					[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 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	
EU NIS2	Articles 21(2)(a)(b)(i), 23(1)	
EU DORA	Articles 5(1)(2), 28(1)(2)	
COBIT 2019	APO10, APO12, DSS05	

PREVIEW ONLY

					[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	

1. **Purpose**
   1.1. This policy establishes the mandatory security requirements for engaging, managing, and terminating relationships with third parties and suppliers who access or influence the organization's data, systems, or services.
   1.2. It ensures that external providers—including IT support vendors, cloud service operators, software developers, and business process contractors—handle company assets securely, in compliance with applicable laws and standards.
   1.3. This policy reduces risks such as data leaks, unauthorized system changes, regulatory fines, or business interruptions caused by insecure or poorly governed third-party arrangements.
2. **Scope**
   2.1. This policy applies to all third parties who:
      2.1.1. Provide software, 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, HR, finance, or customer services
   2.2. It also applies to:
      2.2.1. Internal staff involved in selecting, hiring, or supervising suppliers
      2.2.2. Any personnel managing vendor onboarding, contracts, access, or reviews
      2.2.3. Any system or process reliant 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, privacy, and incident response obligations.
   3.3. Assess and document supplier risks before agreements are signed or access is granted.
   3.4. Apply regular reviews to high-risk or critical suppliers to confirm compliance.
   3.5. Establish a formal process for exceptions, incident management, and contract updates.
   3.6. Support compliance with ISO/IEC 27001:2022, GDPR, NIS2, and DORA obligations related to vendor governance.
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Holds final accountability for supplier selection and security compliance
      4.1.2. Approves contracts, exceptions, and escalations involving vendors
      4.1.3. Oversees incident response and decision-making when vendors fail to meet obligations
   4.2. **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 safe data handling
      4.2.3. Reviews evidence of security controls, certifications, or audit results (where applicable)
   4.3. **Procurement or Administrative Contact**
      4.3.1. Ensures contracts and onboarding documents contain the required security clauses
      4.3.2. Maintains supplier records, including the Supplier Register, approvals, and exceptions

PREVIEW ONLY

4.3.3. Coordinates supplier reviews and update cycles

4.4. **Supplier or Vendor Representative**

4.4.1. Must agree in writing to comply with the organization's information security terms

[……..]

Reference Standards and Frameworks

ISO/IEC 27001:2022

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

ISO/IEC 27002:2022

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

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

Control 5.21 – Controls changes in supplier services that may affect security posture.

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

NIST SP 800-53 Rev.5

SA-9 – Governs external system and service acquisition, requiring risk assessments and defined expectations.

SA-10 – Controls configuration and change procedures involving third-party managed systems.

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

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

EU GDPR (2016/679)

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

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

EU NIS2 Directive (2022/2555)

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

PREVIEW ONLY

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

EU DORA (2022/2554)

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

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

Article 28(1), (2) – Establishes oversight rules for financial-sector ICT third-party risk.

COBIT 2019

APO10 – "Manage Suppliers" outlines sourcing controls and relationship management expectations.

APO12 – "Manage Risk" integrates supplier risk into organizational risk governance.

DSS05 – "Manage Security Services" applies to managed third-party and outsourced service providers

Legal Notice (Copyright & Usage Restrictions)

© 2025 Clarysec LLC. All rights reserved.

This document is the intellectual property of Clarysec LLC. No part may be copied, reused, redistributed, or modified for commercial or implementation purposes without explicit written permission.

Unauthorized use is strictly prohibited and may lead to legal action.

For licensing, contact: info@clarysec.com

PREVIEW ONLY