WaTech
Washington Technology Solutions

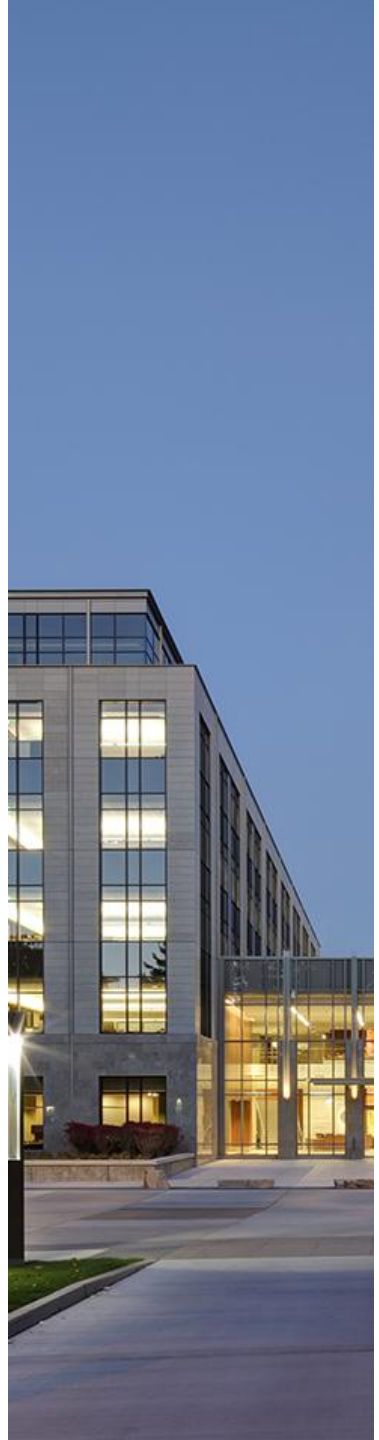
AI Governance and Practical Considerations for Responsible AI Adoption

Katy Ruckle, State Chief Privacy Officer

October 21, 2026







What is AI Governance?

WaTech
Washington Technology Solutions

AI Governance

AI governance is the system of policies, roles, processes, standards, and oversight mechanisms used to ensure that artificial intelligence is developed, purchased, deployed, and used responsibly.

WaTech
Washington Technology Solutions

Overview

- **AI Governance Framework**
  - Policies
  - Roles
  - Processes
  - Standards
  - Oversight

WaTech
Washington Technology Solutions

AI Policy (Data-04)

- 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.

WaTech
Washington Technology Solutions

AI Principles

- Safe, secure, and resilient
- Valid and reliable
- Fairness, inclusion, and non-discrimination
- Privacy and data protection
- Accountability and responsibility
- Transparency and auditability
- Explainable and interpretable
- Public purpose and social benefit

WaTech
Washington Technology Solutions

Roles

Best practice is **cross functional approach** per the NIST AI Risk Management Framework

Executive Leadership – provide strategic direction, and organization-wide accountability by setting the tone for level of risk acceptance in AI use.

SMEs - Data, Enterprise Architects, Technical leads, Security, Privacy, Legal, Risk, Compliance, Business leads

WaTech
Washington Technology Solutions

AI Strategy and Roadmap



Example at WaTech

State Chief Information Officer (CIO) and State Chief Technology Officer (CTO) provide strategic direction along with WaTech SMEs

From AI Strategy and Roadmap:

With a focus on customer experience, operational efficiency, workforce enablement, and measurable public value, this strategy is organized around three interdependent strategic goals that inform investment decisions, agency priorities, and partnership opportunities:

- Goal 1: Improve Customer Experiences and Outcomes with AI
- Goal 2: Support the Workforce in Using AI Effectively
- Goal 3: Scale Trusted AI Across Government

WaTech
Washington Technology Solutions

Roles in AI Governance at WaTech

Lead by Chief Technology Officer (CTO) and includes:

Chief Privacy Officer, Privacy Manager, Data Officer, Emerging Tech Program Manager, Enterprise AI Business Architect, Security Architecture Manager, Computing Services Director, Communications

Disciplines – Privacy, Data, Architecture, Business, Security, Operations, Communications

WaTech
Washington Technology Solutions

AI Governance Processes

Risk Assessments

Training

Monitoring & Oversight

Incident Response

WaTech
Washington Technology Solutions

AI Governance Process Questions

- Who is allowed to use AI?
- For what purposes?
- What risks must be reviewed?
- What data can be used?
- Who is accountable for decisions?
- How are systems tested, monitored, and audited?
- What happens when something goes wrong?

Example Use Case – Copilot Trial

WaTech
Washington Technology Solutions

What Is The Copilot Trial?

MSFT Copilot Trial

The Microsoft 365 Copilot Trial gives state employees the opportunity to experience Copilot in your own environment, understand the real benefits, consider the risks, and make informed decisions about the future.

This trial will help WaTech:

- ✓ **Experience Copilot together**
  Try Copilot in work to see how it can support day-to-day business needs and team collaboration.
- ✓ **Discover what matters most**
  Identify high-value use cases that save time, improve quality and help to deliver better results
- ✓ **Understand impact and risk**
  Evaluate benefits, risks, security, compliance and the changes needed for responsible use.
- ✓ **Build skills and confidence**
  Give staff and leaders hands-on experience, training, and support to grow AI capability.
- ✓ **Use insights to decide our path**
  Use what we learn to guide future decisions for WaTech and help inform the state.

What Success Looks Like

More time for what matters.
Less time on routine work, more time for impact.

Innovation that serves Washington
Lead by example and share what works.

Safe, secure and responsible.
Use Copilot within state guidelines and our standards.

People Feel confident.
Staff and leaders have the skills and confidence to use AI well.

Trial Period: July 1 – December 31, 2026

Participants: State employees

Our commitment: Operate within Washington State policy while creating learning and engagement opportunities.

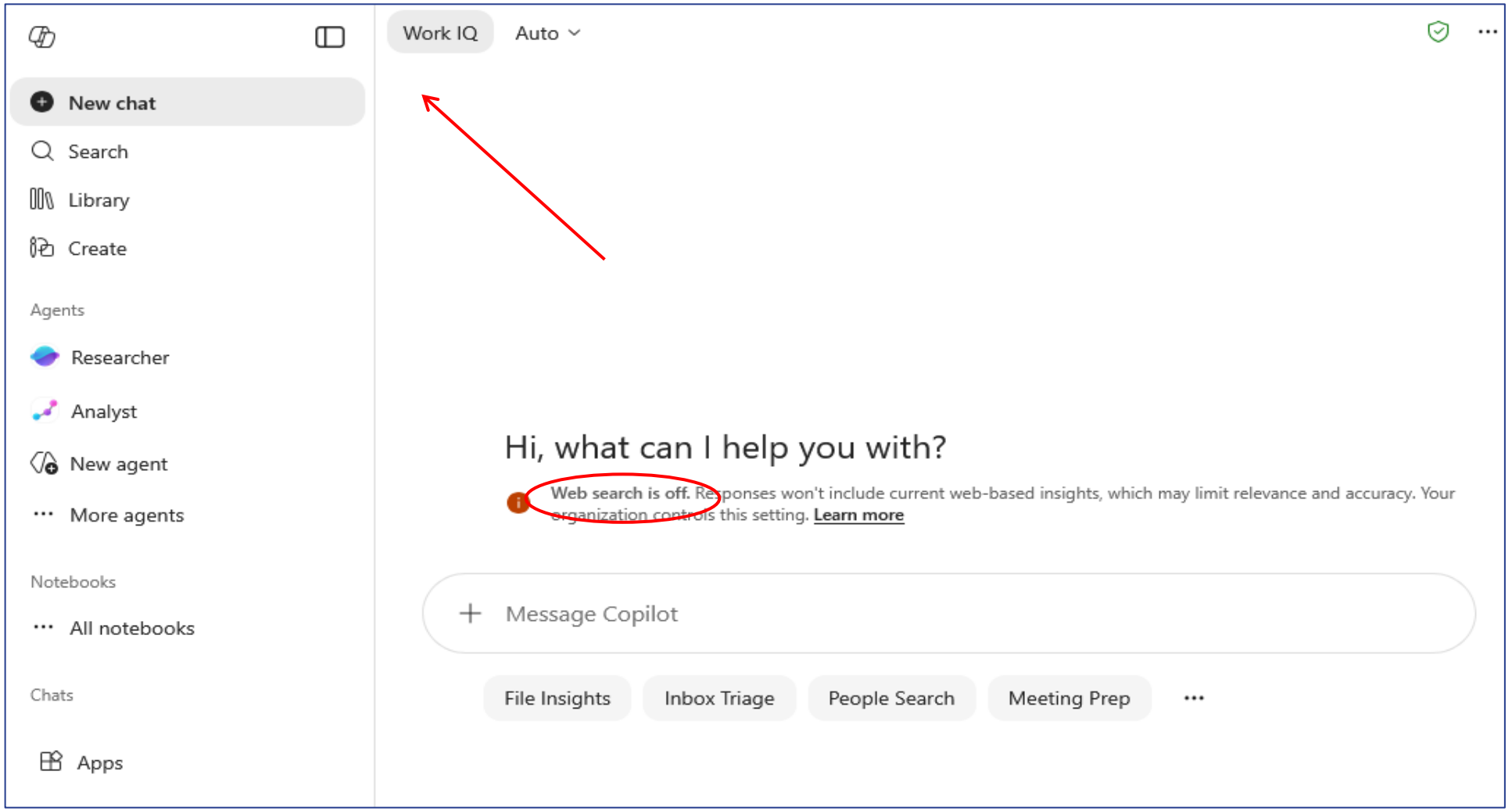
WaTech
Washington Technology Solutions

Webgrounding and Data Considerations Example

- Product terms for Copilot:
- *Excerpt: The Microsoft Products and Services Data Protection Addendum (DPA) doesn't apply to the use of generated web search queries in Microsoft 365 Copilot, Microsoft 365 Copilot Chat, or the Bing search service. Also, HIPAA compliance and the EU Data Boundary don't apply to generated search queries.* Data, privacy, and security for web search in Microsoft 365 Copilot and Microsoft 365 Copilot Chat | Microsoft Learn

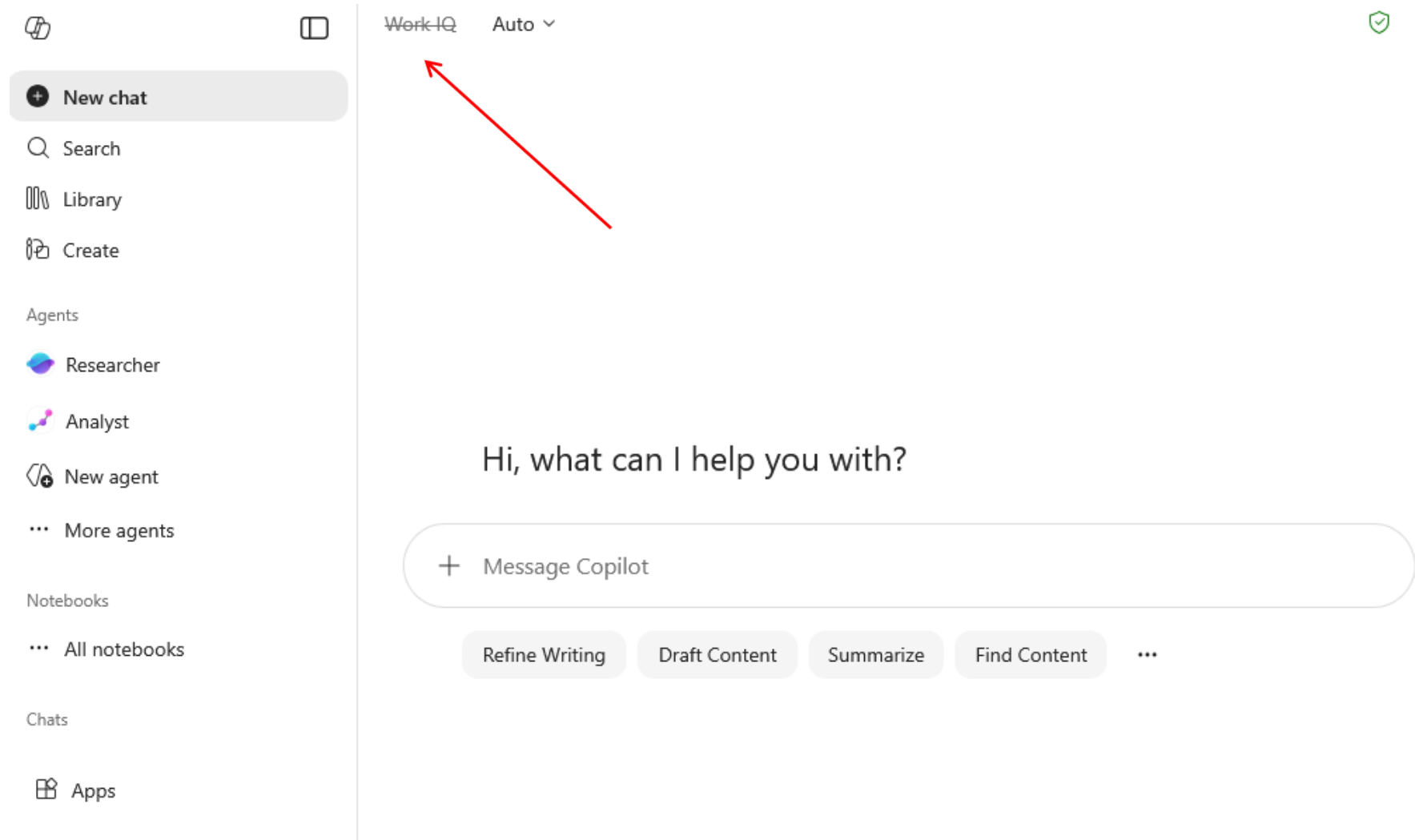
- Mitigations per Microsoft:
- Copilot web query is only a few keywords (not your prompt, not your files) with tenant and user identifiers removed.
- Additional controls available include disabling web search in Work mode via Cloud Policy.
- Enforcing sensitivity labels and Data Loss Prevention
- Use of Zero Query Logging to prevent retention
- Admins can audit Copilot interactions, including web-search-related keywords, through Purview Audit and related compliance workflows.

WorkIQ (webgrounding on)



WaTech
Washington Technology Solutions

WorkIQ (webgrounding on)



WaTecn
Washington Technology Solutions

Copilot Data Classification Considerations

Least risk is for Category 1 and Category 2 information used with Copilot webgrounded. Category 3 or Category 4 information may leave the tenant and can be at risk of leakage.

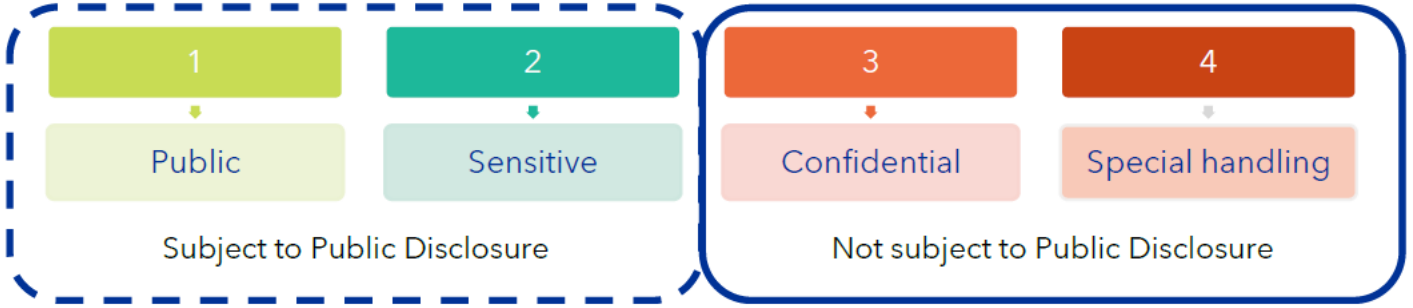
- Recommend that if you would not include information in a normal search engine query, you should not put it into Copilot Chat or Copilot WorkIQ. Category 1 and Category 2 information includes information that is, or could be, made available to the public. Many internal documents, like communications with other employees or internal analysis, are Category 2 unless a specific public records exemption applies. Category 3 and Category 4 information includes any information with a specific public records exemption. Examples include:
- Security or infrastructure information,
- Proprietary financial information,
- Personnel information about employees or job applicants, and
- Information protected by federal laws like the Health Insurance Portability and Accountability Act (HIPAA).

WaTech
Washington Technology Solutions

Data Classification Standards (at a glance)

These data categories are defined in [Data Classification Standard | WaTech]

(SEC 08-01-S Data Classification Standard) and examples are included below:



	Free CoPilot Chat	Full CoPilot **Work**	Full CoPilot **Web**
Upload	Cat 1-2	Cat 1-4	Cat 1-2
Access	Internet	Cat 1-4	Internet

WaTech
Washington Technology Solutions

Risk Assessments

WaTech
Washington Technology Solutions

By December 2024, WaTech will produce guidance on the risk assessments for the deployment of High-Risk Generative AI Systems. Assessments must leverage existing security and privacy assessment processes, and must include the following…

- Executive Order 24-01, sec. 8

Executive Order 24-01 on Artificial Intelligence (Sec. 8)

a. Information about the High-Risk Generative AI System, including whether the High-Risk Generative AI System is provided by a third party, the name and address of the third party, and relevant state agency;

b. The intended uses of the High-Risk Generative AI System;

c. Assessment of the fitness of the High-Risk AI System for the intended purpose;

d. Assessment of impacted communities, benefits, harms, and mitigations of the High-Risk AI System;

e. An evaluation of the potential harms of the High-Risk Generative AI System which may include harms to individuals and groups, discriminatory or unfair outcomes, deceptive practices, societal risks, privacy and cybersecurity considerations, and national security concerns;

f. An assessment of mitigations including but not limited to consideration of restricted uses and limitations on use, policies, deidentified data, and commercial terms; and

g. Information about the agency approach to generative AI governance that is consistent with the AI Risk Management framework published by the National Institute of Science and Technology.



[Artificial Intelligence Resources]

WaTech
Washington Technology Solutions

High-Risk Generative AI System

- "High-Risk Generative AI System" means 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.

- **Executive Order 24-01**

WaTech
Washington Technology Solutions

- Whether a system creates a high risk is dependent on:
  (1) the magnitude of an impact to natural persons' health and safety or fundamental rights, and
  (2) the likelihood of that impact occurring.

- Risks include both:
  - Direct impacts, such as when an AI system is used to determine eligibility for benefits, and
  - Indirect impacts, such as when an AI system is used to allocate resources in a way that impacts the people in a particular community.

WaTech
Washington Technology Solutions

Magnitude	Likelihood
1 – Negligible. No foreseeable direct or indirect impact to natural persons.	**1 – Remote or improbable**. Very low chance of occurring.
2 – Low. Any impact to natural persons is very unlikely to impact health, safety or fundamental rights.	**2 – Unlikely**. Low chance of occurring.
3 – Moderate. Some impact to natural persons that may include indirect impact to health, safety or fundamental rights.	**3 – Possible**. Moderate chance of occurring.
4 – Significant. Major effect causing substantial harm or disruption to health, safety or fundamental rights. May include direct impact in individual circumstances, or indirect, systemic impacts.	**4 – Likely**. High chance of occurring.
5 – Severe or catastrophic. Extreme impact resulting in serious harm, injury or violation of fundamental rights.	**5 – Probable**. Very high chance of occurring.

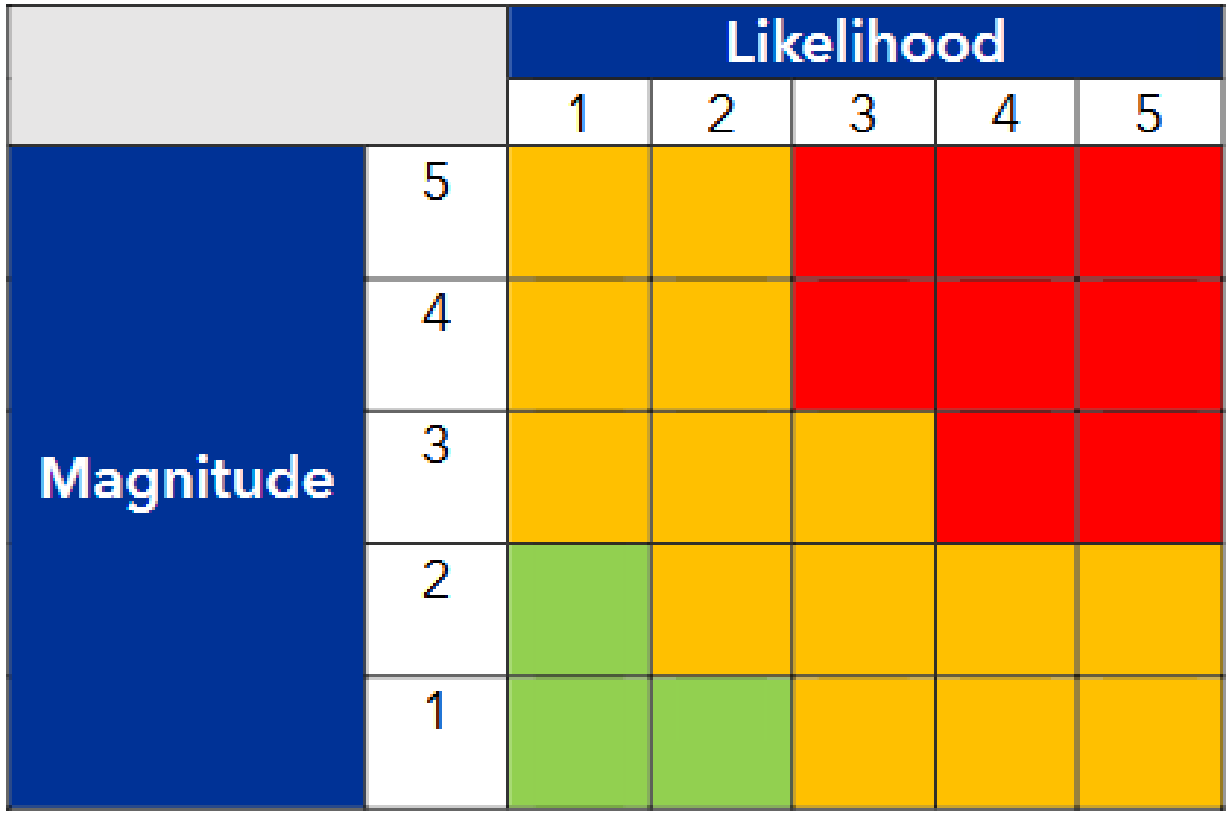
WaTech
Washington Technology Solutions

[Magnitude] x [Likelihood] = Risk level

1-2 = Low

3-11 = Moderate

12-25 = High



The intended use and operating context

- What is the intended use of system outputs and who will benefit?
- Who might be adversely impacted and how? Consider at least the workforce, customers/residents, and vulnerable or underserved populations.
- What is the role of humans in reviewing system outputs? For example, do they have little to no review, do humans review in defined circumstances, or do humans verify, modify, or review all outputs?
- Who are the intended users? Is it intended for internal or external use? Is it intended for broad use or a small group of people?
- What laws apply to agency use of the system?
- What alternatives were considered and why is this the preferred option?

Data characteristics

- What is the highest data classification level for included information? Consider both information used for training and information processed during operation, including intended prompts, inputs, fine-tuning, augmentation or any other system customization.
- What type of information is involved? Will the system process personal information?

System characteristics and safeguards

- Is there evidence of biased, discriminatory, inaccurate or otherwise unreliable outputs? What measures are in place to address unreliable outputs?
- Are there built-in filters or monitoring to detect harmful outputs, manipulation, or misuse?
- How explainable is the system? Do users know the system uses AI? Does the system provide sources or otherwise help identify to users why it is producing a particular output?
- How transparent is system implementation? Are users trained or notified of appropriate use and system limitations

Example Copilot Risk Assessment

Risk Assessment Form to be completed before adoption and deployment of AI System. Example risk assessment form is available on WaTech website for Copilot trial.

[Risk Assessment Template.docx]

Microsoft 365 Copilot Trial

How to get started

Step 1: Complete a Microsoft 365 Copilot training. Some options are listed **here**.

Step 2: Complete a Risk Assessment. This template is provided as a starting point. WaTech does not need to review this; it is up to each agency to complete according to their own standards.

Step 3: Obtain approval from agency executive leadership.

Step 4: Submit a ticket in ServiceNow following **this template**. Once received, each agency will begin a formal onboarding process.

RESOURCES

- FAQs (PDF)
- Risk Assessment Form
- ServiceNow Ticket Template to Request Onboarding
- Sign Up for Updates on GovDelivery
- Statewide M365 Copilot Cohort

WaTech
Washington Technology Solutions

WaTech
Washington Technology Solutions

Risk Assessment Report &
Risk Treatment Plan
for Confidential Systems

<Agency>
<System Name>

Executive Summary

The categorization (criticality) for this Information System is assessed as

Confidentiality	Integrity	Availability
<Low/Moderate/High>	<Low/Moderate/High>	<Low/Moderate/High>

This document presents a Risk Assessment Report (RAR) and a Risk Treatment Plan (RTP) to evaluate and mitigate risks to the information system's confidentiality, integrity, and availability throughout its lifecycle. The system is assessed based on its impact to the organization, following state policies (e.g., SEC-11) and industry standards like NIST SP 800-30 and NIST SP 800-53. The report identifies vulnerabilities, threats, and evaluates their potential impact and likelihood. It also recommends prioritized controls to address these risks.

The assessment focuses on both internal and external risks, particularly those related to the application of NIST SP 800-53 controls. As a Tier 3, "information system level" assessment, it identifies key risks tied to vulnerabilities and controls, though it may not cover all possible issues.

The RTP provides mitigation strategies and assigns responsibility for each identified risk, ensuring compliance with regulatory requirements and data protection standards. Selected controls target specific threats to maintain the system's security and resilience.

The document will be updated after certification testing to incorporate any new vulnerabilities or findings. The goal is to reduce the likelihood of security incidents, protect critical assets, and support the system's long-term security and operational health.

AI Governance Continued

WaTech
Washington Technology Solutions

Monitoring and Oversight

Operations

Service desk tickets

License activity

Records

Audit Logs

Security Tools

System alerts

WaTech
Washington Technology Solutions

Incident Response

- Follow standard incident response protocols regarding reporting potential incident to security or privacy contact.
- Investigate incident to determine potential for breach.
- Evaluate incident and report and notify affected individuals if appropriate.
- Perform remediation and mitigation.

WaTech
Washington Technology Solutions

WaTech
Washington Technology Solutions

AI Governance and Accountability

- Who is allowed to use AI?
  - Employees who have received training
- For what purposes?
  - Business purposes relevant to positions
- What risks must be reviewed?
  - Risk assessment must be completed by AI Governance cross functional team and highest risks need to evaluated and accepted by appropriate authority within organization.
- What data can be used?
  - Depends on use case, security, privacy, legal considerations, product terms of use
- Who is accountable for decisions?
  - Users up to executive management
- How are systems tested, monitored, and audited?
  - Logging and monitoring
- What happens when something goes wrong?
  - Prepare incident response plan

Lessons learned

- Making up nonexistent corporate policies
- Legally binding offers
- Swearing at customers
- Referencing fake legal cases
- Giving harmful health advice
- Recommending glue on pizza
- Advising users to break the law
- Encouraging self harm

- In Washington – Test Drive a Win Marketing Campaign
- **The Concept:** Created by marketing agency, the promotional campaign allowed users to upload a selfie or headshot. The AI would then superimpose their likeness into simulated "dream vacations" they could theoretically buy if they won the lottery jackpot.
- **The Controversy:** A woman from Washington used the app and selected a “swimming with sharks” option. The AI allegedly generated an image that inappropriately depicted her as topless in a bed with fish swimming around her.

Additional AI Governance Tenets

- **Accountability:** Clear ownership and responsibility for AI systems and outcomes.
- **Risk management:** Identifying and managing risks before and after deployment.
- **Privacy and security:** Protecting personal, confidential, and sensitive information.
- **Fairness:** Preventing discriminatory or inequitable outcomes.
- **Transparency:** Providing appropriate notice, documentation, and understanding of how AI is being used.
- **Human oversight:** Ensuring people retain meaningful responsibility for consequential decisions.

Fairness

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.

WaTech
Washington Technology Solutions

Fairness

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

- Controls for potential risks and outline mitigation strategies, including addressing **risk of bias and discrimination** and disparate impacts on vulnerable communities.
- 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.
- Considers if **due process rights** for individuals would be appropriate for High-Risk Generative AI system and create process for human review if appropriate.

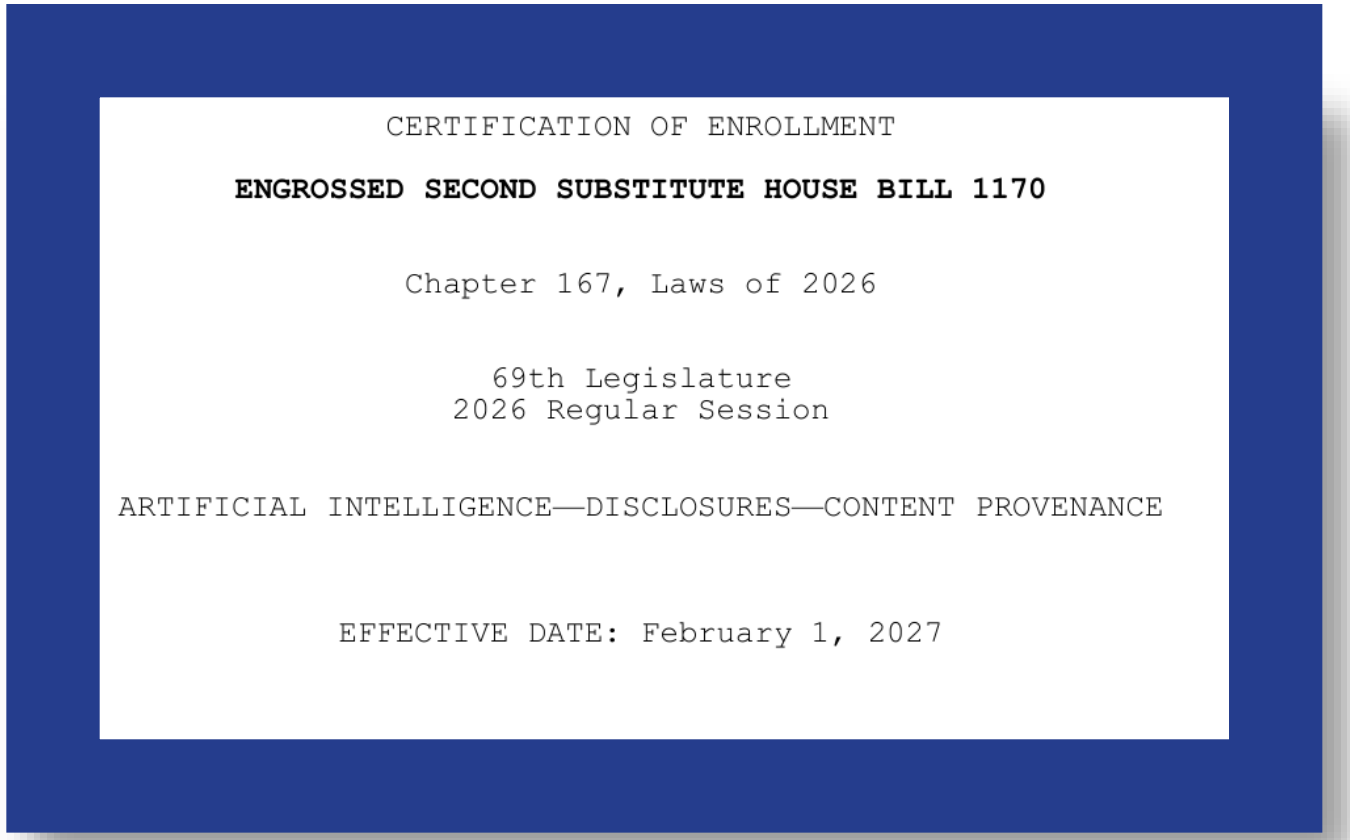
WaTech
Washington Technology Solutions

Government Use of AI Requirements

WaTech
Washington Technology Solutions

Transparency – RCW 42.64.010 (effective February 1, 2027)

- Required by law RCW 42.64:
- A government agency that makes available an artificial intelligence system intended to interact with consumers must disclose to each consumer, before or at the time of interaction, that the consumer is interacting with an artificial intelligence system.



CERTIFICATION OF ENROLLMENT

ENGROSSED SECOND SUBSTITUTE HOUSE BILL 1170

Chapter 167, Laws of 2026

69th Legislature
2026 Regular Session

ARTIFICIAL INTELLIGENCE—DISCLOSURES—CONTENT PROVENANCE

EFFECTIVE DATE: February 1, 2027

WaTech
Washington Technology Solutions

Disclosure Notice Contents

- The disclosure must be:
  - Clear and conspicuously posted;
  - Written in plain language; and
  - May not use a dark pattern
- The disclosure may be provided by using a hyperlink to direct a consumer to a separate web page.

- Clarification –
- "An agency is required to make the disclosure …regardless of whether it would be obvious to a reasonable consumer that the consumer is interacting with an artificial intelligence system."

Disclosures must be clearly and conspicuously posted

- "Clear and conspicuously posted" means information is placed in plain, unobstructed public view, using, size, contrast, and location to ensure it is readily noticeable, readable, and understandable. It must stand out from surrounding text or materials so a person can easily see and comprehend it.

Key Elements

- **Location:** Placed where customers are likely to look when interacting with AI.
- **Format:** Large enough typeface, with high contrast, and unobstructed by other materials.
- **Digital/Online:** Hyperlinks should be in all-caps or higher contrast, appearing before use, and not hidden in pop-ups.

Disclosure must be written in plain language

- Plain language is the practice prioritizing ease of use and ease of understanding in writing and design. The goal of plain language practices is to deliver a message that your recipient will understand on their first read.
- Plain language principles include:
  - Create short sentences.
  - Use common words.
  - Avoid jargon.
  - Use personal pronouns.
- Use active voice so the reader knows who does what.
- Use verb-driven headings to convey order.
- Tag headings for accessibility.
- Create negative (white) space.
- Label images and graphs with alternative text.
- Design clear pages.
- Employ **plain language guidelines** and **plain language resources.**
- See Executive Order 23-02.

WaTech
Washington Technology Solutions

Disclosure may not use a dark pattern

Dark patterns = design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm.

WaTech
Washington Technology Solutions

Dark Pattern Examples

Pattern Type	Examples
Obstruction	One-click subscription with tedious cancellation process
Urgency and scarcity	False low stock or high demand messages Timers or claims of limited time offers
Hiding or delaying information	Hidden costs or drip pricing Unexpected automatic subscription after trial
Interface interference	Ads that appear to be news articles or independent product reviews Formatting misdirection
Coercion	Mislabeled or changing button functionality Repeated requests or requests that don't allow a permanent choice
Asymmetric choice	Difficult to find or change default preferences Preselecting preferred choices Shame statements to influence choices

WaTech
Washington Technology Solutions

FTC Staff Report: Bringing Dark Patterns to Light, Sept. 2022

Notice considerations

- **Timing -Before or at the time of interaction**
  - Not buried after the interaction begins or hidden only in a general website footer.
- **Delivery option - Hyperlink allowed**
  - A short just-in-time notice can link to a separate AI transparency page with more context.
  - Use layered, just-in-time disclosures that are obvious without interrupting service delivery.
- **Presentation**
  - Clear and conspicuously posted
  - Plain language
  - No dark pattern

Example Practical Notice Patterns

Example landing-page banner

You are chatting with an AI assistant. It can help answer questions, but agency staff may review or follow up. Learn more about how this tool works.

Good notices

- Use “AI” and “artificial intelligence” plainly.
- Appear before or as the interaction starts.
- Link to details on use, privacy, and contact route.

Example chat-opening notice

This service uses artificial intelligence to respond to your message. Do not submit sensitive personal information. View AI and privacy details.

Avoid

- Generic “technology may be used” language.
- Tiny footer-only references or misleading button design.
- Dark patterns that obscure or downplay the disclosure.

WaTech
Washington Technology Solutions

Considerations for a linked AI transparency notice or page

Notice Sections	Content Considerations
AI identity	State that the user is interacting with an AI system, and name the service or use case.
Purpose & limits	Explain what the tool is intended to do and what it cannot do.
Data practices	Describe what information is processed, whether personal information is needed, retention, and sharing.
Human support	Explain how to reach staff, request accommodation, report a concern, or seek correction
Governance	Identify agency owner/contact and review/update cadence

WaTech
Washington Technology Solutions

Keep in mind: RCW 42.64 permits a hyperlink. The linked page should support both legal disclosure and public understanding

Implementation Roadmap for Agencies

- Consider a plan to get ready for compliance before Feb. 1, 2027

1

Inventory

List public AI touchpoints: chatbots, voice agents, virtual assistants, image, audio, video AI services, and embedded vendor tools.

2

Classify

Decide whether each tool is intended to interact with consumers and what notice pattern applies.

3

Design notice

Draft a short front-end disclosure and a linked AI transparency page using plain language.

4

Govern

Add procurement, release, and change-management checks; assign owner for each notice.

5

Monitor

Review at least annually and whenever system behavior, vendor, audience, or data processing changes.

WaTech
Washington Technology Solutions

Alignment with Washington State Agency Privacy Principles

Privacy Principle	Implementation Alignment
Transparency & accountability	Clear notice, demonstrable compliance, complaint/response channels.
Lawful, fair, responsible use	No deceptive interactions; evaluate impacts, especially for sensitive contexts.
Individual Participation	Provide accessible contact, correction, access, opt-out or human-assistance routes when appropriate.
Due diligence	Vendor and third-party AI terms should support agency notice, auditing, and privacy commitments.
Purpose limitation	Explain what the AI interaction is for and keep use compatible with that purpose
Data minimization	Discourage unnecessary personal data collection; avoid asking for sensitive information unless needed.

Key Takeaways of RCW 42.64 Requirements for public agencies

Who

Government agency that makes available an AI system intended to interact with consumers.

What

Disclose before or at the time of interaction that the consumer is interacting with AI.

How

- Clear and conspicuous,
- Plain language,
- No dark patterns;
- Hyperlink to a separate page is permitted.

Even if obvious

Disclosure is required even when a reasonable consumer would recognize the AI interaction.

The practical impact: Make public agency AI use visible, understandable, and documented wherever the public interacts with an agency AI system.

WaTech
Washington Technology Solutions

Human Oversight – Focus of AI Strategy

Humans in the Lead – People remain accountable for the outcomes of AI-enabled systems. Human oversight should be applied where appropriate based on the level of risk and potential impact to Washingtonians.

- AI augments human capability rather than displacing it.
- Human judgment, agency accountability, and workforce development must remain central as AI adoption expands.

Strategic objective: Support agencies in using agentic AI and other advanced capabilities for appropriate, high-value use cases, with human oversight, authorization, and safeguards scaled to risk.

https://watech.wa.gov/strategy/washingtons-ai-strategy-and-roadmap

WaTech
Washington Technology Solutions

AI Governance Takeaway

AI governance is the framework by which government ensures that artificial intelligence is used

- lawfully,
- securely,
- transparently,
- equitably, and
- effectively,
- with appropriate human oversight and
- accountability

throughout the AI lifecycle.

WaTech
Washington Technology Solutions

Additional Policy and Governance Resources

- Artificial Intelligence Risk Level Guidance (PDF)
- DATA-03: Privacy and Data Protection Policy (PDF)
- DATA-04: Artificial Intelligence Policy (PDF)
- Executive Order 24-01 Artificial Intelligence (PDF)
- Framework for Accountability in Generative Artificial Intelligence (PDF)
- Guidelines for Deployment of Generative AI_Dec. 2024 (PDF)
- Impact of generative artificial intelligence on the Washington state workforce_Dec. 2024 (PDF)
- Initial Procurement Guideline for GenAI_Sept. 2024 (PDF)
- Managing Generative AI Records_Secretary of State
- MGMT-01-01-S — Technology Portfolio Foundations Applications
- MGMT-01 — Technology Portfolio Foundation
- Overview of Washington's AI Policy_Feb. 2026 (video)
- RCW 39.34.240 Data requests—When written agreement required
- RCW 39.26.340 Data-sharing agreements—When required
- RCW 42.52.050 - Confidential information
- SEC-08 - Data Sharing Policy
- State of Washington Generative Artificial Intelligence Report_Sept. 2024 (PDF)
- Technology Policies, Standards, and Procedures (7.b.)

Questions

Office of Privacy and Data Protection

Washington Technology Solutions

privacy@watech.wa.gov



WaTech
Washington Technology Solutions