					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**

1. Purpose

1.1 This policy establishes mandatory security requirements for software and system development activities across 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 before production deployment.

1.3 This policy supports the implementation of ISO/IEC 27001:2022 Clause 8.1 and Annex A Controls 8.25–8 by standardizing secure development governance, code validation practices, and oversight of third-party development.

2. Scope

2.1 This policy applies to all:

2.1.1 Software, applications, scripts, integrations, and automation tools developed internally or externally

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 in on-premises, private cloud, hybrid, or public cloud environments

2.2 All users and entities involved 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 throughout all phases of software development, from design through deployment, to ensure proactive and continuous risk reduction.

3.2 Prevent the introduction of exploitable vulnerabilities, including 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 guidance.

3.4 Ensure that all code undergoes peer review, automated analysis, and security validation before deployment.

3.5 Manage development risks arising from outsourced activities, third-party code inclusion, and reuse of open-source software.

3.6 Protect development, test, and staging environments from unauthorized access and prevent the use of production data without approved masking or anonymization.

3.7 Promote security awareness among developers, product managers, and quality assurance personnel 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 that secure development requirements are enforced across the organization.

4.1.2 Approves secure coding standards and third-party development agreements.

4.1.3 Validates Risk Treatment Plan decisions for unresolved or deferred vulnerabilities.

4.2 Application Security Lead / DevSecOps Manager

4.2.1 Develops, maintains, and promotes secure coding guidelines.

4.2.2 Integrates static and dynamic security testing into CI/CD pipelines.

4.2.3 Conducts code security reviews and defines mandatory corrective actions.

[... 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 annually, or more frequently in response to:

9.1.1 Major changes in development methodologies or DevOps tooling

9.1.2 Material security incidents arising from application vulnerabilities

9.1.3 Changes in regulatory requirements related to secure software (e.g., GDPR, DORA)

9.1.4 New industry standards or threat intelligence (e.g., OWASP Top 10, SLSA, MITRE CWE)

9.2 Policy review shall be led by the Application Security Lead in coordination with the CISO, software architects, QA leadership, and Legal Counsel (for implications related to third-party code).

9.3 Any revisions must be recorded in the ISMS Document Control Register, maintained under version control, and communicated to affected teams through release notes or mandatory training.

9.4 Legacy versions must be retained in the archive repository for legal and audit traceability.

10. Related Policies and Linkages

10.1 P1 – Information Security Policy. Establishes the strategic mandate for embedding security across all information systems, of which secure development is a foundational operational control.

10.2 P4 – Access Control Policy. Defines the control measures for restricting access to development environments, repositories, build tools, and CI/CD pipelines.

10.3 P5 – Change Management Policy. Ensures that code changes, releases, and deployments are subject to appropriate approval, rollback planning, and post-deployment verification.

10.4 P12 – Asset Management Policy. Supports the inventory and management of development environments, source repositories, and build systems as assets subject to classification and protection.

10.5 P22 – Logging and Monitoring Policy. Applies to development pipelines and ensures that build processes, code promotions, and deployment events are logged, monitored, and analyzed for security anomalies.

10.6 P30 – Incident Response Policy. Provides the framework for analyzing and responding to security flaws discovered after deployment or during application security testing.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

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

11.2 ISO/IEC 27002:2022 – Controls 8.25–8

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

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

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

11.3 NIST SP 800-53 Rev.5

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

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

11.3.3 SR-3 – Supply Chain Protection: Requires due diligence for third-party software, components, and development providers.

11.4 EU GDPR (2016/679)

11.4.1 Article 25 – Data Protection by Design and by Default: Requires the integration of security and privacy into system development.

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

11.5 EU NIS2 Directive (2022/2555)

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

11.6 EU DORA (2022/2554)

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

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

11.7 COBIT 2019

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

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

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