AI in Arkansas

Safety, Security, & Trust Report

Office of State Technology
AI & Analytics Center of Excellence

September 2025

Trust as the Foundation for AI

Summary

The Arkansas Artificial Intelligence & Analytics Center of Excellence (AI CoE) was established by Governor Sarah Huckabee Sanders to study and offer recommendations for the safe use of artificial intelligence within Arkansas state government.

AI offers transformative potential for Arkansas government, but it must be implemented safely, securely, and transparently. This report recommends key elements to establish a foundation of trust to allow AI initiatives to move fast, but always with safety.

Key Recommendations

- Governance & Stewardship:
  - Formalize AI governance as part of statewide IT governance.
  - Establish the Chief Artificial Intelligence Officer role to lead the AI governance and adoption strategy.
  - Apply the National Institute of Standards and Technology (NIST) AI Risk Management Framework to evaluate and approve AI implementations consistently.
  - Publish statewide AI policies to implement responsible AI guardrails including acceptable use, procurement, transparency, and privacy protection.
  - Leverage the Technology Investment Justification (TIJ) process for AI investments to provide consistent, secure, and efficient adoption.
- Data & Infrastructure Foundation:
  - Utilize the Arkansas Data Hub shared service data infrastructure to support the secure deployment and governance of AI government solutions.
- Cybersecurity:
  - Launch an AI & cybersecurity collaboration program with the Arkansas National Guard.
- Transparency:
  - Publish an AI inventory with citizen-facing dashboards.
- Staff AI Literacy:
  - Implement AI literacy training for all state employees.

Governance & Stewardship

AI is already reshaping public service delivery, but without proper governance it can lead to risks including data leakage, unintended biases, and loss of public trust. For Arkansas, governance is not a hindrance to innovation, but instead it is the foundation that makes rapid, responsible adoption possible.

The goal is simple: to move fast, but always with safety.

AI Governance

Arkansas has established a clear, enterprise-wide Information Technology (IT) governance structure under the Office of State Technology (OST). This team ensures that IT, data, cybersecurity, and privacy governance are fully integrated rather than siloed. This centralized governance model should be expanded to include AI governance. This approach is consistent with the White House AI Executive Order (2023) and the Office of Management and Budget (OMB) AI guidance (2024), which require federal agencies to establish clear AI governance structures and inventories. Arkansas should align with these standards to ensure interoperability and strengthen federal partnerships.

Chief AI Officer

A Chief Artificial Intelligence Officer role should be established to lead AI governance practices in alignment with data and IT governance, including an AI advisory panel to ensure responsible oversight of AI initiatives. The State Chief Information Officer would oversee a coordinated governance team consisting of the State Chief Data Officer, State Chief Information Security Officer, and Chief Privacy Officer. This role also mirrors federal direction under the America's AI Action Plan, which emphasizes dedicated leadership capacity to oversee responsible AI adoption.

AI Standards & Frameworks

Adoption of the National Institute of Standards AI Risk Management Framework ensures AI implementations are evaluated consistently across the state. Statewide AI policies should be published covering acceptable use, procurement, transparency, and privacy protections. These standards should ensure that AI tools are vetted for risk before implementation and used in ways that protect Arkansans.

AI Policies

Act 848 of 2025 requires public entities to create a policy concerning the authorized use of artificial intelligence. A draft AI policy for the State of Arkansas is included in Appendix A.

Responsible AI Guardrails

Arkansas' governance and stewardship framework should make clear that AI adoption will be safe, secure, and transparent. This is not about slowing progress, but about creating conditions to innovate, learn by doing, adopt, and scale AI with confidence.

The following principles for responsible AI should be adopted for implementation through AI governance and stewardship:

- **Privacy** – Protect citizen data and use AI in ways that safeguard personal information.
- **Transparency** – Clearly communicate when and how AI is being used.
- **Explainability** – Ensure AI decisions can be understood and explained to stakeholders.
- **Human Oversight** – Keep humans in the loop for high-stakes or sensitive decisions.
- **Accountability** – Create an AI Use Policy to establish clear responsibility for outcomes of AI systems.
- **Security** – Protect AI systems from adversarial attacks or manipulation.
- **Capacity & Literacy** – Equip staff with the skills to use and govern AI responsibly.
- **Misuse Prevention –** Put in place controls to prevent harmful, biased, or unethical uses of AI.

These guardrails reflect national priorities outlined in the White House AI Executive Order and America's AI Action Plan, reinforcing Arkansas' commitment to aligning state practices with federal standards for trustworthy AI.

AI Procurement

Procurement can be a powerful lever for responsible AI adoption. Arkansas should treat it as a strategic enabler, ensuring that acquisitions accelerate innovation while remaining secure and interoperable. The TIJ process should be applied to AI projects and procurements as a consistent, predictable, and streamlined pathway for adoption. This approach would align projects with existing technology standards, ensuring that AI solutions are integrated into a cohesive statewide environment rather than siloed efforts.

This approach advances the America's AI Action Plan priority of modernizing procurement to enable rapid, responsible deployment of AI in government.

Data & Infrastructure Foundation

A strong data and infrastructure foundation is essential for safe, scalable AI. Without it, departments risk fragmented implementations and vulnerabilities that could undermine security, efficiency, and trust. Arkansas' approach should be to build once, share widely, and govern consistently ensuring that every AI solution is anchored in secure, enterprise-grade infrastructure.

Arkansas Data Hub

The Arkansas Data Hub, operated by the Arkansas Data Office within OST, provides the backbone for AI adoption. It integrates data from across departments into a governed, secure environment with enterprise metadata, lineage, and access controls along with robust support for data management, sharing, integration, and use. This ensures that AI models can be trained and deployed on high-quality, trusted data.

Arkansas should utilize the Arkansas Data Hub shared service infrastructure to support secure deployment and governance of AI solutions connected to high-quality data under comprehensive

data and AI governance. This can help ensure that outputs are explainable, traceable, and auditable, preventing data leakage and improper use and increasing trust and adoption.

Arkansas' existing data and infrastructure foundation ensures that AI is not built on shaky ground. By leveraging shared services with embedded privacy, governance, and security controls, Arkansas can leverage its strong existing foundation to accelerate innovation while minimizing risk, enabling departments to scale AI responsibly across the state.

Cybersecurity

AI introduces both opportunities and new vulnerabilities. Adversaries could leverage AI to increase the frequency and maturity of intrusion attempts, while AI can also strengthen cyber defenses by detecting anomalies at scale. Arkansas should integrate AI and cybersecurity from the ground up to ensure a strong state security posture that leverages AI for improved efficiency and effectiveness of security operations and to improve readiness for increasingly advanced threat environments.

Integrated Security Model

Cybersecurity should be embedded across all layers of Arkansas' AI environment:

- **Infrastructure:** AI deployments should run on secure, OST-approved environments with continuous monitoring.
- **Data:** The Arkansas Data Hub should enforce data access protections.
- **Applications:** AI models should undergo security testing for adversarial vulnerabilities before approval.
- **People:** Employees should be trained in safe AI use, including recognizing potential misuse scenarios.

AI as a Security Enabler

AI can also be used to improve Arkansas' cybersecurity posture. AI has the potential to:

- Detect anomalies in network traffic faster than traditional monitoring.
- Automate triage of alerts to reduce analyst workload and speed response times.
- Assist forensics and analyze patterns of exploits.
- Simulate attacker behavior to test defenses.

AI & Cybersecurity Collaboration with the Arkansas National Guard

Arkansas is uniquely positioned to leverage its strong partnership with the Arkansas National Guard. A collaboration program could unite the State Cybersecurity Office and the Arkansas National Guard's cyber units to identify and mitigate AI-specific threats, conduct joint exercises and simulations, and develop dual-use innovation pilots where military-grade capabilities can be adopted for civilian state use. This partnership could strengthen Arkansas' defenses while preparing the state to participate in federal and national security AI initiatives.

By integrating AI with cybersecurity, Arkansas can address risk at its core. An AI & cybersecurity collaboration with the Arkansas National Guard, layered defenses across infrastructure and

applications, and proactive use of AI for detection and response could combine to create a security-first approach. Arkansas has the potential to be a national leader in how AI and cybersecurity can strengthen one another.

Transparency

For Arkansas to succeed with AI, citizens must trust that the technology is being used responsibly, transparently, and for the good of the public. By making AI visible and understandable, Arkansas can strengthen public confidence, trust, adoption, and use of AI-enabled government services.

AI System Inventory

Arkansas should implement and maintain a statewide AI system inventory that catalogues all AI tools and deployments in use across departments. This inventory would provide transparency on where and how AI is used and allow citizens, policymakers, partners, and staff to remain informed. This mirrors federal requirements under OMB AI guidance (2024) for agency AI use case inventories, ensuring Arkansas remains interoperable with national transparency efforts.

Citizen-Facing Dashboards

Transparency should be further reinforced through dashboards that provide clear, non-technical information about AI being used by the state. These dashboards would provide easy access to information on which departments are using AI and for what purpose. They can also provide plain-language explanations of how AI contributes to citizen services and the controls that are in place to ensure safety and effectiveness.

By embedding transparency into its AI governance framework, Arkansas can ensure that citizens remain informed and reinforce the message that AI is a tool for the public good. This openness is essential for building and sustaining the trust necessary to fully harness the potential benefits of AI through widespread adoption and use.

Staff AI Literacy

Effective governance structures and technical protections depend on an informed workforce to succeed. Every state employee who touches AI, whether using AI tools or relying on AI outputs, must understand both the potential and the risks. Therefore, AI literacy should be a cornerstone of Arkansas' governance and safety framework. It ensures employees are equipped to use AI effectively while avoiding misuse that could compromise security, privacy, and trust.

AI Literacy Training

AI literacy should be delivered to ensure that employees know:

- How to identify when AI is being used.
- Proper use of AI tools and when human-in-the-loop review is required.
- How to avoid exposing sensitive data or creating data leakage through improper use.
- The importance of selecting the right tool for the right task.

Role-Based AI Literacy Framework

Arkansas should support an AI-ready state workforce through a role-based AI literacy framework:

- **Foundational AI Literacy:** Equip individuals with a basic understanding of AI concepts, capabilities, limitations, and implications, ensuring informed interactions with AI technologies.
- **Executive AI Literacy:** Equip decision-makers with a strategic understanding of AI's potential, risks, and policy implications to support responsible implementation and effective use.
- **Professional AI Upskilling:** Deliver role-specific training for employees whose work will be enhanced by AI tools, focusing on practical applications in their field.
- **Technical AI Literacy:** Empower technical staff with the skills needed to build, deploy, and govern AI systems, ensuring secure and effective implementation.

Staff AI literacy is critical to reducing risk, building confidence, and enabling effective adoption. This investment in people ensures that governance is lived out daily in the practices of every employee, not just written in policy.

Closing

These governance & security recommendations are designed to ensure that responsible AI is not a barrier to progress, but rather an enabler. By embedding governance and stewardship, strengthening data and infrastructure, integrating cybersecurity, engaging transparently with citizens, and equipping staff with AI literacy, Arkansas can ensure that AI adoption advances without compromising safety.

By aligning with the White House AI Executive Order, OMB AI guidance, and America's AI Action Plan, Arkansas demonstrates that its governance model not only safeguards Arkansans but positions the state as a national AI partner and leader. Governance gives departments the confidence to adopt AI tools, citizens the assurance that their rights are protected, and businesses the signal that Arkansas is a safe and forward-looking place in which to invest.

Appendix A: State of Arkansas Artificial Intelligence (AI) Policy

1. Purpose

This policy establishes a framework for the ethical, effective, and safe use of AI within state government. It ensures that AI adoption aligns with principles of transparency, accountability, fairness, and respect for human rights, while complying with all applicable state and federal laws.

Artificial Intelligence (AI) refers to technologies, systems, or applications that use machine-based processes to perform tasks that normally require human intelligence. These tasks may include learning, reasoning, problem-solving, perception, decision-making, natural language processing, or pattern recognition

This policy does not supersede existing statutes or statewide IT and security policies but operates in conjunction with them.

2. Policy Statement

- All AI initiatives including the development, procurement, and deployment of AI systems and tools must undergo a risk and impact assessment consistent with the NIST AI Risk Management Framework.
- AI systems and tools must be human centered, ensuring that decisions materially affecting individuals (e.g., benefits, funding, enforcement actions) are subject to final human review.
- Third-party vendors providing AI systems and tools must adhere to state AI and IT standards and be subject to oversight and audit.
- AI systems and tools must be designed and operated to ensure security, privacy, nondiscrimination, transparency, and accuracy.

3. Applicability

This policy applies to:

- All executive branch agencies and entities.
- All state employees, contractors, and vendors, and other authorized users of state owned or operated IT systems.

This policy does not apply to:

- AI features embedded in common tools that do not involve generative or decision-making functions (e.g., spam filters, autocorrect, or built-in AI such as those in web browsers).
- Personal use of AI tools on non-state devices for non-state business.

4. Responsibilities

A. State Entity Responsibilities

- Before acquiring or implementing any AI system or tool, departments must obtain approval from OST through the TIJ process.

- Any approved acquisition or implementation of AI systems and tools must be developed in accordance with state AI standards, policies, and applicable laws.
- Departments are responsible for monitoring any AI use through regular risk and impact assessments, including bias testing, data security, evaluation, and model accuracy review. Departments shall submit assessment results to the OST State Cybersecurity Office.
- Departments shall ensure human review and oversight is performed in all systems utilizing AI, including the adoption of an authorized AI use policy in accordance with OST AI standards and guidelines.

B. State Employee, Contractor, and Vendor Responsibilities

- All state employees, contractors, and vendors shall follow all state security and privacy guidelines when using AI systems or tools on state owned IT systems.
- Confidential, sensitive, and personally identifiable information is prohibited from being input into AI systems without prior authorization from the Office of State Technology.
- State employees, contractors, and vendors are responsible for reporting suspected misuse of AI to their supervisor and the OST State Cybersecurity Office.
- Vendors shall report changes in AI modeling, including known or suspected vulnerabilities, to the Office of State Technology.

C. Office of State Technology (OST) Responsibilities

- OST will maintain and update AI governance frameworks.
- OST will conduct periodic audits of state AI systems and tools, including vendor compliance.
- OST will provide training and resources to state employees on responsible use of AI.

5. Compliance

Non-compliance of this policy may result in:

- Loss of or restricted access to IT resources;
- Corrective or disciplinary action, including termination of employment;
- Termination of vendor agreements; or
- Referral to law enforcement in cases of suspected criminal activity.

6. References

- National Institute of Standards and Technology (NIST) AI Risk Management Framework
- OST IT Governance Policies
- State Procurement Laws, Rules, and Policies

7. Contact

For questions, contact the Office of State Technology.
Effective Date: [DATE]
Last Reviewed Date: August 22, 2025
Version Number: 1.0