

2.1 Artificial Intelligence Governance Standard

Applicability Statement

This standard governs the use, procurement, development, administration, and oversight of Artificial Intelligence (AI) and Automated Decision Tools (ADT) when used on Arkansas State University-owned or managed technology resources, or when used to conduct official university business, regardless of whether those activities occur on university-owned or personally owned devices.

This standard is not intended to govern the academic use of AI by students for coursework, assignments, research, or other learning activities, except when students are acting on behalf of the university in an employment or official institutional capacity. Students should refer to the Arkansas State University Ethical Use of Artificial Intelligence Policy, applicable academic integrity policies, and any college-, department-, or course-specific AI requirements established by their instructors regarding permissible uses of AI in academic work.

Effective Date: July 1, 2026

Revised Date: July 1, 2026

1. Purpose

The purpose of this standard is to establish the required controls, governance, and operational requirements for the use of Artificial Intelligence (AI) and Automated Decision Tools (ADT) within the Arkansas State University (A-State) environment. This standard ensures that AI technologies are used ethically and in compliance with applicable laws, regulations, and university policies.

2. Scope

This standard applies to all faculty, staff, students, contractors, affiliates, and members of the A-State community who use, develop, or oversee Artificial Intelligence or Automated Decision Tools when conducting university business or using university technology 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

Artificial intelligence - 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 - A system or service that uses artificial intelligence and 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:

- 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 artificial intelligence governance 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.

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.

Human Resources - Responsible for the maintenance and enforcement of disciplinary requirements outlined in this standard.

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

Procurement Services - Responsible for developing and maintaining processes for the procurement of Artificial Intelligence, Automated Decision Tools, and any third-party platform in partnership with ITS. Responsible for ensuring that risk assessments are performed prior to procurement.

ITS - Responsible for developing and maintaining processes for the procurement of Artificial Intelligence, Automated Decision Tools, and any third-party platform in partnership with Procurement Services. Responsible for maintaining a centralized inventory of all approved AI and ADT Systems.

IT Security - Responsible for completing adequate security risk assessments within the processes maintained by ITS and Procurement Services.

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.

6. Approved AI Tools and Platforms

A-State users are not authorized to use AI or ADT tools that have not been formally reviewed and approved via ITS and Procurement Services vetting processes. To view live applications that have been approved for institutional use, please access the link below.

[Approved Software Directory](#)

7. Artificial Intelligence Assistants

Artificial Intelligence powered meeting transcription and recording tools, such as those integrated into Microsoft Teams or Zoom, are not appropriate for all settings and should only be used in meetings where their presence aligns with meeting objectives, privacy expectations, and institutional policy.

Examples where AI assistants are not permitted include, but are not limited to:

- Any discussion involving regulated data, including FERPA, HIPAA, or CJIS data.
- Any discussion without the informed consent of all attendees and participants.
- Any AI Assistant added to a discussion by a contractor, affiliate, or member of the system community.

All Artificial Intelligence powered meeting transcription and recording tools must be approved through the standard procurement processes as dictated by Procurement Services. This includes any tools that are available for use free of charge.

8. Data Classification

To ensure alignment with the Arkansas State University System Artificial Intelligence Governance Policy and the Data Classification and Security Policy, this standard establishes the following requirements:

- Public data may be used with AI tools as long as no sensitive non-publicly available data is included.
- Internal data is permitted for entry to AI agents, tools, and processing methods on A-State maintained and approved platforms.
- Data classified as confidential or regulated is not permitted for entry to any Artificial Intelligence agent, tool, or processing method unless explicitly authorized.

9. Monitoring and Enforcement

A-State shall monitor university technology resources for unauthorized or inappropriate use of AI or ADT tools. This monitoring includes, but is not limited to:

- Review of network logs to identify unauthorized utilization of AI or ADT tools.
- Review of application installations on university owned and maintained technology resources to identify unauthorized utilization of AI or ADT tools.
- Receipt and subsequent investigation of user reported unauthorized or inappropriate use of AI and ADT tools.

Enforcement mechanisms include, but are not limited to:

- Disablement of the offending user's university account.
- Network containment of noncompliant technology resources.

- Removal of the noncompliant AI or ADT tool from university accounts and technology resources.
- Discipline in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the applicable Handbook.

10. Ethical and Responsible Use of AI and ADT Tools

A-State requires an authorized human user or designee to make any final decision in the course of his or her employment, regardless of what artificial intelligence or automated decision tool the employee or designee recommends.

Use of AI or ADT tools must be ethical, transparent, and aligned with the academic integrity standards and acceptable use standards of A-State. Users remain fully responsible for the accuracy, originality, and compliance of all work produced with AI or ADT assistance.

Users are responsible for disclosing when AI is used for decision making, content generation, or other impactful processes. Unauthorized or undisclosed use of AI or ADT tools may constitute a violation of institutional policy or academic misconduct standards.

11. User Training Requirements

The A-State Employee Training & Development Authority 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 and required in all new employee and student training and will be completed on an annual basis.

12. Risk Management Review

Due to the variable risk that comes with AI products and the function they are set to perform, risk levels may be vastly different based on the AI product. In order to properly assess and secure internal or outsourced data, A-State must ensure a risk assessment is performed to identify, assess, and manage risks associated with AI and ADT tools.

This risk assessment applies to standalone AI tools, ADT tools, artificial intelligence powered meeting transcription and recording tools, as well as third-party platforms and integrations that utilize AI to process institutional data.

Security risk assessments will be completed by the IT Security team as part of the Technology and Digital Services Purchase Pre-Authorization review process jointly maintained with Procurement Services and ITS. Security documentation from this review will be annually reviewed and refreshed to ensure security practices are still in alignment with A-State requirements.

Procurement of Artificial Intelligence, Automated Decision Tools, and any third-party platforms and integrations that utilize AI must follow all standard procurement processes as dictated by

13. 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
- Data Security and Classification Policy
- Faculty, Staff, and Student Handbooks

Revision #4

Created 2026-06-26 01:22:35 UTC by Christopher Boothman

Updated 2026-08-05 14:56:35 UTC by Christopher Boothman