Policy Title: **Artificial Intelligence Policy**
Date Adopted: **May 16, 2024**

1. Purpose

Regional Government Services (RGS) recognizes that Artificial Intelligence (AI) tools can enhance service quality and operational efficiency. This policy establishes a framework guiding the ethical and responsible use of AI systems by, or on behalf of, RGS. It enables RGS to use AI systems to benefit employees and clients while safeguarding against potential harm.

2. Policy

RGS recognizes the value of AI tools that through thoughtful application can significantly benefit our agency, our clients, and the communities they serve. We are equally mindful of the risks and challenges associated with AI and the potential for unintended consequences. Our goal is to understand AI systems and tools, their ethical and equitable use, and manage associated risks. Our approach to AI adoption is a careful balance between innovation and caution.

This policy encompasses all employees, contractors, and partners of RGS. It covers the use of existing and future AI tools, systems, and platforms, including but not limited to Large Language Models (LLMs), AI-powered plug-ins, and data-driven analytical tools. The scope extends to all operational and decision-making processes within RGS where AI technologies are utilized, ensuring our approach to AI remains human-centered, adaptive, and forward-thinking.

When operating, configuring, purchasing, developing, or maintaining AI systems, RGS will:

- Uphold this AI policy and any other related AI policies and procedures. RGS uses AI to provide comprehensive insights, predictive analysis, and streamlined processes, while human expertise ensures that final decisions are made with compassion, ethical consideration, and a deep understanding of the internal and external communities we serve. RGS will also adhere to all relevant legal frameworks governing AI, including data protection, privacy, and intellectual property laws. Our policy mandates continuous monitoring of the legal landscape to ensure compliance with both local and international AI regulations, safeguarding against legal and ethical risks.

- Conduct AI tool/system reviews to assess potential risk. RGS is committed to utilizing AI responsibly, preventing harm and avoiding facilitation of malicious activities. RGS will provide clear information about how AI is being used within our organization, the data it processes, and the decision-making frameworks it supports.

- Obtain technical documentation about AI tools/systems in use.

- Require AI contractors to comply with established requirements. RGS requires adherence to ethical and legal standards from all third-party AI providers and systems

to safeguard the integrity and respect for individual rights in AI-related activities.

- Follow an Incident Response Plan in the event of an AI tool/system incident.

3. Prohibited Uses

The use of certain AI systems or specific activities using AI systems are prohibited due to the sensitive nature of the information processed and severe potential risk. When using AI systems, RGS employees, contractors and business partners may not:

- Enter or otherwise share personal, confidential or individually identifying health information.

- Use real-time and covert biometric identification or falsification (e.g., facial recognition, voice identification or simulation).

- Use emotion analysis.

- Enable fully automated decisions that do not include meaningful human oversight and substantially impact individuals' legal rights, financial status, employment opportunities, workplace accommodation, disciplinary status, access to essential services, health, safety, or privacy.

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

- Engage in cognitive behavioral manipulation of people.

4. AI-Related Definitions

Artificial Intelligence: "Artificial intelligence" or "AI" is any 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.

Cognitive behavioral manipulation of people or specific vulnerable groups: Cognitive behavioral

manipulation refers to AI-driven tools or algorithms designed to influence or alter an individual's decision-making process or belief system. These systems use psychological, behavioral, or emotional data to create targeted strategies that can manipulate thoughts, feelings, or actions, particularly focusing on vulnerable groups or individuals.

Emotion analysis: Computer vision techniques to classify human facial expressions and body language to infer emotions or sentiment (e.g., positive, negative, neutral, happy, angry, nervous).

Personal and medical identifying information: Personal identifying information includes data that identifies an individual personally, such as name, address, email address, social security number, passport number, driver's license number, financial information, and telephone number. Individually identifiable health information includes data related to an individual's physical or mental health condition, provision of health care, or payment for the provision of healthcare that can be linked to a specific individual. This includes medical records, health insurance information, laboratory test results, medical history, and other individually identifiable data collected during the provision of healthcare services.

Real-time and covert biometric identification: The live identification of an individual using technologies including, but not limited to, facial recognition and iris scanning, without that individual's knowledge or meaningful consent.

Social scoring: The use of AI systems to track and classify individuals based on their behaviors, socioeconomic status, or personal characteristics. Refers to artificial intelligence or algorithmic systems that aggregate and interpret an individual's personal data to assign a quantifiable score or rating that ranks them against other individuals and impacts their access to services, opportunities, or societal privileges. These systems are characterized by their use of data related to behavior, preferences, interactions, financial transactions, and other personal attributes which are not directly linked to the application of the score. They can be part of a comprehensive profile that is used to make significant decisions about an individual's rights, opportunities, or social standing.

5. **Responsibilities of Users**

All RGS employees are responsible for following this policy, as well as any other RGS AI-related policies or procedures.

- RGS employees must notify their supervisor when they are using AI tools or systems for work. Supervisors are responsible for ensuring that staff are properly trained to both use the AI tool and to assess and mitigate potential negative consequences.

- If RGS staff become aware of an instance where an AI system has caused harm, staff must report the instance to both their supervisor and the designated RGS administrative staff member. If RGS employees are harmed, staff must also notify RGS' Human Resources Manager.

- If an AI system operated by RGS or on its behalf ceases to provide a positive utility to RGS' employees, clients, and/or client community, then the use of that AI system must be discontinued. If the abrupt cessation of the AI system would significantly disrupt service delivery, usage of the AI system shall be phased out.

- RGS is subject to the California Public Records Act (CPRA). RGS staff must follow all current procedures for records retention and disclosure of any records associated with AI systems.

- Appropriate remedial measures and corrective action, including termination, will be instituted if prohibited behavior or violations of this policy are found.

6. <u>Oversight Roles</u>

RGS' Executive Director will designate a member of administrative management to develop and enforce such procedures or practices as are needed to:

- Ensure AI systems are used in accordance with this policy and any other RGS policies and procedures.

- Oversee AI enterprise security infrastructure, cybersecurity operations, updating security policies, procedures, standards, guidelines, and policy compliance.

- Notify RGS departments when an update to this policy or any other RGS AI policies or procedures are released.

- Oversee the procurement of AI systems and require vendors to comply with RGS organizational values and policy standards through contractual agreements.

- Consult with RGS' Legal Counsel as needed regarding any legal issues or risks associated with RGS AI systems usage.

- At their discretion, inspect the usage of AI systems and require a department/service line to alter or cease its usage of AI systems or a partner's usage of AI systems on behalf of the department/service line.