<table>
<tr><td colspan="5"></td><td colspan="8">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P28</td><td colspan="8">Document Title:
<b>Outsourced Development Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="3">Effective Date:
01.01.2025</td><td colspan="8">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

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, 8.27	
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	
EU GDPR	Articles 28, 32	
EU NIS2	Articles 21(2)(a), (h), 23	
EU DORA	Articles 28(1), (2)	
COBIT 2019	APO10, BAI03, DSS05	

<table>
<tr><td colspan="4"></td><td colspan="8">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="4">Document number:
P28</td><td colspan="8">Document Title:
<b>Outsourced Development Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="2">Effective Date:
01.01.2025</td><td colspan="8">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

1. **Purpose**
   1.1. This policy defines mandatory controls for outsourcing software or system development to external vendors, contractors, or agencies, ensuring secure practices are embedded throughout the development lifecycle.
   1.2. It aims to prevent security vulnerabilities, data loss, intellectual property (IP) exposure, and compliance breaches resulting from external development engagements.
   1.3. The policy enforces vendor governance, secure coding standards, access management, monitoring obligations, and end-of-contract offboarding to uphold confidentiality, integrity, and availability of developed software.
2. **Scope**
   2.1. This policy applies to all organizational units engaging external entities for software or system development, including:
      2.1.1. Web applications, mobile apps, embedded systems, 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. The policy also governs any external entity that accesses source code, test environments, or CI/CD pipelines during development.
   2.3. The requirements are enforceable regardless of contract type, development methodology, or geographic location of the outsourced provider.
3. **Objectives**
   3.1. To enforce secure development life cycle (SDLC) practices across all outsourced engagements, from planning to post-deployment validation.
   3.2. To ensure all contracts with external developers include mandatory clauses covering data protection, secure coding, and IP 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 threats, legal violations, and reputational damage related to externally developed software.
   3.5. To maintain continuous compliance with security frameworks, including ISO/IEC 27001, NIST, GDPR, NIS2, DORA, and COBIT 2019.
4. **Roles and Responsibilities**
   4.1. **Executive Management**
      4.1.1. Approves high-risk outsourced development projects and validates policy exceptions where justified.
      4.1.2. Ensures outsourcing decisions align with strategic objectives and enterprise risk appetite.
   4.2. **Chief Information Security Officer (CISO)**

4.2.1. Approves vendor onboarding from a security perspective.

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

4.3. **Procurement and Legal Teams**

4.3.1. Draft and validate contracts with required security, confidentiality, IP ownership, and audit clauses.

[…..]

11. Reference Standards and Frameworks

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

ISO/IEC 27001:2022

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

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

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

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

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

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

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

NIST SP 800-53 Rev.5

SA-4 - Acquisition Process: Requires secure development requirements to be defined at acquisition time.

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

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

EU GDPR (2016/679)

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

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

EU NIS2 Directive (2022/2555)

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

EU DORA (2022/2554)

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

COBIT 2019

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

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

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