Vulnerability Management Standard

Purpose

Vulnerability management is the process of searching for, prioritizing, and remediating vulnerabilities in enterprise systems and software. The Vulnerability Management Operational Standard provides the processes and procedures for ensuring enterprise assets do not contain vulnerabilities. This policy applies to all departments and all assets connected to the enterprise network.

Responsibility

The IT business unit is responsible for all vulnerability management functions. Specifically, administrators are responsible for assessment and application of patching. Necessary vulnerability information must be relayed to other business units within the enterprise such as finance, accounting, and cybersecurity as required or needed. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them, such as applying updates in a regular manner or restarting their systems.

Exceptions

Exceptions to this policy are likely to occur. Requests for exceptions may include to not scan a device, or additional time to remediate vulnerabilities, or to let certain systems function normally with vulnerabilities in place. Exception requests must be made in writing and must contain:

- The reason for the request,
- Risk to the enterprise of not following the written policy,
- Specific mitigations that will not be implemented,
- Technical and other difficulties in applying patches, and
- Date of review

Standard

Assess

1. A process for performing vulnerability management must be established.
    a. This process must be documented and approved.
    b. At a minimum, the vulnerability management process must be reviewed on an annual basis or following significant changes within the enterprise.
    c. IT must monitor vulnerability announcements and emerging threats applicable to enterprise asset inventory.
    d. All systems connected to the enterprise network must be scanned for vulnerabilities.

Prioritize

1. Identified vulnerabilities must be prioritized, with more critical vulnerabilities addressed first.

Remediate

1. A process for remediating identified vulnerabilities must be established.
    a. This process must be documented and approved.
    b. At a minimum, this process must be reviewed on an annual basis or following significant changes within the enterprise.
    c. Vulnerabilities that cannot be remediated must be submitted through the vulnerability exception process.
2. Operating systems must be configured to automatically update, unless an alternative approved patching process is used.

3. Applications must be configured to automatically update, unless an alternative approved patching process is used.
4. All users of enterprise assets have a duty to install updates for business systems and applications in a timely manner.
5. All users must ensure required reboots occur within a reasonable timeframe to ensure updates are properly installed.
6. High severity vulnerabilities must be addressed as a matter of priority.

Monitor

1. IT should subscribe to a threat information service to receive notifications of recently released patches and other software updates.
2. IT must notify the decision-making authority if vulnerabilities are not mitigated in a timely manner.
3. Every month, IT must create a report containing the status of all known vulnerabilities within the enterprise.

Revision History

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

Version	Revision Date	Revision Description	Name
V1.0	01/02/2023	Initial Written Standard	Scott Tisinger