		[Insert Registered Legal Entity Name Here]
Document number: P25S		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, SI-10	
EU GDPR	Article 25	
EU NIS2	Article 21(2)(a), (e)	
EU DORA	Articles 9(2)(c), 10(2)(c)	
COBIT 2019	BAI03	

<table>
<tr><td colspan="5"></td><td colspan="7">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P25S</td><td colspan="7">Document Title:
<b>Application Security Requirements Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="3">Effective Date:
01.01.2025</td><td colspan="7">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

Purpose

1.1. This policy defines the minimum mandatory application security controls required for all software and system solutions used by the organization, regardless of whether they are developed internally or procured from external vendors.

1.2. It ensures that applications are designed, implemented, and maintained to protect customer, employee, and business data from unauthorized access, misuse, alteration, or destruction.

1.3. This policy supports the organization’s efforts to achieve and maintain ISO/IEC 27001 certification, meet GDPR and NIS2 obligations, and reduce operational risks associated with insecure software deployments.

1.4. It helps create a consistent and auditable approach to application security for SMEs by establishing a uniform checklist of security features and practices, adapted for environments with limited in-house technical resources.

2. Scope

2.1. This policy applies to all applications, systems, tools, and platforms that:

2.1.1. Are developed in-house, customized, or scripted for internal use

2.1.2. Are purchased as commercial software, SaaS, or cloud-based systems

2.1.3. Process, store, or transmit personal data, business records, or sensitive operational information

2.1.4. Are accessed by employees, contractors, customers, or partners via internal networks, the internet, or mobile platforms

2.2. The policy covers:

2.2.1. Developers (internal or contracted)

2.2.2. Software vendors and cloud service providers

2.2.3. IT support personnel or administrators responsible for deployment and support

2.2.4. Application owners and business users involved in system approval and oversight

3. Objectives

3.1. To ensure all applications used by the organization have embedded, verifiable security controls that mitigate common software vulnerabilities.

3.2. To protect the confidentiality, integrity, and availability of data processed by applications, regardless of where they are hosted.

3.3. To require formal testing, review, and validation of application security before any new application or major update is approved for production use.

3.4. To enable consistent, secure handling of user credentials, session data, and access rights across all business-critical systems.

3.5. To require secure logging, audit capabilities, and monitoring features in all applications to support detection of and response to suspicious activity.

3.6. To reduce legal and compliance risks by ensuring applications meet applicable regulatory security requirements.

4. Roles and Responsibilities

4.1. **General Manager (GM)**

4.1.1. Holds overall accountability for application security across the organization.
4.1.2. Approves this policy and ensures all acquisitions or development projects comply with it.
4.1.3.

Reference Standards and Frameworks

ISO/IEC 27001:2022

Clause 8.1 – Requires organizations to establish operational controls to address information security risks, including those related to applications and software systems.

ISO/IEC 27002:2022

Control 8.25 – Advises implementing secure design, development, and code review practices across all applications, including those provided by vendors.

Control 8.26 – Recommends formal testing of application security controls, particularly in areas involving access control, input validation, and session handling.

NIST SP 800-53 Rev.5

SA-11 – Specifies requirements for developer testing, code analysis, and dynamic application scanning before deployment.

SI-10 – Addresses detection and prevention of common software flaws, emphasizing developer awareness and technical safeguards.

EU GDPR (2016/679)

Article 25 – "Data protection by design and by default" mandates embedding privacy and security into the core design of applications handling personal data.

EU NIS2 Directive (2022/2555)

Article 21(2)(a) and (e) – Requires essential and important entities to implement technical measures to secure applications and detect software-related risks.

EU DORA (2022/2554)

Article 9(2)(c), 10(2)(c) – Requires financial-sector SMEs to embed application-level security controls and perform regular assessments to maintain digital operational resilience.

COBIT 2019

BAI03 – "Manage Solutions Identification and Build" guides the development or acquisition of secure software aligned with risk, compliance, and business requirements—even in resource-constrained SME environments.