



Policy Title: Artificial Intelligence Acceptable Use Policy

Policy Version: 1.0

Effective Date: 02/26/2026

1. Purpose

This policy establishes clear standards for the ethical, secure, transparent, and responsible use of Artificial Intelligence (AI) systems by the Executive Branch to protect the security and privacy of Arkansas data. It ensures that all AI use aligns with applicable laws, statewide policies, and the State's mission to serve the public interest with integrity, accountability, and fairness.

2. Scope

This policy applies to all Executive Branch employees, contractors, vendors, and third parties who design, procure, implement, or use AI tools or systems on behalf of the State of Arkansas. It covers all forms of AI and automated technologies, including but not limited to:

- Generative AI and large language models (LLMs)
- Machine-learning and predictive analytics systems
- Automated decision-making tools
- Natural language, image, or signal processing systems
- Other algorithmic, data-driven, or automated decision-support technologies

3. Definitions

Artificial Intelligence: A machine-based system that, given a set of human-defined objectives, can make predictions, recommendations, or decisions influencing real or virtual environments.

Automated Decision System: Any system that uses AI to make or substantially influence consequential decisions affecting individuals, groups, or organizations.

Generative Artificial Intelligence: A class of AI systems designed to create new content such as text, images, audio, code, or other outputs based on patterns learned from training data.

Sensitive Data: Any information subject to enhanced protection, including personally identifiable information, protected health information, criminal justice or law-enforcement data, or any data protected under state or federal law.

4. Guiding Principles

The Department of Shared Administrative Services (SAS) and the Executive Branch shall govern all AI use under the following principles:

- **Lawfulness & Ethics:** AI must comply with all applicable federal and state laws, policies, and ethical standards.



Department Shared Administrative Services Office of State Technology

- **Transparency:** The purpose, data sources, and decision logic of AI systems must be documented and disclosed where practicable.
- **Human Oversight & Accountability:** Human judgment remains essential. No AI system may make final decisions affecting individual rights or obligations without human review.
- **Fairness & Non-Discrimination:** AI must be designed, tested, and monitored to prevent bias or disparate impacts.
- **Security & Privacy:** All AI-related data must conform to SAS cybersecurity, data governance, and privacy protocols.
- **Public Trust:** AI use shall promote safe, secure, and efficient public service while maintaining public confidence in government operations.

5. Acceptable Use

Authorized users may:

- Use SAS-approved AI systems to enhance administrative efficiency, data analysis, research, communications, and innovation in alignment with the mission of the Executive Branch and its policies.
- Use AI for decision support only when final decisions are subject to qualified human verification.
- Procure, develop, or deploy AI systems exclusively through SAS's approved technology governance, procurement, and risk-assessment channels.

6. Prohibited Uses

Users shall not:

- Input sensitive or confidential data, including personally identifiable or protected health information, into public or unapproved AI tools. Any AI use involving sensitive or confidential information shall be approved by SAS prior to being used.
- Rely solely on AI to make binding legal, personnel, financial, or policy decisions without human review.
- Generate or distribute false, misleading, defamatory, or discriminatory content using AI.
- Create audio or visual, including photographs, video, or voice, files of an identifiable individual.
- Use AI to evade records retention requirements, system and cybersecurity obligations, or otherwise engage in any illegal activities or activities otherwise prohibited by federal or state law.
- Deploy AI for surveillance, profiling, or tracking without explicit statutory authority and governance oversight.
- Use AI to engage in any activity for personal financial gain.
- Use AI to engage in lobbying activities.



Department Shared Administrative Services Office of State Technology

7. Data Governance and Security

- All AI systems must comply with SAS and statewide data and cybersecurity standards and policies.
- AI-generated outputs must be traceable, auditable, and retained in accordance with the state records retention policies.
- Data derivation history, model versioning, and change management must be documented.

8. Human Oversight and Accountability

- Employees remain responsible for the accuracy, legality, and appropriateness of all AI-assisted work.
- Supervisors must ensure AI outputs are reviewed for factual accuracy, policy compliance, and tone.
- Automated decision systems that materially affect rights or benefits must include documented review procedures and decision logs.

9. Review & Approval of AI Systems

- SAS may utilize an AI review team to oversee the inventory, risk classification, approval, and lifecycle management of AI systems.
- All new AI tools must be reviewed and approved through the Technology Investment Justification process before deployment, regardless of the cost, including the enablement of new AI features being added to existing tools.
- SAS will maintain a registry of approved AI tools, version histories, and authorized use cases on the Office of State Technology website.
- Use of unapproved AI tools may result in disciplinary action.

10. Training & Awareness

All employees, contractors, and vendors using or overseeing AI must complete AI training covering the ethical and secure use of AI, including data protection and confidentiality requirements. More advanced training may be required for employees in certain positions. Departments are responsible for ensuring employee, contractor, and vendor compliance with training requirements.

11. Compliance & Enforcement

- Violations of this policy may result in disciplinary action, including suspension of access, termination, or referral for administrative or legal review.
- SAS reserves the right to audit AI usage, review decision logs, inspect training data or models, and report findings to oversight authorities.
- SAS will periodically update its AI policies in response to evolving laws, technologies, and risks.



Department Shared Administrative Services
Office of State Technology

12. Statutory & Regulatory References

- Ark. Code Ann. § 25-1-128, as amended by Act 848 of 2025, requiring public entities to establish AI use policies.
- Act 159 of 2025, governing the protection of an individual whose photograph, voice, or likeness is reproduced through means of artificial intelligence.
- Act 827 of 2025, governing the criminal offense of unlawful creation and distribution of deepfake visual material.
- Act 927 of 2025, governing ownership of model training data and generative AI outputs within Arkansas.
- Applicable federal privacy, records, and cybersecurity standards, including the Federal Information Security Modernization Act (FISMA) and NIST AI Risk Management Framework (AI RMF 1.0).

13. Policy Review

This policy shall be reviewed annually, or sooner if significant legal, technological, or organizational changes occur.

14. Revision History

Date	Description of Change	Reviewer
February 26, 2026	Moved from Draft to Final	Jay Harton State Chief Information Officer