[INSERT FIRM LEGAL NAME]

Threat and Vulnerability Management Policy

[Insert Firm Logo]

Version 1.0

[Insert Date]

This document is proprietary and confidential. The document and information contained herein may not be shared outside of [Insert Firm Legal Name] unless approved by authorized personnel.

Contents

Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company-specific document. **Otherwise, it would be a liability exposure to establish a policy and not to comply with it.**

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

Delete the instructions after finalizing and adopting the policy.

Policy Overview

Vulnerability assessments are an essential part of the daily operations of a company. These vulnerabilities include but are not limited to network, hardware, and software. The increasing number of threats, risks, and responsibilities necessitates a regular scan of the network for vulnerabilities.

Policy Detail

Endpoint Protection

The use of the approved endpoint protection software and configuration is mandatory for all organization owned and/or managed Information Resources. The use of approved endpoint protection software and configuration is also mandatory for any non-organization-owned workstations and laptops connecting to an organization's Information Resource.

Each email gateway must utilize IT management-approved email virus protection software and adhere to the organization rules for the setup and use of this software, which includes, but is not limited to, the scanning of all inbound and outbound emails.

All files received over networks or from any external storage device must be scanned for malware before use. This includes webpages, emails, documents, and executables. Once verified that a file is clean, it must not be opened or executed until it has been scanned again and found to be free of malware.

Each new virus that is not cleaned by the virus protection software constitutes a security violation and should be reported to IT Support immediately.

Logging & Alerting
Information Resources must be documented to include baseline configurations. Event logs must be produced based on the organization logging standard and sent to a central log management solution.

The review of log files should be conducted periodically. Exceptions and anomalies identified during the log file reviews must be documented and reviewed.

The organization will use file integrity monitoring or change detection software on logs and critical files to alert personnel to unauthorized modification. 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. Time synchronization is critical for forensic analysis, and logs that are not properly synchronized can complicate investigations. A compromise of a network device or server should be reported immediately to designated personnel in order to minimize risk and ensure continuity of operations. All log files must be maintained for at least one year.

Patch Management
Efficient patch management is critical to the integrity of the systems and data. There is a responsibility to ensure that information resources are scanned on a regular basis to identify missing updates, so that action can be taken, as needed.

All missing software updates must be reviewed according to the risk they pose to the organization and implemented within a time period that is commensurate with the risk as determined by the Patch and Vulnerability Standard.

Software updates and configuration changes applied to the Information Resources must be tested prior to widespread implementation and must be implemented in accordance with the Change Control Policy. The organization patch and vulnerability standard defines a reasonable time period for verification of successful software update deployment.

Penetration Testing
Penetration tests 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 fully repaired.

Vulnerability Scanning

Vulnerability scanning must be conducted on the internal and external network at least quarterly or after any significant change to the network. If a vulnerability scan of any asset returns at least one critical or high risk, then it must be remediated and re-scanned until all critical and high risks are resolved.

The organization is committed to protecting the confidentiality, integrity, and availability of its data. Any evidence of a compromised or exploited information resource during vulnerability scanning must be reported to the organization's information security officer and IT support. Upon identification of new vulnerability issues, configuration standards will be updated accordingly.

Scope and Purpose

Scope

The Threat and Vulnerability Management Policy applies to individuals who are responsible for Information Resource management. The Policy provides guidance on how vulnerabilities will be identified, prioritized, and managed. This policy fulfills the organization’s obligation to its community by protecting information systems from misuse and unauthorized access by threatening entities (e.g., viruses and hackers).

Purpose

The purpose of this policy is to establish standards for periodic vulnerability assessments. This policy reflects the organization’s commitment to identify and implement security controls, which will keep risks to information system resources at reasonable and appropriate levels. The completion of periodic vulnerability assessments will be an integral part of the maintenance and upgrading procedures for all software within the organization.

Compliance

The Information Security team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Exceptions

Any exception to the policy must be approved by the Information Security team in advance.

Revision Table

Revision History				
#	**Version #**	**Date**	**Updates/Changes**	**Owner**
1	1.0	2023	Initial Draft	Riskigy
2				