Nanya Technology Corporation

Information Security Management Policy and Statement

I、Purpose

In order to implement Nanya Technology's information security policy, establish a rationalized information security management system, effectively carry out and complete related information security activities, and continuously improve and strengthen Nanya Technology's information security services and environment, this Information Security Policy (hereinafter referred to as "the Policy") is hereby formulated.

II、Information Security Policy

Nanya Technology is committed to strengthening information security by complying with all legal and regulatory requirements and working closely with supply chain partners to protect the confidentiality, integrity, and availability of information assets. This ensures the rights and interests of our customers, shareholders, employees, and suppliers, while upholding the company's social responsibility.

Nanya Technology Information Security Management Policy Statement is as follows:

1. To actively promote information security management, Nanya Technology has formulated this Policy in accordance with the "Cyber Security Management Act" and the "Guidelines for Cyber Security Management of Listed and OTC Companies."
2. Nanya Technology has been certified by an independent third-party auditor for the ISO/IEC 27001 international standard. To date, the implementation has been expanded to cover 100% of all facilities. In accordance with the requirements of ISO/IEC 27001, the company also conducts annual internal audits of its IT infrastructure and

| ©2025 Nanya Technology Corporation. All Rights Reserved. | NTC Proprietary

information security management system, underscoring Nanya Technology's strong commitment to information security management.

3. Proactively implements information security–related systems and protective measures, striving for the most advanced information security solutions to establish robust physical security defenses：
   (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.
4. Nanya Technology is committed to ensuring information security and personal data protection throughout their entire lifecycle. In alignment with the principle of "need-to-know", the Company implements robust data classification and access control measures to restrict access exclusively to authorized personnel. Furthermore, sensitive information is protected through encryption mechanisms to mitigate the risk of data leakage or unauthorized disclosure. All employees, including contract staff, interns, and dispatched personnel, share the responsibility and obligation to protect Nanya Technology's information assets obtained or used in the course of their work. They must prevent unauthorized access, alteration, destruction, or improper disclosure of such assets.
5. Actively participates in external cyber threat intelligence sharing, conducts regular cybersecurity incident drills, and participates annually in group-level red team exercises to strengthen defense capabilities. To ensure timely incident response, security events are classified into four levels of severity, with defined reporting procedures. For incidents leading to suspension of core business

| ©2025 Nanya Technology Corporation. All Rights Reserved. | NTC Proprietary

operations, major public announcements will be issued accordingly.

Level	Scope of influence	Incident notification Recipients
Level1	Some information equipment is affected, but business can still continue to operate.	Colleagues from relevant internal units
Level2	Non-core businesses are affected, but the business can still operate sustainably.	Colleagues from relevant internal units
Level3	Some core businesses are affected.	Interested parties & (Market Observation Post System,MOPS) Material Information
Level4	Core business suspended.	(Market Observation Post System,MOPS) Material Information

6. Supply chain security protection extends beyond Nanya Technology to its partners. Equipment must pass security inspections before being put into operation. Vendors and their onsite personnel are required to sign security clauses to prevent malicious actors from exploiting supply chain relationships. Necessary confidentiality and privacy agreements are also signed to ensure comprehensive risk prevention.
7. All employees receive information security education, training, and awareness programs to enhance security consciousness and ensure compliance with relevant laws and regulations.

III、Scope of Application

This Policy applies to all information assets of Nanya Technology (including overseas subsidiaries) and their users. Information users include full-time employees, contract staff, interns, customers with access to Nanya Technology's information, outsourced service providers, suppliers, partners, and visitors.

Nanya Technology information security organization is responsible for planning, promoting, auditing, and continuously improving information

| ©2025 Nanya Technology Corporation. All Rights Reserved. | NTC Proprietary

security at Nanya Technology. Information security is the responsibility and obligation of every employee across the Company, as well as a shared responsibility of the management team.

IV. Implementation and Review

This Policy shall be revised as necessary in response to changes in government regulations, technology, and business developments. It shall also be evaluated annually to ensure the effectiveness of information security practices.

| ©2025 Nanya Technology Corporation. All Rights Reserved. | NTC Proprietary