# Product Security Procedure Template

## Introduction

This document outlines the procedure for ensuring product security within the organization, aligning with ISO 27001 standards. Secure product development and maintenance are crucial for safeguarding sensitive information and mitigating risks. This procedure supports compliance with ISO 27001

## Purpose

The purpose of this procedure is to define a consistent and comprehensive approach to integrating security into product design, development, and lifecycle management, ensuring that products meet organizational and regulatory security requirements.

## Scope

This procedure applies to all products developed, maintained, or acquired by the organization. It covers employees, contractors, and third-party providers involved in product-related activities, ensuring security considerations throughout the product lifecycle.

## Policy Statement

1. Security requirements must be identified and documented during the product planning phase.
2. Security controls must be integrated into all stages of product development, testing, and maintenance.
3. Identified vulnerabilities must be addressed promptly before product release or updates.
4. Products must undergo regular security assessments and compliance checks.
5. Documentation must be maintained for all security-related activities and findings.
6. Roles and responsibilities must be clearly defined for all stakeholders involved in product security.

## Roles and Responsibilities

* Product Security Team: Implements and monitors security controls during product development and maintenance.
* Development Team: Ensures adherence to security requirements in design and coding practices.
* Information Security Officer: Oversees the product security procedure and approves final security assessments.
* Third-Party Providers: Comply with organizational security policies and participate in security assessments as required.

## Compliance and Monitoring

* Security reviews conducted at key development milestones.
* Regular vulnerability assessments and penetration testing.
* Metrics tracking, such as the number of vulnerabilities identified and resolved per release.
* Audit trails for all security-related activities and decisions.
* Non-compliance incidents must be reported to senior management and corrective actions documented.

## Related Documentation

* Secure Development Policy
* Risk Management Framework
* Vulnerability Management Procedure
* ISO 27001 Standard

## Review and Revision

This procedure will be reviewed annually or in response to significant changes in regulatory requirements, organizational processes, or product technology. The Information Security Officer will initiate and oversee the review process. Updates will be approved by the Information Security Committee and communicated to relevant stakeholders.

# Step-by-Step Product Security Process

## 1. Planning

* Identify security requirements during the product planning phase.
* Define roles and responsibilities for security tasks.
* Develop a security plan outlining key controls and assessment checkpoints.

## 2. Design

* Incorporate security principles into product architecture and design.
* Conduct threat modeling to identify potential risks.
* Review design against organizational and regulatory security requirements.

## 3. Development

* Follow secure coding practices to prevent vulnerabilities.
* Conduct code reviews and static code analysis for security defects.
* Maintain documentation of development processes and security measures implemented.

## 4. Testing

* Perform security testing, including vulnerability scans, penetration tests, and functional security tests.
* Address and remediate identified vulnerabilities before product release.
* Document test results and maintain an audit trail for future reference.

## 5. Release and Deployment

* Conduct a final security assessment before release or deployment.
* Ensure compliance with all organizational and regulatory requirements.
* Maintain documentation of the release, including security approvals.

## 6. Maintenance

* Monitor products for emerging security threats and vulnerabilities.
* Apply patches and updates promptly to address identified issues.
* Conduct periodic security reviews and assessments throughout the product lifecycle.

## Narrative Guidance

This procedure emphasizes a proactive and structured approach to product security. By embedding security into every phase of the product lifecycle, the organization reduces risks and ensures alignment with ISO 27001 principles. Regular reviews, clear accountability, and continuous improvement are critical to maintaining the security and integrity of products.