University System of New Hampshire

VULNERABILITY AND PATCH MANAGEMENT STANDARD

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: ET&S Cybersecurity GRC
Approved Distribution: Public
Status: In Force

1. Purpose and Overview

Vulnerability and Patch Management, the practice of identifying, classifying, remediating, and mitigating vulnerabilities, is a critical component of USNH's defense-in-depth information security strategy. This standard represents the minimum requirements for vulnerability management on all USNH information technology systems.

2. Scope and Audience

All USNH systems must serve the mission of the University System of New Hampshire and operate in accordance with all University System of New Hampshire policies. Systems managed contrary to USNH's mission or that are not compliant with the minimum-security standards defined in this standard may be subject to disconnection from the USNH network. All USNH employees responsible for administering systems that require vulnerability scanning per the scope outlined above, shall be familiar with this standard and understand how the requirements outlined here affect their job responsibilities. This document describes the requirements for maintaining up-to-date system security patches on all USNH owned and managed workstations, systems, and servers.

3. Standard

In compliance with USNH policy, all information systems and their applicable components must be scanned for vulnerabilities and identified vulnerabilities must be remediated according to the schedule outlined in this standard. ET&S Cybersecurity Operations (CyberOps) administers the vulnerability management program as well as the processes and tools that support it.

In all things pertaining to Vulnerability Management, the CyberOps team, led by the Director of Cybersecurity Operations, Engineering, and IAM, has the authority to take action, as needed, to ensure that systems containing known vulnerabilities do not pose a threat to USNH and its resources. To that end, CyberOps may modify or override any provision in this standard, without prior notification or publication, if deemed necessary to mitigate the potential for loss or damage presented by a vulnerability. The approval of the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO) or those delegated to act on their behalf is required in these circumstances.

VULNERABILITY SCANNING:

ET&S Cybersecurity Operations is responsible for conducting vulnerability scans using industry standard tools and methodologies to identify vulnerabilities, such as software flaws and insecure configurations.

Types of Vulnerability Scans:

External Vulnerability Scans are performed outside the USNH network to identify vulnerabilities in network structures. The frequency of scans is based on industry standards such as the NIST 800-171 requirements.

Internal Vulnerability Scans are conducted to identify vulnerabilities inside the USNH network. The frequency of scans is based on industry standards such as the NIST 800-171 requirements.

Penetration Testing occurs when testers target an application or other components to determine if vulnerabilities can be exploited to compromise the application or its data.

Web Application Scans are automated assessment tools that search for vulnerabilities within web applications.

System Administrators and Service Owners shall enable the installation of required scanning agents on all information systems to enable authenticated (agent-based) vulnerability scanning.

ET&S Cybersecurity Operations will maintain a vulnerability management scanning calendar for transparency and planning. The vulnerability management calendar will be integrated with the ET&S Change Management process and will outline when scans are taking place, the type of scan being conducted, and the target of the scan. The frequency of scans is based on industry standards such as the NIST 800-171 requirements.

All information systems shall be scanned at a set frequency at a minimum of once a year. Additional scans are determined by the security categorization of the service or application supported by the information system. USNH utilizes both passive and active scanning tools. For more information on security categorization, contact the CyberOps team.

Results from each vulnerability scan, including details about the vulnerability, its classification, and any details for remediation, shall be made available to the appropriate System Administrator for remediation. Results are classified as restricted data and will be managed by the CyberOps team.

VULNERABILITY REMEDIATION

Vulnerabilities classified as Critical or High on information systems must be remediated in accordance with the standards outlined below. Those that cannot or will not be remediated must have a documented, approved exception following the exception process.

Vulnerability Classifications

The following classifications, based on the industry standard Common Vulnerability Scoring System (CVSS v3), describe the severity levels that can be assigned to a vulnerability.

Critical: Vulnerabilities that can be easily exploited by a remote, unauthenticated attacker and lead to a complete system compromise without requiring user-interaction are rated as Critical. Critical vulnerabilities pose the highest risk for a system-wide compromise of the network. Vulnerabilities are not rated as Critical if they require a local user, an authenticated remote user, or an unlikely configuration to be exploited. Vulnerabilities with a CVSS score of 9.0- 10.0 are automatically assigned the Critical classification.

High: Vulnerabilities that can easily compromise the confidentiality, integrity, or availability of resources are rated as High. They allow privileged escalation, access to resources that should otherwise be protected by authentication, arbitrary remote code execution, or a denial of service to legitimate users. Vulnerabilities identified based on vendor security advisories that do not yet have a CVE or that do not have a NIST score are automatically assigned this classification. Vulnerabilities with a CVSS score of 7.0-8.9 are automatically assigned the High classification.

Medium: Vulnerabilities that are more difficult to exploit but can still result in a security incident under certain, specific circumstances are rated as Medium. These software flaws could have a critical impact on IT resources but require attackers to be highly sophisticated or for the system where the vulnerability is present to be configured in an unlikely state. Vulnerabilities with a CVSS score of 4.0-6.9 are automatically assigned to the medium classification.

Low: Vulnerabilities that result in minimal impacts and consequences when exploited are rated as Low. They require extremely unlikely circumstances and configurations to be exploited. Low vulnerabilities can be used by attackers to gather information about systems. Vulnerabilities with a CVSS score of 0.1-3.9 are automatically assigned the Low classification.

Informational: Vulnerabilities that do not pose an immediate threat to the host or the USNH network. These vulnerabilities refer mostly to weaknesses in a device that allows an intruder access to information that may be used in the future to compromise the server.

The CyberOps team may reclassify vulnerabilities, when necessary, based on any compensating controls in place and calculated risks levels.

Remediation Timeline

The timeline for remediation begins once a vulnerability has been detected. The vulnerability's classification determines the required remediation timeline as outlined below:

Critical and High: Remediation is required within 30 days of detection unless a documented exception is approved.

Medium and Low: Remediation for medium is required within 90 days and remediation of low within 180 days.

If a vulnerability remains without an exception after 30 days, CyberOps notifies the Sys Admin, Supervisor, and Service Owner of the vulnerable system. The Service Owner or Sys Admin is responsible

for either 1) remediating the vulnerability, or 2) requesting an exception (either temporary or long-term).

Exception requests shall be submitted and approved through TeamDynamix and in accordance with the requirements outlined in the Cybersecurity Exception Standard.

In cases where large enterprise systems require extended test periods prior to applying patches to production systems, when patches occur "out of band" (e.g., those occurring outside of a scheduled patch-release), or if a system has an extremely narrow or infrequent service downtime windows due to business requirements, it may be impossible to remediate all vulnerabilities within the required timeframes. Such systems must apply for and diligently pursue temporary exceptions with CyberOps to allow for the extended remediation timelines required to support business operations.

False Positive Reporting

System administrators who believe an identified vulnerability is a false positive may report this finding to CyberOps. A false positive report will stop the "time to remediate" clock to allow time for review of the false positive report and determination of its validity. If CyberOps determines that the vulnerability is not a false positive, the time to remediate clock will restart upon system administrator notification.

UNREMEDIATED VULNERABILITIES

CyberOps/Networking performs remediation verification scanning as needed to confirm adherence to remediation timelines. System administrators receive notification of any vulnerabilities that are not remediated by the applicable deadline. Systems with vulnerabilities that remain unresolved may be isolated within or removed from the USNH network to mitigate the threat posed to other USNH information systems and technological resources.

For vulnerabilities that cannot or will not be remediated within the required timeframe or at all, an exception and/or risk acceptance may be required from the department, college, or organization responsible for the vulnerable system to ensure that the system has continued accessibility to the USNH network. For more information on temporary or long-term exceptions, contact USNH CyberOps.

High-impact actions such as removing and/or quarantining systems or servers from the USNH network requires written approval of the CISO or their delegate, notification to the CIO, and may involve direct communication with the department head, Dean, or appropriate Vice President, at the CIO's discretion. In the absence of high-risk circumstances (i.e., a vulnerability currently being exploited against a critical system), communication to the impacted business unit shall occur at least five days in advance of any action to be taken.

The CISO has the authority to respond, as needed, to ensure that systems do not pose a threat to USNH resources. This includes taking extreme actions that may include, but are not limited to, blocking vulnerable devices from accessing the network, isolating vulnerable devices within the network, or shutting down vulnerable or exploited devices. If the CISO determines extreme actions are necessary, CyberOps shall make a best effort to communicate directly with the Service Owner and/or System Administrator in advance of said actions. However, advance communication is dependent on the

availability of accurate ownership and staff contact information for the system in question and may not always be possible in high-risk or time-sensitive circumstances.

Therefore, all Service Owners, System Administrators, and Application Owners are advised that vulnerable or exploited devices can 1) be quarantined from the USNH network, 2) be isolated within the USNH network, or 3) shutdown, at any time, without prior notification.

In the event of large-scale, high-risk vulnerabilities detected on systems, CyberOps may use campus-wide communication mechanisms to alert Service Owners and System Administrators of necessary remediation actions.

CyberOps may require compensating controls to be implemented and/or a remediation plan be approved prior to allowing a system that was previously quarantined/isolated back on the network. CyberOps must consider the risk sufficiently mitigated to authorize removal from quarantine and network service restoration.

VULNERABILITY REMEDIATION EXCEPTIONS

Temporary exceptions must be requested using the TBD form in TeamDynamix. Long-term exception requests for vulnerabilities requiring remediation may be submitted to CyberOps via the vulnerability listing available in the Networking Portal or via email to IT.Security@unh.edu.

Exceptions should be requested for vulnerabilities that cannot or will not be remediated in the required timeframe, but that will eventually be remediated.

CyberOps provides a final notification of outstanding Critical or High-severity vulnerabilities to the System Owner and Systems Administrators within three business days of the initial 30-day notification. If no response to the final notification is received within five business days, the vulnerabilities are reported to Cybersecurity management and the appropriate Service Line Leader. If no response is received to the final notification within 10 business days, Cybersecurity management escalates the issue to the appropriate Orchestrator.

System Owners and/or Systems Administrators are responsible for completing the exception request form to the best of their ability as well as initiating the exception request with CyberOps. CyberOps will contact the requester to obtain any additional information required to complete the official request form, which requires input from the business unit and from CyberOps, prior to the request being submitted for review and approval.

The exception review process shall include consideration of the following:

- compensating controls currently in place
- extended timeframe required to achieve remediation
- rationale for choosing not to remediate, within the required timeline or at all
- impact on organizational mission

- any recommendations from USNH resources related to a specific vulnerability or specific system's remediation
- technical obstacles to remediation
- operational obstacles to remediation
- any other environment-specific information provided in the request

While an exception request is under review, the required remediation timeline may be paused to allow for consideration, review, and decision-making. However, depending on risk to the USNH, the CISO may determine that the remediation timeline must be enforced. If an exception is not granted, the remediation timeline resumes.

The department may appeal the denial to the CIO who may request involvement of the affected Department Head. If the result of non-remediation would be removal of the system from the network or other drastic action, the requirements and exclusions outlined in this standard relating to approval and notification apply.

Cybersecurity GRC grants exceptions on a case-by-case basis or as blanket exceptions by vulnerability, for groups of similar systems, for systems sharing the same set of compensating controls, or in other configurations as determined by CyberOps. In cases where an approved blanket exception applies to systems that were not part of the original request, all appropriate system administrators will be notified of the blanket exception once it is approved.

Cybersecurity GRC tracks and manages USNH-wide blanket exceptions and information on these exceptions may be provided to authorized parties upon request.

VULNERABILITY REPORTING

ET&S CyberOps is responsible for timely reporting and notification to affected system owners of vulnerabilities present on systems. ET&S CyberOps may utilizes automated mechanisms to report on vulnerabilities. This reporting can include high level reporting to executive USNH leadership, detailed reporting to USNH senior management, reporting on trends over time, and reporting needed to monitor remediation efforts and to facilitate vulnerability management activities.

Emerging vulnerabilities may warrant the implementation of the cybersecurity incident management process to address zero day and other critical vulnerabilities found within the environment.

4. Exemptions

Requests for exceptions to this standard must be submitted in writing to the USNH Chief Information Security Officer through a Team Dynamic ticket at: https://td.unh.edu/TDClient/60/Portal/Requests/ServiceCatalog?CategoryID=47 and may be granted on a case-by-case basis based on business needs and other factors.

5. Enforcement

Failure to comply with this standard puts USNH information at risk and may result in disciplinary action in accordance with the appropriate disciplinary procedures for students, faculty, and staff, as outlined in the relevant student regulations (e.g., Student Rights, Rules, and Responsibilities), the faculty handbook, or staff handbook. Faculty or staff who are members of USNH-recognized bargaining units are covered by disciplinary provisions set forth in the agreement for their bargaining units.

6. Roles and Responsibilities

Chief Information Security Officer (CISO)

- Ensure compliance with this standard throughout the University for those Information Systems and servers designated as in scope in the USNH Server Protection Policy.
- Adjudicate and escalate exceptions to policies and standards.

Service Owner

- Ensure systems and services under their ownership are administered according to this standard.
- Participate in exception/waiver request and risk acceptance processes as required.
- Maintain visibility to and awareness of critical and high vulnerabilities within their services and support efforts required to achieve remediation within the required timelines.

System Administrator

- Review vulnerability reports for assigned systems.
- Act on each identified vulnerability within the required timeframe; actions include remediation of the vulnerability, requesting an exception, reporting a false positive, or requesting remediation assistance.

Cybersecurity Operations

- Manage the Vulnerability Management process including the implementation of continuous process improvements.
- Manage the Exception Request process.
- Manage the Risk Acceptance process.
- Review and reclassify vulnerabilities based on environmental metrics when needed.
- Confirm/overrule false positive reports.
- Monitor remediation efforts and recommend appropriate action for vulnerabilities.
- Produce reports related to vulnerability management as needed.
- Administer the tools used for vulnerability management.

Networking

- Review and reclassify vulnerabilities based on environmental metrics when needed.
- Confirm/overrule false positive reports.
- Monitor remediation efforts and recommend appropriate action for vulnerabilities.
- Produce reports related to vulnerability management as needed.
- Administer the tools used for vulnerability management.

7. Definitions

See the ET&S Policy & Standard Glossary for full definitions of each term.

CISO

Sensitive Information

Confidentiality

Integrity

Availability

Patch

Zero-day vulnerability

Mitigation

Common Vulnerability Scoring System (CVSS)

Compensating Control

Exception

False Positive

Information System

Patch

Remediate

Risk

Risk Acceptance

Scanning Agent

Security Category

Server

Service Owner

System Administrator

Upgrade

Vulnerability

9. Contact Information

For USNH community members: Questions about this standard, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, & Compliance (GRC) via this Support Form.

A community member may submit other requests here: Submit an IT Question.

10. Document History

Effective Date: September 30, 2022
Drafted: Dave Yasenchock. September 30, 2022 v01
Revised, USNH Cybersecurity GRC Standards Committee, September 15, 2022
Reviewed by: Dr. David Yasenchock, Director Cybersecurity GRC, September 29, 2022
Approved by: Thomas Nudd, Chief Information Security Officer, September 30, 2022