AI Usage Standard

Introduction

This standard is to ensure that the development, deployment and usage of Artificial Intelligence (AI) products and tools by the State of Oklahoma, its agencies and its partners align with ethical principles and values and does not cause harm to individuals or communities. The standard also aims to promote the responsible and effective use of AI to support the delivery of public services.

Purpose

This standard sets forth guidelines and principles for the development, deployment and use of Artificial Intelligence products by the State of Oklahoma.

Definitions

Artificial Intelligence (AI) – the field of computer science and technology that focuses on creating machines capable of performing tasks that typically require human intelligence, which includes, but is not limited to, machine learning, large language models, reinforcement learning, natural language processing, computer vision and deep learning.

OpenAI – an artificial intelligence research organization.

ChatGPT – an advanced language model developed by OpenAI, capable of generating human-like responses to text-based prompts.

Gemini – an experimental, conversational AI chat service developed by Google that pulls information from the web.

Public AI systems – refers to artificial intelligence systems or software applications that are openly accessible and available to the public. Public AI systems can include platforms, APIs, libraries or frameworks that allow individuals or developers to leverage AI functionalities for various purposes such as natural language processing, image recognition, recommendation systems and more.

Private AI systems – refers to artificial intelligence systems or software applications that are developed and used within a specific organization or by a limited set of authorized users. These systems are not openly accessible to the public and are typically implemented to address specific business needs or requirements. Private AI systems may include proprietary machine learning models, custom-built algorithms or specialized software developed by organizations to leverage AI capabilities for internal purposes such as data analysis, process automation, decision-making or improving operational efficiency.

Standard

1. Data quality – AI systems rely heavily on the data they are trained on. Therefore, it is critical to ensure that the data is high-quality (accurate, complete, reliable and current), unbiased (using representative data sets and avoiding stereotypes and assumptions) and free from errors whenever possible.
2. Transparency – It is important to ensure that AI systems are transparent in how they make decisions. This involves providing explanations on how they arrive at their conclusions and ensure that these explanations are understandable and accessible to all stakeholders. The data associated with training AI tools should be considered protected.
3. Data privacy – AI systems often require access to sensitive data such as personal information. It is essential to ensure that this data is collected, stored and used ethically and is in compliance with relevant regulations. Public AI systems, such as ChatGPT and Gemini, should be used with discretion. Private data, which includes, but is not limited to, data regulated by or concerning, HIPAA, FERPA, FTI and CJIS shall not be transmitted when using public AI systems but may be transmitted via private AI tools only after having been approved for such use by the CIO.
4. Data Sharing – AI systems are built off information input into the software. Acceptable types of information that can be transmitted with public AI is public-facing data, such as the information on the Transparent Oklahoma Performance website including government services and programs, legislation and policies, public records, reports and transportation data.
    - Before the AI can be taught from the selected information, approval must first be acquired from the CIO since AI usage falls under technological use.
    - State standards, with CIO approval, will be established for specific AI tools and products such as chatbots, large language models, etc.
5. Accountability – AI systems should be designed to be accountable for their decisions and actions. This means that there should be mechanisms in place to identify and address any errors or biases that may arise and to ensure that the system can be held accountable for any harm caused, including open sourcing models and research to allow for scrutiny and feedback.
    - Due diligence is essential to ensure the accuracy of AI output as it helps identify potential errors or misleading results, promoting reliable decision making. Thorough evaluation and validation on AI results are needed to mitigate risks associated with inaccurate or misleading AI-generated outputs.
6. Security – AI should be designed to protect against unauthorized access, manipulation and misuse of data.
7. Beneficence – AI should be designed and implemented to provide a net benefit to the State of Oklahoma and Oklahoma citizens rather than harming individuals/society or violating individual privacy rights.
8. Electoral integrity – AI systems should not be used unethically to support campaigns and elections of officials for the State of Oklahoma to avoid giving unfair advantages to certain candidates or parties. Voters and election officials should be educated about the use of AI in the electoral process, including how AI is being used and how it can impact the election results.
9. Robustness – AI systems should be designed with the ability to withstand and adapt to unexpected situations or errors with the ability to be audited and tested for safety and reliability.
10. Collaboration – AI systems should be developed through collaboration with a diverse range of stakeholders, including domain experts, technical experts and impacted communities.
11. Ethical governance – AI systems should be developed and governed through an ethical framework that considers the principles of data quality, transparency, data privacy, accountability, security, beneficence, electoral integrity, robustness and collaboration.

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. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

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.

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

Effective date: 07/03/2023	**Review cycle:** Annually
Last revised: 02/09/2024	**Last reviewed:** 7/13/2023
Approved by: Joe McIntosh, Chief Information Officer	