OKLAHOMA
Office of Management
& Enterprise Services

Use of AI in Oklahoma State Government Standard

Introduction

Oklahoma's artificial intelligence strategy aims to establish the state as a leader in the responsible, safe, secure and proactive use of artificial intelligence. By leveraging AI and automation to streamline repetitive tasks within state agencies, Oklahoma aims to enhance operational efficiency, resource allocation and improve mission effectiveness, which will deliver better services to citizens.

Purpose

This standard establishes clear guidelines for the governance and secure use of AI technologies within the Oklahoma state government. It ensures that data is protected, managed responsibly and used to enhance public services while upholding privacy, security and ethical standards.

Definitions

Artificial Intelligence (AI) – machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. AI systems use machine and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner, and use model inference to formulate options for information or action.

AI model – component of an information system that implements AI technology and uses computation, statistical or machine-learning techniques to produce outputs from a given set of inputs, including those such as large language model(s) or other data processing that processes information and uses computation as a whole or as a part of a system to make or execute a decision, facilitate human decision-making or can be used to communicate with clients or prospects in an automated manner.

AI system – any data system, software, hardware, application, tool or utility that operates in whole or in part using AI.

Standard

Types of AI included in the standard.

Deep Learning (DL) – refers to neural networks with many layers that learn to perform tasks by analyzing large amounts of data and is particularly strong in tasks such as image recognition, voice synthesis and autonomous systems. Examples include, but are not limited to: PeopleSoft Digital Assistance, Axon Fusus facial recognition and Adobe Sensei AI.

Generative AI (Gen AI) – models new content (e.g., text, images) that did not exist before based on training data and user inputs. Examples include, but are not limited to: Amazon Transcribe, Murf AI, Legal Files, Microsoft Viva Insights and ServiceNow Now Assist.

Hybrid AI systems – combination of multiple models used within a system that can provide a much larger range of requests by users. Examples include, but are not limited to: Microsoft 365 CoPilot GCC, Azure Open AI and Hyland Software OnBase.

Large Language Models (LLM) – deep learning models for natural language understanding and generation, often trained on vast amounts of text data. Examples include, but are not limited to:

Workday Assistant, Open AI ChatGPT Enterprise, Perplexity Enterprise Pro, Ask Microsoft, Ironclad Jurist, Thomson Reuters CoCounsel and Grammarly.

Machine Learning (ML) – system that improve over time through data analysis without being explicitly programmed. Often used for predictive tasks, data analysis and pattern recognition. Examples include, but are not limited to: GitHub Copilot, Otter.ai, Glean AI, Qualtrics XM, Darktrace ActiveAI and Juniper Mist AI.

AI procurements and CIO authority.

Pursuant to the Information Technology Consolidation and Coordination Act ("ITCCA") and the Oklahoma Central Purchasing Act, the CIO holds sole and exclusive authority over all information technology acquisitions, including AI systems. As the Information Technology and Telecommunications Purchasing Director, the CIO ensures that all AI-related procurements align with state policies, security standards and strategic priorities. See 74 O.S. 85.5, 62 O.S. 35.1 et seq., and OAC 260:115-1-1.

To ensure proper oversight, security and compliance of AI systems, the CIO shall be a required signatory on every acquisition involving AI. This ensures that all AI-related acquisitions align with the organization's security policies and compliance standards.

Governance.

Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act ("ITCCA") the Chief Information Officer has authority over strategic planning, development, acquisition, deployment and implementation of information technology, including AI systems across executive state agencies. The CIO ensures that AI initiatives are implemented efficiently, securely and in alignment with state priorities, including improving government efficiency, service delivery and data-driven decision making.

The CIO is responsible for establishing standards, policies and procedures for AI systems to ensure their ethical use, security and integration with existing state infrastructure. The CIO will govern AI systems through the following review and approval process:

AI systems requested by agencies are subject to the CIO's authority – whether through direct procurement or state contract managed by OMES – must undergo CIO review. The evaluation may consider:

- Alignment with CIO strategic priorities.
- Ethical and security compliance with state and federal laws, regulations and rules.
    - Ethical governance framework:
        - Data quality and transparency.
        - Privacy and security.
        - Accountability and fairness.
        - Robustness, reliability and compliance.
        - Electoral integrity and non-bias.
        - Collaboration and beneficence.
- Data privacy and protection protocols.
- Whether the AI system is a net new system or an AI enhancement to an existing approved solution.

Principles and values for AI systems.

AI systems should be guided by the following principles and values.

- Responsible and ethical AI requires AI systems to respect and enhance human rights, ensuring privacy and equality. By aligning AI with human rights and ethical principles, the goal of the state AI systems is to protect individuals and data.

- AI systems must be transparent with clear lines of accountability. Users of AI systems must be able to explain decisions and processes undertaken by AI systems. Therefore, decisions made by AI must be unbiased, transparent and understandable to users.
- It is crucial to prevent bias in AI decision making to ensure that AI systems provide fair, accurate and non-discriminatory outcomes. It is imperative that AI systems are designed and implemented in a way that prevents discrimination against protected classes, ensuring equitable treatment and compliance with applicable laws regarding protected classes.

Disinformation and misinformation within AI.

Disinformation and misinformation, while differing in intent, both contribute to the spread of false and inaccurate information in the context of government use of AI. Disinformation is intentionally created to deceive users with misinformation is spread unintentionally due to error. In AI systems, these issues emerge when false content is generated or amplified, whether through automated data output, AI-driven content creation or the propagation of uncorrected or flawed data. Both can undermine trust and accuracy, making it critical to implement safeguards against their occurrence.

The do's and do not's.

When using AI systems such as ChatGPT, Gemini or Claude to assist with various work tasks, it is important to be mindful of the information being provided to the software solution. Be mindful of your use by using the following guidelines:

Do:

- Verify all AI-generated content before using it, ensuring the information is accurate, relevant and appropriate.
- Do maintain responsibility of your final work product. AI tools should replace productivity efforts, not replace your work.
- Do be aware of content and agency standards for communication. Ensure that tone, style and language align with agency standards or other professional requirements.
- Do use general or fictional examples, when possible. Public generative AI applications store the information you provide and may resurface it to other users.

Do not:

- Do not use AI-generated answers without fully verifying the content and context is correct. AI tools can present users with inaccuracies ("hallucinations") or omit key information.
- Do not use sensitive topics or sensitive state data within the tool such as personal indefinable information ("PII"), financial information, health data, authentication data or any other sensitive information.
- Do not use when drafting solicitation information or for any procurement processes as the information could be used to gain an advantage by a vendor.
- Do not rely on AI-generated language translations without confirming accuracy, dialect or potential biases with a qualified interpreter or translator.

Example prompt #1: Write a memo to Oklahoma state employees about the return to office executive order. Please include the benefits of returning back to the office, maintain a professional tone and limit the text to be less than 300 words.

Example prompt #2: Write a job description for a State of Oklahoma Executive Administrative Assistant.

Example prompt #3: Draft an email to all state employees announcing the upcoming benefits enrollment period. Include key deadlines, highlight coverage changes and limit the text to 200 words. Use the documents provided as context for the email.

Example prompt #4: Create a one-page FAQ document that addresses common questions about the State of Oklahoma's benefit package.

To ensure responsible AI use, state employees with any questions regarding what should or should not be allowed in AI system should submit a ServiceNow Ticket to the OMES Help Desk for guidance and review.

Auditing.
The CIO may conduct audits to ensure AI systems are not being used without prior approval and to verify that approved AI systems remain in compliance with state policies, security standards and regulatory requirements.

All AI systems will be reviewed during the procurement stage and if awarded a multi-year contract, auditing may be required before a renewal is completed. Once an AI system is approved, it may be subject to continuous monitoring throughout its use to ensure ongoing compliance. At the CIO's discretion, any AI system may be audited at any time to ensure:

- State and federal law;
- Conformance with state standards;
- Applicable regulations;
- Bias testing;
- Data privacy compliance; and
- Any other AI compliance requirements.

Security and privacy.
All AI systems must undergo a third-party security review, which includes assessment of the supplier's Authority to Operate ("ATO") and software product security review. Both reviews are to be conducted by the Chief Information Security Officer (CISO) of OMES before any use of the product, ensuring that all security and compliance requirements are met.

Sensitive data, which includes, but are not limited to, data regulated by or concerning, the Health Insurance Portability and Accountability Act ("HIPAA"), the Family Educational Rights and Privacy Act ("FERPA"), Federal Tax Information ("FTI"), Personally Identifiable Information ("PII"), and Criminal Justice Information ("CJIS") shall not be transmitted when using public AI systems. Such data may be transmitted through a separate secure instance, not a public unsecure instance, but only after having been approved for such use by the CIO. Once CIO approval has been granted for use of sensitive data in any AI tool, continued compliance regarding certain types of sensitive data use must be monitored and will be held accountable by the agency for compliance with any applicable federal regulations.

Compliance
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. All state agencies, boards, and commissions under the CIO's authority, as well as suppliers, contractors and other entities providing services to the state are required to adhere to the most current published standard. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination. All other state entities that fall outside of the CIO's authority are encouraged to adopt this standard.

Rationale
To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References
- Information Technology and Telecommunications Purchasing Director.
- ServiceNow Ticket.

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 03/06/2025	**Review cycle:** Annual
Last revised: 03/06/2025	**Last reviewed:** 03/06/2025
Approved by: Dan Cronin, Chief Information Officer	