Good Information Security Management (II)	New Employee	868
Social Engineering Training	Social Engineering Drills	All employees (excluding TA)	2,520
	Analysis and Identification of Common Social Engineering Attack Methods	Employees clicking on links during drills	5
	URL Identification Training	Employees clicking on links during drills	9
	Supplementary Information Security Course (Emails_in_Real_Life)	New employees in the past two years	347
Information Security Lectures (External Speakers)	Cross-Domain Defense: From Endpoint to Identity and Cloud	Information Security Secretaries and the Information Security Division	123
	Case Sharing on Information Security and Emerging Cyber Fraud Cases	Department supervisors and the Information Security Division	128
	Information Security Seminar Themed Lecture	Information Security Secretaries and the Information Security Division	125
Information Security Management Professional Training	Guidelines on Secure Application System Development and Design	System Development and Maintenance Personnel	41
Others	Information Security Management Quiz	All employees	1,833
Total			11,467

Information Security Goal Achievement

Nanya Technology recognizes the ongoing threats and risks to information security and has implemented appropriate protective measures. In 2025, 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

Supply Chain Information Security

To promote supply chain information security, Nanya Technology evaluates significant Tier 1 suppliers, equipment vendors, subcontractors, and system integrators (150 companies in 2025) 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 2025, Nanya Technology expanded evaluations to 150 suppliers. 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 37% of suppliers currently certified. In 2025, to enhance supplier awareness of information security, Nanya Technology invited suppliers to participate in its Information Security Month event—Security Everywhere: Fortifying Our Operational Defense Line—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 46 participants from 26 suppliers attended the event.

150 companies in total

Key suppliers for management are screened based on factors like Significance, Risk Level, Annual Spend, and Sustainability, including Tier 1 significant suppliers, equipment manufacturers, subcontractors, and system integrators

Supply Chain Information Security Assessment Process

Current Status Assessment → Improvement Guidance → Result Confirmation → Cyclic Survey → Current Status Assessment

grade **B** or **80** points

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

85 points

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