Ropo

Supplier Management Policy

Information Security, Privacy and Supplier Governance

26 June 2026
Kuopio, Finland

1. Scope and Applicability

This policy applies to all suppliers and service providers engaged by Ropo. It covers technology vendors, cloud service providers, professional services firms, and any third parties that process company or customer data, connect to Ropo environments, influence production systems, or support business-critical processes.

The requirements apply regardless of supplier location, contract value, or engagement model. Control depth may vary based on the service criticality, type of data processed, system access, and operational dependency created by the supplier relationship.

All suppliers must implement effective data protection measures. They are required to process personal data lawfully, support data subject rights, maintain records of processing where necessary, and operate documented processes for breach notification, data deletion, and data return upon request.

If sub-processors are used, suppliers must maintain an up-to-date inventory, ensure appropriate contractual controls are in place, and obtain Ropo's approval before making changes that affect personal data processing. Regular privacy and security verification of sub-processors is also expected.

1.1 Supplier Security Requirements

Operational security is a fundamental requirement for all suppliers. Suppliers must enforce robust identity and access management, including multi-factor authentication where appropriate, and define clear controls for privileged access.

Networks should be protected through layered controls, and all traffic must be encrypted. Asset management practices must include up-to-date inventories, vulnerability and patch management, and hardened configurations for servers and endpoints.

Suppliers are required to log relevant events, including administrative actions, and retain these logs for an agreed period. An incident response process must be in place, with defined classification, escalation, and communication steps.

Suppliers should be prepared to coordinate with Ropo on investigation and remediation activities when an incident, material vulnerability, or security event affects Ropo data, services, or environments.

1.2 Secure Development and Change Management

Suppliers that develop or deliver software are expected to follow secure development practices. This includes, but is not limited to, code reviews, automated security testing, management of third-party components, and the use of quality gates to prevent insecure changes from reaching production.

Development, testing, and production environments must be separated and controlled. Release processes should be documented, repeatable, and subject to appropriate approval before deployment to production environments.

2. Supplier Lifecycle Management

Supplier management at Ropo follows a defined lifecycle. The requesting business unit begins by describing the purpose of the engagement, the information and systems involved, and the criticality of the service.
This analysis establishes the required control depth, fallback arrangements, and contractual safeguards. Evidence is then collected either through certifications or completion of Ropo's supplier questionnaire. Submissions are evaluated against minimum acceptance criteria and recognized standards. Any risks identified during due diligence must be addressed before contract signature through remediation, compensating controls, or documented exceptions that are time-bound and approved at the appropriate level.
Contracting embeds the necessary clauses, particularly for cloud services. These clauses include audit rights, data protection obligations, security control expectations, incident notification timelines, continuity commitments, data ownership, and post-termination data return and erasure.

2.1 Ongoing Monitoring

Throughout the cooperation, Ropo monitors the supplier's security posture and service performance. Certificates and evidence are reviewed at least annually or whenever there is a material change. Incidents, material outages, and changes to processing locations or sub-processors must be reported promptly and handled through established processes. Upon termination, data is returned and securely erased, and access is removed without delay.

3. Roles and Responsibilities

The requesting business unit is responsible for defining requirements, classifying criticality, and governing user access for the services it consumes. Security and Compliance lead the evaluation of questionnaires, advise on risk treatments, and track remediation activities.
Legal is responsible for validating legal bases for processing, data transfer mechanisms, and the inclusion of appropriate contractual clauses. Procurement ensures that policy requirements are embedded in sourcing activities and contract templates and supports enforcement throughout the supplier lifecycle.

4. Review and Maintenance

This policy is reviewed at least annually to ensure continued suitability, adequacy, and effectiveness. The Chief Information Officer is responsible for initiating the review, and the Security Council approves updates.
Interim updates may be made when there are material changes to regulations, business operations, technology platforms, or threat conditions. The latest approved version is made available through Ropo's Compliance Portal.

5. Policy Outcome

By applying uniform, evidence-driven requirements to the supplier ecosystem and enforcing them throughout a defined lifecycle, Ropo protects its customers and its brand while enabling the business to adopt external solutions with confidence.
This policy establishes supplier due diligence as an ongoing, measurable discipline and provides a foundation for continuous improvement across Ropo and its partners.