# Secure Software Development Policy

Information Security

Version 1.0

Prepared By:
Hrushikesh Mehendale

Reviewed By:
Shruti Deshpande

FlaggGRC

## Document Control

| Last Modified | Reason For Change | Suggested By | Approved By |
|---|---|---|---|
| 6 April 2025 | Document created | Hrushi M | Shruti D |
| 25 Mar 2026 | Document reviewed, no change | Hrushi M | Shruti D |
| 7 Oct 2026 | Document reviewed, no change | Hrushi M | Shruti D |

## Purpose

This policy shall define principles, roles, and guidelines for secure software engineering practices to ensure that security is integrated throughout the Software Development Lifecycle (SDLC). The objective shall be to protect information assets by mitigating security risks, ensuring confidentiality, integrity, and availability of data.

## Scope

This policy shall apply to all software development activities, including design, development, testing, deployment, maintenance, and change management. It shall encompass both internal and outsourced development processes.

# Secure Software Development Principles

- Security by Design: Security requirements shall be incorporated at the initial stages of software design and planning.
- Least Privilege: Software components and users shall operate with the minimum privileges required to perform tasks.
- Data Protection: Mechanisms for data confidentiality, integrity, and availability shall be enforced.
- Secure Coding Practices: Industry-standard secure coding guidelines such as OWASP and CERT shall be adopted.
- Security Testing: Routine security assessments, including penetration testing, code reviews, and vulnerability scans, shall be conducted.
- Environment Separation: Development, testing, and production environments shall be segregated.
- Dependency Management: Only trusted and updated third-party components shall be used.

# Secure Development Practices

- Design Stage
    - Risk Assessment: Identify potential threats and vulnerabilities in the software architecture.
    - Confidentiality Assessment: Evaluate the likelihood of unauthorized data disclosures.
    - Integrity Assessment: Ensure mechanisms are in place to protect data from unauthorized modifications.
    - Availability Assessment: Protect systems against downtime and denial-of-service attacks.
    - Compliance Assessment: Ensure alignment with regulatory/customer requirements, including ISO 27001.
- Development Stage
    - Environment Segregation: Maintain clear boundaries between development, testing, and production environments.
    - Input Validation: Implement strong input validation mechanisms to prevent vulnerabilities.
    - Authentication & Authorization: Enforce role-based access control (RBAC).
    - Secure Storage: Store sensitive information, including keys and credentials, in secure encrypted vaults.
- Testing Stage
    - Static and Dynamic Analysis: Perform automated code analysis to detect security vulnerabilities.
    - Penetration Testing: Conduct simulated attacks to evaluate security resilience.

FlaggGRC

    - Regression Testing: Ensure changes do not introduce new security risks.
- Release and Deployment Stage
    - Secure Deployment: Automated pipelines with security validation checks shall be used.
    - Configuration Hardening: Debug modes and unnecessary features shall be disabled in production.
    - Post-Deployment Security Validation: Conduct vulnerability scans and audits.
    - Patch Management: Establish a process for regular patching and updates.

# Software Change

The software change process shall be documented.

⚙️Software Change Process

# Monitoring

Any exception to this policy shall be approved and recorded by the CISO in advance and reported to the Management Review Team.

# Policy Compliance

## Exceptions

Any exception to this policy shall be approved and recorded by the CISO in advance and reported to the Management Review Team.

## Non-Compliance

Any staff found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment.

## Continual Improvement

This policy is updated and reviewed as part of the continual improvement process.

FlaggGRC