Policy number	Title:	Effective Date:
<your ID format>	VULNERABILITY MANAGEMENT POLICY	<your date format>

REFERENCE

- ISO 27002: 12, 18,
- NIST CSF: PR.IP-12, DE.AE-2, 3, DE.CM-1, 4, 6, 8

SUPPORTING DOCUMENTS

- **This is a contents link space for any related documentation.**

CONTENTS

PURPOSE

The purpose of the **<company name>** Vulnerability Management Policy is to establish the rules for the review, evaluation, application, and verification of system updates, and to mitigate vulnerabilities in the IT environment and the risks associated with them.

SCOPE

This policy encompasses all systems, automated and manual, for which **<company name>** has administrative responsibility, including systems managed or hosted by third parties on behalf of **<company name>**. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

POLICY

Scanning and Penetration Testing

- Penetration testing of the internal network, external network, and hosted applications must be conducted at least annually or after any significant changes to the environment.
- Any exploitable vulnerabilities found during a penetration test will be corrected and re-tested to verify the vulnerability was corrected.
- All systems must be penetration tested and scanned for vulnerabilities before being installed in production, and periodically thereafter.
- Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by a **<designated security representative>**
- Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested, and always followed to minimize the possibility of disruption.
- Where **<company name>** has outsourced a system to another entity or a third party, vulnerability scanning/penetration testing must be coordinated.

Patching Management

- The **<company name>** IT team maintains overall responsibility for patch management implementation, operations, and procedures.
- **<company name>** IT will provide a **<Patch Management Plan>**
- All Information systems must be scanned on a regular basis to identify missing updates.
- All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.
- Software updates and configuration changes applied to information systems must be tested prior to widespread implementation and must be implemented in accordance with a **<Change Management Policy>**
- All missing software updates must be evaluated according to the risk they pose to **<company name>**.
- All security patches must be reviewed, evaluated, and appropriately applied in a timely manner. This process must be automated, where technically possible.
- Systems which can no longer be supported or patched to current versions must be removed.

Endpoint Protection and Detection

- All **<company name>** owned and/or managed information systems must use the **<company name>** IT approved endpoint protection software and configuration.
- Controls must be in place to detect the connection of removable media.
- Controls must be in place to prevent or detect the use of known or suspected malicious websites.
- Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound, and internal network traffic.
- All files received over networks, or from any external storage device can only be opened on systems with company sanctioned endpoint protection.
- Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

Disabling Endpoint Protection

- The endpoint protection software must not be altered, bypassed, or disabled.
- Controls must be in place to detect the bypassing or disabling of endpoint protection.
- Any exception where endpoint protection is altered, bypassed, or disabled must be justified and documented in a Change Request made in accordance with a **<Change Management Policy>**

Logging & Alerting

- Documented baseline configurations for information systems must include log settings to record actions that may affect, or are relevant to, information security.
- Event logs must be produced based on a **<Logging Standard>** and sent to a central log management solution.
- A review of log files must be conducted periodically **<state timeframe>**
- All exceptions and anomalies identified during the log file reviews must be documented and reviewed.
- Log files must be protected from tampering or unauthorized access.
- All servers and network equipment must retrieve time information from a single reference time source on a regular basis so that timestamps in logs are consistent.
- All log files must be maintained for at least one year.

DATE ISSUED/DATE REVIEWED

_____

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY