Shared Administrative Services | Office of State Technology

Policy Title: Artificial Intelligence Policy
Policy Version: 1.0
Effective Date: 02/24/2026
Review Date: 02/24/2026

---

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. 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.

3. 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.

4. Responsibilities

A. State Entity Responsibilities

- Before acquiring or implementing any AI system or tool, departments must obtain approval from OST through the Technology Investment Justification 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. Revision History

This policy shall be subject to periodic review according to the Office of State Technology (OST).

Date	Description of Change	Reviewer
02/24/2026	Moved from Draft to Final	Jay Harton, State Chief Information Officer