					Insert Registered Legal Entity Name Here							
Document number: P28S					Document Title: **Outsourced development 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	Clauses 5.1, 6.1, 8	Applicable ISMS and supplier-related controls
ISO/IEC 27002:2022	Controls 5.19, 5.20, 8.25–8.27	Supplier and secure development lifecycle controls
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Acquisition, supply chain, secure development, and supplier agreement requirements
EU GDPR	Article 28	Contractual and data protection requirements for third-party processing
EU NIS2	Article 21(2)(a), (h)	Supply chain and secure application development controls
EU DORA	Article 10	ICT third-party risk management, including outsourced development
COBIT 2019	BAI03, DSS05	Requirements for external development and IT service providers

1. Purpose

1.1 This policy ensures that all outsourced software development, whether performed by freelancers, agencies, or third-party providers/vendors, is carried out securely, is governed by contract, and is aligned with applicable legal, regulatory, and audit requirements.

1.2 It protects the organization from risks related to insecure code, unclear ownership, data exposure, and inadequate vendor management by enforcing documented development standards and provider oversight, including where no dedicated IT function exists.

1.3 This policy supports ISO/IEC 27001:2022 certification by establishing clear development expectations, accountability, and documented controls for third-party development activities.

2. Scope

2.1 This policy applies to:

2.1.1 All outsourced developers, including freelancers and development agencies

2.1.2 Any development work involving internal tools, public-facing websites, software applications, or business automation

2.1.3 Personnel responsible for selecting, managing, or overseeing external developers

2.1.4 Any third-party system integration, scripting, or development that interacts with company data or systems

2.2 It also applies to any party or platform with access to company authentication credentials, data repositories, source code repositories, staging environments, or production systems.

3. Objectives

3.1 Ensure that all outsourced development adheres to secure coding principles and that developers are contractually required to follow documented standards and confidentiality obligations.

3.2 Establish ownership of all deliverables, including code, assets, credentials, and documentation, ensuring full transfer of rights to the company and a traceable handover at project completion.

3.3 Prevent common development risks, including reuse of proprietary code, supply chain attacks through libraries, use of unsupported frameworks, and unapproved administrative access.

3.4 Require pre-engagement documentation for every outsourced project, including contracts, non-disclosure agreements (NDAs), and minimum security expectations.

3.5 Protect customer data, systems, and internal processes by enforcing strong development oversight, post-delivery testing, and secure access management.

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Approves all vendor relationships and signs development agreements.

4.1.2 Ensures all outsourced development complies with this policy.

4.1.3 Removes access to company systems after project completion.

4.1.4 Reviews post-delivery documentation and results.

4.2 Project Owner (typically an internal employee or designated coordinator)

4.2.1 Manages day-to-day coordination with the external developer.

4.2.2 Verifies that functional requirements are met and deliverables are tested.

4.2.3 Ensures secure delivery of code and credentials.

4.2.4 Reports any development-related issues or incidents to the GM.

[... 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 Annual Review

9.1.1 This policy must be reviewed by the General Manager (GM) at least annually. The review ensures that it continues to meet:

9.1.1.1 ISO/IEC 27001 certification requirements

9.1.1.2 Changes in legal obligations, for example GDPR Article 28 and DORA Article 10

9.1.1.3 Current SME-level development practices and third-party risks

9.2 Interim Reviews

9.2.1 Policy reviews must also occur when:

9.2.1.1 A new outsourced development vendor or platform is onboarded

9.2.1.2 A significant incident involving outsourced development occurs

9.2.1.3 There are material changes in the tools, platforms, or environments used

9.3 Review Process

9.3.1 The GM is responsible for:

9.3.1.1 Verifying that contracts, non-disclosure agreements (NDAs), and access control processes remain effective

9.3.1.2 Confirming that current vendors and freelancers comply with the policy

9.3.1.3 Revising terms based on feedback from past projects or incidents

9.4 Version Control and Communication

9.4.1 All changes must be:

9.4.1.1 Recorded with the date, reason, and description of the change

9.4.1.2 Approved by the GM and added to the version history

9.4.1.3 Communicated to all personnel or Project Owners working with external developers

9.4.1.4 Reissued to all affected vendors and third parties where necessary

10. Related Policies and Linkages

10.1 This policy directly supports and depends on implementation of the following SME-aligned policies:

10.1.1 P2S – Governance Roles and Responsibilities Policy: Clarifies responsibility for vendor approval, access control, and risk acceptance when using outsourced developers.

10.1.2 P4S – Access Control Policy: Defines the proper creation, restriction, and termination of user accounts and administrative access used during outsourced development.

10.1.3 P8S – Information Security Awareness and Training Policy: Ensures internal staff understand how to coordinate securely with external developers, including handling credentials and project files.

10.1.4 P17S – Data Protection and Privacy Policy: Establishes security and legal requirements for handling personal data that may be processed by outsourced developers under GDPR.

10.1.5 P24S – Secure Development Policy: Specifies how internal and external development must follow secure coding practices and the vetting of libraries and frameworks.

10.1.6 P30S – Incident Response Policy: Required when outsourced development leads to security incidents or vulnerabilities, guiding coordinated investigation and remediation.

10.2 These policies must be implemented in parallel to ensure outsourced development does not create unmanaged risk or violate SME compliance obligations.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 6.1 – Organizations must assess and treat information security risks associated with suppliers.

11.1.2 Clause 8.1 – Requires operational planning and control, including third-party services such as outsourced development.

11.2 ISO/IEC 27002

11.2.1 Control 5.19 – Recommends evaluating suppliers' ability to meet information security requirements.

11.2.2 Control 5.20 – Recommends regular monitoring and periodic review of third-party services.

11.2.3 Controls 8.25–8.27 – Set out secure development lifecycle practices applicable to outsourced development.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Requires acquisition strategies to include information security measures.

11.3.2 SA-9 – Addresses external system development and supply chain risks.

11.3.3 SA-11 – Defines secure development practices including code reviews and flaw remediation.

11.3.4 SA-15 – Recommends automated tools for flaw detection and software assurance.

11.3.5 SR-3 – Requires supplier agreements to include cybersecurity requirements.

11.4 EU General Data Protection Regulation (GDPR)

11.4.1 Article 28 – Requires contracts with third-party processors to ensure appropriate data protection safeguards, directly applicable to developers processing or accessing personal data.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(a), (h) – Requires supply chain security controls and secure software development practices for in-scope digital service providers, including SMEs where applicable.

11.6 EU Digital Operational Resilience Act (DORA)

11.6.1 Article 10 – Requires ICT third-party risk management, including development agreements, security obligations, and risk controls related to third-party providers.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build – Ensures external development meets business requirements and security expectations.

11.7.2 DSS05 – Manage Security Services – Requires external security services and development providers to operate under enforced security rules and oversight.