# ISO 27001-Compliant SDLC Procedure Template

## Introduction

This Software Development Lifecycle (SDLC) Procedure aligns with ISO 27001 standards, ensuring the secure and efficient development of software while maintaining compliance with organizational information security objectives. The procedure establishes a structured approach to managing development processes to mitigate risks and protect information assets.

## Purpose

The purpose of this procedure is to define a standardized framework for software development that integrates information security at each stage. This ensures that software solutions meet organizational requirements, comply with legal and regulatory standards, and align with ISO 27001 principles.

## Scope

This procedure applies to all software development activities within the organization, including:

- Internal and external development projects

- Employees, contractors, and third-party developers involved in the SDLC process

- All software systems, applications, and related infrastructure

## Policy Statement

All software development activities shall follow the established SDLC framework to ensure that information security considerations are incorporated at every stage. The procedure includes the following six steps, addressing key security requirements:

- Requirements Analysis: Ensures access control mechanisms are defined and risk assessment is conducted to identify potential threats early.

- Design: Incorporates security-by-design principles, such as data encryption and secure architecture, to mitigate risks during system operation.

- Development: Implements secure coding practices to prevent vulnerabilities like SQL injection or cross-site scripting.

- Testing: Validates security controls through vulnerability assessments and penetration testing, ensuring compliance with organizational standards.

- Deployment: Follows change management protocols to ensure secure configuration and minimize exposure during rollouts.

- Maintenance and Review: Addresses incident management by regularly monitoring for security events and applying updates or patches promptly.

## Roles and Responsibilities

- Development Team: Ensure adherence to secure coding practices and implement the defined SDLC steps.

- Information Security Officer: Oversee the integration of security requirements and conduct regular audits.

- Project Managers: Ensure compliance with the SDLC framework and manage resource allocation.

- Quality Assurance Team: Perform testing and validation to verify security and functionality.

- Third-Party Vendors: Adhere to contractual obligations for secure development practices.

## Compliance and Monitoring

Compliance with this procedure will be monitored through:

- Periodic audits and assessments of development activities

- Regular reviews of development documentation and test results

- Incident reporting and post-mortem analysis of security breaches

- To enhance traceability, a version control system or change log will be maintained, and specific metrics, such as the number of vulnerabilities identified during testing, will be tracked to measure the effectiveness of compliance monitoring.

## Related Documentation

- Information Security Policy

- Risk Assessment Procedure

- Change Management Policy

- Secure Coding Guidelines

## Review and Revision

This procedure shall be reviewed annually or when significant changes to the SDLC process occur. Feedback from audits, incidents, and stakeholders will be incorporated into revisions to ensure continuous improvement. A change log or version control system shall be maintained to track all modifications, ensuring transparency and traceability.

## Narrative Guidance

This SDLC procedure template has been designed to provide a comprehensive yet adaptable framework for integrating information security into software development processes. It reflects the principles of ISO 27001, emphasizing risk management, continuous improvement, and stakeholder involvement. Organizations should tailor this procedure to their unique requirements while maintaining the integrity of the outlined steps and principles.

## Instructions for Use

- Replace placeholder text with organization-specific details.

- Review the template for alignment with existing policies and procedures.

- Engage stakeholders during the customization process to ensure alignment with operational needs and objectives.