Information and Technology Resource Security Policy

Effective Date: October 16, 2026

1. Purpose

The purpose of this policy is to establish requirements, responsibilities, and governance for the secure use and management of institutional data and technology resources within the Arkansas State University System (ASU System). This policy ensures compliance with Arkansas Act 504 and provides a governance structure that promotes transparency, accountability, and responsible management of university technology resources.

2. Scope

This policy applies to all faculty, staff, students, contractors, affiliates, and members of the ASU System community, who use technology resources or interact with institutional data when conducting university business, as defined in this policy. This policy 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

- **Artificial Intelligence (AI)** - A machine-based system that can, based on a given set of human-defined objectives, make predictions, recommendations, or decisions influencing a real or virtual environment.
- **Automated Decision Tool (ADT)** - A system or service that uses artificial intelligence and that has been specifically developed and marketed, or specifically modified, to make, or to be, a controlling factor in making consequential decisions.
- **Technology Resources** – The machines, devices, systems, services, and related components used in information processing. This includes the following:
    - Machines, devices, and transmission facilities used in information processing, including 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 ASU 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 ASU System community.
- **Institutional Data** - Any data created, collected, maintained, transmitted, or recorded by the ASU System, or its individual campuses, in support of academic, administrative, research, or operational functions. This includes data used to conduct official university business, regardless of format or storage location (e.g., digital systems, paper records, cloud services).
- **IT Organization** - The unit at each institution responsible for providing information-technology solutions and services.
- **ASU System Community -** Any person who accesses the ASU System's IT infrastructure and who is not classified as a member of the faculty (full- or part-time), staff (full- or part-time), or enrolled student.
- **Systems Authority** – The 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 they are personally responsible.
- **Systems Administrator** - A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to them. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular technology resources.
- **Privileged Access** – Authorized access that allows a user or account to perform administrative or security-sensitive actions on a technology resource that a standard user cannot perform.

4. Policy Exceptions

The Chief Information Officer (CIO) for the campus is authorized to review and approve exceptions to this policy when organizational needs justify a deviation, and when the associated risks are deemed acceptable. All exceptions must be documented, including a defined scope and, a scheduled review date, and must incorporate compensating controls

when appropriate. The CIO may delegate this authority, as necessary, but retains overall accountability for exception management and review.

5. Responsibilities

The university personnel involved in the management, authorization, monitoring, and review of standards and procedures governing the use of AI and ADT for each ASU System campus, includes the following:

- **Chief Information Officer (CIO)** - Responsible for executive sponsorship and oversight of the university's information and technology resource security program. Ensures that appropriate resources, policies, and enforcement mechanisms are in place to support compliance with this policy. Approves risk-based exceptions, resolves cross-unit tool management issues, and provides executive accountability for institutional data protection, as it pertains to technology resources.
- **Data Custodians (Digital Records) -** Responsible for implementing and operating the technical and administrative controls that protect digital institutional data in accordance with applicable compliance frameworks and institutional policy. This includes enforcing artificial-intelligence usage guidelines, safeguarding data throughout its lifecycle, and supporting audit, monitoring, and incident response activities.
- **Data Custodians (Physical Records) –** Responsible for implementing and operating administrative and operational controls to protect physical institutional data outside the scope of this policy.
- **Human Resources –** Responsible for the development and maintenance of compliance and enforcement requirements outlined in this policy.
- **Employee Training and Development Coordinator –** Responsible for the coordination of user training requirements and training record maintenance outlined in this policy.
- **Procurement Services -** Responsible for developing and maintaining processes for the procurement of technology resources and any third-party platforms, as well as ensuring that risk assessments are performed prior to procurement.

6. Information and Technology Resource Security Structure

Given the broad scope of this policy, it is intentionally structured to be supported by more detailed standards. This policy establishes institutional intent and minimum requirements, while governance is achieved through the supporting standards that outline the specific technical and operational requirements for full compliance with this policy.

The next twelve (12) sections of this policy will outline and establish these supporting standards.

7. Technology Resource Management Standard

Each ASU System IT Organization shall maintain a supplemental Technology Resource Management Standard, separate from this policy, which outlines the ways in which technology resources are maintained in accordance with state, federal, and university regulations and policies. At a minimum, this will include and establish the following subjects:

- Devices shall be named in alignment with the IT Organization's approved naming scheme.
- Devices shall be centrally managed through an approved Mobile Device Management (MDM) platform (e.g., Microsoft Intune, JAMF).
- Devices shall be joined to the IT Organization's institutional domain (e.g., Entra or on-premises domains).
- Devices shall display a system-use notification to users before granting access to the system. This notification must comply with Criminal Justice Information Services (CJIS) policy v6.0 control AC-8.
- Full-disk encryption shall be enabled, using an IT Organization-approved encryption standard (e.g., BitLocker with TPM 2.0).
- Local administrator privileges shall be restricted, as follows:
    - Standard users shall not have standing local administrator rights.
    - Privileged access shall be limited to authorized ASU System IT Organization personnel.
    - Authorized privileged access shall not be granted via the use of static local accounts and will instead utilize an approved Privileged Access Management (PAM) solution (e.g., Microsoft Local Administrator Password Solution (LAPS)).
- Automatic screen lock shall be enforced after no more than five (5) minutes of inactivity.
- An institutionally approved endpoint detection and response (EDR) solution (e.g., CrowdStrike) shall be installed and shall actively report to the central management console.

8. Technology Resource Vulnerability and Patch Management Standard

Each ASU System IT Organization shall maintain a supplemental Technology Resource Vulnerability and Patch Management Standard, separate from this policy, which outlines the ways in which technology resources vulnerabilities and patch versions are maintained, in accordance with state, federal, and university regulations and policies. At a minimum, this will include and establish the following subjects:

- IT Organization-approved target remediation timelines. (e.g., Critical vulnerabilities on assets processing confidential data must be remediated within 14 days.)

- Any technology resource, owned by the ASU System or connecting to ASU System networks, will be subject to vulnerability scanning, as warranted by the respective IT Organization.
- Failure to remediate an identified vulnerability within the outlined timeline, on any technology resource owned by the ASU System or connecting to ASU System networks, may result in the removal of the system or device from the network without notification.
- For the purposes of data classification, any information or scan results, detailing sensitive security flaws within ASU System technology resources, will be considered **confidential**.
- The establishment and assignment of responsibility for a centrally administered patch management system for the IT Organization's technology resources.
- Patching/upgrading major systems which 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/upgrade.

9. Network Security Standard

Each ASU System IT Organization shall maintain a supplemental Network Security Standard, separate from this policy, that outlines the ways in which network resources are maintained in accordance with state, federal, and university regulations and policies. At a minimum, this will include and establish the following subjects:

- All access to network resources shall be authenticated, authorized, and restricted to approved users, devices, and services.
- All network infrastructure devices shall be configured, using documented, security hardened baselines, and shall not operate with vendor default credentials.
- All network infrastructure shall be regularly assessed for vulnerabilities, and security patches and updates shall be applied within acceptable timeframes based on risk and criticality.
- All third-party, vendor, and remote network connections shall be explicitly approved, documented, securely configured, and annually reviewed for continued necessity.
- All network traffic shall be logically or physically segmented, based on risk, function, and data classification. This segmentation shall be documented and supplemented with data flow diagrams.
- Examples of both appropriate and inappropriate use of network infrastructure.
- Each ASU System campus shall develop and enforce disciplinary procedures for tampering with networking infrastructure (e.g., Wireless Access Point (WAP) removal). This shall be reflected in the student, faculty, and staff handbooks for each ASU System campus, and a clear reporting structure will be established for

the campus IT Organization to report instances of this to the respective disciplinary body.

10. Technology Resource Physical and Environmental Security Standard

Each ASU System IT Organization shall maintain a supplemental Technology Resource Physical and Environmental Security Standard, separate from this policy, which outlines how the infrastructure, necessary to provide physical resources and users a safe and secure working environment, is managed. This standard is maintained in accordance with state, federal, and university regulations and policies and, at a minimum, will include and establish the following subjects:

- How credential-based electronic physical access requests are structured and processed to ensure that access requests are handled in a secure manner.
- How credential-based electronic physical access is audited to ensure that accounts only have access to necessary locations across sites.
- Requirements for technology resource-related physical infrastructure installations, include the following:
    - Network cabling requirements, including rating, plenum vs. non-plenum, shielding, and coloring.
    - Fiber optic cabling and connector requirements.
    - MDF and IDF minimum requirements.
    - Exposed wiring requirements.
- MDF and IDF Physical Access Security Controls, including, but not limited to the following:
    - Point(s) of entry must be secured with either key-based or credential-based electronic access controls.
    - Key and credential-based electronic access to such spaces must be limited to only IT Organization staff.
    - Keys to access these spaces shall be managed only by IT Organization staff.
    - The room cannot be a shared space or be utilized for any unauthorized purpose (e.g. custodial closet, general storage, general workspace).
- MDF and IDF Environmental Security Control requirements.
- MDF and IDF Physical and Environmental security auditing requirements.

11. Logical Access Security Standard

Each ASU System IT Organization shall maintain a supplemental Logical Access Security Standard, separate from this policy, which establishes standards for account creation, management, and information system management across all systems and accounts within the university. This standard is maintained in accordance with state, federal, and university regulations and policies and, at a minimum, will include and establish the following subjects:

- Restrictions regarding duplicated passphrases used to access campus information systems.
- Establishes security levels for use in determining account security requirements.
- Establishes minimum passphrase length requirements based on account security level.
- Establishes minimum passphrase complexity requirements based on account security level.
- Establishes passphrase rotation schedules based on account security level.
- Establishes account lockout thresholds based on account security level.
- Restrictions regarding the management and use of default administrative accounts on endpoints, in alignment with the requirements outlined in this policy for the technology resource management standard.
- Restrictions regarding the configuration, use, and access of local user accounts in alignment with the requirements outlined in this policy for the technology resource management standard.
- Detailed account management requirements to ensure that accounts are handled in a secure manner during their lifecycle.

12.Artificial Intelligence Governance Standard

Each ASU System IT Organization shall maintain a supplemental Artificial Intelligence Governance Standard, separate from this policy, which outlines how AI agents, tools, and processing are maintained in accordance with state, federal, and university regulations and policies. At a minimum, this will include and establish the following subjects:

- Information regarding the AI and ADT approved for use on the campus.
- Information regarding the AI-powered, meeting transcription and recording tools approved for use on the campus.
- Enforcement and monitoring mechanisms of AI and ADT usage on the campus.
- Information outlining the ethical use of AI on campus, ensuring transparency in its official use.
- Defined platform-review cadence and risk-management steps for AI and ADT utilized on the campus.
- Data, classified as **confidential** or **regulated,** is not permitted for entry to any AI agent, tool, or processing method, unless explicitly authorized.
- Internal data is permitted for entry to AI agents, tools, and processing methods on university-maintained-and-approved platforms.

13. Risk Assessment and Vendor Management Standard

Each ASU System IT Organization shall maintain a supplemental Risk Assessment and Vendor Management Standard, separate from this policy, which outlines the ways in which technology resource risk is assessed and the relevant ways that technology vendors are managed. This standard is maintained in accordance with state, federal, and university

regulations and policies and, at a minimum, will include and establish the following subjects:

- Security documentation requirements for vendor risk assessments to be performed. (e.g., SOC 2, ISO 27001).
- Information regarding which security documentation is required, based on the class of data the technology or digital service will interact with.
- Vendor security documentation review cadence.
- Vendor security documentation storage and management.
- Minimum vendor security requirements, based on the class of data the technology or digital service interacts with.
- Enforcement and non-compliance requirements.

14. Compliance Framework Implementation and Assurance Standard

Each ASU System IT Organization shall maintain a supplemental Compliance Framework Implementation and Assurance Standard, separate from this policy, which outlines the ways in which external compliance frameworks are managed and audited, in order to ensure compliance with their requirements. This standard is maintained in accordance with state, federal, and university regulations and policies and, at a minimum, will include and establish the following subjects:

- An exhaustive list of each compliance framework that ASU System campuses are required to comply with.
- Shared compliance controls for each listed compliance framework, including the following:
    - Maintaining a formal internal audit schedule for each framework. This audit will serve as a self-study of university compliance and will be used to determine gaps for formal remediation. This internal audit shall occur no less than once every 12 months.
    - Maintaining a formal audit procedure for each compliance framework.
    - Establishing scope of responsibility for each framework. This will ensure that the correct stakeholders are identified and held accountable for their portion of framework compliance requirements.
- Unique compliance controls and requirements for each individual compliance framework.
- Monitoring and enforcement mechanisms to ensure that all ASU System campuses are regularly reviewing and attesting to the requirements for each compliance framework.

15. Incident Response Plan

Each ASU System IT Organization shall maintain a supplemental Incident Response Plan, separate from this policy, which outlines the ways in which the IT Organization would respond to an IT security incident or emergency. This standard is maintained in accordance

with state, federal, and university regulations and policies and, at a minimum, will include and establish the following subjects:

- Law enforcement and external entity notification information. (e.g. FBI, University Police Department, City Police)
- Containment and evidence preservation requirements.
- Roles, responsibilities, and decision-making authority details.
- Post-incident review checklist.
- Security Panel or IT Organization specific group tasked with incident response) contact information.
- A template incident report within an appendix.
- A responsibility matrix detailing which responsible parties are charged with certain duties.
- A full step-by-step guide detailing the ways in which a potential incident should be worked from the first notification/initial discovery.

16. Business Continuity and Disaster Recovery Plan

Each ASU System IT Organization shall maintain a supplemental Business Continuity and Disaster Recovery Plan, separate from this policy, which outlines the ways in which the IT Organization plans to ensure continuity of business operations and recovery from an environmental disaster. This standard is maintained in accordance with state, federal, and university regulations and policies and, at a minimum, will include and establish the following subjects:

- An incident classification matrix that outlines the ways that incidents and disasters will be categorized.
- The establishment of a Crisis Assessment and Management Team (CAMT) within each IT Organization that is responsible for evaluating incidents, assigning crisis classification, authorizing plan activation, and providing executive updates.
- Recovery objectives based on both incident classification and resource criticality.
- IT Organization backup and data protection practices that ensure both restoration from a severe incident and retention in alignment with campus and state requirements and regulations.
- A formal restoration sequence, with critical services, such as E911 and communication methods being the first in the sequence for restoration.
- Internal and external communication requirements and responsibilities.
- A formal testing, training, exercise, and review process that requires, at a minimum, that the following activities be completed by the IT organization:
    - Business Continuity & Disaster Recovery tabletop exercises are conducted annually to validate roles, decision making authority, escalation paths, and internal and external communication coordination.

- Comprehensive After Action Reviews (AARs) are completed following annual exercises, as well as declared major incidents to document lessons learned, identify gaps, and develop corrective action plans. Corrective actions are tracked to completion.
- Targeted technical recovery tests for critical enterprise systems, communications infrastructure, ERP data, and cloud hosted services are conducted on a recurring basis, not less than annually, and may be scheduled more frequently for systems classified as Critical or Priority.
- Backup restoration drills are performed quarterly to validate data recoverability, backup integrity, immutability protections, and alignment with defined RTO and RPO targets.

17. Technology Resource User Education Standard

Each ASU System IT Organization shall maintain a supplemental Technology Resource User Education Standard, separate from this policy, which outlines the ways in which the IT Organization plans to ensure that users are adequately educated on basic technology resource topics and skills. This standard is maintained in accordance with state, federal, and university regulations and policies and, at a minimum, will include and establish the following subjects:

- New user training requirements for faculty, staff, students, contractors, affiliates, and members of the ASU System community.
- Ways that on-demand educational documents are maintained and stored for user access.
- Methods for contacting the IT Organization's help desk, or tier 1 user support staff, for assistance.
- Procedures for finding and accessing *ad hoc* training sessions that may be provided throughout the semester.
- Information regarding mandatory, technology resource specific, training, such as Criminal Justice Information Services (CJIS) training.
- Information regarding mandatory AI and ADT training.
- Information regarding annual employee compliance training required by the Board of Trustees.
- Information regarding IT Organization tabletop exercises.
- Techniques for finding ways that the effectiveness of the user education program is monitored and updated.

18. Enterprise Resource Planning (ERP) Standard

Each ASU System IT Organization shall maintain a supplemental Enterprise Resource Planning (ERP) Standard, separate from this policy, which outlines the ways in which the IT Organization plans to ensure that ERP technology resources are effectively managed, maintained, and utilized by relevant users. This standard is maintained in accordance with

state, federal, and university regulations and policies and, at a minimum, will include and establish the following subjects:

- ERP governance structure, including institutional data steward roles and responsibilities, decision-making authority, and cross-functional stakeholder participation.
- Governance processes for shared ERP tables, configurations, integrations, and enterprise-wide data structures, including stakeholder review, approval, communication, and change management requirements.
- Data standardization, integrity, and institutional data management requirements for institution-specific ERP tables, configurations, and data elements.
- ERP integration, change management, patch management, testing, deployment, and vendor coordination requirements.
- ERP access provisioning, least privilege, segregation of duties, service account management, and annual access review requirements.
- Direct Banner ERP access shall be audited no less than once per year.
- Platforms that integrate with the Banner ERP system shall have their access audited no less than once per year.
- Requirements for protecting Confidential and Regulated institutional data within the ERP environment, including applicable AI governance restrictions and data handling requirements.
- ERP incident response, recovery, business continuity, backup, and vendor coordination requirements for cloud-hosted and institutionally managed ERP services.
- Compliance, vendor management, and third-party risk management requirements associated with ERP operations, including applicable regulatory, contractual, and institutional obligations.

19. Policy Review

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

Effective Date: October 16, 2026
Next Review Date: October 16, 2027
Version: 1.0

Referenced Policies, Standards, and Procedures:

- Data Security and Classification Policy
- Arkansas Act 848

(Adopted by the Arkansas State University System Board of Trustees on October 16, 2026, Resolution 26-50.)