					Insert Registered Legal Entity Name Here							
Document number: P28					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	Clause 8.1	N/A
ISO/IEC 27002:2022	Controls 5.19-5.22, 8	N/A
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-10	N/A
EU GDPR	Articles 28, 32	N/A
EU NIS2	Articles 21(2)(a), (h), 23	N/A
EU DORA	Articles 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS05	N/A

1. Purpose

1.1 This policy defines mandatory controls for outsourcing software or system development to external vendors, contractors, third-party service providers, or agencies, to ensure that secure practices are embedded throughout the development lifecycle.

1.2 It is intended to prevent security vulnerabilities, data loss, intellectual property (IP) exposure, and compliance breaches arising from external development engagements.

1.3 This policy mandates vendor governance, secure coding standards, access management, monitoring obligations, and end-of-contract offboarding to preserve the confidentiality, integrity, and availability of developed software.

2. Scope

2.1 This policy applies to all organizational units that engage external parties for software or system development, including:

2.1.1 Web applications, mobile applications, embedded systems, application programming interfaces (APIs), scripts, automation workflows, or platform modules

2.1.2 Custom development for internal platforms, client-facing systems, or commercial products

2.1.3 Engagements with third-party developers, freelancers, agencies, or offshore teams

2.2 This policy also governs any external party that accesses source code, test environments, or CI/CD pipelines during development.

2.3 These requirements are mandatory regardless of contract type, development methodology, or the geographic location of the outsourced provider.

3. Objectives

3.1 To enforce secure software development lifecycle (SDLC) practices across all outsourced engagements, from planning through post-deployment validation.

3.2 To ensure that all contracts with external developers include mandatory clauses covering data protection, secure coding, and IP ownership and retention.

3.3 To define access control, monitoring, and audit requirements for third-party developers interacting with internal systems.

3.4 To protect the organization from supply chain risks, legal violations, and reputational damage associated with externally developed software.

3.5 To maintain ongoing compliance with security frameworks, including ISO/IEC 27001, NIST, GDPR, NIS2, DORA, and COBIT 2019.

4. Roles and Responsibilities

4.1 Top Management

4.1.1 Approves high-risk outsourced development projects and validates policy exceptions where justified.

4.1.2 Ensures that outsourcing decisions align with strategic objectives and the organization's risk appetite.

4.2 Chief Information Security Officer (CISO)

4.2.1 Approves vendor onboarding from an information security perspective.

4.2.2 Defines security control requirements for outsourced engagements and reviews incident reports.

[... 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, or more frequently under the following circumstances:

9.1.1 Introduction of new outsourced development models, vendors, or jurisdictions

9.1.2 Updates to regulatory frameworks such as GDPR, NIS2, or DORA

9.1.3 Following a security incident involving outsourced code, access, or deliverables

9.1.4 As a result of Internal Audit and Compliance findings or Information Security Management System (ISMS) improvements

9.2 The Chief Information Security Officer (CISO) is responsible for initiating and coordinating the policy review in consultation with:

9.2.1.1 Legal and Procurement (for alignment of contractual enforcement)

9.2.1.2 Project and Product Owners (for operational feasibility)

9.2.1.3 Information Security (for threat and control updates)

9.2.1.4 Top Management (for final approval)

9.3 All policy updates must be:

9.3.1.1 Version-controlled and stored in a designated document repository

9.3.1.2 Communicated to stakeholders involved in outsourced development activities

9.3.1.3 Linked to any updates in related policies or procedural documentation

9.4 A change log must accompany each policy version to provide traceability of modifications and approvals.

10. Related Policies and Linkages

10.1 This policy supports, and is supported by, the following related documents:

10.1.1 P1 - Information Security Policy: Establishes enterprise-level security principles applicable across internal and third-party development contexts.

10.1.2 P5 - Change Management Policy: Ensures that all deployment-related changes from outsourced codebases are reviewed and approved before implementation.

10.1.3 P13 - Data Classification and Labeling Policy: Defines how sensitive data is identified before being exposed to development vendors or repositories.

10.1.4 P18 - Cryptographic Controls Policy: Defines how keys, secrets, and sensitive credentials must be handled during development and delivery.

10.1.5 P24 - Secure Development Policy: Defines baseline requirements for internal and external software development practices.

10.1.6 P30 - Incident Response Policy: Governs how breaches or security issues involving outsourced development are escalated, investigated, and resolved.

10.1.7 P33 - Audit and Compliance Monitoring Policy: Provides requirements for reviewing outsourced development activities during audits or compliance reviews.

11. Reference Standards and Frameworks

11.1 This policy is aligned with internationally recognized security frameworks and regulations to ensure secure outsourcing of software development and effective vendor management practices.

11.2 ISO/IEC 27001

11.2.1 Clause 8.1 - Operational Planning and Control: Requires process controls for secure development and third-party delivery.

11.3 ISO/IEC 27002:2022 - Controls 5.19 to 5.21, 8.27

11.3.1 Annex A Control 5.19 - Supplier Relationship Management: Requires formal agreements that include security and compliance clauses.

11.3.2 Annex A Control 5.20 - Addressing Information Security Within Supplier Agreements: Ensures that development-specific controls are embedded in contracts.

11.3.3 Annex A Control 5.21 - Managing Supplier Service Delivery: Requires monitoring of third-party development deliverables and associated risks.

11.3.4 Annex A Control 8.27 - Outsourced Development: Requires defined security requirements and access control over externally developed software.

11.3.5 These controls establish structured requirements for selecting, contracting, and overseeing outsourced developers, including secure development practices, code handling, and delivery validation.

11.4 NIST SP 800-53 Rev. 5

11.4.1 SA-4 - Acquisition Process: Requires secure development requirements to be defined during acquisition.

11.4.2 SA-9 - External System Services: Governs how third-party developers interact securely with internal services.

11.4.3 SA-10 - Developer Configuration Management: Aligns with version control, code access, and change-tracking obligations for external teams.

11.5 EU GDPR (2016/679)

11.5.1 Article 28 - Processor Obligations: Requires contracts with third-party developers to specify security, control, and audit requirements for handling personal data.

11.5.2 Article 32 - Security of Processing: Requires appropriate safeguards (e.g., encryption, access control) when developing systems that process personal data.

11.6 EU NIS2 Directive (2022/2555)

11.6.1 Articles 21(2)(a), (h), 23: Require secure development practices to be applied across third-party engagements and digital supply chains, with oversight and technical verification.

11.7 EU DORA (2022/2554)

11.7.1 Articles 28(1), (2): Require financial entities to manage ICT third-party risk through contractual controls and secure development oversight, particularly for critical outsourced development.

11.8 COBIT 2019

11.8.1 APO10 - Manage Suppliers: Establishes structured requirements for vendor evaluation, contracts, and performance monitoring.

11.8.2 BAI03 - Manage Solutions Build: Directly maps to secure SDLC processes, code reviews, and development validation.

11.8.3 DSS05 - Manage Security Services: Aligns with the monitoring and protection of systems developed externally or by third parties.