Artificial Intelligence (AI) Policy

Scope: CITYWIDE

Policy Contact:
Information Technology Department
(916) 808-7111
itservicedesk@cityofsacramento.org

Table of Contents:

I. Purpose 2
II. Scope 2
III. Definitions 2
IV. Guiding Principles for Responsible AI Systems 3
V. Roles & Responsibilities 4
VI. Policy 5
A. AI Consideration 5
B. Use of AI and/or GenAI 6
C. Privacy Considerations for Public Safety Employees 6
VII. Prohibited Uses 6
VIII. Violations of the AI Policy 7
Charter Officer Review and Acknowledgement 8

Supersedes:
N/A - New

Reviewed/Effective:
01/09/2026

I. Purpose

This policy establishes a comprehensive, yet flexible, governance and management of Artificial Intelligence (AI) systems used by, or on behalf of, the City of Sacramento (City). This policy enables the City to use AI systems for the benefit of the City and community while safeguarding against potential harm.

The key objectives of the AI Policy are to:

A. Provide guidance that is clear, easy to follow, and supports decision-making for all end users who purchase, configure, develop, implement, maintain, operate, or use the City's AI systems.

B. Ensure that end users adhere to Section 4, Guiding Principles.

C. Define roles and responsibilities related to the usage of AI systems.

D. Establish and maintain processes to assess, manage, and mitigate risks presented by AI systems.

E. Align the governance of AI systems with existing data governance, security, and privacy measures in accordance with the City's Information Security Policy.

F. Define prohibited uses of AI systems.

G. Define how AI systems may be used for authorized City purposes in accordance with applicable local, state, and federal laws.

II. Scope

This policy applies to:

A. All systems with AI capabilities deployed by the City; and

B. End users.

III. Definitions

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

B. **Artificial Intelligence (AI)**: a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine-based and human-based inputs to:

1. Perceive real and virtual environments.

2. Abstract such perceptions into models through analysis in an automated

manner.

3. Use model inference to formulate options for information or action.

C. **Artificial Intelligence (AI) System**: Any system, software, sensor, or process that automatically generates outputs including, but not limited to, predictions, recommendations, or decisions that augment or replace human decision-making. This extends to software, hardware, algorithms, and data generated by these systems, used to automate large-scale processes or analyze large data sets.

D. **End Users**: City employees, administrators, contractors, consultants, vendors, volunteers, temporary agency employees, student interns, or any other person who uses or is provided access to Information Technology resources in accordance with this policy.

E. **Generative Artificial Intelligence (GenAI)**: A type of AI that is algorithmically trained on one or more large datasets and designed to generate new and unique data (e.g., text, pictures, video) in response to a prompt (generally questions, instructions, images, or video) input by the user.

F. **Human in the Loop**: The application of human oversight, intervention, or review throughout the various stages of an AI system's decision-making process. It provides for human oversight to ensure the AI's actions will align with desired outcomes and guiding principles for responsible use of AI.

IV. Guiding Principles for Responsible AI Systems

These principles describe the City's values regarding how AI systems are purchased, configured, developed, operated, implemented, or maintained.

A. **Human-Centered Design**: AI systems are developed and deployed with a human-centered approach that evaluates AI-powered services for their impact on the public.

B. **Security & Safety**: AI systems maintain confidentiality, integrity, and availability through safeguards that prevent unauthorized access and use. Implementation of AI systems is reliable and safe and minimizes risks to individuals, society, and the environment.

C. **Privacy**: Privacy is preserved in all AI systems by safeguarding personally identifiable information (PII) and sensitive data from unauthorized access, disclosure, and manipulation.

D. **Transparency**: The purpose and use of AI systems is proactively communicated and disclosed to the public. An AI system, its data sources, operational model, and policies that govern its use are understandable and documented.

E. **Equity**: AI systems are designed to ensure fair outcomes for everyone. Bias in AI systems is managed to minimize any potential harm to those affected by their use.

F. **Accountability**: Roles and responsibilities govern the deployment and maintenance of AI systems, and human oversight ensures adherence to relevant laws and regulations.

G. **Effectiveness**: AI systems are reliable, meet their objectives, and deliver precise and dependable outcomes for the utility and contexts in which they are deployed.

H. **Workforce Empowerment**: End users are empowered to use AI in their roles through education, training, and collaborations that promote participation and opportunity.

V. Roles & Responsibilities

Several roles are responsible for enforcing this policy, as outlined below.

A. **Chief Information Officer (CIO)** is responsible for:

1. Directing City technology resources, policies, projects, and services, and coordinating the same with other City departments.
2. Designating the Information Security Officer (ISO) to actively ensure AI systems are used in accordance with the Information Security Policy.
3. Designating the Artificial Intelligence Officer (AIO) to actively ensure AI systems are used in accordance with this policy and the Information Security Policy.
4. Updating this policy as needed.
5. Performing such other duties necessary to implement this policy.

B. **Information Security Officer (ISO)** is responsible for overseeing the enterprise cybersecurity infrastructure, cybersecurity operations, and updating information security policies, procedures, standards, and guidelines.

C. **The Artificial Intelligence Officer (AIO)** is responsible for:

1. Overseeing the enterprise digital privacy practices, data processing practices, and responsible usage of technology in compliance with this policy; and monitoring policy compliance.
2. Overseeing the privacy practices of AI systems used by or on behalf of City departments.
3. Coordinating the review of AI systems.

D. **Charter Officers and Department Directors** are responsible for:

1. Ensuring that their respective departments engage the AIO before seeking to procure new technology and data initiatives that involve an AI system.

2. Ensuring that end users within their respective departments receive and review this policy through the City's Learning Management System (LMS).

E. **The City Attorney's Office** is responsible for advising of any legal issues or risks associated with AI systems usage by or on behalf of City departments.

VI. Policy

A. **AI Consideration**

When purchasing, configuring, developing, operating, implementing, or maintaining AI systems, the City will:

1. Uphold Section 4, Guiding Principles for Responsible AI Systems.

2. Follow Procurement of Goods for items requiring IT Department review in procuring and implementing AI systems and solutions.

3. Conduct an AI Review to assess the potential risk(s) of AI systems.

4. Ensure all content generated by Generative AI is reviewed by a human to ensure accuracy and eliminate bias prior to being used, also known as "human in the loop."

5. Obtain technical documentation about AI systems.

6. In the event of a cybersecurity incident involving the use of the AI system, the City will follow an established incident response procedures. The ISO is responsible for overseeing the cybersecurity practices of AI systems used by or on behalf of the City.

7. Consistent with its obligations under the Meyers-Milias-Brown Act (MMBA), the City shall endeavor to provide notice to Recognized Employee Organizations (REOs) of the introduction of new AI technologies that the City reasonably anticipates may have more than a de minimis impact on employees' working conditions. Upon request, the City shall meet and confer regarding such impacts. Failure to provide prior notice shall not preclude the REO from requesting to meet and confer upon learning of such implementation. Nothing in this provision shall be construed to limit the City's authority under applicable MOU City Rights articles or other provisions of law.

B. **Use of AI and/or GenAI**

The use of AI and/or GenAI systems by end users shall be limited to official work-related purposes, and end users shall only access and use GenAI systems for which they have been authorized and received proper training.

Any function carried out by an end user using AI and/or GenAI is subject to the same laws, rules, and policies as if carried out without the use of AI and/or GenAI. The use of AI and/or GenAI does not permit any law, rule, or policy to be bypassed or ignored.

End users shall use AI-generated content as an informational tool and not as a substitute for human judgment or decision-making. End users shall not represent AI-generated content as their own original work.

AI-generated content is considered draft material only and shall be thoroughly reviewed prior to use. Before relying on AI-generated content, end users should:

1. Obtain independent sources for information provided by AI and/or GenAI and take reasonable steps to verify that the facts and sources provided by AI and/or GenAI are correct and reliable.

2. Review prompts and output for indications of bias and discrimination and take steps to mitigate its inclusion when reasonably practicable.

C. **Privacy Considerations for Public Safety Employees**

Information not otherwise available to the public, including data reasonably likely to compromise an investigation, reveal confidential law enforcement techniques, training, or procedures, or risk the safety of any individual if it were to become publicly accessible, confidential medical or patient information shall not be input into a GenAI system unless contractual safeguards are in place to prevent such information from becoming publicly accessible. End users should instead use generic unidentifiable inputs, such as “suspect,” “victim,” or “patient” and hypothetical scenarios whenever possible.

Protected information shall only be input into GenAI systems that have been approved for such use and comply with applicable privacy laws and standards.

VII. Prohibited Uses

A. AI Systems and IT resources may not be used to violate laws, policies, or contracts. End users may not use AI tools or services to generate content that enables harassment, threats, defamation, hostile environments, stalking, or discrimination.

B. If an employee becomes aware that an AI system is malfunctioning or producing inaccurate, misleading, discriminatory, or disruptive results (e.g., generating errors

in communication, calculations, or decision-making), they must promptly report the issue to their supervisor and the CIO.

C. Current employees and external job candidates are prohibited from utilizing AI to assist them with answering job interview questions. Utilizing AI for this purpose may result in the job candidate being disqualified from the recruitment.

D. End users shall not use AI and/or GenAI systems to rationalize a law enforcement decision, or as the sole basis of research, interpretation, or analysis of the law or facts related to a law enforcement contact or investigation.

E. End users are prohibited from inputting work-related data, including information learned solely in the scope of their employment with the City, into publicly available AI and GenAI systems. This restriction applies unless the system has been approved by the CIO or an authorized designee for the intended use. This policy is in place to ensure data security and compliance with City policies.

VIII. Violations of the AI Policy

A. City employees and volunteers who violate this policy may be subject to disciplinary action, up to and including termination of employment.

B. Contractors or vendors who violate this policy may be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the City.

City of SACRAMENTO

Charter Officer Review and Acknowledgement

ARTIFICIAL INTELLIGENCE POLICY

(Signature by all Charter Officers is not a requirement for policy adoption)

Maraskeshia Smith

Maraskeshia Smith (Jan 14, 2026 19:26:31 PST)

City Manager 01/14/2026

Gus Martinez (Jan 9, 2026 11:28:37 PST)

City Attorney 01/09/2026

City Clerk 01/12/2026

City Treasurer 01/09/2026

City Auditor 01/20/2026