

# 2.5 Network Security Standard

**Effective Date:** July 1, 2026

**Revised Date:** July 1, 2026

## 1. Purpose

This Standard establishes the mandatory requirements for the management of network resources and network infrastructure at Arkansas State University (A-State). The purpose of this standard is to ensure that these resources are managed in a manner that protects university data and mitigates institutional risk. Through the processes outlined in this standard, University staff will be equipped to manage institutional network resources and network infrastructure at every stage of their lifecycle within A-State.

## 2. Scope

This standard applies to all faculty, staff, students, contractors, affiliates, and members of the Arkansas State University System community who access Arkansas State University information technology infrastructure and associated resources. This standard applies to all network infrastructure components such as wired and wireless networks, devices, systems, servers, and applications that are connected to the university's network and applies in all work settings, including on campus, remote work locations, and approved telecommuting arrangements.

## 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 A-State.

**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.

## 4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and coordination of network security controls. This includes:

**Chief Information Officer (CIO)** - Responsible for the executive sponsorship, governance, and oversight of the University's network security 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** - Provides strategic leadership for enterprise IT infrastructure and operations, ensuring secure, reliable, and scalable services aligned with institutional goals. Oversees networking, systems, cloud, data centers, and IT security while managing budgets, vendors, governance, and risk.

**ITS Networking Team** - Designs, implements, and maintains the university's wired, wireless, and wide area network infrastructure to ensure secure, reliable, and high-performance connectivity across academic, administrative, residential, and public environments. Manages network hardware, services, data center and cloud connectivity, monitoring performance, capacity, and availability while implementing security controls in coordination with ITS Security. Supports new construction and technology initiatives, maintains network standards and documentation, and participates in incident response and on-call support for critical network services.

**ITS Security** - Responsible for establishing and maintaining the university's IT security program. Responsible for ensuring institutional data, systems, and networks are monitored for cybersecurity threats, vulnerabilities, and unauthorized access. Ensures that identified incidents are assigned to the appropriate responsible party for remediation.

## 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. Network Infrastructure

The A-State network infrastructure ensures the security, availability, and integrity of institutional data. The primary components responsible for these requirements are the firewall and the dual network core, which are designed to align with the Arkansas State Cybersecurity Standards and Act

**Perimeter Firewalls:** Firewalls are deployed at strategic points in a high-availability pair to control traffic between internal and external networks. Specific throughput requirements and connectivity patterns are maintained in the A-State Network Standard Operating Procedures to ensure alignment with current institutional demands.

**Access Control and Least Privilege:** Firewalls utilize Access Control Lists (ACLs) to permit only necessary traffic by default. All firewall rule changes require formal approval before implementation.

**Logging and Monitoring:** In accordance with state recommendations and institutional security practices, firewall logs must be reviewed on a defined and recurring basis to identify potential security threats, unauthorized activity, configuration issues, or policy violations. At a minimum, automated monitoring and alerting should occur continuously where supported by the platform, with formal manual reviews conducted no less than weekly by ITS personnel based on platform responsibility.

High-risk events, critical alerts, and indicators of compromise should be reviewed daily or in near real-time as feasible and should be reported by the responsible party to the IT Security team when the identified risk is a security incident.

Findings requiring action must be documented, escalated, and tracked through established ITS incident response procedures.

**Dual Network Core:** The university maintains a redundant dual-core infrastructure to provide high availability and support campus-wide traffic.

**Redundancy:** Core devices are geographically distributed across campus to ensure continuity in the event of a localized incident.

**Connectivity:** The core supports industry-standard Link Aggregation (LAG) and provides high-speed fiber connectivity to every building on campus.

**Performance:** Core hardware is selected to perform simultaneous routing and switching at scales sufficient to handle all campus internet and internal traffic.

**Note:** For specific hardware specifications, link speeds, and physical installation locations, please refer to the Internal Network Infrastructure Appendix. This ensures the security standard remains current as technology evolves.

## 7. Use of Network Infrastructure

Arkansas State University invests in substantial and sufficient resources to acquire and operate information technology assets, such as hardware, software, and Internet connections. ITS has a responsibility to manage its resources in the most efficient and effective manner possible and in compliance with all laws, regulations, and sound business practices, while at the same time

protecting and preserving the right to academic freedom. Effective management of these resources will assure students, faculty, and staff adequate access to information and technology over the long term and ensures compliance with Arkansas State University System policy.

Examples of appropriate and inappropriate uses of network infrastructure include, but are not limited to, the following:

### **Appropriate Use of Network Infrastructure**

- Accessing the Internet for work-related research and information gathering.
- Conducting approved research activities in compliance with university policies, grant requirements, and applicable regulations.
- Supporting teaching and learning activities, including course delivery, instructional design, and student engagement.
- Utilizing the network in approved telecommunication services such as Cisco Webex, Jabber, Microsoft Teams, or Zoom.

### **Inappropriate Use of Network Infrastructure**

- Users must not share credentials or allow others to access resources using their unique accounts.
- Users may not physically tamper with networking infrastructure, including Wireless Access Point removal or modifying or removing physical network cabling.
- Users may only access computer accounts that have been authorized for their use.
- Users may only use accounts for their authorized purposes. This restriction shall not prevent informal communication, but resources must not be used for private consulting or personal gain without ASU System General Counsel approval.
- Use in violation of civil or criminal law or regulation at the federal, state, or local levels is prohibited.
- Use in violation of the Arkansas State University System Appropriate Use of Information and Technology Resources is prohibited.
- Use in violation of the Arkansas State University student, faculty, or staff handbooks, as applicable, is prohibited.

Violations of this standard may result in disciplinary action in accordance with Arkansas State University System policies, up to and including revocation of network access, disciplinary action under applicable faculty, staff, or student handbooks, termination of contracts, and/or legal action.

## **8. Firewall Configuration**

To ensure compliance with university standards, the ITS Networking Team will maintain, support, and centrally administer university-owned firewalls with the institutional goal of reducing operational and cybersecurity risk associated with utilizing these resources. The ITS Networking Team shall maintain a supplemental Firewall Management Procedure, separate from this standard, that outlines how these resources are requested to be changed, configured, monitored, recorded for audit purposes, and managed.

This procedure will, at a minimum, include and establish the following requirements:

- Default-deny rule: block all incoming traffic unless explicitly allowed.
- Encryption for traffic where possible, such as using TLS for web traffic.
- Strong security policies for remote access, such as VPN and secure protocols like SSH.
- Regular updates and patches to firewall software and firmware.

## 9. Network Segmentation

Arkansas State University utilizes network segmentation to isolate certain types of traffic and ensure the security of sensitive data types. The following networks are segmented and isolated:

- **Academic Network** - Used by students, faculty, and staff for routine academic activities.
- **Administrative Network** - Contains sensitive financial, HR, and student information and utilizes stricter access controls.
- **Guest Network** - Isolated from the main network to provide internet access for visitors while limiting access to internal systems.
- **Cardholder Data Environment (CDE)** - Used for university point-of-sale devices and other resources that process cardholder data. Isolated from the main network to reduce the scope of PCI DSS auditing requirements.
- **Research Network / HIPAA** - Contains sensitive research and HIPAA information and utilizes stricter access controls.

## 10. Remote Access

Remote access to the university network will require approved VPN or Zero Trust Network Access (ZTNA) connections with strong authentication methods, including Multi-Factor Authentication (MFA), and all traffic must pass through firewalls for inspection and protection.

## 11. Patch Management

To ensure compliance with university standards, technology resources shall be actively patched for system and security updates. ITS will maintain, support, and centrally administer a patch management system with the institutional goal of reducing cybersecurity risk associated with unsupported or out-of-date operating systems. ITS shall maintain a supplemental Technology Resource Vulnerability and Patch Management Standard, separate from this standard, that outlines how technology resource patch versions are maintained.

## 12. Network Monitoring, Logging, and Auditing

To ensure compliance with university standards, the ITS Networking Team will create and maintain a procedure that encompasses network monitoring, logging, and auditing processes. This procedure shall outline how all network security logs are collected and stored for devices such as firewalls, IDS, and IPS.

This procedure will include and establish, at a minimum, the following requirements:

- How all network logs are stored securely and monitored in real time by the responsible ITS team to detect and respond to incidents.
- Network logs will include VPN authorization attempts, firewall alerts, and other relevant security alerts.
- Network logs must be retained in accordance with the university's data retention policy. Any attempts or successful deletion of logs or disabling of log collection must be documented and reported.

## 13. Incident Response

To ensure compliance with university standards, ITS will maintain, support, and centrally coordinate a formal Incident Response process with the institutional goal of responding to IT operational and IT security incidents. ITS shall maintain a supplemental Incident Response Plan, separate from this standard, that outlines how the IT organization would respond to an IT security incident or emergency.

## 14. Bring Your Own Device (BYOD) Management

To ensure compliance with university standards, personal technology resources shall have restrictions and controls separate from those outlined in this standard. ITS will maintain, support, and centrally administer these controls with the institutional goal of reducing operational and cybersecurity risk associated with BYOD equipment. ITS shall maintain a supplemental Bring Your Own Device (BYOD) Governance Standard, separate from this standard, that outlines how these resources are managed.

## 15. 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

- Bring Your Own Device (BYOD) Governance Standard
- Arkansas Code § 5-71-215 (Computer-Related Crime)
- Firewall Management Procedure

---

Revision #1

Created 2026-06-26 02:04:03 UTC by Christopher Boothman

Updated 2026-06-26 02:06:20 UTC by Christopher Boothman