UNIVIEW AND NIS 2 White Paper

Cybersecurity White Paper August 2026

Table of Contents

---

1 Introduction

1.1 What is NIS 2?

The NIS 2 (Directive (EU) 2022/2555) is an EU directive that member states were required to transpose into national legislation by October 17, 2024. It aims to achieve a high common level of cybersecurity across the EU, contributing to the security of the region and the effective functioning of its economy and society. NIS 2 requires entities providing essential and important services to build cybersecurity capabilities, mitigate threats to network and information systems, ensure continuity of

services during incidents, and report significant incidents to the competent authorities. Non-compliance can result in heavy fines and personal liability for management.

1.2 Who does NIS 2 affect?

Directly affected

- Essential entities: energy, transport, banking/finance, health, drinking water, waste water, digital infrastructure, public administration, space.
- Important entities: postal services, waste management, chemicals, food, manufacturing, digital providers, research organizations.

Note:Entities potentially subject to NIS 2 include organizations operating in sectors listed in Annex I and Annex II of Directive (EU) 2022/2555. Their classification as essential or important entities depends on the applicable criteria under Article 3, including sector, type of service, and other conditions defined by the Directive and national implementing legislation.

- National competent authorities designated by member states to oversee implementation and enforcement.

Indirectly affected

- Vendors and suppliers — including manufacturers of video surveillance and AIoT products such as Uniview. NIS 2 entities must secure their supply chains, so they will increasingly pass contractual cybersecurity requirements down to their suppliers. Customers subject to NIS 2 may require their suppliers to provide relevant information and evidence regarding the cybersecurity of their products, services, and development processes as part of supplier risk assessment and management activities.
- Users of essential and digital services, who benefit from the improved security and resilience the directive mandates.

2 NIS 2 requirements for essential and important entities

Under Articles 20, 21, and 23 of the NIS 2 Directive, essential and important entities are required to establish cybersecurity governance, implement cybersecurity risk-management measures, and comply with incident reporting obligations. These requirements include:

- **Security measures** based on risk assessment and best practice, covering network and information system security.
- **Incident handling and reporting** — early warning within 24 hours, incident notification within 72 hours, and a final report within one month for significant incidents.
- **Risk management** — identify threats and vulnerabilities and mitigate them.
- **Business continuity** — backup management, disaster recovery, and crisis management.
- **Supply chain security** — including the security of relationships with direct suppliers and service providers.
- **Cooperation with competent authorities**, continuous monitoring, cryptography and encryption policies, access control, and security training.

3 Impact on suppliers

As a global provider of AIoT and video surveillance products whose equipment is deployed within the infrastructure of NIS 2 entities, Uniview supports its customers' compliance by addressing the following supplier-level expectations:

Supplier-security consideration	How Uniview supports customers' supplier cybersecurity assessments
Security by design	Security built into products from the design phase
Regular updates and patching	Timely security updates across the product lifecycle
Authentication and authorization	Strong authentication and proper access control
Data encryption	Encryption of data in transit and at rest
Incident reporting	Transparent vulnerability disclosure and incident response
Privacy	Compliance with GDPR alongside NIS 2
Supply chain security	Ensuring the security of the entire supply chain, from component suppliers to customers

4 The Uniview response

The following describes how Uniview, as a supplier, assists customers subject to NIS 2 in assessing and managing supplier-related cybersecurity risks. The practices below reflect the cybersecurity measures applicable to those products.

Supplier-security consideration	Uniview practice	Section
Security by design	IPD SDL, security testing and validation	4.1
Updates and patch management	Signed firmware, secure upgrade, OTA, security advisories	4.2
Access control and identity management	RBAC, strong authentication, 802.1X, account/password policy	4.3
Data security and encryption	Secure protocols, transit/at-rest encryption, key management	4.4
Incident handling and vulnerability management	CNA status, emergency response team, coordinated disclosure	4.5
Privacy and data protection	GDPR alignment, ISO 27701, in-product privacy protection	4.6
Supply chain security	Secure boot, signed firmware, ISO 28000 controls	4.7
Business continuity and resilience	EZCloud DR/backup, monitoring, emergency drills	4.8
Cybersecurity awareness and training	Mandatory awareness program, role-based training	4.9

4.1 Security by design

Uniview treats security as an integral part of product design and development, not an afterthought:

- **IPD secure development system (SDL)**: Security is integrated into requirements analysis, design, coding, testing, deployment, and maintenance. Security requirement analysis and security/reliability design are mandatory steps in product development and a formal part of product assessment testing.
- **Security testing in development**: Vulnerability scanning, static code security review, black-box scanning, mobile app scanning, and internal plus third-party penetration testing through Uniview's security lab and partner security vendors. Systems may only be released to production after passing security testing.
- **Hardware root of trust**: Products incorporate OTP (one-time programmable) storage for key digests, true random number generators, and TEE (Trusted Execution Environment) for hardware-isolated execution and trusted encrypted storage of keys and certificates.
- **Secure default configuration**: Minimum-open-port principle (non-essential services such as SSH and UPnP disabled by default), mandatory change of default passwords to strong passwords at first login, and restricted secure shell with per-device dynamic authentication keys.

4.2 Regular updates and patches

- **Secure upgrade with signed firmware**: All firmware is digitally signed; devices verify integrity and authenticity before any firmware is written, rejecting illegal or tampered images.
- **Firmware encryption**: Firmware remains encrypted throughout its lifecycle, including distribution and storage, to resist reverse engineering.
- **OTA security**: Devices verify firmware against pre-installed signed integrity information after download; only verified firmware is installed.
- **Security patch delivery**: Security fixes are released through firmware updates, with availability and advisories published in the security column of the Uniview website (https://global.uniview.com/About_Us/Security).

4.3 Authentication and authorization

- **Role-based access control (RBAC)**: A user and permission management model meets access control requirements across scenarios (administrator/operator/viewer-type role separation).
- **Secure identity authentication**: Digest authentication for HTTP, RTSP, and ONVIF; WS-Security (WSSE) UsernameToken authentication for ONVIF — protecting credential confidentiality and preventing replay.
- **Strong password enforcement** at first login and **brute-force protection** through login lockout after repeated failed attempts.
- **Session security**: Automatic session timeout with re-authentication after inactivity.
- **Network access admission**: IEEE 802.1X port-based network access control, plus IP and MAC address filtering, restricting unauthorized devices and hosts.
- **Audit logs**: Standardized logging of all critical operations, with synchronization to syslog servers to prevent loss or malicious deletion.

4.4 Data encryption

- **Secure protocols**: HTTPS, TLS 1.2/1.3, DTLS, WSS, and SNMPv3 with secure cipher suites.
- **Video encryption in transit**: Frame-level or channel encryption protects video streams from interception.

- **Video encryption at rest:** Implements LUKS-based storage encryption with encryption keys derived from user passwords, ensuring that recordings stored on memory cards or hard drives are accessible only to authorized users.
- **Hierarchical key management**: Keys are stored in hardware security zones with a layered architecture (Master Key → Key Encryption Keys → Business Keys), combining security with flexible key management.
- **Encrypted configuration storage and export**: Sensitive configuration data is encrypted both on-device and when exported.
- **Digital watermarking**: Invisible watermarks embedded in video streams allow verification of video integrity and authenticity — important for evidential use.
- **International standard algorithms**: SHA-256, RSA, AES.

4.5 Incident reporting and vulnerability management

NIS 2 entities depend on transparent, responsive suppliers for their own 24h/72h reporting obligations. Uniview provides:

- **CVE Numbering Authority (CNA) status**: Uniview has joined the CVE Program and is an authorized CVE Numbering Authority, able to assign and publish CVE IDs for vulnerabilities in its own products. This reflects an active, self-managed vulnerability disclosure posture aligned with global industry best practice and CNA peers in the industry.
- **Professional vulnerability scanning**: Uniview has procured specialized security scanning software to conduct network and system vulnerability scans, ensuring that discovered issues are mapped to standard CVE identifiers for precise tracking and disclosure.
- **Dedicated security emergency response team**:Security incidents and vulnerabilities are strictly classified by severity, with reporting, response, investigation, and remediation procedures carried out according to the assigned severity level.
- **Public security portal** (https://global.uniview.com/About_Us/Security) containing security notices, the vulnerability response process, a vulnerability reporting channel, Uniview Security Lab, and a unified contact point: **security@uniview.com**.
- **Coordinated vulnerability disclosure**: Uniview accepts vulnerability submissions from external security researchers and white-hat hackers. Reports are rated based on factors such as attack complexity, impact scope, discoverability and exploitability, business criticality, and severity of harm, and are tracked to remediation through issue tickets. Reported vulnerabilities are addressed within the committed response time, with fixes delivered via firmware/software version upgrades.
- **Customer notification**: Quick notification channels respond to vulnerabilities and data-leakage incidents according to severity; investigation reports are provided to affected customers upon request.

4.6 Privacy considerations

- Uniview publishes its **privacy policy** describing what personal data is collected and how it is processed, and reminds users that products may process personal data (faces, license plates, etc.) subject to local law including **GDPR**.

- Uniview's management systems are certified by DNV to **ISO/IEC 27001** (information security), **ISO 27017** (cloud security controls), **ISO 27018** (PII protection in public clouds), and **ISO/IEC 27701** (privacy information management).
- **Privacy protection in products**: Intelligent identification and encryption of face/privacy regions in video — displayed as mosaics to low-privilege or unauthorized users, with originals recoverable only by high-privilege users.
- **EU data residency**: For EZCloud users in EU countries, data is stored in the German data center. The customer retains the role of data controller.In typical customer deployments,Uniview generally acts as a processor under written instructions and contractual agreements. However, the allocation of controller and processor roles must be assessed separately for each processing activity based on the parties' actual roles and responsibilities.
- **Privacy principles**: integrity, consent, clear purpose, restricted collection, minimum necessity, transparency, balanced rights and responsibility, security, and compliance.

4.7 Supply chain security

NIS 2 requires entities to secure their supply chains; Uniview protects product integrity from production through delivery and operation:

- **Secure boot**: Chain-of-trust verification with digital signatures ensures only authorized software and firmware load at startup; tampered images abort the boot process.
- **Signed and encrypted firmware** prevents implantation of unauthorized code during distribution.
- **OTP-anchored trust**: Key digests written once to one-time programmable storage cannot be modified, anchoring device integrity in hardware.
- **Application code signing** based on PKI binds binaries to the publisher's identity, preventing tampering and forgery of client software.
- **ISO 28000 supply chain security management**: Uniview operates supply chain security controls covering supplier evaluation, third-party component management, and ongoing monitoring of cybersecurity risks, improving transparency and reducing supply chain exposure.
- **Cloud infrastructure partners**: EZCloud builds on globally audited cloud providers (AWS, Alibaba Cloud, Tencent Cloud) for physical and infrastructure security, while all service deployment and O&M are performed independently by the EZCloud team.
- **Export compliance**: Uniview complies with applicable export control laws and regulations worldwide.

4.8 Service security and business continuity

NIS 2 explicitly requires business continuity and backup management.

Uniview maintains measures intended to support service continuity, system resilience, and recovery in the event of security incidents or operational disruptions. These measures include backup, recovery, and related resilience practices designed to support the reliability of products and related operations.

For customers using Uniview's EZCloud platform:

- **Resilience**: multi-copy redundant distributed storage, remote synchronous hot-standby databases with automatic failover, remote asynchronous backups, residual data erasure (zeroing, degaussing, physical destruction) on decommissioned media.
- **Business continuity management**: real-time monitoring of all hosts, applications, services, and networks; documented emergency plans; and regular large-scale emergency drills for hardware failure and security incident scenarios.
- **Operational security**: unified account management, least privilege and segregation of duties, bastion-host-only production access with full operation recording and centralized audit logging, and 24/7 customer security support.

4.9 Training and guidance

- **Internal security awareness**: The Uniview Employee Information Security Manual underpins regular all-staff training; security and audit teams conduct quarterly training on privacy compliance, data protection, and security compliance systems, plus secure-development training for engineers.
- **Personnel security**: Background and qualification vetting aligned with business requirements, and rigorous resource-recovery processes on employee departure.
- **Customer enablement**:Global tech support center; the security team offers consultation on security solutions, and security configuration guidance is published via the security portal.

5 Security certifications

Scope	Certification
Product cybersecurity	**ETSI EN 303 645** (consumer IoT baseline security)
EU Radio Equipment Directive	**EN 18031** (general cybersecurity requirements for radio equipment)
IoT security rating	**UL MCV 1376 — GOLD level**
Development process	**CMMI Level 5**
Information security management	**ISO/IEC 27001**
Cloud service security	**ISO/IEC 27017**, **ISO/IEC 27018**
Privacy management	**ISO/IEC 27701**
IT service management	**ISO/IEC 20000-1**
Supply chain security management	**ISO 28000**
Vulnerability disclosure	**CVE Numbering Authority (CNA)**

These certifications, audited by independent third parties (UL, DNV, etc.), provide NIS 2 entities with verifiable evidence for their supplier risk assessments. Collectively, the ISO/IEC 27001/27017/27018/27701, ISO/IEC 20000-1, and ISO 28000 certifications support Uniview's risk management and governance, information security and data protection, cloud security and privacy, and supply chain security — directly underpinning alignment with the key requirements of NIS 2.

6 Summary

Network security is a systematic undertaking — no single node can secure an entire system. Uniview has established a product security framework spanning physical hardware security, system security,

application security, data security, and network security, embedded security throughout its IPD development lifecycle, and built transparent vulnerability response and incident management mechanisms. Uniview provides relevant supporting information for customers subject to NIS 2 in their risk assessments. Uniview will continue to cooperate with customers, security vendors, standards organizations, and researchers to jointly safeguard industry information security.

Legal Notice and Disclaimer

This White Paper is provided for general informational purposes only. It does not constitute legal advice, a contractual commitment, warranty, or certification that Uniview, any product or service, or any customer deployment complies with NIS 2 or other applicable laws.

The availability of the features and measures described may vary depending on the relevant product, model, software or firmware version, configuration, region and support arrangement. Any certifications, assessments or industry credentials apply only within their stated scopes. Customers remain responsible for conducting their own legal, technical and risk assessments.

To the maximum extent permitted by applicable law, Uniview may update or correct this White Paper without prior notice. In the event of any inconsistency, applicable law and executed agreements shall prevail.

Contact: security@uniview.com https://global.uniview.com/About_Us/Security