Artificial Intelligence (AI) Policy

[Agency]

I. Purpose

This policy establishes a comprehensive, yet flexible, governance structure for AI systems used by, or on behalf of, the [Agency]. This policy enables the [Agency] to use AI systems for the benefit of the community while safeguarding against potential harms.

The key objectives of the AI Policy are to:

- Provide guidance that is clear, easy to follow, and supports decision-making for the staff (full-time, part-time), interns, consultants, contractors, partners, and volunteers who may be purchasing, configuring, developing, operating, or maintaining the [Agency's] AI systems or leveraging AI systems to provide services to the [Agency].
- Ensure that when using AI systems, the [Agency] or those operating on its behalf, adhere to the Guiding Principles that represent values with regards to how AI systems are purchased, configured, developed, operated, or maintained.
- Define roles and responsibilities related to the [Agency's] usage of AI systems.
- Establish and maintain processes to assess and manage risks and values presented by AI systems used by the [Agency];
- Align the governance of AI systems with existing data governance, security, and privacy measures in accordance with the [Agency's Information Security Policy] and [Agency's Data Governance Policy].
- Define prohibited uses of AI systems;
- Establish "sunset" procedures to safely retire AI systems that no longer meet the needs of the [Agency];
- Define how AI systems may be used for legitimate [Agency] purposes in accordance with applicable local, state, and federal laws, and existing agency policies.

The [Agency] defines "artificial intelligence" or "AI" to be a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.[1] AI systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate

[1] Definition from 15 U.S.C. 9401(3).

options for information or action.

The [Agency] defines an “AI system” to be any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

The [Agency’s] AI systems and the data contained therein will be purchased, configured, developed, operated, and maintained using the [Agency’s] [AI Governance Manual, or applicable handbook].

II. Scope

This policy applies to:

1. All AI systems deployed by the [Agency] or on the [Agency’s] behalf; and

2. Staff (full-time, part-time), interns, consultants, contractors, partners, and volunteers who may be purchasing, configuring, developing, operating, or maintaining the [Agency’s] AI systems or who may be leveraging AI systems to provide services to the [Agency].

III. Guiding Principles for Responsible AI Systems

These principles describe the [Agency’s] values with regards to how AI systems are purchased, configured, developed, operated, or maintained.

1. **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.

2. **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.

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

4. **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.

5. **Equity:** AI systems support equitable outcomes for everyone. Bias in AI systems is effectively managed with the intention of reducing harm for anyone impacted by its use.

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

regulations.

7. **Effectiveness:** AI systems are reliable, meet their objectives, and deliver precise and dependable outcomes for the utility and contexts in which they are deployed.
8. **Workforce Empowerment:** Staff are empowered to use AI in their roles through education, training, and collaborations that promote participation and opportunity.

IV. Roles & Responsibilities

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

- The [Chief Information Officer (CIO), or equivalent] is responsible for directing [Agency] technology resources, policies, projects, services, and coordinating the same with other [Agency] departments. The [CIO, or equivalent] shall designate the [Chief Information Security Officer (CISO), or equivalent] to actively ensure AI systems are used in accordance with the [Agency Information and System Security Policy, or applicable policy]. The [CIO, or equivalent] shall also designate the [Chief AI Officer (CAIO), or equivalent].
- The [CAIO, or equivalent] is responsible for ensuring that the [Agency's] use of AI systems is done so in accordance with this policy and the [other related Agency policy].
- The [CISO, or equivalent] is responsible for overseeing the enterprise security infrastructure, cybersecurity operations, updating security policies, procedures, standards, guidelines, and monitoring policy compliance.
- The [Chief Privacy Officer (CPO), or equivalent] is responsible for overseeing the enterprise digital privacy practices, data processing practices, and responsible usage of technology in compliance with the [Agency Privacy Policy, or applicable policy].
- [Agency] departments are responsible for following this policy and following updates to this policy and the [AI Governance Manual, or applicable policy], and shall check compliance with these documents at least annually.
- The [CIO or designee, or equivalent] shall notify [Agency] departments when an update to this policy or the [AI Governance Manual, or applicable policy] is released.
- The [Attorney's Office, or equivalent] is responsible for advising of any legal issues or risks associated with AI systems usage by or on behalf of [Agency] departments.
- The [Executive Office or designee, or equivalent] may, at its discretion, inspect the usage of AI systems and require a department to alter or cease its usage of AI

systems or a partner's usage of AI systems on behalf of the department.

- The [Finance Department – Purchasing Office, or equivalent] is responsible for overseeing the procurement of AI systems in alignment with existing IT procurement and governance processes and requiring vendors to comply with [Agency] policy standards through contractual agreements.

V. Policy

When purchasing, configuring, developing, operating, or maintaining AI systems, the [Agency] will:

1. Uphold the Guiding Principles for Responsible AI Systems;

2. Conduct an AI Review to assess the potential risk of AI systems. The [CAIO, or equivalent] is responsible for coordinating review of AI systems used by the [Agency] as detailed in the [AI Governance Manual, or applicable policy];

3. Obtain technical documentation about AI systems using the AI FactSheet or create equivalent documentation if internally developing the AI system. The [Finance Department, Purchasing Office, or equivalent] is responsible for requiring vendors to complete the AI FactSheet;

4. Require contractors to comply with the [Requirements for AI Systems, or applicable legal addendum] overseen by the [Finance Department, Purchasing Office or equivalent]; and

5. In the event of an incident involving the use of the AI system, the [Agency] will follow an Incident Response Plan as detailed in the [AI Incident Response Plan, or equivalent]. The [CISO, or equivalent] is responsible for overseeing the security practices of AI systems used by or on behalf of [Agency] departments.

Prohibited Uses

The use of certain AI systems is prohibited due to the sensitive nature of the information processed and severe potential risk. This includes the following prohibited purposes:

- [Real-time and covert biometric identification.]

- Classification of human facial or body movements into certain emotions or sentiment with the use of computer vision techniques or emotion analysis. (e.g., positive, negative, neutral, happy, angry, nervous).]

- [Fully automated decisions that do not require any meaningful human oversight but substantially impact individuals.]

- [Social scoring, or the use of AI systems to track and classify individuals based on their behaviors, socioeconomic status, or personal characteristics.]

- [Cognitive behavioral manipulation of people or specific vulnerable groups.]
- [Autonomous weapons systems.]

If [Agency] staff become aware of an instance where an AI system has caused harm, staff must report the instance to their supervisor and the [CAIO, or equivalent].

Sunset Procedures
If an AI system operated by the [Agency] or on its behalf ceases to provide a positive utility to the [Agency's] residents as determined by the [CAIO, or equivalent], then the use of that AI system must be halted unless express exception is provided by the [City Manager or City Council, or equivalents]. If the abrupt cessation of the use of that AI system would significantly disrupt the delivery of [Agency] services, usage of the AI system shall be gradually phased out over time.

Public Records
The [Agency] is subject to the [applicable public records act policy]. [Agency] staff must follow all current procedures for records retention and disclosure.

Policy Enforcement
All employees and agents of the [Agency], whether permanent or temporary, interns, volunteers, contractors, consultants, vendors, and other third parties operating AI systems on behalf of the [Agency] are required to abide by this Policy and the associated [AI Governance Manual, or applicable policy].

VI. Violations of the AI Policy

Violations of any section of the AI Policy, including failure to comply with the [Agency's] [AI Governance Manual, or applicable handbook], may be subject to disciplinary action, up to and including termination. Violations made by a third party while operating an AI system on behalf of the [Agency] may result in a breach of contract and/or pursuit of damages. Infractions that violate local, state, federal or international law may be remanded to the proper authorities.

VII. Exceptions (optional)

Staff, as described in the scope of this policy, must adhere to all controls outlined in this policy document unless a specific documented exception is explicitly granted by [CAIO, or equivalent]. Policy violations that have not been formally documented as an exception will be treated as a security incident in accordance with [Agency] policy. [Agency] staff or Departments may encounter emergency situations that necessitate the immediate use of AI tools or technologies. In these circumstances, each incident use case must obtain documented approval via the [Department Director, or equivalent] prior to use. In such situations, the [Department, staff or equivalent] must submit the [Department] approved use case to the [CAIO, or equivalent] for review within [30 days, or other duration] of the incident.

Restricted Platform Alternatives (optional)
In the event that the [Agency] restricts access to certain AI platforms, whenever practicable, the [Agency] will provide a URL redirect to a [Agency intranet website] that will provide the employee with alternative AI platforms which have been vetted and approved by the [Agency] for use.

The purpose of this policy is to help prevent the exfiltration of [Agency] data to personal devices which would violate [Agency Acceptable Use Policies, Privacy Policy, Information Security Policy]. This approach allows employees to choose amongst various platforms which meet applicable privacy and security standards established by the [Agency] to facilitate productivity.

The [CISO, or equivalent] will designate a department to perform regular assessments of AI platforms and to regularly monitor such platforms so that the [Agency] can restrict and remove access in the event of a security or privacy incident.

VIII. Terms & Definitions

Artificial Intelligence: “Artificial intelligence” or “AI” to be a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

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

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.

Additional terms and definitions are provided in the AI Governance Manual.

IX. Acknowledgement

This policy was developed through the coordinated efforts of thousands in the GovAI Coalition who empower governments to leverage AI for the public good.

Approved:

______________________________ ______________________

[Chief Information Officer or
equivalent]

Date

Approved for posting:

______________________________ ______________________

[Director of Employee Relations
Director of Human Resources, or
equivalents]

Date