					Insert Registered Legal Entity Name Here							
Document number: P26S					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 controls for third-party and supplier relationships
ISO/IEC 27002:2022	Controls 5.19–5.22	Supplier security controls, contractual security terms, change management, monitoring, and review
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Acquisition, configuration, interconnection agreements, and controls for external personnel
EU GDPR	Articles 28, 32	Data processing agreements, processor security requirements
EU NIS2	Articles 21(2)(a)(b)(i), 23(1)	Supply chain risk management, oversight of third-party services
EU DORA	Articles 5(1)(2), 28(1)(2)	ICT risk management for third-party service providers
COBIT 2019	APO10, APO12, DSS05	Supplier management and risk integration

1. Purpose

1.1 This policy establishes the mandatory security requirements for engaging, managing, and terminating relationships with third parties and suppliers that access or influence the organization's data, systems, or services.

1.2 It ensures that external providers—including IT support providers, cloud service providers, software developers, and business process contractors—handle company assets securely and in compliance with applicable laws and standards.

1.3 This policy reduces risks such as data leakage, unauthorized system changes, regulatory fines, and business interruptions caused by insecure or poorly governed third-party arrangements.

2. Scope

2.1 This policy applies to all third parties that:

2.1.1 Provide software, IT infrastructure, hosting, or cloud services

2.1.2 Access or manage internal systems, devices, or applications

2.1.3 Handle company data, documents, or backups

2.1.4 Support business operations, Human Resources (HR), finance, or customer services

2.2 It also applies to:

2.2.1 Internal staff involved in selecting, engaging, or supervising suppliers

2.2.2 Any personnel responsible for supplier onboarding, contracts, access, or reviews

2.2.3 Any system or process that relies on third-party components or services

3. Objectives

3.1 Ensure that all suppliers meet clearly defined security expectations.

3.2 Require supplier contracts to include enforceable security, data privacy, and incident reporting and management obligations.

3.3 Assess and document supplier risks before agreements are signed or access is granted.

3.4 Conduct regular reviews of high-risk or critical suppliers to confirm compliance.

3.5 Establish a formal process for exceptions, incident reporting and management, and contract updates.

3.6 Support compliance with ISO/IEC 27001:2022, GDPR, NIS2, and DORA obligations related to supplier governance.

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Has overall accountability for supplier selection and security compliance

4.1.2 Approves contracts, exceptions, and escalations involving suppliers

4.1.3 Oversees incident response and decision-making when suppliers fail to meet their obligations

4.2 External IT Provider or internal security contact

4.2.1 Evaluates technical access requested by suppliers

4.2.2 Implements access control rules, reviews logs, and verifies secure data handling

4.2.3 Reviews evidence of security controls, certifications, or audit results, where applicable

[... 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 must be reviewed at least annually by the General Manager, with participation from the External IT Provider or supplier manager.

9.2 The policy must also be reviewed:

9.2.1 After any significant change in legal, regulatory, or contractual obligations

9.2.2 Following a supplier-related security incident or audit finding

9.2.3 When introducing new supplier categories (e.g., critical SaaS platforms)

9.3 All updates must be:

9.3.1 Documented with version history and rationale

9.3.2 Approved by the General Manager

9.3.3 Communicated to relevant internal staff and supplier managers

9.3.4 Retained with previous versions in accordance with the P14S – Data Retention Policy and Disposal Policy

10. Related Policies and Linkages

10.1 The effectiveness of this policy depends on coordination with the following SME Information Security policies:

10.1.1 P2S – Governance Roles and Responsibilities Policy: Assigns accountability for supplier oversight and contract enforcement.

10.1.2 P4S – Access Control Policy: Provides the access restriction rules that must be applied when suppliers are granted system access.

10.1.3 P17S – Data Protection and Privacy Policy: Ensures that suppliers handling personal data comply with data protection principles and legal requirements.

10.1.4 P14S – Data Retention Policy and Disposal Policy: Applies to any data or records shared with or stored by suppliers and governs secure deletion following contract termination.

10.1.5 P30S – Incident Response Policy: Defines how to respond when a supplier causes or is involved in a security incident, including escalation and evidence-handling procedures.

10.2 These policies work together to ensure that supplier risk is controlled throughout the contract lifecycle.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Requires implementation of operational controls, including those applicable to third-party and supplier relationships.

11.2 ISO/IEC 27002

11.2.1 Control 5.19 – Ensures supplier security measures are aligned with organizational requirements.

11.2.2 Control 5.20 – Requires formal agreements covering security terms, responsibilities, and breach obligations.

11.2.3 Control 5.21 – Addresses changes in supplier services that may affect the security posture.

11.2.4 Control 5.22 – Requires monitoring and review of supplier services and compliance.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Governs external system and service acquisition and requires risk assessments and defined expectations.

11.3.2 SA-10 – Controls configuration and change procedures involving systems managed by third parties.

11.3.3 CA-3 – Requires interconnection agreements for systems involving external entities.

11.3.4 PS-7 – Specifies screening and accountability requirements for external personnel.

11.4 EU GDPR (2016/679)

11.4.1 Article 28 – Requires data processing agreements with suppliers acting as processors.

11.4.2 Article 32 – Requires appropriate technical and organizational security measures for all data processors.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(a), (b), (i) – Requires ICT supply chain risk management and third-party controls.

11.5.2 Article 23(1) – Requires documented oversight of third-party services for essential and important entities.

11.6 EU DORA (2022/2554)

11.6.1 Article 5(1) – Requires an ICT risk management framework covering all critical third-party providers.

11.6.2 Article 5(2) – Requires contractual and operational controls for ICT service dependencies.

11.6.3 Article 28(1), (2) – Establishes oversight requirements for ICT third-party risk in the financial sector.

11.7 COBIT 2019

11.7.1 APO10 – “Manage Suppliers” outlines sourcing controls and relationship management expectations.

11.7.2 APO12 – “Manage Risk” integrates supplier risk into organizational risk governance.

11.7.3 DSS05 – “Manage Security Services” applies to managed third-party and outsourced service providers.