					[Insert Registered Legal Entity Name Here]							
Document number: P24S					Document Title: **Secure 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 where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 8.1	
ISO/IEC 27002:2022	Controls 8.25–8.27	
NIST SP 800-53 Rev.5	SA-3–SA-15, SI-10	
EU GDPR	Article 25	
EU NIS2	Article 21(2)(a), (e), (h)	
EU DORA	Articles 6(7), 9(1)(c), 10(2)(c)	
COBIT 2019	BAI03	

					[Insert Registered Legal Entity Name Here]							
Document number: P24S					Document Title: **Secure 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 software, scripts, and web-based tools created or modified by the organization or its external partners are developed securely, minimizing the risk of vulnerabilities, unauthorized data access, or operational disruption.
   1.2. It defines mandatory secure development rules and coding practices that all internal developers, contractors, and vendors must follow, regardless of project size or complexity.
   1.3. This policy is designed to protect customer data, prevent breaches, and ensure that software created or customized by or for the organization can pass security audits, meet legal requirements (e.g., GDPR, NIS2, DORA), and support ISO/IEC 27001 certification.
2. **Scope**
   2.1. This policy applies to all individuals and entities involved in developing, customizing, deploying, or managing the following on behalf of the organization:
      2.1.1. Websites, applications, or automation tools
      2.1.2. Internally developed scripts or software
      2.1.3. Code created by third-party developers or freelancers
      2.1.4. Plugins, libraries, and software components integrated into production systems
   2.2. It covers all environments used in development activities, including:
      2.2.1. Development and test environments
      2.2.2. Staging and pre-production environments
      2.2.3. Production systems used to run custom-developed code
   2.3. The policy also governs the handling of data during development and deployment, especially any use of production data in non-production systems.
3. **Objectives**
   3.1. To prevent the introduction of security flaws or vulnerabilities in custom or third-party-developed software.
   3.2. To ensure that secure coding practices and vulnerability prevention are integrated into every phase of the software development lifecycle.
   3.3. To reduce risks associated with the use of open-source or third-party components by mandating proper vetting and tracking.
   3.4. To require formal code review and application security testing before release.
   3.5. To control access to development environments and ensure separation from live production systems.
   3.6. To meet mandatory requirements under international standards and regulations (e.g., ISO/IEC 27001, GDPR, DORA, NIS2).
4. **Roles and Responsibilities**
   4.1. **General Manager (GM)**
      4.1.1. Approves and owns this policy.
      4.1.2. Ensures all software development (internal or outsourced) complies with this policy.

      […….]

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 8.1 – Requires implementation of operational controls, including secure development, that align with business objectives and risk posture.

ISO/IEC 27002:2022

Control 8.25 – Recommends integrating security throughout the software lifecycle, including source control, versioning, and developer access.

Control 8.26 – Specifies methods for application testing and verification of security functionality before go-live.

Control 8.27 – Requires third-party developers to adhere to the same development standards and have their security responsibilities clearly defined.

NIST SP 800-53 Rev.5

SA-3 to SA-15 – Define secure development processes, including developer access control, testing, threat modeling, and documentation.

SI-10 – Requires developers to identify and mitigate common software weaknesses and to use automated tools where applicable.

EU GDPR (2016/679)

Article 25 – "Data protection by design and by default" mandates integrating security and privacy protections during software design and development, especially where personal data is processed.

EU NIS2 Directive (2022/2555)

Article 21(2)(a), (e), and (h) – Requires secure development policies, oversight of open-source use, and documented mitigation of application-related risks in essential and important entities.

EU DORA (2022/2554)

Articles 6(7), 9(1)(c), and 10(2)(c) – Impose development lifecycle security obligations for financial-sector entities, including SMEs, particularly for critical ICT systems.

COBIT 2019

BAI03 – "Manage Solutions Identification and Build" supports implementation of structured development controls that emphasize security, traceability, and resilience, tailored to SME constraints.

					[Insert Registered Legal Entity Name Here]							
Document number: P24S					Document Title: **Secure Development Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	