					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**

Legal Notice (Copyright & Usage Restrictions)

(C) 2025 Clarysec LLC. All rights reserved.

This document is the intellectual property of Clarysec LLC. No part may be copied, reused, redistributed, or modified for commercial or implementation purposes without explicit written permission.
Unauthorized use is strictly prohibited and may lead to legal action.
For licensing, contact: info@clarysec.com

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	Operational controls, including application security
ISO/IEC 27002:2022	Controls 8.25–8.26	Secure design, development, testing, and code review
NIST SP 800-53 Rev.5	SA-11, SI-10	Developer/application testing, code analysis, flaw prevention
EU GDPR	Article 25	Data protection by design and by default
EU NIS2	Article 21(2)(a), (e)	Technical measures to secure applications and detect risks
EU DORA	Articles 9(2)(c), 10(2)(c)	Application security for digital operational resilience
COBIT 2019	BAI03	Manage secure software development/acquisition

1. Purpose

1.1 This policy defines the minimum mandatory application security controls required for all software and system solutions used by the organization, whether 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 Risk associated with insecure software deployments.

1.4 It establishes a consistent and auditable approach to application security for SMEs by defining a uniform checklist of security features and practices adapted to 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, Third-Party Service Providers, customers, or partners via internal networks, the internet, or mobile platforms.

2.2 This 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 IT 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 that all Applications used by the organization include 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 hosting location.

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

3.4 To enable the consistent and secure handling of authentication credentials, session data, and Access privileges across all business-critical systems.

3.5 To require secure Audit Logging, audit functionality, and Monitoring and Threat Detection capabilities in all Applications to support the detection of and response to suspicious activity.

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

4. Roles and Responsibilities

4.1 General Manager (GM)

4.1.1 Has overall accountability for application security across the organization.

4.1.2 Approves this policy and ensures that all acquisitions and development projects comply with it.

4.1.3 Ensures that vendors and service providers are contractually bound to application security requirements.

4.1.4 Reviews and approves exceptions where full compliance cannot be achieved due to business constraints.

4.2 Application Owner (if designated)

4.2.1 Identifies application-specific security requirements during system selection or project initiation.

4.2.2 Verifies that key features such as login protection, encryption, and activity logging are included.

4.2.3 Participates in pre-deployment reviews and confirms that security controls meet business needs.

[... 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 once per calendar year to:

9.1.1 reflect changes in regulatory requirements (e.g., GDPR, NIS2, DORA).

9.1.2 incorporate new or emerging threats and attack techniques.

9.1.3 update language and requirements to reflect changes in platforms, vendors, or development methods.

9.2 Interim reviews must also be conducted when:

9.2.1 new Applications are introduced.

9.2.2 existing Applications undergo significant updates or integration.

9.2.3 an application-related incident or breach occurs.

9.2.4 new risks are identified from external advisories or industry alerts.

9.3 All updates to this policy must be:

9.3.1 approved by the General Manager.

9.3.2 documented with version history and the reason for change.

9.3.3 communicated to all employees, developers, and vendors involved in application management.

9.3.4 stored securely for audit and compliance purposes.

10. Related Policies and Linkages

10.1 This policy is directly supported by, and contributes to the enforcement of, the following SME-aligned security policies:

10.1.1 P2S – Governance Roles and Responsibilities Policy: Assigns responsibility for approving Applications, enforcing policy, and managing vendors.

10.1.2 P4S – Access Control Policy: Ensures that application access aligns with least privilege and Session control principles.

10.1.3 P8S – Information Security Awareness and Training Policy: Ensures that users and developers are trained to recognize and report application-related threats.

10.1.4 P17S – Data Protection and Privacy Policy: Provides Data privacy safeguards that must be enforced by any application processing personal information (PII).

10.1.5 P14S – Data Retention Policy and Disposal Policy: Governs how application-generated logs, backups, and sensitive data must be retained, archived, and securely destroyed.

10.1.6 P30S – Incident Response Policy: Outlines the steps for identifying, reporting, and Containment of application-related security events.

10.2 Together, these policies ensure that application security is fully integrated into the organization's Information Security Management System (ISMS) and audit readiness.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001

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

11.2 ISO/IEC 27002

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

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

11.3 NIST SP 800-53 Rev.5

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

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

11.4 EU GDPR (2016/679)

11.4.1 Article 25 – "data protection by design and by default" requires privacy and security to be embedded into the core design of Applications handling personal data.

11.5 EU NIS2 Directive (2022/2555)

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

11.6 EU DORA (2022/2554)

11.6.1 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.

11.7 COBIT 2019

11.7.1 BAI03 – “Manage Solutions Identification and Build” provides guidance for the development or acquisition of secure software aligned with risk, compliance, and business requirements, including in resource-constrained SME environments.