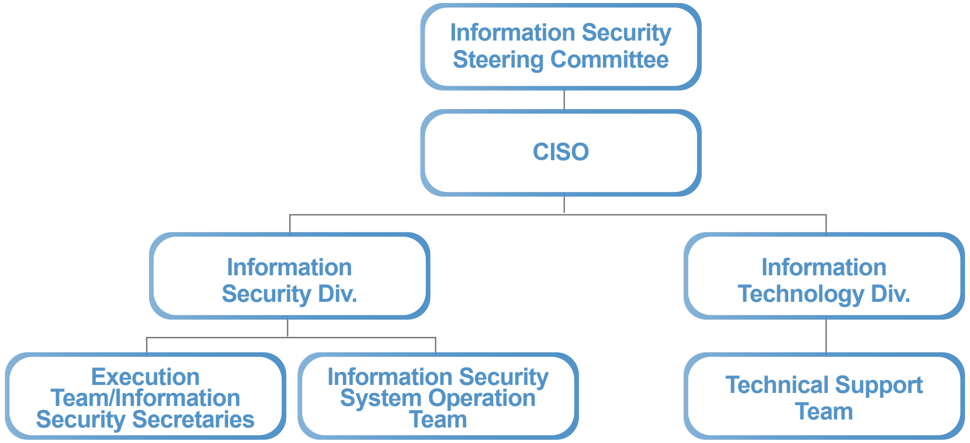
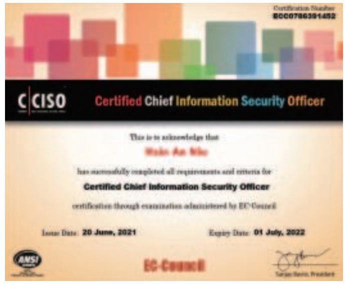
Information Security

Nanya has actively promoted related information security systems to ensure the security of the information of the Company and customers. In 2019, we obtained the ISO 27001: 2013 Information Security Management System certification. The initial verification scope included DRAM technology transfer documents and information on process technologies we independently developed, as well as information flows of the Information Security Management System, including maintenance of related facilities, network services, and the development, operation, and maintenance of information systems. The verification scope covered DRAM R&D, information security management of the production system (including OA and network systems, design and mask tape out system EDA, product testing services, and laboratory management system and PIS system), and all the staff at all plants, so that information security control measures could be strengthened to ensure the smooth operations of the Company and we could earn trust from suppliers and customers.

We 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 is required to obtain 4 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), 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
CISO
Information Security Div.
Information Technology Div.
Execution Team/Information Security Secretaries
Information Security System Operation Team
Technical Support Team


Certification Number
ECC0786391452

C|CISO Certified Chief Information Security Officer

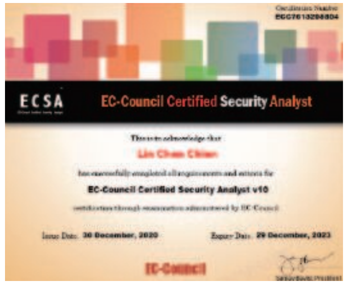
This is to acknowledge that
Hsin An Niu
has successfully completed all requirements and criteria for
Certified Chief Information Security Officer
certification through examination administered by EC-Council

Issue Date: 20 June, 2021 Expiry Date: 01 July, 2022

EC-Council

Sanjay Bavisi, President

Certified Chief Information Security Officer


Certification Number
ECC7613298804

ECSA EC-Council Certified Security Analyst

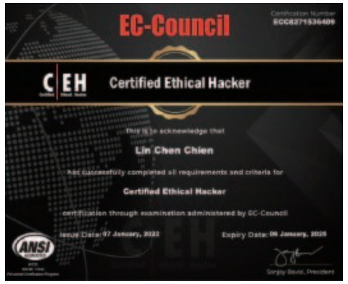
This is to acknowledge that
Lin Chen Chien
has successfully completed all requirements and criteria for
EC-Council Certified Security Analyst v10
certification through examination administered by EC-Council

Issue Date: 30 December, 2020 Expiry Date: 29 December, 2023

EC-Council

Sanjay Bavisi, President

EC-Council Certified Security Analyst


EC-Council

Certification Number
ECC8271536409

C|EH Certified Ethical Hacker

This is to acknowledge that
Lin Chen Chien
has successfully completed all requirements and criteria for
Certified Ethical Hacker
certification through examination administered by EC-Council

Issue Date: 07 January, 2022 Expiry Date: 06 January, 2025

Sanjay Bavisi, President

Certified Ethical Hacker

SGS

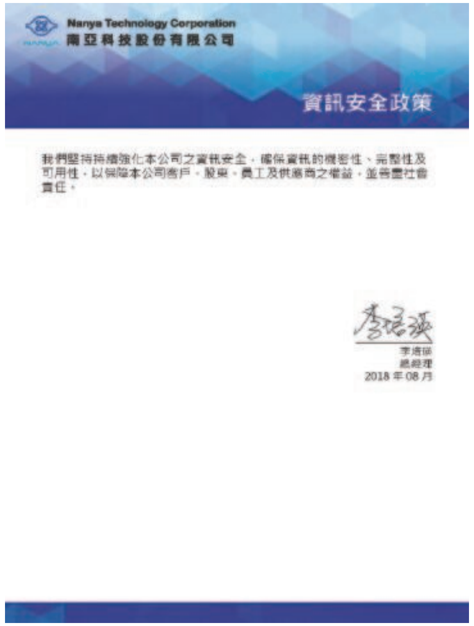
Cheng Hung Shen

ISO/IEC 27001:2013 - Information Security Management Systems Auditor/Lead Auditor Training Course

Taipei, Taiwan

CQI IRCA

ISO 27001 Lead Auditor

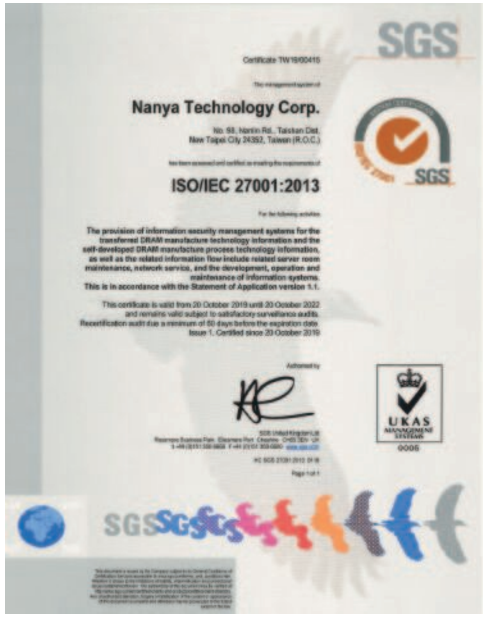

Nanya Technology Corporation
南亞科技股份有限公司

資訊安全政策

我們堅持持續強化本公司之資訊安全，確保資訊的機密性、完整性及可用性，以保障本公司客戶、股東、員工及供應商之權益，並善盡社會責任。

李培瑛
總經理
2018 年 08 月

Information Security Policy


SGS

Certificate TW19/00415

Nanya Technology Corp.
No. 98, Nanlin Rd., Taishan Dist.
New Taipei City 24352, Taiwan (R.O.C.)

ISO/IEC 27001:2013

The provision of information security management systems for the transferred DRAM manufacture technology information and the self-developed DRAM manufacture process technology information, as well as the related information flow include related server room maintenance, network service, and the development, operation and maintenance of information systems.
This is in accordance with the Statement of Application version 1.1.

This certificate is valid from 20 October 2019 until 20 October 2022 and remains valid subject to satisfactory surveillance audits.
Recertification audit due a minimum of 60 days before the expiration date.
Issue 1. Certified since 20 October 2019

Authorised by

SGS United Kingdom Ltd

Page 1 of 1

UKAS MANAGEMENT SYSTEMS 0005

ISO 27001 Statement

Nanya's improvement measures for information security management

The Company has obtained ISO 27001 information security certification that can satisfy customer demandsand attain international information security management standards.

The employment statement signed by the Company's employees upon hiring include the confidentiality obligations for during and after employment.

The Company has established the employee service guidelines and confidentiality requirements in the "Employee Handbook" to provide employees with guidance for their conduct.

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 has established the Information Security Division to take charge of planning, executing, auditing, and improving information security management.

Where the Company discovers a violation of laws by current or resigned employees, such violation shall be prosecuted to the fullest extent of the law. Since the Company's establishment of the Information Security Division in July 2017, there has been no violationsof laws by resigned employees.

In response to the frequent occurrence of domestic and foreign information security attacks, cyber hackers destroy and leak secrets through social engineering, illegal intrusion or ransomware, etc., and the attack methods emerge in an endless stream. It is imperative to continuously develop external hacker protection strategies and in-depth solutions.

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.

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.

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.

Established physical security measures

Access control, system login identity authentication, password control, access right control, and periodic vulnerability scanning.

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.

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.

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.

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.

Information Security Risk Assessment and Drills

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 to ensure the regular operations of the system. The Company has a total of 17 systems that required drills in 2021. 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 Training and Objectives

In terms of information security training, Nanya has invested many resources in hopes of improving information security protection awareness. It also organizes information security month activities each year to consolidate consensus for information security protection. Social engineering exercises are also implemented each quarter. The Company organizes training sessions for information security officers in routine information security meetings and monthly information security meetings. The Company compares the performance of reports from supervisors ranked level 1 or above in quarterly information security meetings. To develop a culture for the management of confidential information, all employees of the head office must complete the online assigned reading courses of the "Company Confidential Information Management Regulations" each year. The completion rate in 2021 was 100%.

Subjects (department and title)	Number of people	Hours	Training completion rate
Social engineering exercises All employees (excluding TA)	27,583	2,299 hours	100%
Social engineering training Employees who clicked on the link	140	70 hours	100%
Monthly information security activities Information Security Month event - online questionnaire with gifts All employees	3,423	1,712 hours	99%
Analysis and identification of common social engineering attack methods (A)(B) All employees	3,442	1,147 hours	100%
Information security seminars Information security relationship between development and operation & maintenance from the perspective of hackers System Management Department,Information Security Section	43	43 hours	100%
Information security seminars New perspective of information security threat management in the IoT era Information security officers, Information Security Section	58	87 hours	100%
Information security seminars Insights and quantification of asset vulnerabilities to eliminate information security risks Information security officers, Information Security Section	42	84 hours	100%
Information security seminars Techniques of several hacker groups – Understanding and information security habits that employees should have Information security officers, Information Security, SectionEmployees who clicked on the social ngineering link	63	126 hours	100%
Total		**5,568 hours**	

Information Security Goals

To implement information security management and strictly review the implementation status, we set quantitative management goals for information security. In 2021, a total of 10 information security goals were set on the aspects of confidentiality, integrity, and availability. Because we use realistic cases for the exercise and some employees, who lack of information security awareness, click links, which lead to " Click rate and attachment opening rate in social engineering exercises " did not achieve the goal. The other 9 items have all achieved the goals.

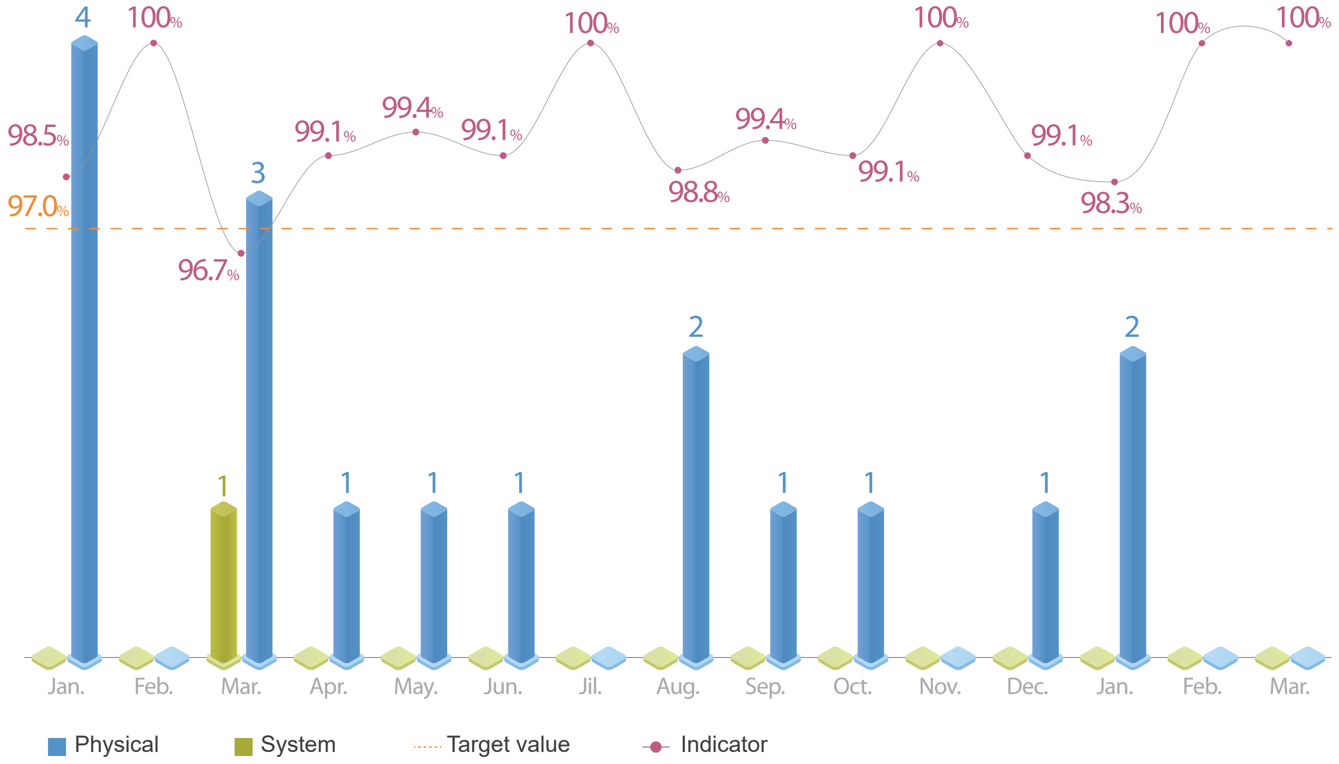
Confidentiality	2021 Goals	Annual average	Description
Information security indicators	≧ 97%	99.1%(Average for the year)	Goal not achieved 1 time in 12 months (2021/03)
Number of unauthorized access or use of technology transfer documents	0 times each year	0	All goals were achieved
Number of times AIP encrypted files being opened successfully without authorization outside of the plants	0 times each year	0	All goals were achieved

Completeness	2021 Goals	Annual average	Description
Click rate and attachment opening rate in social engineering exercises (%)	< 0.5%	1.0%	Goal not achieved, conducted 8 drills Goal not achieved 3 times (Q1 、Q3 、Q4)
OA Client Hot-Fix Deployment completion rate (%)	≧ 99%	99.3%	All goals were achieved
Implementation completion rate of OA active anti-virus protection operations (%)	100%	100%	All goals were achieved
(New) Major cybersecurity incident caused by hackers	0 times each year	0	All goals were achieved (Newly added item)

Availability		2021 Goals	Annual average	Description
OA System Down Time(Year)		< 1 min	0	All goals were achieved
R&D Database Down Time (Year)	Design	≤ 1 time, < 24 hours	0/0	All goals were achieved
	Technology development	≤ 1 time, < 24 hours	0/0	All goals were achieved

Note: Review and improvements are reported during quarterly meetings for items that do not reach the performance goal, and an e-CAR is issued to make improvement according to the PDCA cycle of IS0 27001.

Information security indicator [Note]



Note: The information security indicator is the monthly statistical indicator for information security violations. It is calculated based on the weight of the risks and threats of violations. A higher value indicates a lower number of information security violations or a lower level of information security threats.

Information Security Risk Protection

We understand that we must face information security risks at any time, so the Company's computers all have a SEP (Symantec Endpoint Protection) system, and computers for production machinery in the clean room have Media Access Control Address to prevent them from being targeted by computer viruses. We use Tenable and Nessus vulnerability scanning tools to find major vulnerabilities and risks that online systems, applications, and computers may have. Scanning results and virus prevention reports are provided to system administrators as reference for necessary updates and upgrades. We immediately execute updates for high risk system vulnerabilities, in order to improve system security and stability.

In response to the frequent cyber security attacks in Taiwan and overseas, as well as the endless stream of attack methods used by hackers for sabotage and data leakage, such as social engineering, illegal invasion, or ransomware, we have no time to delay the development of hacking prevention strategies and defense-in-depth plans. We are using AI technology for analysis and CDR (Content Disarm and Reconstruction) to lower the risk of social engineering, and looking into emerging information security issues and cyberattack methods, in order to predict the development and trends in information security threats. We are also looking into information security risks of future information technology applications, so as to take preventive measures in advance.

Results of information security management

	2018	2019	2020	**2021**
Violations of information security or network security incidents (number of cases)	0	0	0	**0**
Data leakage incidents (number of cases)	0	0	0	**0**
Number of information security violations involving customers' personal data	0	0	0	**0**
Number of customers and employees affected by data leakage	0	0	0	**0**
Amount of fines due to information security or network security incidents (NTD)	0	0	0	**0**