# Vulnerability Management Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### **S**ecurity boundary under scope

1. [List of applicable systems]

### References

1. ISO 29147: <https://www.iso.org/standard/72311.html>
2. NIST SP 800-40: <https://csrc.nist.gov/pubs/sp/800/40/r4/final>
3. ISO/IEC 27001:2022: A.5.7, A.7.13, A.8.8
4. NIST 800-53 rev. 5: CM-4, MA-3(2), RA-5, RA-5(2), RA-5(3), RA-5(11), SA-11(2), SA-22, SI-2, SI-2(2), SI-4(2), SI-3, SI-5, SI-16, SR-11, SR-11(1), SR-11(2)
5. CIS v8: 7.1, 7.3, 7.4, 7.5, 7.6, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 16.2, 16.6, 16.14
6. PCI DSS 4.0: 5.1.1, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.2.1, 6.3.1, 6.3.3, 6.4.1, 9.1.5.2, 9.1.5.2.1, 11.3.1, 11.3.1.1, 11.3.1.2, 11.3.1.3, 11.3.2, 11.3.2.1, 11.4.4
7. AICPA SOC 2 TSC: CC2.1, CC3.2, CC6.8, CC7.1, CC7.3

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

The purpose of this Vulnerability Management Policy is to establish a comprehensive framework for identifying, evaluating, and mitigating vulnerabilities in the organization's information systems, applications, and network infrastructure. This policy aims to protect the organization's assets, data, and reputation by ensuring systematic and proactive management of security vulnerabilities. By implementing robust vulnerability management practices, the organization seeks to minimize the risk of security incidents, unauthorized access, and data breaches, thereby maintaining the confidentiality, integrity, and availability of its information resources.

## Scope

This policy applies to all employees, contractors, consultants, temporary staff, and any other personnel with access to [Organization]'s information systems, applications, and network infrastructure. It covers all organizational assets, including but not limited to:

* Servers, desktops, laptops, and mobile devices
* Network devices such as routers, switches, and firewalls
* Software applications, both in-house developed and third-party
* Cloud services and infrastructure
* Physical ports, jacks, and other network access points

The scope of this policy includes the following key areas of vulnerability management:

* Vulnerability scanning
* Threat and vulnerability feeds and organizational awareness
* Threat detection
* Patch management
* Malicious code protection for devices, systems, and networks
* Integration with security monitoring and incident response management
* Reviewing and testing code, components, and new systems for vulnerabilities prior to deployment
* Detection and prevention of tampering and counterfeit devices, software, and system components

All organizational units and personnel are required to adhere to the guidelines and procedures outlined in this policy to ensure a consistent and effective approach to managing vulnerabilities across the organization.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], **[owner title]** | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | **Executive Team** | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | **Executive Team** | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], **[Information officer title]** | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], **Operational owner title]** |  |
| Information Systems Administrators | **System Administrators**  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], **[HR title]** | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  **End Users** | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | **[provider type]** | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
	2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. **Vulnerability Scanning**: The process of identifying and assessing vulnerabilities in systems, networks, and applications through automated tools and methodologies.
	2. **Threat Intelligence Feeds**: Sources of information providing timely data on current threats, vulnerabilities, and risks, aiding in proactive defense measures.
	3. **Continuous Monitoring**: An ongoing process of observing, detecting, and analyzing security events to identify potential threats and vulnerabilities in real-time.
	4. **Intrusion Detection Systems (IDS)**: Tools or software designed to monitor network traffic for suspicious activity and known threats, issuing alerts when such activities are detected.
	5. **Patch Management**: The process of managing updates for software, applications, and systems to fix vulnerabilities and improve security.
	6. **Malicious Code Protection**: Mechanisms deployed to prevent, detect, and remediate malware infections on devices, systems, and networks.
	7. **Security Information and Event Management (SIEM)**: A solution providing real-time analysis of security alerts generated by hardware and software applications, integrating various monitoring and logging tools.
	8. **Code Review**: A systematic examination of computer source code intended to find and fix mistakes overlooked in the initial development phase, improving the overall quality of software.
	9. **Security Testing**: Testing methodologies including static application security testing (SAST) and dynamic application security testing (DAST) to identify vulnerabilities in applications before deployment.
	10. **Continuous Integration/Continuous Deployment (CI/CD)**: Practices of automating the integration of code changes from multiple contributors into a shared repository and automatically deploying the application to production environments.
	11. **Penetration Testing**: Simulated cyberattacks on systems, networks, or applications to identify vulnerabilities that could be exploited by attackers.
	12. **Tampering**: Unauthorized alteration or interference with devices, software, or system components that compromises their integrity and security.
	13. **Counterfeit Components**: Unauthorized copies or substitutes of genuine hardware or software, often of inferior quality, which pose security risks.
	14. **Chain of Custody**: A process that tracks the handling of devices, software, or system components from procurement through delivery, ensuring security and integrity at each stage.
	15. **Procurement Controls**: Measures and policies in place to ensure that all purchased hardware, software, and system components are sourced from trusted and verified suppliers.
	16. **Inspection and Testing**: Procedures to examine and test incoming hardware and software for authenticity, integrity, and absence of tampering or counterfeiting.
	17. **Automated Testing Tools**: Software tools that perform automated security tests on code, systems, and components to identify vulnerabilities and ensure compliance with security standards.
	18. **Incident Response**: A structured approach to handle and manage the aftermath of a security breach or attack, including identification, containment, eradication, recovery, and documentation of the incident.
	19. **Configuration Scans**: Scans performed to check system and network configurations for compliance with security policies and to identify potential security misconfigurations.

## Policy

#### Vulnerability Scanning

##### Scheduled Scanning:

* + - 1. The [responsible party] shall perform regular vulnerability scans on all devices, systems, and applications at least biweekly.
			2. Quarterly configuration scans shall be conducted specifically for the cloud infrastructure used for customer services.

##### Ad Hoc Scanning:

* + - 1. Vulnerability scans shall also be performed on a by-request or as-needed basis, particularly after significant system changes, newly identified threats, or post-incident.

##### Tools and Methodologies:

* + - 1. The [responsible party] shall employ accredited and up-to-date vulnerability scanning tools and techniques.
			2. Ensure tools are capable of enumerating platforms, software flaws, and configurations accurately.

#### Threat and Vulnerability Feeds and Organizational Awareness

##### Subscription to Threat Feeds:

* + - 1. The [responsible party] shall subscribe to relevant threat intelligence feeds, including US-CERT, CISA, and other industry-specific sources.

##### Threat Awareness:

* + - 1. The [responsible party] shall disseminate critical threat intelligence to relevant stakeholders promptly.
			2. The [responsible party] shall update scanning tools and processes within 24 hours of receiving new threat information.

##### Public Disclosure Program:

* + - 1. The [responsible party] shall establish a channel for public reporting of vulnerabilities, ensuring timely investigation and remediation.

#### Threat Detection

##### Continuous Monitoring:

* + - 1. The [responsible party] shall implement continuous monitoring mechanisms to detect attacks and indicators of potential attacks.
			2. Utilize intrusion detection systems (IDS), boundary protection, and log anomaly detection tools.

##### Event Analysis:

* + - 1. The [responsible party] shall regularly analyze detected events and anomalies to adjust monitoring strategies and improve threat detection accuracy.

#### Patch Management

##### Patch Deployment:

* + - 1. The [responsible party] shall ensure that all critical patches are applied within five days of release.
			2. High, medium, and low-severity patches should be applied within 30, 90, and 180 days respectively.

##### Patch Testing and Validation:

* + - 1. The [responsible party] shall ensure all patches are tested in a controlled environment before deployment to production systems.
			2. Post-deployment, verify patch effectiveness through additional scans and monitoring.

#### Malicious Code Protection

##### Protection Mechanisms:

* + - 1. The [responsible party] shall deploy signature-based and non-signature-based malicious code protection mechanisms at system entry and exit points.
			2. Configure these mechanisms to perform real-time and periodic scans, blocking and quarantining detected malicious code.

##### Automatic Updates:

* + - 1. The [responsible party] shall ensure malicious code protection tools are updated automatically in line with new releases and organizational policies.

#### Integration with Security Monitoring and Incident Response Management

##### Integration with SIEM:

* + - 1. The [responsible party] shall integrate vulnerability management tools with the Security Information and Event Management (SIEM) system for centralized monitoring and correlation of security events.

##### Incident Response:

* + - 1. The [responsible party] shall establish a clear incident response workflow for addressing vulnerabilities, including detection, analysis, remediation, and post-incident review.
			2. The [responsible party] shall ensure incidents are logged, and lessons learned are documented and acted upon to prevent recurrence.

#### Reviewing and Testing Changes for Vulnerabilities

##### Code Review Process:

* + - 1. The [responsible party] shall implement a review process for all new code and significant changes to existing code for common vulnerabilities in code.
			2. Ensure code reviews are conducted by knowledgeable personnel, leveraging automated tools where appropriate.

##### Component and System Review:

* + - 1. The [responsible party] shall conduct thorough reviews and testing of all new components and systems before deployment to identify and mitigate potential vulnerabilities.
			2. Utilize both manual and automated testing methods to ensure comprehensive coverage.

##### Security Testing:

* + - 1. The [responsible party] shall conduct security testing, including static application security testing (SAST) and dynamic application security testing (DAST), on all applications before deployment.
			2. The [responsible party] shall perform or retain services for regular penetration testing to identify vulnerabilities in applications, systems, and networks.

##### Automated Testing:

* + - 1. The [responsible party] shall utilize automated testing tools to ensure consistent and thorough testing of code, components, and system integrity.
			2. Incorporate automated tests into the continuous integration/continuous deployment (CI/CD) pipeline to catch vulnerabilities early in the development lifecycle.

#### Tampering and Counterfeit Protection

##### Procurement Controls:

* + - 1. The [responsible party] shall source all hardware, software, and system components from trusted, verified suppliers.
			2. The [responsible party] shall establish contractual obligations with suppliers to guarantee the authenticity and integrity of products.

##### Inspection and Testing:

* + - 1. The [responsible party] shall implement inspection and testing procedures for all incoming hardware and software to detect signs of tampering or counterfeiting.
			2. The [responsible party] shall utilize tools and techniques such as hash verification, digital signatures, and physical inspections to validate authenticity.

##### Chain of Custody:

* + - 1. The [responsible party] shall maintain a documented chain of custody for all critical components from procurement through delivery, installation, and deployment.
			2. The [responsible party] shall ensure all personnel handling these components are trained in secure handling practices.

##### Monitoring:

* + - 1. The [responsible party] shall regularly monitor and audit the supply chain to identify and mitigate risks related to tampering and counterfeiting.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |