POLICY

Artificial Intelligence (AI) Policy

POL-211

I. PURPOSE

This policy establishes the standards that City of Seattle (City) departments, staff, and representatives shall observe when acquiring and using Artificial Intelligence (AI) solutions in City service delivery and decision-making, ensuring effective, secure, and responsible practices.

Objectives:

- Define the processes that enable solutions that use AI systems to solve City challenges and enhance service delivery, while simultaneously ensuring responsible use of AI at the City in a manner that is reflective of the City's values, as detailed in the City's AI Guiding Principles.
- Provide clear, easy-to-follow guidance that supports decision-making for City staff, vendors, and partners who purchase, configure, develop, operate, and/or maintain systems that provide municipal services.
- Ensure that when using AI, the City or those operating on its behalf, adhere to the Guiding Principles that represent the City's values regarding how AI solutions are purchased, configured, developed, operated, or maintained.
- Enable partnerships with the private, academic, and non-profit sectors that support the City's understanding, learning, responsible testing, and effective operationalizing of new technologies and improve City services provided they meet defined performance, security, privacy, and responsible use requirements.
- Define roles and responsibilities related to the intake, review, and sustainment of AI solutions.
- Set required processes to detect, assess, and manage risks presented by AI solutions at points of acquisition, implementation, and adoption, including preventing prohibited uses.
- Align the governance of AI with the City's ongoing data governance, security, privacy, and contracts programs in compliance with applicable local, state, and federal laws, and existing City agency policies.

II. SCOPE

This policy applies to:

- All staff (full-time, part-time), interns, consultants, vendors, contractors, partners, and volunteers who provide City services or otherwise act on behalf of the City.

III. AUTHORITIES & ENFORCEMENT

The City's AI Policy is created and maintained under the CTO ordinance, SMC 3.23.030, and authority granted therein as coordinated with the Mayor's Office of the City of Seattle.

The CTO or their designee may, at their discretion, inspect the usage of AI solutions to ensure the City's responsible use and adherence to this policy in order to protect the City and the

residents we serve. They may require a department to alter or cease a partner's usage of AI on behalf of the department, which may include service or contract termination.

IV. TERMS & DEFINITIONS

Artificial Intelligence or AI: A machine-based system that, for explicit or implicit objectives, infers from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[1]

Algorithm: A series of logical steps through which an agent (typically a computer or software program) turns particular inputs into particular outputs.

AI Review: A process to evaluate a proposed AI solution to ensure that it complies with the City's AI Guiding Principles and relevant IT Security and Privacy Policies.

AI System: Any system, software, hardware, application, tool, algorithm, model, or utility that, in whole or in part, leverages artificial intelligence technologies—such as machine learning, natural language processing, or predictive analytics—to perform tasks, generate insights, or support decision-making traditionally requiring human intelligence.[2]

AI Solution: A deployed or implemented application of any of AI systems to solve problems, improve services or support City operational goals.

Consequential Decision-making: A decision or judgment that has a legal, material, or similarly significant effect on an individual's life relating to the impact of, access to, or the cost, terms, or availability of rights, services, or legal action.[3]

Generative Artificial Intelligence (Generative AI): is a class of computer software and systems, or functionality within systems, that use large language models, algorithms, deep-learning, and machine learning models, and are capable of generating new content, including but not limited to text, images, video, and audio, based on patterns and structures of input data. These also include systems capable of ingesting input and translating that input into another form, such as text-to-code systems.

Partners: Individuals, agencies, organizations, or institutions working with or on behalf of the City, including but not limited to non-profit organizations, other government agencies, academic institutions, community-based organizations, or other organizations external to the City, otherwise not represented as "users".

Responsible AI Use: An approach to developing, procuring, and using AI solutions ethically, in a manner that centers community needs and considers equity, innovation, efficiency, transparency, privacy, security, and resiliency in delivery of exceptional City services. Use of AI that aligns with City and community values rooted in trust and consideration of impacts to residents.

---

[1] Organisation for Economic Co-operation and Development (OECD), "Updates to the OECD's definition of an AI system explained", 2023.
[2] White House Briefing Room, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence", 2023, (accessed on 7/1/2024).
[3] California Legislature: 2023-2024 Regular Session, "California Assembly Bill 331 (2023 CA A 331)", 4/19/2023.

Vendor: A person or entity who delivers services and/or products to the City under a contract. For purposes of this document, "vendor" is indistinguishable from a "contractor," and "consultant."

Additional terms and definitions are provided in the AI Acquisition & Operation Manual.

V. GUIDING PRINCIPLES

The City's use of AI shall align with its values and responsibilities to the residents it serves. City employees shall adhere to the principles and requirements set forth in this policy and will be held accountable for compliance with these commitments.

The City's AI Principles were developed with input from industry experts and researchers.

Innovation and Sustainability: The City values public service innovation to meet our residents' needs. We commit to responsibly explore and evaluate AI technologies, which will improve our services and advance beneficial outcomes for both people and the environment.

Transparency and Accountability: The City values transparency and accountability and understands the importance of these values in our use of AI systems. The City will ensure that the development, use, and deployment of AI systems are evaluated for and compliant with all laws and regulations applicable to the City prior to use and will make documentation related to the use of AI systems available publicly.

Validity and Reliability: The City must ensure that AI systems perform reliably and consistently under the conditions of expected use, and that ongoing evaluation of system accuracy throughout the development and/or deployment lifecycle is managed, governed, and auditable, to the greatest extent possible.

Bias, Harm Reduction, and Fairness: The City acknowledges that AI systems have the potential to perpetuate inequity and bias resulting in unintended harms on Seattle residents. The City will evaluate AI systems through an equity lens in alignment with our Race and Social Justice commitments for potential impacts such as discrimination and unintended harms arising from data, human, or algorithmic bias to the extent possible.

Privacy Enhancing: The City values data privacy and understands the importance of protecting personal data. We work to ensure that policies and standard operating procedures are in place to reduce privacy risk, and are applied to AI systems throughout development, testing, deployment, and use to the greatest extent possible.

Explainability and Interpretability: The City understands the importance of leveraging AI systems, models, and outputs that are easily interpreted and explained. We work to ensure all AI systems and their models are explainable to the extent possible, and that system outputs are interpretable, communicated in clear language, and representative of the context for use and deployment.

Security and Resiliency: Securing our data, systems, and infrastructure is important to the City. We will ensure AI systems are evaluated for resilience and security, and can maintain confidentiality, integrity, and availability of data and critical City systems, through protection mechanisms to minimize security risks to the greatest extent possible, in alignment with governing policy and identified best practices.

VI. RESPONSIBLE USE OF AI SOLUTIONS

The City is committed to using AI solutions responsibly. Responsible use requires the balance of protecting the privacy of residents, providing exceptional municipal services, and responding to community needs prioritized by the Mayor, Council, and City departments.

Specific guidance on Responsible AI use can be found in the AI Acquisition & Operations Manual and the Responsible AI Use Guideline protocol documents.

The Seattle Information Technology Department is responsible for providing training and new-skilling resources for AI foundations, approaches to AI, and specific solution building. City employees should complete these trainings and the skill development work to properly prepare for creating AI-driven municipal solutions.

VII. RESPONSIBILITIES

Enforcement of and compliance with this policy requires the following roles and responsibilities:

Role	Responsibility
Chief Technology Officer (CTO)	Directing the City of Seattle technology resources, policies, projects, services, and coordinating the same with other City departments.
	Designating oversight roles associated with AI use, policy maintenance, and compliance.
	Leading communication of, adherence with, and enforcement for this policy, as well as updates to the policy.
Chief Information Security Officer (CISO)	Ensuring AI solutions have required controls, monitoring, and incident response, in accordance with the City's IT Security Policy (ITSP).
	Overseeing the security practices of AI solutions.
Chief Privacy Officer (CPO)	Ensuring AI solutions are used in accordance with this policy and the City's Privacy Policy.
	Coordinating review of AI solutions procured through ITD for use by City departments, including coordinating completion of the AI Vendor FactSheet, as detailed in the AI Acquisition & Operation Manual.
	Overseeing the privacy practices of AI solutions.
	Creating and maintaining AI risks and impact criteria and the documentation to support the exception review process for AI solutions.
Departments	Complying Acquisition of Technology Resource Standard when acquiring or using AI solutions, and requiring vendors to comply with City Policies through contractual agreements.
	Complying with this policy and following updates to associated guidelines and the AI Acquisition & Operation Manual.
City Attorney's Office (CAO)	Advising on any legal issues or risks associated with AI solutions usage by or on behalf of City departments.
City Procurement Teams	Ensuring the City's AI standard contract terms are represented in contracts involving AI solutions.

VIII. POLICY

City of Seattle AI solutions must be used to solve meaningful challenges and enhance service delivery. At the same time, they must reflect Seattle values through responsible, secure and transparent use.

Failures in AI-driven solutions erode public trust in City services and confidence in our staff, often at a greater scale than in traditional technologies. To mitigate these risks, all AI work, systems, and solutions must:

1. Adhere to established City security, privacy, and responsible use practices and principles.
2. Assess and control for risks at every stage from procurement to deployment ("go-live").
3. Monitor and manage performance and impact throughout the solution's lifecycle.

The City's AI Acquisition & Operation Manual and other policies, guidelines, and procedures shall provide guidance as relevant. All AI solutions acquired, configured, developed, operated, or maintained by or on behalf of the City should align with requirements below.

General AI

1. Be in compliance with and uphold the City's AI Guiding Principles.

Acquisition

1. Undergo an AI Review in addition to the standard applicable reviews associated with all non-standard/new technology acquisitions, to assess the potential risks of the AI solution and associated use case. High risk systems and/or use cases, as defined by federal and state policies and the City Responsible AI Program's review are subject to an Algorithmic Impact Assessment. This applies to free-to-use software or software-as-a-service tools.
2. Require technical documentation about AI solutions using the AI FactSheet or create equivalent technical documentation about AI solutions. Require City standard contract terms and conditions, including AI standard terms for bias detection, transparency, correction, data use and ownership, security, quality and auditing, human oversight, termination or disengagement, record-keeping, and liability, to be in place in contracts involving procurement, development, use, deployment, or maintenance of AI solutions. Components of AI standard contract terms can be found in Responsible AI Use Guideline.
3. Engage with the Privacy and Responsible AI Program for review if a previously acquired technology in use at the City adds or incorporates new AI capabilities. Seattle IT may restrict the use or revoke authorization for a technology if, in its judgment, those AI capabilities present risks that cannot be effectively mitigated to comply with this policy or other City policies.

Use and Operation

1. Users may only access, install, or utilize AI solutions that have been reviewed and approved by the IT Department.

2. Prohibit use of City data to train public instances of AI solutions that are not covered under the City's standard contractual terms, as doing so may increase security and legal risks and may result in a data leak.

3. Be subject to AI solution incident monitoring. In the event of an incident involving the use of an AI solution, the City will follow incident response protocols as detailed in the AI Incident Response Plan, as scoped to information technology solutions. The CISO is responsible for overseeing the security practices of AI solutions used by or on behalf of City departments. In the event of an AI incident, the CPO will support the AI incident response as detailed in the AI Incident Response Plan. AI incidents associated with operational technologies are driven by associated departmental response plans, with support from the CPO and CISO as applicable.

4. Align AI solution use and data processing activities with City Privacy Principles and Information Technology Security requirements associated with the use of personal data in AI solutions.

Reducing Bias and Harm

1. AI solutions may produce outputs based on stereotypes or use data that is historically biased against protected classes. City employees must leverage RSJI resources (e.g., the Racial Equity Toolkit) and/or work with their departmental RSJI Change Team to conduct and apply a Racial Equity Toolkit (RET) prior to the use of an AI solution, especially uses that will analyze datasets or be used to inform decisions or policy. As per the objectives of the RSJ program, the RET should document the steps the department will take to evaluate AI-outputs to ensure they are accurate and free of discrimination and bias against protected classes.

Generative AI

Generative AI introduces specific capabilities applied to the creation of new content. As we seek to use and implement these technologies responsibly and efficiently, there are some unique aspects of generative AI solutions. The provisions below aim to support deployment and use of these systems.

Oversight in Use of Generative AI Outputs

1. Outputs of Generative AI solutions must be reviewed by humans prior to each use in an official City capacity (“Human in the Loop” or HITL). HITL review processes shall be documented by owning departments and shall demonstrate how the HITL review was conducted to adhere to the principles outlined in this document. For real time or public facing use-cases risk will be evaluated and mitigated by controls determined during the AI review process. Documentation of HITL reviews shall be retained according to the appropriate records retention schedule.

Attribution, Accountability, and Transparency of Authorship

2. All images and videos created by Generative AI solutions must be attributed to the appropriate Generative AI solution. Wherever possible, attributions and citations to the City should be embedded in the image or video (e.g., via digital watermark).

3. If text generated by an AI solution is used substantively in a final product, attribution to the relevant AI solution is required.

4. If a significant amount of source code generated by an AI solution is used in a final software product, or if any amount is used for an important or critical function, attribution to the appropriate AI solution is required via comments in the source code and in product documentation.

5. All attributions should include the name of the AI solution used plus an HITL assertion (which should include the department or group who reviewed/edited the content).

   Example: Some material in this brochure was generated using ChatGPT 4.0 and was reviewed for accuracy by a member of the Department of Human Services before publication.

6. Departments shall interpret "substantive use" thresholds to be consistent with the principles outlined in this document as well as relevant intellectual property laws.

Prohibited Uses

The following uses of AI are prohibited:

- Emotion analysis that uses computer vision techniques to classify members of the public's facial and body movements into certain emotions or sentiments (e.g., positive, negative, neutral, happy, angry, nervous).
- Social scoring, or the use of AI solutions to track and classify individuals based on their behaviors, socioeconomic status, or personal characteristics in ways that harm individuals.
- Cognitive behavioral manipulation or deception of people or specific vulnerable groups.
- Directing or integration with autonomous weapons systems.
- Consequential decisions made solely by AI solutions with no human oversight including hiring, performance reviews, discipline, investigations, terminations, and financial grants and awards.
- Creation or distribution, even with attribution or disclosure, of digitally generated or digitally altered depictions of an individual without their consent, or of any subject with the purpose or intent of deceiving City employees or members of the public.
- Use of mass media sources for facial recognition data without permission or court authorization.
- Biometric and social categorization and/or scoring to determine protected class information or political opinions.

If City staff become aware of an instance where an AI solution has caused harm either through direct action taken or as a result of the system being compromised, staff must report the instance to their supervisor and the CPO.

High-Risk Uses

High-risk uses are identified through the AI Review and risk analysis and assessed based on an NIST-aligned risk framework, as detailed in the AI Acquisition & Operation Manual.

The following uses and characteristics of AI solutions are considered high-risk. A classification as high-risk does not disqualify use but requires an AI assessment (AIA) and additional controls be put into use. The AIA process will recommend mitigations and controls that will allow for the responsible use of the AI solution.

- Fully automated decisions that do not apply meaningful human oversight but may cause significant harm to members of the public. This includes using AI solutions that are used to automatically make health, financial, or life opportunity decisions, or that manage essential services or critical infrastructure for the City.

- Using AI solutions to perform real-time and covert biometric identification, or process the data collected from such systems**,** excluding identification as required for law enforcement/police purposes under expressed authority by Seattle Municipal Code, statute (e.g., CFR, RCW), case law, and/or state or federal law or constitutions (e.g., Probable Cause, Warrant, etc.).
- AI solutions that monitor or control water supply, energy distribution, or telecommunications, or other elements of critical infrastructure. See Cybersecurity and Infrastructure Security Agency (CISA) for a list and definitions of Critical Infrastructure Sectors.[4]
- Employment and worker management systems (HR systems), such as tools used for recruitment, or resume/applicant screening; or systems used for internal employee work management, such as analysis of employee performance or behavior that could result in discipline or termination.
- Systems that are known to cause significant or irreversible environmental damage.[5]

Environmental Impact

The City is committed to the responsible use of technology to improve services and advance beneficial outcomes for both people and the environment. In alignment with our Climate Action Plan[6], the City will consider the environmental impacts related to the use of this technology with the benefits that have been demonstrated by it. Departments should work with vendors to understand the environmental impact of the AI solution in alignment with the City's Climate Action Plan prior to procurement or use.

Records Retention & Public Records

The City is subject to RCW 40.14, governing Preservation and Destruction of Public Records for state and local agencies, and RCW 42.56 (Washington State Public Records Act). City staff must follow the laws and current procedures and policies for records retention and disclosure.

Retention requirements are based on the content of the records, not their format. Regardless of the required retention period, if records responsive to a public disclosure request exist, they must be disclosed. When using an AI solution, departments must preserve or destroy records created when using AI products pursuant to the retention schedule and are responsible for searching for and retrieving them if a public disclosure request is received.

The City will work to improve transparency efforts and align our AI solution implementation with the City's data priorities, by evaluating and making information available on public-facing data portals when possible

IX. COMPLIANCE WITH THE AI POLICY

Applicability

If implementing a new technology (e.g., solutions, systems, software, hardware and networks), that technology may not go live unless it is in compliance with this Policy. Existing (legacy) technology must implement this Policy as part of any major upgrade.

---

[4] Cybersecurity & Infrastructure Security Agency (CISA), "Critical Infrastructure Sectors", 2023.
[5] White House Office of Management & Budget (OMB), "Advancing Governance Innovation and Risk Management for Agency Use of Artificial Intelligence: Safety-Impacting AI", 4/28/24.
[6] Seattle Office of Sustainability & Environment (OSE), "The 2013 Climate Action Plan (CAP)", 4/22/2013.

Exceptions

Exceptions to this policy must undergo a risk evaluation through an AI Review, as defined in policy section 8.2 above.

Non-Compliance

The Chief Technology Officer (CTO) is responsible for compliance with this policy. Enforcement may be imposed in coordination with individual division directors and department leaders. Non-compliance may result in disciplinary action, restriction of access, or more severe penalties up to and including termination of employment or vendor contract.

Promulgation

The CTO or their designee shall notify City departments when an update to this policy is released. Any updates to this policy will be communicated through standard protocol and process. This policy will be maintained within the Controlled Document Repository and other accessible SharePoint sites.

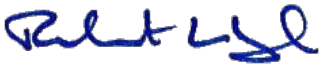
X. RELATED STANDARDS & POLICIES

Information Technology Security Policy (ITSP)	Generative AI Policy - POL-209
Acquisition of Technology Resources - STA-209	Data Classification Guideline - GUI-110
AI Acquisition & Operation Manual	Privacy Policy – POL-202
Responsible Use of AI Guideline	Washington State: Public Records Guideline
DHS: Generative AI Public Sector Playbook	The White House: Blueprint for an AI Bill of Rights
WS HB 1999: Fabricated Intimate or Sexually Explicit Images and Depictions	Federal Register: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
WA State Facial Recognition Law	

XI. DOCUMENT CONTROL

This policy shall be effective on 12/31/2024 and shall be reviewed at least every year.

Version	Content	Contributors	Approval Date
V1.1	Draft	Ginger Armbruster, Sarah Carrier, Keith Cooke, Rob Lloyd, Jim Loter	**12/31/2024**
V1.2	Final Draft	Ginger Armbruster, Sarah Carrier, Keith Cooke, Rob Lloyd	**3/12/2025**
V1.3	Absorbed Gen AI Policy	Keith Cooke, Rob Lloyd	**4/30/2025**
V1.4	**Final**	**Approved: Rob Lloyd** **Rob Lloyd – Chief Technology Officer**	**5/6/2025**



Acknowledgement

This Policy was based in-part on material developed through the coordinated efforts of over 140 state and local agencies in the GovAI Coalition, which is dedicated to the responsible use of AI. It was developed in partnership with the Community Technology Advisory Board (CTAB) and external subject matter experts from industry and academia.