# ISO 27001-Compliant Security and Vulnerability Management Procedure Template

## Introduction

This Security and Vulnerability Management Procedure aligns with ISO 27001 standards, establishing a systematic approach to identifying, assessing, and mitigating security vulnerabilities in the organization’s systems and applications. The procedure ensures risks associated with vulnerabilities are managed effectively to maintain the confidentiality, integrity, and availability of information assets.

## Purpose

The purpose of this procedure is to provide a structured framework for managing security vulnerabilities. This includes the identification, assessment, remediation, and monitoring of vulnerabilities to reduce risks and maintain compliance with legal, regulatory, and contractual obligations.

## Scope

This procedure applies to all organizational systems, applications, and devices, including:

* Internal and external network infrastructure
* Cloud-based and on-premises systems
* Third-party software and services
* Employees, contractors, and third-party vendors

## Policy Statement

The organization is committed to proactively managing security vulnerabilities to minimize risks to information assets. The procedure includes the following six steps, utilizing frameworks such as the Common Vulnerability Scoring System (CVSS) for assessment and automated tools like vulnerability scanners to enhance identification and prioritization:

1. Vulnerability Identification: Utilize automated tools and manual processes to detect vulnerabilities across all systems and applications.
2. Risk Assessment: Evaluate the potential impact and likelihood of exploitation for identified vulnerabilities, prioritizing them based on severity.
3. Remediation Planning: Develop and implement plans to address identified vulnerabilities, including applying patches, configuration changes, or other mitigations.
4. Implementation: Execute remediation actions in a timely manner, ensuring minimal disruption to business operations.
5. Monitoring: Continuously monitor systems for new vulnerabilities and the effectiveness of remediation efforts.
6. Review and Reporting: Regularly review vulnerability management activities, generate reports for stakeholders, and update processes based on lessons learned.

## Roles and Responsibilities

* Information Security Officer: Oversees the vulnerability management framework and ensures alignment with ISO 27001 requirements.
* IT Operations Team: Conducts vulnerability scans, applies patches, and performs system updates.
* Risk Management Team: Assesses risks associated with identified vulnerabilities and prioritizes remediation efforts.
* Application Development Team: Ensures secure coding practices and addresses vulnerabilities in application code.
* Third-Party Vendors: Comply with organizational requirements for vulnerability management and provide timely updates for their systems or services.

## Compliance and Monitoring

Compliance with this procedure will be ensured through:

* Regular vulnerability scans and penetration tests
* Continuous monitoring for emerging threats and vulnerabilities
* Implementation of key performance indicators (KPIs), such as:

- Percentage of high-severity vulnerabilities resolved within SLA

- Time taken to remediate vulnerabilities

- Number of recurring vulnerabilities identified

The effectiveness of the vulnerability management program will be evaluated by benchmarking against industry standards, reviewing trends over time, and incorporating feedback from audits and incidents.

## Related Documentation

* Information Security Policy
* Incident Response Plan
* Patch Management Policy
* Risk Assessment Procedure

## Review and Revision

This procedure will be reviewed annually or when significant changes occur in the threat landscape, organizational environment, or regulatory requirements. The Information Security Officer will initiate the review process, and updates will be communicated to stakeholders through official channels. All updates will be documented and approved through a formal review process.

## Narrative Guidance

This procedure provides a comprehensive framework for managing security vulnerabilities, emphasizing the principles of risk management and continuous improvement inherent to ISO 27001. Organizations should tailor this template to reflect their specific infrastructure, operational needs, and compliance obligations.

## Instructions for Use

* Replace placeholders with organization-specific details.
* Ensure alignment with related policies and standards.
* Engage stakeholders in the customization process to address unique organizational risks and objectives.