					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	Relevant security controls for operational practices, including secure development
ISO/IEC 27002:2022	Controls 8.25–8.27	Covers the secure development lifecycle, testing, and third-party developer security responsibilities
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Addresses secure SDLC, access control, and vulnerability management in development
EU GDPR	Article 25	Requires data protection by design and by default in software development
EU NIS2	Article 21(2)(a), (e), (h)	Requires secure development policies, oversight of open-source software, and mitigation documentation
EU DORA	Articles 6(7), 9(1)(c), 10(2)(c)	Requires lifecycle security for critical ICT systems in the financial sector
COBIT 2019	BAI	Framework for structured, traceable, and resilient secure development management

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, and operational disruption.

1.2 It defines mandatory secure development requirements and coding practices that all internal developers, contractors, and vendors must follow, regardless of project size or complexity.

1.3 This policy is intended to protect customer data, prevent security breaches, and ensure that software created or customized by or for the organization can withstand security audits, meet legal and regulatory 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 reviews for deliverables created by third-party providers, vendors, or freelancers

2.1.4 Plugins, libraries, and software components integrated into production systems

2.2 It applies to 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 This policy also governs data handling during development and deployment, especially any use of production data in non-production systems.

3. Objectives

3.1 Prevent the introduction of security flaws or vulnerabilities in custom-developed or third-party-developed software.

3.2 Ensure that secure coding practices and vulnerability prevention are integrated into every phase of the software development lifecycle.

3.3 Reduce risks associated with the use of open-source or third-party components by requiring appropriate vetting and tracking.

3.4 Require formal code review and application security testing before release.

3.5 Control access to development environments and ensure separation from live production systems.

3.6 Meet mandatory requirements under applicable 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 that all software development activities, whether internal or outsourced, comply with this policy.

4.1.3 Reviews and approves development or service contracts that include secure development clauses.

4.1.4 Verifies vendor compliance through periodic reviews or by requesting security evidence.

4.2 Internal Developer or Application Owner

4.2.1 Follows secure coding and deployment practices.

4.2.2 Applies the secure development checklist to every project.

4.2.3 Validates the security of any open-source or third-party components used.

4.2.4 Reports any identified vulnerabilities to the GM immediately.

[... 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 by the General Manager at least annually to:

9.1.1 Verify continued compliance with ISO/IEC 27001, GDPR, NIS2, and DORA

9.1.2 Reflect evolving threats or changes in secure development good practice

9.1.3 Ensure compatibility with any new tools, platforms, or vendor relationships

9.2 Interim reviews must be triggered by:

9.2.1 Any reported software security incident

9.2.2 Introduction of a new development framework or hosting platform

9.2.3 A change in third-party development partners

9.2.4 Regulatory updates affecting software or security obligations

9.3 All changes to this policy must be:

9.3.1 Documented with the date, summary of change, and GM approval

9.3.2 Communicated clearly to all internal and external development personnel

9.3.3 Retained as part of the organization’s policy version control and change history

9.4 Updated versions must be made readily accessible through internal platforms, printed documentation, or cloud services accessible to vendors.

10. Related Policies and Linkages

10.1 This policy supports and depends on the effective implementation of several other SME policies:

10.1.1 P2S – Governance Roles and Responsibilities Policy: Establishes accountability for assigning and verifying development security controls across projects and vendors.

10.1.2 P4S – Access Control Policy: Provides baseline rules for restricting access to development environments and code repositories, including segregation of duties.

10.1.3 P8S – Information Security Awareness and Training Policy: Ensures that internal developers and contractors understand secure coding practices and related security responsibilities.

10.1.4 P17S – Data Protection and Privacy Policy: Clarifies how personal data must be handled during development, testing, and logging processes to maintain GDPR compliance.

10.1.5 P30S – Incident Response Policy: Defines how development-related security incidents must be reported, assessed, and remediated, including code-related exposures.

10.2 These policies operate together to ensure that secure development is both achievable and verifiable, even in a small or non-technical organization.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Requires the implementation of operational controls, including secure development, aligned with business objectives and risk posture.

11.2 ISO/IEC 27002

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

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

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

11.3 NIST SP 800-53 Rev.5

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

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

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 protections during software design and development, especially where personal data is processed.

11.5 EU NIS2 Directive (2022/2555)

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

11.6 EU DORA (2022/2554)

11.6.1 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.

11.7 COBIT 2019

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