MAXHUB-NIS2

Overview

As a leading company in the industry, Guangzhou Shirui Electronics Co., Ltd. (“MAXHUB” or “we”) consistently integrates the principle of independent innovation into our long-term development strategy, focusing on future-oriented advancements. With a robust self-developed Research & Development system, MAXHUB specializes in intelligent human-machine interaction applications. Our expertise extends to project research and product development across diverse fields, including touch technology, liquid crystal display driving, board design, system integration, software development, and industrial design. Our products and services encompass artificial intelligence, internet, and smart Internet of Things (IoT) solutions.

As a user-centric company, MAXHUB prioritizes network and information security to ensure the delivery of high quality, secure and reliable products and services. Aligned with the NIS2 Directive's technical and methodological requirements for cybersecurity risk management , we are committed to maintaining compliant service frameworks and operational environments that adhere to NIS2 standards.

NIS2 Directive Introduction

What is the NIS2 Directive

The NIS2 Directive formally identified as “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union” is a legislative act that aims to achieve a high common level of cybersecurity across the European Union. EU Member States authorities were required to transpose NIS2 Directive into national laws by October 17, 2024.

What is needed: 10 NIS2 risk management measures

NIS2 defines 10 cyber security risk management measures that regulated entities must implement. Organizations should implement measures

proportionate to the risk presented by cyber threats. And they should implement additional measures to protect against any hazards that could impact information systems and their physical environment, ranging from actual cyber-attacks to power outages and natural disasters.

1. Risk analysis and information system security policies

   Organizations must develop comprehensive information security policies and implement risk management procedures which provide the foundation for information security framework.

2. Incident handling

   Incident handling includes any actions aimed at preventing, detecting, analyzing, containing, responding to, and recovering from a security incident.

3. Business continuity

   Organizations should take steps to ensure they can continue to operate even in the event of a cyber-attack or natural disaster. Beyond having a data backup strategy in place, requirements and processes for responding to disruptions should be developed to ensure business continuity.

4. Supply chain security

   Supply chain security focuses on managing risks relating to external vendors and suppliers. Organizations should assess the quality, resilience, and cyber security practice of the third-party products and services they use.

5. Security in network and information systems acquisition, development, and maintenance

   Organizations must implement measures to enhance security throughout the full lifecycle of network and information systems, including vulnerability handling and disclosure

6. Assessing the efficacy of risk management measures

   Organizations should continuously monitor and refine implemented risk management measures, such as using key performance indicators (KPIs) and conduct periodic risk assessments to ensure security measures are operating correctly and consistently.

7. Training and basic cyber hygiene

   Organizations should provide regular cybersecurity training to both management and employees, equipping them to identify risks and evaluate risk management practices. Additionally, they must implement fundamental cyber hygiene measures, including Zero Trust principles, software updates, secure configurations, network segmentation, identity management, access controls, and regular data backups.

8. Cryptography and encryption

   Organizations should establish processes for encryption key management in aspect of key generation, distribution, storage, and deletion.

9. Human resources security, access control, and asset management

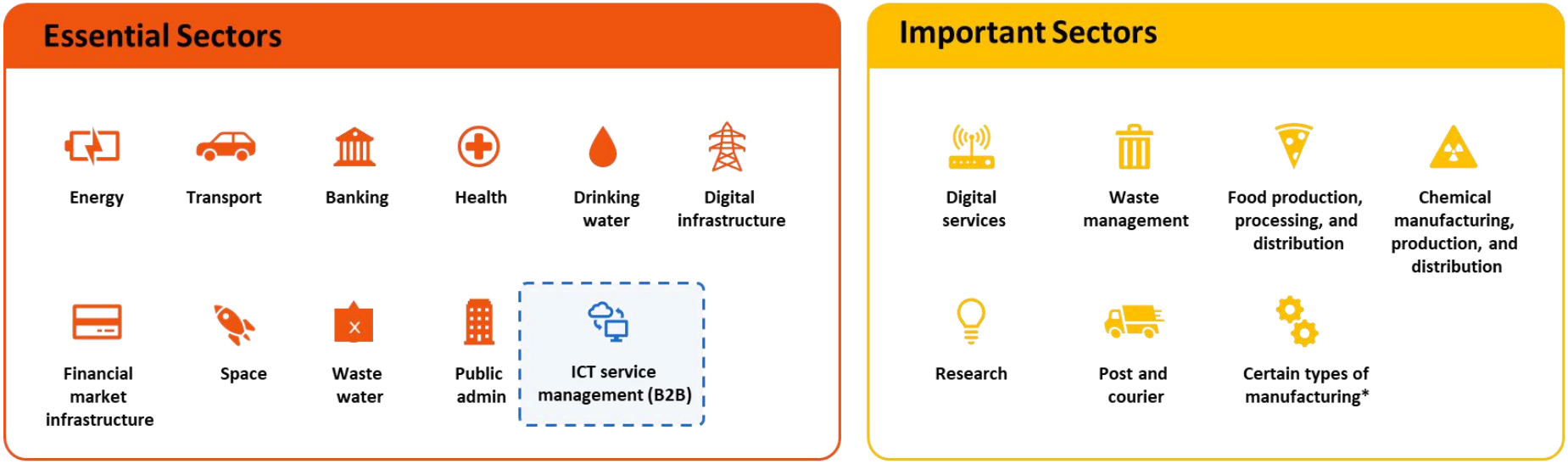
   Human resources security can be understood as protecting sensitive employee data and ensuring that only authorized and vetted personnel have access to an organization's physical sites and information systems.

10. Multi-factor authentication and secure/emergency communications

    Multi-factor authentication (MFA) provides stronger identity verification than passwords alone, using methods such as physical tokens, security questions, or one-time codes. Additionally, organizations must establish secure backup communication channels to maintain contact during incidents or outages if primary channels fail.

Which sectors does NIS2 cover?

With the introduction of NIS2, more organizations, in more industries, will be subject to cyber security requirements. Those requirements should be stronger and enforcement will be stricter than before. NIS2 applies to medium-sized and large entities in below sectors, requiring even more organizations to comply with these requirements. In simplified terms, such organizations can be defined as having more than 50 employees and a turnover of more than €10 million.



**relating to health, electrical equipment, some electronics, machinery, automobiles, and other transport equipment*

How MAXHUB complies with NIS2

The SOC (System and Organization Controls Report) report is an assurance report issued by an accounting firm based on the standards of the American Institute of Certified Public Accountants (AICPA). The purpose is to help service organizations build trust and confidence in the services provided by user entities and related internal control through reports issued by independent auditors. The nature of the assurance report enables the report to be directly relied on by internal and external auditors of user entities for the purpose of performing audit work on the effectiveness of internal control of the enterprise.

The areas of inspection for SOC2 are highly coincident with the requirements for NIS2, covering all of the measures mentioned above. MAXHUB has obtained

SOC 2 attestation report by virtue of its own information security management system and security control measures, and the certification scope includes MAXHUB OS and PIVOT Plus. This assurance also facilitates organizational adherence to the NIS2 Directive compliance framework.

NIS2 Requirements	MAXHUB **Response**
Risk analysis and information system security policies	MAXHUB has established policies governing information security risk management, including risk identification, assessment and mitigation. MAXHUB has also implemented standardized procedure addressing information security governance, asset management, human resources security and compliance. MAXHUB conducts an internal audit of the information security management system annually.Furthermore, MAXHUB engages independent third-party to conduct financial audits,privacy-related audit and information security management system audit.
Incident handling	MAXHUB has established information security incident management policies regarding the classification, handling, and reporting processes for security incidents. Furthermore, MAXHUB has adopted security analytics platform, security incident alert platform and security incident ticket software to ensure that the security incidents can be detected, identified and handled in a timely manner.
Business continuity	MAXHUB has established comprehensive policies and procedures regarding business continuity management, data backup management and cloud resource capacity management. MAXHUB conducts annual business continuity plan assessments and drills, implementing a robust backup strategy with annual data recovery test, and maintaining high-availability cloud configurations supported by real-time monitoring and alerts.

NIS2 Requirements	MAXHUB Response
Supply chain security	MAXHUB has formulated supply chain management policies to define processes and security requirements for supplier onboarding, evaluation, performance assessment, and termination. The Procurement Department conducts an annual performance evaluation of cloud service providers in aspect of cloud product capability, security compliance and service coordination.
Security in network and information systems acquisition, development, and maintenance	MAXHUB has formulated relevant policies for change initiation, development security, testing security and deployment security. To operationalize these policies, MAXHUB implements secure tools including version-controlled management systems and incorporates security testing workflows into change processes. The environmental isolation framework enforces strict logical separation between development, test and production environments.Furthermore, vulnerability scanning and penetration testing are conducted annually to ensure the security of key systems.
Assessing the efficacy of risk management measures	MAXHUB conducts an information security risk assessment annually. The assessment process includes evaluating the value of information assets, identifying vulnerabilities, calculating the risk level of information assets, and developing corresponding risk mitigation plans.
Training and basic cyber hygiene	MAXHUB has established information security management and human resource management policies to standardize conduct for employees in information security. Building upon this framework, MAXHUB conducts annual information awareness training mandated for all personnel.
Cryptography and encryption	MAXHUB has developed robust policies of user password, data classification and data lifecycle management. MAXHUB has adopted encrypted transmission channels and data encryption to ensure the confidentiality and integrity of data during transmission and storage.

NIS2 Requirements	MAXHUB Response
Human resources security, access control, and asset management	MAXHUB ’s human resource management policy has been integrated with the information security management policies. MAXHUB conducts background investigations on prospective employees and they are required to sign Confidentiality Agreement to ensure that employees understand, demonstrate and commit to their security responsibilities. MAXHUB has developed management procedures regarding access provisioning, access de-provisioning and periodic user access review, to ensure secure access control. The procedures of issuance, return and security management of terminal devices have been established to ensure the safeguard of MAXHUB ’s assets. MAXHUB also develops a platform to monitor and manage cloud assets for key systems.
Multi-factor authentication and secure/emergency communications	MAXHUB has implemented strong identity authentication mechanisms such as Muti-Factor Authentication, in its key infrastructure and key support tools. In addition, secure access control strategies has been implemented, including system access and remote access.

MAXHUB 's Compliance Commitment

MAXHUB acknowledges the significant impact of NIS2 Directive and the obligation it places on organizations. MAXHUB is committed to a proactive and strategic approach to cybersecurity, viewing compliance not merely as a regulatory requirement but as a fundamental component of operational resilience and commitment to MAXHUB ’s global users and partners.

Our commitment begins with aligning existing security frameworks, including ISO 27001 - certified processes, SOC2 - audited Internal control system, and

NIS2 - advanced network protection. We are systematically addressing critical areas outlined in the directive, including supply chain resilience, 24/7 incident monitoring, and mandatory reporting of significant cyber incidents. To ensure accountability, we have established cross-functional oversight led by executive leadership and technical experts, embedding NIS2's "systemic risk management" principles into corporate governance.

Acknowledging the dynamic nature of NIS2 implementation across EU member states, we maintain dedicated teams to monitor legislative updates and refine our policies accordingly. Partner collaboration is essential to our strategy: we enforce stringent supplier agreements with enforceable cybersecurity clauses and provide partners with tailored NIS2 compliance guidelines to fortify ecosystem-wide security.

MAXHUB pledges to transparently communicate compliance milestones through annual reports and stakeholder briefings, while embedding "security-by-design" principles into product development. We will continuously invest in employee training, threat intelligence sharing, and technologies such as encryption and vulnerability management to not only meet but exceed NIS2 standards.
Our ultimate goal is to safeguard global users against emerging cyber threats, upholding trust in an interconnected digital world.