Oregon
Tina Kotek, Governor

Enterprise Information Services
State Chief Information Officer
550 Airport Road SE, Suite C
Salem, OR 97301
503-378-3175

MEMORANDUM

To: Agency IT Leadership

From: Terrence Woods, State CIO

Date: September 12, 2025

Subject: Updated Interim Generative AI Access and Usage Guidance

---

Purpose
Outline requirements for Oregon state agency users accessing Generative AI (GenAI) tools, including Microsoft Copilot and AI embedded in software applications. Users must follow the guidance to ensure that such tools are used while safeguarding data in accordance with existing policies on data classification and security.

Scope
This guidance applies to all Executive Branch agencies, boards and commissions under the purview of the State Chief Information Officer, as defined in ORS 276A.230. The use of Microsoft Copilot and similar GenAI tools shall be restricted to Level 1 ("Published") and Level 2 ("Limited") data only, as classified in the Information Asset Classification Policy (107-004-050).

Principles
Agencies are to review and act in accordance with the Oregon's Artificial Intelligence Guiding Principles as captured in the Final Recommended Action Plan.

Use Case Recommendations

- Generative AI is permissible for tasks such as drafting documents, summarizing information, and generating creative content.
- For public meetings, users should not use AI-powered translation or transcription services, including those offered by Microsoft Copilot, or Teams Premium for translating speech in real-time, as federal and Oregon laws mandate equal access to government information regardless of language. For public meetings requiring language translation, agencies should continue to use qualified human interpreters to ensure accuracy and compliance with legal requirements.

Recommended Use of Generative AI ✔ = recommended, **Supervisor**=With approval, X= not recommended					
Breadth of Distribution	**Proofreading, Grammar**	**Brainstorming/ First Draft** **<25% AI**	**Collaborative Writing** **About 50% AI**	**Human Edited** **>75% AI**	**Copy-paste generated Content**
Press release, prepared remarks	✔	**Supervisor**	✖	✖	✖
Replies to public inquiry	✔	**Supervisor**	✖	✖	✖
Public facing web content	✔	**Supervisor**	**Supervisor**	✖	✖
Memos, broad internal comm	✔	**Supervisor**	**Supervisor**	✖	✖
Internal process docs	✔	✔	**Supervisor**	✖	✖
Source code	✔	✔	**Supervisor**	✖	✖
Emails	✔	✔	**Supervisor**	**Supervisor**	✖
Chat	✔	✔	**Supervisor**	**Supervisor**	✖

Monitoring and Compliance

Agencies will be responsible for monitoring compliance, auditing access, and reporting incidents or violations to the EIS Cybersecurity Services. Violations may result in revocation of access, disciplinary action, and potential legal implications under state and federal guidelines.

Responsibilities

Agency must:

1. Agency directors are responsible for ensuring that their employees comply with this guidance.
2. Use of GenAI must have a defined business purpose. Use cases not identified above must be approved by the agency's IT and data governance teams. Enterprise approved tools

such as Copilot have already been approved and do not need to have an additional defined business purpose approved by the agency's IT and data governance teams.

3. Procuring or use of non-enterprise GenAI tools must submit the Information Technology Investment form (ITI) and follow the interim guidelines. Refer to the list of authorized AI tools.
4. Agencies must ensure that sensitive or legally protected information, including data classified as Level 3, 4, or confidential information, is never exposed to GenAI tools. This includes preventing:
    a. Used as input to a GenAI tool.
    b. Included in GenAI queries.
    c. Used for building or training GenAI tools.
    d. Provided to any publicly accessible GenAI tool.
5. For external documents that incorporate GenAI output, an explicit disclosure or attribution is recommended (e.g., via a footnote or header), at the discretion of the agency or organization.
6. All user interactions should be excluded from model training to ensure privacy and data protection. If a GenAI tool allows usage history to be saved, that history feature must be disabled (turned off). In the case of Microsoft Copilot with Enterprise Data Protection (EDP) enabled the history may remain enabled if the user is logged in to the enterprise active directory.
7. Vendors or contractors creating any information asset must explicitly declare any GenAI usage, including the nature of the data used as input, and may be subject to a risk assessment during procurement.

Users must:

1. Complete a state-provided GenAI security and ethics training course through Workday.
2. Prior to using GenAI tools, users must accurately classify all input data in compliance with Statewide Policy 107-004-050, ensure that only Level 1 and Level 2 data is used, and classify the GenAI outputs with the same level of sensitivity as the input data.
3. Promptly report any anomalies or suspected data breaches.
4. Be aware of the potential for GenAI to produce biased or inaccurate outputs and critically evaluate the results. Users are responsible for content of materials produced by GenAI.
5. All personnel must adhere to guiding principles when using GenAI to enable the delivery of government services.
6. A GenAI output must never:
    a. Be used without human review.
    b. Be assumed to be truthful, accurate, credible, or trustworthy.
    c. Serve as the sole source of reference.
    d. Be used in total to issue official statements (e.g., policy, legislation, regulations).
    e. Be used to arrive at a final decision.
    f. Be used to impersonate individuals or organizations.
7. If a GenAI tool is used to generate a batch output, an appropriate expert must apply domain knowledge and statistical sampling techniques to vet that output.

8. Users must not input proprietary, copyrighted, or otherwise protected material into GenAI tools unless they have explicit authorization or licensing to do so.
9. Before any GenAI output is disseminated or acted upon, it must:
    a. Be vetted by a qualified human operator, with the operator's seniority matching the importance of the content.
    b. Follow the human-in-the-loop (HITL) model for AI accuracy and legal, regulatory, and ethical compliance.
10. Users must not use GenAI to make critical decisions, provide legal or medical advice, or generate sensitive information.
11. Users must not use GenAI tools in any way that violates laws, regulations, organizational policies, or contractual obligations.

Additional Safeguards
The Cybersecurity Services and/or Agency IT teams will conduct periodic risk assessments for AI use and AI systems.

This guidance is subject to change as GenAI technology evolves, and new guidance becomes available.

By adhering to this guidance, state agencies and users will enable GenAI's safe, ethical, and efficient use while ensuring data privacy, security, and compliance with statewide policies.

References
- Information Asset Classification Policy (107-004-050)
- State Government Artificial Intelligence Advisory Council Final Recommended Action Plan
- EIS Interim Guidance on Artificial Intelligence, June 2024
- Executive Order No. 23-26: AI Council and Ethical AI Use
- Blocking Access to DeepSeek AI on State Resources

Additional Resources:
- Blueprint for an AI Bill of Rights: https://www.brookings.edu/events/unpacking-the-white-house-blueprint-for-an-ai-bill-of-rights/
- Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence: https://www.brookings.edu/articles/one-year-later-how-has-the-white-house-ai-executive-order-delivered-on-its-promises/
- AI Risk Management Framework (AI RMF) 1.0: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf