<table>
<tr><td colspan="4"></td><td colspan="8">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="4">Document number:
P26</td><td colspan="8">Document Title:
<b>Third-Party and Supplier Security Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:
01.01.2025</td><td colspan="8">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

Revision history

Revision number	Revision Date	Changes	Reviewed by	Process owner

Approvals

Name	Title	Date	Signature

Aligned with standards and regulations where applicable

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8.1	
ISO/IEC 27002:2022	Controls 5.19–5.22	
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	
EU GDPR	Articles 28, 32, 33	
EU NIS2	Article 21(2)(e–f)	
EU DORA	Articles 28, 30	
COBIT 2019	BAI05, DSS02, MEA03	

Legal Notice (Copyright & Usage Restrictions)

<table>
<tr><td colspan="5"></td><td colspan="7">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P26</td><td colspan="7">Document Title:
<b>Third-Party and Supplier Security Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="3">Effective Date:
01.01.2025</td><td colspan="7">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

1. **Purpose**
   1.1. This policy defines the information security requirements for establishing, managing, and maintaining secure relationships with third-party suppliers and service providers.
   1.2. It ensures that all suppliers with access to the organization’s data, systems, or infrastructure are subject to rigorous security controls, contractual safeguards, and continuous oversight throughout the service lifecycle.
   1.3. The policy supports ISO/IEC 27001 Annex A Controls 5.19 to 5.22 by embedding security requirements into procurement, onboarding, due diligence, contract management, service monitoring, and termination processes.
2. **Scope**
   2.1. This policy applies to:
      2.1.1. All third-party suppliers, contractors, cloud providers, and service organizations processing or accessing organizational information assets
      2.1.2. All internal roles involved in supplier evaluation, onboarding, contracting, risk management, monitoring, or termination
      2.1.3. All supplier relationships that include access to sensitive data, integration with production services, or support for critical business functions
   2.2. It covers both direct suppliers and their subcontractors where applicable, and includes third-party software, infrastructure, support, and managed services.
3. **Objectives**
   3.1. Ensure that supplier security risks are consistently identified, assessed, and mitigated throughout the relationship lifecycle.
   3.2. Embed standardized security requirements into all supplier contracts, including breach notification obligations, right-to-audit clauses, and data protection responsibilities.
   3.3. Require formal due diligence and documented risk assessments before engaging new suppliers or renewing high-risk service agreements.
   3.4. Establish mechanisms for continuous monitoring of supplier compliance, including performance reviews, audits, and incident escalation.
   3.5. Manage changes to supplier services and enforce secure offboarding and data return/destruction during termination.
   3.6. Align third-party security controls with applicable regulatory and contractual obligations, including GDPR, NIS2, DORA, and ISO/IEC 27001 standards.
4. **Roles and Responsibilities**
   4.1. **Chief Information Security Officer (CISO)**
      4.1.1. Owns this policy and ensures its alignment with the overall ISMS, risk management, and compliance strategy.
      4.1.2. Approves supplier classification tiers, security review outcomes, and high-risk exceptions.
      4.1.3. Participates in serious supplier incident escalation and contract negotiations for critical services.
   4.2. **Procurement and Vendor Management**

4.2.1. Ensures all new and renewed supplier contracts incorporate approved security and data protection clauses.

4.2.2. Maintains the centralized supplier register and coordinates with Legal and Compliance on third-party risk documentation.

[….]

11. Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 8.1 – Operational Planning and Control: Requires formal controls over third-party services impacting the ISMS.

ISO/IEC 27002:2022 – Controls 5.19 to 5.22

Annex A Control 5.19 – Policies and Procedures for Supplier Relationships: Mandates controls for managing supplier interactions.

Annex A Control 5.20 – Managing Supplier Risk: Focuses on identification, assessment, and ongoing oversight of supplier security posture.

Annex A Control 5.21 – Supplier Service Delivery Management: Requires performance and security alignment with contractual expectations.

Annex A Control 5.22 – Monitoring and Review of Suppliers: Reinforces the need for ongoing validation and reassessment of third-party compliance.

NIST SP 800-53 Rev.5

SA-9 – External System Services: Defines security and risk requirements for systems operated by external entities.

SA-10 – Developer Configuration Management: Applies when third parties deliver software or environments.

CA-3 – System Interconnections: Requires oversight and agreement on system data flows between entities.

PS-7 – Third-Party Personnel Security: Ensures contractors and vendor staff are screened and monitored appropriately.

EU GDPR (2016/679)

Article 28 – Processor Obligations: Requires written agreements with data processors including technical and organizational measures.

Article 32 – Security of Processing: Mandates appropriate safeguards by both controllers and processors.

Article 33 – Notification of a Personal Data Breach: Requires prompt notification from suppliers in case of breach.

EU NIS2 Directive (2022/2555)

Article 21(2)(e–f): Requires risk-based supplier management and security oversight, particularly in essential and important entities' digital supply chains.

EU DORA (2022/2554)

Article 28 – ICT Third-Party Risk: Imposes obligations for risk assessment, contractual security terms, and exit strategies for financial services providers.

Article 30 – Oversight of Critical ICT Third-Party Providers: Establishes enhanced monitoring and supervisory expectations for key vendors.

COBIT 2019

BAI05 – Manage Organizational Change Enablement: Ensures supplier transitions are governed securely.

DSS02 – Manage Service Requests and Incidents: Applies to supplier-reported issues and incident handling integration.

MEA03 – Monitor, Evaluate and Assess Compliance: Reinforces supplier performance measurement and compliance monitoring.