# ISO 27001 Vulnerability Management Policy Template

# 1. Introduction

This document outlines the Vulnerability Management Policy for [Organization Name], ensuring compliance with ISO/IEC 27001:2022 requirements. The policy establishes a framework for identifying, assessing, and mitigating vulnerabilities to protect the organization’s information assets.

# 2. Purpose

The purpose of this policy is to:

- Provide a systematic approach to managing vulnerabilities within the organization.

- Minimize risks associated with known and unknown vulnerabilities.

- Ensure compliance with ISO 27001 and other applicable regulations.

- Protect the confidentiality, integrity, and availability of information assets.

# 3. Scope

This policy applies to all systems, applications, and networks within [Organization Name]. It includes:

- Internal and external infrastructure

- Third-party software and services

- Cloud environments and on-premises systems

# 4. Roles and Responsibilities

- IT Department: Perform vulnerability scans, apply patches, and ensure remediation activities are completed.

- Information Security Officer (ISO): Oversee the vulnerability management program and ensure compliance with ISO 27001.

- System Administrators: Implement security patches and configuration changes as required.

- Risk Management Team: Evaluate the risk posed by vulnerabilities and prioritize mitigation efforts.

# 5. Vulnerability Management Process

5.1 Identification

- Conduct regular vulnerability scans using approved tools (e.g., Nessus, Qualys).

- Monitor threat intelligence feeds and vendor advisories for emerging vulnerabilities.

- Maintain an inventory of all systems and applications subject to vulnerability management.

5.2 Assessment

- Assess vulnerabilities based on severity, likelihood, and potential impact. Use a scoring system, such as CVSS, for standardization.

- Assign risk levels (e.g., low, medium, high, critical) to prioritize remediation efforts.

- Document assessment results in the vulnerability register.

5.3 Remediation

- Develop remediation plans for critical and high-risk vulnerabilities.

- Apply security patches or configuration changes within defined timelines, for example:

- Critical: 24-48 hours

- High: 7 days

- Medium: 30 days

- Low: 90 days

- Verify the effectiveness of remediation through follow-up scans.

5.4 Reporting

- Generate regular reports on vulnerability status and remediation progress.

- Provide updates to executive leadership on significant vulnerabilities and mitigation efforts.

# 6. Exception Management

- Document and approve exceptions for vulnerabilities that cannot be remediated.

- Apply compensating controls to minimize risks associated with exceptions.

- Review and reevaluate exceptions periodically.

# 7. Compliance and Auditing

- Conduct periodic audits to ensure adherence to this policy.

- Non-compliance may result in disciplinary action or escalation to executive leadership.

# 8. Policy Review

This policy will be reviewed annually or whenever significant changes occur in the organization’s infrastructure or regulatory environment. Updates will be coordinated by the Information Security Officer.

# 9. Acknowledgment

All employees, contractors, and third-party vendors must acknowledge receipt and understanding of this policy. Signed acknowledgment forms will be retained for audit purposes.

# Appendices

## Appendix A: Vulnerability Register Template

| Vulnerability ID | Description | Risk Level | System/Application | Remediation Timeline | Status |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Appendix B: Vulnerability Assessment Checklist

| Assessment Area | Question | Response | Notes |
| --- | --- | --- | --- |
|  |  |  |  |

## Appendix C: Policy Acknowledgment Form

I acknowledge that I have read and understood the Vulnerability Management Policy and agree to comply with its requirements.  
  
Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_