<table>
<tr><td colspan="5"></td><td colspan="7">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P28S</td><td colspan="7">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="7">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	Clauses 5.1, 6.1, 8.1	
ISO/IEC 27002:2022	Controls 5.19, 5.20, 8.25–8.27	
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	
EU GDPR	Article 28	
EU NIS2	Article 21(2)(a), (h)	
EU DORA	Article 10	
COBIT 2019	BAI03, DSS05	

	[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

1. Purpose

1.1. This policy ensures that all outsourced software development—whether handled by freelancers, agencies, or third-party providers—is conducted securely, contractually controlled, and 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 vendor mismanagement by enforcing enforceable development standards and supplier oversight, even in the absence of a dedicated IT department.

1.3. This policy supports ISO/IEC 27001:2022 certification by providing clearly defined development expectations, accountability, and documented controls over 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. Staff 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 includes any party or platform with access to company 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 obligated to follow documented standards and confidentiality clauses.

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

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

3.4. Require pre-engagement documentation for every outsourced project, including contracts, NDAs, and minimum security expectations.

3.5. Protect customer data, systems, and internal processes by enforcing strong development oversight, post-delivery testing, and secure system 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 follows this policy.

[……]

11. Reference Standards and Frameworks

ISO/IEC 27001:2022

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

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

ISO/IEC 27002:2022

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

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

Controls 8.25–8.27 – Outline secure development lifecycle practices applicable to outsourced development.

NIST SP 800-53 Rev.5

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

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

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

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

SR-3 – Mandates supplier agreements to include cybersecurity requirements.

EU General Data Protection Regulation (GDPR)

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

EU NIS2 Directive (2022/2555)

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

EU Digital Operational Resilience Act (DORA)

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

COBIT 2019

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

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

<table>
<tr><td colspan="6"></td><td colspan="6">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="6">Document number:
P28S</td><td colspan="6">Document Title:
<b>Outsourced Development Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="4">Effective Date:
01.01.2025</td><td colspan="6">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>