RESPONSIBLE ARTIFICIAL INTELLIGENCE USAGE POLICY

NUMBER: 107-004-190

EFFECTIVE DATE: June 16, 2026

DIVISION: Enterprise Information Services (State CIO)

POLICY OWNER: Privacy and Artificial Intelligence

INTERNAL OR STATEWIDE POLICY: Statewide

LAST REVIEWED DATE: June 16, 2026

SUPERSEDES: Updated Interim Guidance on Generative AI Usage and Access memo (Feb.10, 2026)

REFERENCE/AUTHORITY:

- ORS 276A.203; 276A.206
- Information Technology Investment Oversight Policy 107-004-130
- Information Asset Classification Policy 107-004-050
- Data Governance and Transparency Policy 107-004-160
- Responsible Artificial Intelligence Usage Procedure 107-004-190_PR

APPROVED SIGNATURE:

Terrence Woods, State Chief Information Officer

Statement

The main purpose of this policy is the creation of a robust governance structure that instills confidence and trust in the use of artificial intelligence (AI) at the state. This policy has the following objectives:

- **Establish enterprise governance:** create a governance structure for AI policy and oversight that can keep pace with rapidly evolving technology and standards.
- **Identify and address risks**: establish a risk management model to identify and address potential issues related to bias, fairness, privacy, safety, and security.

- **Ensure accountability**: mandate clear lines of human responsibility for all AI systems.
- **Foster transparency**: require mechanisms for internal and public transparency regarding the state's use of AI.
- **Empower the workforce**: build AI literacy and technical competency across the state workforce.
- **Monitor progress**: establish systems for monitoring and reporting AI use.

Applicability

This policy outlines requirements for AI use in state agencies as defined in ORS 174.112, and includes any board, commission, department, office or other entity within the Oregon executive department. The following agencies are excluded:

- Secretary of State
- State Treasurer

The policy applies to generative and agentic AI systems used to conduct the business of the state, including both standalone systems and components embedded in other software.

Definitions

Agentic artificial intelligence: AI systems designed to autonomously pursue complex goals and take actions with limited human intervention, and adapt approaches based on environmental feedback.

Artificial intelligence (AI): a machine-based system that is capable, for a given set of human-defined objectives, of making predictions, recommendations or decisions influencing real or virtual environments and uses machine- or human-based inputs.

Foundation model: an AI model trained on vast datasets and applicable across a wide range of contexts.

Generative artificial intelligence (GenAI): a software system that generates new content, data, or other output, including images, video, audio, and text, autonomously. It uses algorithms and models to create new and original information from patterns and information it learned previously from a given set of data. Large language models and foundation models are both GenAI. GenAI is distinguished from other AI systems by its primary function of creating new content rather than solely classifying, predicting, or recommending from predefined categories.

Human in the loop (HITL): Human in the loop refers to a system or process in which a human actively participates in the operation, supervision and decision-making of an

automated system. In the context of AI, HITL means that humans are involved in the AI workflow to ensure accuracy, safety, accountability and ethical decision-making.

Oregon AI transparency disclosure: a plain language summary of what an AI system does, what data it touches, how it was tested and how it is being overseen.

Prompt: the question, instruction or other information entered by a user to generate a response from a GenAI system. It serves as the starting point for the model to generate a relevant reply.

Exclusions and Special Situations

Non-GenAI powered automated decision-making systems of numerous kinds have been in use by state agencies for many years. Systems that are explicitly architected and use only data analytics, statistical modeling or machine learning are not covered by this policy.

This policy does not apply to:

(1) Basic calculations, spreadsheet operations, or mathematical computations following predetermined formulas

(2) Traditional statistical modeling using regression analysis, time series analysis, or other established statistical methods

(3) Data analytics, business intelligence tools, or reporting dashboards that aggregate, visualize, or summarize data

(4) Rule-based automation using pre-recorded conditional logic with predefined triggers that automatically initiate predetermined actions (such as "if, then" systems)

(5) Database queries, sorting operations, or filtering functions

(6) Basic AI features embedded in common commercial products used for recommendation purposes, including predictive text in word processors (e.g. Microsoft Word), dynamic route adjustment based on real-time traffic conditions in map navigation systems (e.g. Apple Maps, Google Maps), and results from web-based search engines (e.g. Google, Bing, Edge, DuckDuckGo).

General Information

Principles of Responsible AI Usage

The following are the state of Oregon's principles related to the responsible use of artificial intelligence:

- Human Oversight and Review: Human oversight must be intentionally built into AI adoption and day-to-day use, with clear roles and responsibilities for governance and decision-making. AI must not replace subject matter expertise.
- Equity and Representation: AI systems should support equitable outcomes and be designed and used with attention to representation, accessibility, and potential disparate impacts. AI systems should be regularly monitored for fairness and accuracy.
- Privacy and Confidentiality: AI systems must protect privacy and confidentiality, with clear oversight responsibilities and heightened review where sensitive data is involved.
- Risk Management: AI risks must be identified, assessed, measured, and managed throughout the lifecycle of AI usage.
- Safety: AI systems should not reduce overall safety and should be subject to clear safety requirements, including measurable evaluation methods.
- User Experience, Disclosure and Feedback: AI should improve staff and constituent experience in their engagement with state government. Disclosure of AI usage and opportunity to provide user feedback on AI-generated results are required. Transparency, explainability, and disclosure of AI use, including processes and evaluations, must increase proportionate to risk.
- Workforce Preparedness and Understanding: Workers should develop a baseline understanding of AI capabilities, uses, and implications. They should be involved in AI adoption and review processes and receive the training needed to use AI appropriately.

Enterprise AI Advisory Committee

The State CIO will establish an Enterprise AI Advisory Committee comprised of representatives from Enterprise Information Services (EIS) and executive branch agencies and chaired by the State CIO or designee. The committee will serve as advisory to EIS and the State CIO. The responsibilities of the Enterprise AI Advisory Committee include reviewing and providing recommendations to EIS on enterprise AI policy.

General Recommended Usage

EIS will provide policy for generative AI use by state employees on enterprise AI tools including Copilot Chat.

AI Risk Management Framework and Usage Requirements

EIS will establish an AI Risk Management Framework to provide detailed standards, requirements and guidance to state agencies for using generative or agentic AI. Any use of AI meeting the applicability standards must comply with the AI Risk Management Framework. The AI Risk Management Framework will align with the National Institute of Standards and Technology (NIST) AI Risk Management Framework and provide clear definitions for proposed use cases that are considered higher-risk.

EIS will specify standards for the following:

- Generative AI model and system card disclosure
- Use of data for model training
- User disclosure
- User feedback
- Human in the loop documentation
- Baseline testing and monitoring
- Additional requirements for higher-risk uses

Agency AI Adoption Plans

Agencies will create and keep updated an AI Adoption Plan for their agency that is inclusive, action-oriented and adaptable.

Statewide AI Registry

The State CIO or their designee will oversee the creation and maintenance of a statewide registry of all AI-using applications in use or development by state agencies, including details on their uses, as part of an enterprise application portfolio management system.

Security

Secure Environments: To manage supply chain and infrastructure risk, all AI development, training, and hosting will be limited to approved, secure environments, including EIS Data Center Services facilities or other platforms with approved certifications.

Integration with Cybersecurity: AI risk monitoring will be integrated into the state's Security Operations Center (SOC) and incident response plans.

Unauthorized Usage

Agencies are accountable for AI usage by employees for work-related purposes. Work usage by state employees of unapproved AI systems is prohibited. EIS will monitor enterprise AI usage to identify unapproved or high-risk use, evaluate associated security and operational risks, and make recommendations to the State CIO to limit or address unapproved usage.

Workforce Development and Training

An informed state workforce is essential to the responsible and effective adoption of AI. A statewide training program will be developed and maintained by EIS in collaboration with the Department of Administrative Services and include AI literacy and risk awareness.

Transparency and Public Reporting

EIS will publish an annual report on AI use in state government based on the State AI Registry. EIS will also maintain a publicly accessible website that provides access to these annual reports as well as Oregon AI transparency disclosure information for all higher-risk systems.

Sandbox for Custom Development and AI Model Installation

Agencies developing custom AI-powered software systems, including in Azure Foundry and Copilot Studio, must do so in a sandbox or development environment approved by EIS. Customers of Data Center Services are prohibited from installing, deploying, or operating AI models within EIS Data Center Services facilities without prior written approval from EIS. EIS will provide guidance and procedures for agencies to follow to support this requirement.