					[Insert Registered Legal Entity Name Here]							
Document number: P24					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 to SA-15, SI-10, SR-3	
EU GDPR	Articles 25, 32	
EU NIS2	Article 21(2)(e), (f)	
EU DORA	Articles 9, 10	
COBIT 2019	BAI03, BAI07, DSS05	

					[Insert Registered Legal Entity Name Here]									
Document number: P24					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 defines mandatory security requirements for software and system development activities within the organization, including internal projects, outsourced development, and third-party code integration.
   1.2 The objective is to ensure that security is embedded throughout the Software Development Life Cycle (SDLC) and that vulnerabilities are identified, mitigated, and prevented prior to production deployment.
   1.3 This policy supports the enforcement of ISO/IEC 27001:2022 Clause 8.1 and Annex A Controls 8.25–8.27 by standardizing secure development governance, code validation practices, and third-party development oversight.
2. **Scope**
   2.1 This policy applies to all:
      2.1.1 Internally or externally developed software, applications, scripts, integrations, and automation tools
      2.1.2 Development teams, product owners, DevOps, QA, architects, project managers, and contractors
      2.1.3 SDLC environments including development, testing, staging, and pre-production systems
      2.1.4 Open-source and third-party components integrated into internal applications
      2.1.5 Software deployed on-premises, in private cloud, hybrid, or public cloud environments
   2.2 All users and entities participating in system development, testing, or deployment within the organizational context are subject to this policy, including managed service providers and platform vendors.
3. **Objectives**
   3.1 Embed security controls across all phases of software development, from design to deployment, ensuring risk reduction is proactive and continuous.
   3.2 Prevent the introduction of exploitable vulnerabilities such as injection flaws, insecure authentication, and exposure to known third-party weaknesses.
   3.3 Establish and enforce secure coding practices aligned with OWASP, SANS CWE, and framework-specific guidelines.
   3.4 Ensure that all code undergoes peer review, automated analysis, and security validation prior to deployment.
   3.5 Manage development risks stemming from outsourced activities, third-party code inclusion, and open-source software reuse.
   3.6 Protect development, test, and staging environments from unauthorized access and prevent use of production data without approved masking or anonymization.
   3.7 Promote security awareness among developers, product managers, and quality assurance professionals through role-based training and continuous updates on emerging threats.
4. **Roles and Responsibilities**
   4.1 **Chief Information Security Officer (CISO)**
      4.1.1 Owns this policy and ensures secure development requirements are enforced organization-wide.
      4.1.2 Approves secure coding standards and third-party development agreements.
      4.1.3 Validates risk treatment decisions for unresolved or deferred vulnerabilities.

4.2 **Application Security Lead / DevSecOps Manager**

4.2.1 Develops, maintains, and promotes secure coding guidelines.

[….]

11. Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 8.1 – Operational Planning and Control: Requires integration of secure development processes and controls into operations.

ISO/IEC 27002:2022 – Controls 8.25–8.27

Annex A Control 8.25 – Secure Development Life Cycle: Enforces formal inclusion of security in software design and development.

Annex A Control 8.26 – Application Security Requirements: Requires definition of secure coding and security acceptance criteria.

Annex A Control 8.27 – Secure System Architecture and Engineering Principles: Demands application of security design principles and mitigation of known weaknesses.

NIST SP 800-53 Rev.5

SA-3 to SA-15: Establishes structured application security development practices, including requirements for design, code integrity, and testing.

SI-10 – Information Input Validation: Addresses secure coding defenses.

SR-3 – Supply Chain Protection: Requires vetting of third-party software, components, and development providers.

EU GDPR (2016/679)

Article 25 – Data Protection by Design and by Default: Mandates embedding security and privacy into system development.

Article 32 – Security of Processing: Supports technical measures like input validation, access controls, and secure deployment.

EU NIS2 Directive (2022/2555)

Article 21(2)(e–f): Requires software development practices that include vulnerability management, code security, and incident reporting.

EU DORA (2022/2554)

Article 9 – ICT Risk Management: Demands secure development practices for financial entities, including software quality controls and defect remediation.

Article 10 – Business Continuity and Testing: Encourages rigorous testing and validation of ICT systems, including applications.

COBIT 2019

BAI03 – Manage Solutions Identification and Build: Governs design, development, and security integration into new solutions.

BAI07 – Manage Change Acceptance and Transitioning: Ensures secure deployment and post-deployment evaluation.

DSS05 – Manage Security Services: Applies security validation to software and service provisioning.