VENDOR CYBERSECURITY DECLARATION
Support for NIS2 Cybersecurity Compliance

Vendor Declaration
Regarding Cybersecurity Capabilities of Video Surveillance and Security Products
In support of organizations subject to Directive (EU) 2022/2555 (NIS2)

Issued by:
COMELIT GROUP S.p.A.
Via Don Arrigoni 5
24020 Rovetta S. Lorenzo (BG), Italy

Reference: Cybersecurity Declaration – NIS2 Support

1. Purpose of this Declaration

This declaration is issued to provide information regarding the cybersecurity capabilities of Comelit products and solutions intended for use in networked security environments, including organizations subject to cybersecurity obligations under Directive (EU) 2022/2555 (NIS2) and related national implementing legislation.

This document is intended to support customers, integrators, operators, and contracting authorities in assessing the suitability of Comelit solutions within cybersecurity-governed environments.

This declaration does not constitute a regulatory certification of NIS2 compliance, as NIS2 establishes obligations for organizations rather than product certification schemes.

2. Organizational Context

COMELIT GROUP S.p.A. has been identified as an Important Entity under the national implementation of Directive (EU) 2022/2555 in Italy, within the applicable industrial sectors.

As an organization operating within the NIS2 regulatory framework, Comelit recognizes the importance of cybersecurity governance, operational resilience, and supply chain security.

3. Scope of Products Covered

This declaration applies, where technically supported by the relevant product models, to Comelit solutions including:

- IP video surveillance cameras
- Network Video Recorders (NVR)
- Digital Video Recorders (DVR)
- Video Management Systems (VMS)
- Remote management platforms
- Cloud-connected security services
- Video intercom systems with IP/network connectivity
- Mobile access applications related to supported platforms

Specific feature availability may vary by product family, firmware version, software release, and deployment architecture.

4. Cybersecurity Design Principles

Comelit products are developed and maintained with consideration for cybersecurity principles relevant to network-connected environments, including:

- controlled access management
- secure authentication mechanisms
- encrypted communications where supported
- firmware lifecycle management
- vulnerability remediation processes
- event traceability capabilities
- secure remote management mechanisms

- resilience and recoverability considerations
- product lifecycle governance

5. Product Cybersecurity Capabilities

Depending on model and platform applicability, Comelit solutions may support cybersecurity capabilities such as:

Access Security

- individual user account management
- role-based access control
- password policy enforcement
- privileged access restriction
- session management controls

Secure Communications

- HTTPS support
- TLS encrypted communication
- certificate-based trust mechanisms
- secure API communication

Infrastructure Security

- support for controlled network deployment
- integration into segmented enterprise architectures
- secure remote administration mechanisms

Monitoring and Auditability

- event logging
- audit traceability
- security event visibility
- administrative action tracking

Operational Security

- firmware management
- controlled software update procedures
- lifecycle management
- security maintenance support

6. Vulnerability Management Commitment

Comelit maintains cybersecurity governance processes intended to support responsible vulnerability management.

These processes may include:

- security issue assessment
- remediation analysis
- corrective firmware/software release processes
- security advisory communications
- vulnerability handling procedures

Customers remain responsible for timely implementation of applicable updates and operational cybersecurity controls.

7. Lifecycle Management

Comelit recognizes the importance of product lifecycle governance in cybersecurity-sensitive environments.

Lifecycle management practices may include:

- software maintenance planning
- firmware support periods
- product transition planning
- end-of-life communication
- support policy management

Customers should ensure lifecycle planning aligns with their internal cybersecurity governance requirements.

8. Secure Deployment Responsibility

Cybersecurity effectiveness depends on secure deployment, integration, and operational governance.

Appropriate implementation practices include:

- controlled access configuration
- secure credential management
- secure remote access controls
- controlled maintenance access
- patch management governance
- backup and recovery procedures
- event monitoring integration
- incident response alignment

9. Integrator Responsibilities

Where solutions are deployed by third-party integrators or service providers, cybersecurity outcomes depend on proper implementation and operational management.

Integrators should apply:

- documented commissioning procedures
- secure configuration practices
- access governance
- maintenance controls
- cybersecurity operational procedures

10. Customer Governance Responsibilities

Directive (EU) 2022/2555 establishes obligations at the organizational level.

Accordingly, compliance remains dependent on:

- organizational risk management
- cybersecurity governance
- incident response capability
- access management
- supplier oversight
- infrastructure security controls
- operational monitoring
- regulatory reporting processes

No standalone product can independently establish organizational NIS2 compliance.

11. Declaration Statement

COMELIT GROUP S.p.A. declares that its relevant network-connected security solutions are designed to support deployment within cybersecurity-managed environments and provide technical capabilities that may assist organizations in implementing cybersecurity controls relevant to NIS2 obligations.

12. Authorized Signature

For and on behalf of:

COMELIT GROUP S.p.A.