Vulnerability Management Policy Template

[Organization Name]
Document Version: [Version Number]
Date: [Date of Creation]

Purpose

This policy aims to establish a framework for identifying, assessing, and managing vulnerabilities within [Organization Name]'s information systems and networks to protect sensitive data and maintain operational integrity.

Scope

This policy applies to all employees, contractors, and third-party vendors of [Organization Name] who access, manage, or control company technology resources.

Contents

- *Endpoint Protection*
- *Logging & Alerting*
- *Patch Management*
- *Vulnerability Scanning*

Endpoint Protection (Anti-Virus & Malware)

- Every Information Resource owned or managed by *[Company-Name]* is required to utilize endpoint protection software and configuration approved by *[Company-Name]* IT management.
- Workstations and laptops not owned by *[Company-Name]* must have endpoint protection software and configuration approved by *[Company-Name*] IT management installed before connecting to any *[Company-Name]* Information Resource.
- Altering, bypassing, or disabling the endpoint protection software is prohibited.
- Email gateways must employ email virus protection software approved by *[Company-Name]* IT management, and must comply with *[Company-Name]* guidelines

for setting up and using this software. This includes mandatory scanning of all incoming and outgoing emails.

- Measures must be in place to prevent or detect access to websites that are known or suspected to be malicious.
- All files received via networks or from external storage devices must undergo malware scanning before they are used.
- Any virus that is not automatically removed by the virus protection software must be treated as a security incident and reported to *[Company-Name]* IT Support.

Logging & Alerting

- Baseline configurations for Information Resources should include log settings that capture activities pertinent to information security.
- Event logs should be generated following the *[Company-Name]* Logging Standard and forwarded to a centralized log management system.
- There should be regular reviews of log files.
- Any exceptions or irregularities found during reviews of log files should be recorded and examined.
- *[Company-Name]* will employ file integrity monitoring or change detection tools on logs and critical files to notify staff of any unauthorized alterations.
- Measures must be in place to safeguard log files against alteration or unauthorized access.
- To ensure uniform timestamps in logs, all servers and network devices should synchronize their time settings regularly with a single reference time source.
- Log files should be retained for a minimum duration of one year.

Patch Management

- The IT team at *[Company-Name]* is charged with the comprehensive management, operation, and establishment of procedures for patch management.
- Regular scans are required for all Information Resources to detect any missing updates.
- Each missing software update must undergo a risk evaluation to determine its impact on *[Company-Name]*.
- Software updates deemed to present an unacceptable risk to *[Company-Name]* Information Resources must be applied within a timeframe appropriate to the identified risk, as decided by *[Company-Name]*.

- Prior to broad application, software updates and configuration modifications to Information Resources need to be thoroughly tested and implemented following *[Company-Name]* guidelines.
- Confirmation of successful deployment of software updates should be carried out within a timeframe deemed reasonable by *[Company-Name]*.

Vulnerability Scanning

- Scans for vulnerabilities in both the internal and external network should take place at a minimum of every three months or following any substantial modifications to the network.
- If a vulnerability scan identifies risks deemed Critical or High, these must be addressed and the system rescanned until all such risks are eliminated.
- Should any signs of compromised or exploited Information Resources be discovered during a scan, this must be communicated to the Information Security Officer and IT support of the company.
- When new vulnerabilities are identified, the configuration standards will be revised to reflect these findings.

Enforcement

Employees who breach this policy could face disciplinary measures, potentially leading to job termination, along with possible civil or criminal consequences. Vendors, consultants, or contractors in violation may face penalties including but not limited to the revocation of access rights, contract termination, and associated civil or criminal repercussions.

Version History

Version	Modified Date	Approved Date	Approved By	Comments
