					[Insert Registered Legal Entity Name Here]							
Document number: P25					Document Title: **Application Security Requirements 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 8.25–8.26	
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	
EU GDPR	Articles 25, 32	
EU NIS2	Articles 21(2)(f), 23	
EU DORA	Articles 9, 11	
COBIT 2019	BAI03, BAI09, DSS05	

					[Insert Registered Legal Entity Name Here]									
Document number: P25					Document Title: **Application Security Requirements 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 application-layer security requirements for software developed, acquired, integrated, or deployed by the organization. It ensures that all applications are designed, implemented, and maintained in accordance with secure development principles, regulatory obligations, and organizational risk appetite.

1.2 The policy enforces the inclusion of security throughout the application lifecycle—covering user authentication, data handling, interface protection, and secure interaction with APIs or services.

1.3 By adopting this policy, the organization aims to prevent the introduction of software vulnerabilities, protect sensitive data, and ensure traceability and resilience against exploitation and abuse.

2. Scope

2.1 This policy applies to all:

2.1.1 Internally developed or externally sourced applications, including SaaS and custom-built tools

2.1.2 Applications supporting critical business operations, customer access, or processing regulated data

2.1.3 Development, DevOps, QA, product, and security teams

2.1.4 Third-party developers, software vendors, and integration partners with access to organizational applications or APIs

2.2 It applies across all environments: development, testing, staging, production, and disaster recovery, regardless of whether hosted on-premises, in private data centers, or public cloud environments.

3. Objectives

3.1 Define baseline functional and non-functional security requirements to be met by all applications, irrespective of development method or technology stack.

3.2 Ensure integration of application-layer protections including input validation, output encoding, error handling, and session security.

3.3 Require secure implementation of authentication, authorization, and access control mechanisms aligned with organizational identity and access policies.

3.4 Mandate secure interaction with APIs, web interfaces, and third-party components using approved protocols and security controls.

3.5 Enable early detection and mitigation of vulnerabilities through static and dynamic analysis, code reviews, and threat modeling.

3.6 Protect sensitive data in compliance with regulatory requirements by enforcing encryption, classification, and data retention logic.

3.7 Ensure continuous validation of application security posture post-deployment, through testing, monitoring, and audit readiness.

4. Roles and Responsibilities

4.1 **Chief Information Security Officer (CISO)**

4.1.1 Owns this policy and ensures its alignment with the organization's information security strategy and risk posture.

4.1.2 Approves application security requirements and enforces mandatory controls across development and procurement functions.

4.2 **Application Security Lead / DevSecOps Manager**

4.2.1 Defines baseline security controls and testing methodologies for application components.

4.2.2 Oversees secure integration of tools such as SAST, DAST, IAST, and SCA into the software delivery pipeline.

[….]

11. Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 8.1 – Operational Planning and Control: Requires application security to be embedded into processes and systems to ensure confidentiality, integrity, and availability.

ISO/IEC 27002:2022 – Controls 8.25–8.26

Detail the expectations for application-layer security, including secure coding practices, threat modeling, architectural controls, and third-party software validation.

Annex A Control 8.25 – Secure Development Life Cycle: Enforces security integration across the application lifecycle.

Annex A Control 8.26 – Application Security Requirements: Mandates the definition and enforcement of technical controls to protect applications against misuse and compromise.

NIST SP 800-53 Rev.5

SA-11 – Developer Security Testing and Evaluation: Mandates static, dynamic, and penetration testing during development.

SA-15 – Development Process, Standards, and Tools: Establishes formal standards for secure application development.

SI-10 – Information Input Validation: Requires control mechanisms for preventing injection and parsing attacks.

EU GDPR (2016/679)

Article 25 – Data Protection by Design and by Default: Requires integration of data protection and privacy into application logic and workflows.

Article 32 – Security of Processing: Mandates appropriate technical measures, such as input validation, encryption, and secure access controls.

EU NIS2 Directive (2022/2555)

Article 21(2)(f): Requires vulnerability handling and secure application lifecycle practices for essential and important entities.

Article 23 – Reporting of Security Incidents: Necessitates application-layer logging and monitoring capabilities to detect and report significant incidents.

EU DORA (2022/2554)

Article 9 – ICT Risk Management: Obligates financial entities to ensure applications are secure, tested, and resilient to cyber threats.

Article 11 – Testing of ICT Tools: Encourages periodic penetration testing and red teaming of critical applications and services.

COBIT 2019

BAI03 – Manage Solutions Identification and Build: Establishes design and control requirements during application development.

BAI09 – Manage Applications: Emphasizes secure maintenance, monitoring, and enhancement of live applications.

DSS05 – Manage Security Services: Links application protection to broader organizational security operations and controls.