VULNERABILITY MANAGEMENT AND SCANNING

Northern Arizona University owns or controls, and acts as custodian for, a broad array of information, including Highly Sensitive Information protected by law. Maintaining the integrity and availability of this information is an important University function. To this end, Information Security Services deploys a comprehensive framework of *Information Security Standards* of which this document is a part. All members of the University community are required to comply with these requirements. Capitalized terms used herein are defined in the *Information Security* policy or the *Data Classification and Handling* policy. Questions regarding these *Information Security Standards* should be directed to Information Security Services.

In accordance with the *Software Patch Management Information Security Standard*, the Chief Information Officer ("CIO") and the Director of Information Security Services will establish, update, and revise as necessary and appropriate the vulnerability management and scanning standards outlined below, which are based on the University's four patch severity rating classifications:

- **Level 1 Low Severity – Low Risk**
- **Level 2 Medium Severity – Medium Risk**
- **Level 3 High Severity – High Risk**
- **Level 4 Critical Severity – Very High Risk**

The purpose of this standard is to implement a Vulnerability Management Program framework while providing additional specifics for the monitoring, reporting, and validating portion of the *Software Patch Management Information Security Standard*. The Vulnerability Management Program goal is to identify and remediate vulnerabilities before networks and systems are compromised.

1. **Identification of Vulnerabilities**. Information Security Services will identify vulnerabilities using several methods, including, but not limited to:

    - Information sharing resources, peers, and third-parties
    - Forums, mailing lists, and vendor update feeds
    - Vulnerability Management Program weekly or monthly scan results
    - Vulnerability and network mapping/scanning results from ad-hoc and on-demand scans
    - System administrators, network administrators, developers, and vendor liaisons
    - Manual penetration testing of systems or services

2. **Detecting, Monitoring, Scanning.** Information Security Services will employ a variety of scanning and monitoring methods, including, but not limited to:

    - Automated, scheduled weekly or monthly scans using vulnerability management tools
    - Weekly scans will include, but not be limited to, scanning for credit card handling environment vulnerabilities and end of life operating systems
    - Monthly scans will include, but not be limited to, the above and all IT Resources handling sensitive or highly sensitive data
    - Unscheduled, on-demand and ad-hoc scans at the request of a department or based upon vulnerabilities detected during automated or scheduled scans in order to confirm/validate mitigations
    - Authenticated and unauthenticated scans
    - Scans from within and outside the network, as well as scans of cloud-hosted environments with regulatory and compliance requirements (*e.g.*, Payment Card Industry, PCI, and Highly Sensitive research data)

- Scans of web applications, systems, services, operating systems, and devices with regulatory and compliance requirements (*e.g.*, Payment Card Industry, PCI, and Highly Sensitive research data) will be performed as part of the Vulnerability Management Program

- The scanning tools will actively test network connected devices and systems for vulnerabilities, using a database of known security vulnerabilities to identify weaknesses or missing security patches

3. **Analysis and Evaluation.** Vulnerability analysis and evaluation will follow a defined and documented process and will produce severity ratings. Information Security Services will maintain detailed process documentation. Decisions for manual penetration testing will be determined from this analysis and evaluation, as well as the Risk Rating described below. Analysis and evaluation will follow the Common Vulnerability Scoring System ("CVSS") risk-rating system and will include the following elements:

   - Ease of compromise and availability of exploits
   - Capability for remote code execution
   - Privileged account escalation assessment
   - Patch/update availability
   - Sensitivity of data processed
   - Likelihood of exploitation or risk to University IT Resources

4. **Severity and Risk Rating.** Vulnerabilities analysis will produce severity and risk ratings similar to those established in the *Software Patch Management Information Security Standard*:

   - **Low** – vulnerability with low or minimal risk, severity, impact to University IT resources. It has an associated risk rating, or CVE ratings 0.1-3.9.
   - **Medium** – vulnerability has a medium risk and medium severity rating with medium impact and risk to University IT resources. It has an associated risk rating, or CVE ratings 4.0-6.9.
   - **High** – vulnerability has a high risk, high severity, and potentially high impact or risk to University IT resources. It has an associated risk rating, or CVE ratings 7.0-8.9.
   - **Critical** – vulnerability has a high risk, high severity, and likelihood of immediate impact or risk to University IT resources. It has an associated risk rating, or CVE ratings 9.0-10.

Following the above risk-based decision-making process, vulnerabilities may be selected for in-depth and manual penetration testing in order to assess actual threats, likelihood of impact, and compensating controls in the University environment. Penetration testing will not generally be required and will not occur on a specific scheduled frequency due to the nature of changing threats, vulnerabilities, and impacts to the University environment. Some situations where penetration testing may be utilized and determined as necessary include, but are not limited to:

- Third party intelligence or peer institution communications of known attacks or exploits with associated indicators of compromise ("IOC")
- As deemed necessary for proving the results of a vulnerability and/or the lack of security controls resulting in real threat
- Expanded testing or additional rigor is needed due to the data involved or the criticality of a system, service, or application
- Upon request by departments
- As required by law or regulation

5. **Notification, Reporting, Remediation**.

   5.1. Scan results will be provided to system administrators, network administrators, and/or asset owners via website, email, email with attached reports, and/or the ServiceNow system. Additional analysis, evaluation and comments will be provided by the Information Security Services analyst to highlight the most critical results.

   5.2. Email or ServiceNow will be used to share remediation progress reporting, rescanning results, and documentation of mitigating controls. Reports and related communications will include prioritization by Information Security Services analyst based upon a severity rating of Low, Medium, High, and Critical.

5.3. Critical and High vulnerabilities must be patched as soon as possible, according to the timelines detailed in the *Software Patch Management Information Security Standard*. ServiceNow tickets will not be closed until remediation and clean rescans are completed, or until mitigating controls have been established, documented, tested/validated, and an exception request has been approved by the CIO.

5.4. In some instances, the CIO will approve the network quarantine of an IT Resource with Critical or High vulnerability if Information Security Services assesses the risk and lack of remediation. In such cases, a notice will be sent to the system owner prior to the quarantine.

6. Exceptions Review. In the event that vulnerability remediation (patching, updating, or establishing mitigating controls) cannot follow the stated schedule, an exception request must be made that details why postponement or deferral is needed. The CIO or authorized designee must grant remediation exception request approvals, which will be submitted through the ServiceNow system. Exceptions may include:

- Production system freeze or change blackout periods where remediation work is delayed
- Conflicts with other critical changes scheduled during the same period
- Tested patches or remediation steps break functionality in non-production environment
- Products that do not have patches or are managed by vendor and not under University control (alternative security controls should be established and documented)
- Systems, applications, or devices where appropriate risk-mitigation controls are put in place, documented and validated