					Insert Registered Legal Entity Name Here							
Document number: P26					Document Title: **Third party and supplier security policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	Operational Planning and Control: Requires formal controls over third-party services impacting the ISMS
ISO/IEC 27002:2022	Controls 5.19–5.22	Policies and Procedures for Supplier Relationships; Managing Supplier Risk; Supplier Service Delivery Management; Monitoring and Review of Suppliers
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	External System Services; Developer Configuration Management; System Interconnections; Third-Party Personnel Security
EU GDPR	Articles 28, 32, 33	Processor Obligations, Security of Processing, Notification of a Personal Data Breach
EU NIS2	Article 21(2)(e–f)	Risk-based supplier management and security oversight
EU DORA	Articles 28, 30	ICT Third-Party Risk, Oversight of Critical ICT Third-Party Providers
COBIT 2019	BAI05, DSS02, MEA03	Manage Organizational Change Enablement; Manage Service Requests and Incidents; Monitor, Evaluate and Assess Compliance

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 robust security controls, contractual safeguards, and ongoing oversight throughout the service lifecycle.

1.3 This 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 that process or access 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 involving access to sensitive data, integration with production services, or support for critical business functions

2.2 It covers both direct suppliers and, where applicable, their subcontractors, and includes third-party software, infrastructure, support, and managed services.

3. Objectives

3.1 Ensure that supplier security risks are consistently identified, assessed, and treated throughout the relationship lifecycle.

3.2 Embed standardized security requirements into all supplier contracts, including breach notification obligations, audit rights, 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 ongoing 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 or destruction upon termination.

3.6 Align third-party security controls with applicable regulatory and contractual obligations, including GDPR, NIS2, DORA, and ISO/IEC 27001.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns this policy and ensures alignment with the overall ISMS, risk management framework, and compliance strategy.

4.1.2 Approves supplier classification tiers, security review outcomes, and high-risk exceptions.

4.1.3 Participates in the escalation of serious supplier incidents and in contract negotiations for critical services.

4.2 Procurement and Vendor Management

4.2.1 Ensures that 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.

4.2.3 Initiates onboarding processes and ensures alignment with pre-contract security assessments.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 This policy shall be reviewed at least annually, or earlier in the event of:

9.1.1 Material changes to procurement strategy or the supplier ecosystem

9.1.2 Updates to legal or regulatory frameworks (e.g., DORA, GDPR)

9.1.3 Major third-party incidents, data breaches, or audit failures

9.1.4 Findings from risk assessments or external certification bodies

9.2 The review process is jointly owned by the CISO, Procurement, Legal, and Risk Management functions.

9.3 All policy revisions must be documented in the ISMS Document Control Register, version controlled, and communicated to relevant stakeholders through supplier governance channels and employee awareness programmes.

9.4 Superseded versions must be archived for a minimum of three years for traceability and legal compliance purposes.

10. Related Policies and Linkages

10.1 P1 – Information Security Policy. Establishes the overarching commitment to securing all organizational operations, including those dependent on third-party suppliers and external service providers.

10.2 P6 – Risk Management Policy. Governs the identification, assessment, and treatment of risks associated with third-party relationships, including inherited or systemic risks arising from supplier ecosystems.

10.3 P17 – Data Protection and Privacy Policy. Applies to all suppliers that handle personal data and requires appropriate contractual terms, transfer safeguards, and privacy-by-design principles.

10.4 P4 – Access Control Policy. Governs how third-party personnel obtain access to organizational systems, enforcing role-based permissions, session control, and access revocation procedures.

10.5 P22 – Logging and Monitoring Policy. Requires supplier access to systems to be monitored, logged, and reviewed, particularly in environments where privileged or data-centric activities take place.

10.6 P30 – Incident Response Policy. Defines escalation procedures and breach reporting requirements for supplier-originated security events or joint investigations involving third-party systems.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001: Clause 8.1 – Operational Planning and Control: Requires formal controls over third-party services impacting the ISMS.

11.2 ISO/IEC 27002:2022 – Controls 5.19 to 5.22:

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

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

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

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

11.3 NIST SP 800-53 Rev.5:

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

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

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

11.3.4 PS-7 – Third-Party Personnel Security: Ensures that contractors and supplier personnel are screened and monitored appropriately.

11.4 EU GDPR (2016/679):

11.4.1 Article 28 – Processor Obligations: Requires written agreements with data processors, including technical and organizational measures (TOMs).

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

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

11.5 EU NIS2 Directive (2022/2555):

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

11.6 EU DORA (2022/2554):

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

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

11.7 COBIT 2019:

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

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

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