Introduction and Overview

What is NIS2 ?

NIS2 refers to a directive that establishes a set of cybersecurity risk management measures. It imposes requirements on relevant entities to implement "appropriate and proportionate" security measures to safeguard cybersecurity.

Specifically, the core requirements of NIS2 cover the following key areas:

Information System Risk Management: Entities are required to implement systematic risk management procedures, including formulating risk countermeasures, establishing risk assessment processes, maintaining risk registers, and developing written risk handling plans.

Incident Handling and Reporting: A security incident handling process must be established to confirm, respond to security incidents within strict time limits (submitting a preliminary report within 24 hours and a detailed report within 72 hours), and notify customers and regulatory authorities.

Business Continuity: Ensure that business operations or service delivery can maintain appropriate continuity when security incidents or vulnerabilities occur.

Supply Chain Security: Properly address risks brought by third parties and the impacts of these risks on the security of the entity's own products or services.

Network and Information System Security: Clarify the security conditions that network and information systems must meet, including the application of encryption technologies, the adoption of robust identity authentication mechanisms, and compliance with the principle of least privilege.

Cyber security Training: Conduct regular training for the management body and cyber security personnel of the entity.

Purpose and Scope of the Declaration

The directive applies to both private and public entities, specifically, the directive applies to:Public or private entities of a type as described in Annex I or II to the directive; and Qualify (at least) as a medium-sized enterprise, meaning they have more than 50 employees, annual turnover/balance sheet total exceeding EUR 10 million (important entity);

Qualify as a large organization, having more than 250 employees, annual turnover exceeding EUR 50 million and a balance sheet total exceeding EUR 43 million (essential entity)

In addition, regardless of the size of the public or private entity, NIS2 applies to entities that are trust service providers, TLD - name registries, domain name registration service providers, providers of public communication networks and providers of publicly available electronic communications services.

What's more, the vendors that supply products and services to "essential" and "important" entities are indirectly affected . Those organizations need to ensure the security of their services and products.

Core Security Features of the Product

This declaration aims to clarify the core requirements of the NIS2 Directive, present Tiandy Technologies Co., Ltd.'s product core security features and specific NIS2 compliance measures, and confirm the company's compliance status as a digital service provider under the directive—serving as a reference for internal management, customers, and regulatory authorities. Its scope covers the company's network-connected, information-processing products (with core security features like secure boot and encryption) and key business links (R&D, risk management, incident response, supply chain, business continuity), excluding non-core product parameters and confidential commercial data.

Security Layer	Feature	Description
Hardware Security	Secure Boot	Based on the hardware root of trust, ensuring the device only loads signed and trusted software
	Hardware	Integrates an AES-128/SHA-256

Security Layer	Feature	Description
	Encryption Engine	encryption coprocessor to provide high-performance encryption operations
	Tamper-Resistant Mechanism	Equipped with hardware anti-tampering capability
Firmware Security	Secure Update	Adopts an update mechanism verified by digital signatures
	Vulnerability Management	Commitment to regular security updates and vulnerability fixes (for at least 36 months)
	Permission Management	Implements a security policy based on the separation of different user permissions, restricts access rights for each function, and maintains comprehensive log records
Data Security	Transmission Encryption	Supports TLS 1.2/TLS 1.3 for encrypted data transmission

Security Layer	Feature	Description
	Storage Encryption	Encrypts and stores usernames, passwords, certificate files, and other data involved in various device functions
	Privacy Protection	Camera devices support privacy area masking, and sensitive data is processed locally on the device without being uploaded to the server
Access Security	Identity Authentication	Strict username and password verification mechanism, prohibiting the setting of weak passwords
	Access Control	Fine-grained role-based access control (RBAC)
	Secure Communication	All communications are encrypted by default, and plain text transmission is prohibited. Supports HTTPS and SSHv2

NIS2 Compliance Framework

Core Requirements of NIS2

The NIS2 Directive specifies a series of cybersecurity risk management measures and requires relevant entities to implement these "appropriate and proportionate" security

measures. In accordance with the requirements of the Directive, Tiandy Technologies Co., Ltd. focuses on the following core areas:

1. Information System Risk Management: Implement systematic risk management procedures, including risk countermeasures, risk assessment processes, risk registers, and written risk handling plans.
2. Incident Handling and Reporting: Establish security incident handling procedures to ensure the identification, response to security incidents within strict time limits (preliminary report within 24 hours, detailed report within 72 hours), and notify customers and regulatory authorities.
3. Business Continuity: Ensure the maintenance of appropriate continuity of business operations or service delivery in the event of security incidents or vulnerabilities.
4. Supply Chain Security: Properly address risks posed by third parties and their impacts on the security of the enterprise's own products or services.
5. Network and Information System Security: Clarify the security requirements that network and information systems must meet, including encryption technologies, robust authentication mechanisms, the principle of least privilege, etc.
6. Cybersecurity Training: Conduct regular training for the management body and its cybersecurity personnel.

Compliance Analysis

In accordance with the NIS2 Directive, Tiandy Technologies Co., Ltd. is regarded as a digital service provider and falls within the scope of key entities governed by the Directive. We have conducted a comprehensive assessment of the requirements of the NIS2 Directive and confirm that the company's existing and planned security measures are fully compliant with the provisions of the Directive. The following table details the correspondence between the main requirements of NIS2 and the company's response measures:

NIS2 Requirement	Company's Response Measure	Compliance Status
Risk Management	Establish a comprehensive risk management framework and conduct regular risk assessments	Implemented
Incident Reporting	Implement a 24/7 security monitoring and incident response process to meet the 24-hour reporting requirement	Implemented
Access Control	Conduct security assessments on key suppliers and include security requirements in contracts	Implemented
Encryption Protection	Implement multi-factor authentication and the principle of least privilege	Implemented
Security Training	Encrypt all data transmissions and key static data by default	Implemented
Business Continuity	Conduct annual cybersecurity training for all employees and specialized training for technical personnel	Implemented
Vulnerability Management	Implement regular vulnerability scanning and patching procedures, and establish a vulnerability	Implemented

NIS2 Requirement	Company's Response Measure	Compliance Status
	disclosure policy	

Specific Compliance Measures

Cybersecurity Risk Management

Tiandy Technologies Co., Ltd. has implemented a comprehensive information system risk management program, which is approved and led by the management body. Our risk management approach includes:

1. Risk Countermeasures and Assessment Process: We adopt the risk assessment method specified in the ISO 27005 standard, conduct formal risk assessments on all key systems quarterly, and identify and evaluate potential threats, vulnerabilities, and business impacts. The assessment results are recorded in the risk register, and clear risk handling plans are formulated.
2. Risk Monitoring and Reporting: The company's Cybersecurity Committee reviews high-risk projects and handling progress monthly to ensure timely mitigation of risks. All major risks are reported to the top management, and appropriate resources and attention are allocated.
3. Security and Privacy Protection in Design: We adopt the principles of Security-by-Design and Privacy-by-Design, integrating security considerations into the earliest stages of product development. All new products and functions must undergo threat modeling and security design reviews to ensure that security is not a feature added after the fact but an inherent attribute of the product.

Incident Handling and Reporting

To meet the strict incident reporting requirements of NIS2, we have established a standardized incident response process to ensure the timely identification, assessment, reporting, and response to security incidents:

1. Incident Detection and Classification: We implement a 24/7 security monitoring system, using AI-based anomaly detection and behavioral analysis technologies to identify potential security incidents in real time. Incidents are classified into

four levels based on severity and impact, corresponding to different response processes.

2. Rapid Response Mechanism: A dedicated Computer Incident Response Team (CIRT) has been established, which can initiate the response procedure within 15 minutes of discovering an incident. The team is organized in accordance with the NIST CSF framework and has professional capabilities to handle various types of security incidents.
3. Compliance Reporting Process: We strictly comply with the NIS2 Directive's requirements for preliminary reporting within 24 hours and detailed reporting within 72 hours. For all major incidents, a preliminary report will be submitted to the relevant regulatory authorities within 24 hours of discovery, a detailed technical analysis will be provided within 72 hours, and a final handling plan will be submitted within one month.
4. Customer Notification: Depending on the severity of the incident, we will promptly notify affected customers, providing details of the incident, potential impacts, and recommended response measures. Customers can obtain incident notifications through the customer portal or API integration.

Business Continuity and Recovery

To ensure business continuity in the event of a security incident, we have implemented the following measures:

Backup Management: We have established a comprehensive data backup strategy to encrypt and back up all key business data and configurations. Backups adhere to the 3-2-1 rule (three copies, two media types, one offline storage) and regular tests on backup integrity are conducted.

Disaster Recovery Plan: We have formulated detailed disaster recovery and crisis management plans, which are tested and drilled every six months. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are clearly defined for different systems to ensure rapid service restoration after an interruption incident.

Supply Chain Security

Tiandy Technologies Co., Ltd. attaches great importance to supply chain security and

has implemented a series of measures to ensure effective management of risks associated with third-party products and services:

1. Supplier Security Assessment: We have established a comprehensive supplier security assessment process to conduct security reviews on all key suppliers and service providers. The assessment covers various factors such as security practices, compliance status, incident history, and security certifications.
2. Contractual Security Requirements: All supplier contracts include clear security requirements, including SLAs for vulnerability reporting and remediation, obligations for security incident notification, rights to security audits, and data protection requirements. We require suppliers to comply with security standards equivalent to those of our company.
3. Software Bill of Materials (SBOM): We provide a Software Bill of Materials for all products, transparently disclosing all software components and their sources. This enables us to quickly identify and respond to vulnerability risks in the supply chain.
4. Continuous Monitoring: We conduct continuous monitoring of the security status of key suppliers and re-evaluate their security conditions regularly. Any supplier security incident will trigger a special review, and a supplier replacement process will be initiated if necessary.

Technical Security Measures

Encryption Technology: Strong encryption is enabled by default in all products. Data transmission uses TLS 1.2/TLS 1.3 encryption, static data uses AES-128 encryption, and supports HTTPS and Secure Shell.

Strict Identity Authentication: Based on the RBAC policy, strict password verification is implemented, and functions such as certificate management and import are supported.

Secure Communication: We ensure that all communication channels are fully protected, especially voice, video, and text communications as well as emergency communication systems. All communications are end-to-end encrypted by default to prevent eavesdropping and tampering.

Vulnerability Management: We have established a systematic vulnerability management

program, including regular security testing, vulnerability scanning, and penetration testing. After vulnerabilities are discovered, we handle them according to severity levels, and critical vulnerabilities are addressed within 24 hours.

Secure Update Mechanism: We provide a secure and reliable firmware update mechanism. All updates are digitally signed, and the device verifies the validity of the signature before updating to prevent the installation of malicious firmware.

Hardware Secure Boot: During system startup, signature verification of the firmware is supported, and the device can only start if the verification is passed, strictly preventing malicious tampering of the image.

Current Compliant International Security Standards

Tiandy maintains extremely high standards to protect security and privacy. Tiandy continuously evolves product development process, maintaining a security baseline program to enhance security by design. Tiandy products are certified with CE-RED （EN18031） as well as many others. Tiandy information security system and security management have been audited by independent third-party organizations with certifications including：

• ISO 27001 Information Security Management System

• ISO 27701 Privacy Information Management System

• ISO 29151 Personal Identity Information Protection Management System

• ISO 22301 Business Continuity Management System

• ISO 20000-1 Information Technology Service Management System

Additionally, Tiandy adheres to its core values of openness and constantly seeks cooperation with international authoritative security institutions to jointly build a robust security ecosystem while improving its own security capabilities and solutions.

Tiandy's Commitment

Tiandy places paramount importance on cybersecurity operations and development. While conducting business operations in compliance with relevant laws and regulations, Tiandy has established a comprehensive cybersecurity management system. We adhere to essential industry standards, implement rigorous risk assessments, employ cutting-edge security technologies, establish robust vulnerability management mechanisms,

and conduct security training and audits to safeguard our products and services from unforeseen threats. We consistently integrate cybersecurity considerations as a vital component throughout product development and upgrades. All these endeavours are dedicated to fully supporting our customers in enhancing their cybersecurity defences. Tiandy pledges to adhere to industry best practices and international standards, handling all security incidents in a transparent and efficient manner.

Thank you for choosing and trusting Tiandy.