# SOFTWARE PATCH MANAGEMENT

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.

This Information Security Standard establishes a patch severity classification structure and patching protocols to help limit the exposure of University IT Resources to threats and vulnerabilities by establishing timeframes for software patching, updating, and confirming patch management compliance.

## 1. Patch Rating and Scheduling.

**1.1.** Patches, releases, and updates shall be characterized and identified by the four severity classifications described below, which shall apply to all IT Resources that qualify for patches, releases, and updates from vendors, third-parties, contractors, or University developers. All system administrators, network administrators, developers, and Information Security Services will use these classifications to determine the appropriate risk, severity, and timeline for application of the patches, releases, and updates.

**1.2.** Patching schedules must take into consideration the level of interruption to critical University operations. Application of patches or updates must balance the security, criticality, and the need to maintain operations during critical-use and high-demand hours.

**1.3.** Patching must be performed on a regular and consistent schedule, not to exceed 90 days from vendor release of the update, to reduce unplanned outages, prevent unknown issues, and provide a more secure environment. In lines with this NAU ITS will perform forced reboots on workstations to assist with timely installation of routine patches. A standard grace period of 7 days will be granted after an update becomes available through NAU ITS prior to the workstation automatically being rebooted.

**1.4.** For out of band patching, criticality and risk ratings will determine the timeline for patch deployment. Ratings will be supplied by vendors, Common Vulnerability Scoring System (“CVSS”), or from the Information Security Services vulnerability risk-rating procedure. Risk and severity ratings with patch timelines are shown below:

**Level 1 Low Severity – Low Risk**

- Patch will be applied within the normal patch cycle or as vendors release updates and patches as part of regular release intervals (monthly, quarterly, annually)
- A vulnerability with low or minimal risk, severity, impact to NAU IT Resources
- Normal or standard change request types are typically used
- Issued by vendor with an associated risk rating, or CVE ratings 0.1-3.9

**Level 2 Medium Severity – Medium Risk**

- Patch must be applied within the normal patch cycle, not to exceed ninety (90) days from release
- A vulnerability with a medium risk and medium severity rating with medium impact and risk to NAU IT Resources
- Normal or standard change request types are typically used
- Issued by vendor with an associated risk rating, or CVE ratings 4.0-6.9

**Level 3 High Severity – High Risk**

- Patch must be applied within fourteen (14) days
- A vulnerability with a high risk, high severity, and potentially high impact or risk to NAU IT Resources
- Emergency Change request may be necessary
- Issued by vendor with an associated risk rating, or CVE ratings 7.0-8.9

**Level 4 Critical Severity – Very High Risk**

- Patch must be applied as soon as possible but not to exceed seven (7) days
- A vulnerability with a high risk, high severity, and likelihood of immediate impact or risk to NAU IT Resources
- An Emergency Change request may be necessary
- Issued by vendor with an associated risk rating, or CVE ratings 9.0-10

**1.5.** Software that has reached end-of-life or ~~are~~is no longer supported by the vendor, contract, or extended support must be removed from University systems immediately.

2. **Change Management and Approval**. The University's IT Change Management process shall be followed when performing Software Patch Management. This includes a formal submittal of a change request, the review of change requests by a change advisory board, testing and implementation plan documentation, and change request closures with lessons learned recorded. Regular and normal patching and updating must receive approval to become normal or standard changes.

3. **Sources of Software Updates, Patches, and Releases**. Downloads for all patches, releases, and updates must be from verified trusted sources only.

4. **Logging**. System administrators, developers, and asset owners will maintain knowledge of updates, patches, and releases through mailing lists, vendor release notes, and/or from scheduled vulnerability scan results provided by Information Security Services. Tracking and logging of patches, updates, releases, changes, and all testing will be documented in a system of record or a log repository identified and designated by the Chief Information Officer ("CIO"), or their designee, (e.g., ServiceNow).

5. **New IT Resources**. New systems must be fully patched and updated to the most current levels prior to being implemented for production uses and interactions.

6. **Testing**. All patches, releases, and updates must be tested, when practical, in a non-production environment prior to production deployment.

7. **Monitoring, Reporting, and Validating**.

**7.1.** The CIO, or their designee, with the concurrence of the Director of Information Security Services, shall establish, update, revise, and republish, as necessary and appropriate, a comprehensive set of protocols designed to monitor compliance with this Information Security Standard. The *Vulnerability Management and Scanning Protocols* shall be based on the severity ratings and classifications established in this Information Security Standard. The *Vulnerability Management and Scanning Protocols* establishes standards for monitoring and scanning of patches, vulnerabilities, and threats to the University's IT Resources.

- Vulnerability scans will occur on a regular weekly and monthly schedule established by Information Security Services to monitor patch management compliance

- To confirm and validate security patches or updates made outside of the normal patch cycle, Information Security Services will manage ad-hoc scan requests to assist with validation
- Credentials for authenticated scans will be granted where applicable and necessary to validate patching
- Scan results indicating systems out of compliance with patch policy timelines will be entered into the system of record, currently ServiceNow, for further monitoring

**7.2. Endpoints**. The use of centralized desktop management tools such as System Center Configuration Manager ("SCCM"), Microsoft Defender for Endpoint, and JAMF may be used to report on patch and update levels for operating systems and applications.

**8. Exception Requests**. In the event patches, ~~and~~ updates, or remediation cannot follow the stated schedule, an exception request must be made that details why postponement or deferral is needed. The CIO, or their designee, or authorized designee will grant patch-postponement request approvals that will be submitted through the system designated by the CIO, or their designee, (e.g., ServiceNow, OnBase).

Reasons for exception requests may include:

- Production system freeze or change blackout periods
- Conflicts with other critical changes scheduled during the same period
- Tested patches break functionality in non-production environment
- End of life products that must remain in place (additional or alternative security controls must be established and documented)
- Systems, applications, or devices where appropriate risk-mitigation controls are in place, documented, and validated