**DATA-04**
**State CIO Adopted:** 12/11/2025
**TSB Approved:** 12/11/2025
**Sunset Review:** 12/11/ 2028

**Replaces:** N/A

WaTech
Washington Technology Solutions

# ARTIFICIAL INTELLIGENCE POLICY

**See Also:**
RCW 43.105.054 WaTech Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"

1. **Artificial Intelligence (AI) technologies that provide services and perform government functions must be used by state agencies responsibly. Agencies must incorporate Washington state's AI Principles into agency implementation of AI-enabled technology and Generative AI and consider the guidelines for public sector procurement, deployment and monitoring of Generative AI technology.**

2. **Agencies must designate an AI Contact.**

    a. The designated contact serves as the primary point of contact on AI-related matters.

    b. The designated contact may or may not be a technical position but should have knowledge about AI-enabled technologies in use at the agency.

3. **Agencies must identify and document AI-enabled technology. The annual certification process for the agency application inventory must identify applications which use artificial intelligence and specify applications that use Generative AI. See Technology Policies, Standards, and Procedures (7.b.), MGMT-01 – Technology Portfolio Foundation and MGMT-01-01-S – Technology Portfolio Foundations-Applications.**

4. **Prior to implementing new AI-enabled technologies, agencies must identify intended business outcomes and ensure the AI technology is an appropriate fit to support those outcomes.**

5. **When implementing AI-enabled technologies, agencies must maintain processes to identify, assess, and manage artificial intelligence risks and implement appropriate controls.**

6. **Agencies must identify and document High-Risk AI Systems, which include High-Risk Generative AI Systems.**
    a. At a minimum, agencies must determine whether an AI-enabled technology is high-risk:
        i. During any Security Design Review that involves an AI-enabled technology. See SEC-02 – Security Assessment and Authorization Policy.
        ii. During any risk assessment as required by the Washington state Risk Assessment Standard (SEC-11-01-S).
    b. Agencies must conduct an Artificial Intelligence Risk Assessment prior to implementing a High-Risk AI System to identify specific risks and determine and document the controls that will be used to measure and manage those risks. See Executive Order 24-01 and AI Risk Assessment Guidance.

7. **Agencies must take reasonable steps to ensure that Generative AI content (including outputs, predictions or recommendations) is accurate and minimizes risk of harm. AI generated content should be reviewed and fact-checked if used in public communication or decision-making to avoid confusion or misrepresentation.**
    a. Agencies generating content with AI-enabled technology must verify that the content is accurate, updated information, and not potentially harmful or offensive material.
    b. Given that Generative AI systems may reflect biases in their training data or algorithms, state personnel should also review and edit AI-generated content to reduce potential or actual biases.

8. **In accordance with risk level (low, moderate, high), agencies must monitor outputs of AI technology for accuracy. Appropriate controls must be implemented based on risk level.**

9. **Agencies must ensure all employees receive sufficient AI awareness training related to their roles and responsibilities and the category of data to which they have access.**
    a. At a minimum, employees must receive basic training that addresses how AI works, common uses of AI, and the employee responsibilities for ethical and responsible use of the technology and risk of automation bias.

b. Basic AI training must be completed:
    i. As part of onboarding for new employees within 60 days of start date.
    ii. At least annually.
c. Additional AI skills training may be provided consistent with:
    i. Individual roles and responsibilities.
    ii. The scale, complexity, risk level, and sensitivity of AI use in the agencies, including use of Generative AI High-Risk systems.
    iii. Other applicable system-specific AI requirements and how AI inputs and outputs may be public records subject to the same laws and retention requirements as other government records.

10. **It is prohibited to use AI to create content, such as a video, image, or voice, of an actual person's likeness without their awareness or consent, consistent with applicable law.**

11. **Agencies must enter into written data sharing agreements when sharing Category 3 or Category 4 data outside the agency unless otherwise prescribed by law. See SEC-08 – Data Sharing Policy; RCW 39.26.340 Data-sharing agreements – When required; RCW 39.24.240 Data requests – When written agreement required.**

    a. Agencies must include contract terms regarding how outside agencies or vendors are restricted or may use or train public or private AI models with Category 3 or Category 4 data.

    b. Agencies must require that any vendor or contractor, providing a High-Risk Generative AI System to an agency, certify that the vendor has implemented an AI governance program consistent with the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework. See Executive Order 24-01 – Artificial Intelligence.

12. **Agencies must not integrate, enter, or otherwise incorporate any non-public data or information into unlicensed AI-enabled technologies without appropriate contracts, including a data share agreement. The sharing or use of such data could lead to unauthorized disclosures, legal liabilities, and other consequences. See RCW 42.52.050.**

13. **Agencies must be transparent about how they are processing personal information in AI-enabled technologies. AI processing activities of personal information may be included in existing privacy notices. See Executive Order 24-01 – Artificial Intelligence, Data 03 – Privacy and Data Protection Policy.**

14. **Agencies implementing High-Risk Generative AI technologies must develop an adoption plan that:**

    a. Defines the goals and intended use cases for Generative AI, which may include details of testing, continuous improvement, refining, and evaluating those use cases for accuracy, impact and performance.

    b. Controls for potential risks and outline mitigation strategies, including addressing risk of bias and discrimination and disparate impacts on vulnerable communities.

    c. Considers environmental impacts (for example water consumption, energy usage, carbon emissions, electronic waste).

    d. Establishes data quality standards for use cases.

    e. Identifies measurable results from Generative AI, which may include efficiency improvements measured in areas such as time, cost, or resources.

    f. Establishes a formal process to regularly (at least annually) monitor outputs post-deployment to identify any potential issues, biases, inaccuracies, or unintended consequences. Monitoring should include collection and analysis of relevant data to evaluate the High-Risk Generative AI system's effectiveness, fairness, and reliability over time.

    g. Provides opt-out rights or options for individuals subject to decisions or outputs of High-Risk Generative AI systems or document why such options would create undue burdens to the agency.

    h. Reviews and incorporates recommendations from the state's Guidelines for Public Sector Procurement, Deployment, and Monitoring of Generative AI when procuring or use a High-Risk Generative AI system.

    i. Considers if due process rights for individuals would be appropriate for High-Risk Generative AI system and create process for human review if appropriate.

15. **Agencies with union-represented employees must include the following statement in their internal policies on Artificial Intelligence: "If a provision of this policy conflicts with an applicable collective bargaining agreement (CBA), the CBA will supersede the provision with which it conflicts."**

## REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. Executive Order 24-01 – Artificial Intelligence.
3. Secretary of State - Managing Generative AI Records
4. Risk Assessment Standard | WaTech
5. AI Risk Assessment Guidance
6. https://www.nist.gov/itl/ai-risk-management-framework
7. AI Procurement Guidelines
8. Technology Policies, Standards, and Procedures (7.b.)
9. MGMT-01 – Technology Portfolio Foundation
10. MGMT-01-01-S – Technology Portfolio Foundations-Applications
11. SEC-08 – Data Sharing Policy
12. DATA-03 – Privacy and Data Protection Policy

### Referenced RCWs

1. RCW 39.26.340 Data-sharing agreements — When required
2. RCW 39.24.240 Data requests — When written agreement required
3. RCW 42.52.050 Confidential information — Improperly concealed records

## CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For questions about artificial intelligence, please email ai@watech.wa.gov.

## DEFINITIONS

- **Artificial Intelligence (AI):** The use of machine learning and related technologies that use data to train statistical models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, speech or natural language processing, and content generation.
- **Machine learning:** The process by which artificial intelligence is developed using data and algorithms to draw inferences therefrom to automatically adapt or improve its accuracy without explicit programming.
- **Training data:** Labeled data that is used to teach artificial intelligence models or machine learning algorithms to make proper decisions. Training data may include, but is not limited to, annotated text, images, video, or audio.
- **Generative Artificial Intelligence:** Technology that can create content, including text, images, audio, or video, when prompted by a user. Generative AI systems learn patterns and relationships from large amounts of data, which enables systems to generate new content that may be similar, but not identical, to the underlying training data.
- **High-Risk Generative AI System:** Systems using generative AI technology that creates a high-risk to natural persons' health and safety or fundamental rights. Examples include biometric identification, critical infrastructure, employment, health care, law enforcement, and administration of democratic processes.
- **High-risk AI system:** At a minimum, a high-risk AI system is a system using AI technology that creates a high-risk to natural persons' health, safety or fundamental rights. Agencies may identify additional categories of high-risk AI systems.