Ropo

NIS2 Compliance Policy

Cyber resilience, governance and supplier security requirements

June 2026

Ropo

1. Purpose and scope

Ropo is committed to strengthening cyber resilience in line with the EU's NIS2 Directive and to protecting the confidentiality, integrity and availability of information across its operations and supply chain.
This policy explains how NIS2-aligned practices are interpreted and applied within Ropo's management system. It is intended to provide customers, regulators, partners and employees with a consistent and demonstrable view of the safeguards applied across services, systems and supplier arrangements.
The policy applies to all entities and functions that support the delivery of services, including information systems, operational processes and third parties whose performance could affect service continuity, information security or data protection outcomes.

2. Applicability and minimum standard

Where national transpositions of NIS2 apply directly to an entity, those provisions are mandatory. Where formal statutory applicability differs by entity or jurisdiction, the principles in this policy constitute the minimum internal standard.
The purpose is to ensure that cyber resilience expectations are embedded into day-to-day work, governance, supplier management and operational decision-making. This supports business continuity, improves incident readiness and provides clear accountability for controls and evidence.

3. Governance and accountability

3.1 Management oversight

Top management retains overall accountability for NIS2-aligned governance. Management is responsible for ensuring appropriate resources, reviewing performance and driving continuous improvement.
The CIO and Security Council coordinate direction, approve policies and review the effectiveness of security and resilience measures. Security, Compliance, Legal, business owners and IT operations each maintain responsibilities that support implementation and evidence.

3.2 Risk-based control model

NIS2 is operated from a risk-based point of view and through expected controls. Cyber risks that could affect services are identified, evaluated and treated through the formal risk management process.
Risk results are recorded, owners are assigned and treatment measures are tracked to completion. The control model is reassessed when material changes occur, including system changes, service expansions, supplier changes, location changes, sub-processor changes or new regulatory guidance.

4. Security and resilience controls

4.1 Technical and organisational measures

Technical and organisational measures are applied according to risk, service criticality and regulatory expectations. These measures support confidentiality, integrity, availability and continuity of services.

- Access management, including multi-factor authentication where appropriate.
- Network, endpoint and system hardening.
- Vulnerability management and patch management.
- Logging, monitoring and security event handling.
- Encryption and protection of sensitive information.
- Secure development practices where applicable.
- Tested continuity and recovery arrangements.

4.2 Incident management

Incidents are managed through an established process covering classification, escalation, containment, investigation and lessons learned. The process supports timely stakeholder communications and, where legally required, notification to competent authorities.
Findings from incidents, tests and audits are converted into actions. Actions are prioritised by risk and tracked until completion.

5. Supplier and cloud controls

Suppliers and cloud service providers must meet expectations equivalent to Ropo's internal security and privacy requirements. This may be demonstrated through recognised certifications or by completing Ropo's assessment process.
Supplier agreements must include appropriate provisions for audit rights, security and privacy obligations, incident notification, data ownership and erasure, service continuity and change control for locations and sub-processors.
Supplier risks are reviewed when onboarding, when material changes occur and when incidents or audit findings indicate that reassessment is required.

6. Roles and responsibilities

Roles and responsibilities must be clear enough to support governance, implementation and auditability.

- Top management retains overall accountability.
- The CIO and Security Council coordinate direction, approve policies and review performance.
- Security and Compliance advise on controls, run assessments and audits, operate the incident process and track remediation.
- Legal confirms statutory applicability and reporting obligations and ensures that contracts reflect required terms.
- Business owners and IT operations classify systems, apply controls, keep records current and ensure suppliers perform as agreed.

7. Review and continuous improvement

This policy is reviewed at least annually to confirm continued suitability and effectiveness. The CIO initiates the review and the Security Council approves updates.
Interim updates are made when there are material changes to regulations, business operations, systems, supplier arrangements or threats. The current version is published in the Compliance Portal.
By integrating NIS2 practices into governance, operations and supplier management, Ropo improves resilience, reduces risk and strengthens trust without disrupting the efficiency of its services.