

2.10 Vulnerability and Patch Management Standard

Effective Date: July 1, 2026

Revised Date: July 1, 2026

1. Purpose

This Standard establishes the mandatory requirements for assessing, managing, and monitoring risk associated with vulnerabilities and operating system patches on Arkansas State University technology resources. The purpose of this standard is to ensure that these risks are managed in a manner that protects university data and mitigates institutional risk.

2. Scope

This standard applies to all Arkansas State University employees who work to manage or oversee Arkansas State University technology resources. This includes all individuals that directly report to the central Information Technology Services department and any systems authority who has been delegated access to maintain a technology resource.

3. Definitions

Technology Resources – The machines, devices, systems, services, and related components used in information processing. This includes:

- Machines, devices, and transmission facilities used in information processing, such as computers, word processors, terminals, telephones, cables, software, and related products.
- Devices used to process information through electronic capture, collection, storage, manipulation, transmission, retrieval, and presentation of information in the form of data, text, voice, or image, including telecommunications and office-automation functions.
- Any component related to information processing and wired or wireless telecommunications, including hardware, software, services, planning, personnel, facilities, and training.
- Procedures, equipment, and software designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, along with associated personnel such as consultants and contractors.
- All email accounts issued by the Arkansas State University System.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates, and members of the system community.

System Community - Any person who accesses the ASU System's IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

Systems Authority - ASU System delegates oversight of particular systems to the head of a specific unit of the ASU System or to an individual faculty member, in the case of technology resources purchased with research or other funds for which he or she is personally responsible.

Systems Administrator - A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular technology resources.

Certifying Authority - This is the Systems Administrator or other ASU System authority who certifies the appropriateness of an official ASU System document for electronic publication in the course of ASU System business.

Specific Authorization - This means documented permission provided by the applicable Systems Administrator.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and remediation of technology resource vulnerabilities. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University's vulnerability and patch management processes within the scope of this standard. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

Assistant Vice Chancellor of IT Infrastructure and Operations - Responsible for the management and coordination of the university's patch management program, lifecycle management program, and the technology resource inventory program. Responsible for ensuring ITS Endpoint Technicians and ITS Systems Team remediate identified vulnerabilities in the required timeframes.

IT Security Team - Responsible for configuring, maintaining, and coordinating the effective management of vulnerabilities on university technology resources. This includes the identification of applicable vulnerabilities, including insufficient patch versions, and communicating the relevant data to the party responsible for remediation.

ITS Endpoint Technician - Responsible for the remediation of identified vulnerabilities and insufficient patch versions on university technology resources in alignment with SLA standards and remediation timelines outlined in this standard.

ITS Systems Team – Responsible for the remediation of identified vulnerabilities on university infrastructure, such as servers, in alignment with SLA standards and remediation timelines outlined in this standard.

Systems Authority / Delegated Authority – Responsible for the remediation of identified vulnerabilities on university technology resources outside the management of Information Technology Services (ITS) in alignment with the SLA standards and remediation timelines outlined in this standard.

5. Standard Exceptions

The Chief Information Officer is authorized to review and approve exceptions to this standard when organizational needs justify a deviation, and the associated risks are deemed acceptable. All exceptions must be documented, including a defined scope, a scheduled review date, and compensating controls when appropriate. The CIO may delegate this authority as necessary but retains overall accountability for exception management and review.

6. Target Remediation Timelines

All identified vulnerabilities and misconfigurations shall be targeted for remediation in alignment with the following timelines. This timeline will be set based on the criticality of the vulnerability with an enhancement based on potential data classification impact.

Tier	Low	Medium	High	Critical
Public	180 Days	180 Days	90 Days	30 Days
Internal	180 Days	90 Days	60 Days	30 Days
Confidential	90 Days	45 Days	30 Days	14 Days
Regulated	30 Days	14 Days	7 Days	24-48 Hours

Remediation timeline and classification are set by the Arkansas State University IT Security Team at the time of remediation assignment. Excessive noncompliance with the targeted remediation timeline may result in the technology resource(s) being removed from the university network.

Vulnerabilities that are compensated for by another control or that have their risk accepted by the CIO shall be tracked and documented via the vulnerability management platform's suppression rules or other comparable mechanism.

7. Vulnerability Management

To ensure compliance with university standards, technology resources shall be actively monitored for vulnerabilities. The IT Security Team will maintain, support, and centrally administer a vulnerability detection system with the institutional goal of reducing cybersecurity risk associated with globally reported and documented vulnerabilities.

This vulnerability management will include the following requirements:

- The authority to manage and administer Arkansas State University’s vulnerability management program is delegated solely to the IT Security Team by the CIO. The CIO maintains full authority and executive oversight of this program despite this delegation.
- Any technology resource owned by Arkansas State University or connecting to Arkansas State University’s network will be subject to vulnerability scanning as warranted by the IT Security Team.
- Failure to remediate an identified vulnerability within the outlined timeline on any technology resource owned by Arkansas State University or connecting to Arkansas State University’s network may result in the removal of the system or device from the network without notification.
- Compliance reviews of Arkansas State University’s vulnerability management program will be regularly conducted.
- Users not listed within the responsibilities section of this standard will be prohibited from viewing or accessing detailed vulnerability scan results for systems and/or devices in which they do not have a need to know.
- Users not listed within the responsibilities section of this standard will be prohibited from running vulnerability detection applications on or against systems for which they have not been approved.
- For the purposes of data classification, any information or scan results detailing sensitive security flaws within Arkansas State University’s technology resources will be considered confidential.
- IT Security shall establish and maintain automated reports or publish dashboards to relevant users listed in the responsibilities section to assist with the preventative remediation of vulnerabilities prior to a formal communication being sent out by IT Security.

8. Vulnerability Remediation

Identified vulnerabilities will be communicated to the group responsible for remediation based on the responsibilities outlined in Section 4 of this document by the IT Security Team. This communication shall use the following communication methods:

Tier	Low	Medium	High	Critical
Public	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P4)
Internal	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P4)	Team Dynamix Ticket (P3)
Confidential	Team Dynamix Ticket (P3)	Team Dynamix Ticket (P3)	Team Dynamix Ticket (P3)	Team Dynamix Ticket (P2) & Direct Email
Regulated	Team Dynamix Ticket (P3)	Team Dynamix Ticket (P2) & Direct Email	Team Dynamix Ticket (P2) & Direct Email	Team Dynamix Ticket (P1) & Direct Email

Failure to remediate an identified vulnerability within the outlined timeline on any technology resource owned by Arkansas State University or connecting to Arkansas State University’s network may result in the removal of the system or device from the network without notification.

9. Patch Management

To ensure compliance with university standards, technology resources shall be actively patched for system and security updates. The Assistant Vice Chancellor of IT Infrastructure and Operations will maintain, support, and coordinate a centrally administered patch management system with the institutional goal of reducing cybersecurity risk associated with unsupported or out-of-date operating systems.

This patch management will include the following requirements:

- The authority to manage and administer Arkansas State University's vulnerability management program is delegated solely to the Assistant Vice Chancellor of IT Infrastructure and Operations by the CIO. The CIO maintains full authority and executive oversight of this program despite this delegation.
- Any technology resource owned by Arkansas State University will be subject to these patch management practices as warranted by the Assistant Vice Chancellor of IT Infrastructure and Operations.
- Patches, system upgrades, or other vendor releases must be obtained from trusted sources such as approved vendors or other external parties.
- Testing of all applied patches, upgrades, and change management procedures are required to ensure effectiveness and reduce potential side effects.
- Patching or upgrading major systems that could impact a substantial number of campus users must be completed during regular maintenance windows unless an emergency maintenance window is required due to the criticality of the patch or upgrade.
- Failure to patch or update a technology resource in a timely manner may result in its removal from the Arkansas State University infrastructure without notification for the protection of other technology resources and institutional data.

10. Standards Review

This document will be reviewed and reaffirmed annually, or upon significant changes to university IT governance, systems, or regulatory requirements.

Effective Date: July 1, 2026

Next Review Date: July 1, 2027

Version: 1.0

Referenced Policies, Standards, and Procedures

- Technology Resource Management Standard
- Information Technology Services (ITS) Communication & Service Level Agreement (SLA) Standards
- Data Security and Classification Policy

Revision #1

Created 2026-06-26 02:21:33 UTC by Christopher Boothman

Updated 2026-06-26 02:25:38 UTC by Christopher Boothman