

2.9 Technology Resource User Education Standard

Effective Date: July 1, 2026

Revised Date: July 1, 2026

1. Purpose

This standard establishes the mandatory requirements for the management of technology resources 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 technology resources 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 institutional data as governed by the Data Security and Classification Policy 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 technology resource user education. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University's technology resource user education 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.

Employee Training & Development Authority – Responsible for the coordination of mandatory user training requirements, assignment, and record maintenance outlined in this standard.

ITS Helpdesk – Responsible for the development and maintenance of ITS' primary documentation repository and education of users who reach out to tier 1 support staff. Provides ad hoc technology resource training on a requested and scheduled basis.

ITS Security – Responsible for the coordination of institutional technology resource tabletop exercises and phishing campaigns. Provides ad hoc security training on a requested and scheduled basis.

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. Documentation Repository

ITS shall maintain a centralized knowledge base to support self-service learning and consistent guidance across the university. This knowledge base will include the following:

- IT Helpdesk Knowledge Base articles
- Getting-started guides for major systems and applications
- Arkansas State University IT policies and standards
- System usage guidance
- Security best practices

- Common troubleshooting and FAQ resources

Documentation in this knowledge base shall be reviewed and updated annually to ensure the content accurately reflects system changes and new services available to university users.

7. Contacting the ITS Helpdesk

Users may request assistance via ticketing system, email, phone, or in-person support. Support hours are published on the university website.

Users can request assistance through multiple methods, which may include:

- Online ticketing system
- Email support – itshelpdesk@astate.edu
- Phone support – 870-972-3933
- In-person support location: Dean B. Ellis Library – Room 149
- In-person support hours: Monday-Friday, 8:00 a.m.-5:00 p.m.

8. Ad Hoc Training Sessions

Information Technology Services offers various supplemental training sessions throughout the year. These trainings are open to all students, faculty, and staff that feel the content is relevant to their job duties and educational experience.

At times, IT Security may assign phishing training when a user interacts with scheduled phishing campaigns. These non-malicious campaigns help prepare users for when they receive a real threat and allow short informational training to be assigned following a user interacting with this “fake” phish.

IT Security also accepts requests from departments to hold customized training sessions depending on their needs. This training can be requested via the Department Training Request form.

To find and attend pre-scheduled ad hoc training sessions, users can view these upcoming events on the university calendar or by viewing their listings on the Daily Digest. Examples of past training topics include:

- Phishing, Social Engineering and Scam Detection
- Cybersecurity Fundamentals and Data Protection
- Formstack virtual training session
- Secure Document Sharing Process Training

9. Criminal Justice Information Services (CJIS) Training

Individuals with authorized access to Criminal Justice Information Services (CJIS)-protected information are required to complete annual CJIS-specific training, as mandated by the Federal Bureau of Investigation (FBI).

This includes, but is not limited to:

- UPD personnel
- All ITS staff with access to data center systems that store or transmit CJIS-related data
- Any other staff or contractors with direct or indirect CJIS system access

CJIS training must be completed annually, in accordance with the FBI's CJIS Security Policy, and records of completion will be maintained for audit and compliance purposes.

10. Artificial Intelligence (AI) and Automated Decision Tool (ADT) Training

In alignment with the Artificial Intelligence Governance Policy, the Arkansas State University System shall develop a training program for all students, faculty, staff, and users of the system concerning the appropriate use of artificial intelligence and automated decision tools in deciding an outcome in the course of their time as an authorized user of the system's technology resources. This training shall be included in all new employee and student training and will be completed on an annual basis.

11. Annual Employee Compliance Training

At the recommendation of the ASU System Office and our Board of Trustees, A-State has implemented a series of required monthly training courses for employees. These trainings reinforce our shared commitment to professionalism, safety, compliance, and a supportive campus environment.

At the start of each month, users will receive an email from training@AState.edu with instructions for accessing the assigned course(s) through the Employee Learn Center.

12. Tabletop Exercises

To support user awareness and reinforce required security practices, Information Technology Services will conduct periodic tabletop exercises. These exercises provide scenario-based discussions that help users understand expected behaviors during security or operational incidents. Participation requirements will be communicated in advance and may include faculty, staff, or designated departmental representatives as appropriate.

Each exercise will document the scenario, participant decisions, identified gaps, and required follow-up actions to ensure continuous improvement of institutional processes and user readiness.

13. Key Performance Indicator (KPI) Monitoring

To ensure the efficacy of user education materials, Information Technology Services shall monitor certain metrics such as phishing simulation failure rates or relevant disciplinary events. KPI monitoring is intended to ensure consistent application of this standard and to identify opportunities for improvement. In the execution of this goal, ITS shall complete the following:

- Conduct periodic phishing simulations.
- Track user susceptibility metrics.
- Report trends to leadership.
- Adjust training programs based on risk indicators.
- Provide additional targeted training sessions for areas identified at risk.

14. 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

- Artificial Intelligence Governance Policy
-

Revision #1

Created 2026-06-26 02:19:29 UTC by Christopher Boothman

Updated 2026-06-26 02:21:27 UTC by Christopher Boothman