Appropriate Use of Information and Technology Resources Policy

Effective Date: October 16, 2026

1. Purpose

The Arkansas State University System (ASU System) invests substantial and sufficient resources to acquire and operate information technology (IT) assets, such as hardware, software, and internet connections. The ASU System 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 IT resources will ensure that students, faculty, and staff have adequate access to information and technology over the long term. The following regulations are established to define acceptable uses of IT resources, and to ensure that information technology resources promote the basic functions of the ASU System in teaching, learning, research, administration, and public service.

2. Scope

This policy applies to all faculty, staff, students, contractors, affiliates, and members of the ASU System community who access the ASU System IT infrastructure and associated resources. This policy applies to all digital 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 the following:
    - Machines, devices, and transmission facilities used in information processing, including computers, word processors, terminals, telephones, cables, software, and related products.
    - Devices that 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, including consultants and contractors.
    - All email accounts issued by the ASU System.
- **IT Organization** - The unit at each institution responsible for providing information technology solutions and services.
- **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.
- **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.
- **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 during the course of ASU System business.
- **Specific Authorization** - Documented permission provided by the applicable Systems Administrator.

4. Appropriate Use of Technology Resources

The ASU System's information and technology resources may be used only for their authorized purposes – that is, to support the research, education, administrative, and other functions of ASU System institutions. Appropriate uses of technology include, but are not limited to, the following:

- Accessing the internet for work-related research and information gathering.
- Utility and applications software that accomplish tasks and fulfill job functions.
- Communication and collaboration between staff and/or other appropriate entities.

- Supporting teaching and learning activities, including course delivery, instructional design, and student engagement.
- Using technology resources to support campus operations, events, and official university business functions.
- Conducting approved research activities in compliance with university policies, grant requirements, and applicable regulations.
- Engaging in data analysis, reporting, and decision-making activities that support institutional planning and assessment, in accordance with the Data Classification Policy.

5. Appropriate Network Use and User Account Guidelines

The ASU System's networks and user accounts may be used only for their authorized purposes – that is, to support the research, education, administrative, and other functions of ASU System institutions. Use of the ASU System's internet connection and email resources is a privilege, and it is expected that all users will abide by acceptable use requirements as outlined by this policy. Appropriate uses of ASU System networks and user accounts include, but are not limited to, the following:

- Users may only access those computer accounts which have been authorized for their use.
- Users may only use accounts for their authorized purposes. This restriction shall not prevent informal communication, but accounts must not be used for private consulting or personal gain.
- Users must understand that network administrators may review files and communications to maintain system integrity and ensure that they are using the system responsibly. Employees should not expect files and documents to remain private.
- Users must not share credentials or allow others to access resources of their unique accounts.

6. Appropriate Use of Artificial Intelligence (AI) and Automated Decision Tools (ADT)

The ASU System permits the use of artificial intelligence (AI) and automated decision tools (ADT) for academic, instructional, research, and administrative purposes, when such use is explicitly authorized by institutional policy, academic program, or course instructor.

This authorized use must be ethical, transparent, and aligned with the academic integrity standards and acceptable use standards of each campus. Users remain fully responsible for the accuracy, originality, and compliance of all work produced with AI or ADT assistance, and all outputs must be reviewed and validated by the user prior to utilizing in institutional decision-making. Unauthorized or undisclosed use of AI or ADT may constitute a violation of institutional policy or may constitute academic misconduct standards.

Artificial intelligence and automated decision tools are authorized for use with data that is classified as appropriate for such systems, as outlined in the Data Security and Classification Policy. Regulated, confidential data, as outlined in the Data Security and Classification policy, shall not be entered into AI and ADT unless explicitly approved and contractually protected.

7. Process

Although this policy sets forth the general parameters of appropriate use of technology resources, the ASU System's faculty, students, and staff should consult their respective handbooks and campus operating procedures for more detailed statements on permitted use and the extent of use that the ASU System considers appropriate, in light of its varying roles within the community. In the event of conflict between other guidelines and the System Appropriate Use of Information and Technology Resources Policy, the System Appropriate Use Policy will prevail. The following sections outline details of this process.

8. Proper Authorization

Users are entitled to access only those technology resources that are consistent with their authorization. Access is limited to members of the ASU System community, its faculty, staff, students, and other specifically authorized individuals.

9. Ownership

All data, stored on university technology resources, is owned by the ASU System. Intellectual property rights will, of course, be recognized as established by policy. Possession, assignment, or use of an institutional technology resource does not constitute ownership. All institutional technology resources will remain the sole property of the institution at all times, regardless of who is in physical custody of the technology resource.

10. Privacy

Appropriate uses of technology concerning privacy of information include the following:

- The ASU System reserves the right to monitor and/or log all network activity, with or without notice, including email and all website communications, and, therefore, users should have no reasonable expectation of privacy in the use of these resources.
- The ASU System will not monitor email transmissions on a regular basis, though the construction, repair, operations, and maintenance of electronic messaging systems may occasionally result in monitoring transmitted or stored messages.
- Messages may be monitored during the course of investigations of suspected illegal or prohibited activity; in order to respond to a Freedom of Information Act request; in order to respond to a discovery request or other legal process or proceeding; and when otherwise necessary to the operations of the agency. Because the ASU System is a state agency, all electronic communications and documents are presumed to be subject to the Freedom of Information Act.

11. Specific Proscriptions of Use

The following categories of use are inappropriate and are prohibited:

I. **Use in violation of law.** Illegal use of technology resources – that is, use in violation of civil or criminal law or regulation at the federal, state, or local levels – is prohibited. Examples of such uses include the following: promoting a pyramid scheme, accessing or distributing illegal material, copyright infringements, and/or making terroristic threats.

With respect to copyright infringements, users should be aware that copyright law governs (among other activities) the copying, display, or use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

II. **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others.** Users must not deny, attempt to deny, or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or flooding an individual, group, or system with numerous or large email messages. Other behaviors that may cause excessive network traffic, or computing load are also prohibited.

III. **Use that is inconsistent with the ASU System's public service status.** The university is a nonprofit, public service organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of technology resources for non-ASU System purposes is generally prohibited, except if specifically authorized and permitted under the ASU System's conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the ASU System's educational, administrative, research, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization. Commercial advertising is strictly prohibited unless authorized by contract with the commercial vendor.

Utilization of technology resources, in a way that suggests ASU System endorsement of any political candidate or ballot initiative, is also prohibited. Users must refrain from using technology resources for the purpose of lobbying that connotes ASU System involvement. Technology resources shall not be used to express a personal political opinion to an elected official, unless the opinion is within the scope of the employee's regular job duties or requested by an elected official or public entity. (Act 504 of 2023)

IV. **Harassing or threatening use.** This category includes, for example, repeated unwelcome contacts with another.

V. **Use damaging the integrity of the ASU System or other technology resources.** This category includes, but is not limited to, the following:

a. **Attempts to defeat system security.** Users must not defeat, or attempt to defeat, any IT system's security – for example, by "cracking," decoding, guessing, or applying the identification or password of another user, or compromising system/data security mechanisms. (This provision does not prohibit, however, the IT Organization or Systems Administrators from using security-related programs within the scope of their Systems Authority.)

b. **Unauthorized access or use.** The ASU System recognizes the importance of preserving the integrity of data stored by individuals in technology resources. Users must honor this principle by neither seeking to obtain unauthorized access to technology resources, nor permitting or assisting any others doing the same. For example, a non-ASU System organization or individual may not use non-public technology resources without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-ASU System organizations or individuals across the ASU System network without specific authorization. Similarly, users are prohibited from accessing technology resources that they are not authorized to access. Furthermore, users must not make, or attempt to make, any deliberate, unauthorized changes to data on an IT system. Users must not intercept, or attempt to intercept or access, data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

c. **Disguised use.** Users must not conceal their identity when using technology resources, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as, or impersonating, others or otherwise using a false identity.

d. **Distributing computer viruses.** Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

e. **Modification or removal of data or equipment.** Without specific authorization, users may not remove or modify any ASU System-owned-or-administered equipment or data from ASU System property or technology resources.

f. **Use of unauthorized devices.** Users must not physically or electronically attach any additional devices to the IT infrastructure or related resources that impede, interfere, or otherwise cause harm to the IT infrastructure or related resources.

VI. **Use in violation of external data network policies.** Users must observe all applicable policies of external data networks when using such networks.

12. ASU System Access

In accordance with state and federal law, the ASU System may access all aspects of technology resources without the consent of the user. Such access will be made in circumstances including, but not limited to, the following:

- When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the technology resources; or
- When authorized by federal, state, or local law or administrative rules; or
- When there are reasonable grounds to believe that a violation of law or a breach of ASU System policy, may have taken place, and access and inspection or monitoring may produce evidence related to the transgression; or
- When such access to a technology resource is required to carry out essential business functions of the ASU System; or
- When required to preserve public health and safety and/or system or data integrity or user privacy.

ASU System access without the consent of the user, will occur only with the approval of the appropriate administrator, or their respective delegates, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. The ASU System, through the Systems Administrators, will log all instances of access without consent. Systems Administrators will also log any emergency entry, within their control, for subsequent review by appropriate university authority.

In addition to accessing the technology resources, the ASU System, through the appropriate System Administrator, may deactivate a user's IT privileges, whether or not the user is suspected of any violation of this policy, when it is necessary to preserve the integrity of facilities, user services, or data. The System Administrator will attempt to notify the user of any such action.

By attaching privately owned personal computers or other devices to the ASU System's network, users consent to the ASU System's use of scanning programs for security purposes of those resources while attached to the network.

Most Systems Administrators routinely log user actions, in order to facilitate recovery from system malfunctions and for other management purposes. All Systems Administrators are required to establish and post procedures concerning logging of user actions, including the extent of individually identifiable data collection, data security, and data retention. Encrypted files, documents, and messages may be accessed by the university under the above guidelines.

13. Enforcement Procedures

- **Complaint of Alleged Violations.** An individual, who believes that they have been harmed by an alleged violation of this policy, may file a complaint in accordance with established ASU System grievance procedures (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to

report the alleged violation to the Systems Authority overseeing the facility most directly involved, or to the IT Organization, which must investigate the allegation and (if appropriate), must refer the matter to ASU System's disciplinary and/or law enforcement authorities.

- **Reporting Observed Violations.** If an individual has observed or is otherwise aware of a violation of this policy, but has not been harmed by the alleged violation, they may report any evidence to the Systems Authority overseeing the facility most directly involved, or to the IT Organization, which must investigate the allegation and (if appropriate), refer the matter to ASU System's disciplinary and/or law enforcement authorities.
- **Disciplinary Procedures.** Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the applicable Handbook.
- Systems Administrators and the IT Organization may participate in the disciplinary proceedings, as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, Systems Administrators, and the Information and Technology Services unit are authorized to investigate alleged violations.
- **Legal Liability for Unlawful Use**. In addition to ASU System discipline, users may be subject to criminal prosecution, civil liability, or both, for unlawful use of any technology resources.
- **Appeals.** Users found in violation of this policy may appeal or request reconsideration of any imposed disciplinary action, in accordance with the appeals provisions of the relevant disciplinary procedures.

14. 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: 1.3

Referenced Policies, Standards, and Procedures:Arkansas Act 504

(Adopted by the Arkansas State University Board of Trustees on March 4, 2011, Resolution 11- 03 supersedes Arkansas State University-Jonesboro Appropriate Use of Information and Technology Resources Policy (Appropriate Use Policy) of March 8, 2002. Revised August 1, 2023, to comply with Act 504 of 2023. Revised October 16, 2026, Resolution #26-47.)