#

# Threat and Vulnerability Management Policy Template

## Policy Statement

This policy establishes the framework for managing threats and vulnerabilities within [Organization Name], ensuring that potential security issues are identified, assessed, and mitigated in a timely and effective manner.

## Purpose

The purpose of this policy is to protect [Organization Name]'s information assets from threats and vulnerabilities that could compromise their confidentiality, integrity, or availability.

## Scope

Applies to all employees, contractors, and third-party users of [Organization Name]'s IT systems and data.

## Policy Owner

The Chief Information Security Officer (CISO) is responsible for overseeing the implementation and adherence to this policy.

## Definitions

* **Threat:** Any circumstance or event with the potential to adversely impact organizational operations.
* **Vulnerability:** Weakness in an information system, system security procedures, internal controls, or implementation.

## Roles and Responsibilities

* **CISO:** Oversees threat and vulnerability management.
* **IT Department:** Conducts regular scans, assessments, and mitigation activities.
* **Employees:** Report security incidents and comply with policy requirements.

## Threat and Vulnerability Identification

* Regular scans of IT infrastructure.
* Use of threat intelligence sources.
* Employee training to identify potential threats.

## Assessment and Prioritization

* Assess identified threats and vulnerabilities based on potential impact and likelihood.
* Prioritize remediation activities based on risk level.
* The process for managing vulnerabilities should be evaluated at least once every year, or whenever there are substantial changes in the organization.
* The IT department is responsible for keeping track of vulnerability alerts and new threats that could affect the company's asset inventory.
* Vulnerability scans must be conducted on all systems that are part of the company's network.

## Mitigation and Remediation

* Develop and implement a remediation plan for high-risk vulnerabilities.
* Apply security patches and updates regularly.
* Operating systems should be set up for automatic updates, except when a different authorized patching method is employed.
* Applications should be set up for automatic updates, except when a different authorized patching method is employed.
* It is the responsibility of all enterprise asset users to promptly install updates for business systems and applications.
* All users are required to execute necessary reboots promptly to guarantee the effective installation of updates.
* Addressing high severity vulnerabilities must be treated as a high priority.

## Monitoring and Reporting

* Continuous monitoring for new threats and vulnerabilities.
* Regular reporting to the CISO and relevant stakeholders.
* The IT department is advised to sign up for a service that provides alerts about new patches and software updates.
* Should there be a delay in resolving vulnerabilities, IT is obligated to inform the decision-makers.
* IT is required to produce a monthly report detailing the current status of all identified vulnerabilities in the organization.

## Training and Awareness

* Regular training sessions for employees on threat and vulnerability management.
* Awareness campaigns on current cybersecurity threats.

## Policy Review and Update

* Annual review of the policy or after significant changes in the IT environment.
* Updates as necessary to address new threats and technologies.

## Compliance

* Failure to comply with this policy may result in disciplinary action.
* Regular audits to ensure compliance with the policy.

## Incident Response

* Clear procedures for responding to detected threats.
* Coordination with the Incident Response Team for serious incidents.

## Revision History

Each time this document is updated, this table should be updated.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Revision Description** | **Name** |
|  |   |   |   |
|  |   |   |   |
|  |   |   |   |
|  |   |   |   |
|  |   |   |   |
|  |   |   |   |

## Policy Approval

Approved by: [Approver's Name]

Position: [Approver's Position]

Date: [Date of Approval]