Vulnerability Management Policy Template

Document Control Information

- **Document Title:** Vulnerability Management Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Vulnerability Management Policy establishes [ORGANIZATION NAME]'s requirements for identifying, assessing, remediating, and monitoring security vulnerabilities in information systems, applications, and infrastructure in accordance with ISO 27001:2022 requirements. It provides a framework for systematically addressing vulnerabilities to reduce security risks.

1.2 Scope

This policy applies to: - All information systems, applications, and infrastructure owned or managed by [ORGANIZATION NAME] - All technology platforms, including servers, endpoints, network devices, cloud services, and applications - All environments, including production, development, test, and disaster recovery - All employees, contractors, and third parties responsible for managing systems and applications - All locations where [ORGANIZATION NAME] operates

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing a comprehensive vulnerability management program - Regularly identifying and assessing vulnerabilities in information systems - Prioritizing vulnerabilities based on risk to the organization - Remediating vulnerabilities in a timely manner according to their severity - Monitoring the effectiveness of vulnerability management activities - Continuously improving vulnerability management processes

2. Vulnerability Identification

2.1 Vulnerability Scanning

- Regular vulnerability scanning shall be performed on all systems and applications
- Scanning frequency shall be based on system criticality:
    - Critical systems: At least monthly
    - High-risk systems: At least quarterly
    - Other systems: At least semi-annually
- Scanning shall be performed after significant changes
- Scanning tools shall be kept up to date
- Scanning shall be performed by qualified personnel
- Scanning shall be authorized and documented
- Scanning results shall be securely stored

2.2 Penetration Testing

- Penetration testing shall be performed on critical systems and applications
- Testing frequency shall be at least annually for critical systems
- Testing shall be performed after significant changes
- Testing shall be performed by qualified personnel
- Testing scope and methodology shall be documented
- Testing shall be authorized and controlled
- Testing results shall be securely stored
- Testing shall not impact production operations

2.3 Threat Intelligence

- Threat intelligence shall be collected and analyzed
- Intelligence sources may include:
    - Vendor security advisories
    - Security mailing lists
    - Industry groups
    - Government agencies
    - Security researchers
    - Commercial threat feeds
- Intelligence shall be assessed for relevance and impact
- Relevant intelligence shall be incorporated into vulnerability management
- Intelligence shall be shared with appropriate stakeholders
- Intelligence effectiveness shall be regularly assessed

2.4 Security Research

- Security research findings shall be monitored
- Research sources may include:
    - Academic publications
    - Security conferences
    - Security blogs and websites
    - Social media
    - Open source intelligence
- Research shall be assessed for relevance and impact
- Relevant research shall be incorporated into vulnerability management
- Research shall be shared with appropriate stakeholders
- Research monitoring effectiveness shall be regularly assessed

3. Vulnerability Assessment

3.1 Vulnerability Validation

- Identified vulnerabilities shall be validated
- Validation shall confirm:
    - Vulnerability existence
    - Applicability to the environment
    - Potential impact
    - Exploitation difficulty
- False positives shall be documented
- Validation shall be performed by qualified personnel
- Validation results shall be documented
- Validation methods shall be appropriate to the vulnerability

3.2 Risk Assessment

- Vulnerabilities shall be assessed for risk
- Risk assessment shall consider:
    - Vulnerability severity
    - System criticality
    - Data sensitivity
    - Exploitation likelihood
    - Potential impact
    - Existing controls
- Risk assessment shall follow established methodology
- Risk assessment shall be documented
- Risk assessment shall inform prioritization
- Risk assessment methodology shall be regularly reviewed

3.3 Vulnerability Prioritization

- Vulnerabilities shall be prioritized based on risk
- Prioritization shall use a defined rating system
- Rating system shall include:
    - Critical: Severe vulnerabilities in critical systems requiring immediate attention
    - High: Significant vulnerabilities requiring prompt attention
    - Medium: Moderate vulnerabilities requiring planned attention
    - Low: Minor vulnerabilities requiring routine attention
- Prioritization shall consider business context
- Prioritization shall be documented
- Prioritization shall inform remediation timeframes
- Prioritization methodology shall be regularly reviewed

4. Vulnerability Remediation

4.1 Remediation Planning

- Remediation plans shall be developed for identified vulnerabilities
- Plans shall include:
    - Remediation actions
    - Required resources
    - Responsible parties
    - Timeframes
    - Testing requirements
    - Verification methods
- Plans shall be documented and approved
- Plans shall be communicated to stakeholders
- Plan progress shall be tracked
- Plan effectiveness shall be assessed

4.2 Remediation Timeframes

- Remediation timeframes shall be based on vulnerability priority:
    - Critical vulnerabilities: [X] days
    - High vulnerabilities: [X] days
    - Medium vulnerabilities: [X] days
    - Low vulnerabilities: [X] days
- Timeframes shall be measured from vulnerability validation
- Timeframes shall be documented and communicated
- Timeframe exceptions shall be approved and documented
- Timeframe compliance shall be monitored

- Timeframes shall be regularly reviewed

4.3 Remediation Methods

- Appropriate remediation methods shall be selected
- Methods may include:
  - Applying patches or updates
  - Implementing configuration changes
  - Deploying additional security controls
  - Implementing workarounds
  - Accepting risk (with approval)
- Method selection shall consider:
  - Effectiveness
  - Impact on operations
  - Resource requirements
  - Implementation timeframe
- Method selection shall be documented
- Method effectiveness shall be verified
- Method selection shall be reviewed for improvement opportunities

4.4 Patch Management

- Security patches shall be applied according to the Patch Management Policy
- Patch deployment shall follow change management procedures
- Patches shall be tested before deployment
- Patch deployment shall be prioritized based on vulnerability risk
- Patch compliance shall be monitored
- Patch exceptions shall be documented and approved
- Patch effectiveness shall be verified
- Patch management shall be regularly assessed

4.5 Compensating Controls

- Compensating controls shall be implemented when immediate remediation is not possible
- Controls shall reduce risk to acceptable levels
- Controls shall be documented and approved
- Controls shall be temporary where possible
- Control effectiveness shall be verified
- Controls shall be regularly reviewed
- Controls shall be removed when remediation is complete
- Control implementation shall follow change management procedures

5. Vulnerability Tracking and Reporting

5.1 Vulnerability Tracking

- A vulnerability management system shall be maintained
- The system shall track:
  - Identified vulnerabilities
  - Validation status
  - Risk assessment
  - Remediation plans
  - Remediation status
  - Verification status
  - Exceptions
- The system shall be regularly updated
- The system shall be accessible to authorized personnel
- The system shall be secured against unauthorized access
- The system shall support reporting and metrics

5.2 Metrics and Reporting

- Vulnerability management metrics shall be defined and collected
- Metrics may include:
  - Vulnerability counts by severity
  - Average time to remediate
  - Remediation compliance rates
  - Aging vulnerabilities
  - Recurring vulnerabilities
  - Exception counts
- Reports shall be generated regularly
- Reports shall be provided to appropriate stakeholders
- Reports shall be used for program improvement
- Metrics and reporting shall be regularly reviewed
- Reporting shall support compliance requirements

5.3 Status Meetings

- Regular vulnerability status meetings shall be conducted
- Meetings shall include appropriate stakeholders
- Meetings shall review:
  - New vulnerabilities
  - Remediation progress
  - Overdue remediations
  - Exceptions

    - Metrics and trends
- Meeting actions shall be documented and tracked
- Meeting frequency shall be appropriate to risk level
- Meeting effectiveness shall be regularly assessed
- Meeting format shall be adjusted as needed

6. Vulnerability Disclosure

6.1 Internal Disclosure

- Vulnerabilities shall be disclosed to internal stakeholders
- Disclosure shall be timely and appropriate
- Disclosure shall include:
    - Vulnerability description
    - Affected systems
    - Potential impact
    - Remediation plans
    - Required actions
- Disclosure shall be to authorized personnel only
- Disclosure shall follow established procedures
- Disclosure effectiveness shall be assessed
- Disclosure procedures shall be regularly reviewed

6.2 External Disclosure

- External vulnerability disclosure shall follow established procedures
- Disclosure may be required for:
    - Customers
    - Partners
    - Regulators
    - Public
- Disclosure shall be approved by management and legal
- Disclosure shall be accurate and timely
- Disclosure shall include appropriate information
- Disclosure shall comply with legal and contractual requirements
- Disclosure shall be coordinated with stakeholders
- Disclosure procedures shall be regularly reviewed

6.3 Responsible Disclosure Program

- A responsible disclosure program shall be established
- The program shall provide a mechanism for external parties to report vulnerabilities

- The program shall include:
    - Reporting channels
    - Scope definition
    - Response timeframes
    - Recognition approach
    - Legal safe harbor provisions
- Reports shall be acknowledged and investigated
- Reporters shall be kept informed of progress
- Program effectiveness shall be regularly assessed
- Program shall be publicly documented

7. Vulnerability Management for Development

7.1 Secure Development

- Security vulnerabilities shall be addressed during development
- Secure development practices shall be followed
- Development shall include:
    - Security requirements
    - Secure coding standards
    - Security testing
    - Code reviews
    - Vulnerability scanning
- Development tools shall include security capabilities
- Development teams shall receive security training
- Development security shall be regularly assessed
- Development security shall align with the Secure Development Policy

7.2 Pre-Release Testing

- Security testing shall be performed before release
- Testing shall include:
    - Vulnerability scanning
    - Static application security testing
    - Dynamic application security testing
    - Penetration testing where appropriate
- Testing results shall be addressed before release
- Critical and high vulnerabilities shall be remediated
- Other vulnerabilities shall be documented and planned
- Testing shall be appropriate to application risk
- Testing shall be documented
- Testing effectiveness shall be regularly assessed

7.3 Third-Party Code

- Third-party code shall be assessed for vulnerabilities
- Assessment shall include:
  - Open source components
  - Commercial libraries
  - Frameworks
  - APIs
- Software composition analysis shall be performed
- Vulnerable components shall be identified and addressed
- Component inventory shall be maintained
- Component updates shall be monitored
- Component selection shall consider security
- Component assessment shall be regularly performed

8. Cloud and Third-Party Vulnerability Management

8.1 Cloud Services

- Cloud service vulnerabilities shall be managed
- Management shall include:
  - Understanding shared responsibility model
  - Implementing customer-side controls
  - Monitoring provider security status
  - Reviewing provider security assessments
  - Implementing additional controls where needed
- Provider security capabilities shall be assessed
- Provider security incidents shall be monitored
- Provider vulnerability management shall be verified
- Cloud security posture shall be regularly assessed

8.2 Third-Party Systems

- Third-party system vulnerabilities shall be managed
- Management shall include:
  - Defining security requirements
  - Assessing security capabilities
  - Reviewing security assessments
  - Monitoring security status
  - Addressing identified vulnerabilities
- Third-party security shall be contractually required
- Third-party security shall be regularly verified
- Third-party security incidents shall be monitored

- Third-party vulnerability management shall align with the Third-Party Security Policy

9. Vulnerability Management Program

9.1 Program Governance

- A vulnerability management program shall be established
- The program shall include:
    - Policies and procedures
    - Roles and responsibilities
    - Tools and technologies
    - Processes and workflows
    - Metrics and reporting
- The program shall be approved by management
- The program shall be adequately resourced
- The program shall be regularly reviewed
- The program shall be continuously improved
- The program shall align with the Information Security Policy

9.2 Tools and Technologies

- Appropriate tools shall be implemented for vulnerability management
- Tools may include:
    - Vulnerability scanners
    - Penetration testing tools
    - Patch management systems
    - Configuration management tools
    - Threat intelligence platforms
    - Vulnerability tracking systems
- Tools shall be properly configured and maintained
- Tools shall be regularly updated
- Tool effectiveness shall be assessed
- Tool selection shall be regularly reviewed
- Tool integration shall be implemented where appropriate

9.3 Continuous Improvement

- The vulnerability management program shall be continuously improved
- Improvement shall be based on:
    - Performance metrics
    - Industry best practices
    - Lessons learned

    - Audit findings
    - New technologies
    - Changing threats
- Improvement initiatives shall be documented
- Improvement progress shall be tracked
- Improvement effectiveness shall be assessed
- Improvement shall be a program objective
- Improvement shall be regularly reviewed

10. Roles and Responsibilities

10.1 Management

- Approve vulnerability management policy
- Provide resources for vulnerability management
- Review vulnerability management performance
- Address significant vulnerability issues
- Support vulnerability management initiatives
- Ensure compliance with requirements
- Approve risk acceptance when necessary

10.2 Information Security Team

- Develop and maintain vulnerability management policy
- Oversee vulnerability management program
- Coordinate vulnerability assessments
- Prioritize vulnerabilities
- Monitor remediation progress
- Report vulnerability status
- Provide security expertise
- Coordinate with stakeholders

10.3 IT Operations Team

- Implement vulnerability remediation
- Apply patches and updates
- Implement configuration changes
- Deploy security controls
- Verify remediation effectiveness
- Report remediation status
- Maintain system security
- Support vulnerability assessments

10.4 Development Team

- Address vulnerabilities in code
- Implement secure coding practices
- Perform security testing
- Remediate identified vulnerabilities
- Report remediation status
- Maintain component security
- Support vulnerability assessments
- Implement security requirements

10.5 System Owners

- Approve vulnerability remediation plans
- Allocate resources for remediation
- Accept residual risk when necessary
- Ensure timely remediation
- Report remediation status
- Support vulnerability assessments
- Maintain system security
- Comply with vulnerability management requirements

11. Compliance and Exceptions

11.1 Compliance Monitoring

- Compliance with this policy shall be regularly monitored
- Monitoring shall include:
  - Scanning coverage
  - Remediation timeliness
  - Exception management
  - Documentation completeness
- Non-compliance shall be addressed
- Compliance reports shall be provided to management
- Compliance trends shall be analyzed
- Compliance monitoring shall be regularly reviewed

11.2 Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate - Tracked in the vulnerability management system - Reported in vulnerability management metrics - Minimized to the extent possible

12. Related Documents

- Information Security Policy
- Patch Management Policy
- Change Management Policy
- Risk Management Policy
- Secure Development Policy
- Third-Party Security Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

13. Approval

This Vulnerability Management Policy is approved by:

Name: _________________________ Position: _______________________ Date: __________________________ Signature: ______________________