ISO 27001 Vulnerability Management Policy Template

Organization Name: [Organization Name]
Version: [Version Number]
Approval Date: [Date]
Last Reviewed: [Date]
Next Review Date: [Date]
Approved By: [Approver's Name and Title]

Purpose

This policy aims to define the approach of [Organization Name] to manage vulnerabilities in our information systems and technology, in compliance with ISO 27001 standards. It outlines the processes for identifying, evaluating, treating, and monitoring vulnerabilities to ensure the confidentiality, integrity, and availability of information assets.

Scope

This policy aims to define the approach of [Organization Name] to manage vulnerabilities in our information systems and technology, in compliance with ISO 27001 standards. It outlines the processes for identifying, evaluating, treating, and monitoring vulnerabilities to ensure the confidentiality, integrity, and availability of information assets.

Policy Statement

[Organization Name] is committed to identifying and managing vulnerabilities in our IT infrastructure and applications as an integral part of our ISMS. We aim to minimize security risks and protect against unauthorized access or compromise of our information assets.

Roles and Responsibilities

Information Security Manager: Oversee vulnerability management processes, report on vulnerabilities and their mitigation to top management.

IT Department: Conduct regular vulnerability assessments, implement security patches, and maintain up-to-date systems.
Employees: Report any identified vulnerabilities or security incidents to the IT department or Information Security Manager.

Identification and Assessment of Vulnerabilities

1. Regular vulnerability scans using approved tools.
2. Evaluation of public vulnerability notifications and advisories.
3. Risk assessment to prioritize vulnerabilities based on potential impact and likelihood.

Response and Mitigation

1. Implementing patches and updates in a timely manner.
2. Applying temporary fixes or workarounds when immediate patching is not feasible.
3. Regular review and testing of the effectiveness of implemented controls.

Monitor and Review

1. Continuous monitoring for new vulnerabilities and threats.
2. Regular reviews of vulnerability management processes.
3. Audit trails and logs to be maintained for all vulnerability management activities.

Reporting

1. Regular reporting to management on vulnerabilities and mitigation efforts.
2. Documentation of all identified vulnerabilities and actions taken.

Training and Awareness

1. Regular training for all staff on security best practices and vulnerability reporting.
2. Awareness campaigns to promote a security-conscious culture.

Review and Improvement

1. Annual review of the Vulnerability Management Policy.
2. Incorporating feedback and lessons learned into policy improvements.

Compliance

1. Adherence to ISO 27001 standards and regulatory requirements.
2. Cooperation with internal and external audits related to vulnerability management.