**Board Administration Policy**

# Artificial Intelligence Policy

## I. Purpose

A. To establish a framework for the development, acquisition, use, and oversight of Artificial Intelligence (AI) systems within SJCERA. This includes defining acceptable use, mitigating risks, protecting data privacy and member interests, and ensuring alignment with legal, regulatory, and ethical standards. The Policy also seeks to promote transparency, accountability, and trust in SJCERA's use of AI technologies.

## II. Objective

A. To be responsible and ethical in the use of AI technologies to enhance service delivery, strengthen administrative efficiency, and safeguard member data. As AI capabilities continue to evolve, it is essential that their deployment aligns with SJCERA mission, vision, and values, including transparency, accuracy, security, and service excellence. This Policy establishes guiding principles to ensure AI is implemented in a manner that is lawful, equitable, explainable, and respectful of the public trust.

## III. Provisions

A. Scope

1. This Policy applies to all employees, both direct and county, contractors, and third-party service providers who develop, deploy, manage, or interact with AI tools and systems used by or on behalf of SJCERA.

B. Roles and Responsibilities

1. Executive Leadership:

   i. Provide strategic direction and ensure AI initiatives align with organizational goals.

   ii. Oversee risk management processes related to AI deployment and development.

   iii. Foster a culture of responsible AI innovation by promoting awareness, education, and collaboration across the organization.

   iv. Develop and maintain the AI Policy, risk management processes, and governance frameworks.

   v. Review and approve AI use cases, ensuring alignment with ethical and security considerations.

   vi. Ensure periodic assessments of AI systems and their impact on organizational objectives and relevant stakeholders.

2. Information Technology:

i. Design and implement AI systems in accordance with risk management and ethical principles.

ii. Document AI methodologies to ensure transparency and explainability.

iii. Regularly test AI models to prevent bias, inaccuracies, or unintended consequences.

iv. Implement security controls to protect AI systems and the data they process.

v. Assess third-party AI tools and services for adherence to security and privacy policies.

vi. Educate employees on responsible AI use and data protection practices.

3. Legal:

   i. Ensure AI systems comply with data governance policies, applicable regulations, and ethical standards.

   ii. Conduct assessments and evaluations to verify alignment with internal policies and external legal requirements.

   iii. Monitor AI-related legal and ethical risks, providing guidance to ensure responsible and lawful AI use.

4. Users:

   i. Use AI responsibly in compliance with AI Guidelines.

   ii. Validate AI-generated outputs before applying them to decisions or operations.

   iii. Report any potential risks, biases, or unintended impacts observed in AI tools to a member of the Executive Team

   iv. .

   v. Only use approved AI tools.

C. Definitions

1. Artificial Intelligence (AI): A broad category of technologies that enables machines to perform tasks that typically require human intelligence, such as learning, reasoning, problem-solving, and decision-making.

2. AI Tools: Applications that use AI capabilities to support general employee productivity and efficiency, such as analyzing data or generating content, often used in daily activities.

3. AI Systems: Integrated AI-driven solutions, which are internally developed or externally procured, that operate within SJCERA's

technology infrastructure to support SJCERA operations, enhance decision-making, or provide services.

4. Confidential Information: Includes but is not limited to member or employee Personally Identifiable Information, medical records, or personal data, business and financial records, personnel files, proprietary SJCERA information, and any data classified as confidential under applicable laws and SJCERA policies.

5. Personally Identifiable Information (PII): Refers to information that can be used to identify an individual, such as name, address, SSN, financial data, or health information.

## IV. Principles

A. Responsible Use

1. AI technologies shall only be used for work-related purposes related to SJCERA operations and mission.

2. Using AI to engage in any form of illegal, unethical, or harmful activity is strictly prohibited.

3. AI shall not be used in ways that result in discriminatory, biased, or unfair treatment of individuals or groups.

B. Privacy, Confidentiality, and Security

1. AI systems shall only use data collected and maintained in compliance with applicable data protection regulations and internal security policies.

2. AI systems may only process PII or Confidential Information when authorized, necessary, and in compliance with applicable data protection laws and internal controls.

3. AI must not compromise the confidentiality, integrity, or availability of SJCERA or member data.

C. Human Oversight and Accountability

1. All AI outputs used to inform decisions affecting members or staff must be reviewed by authorized personnel.

2. AI shall not be used to make final eligibility or benefits determinations without human review and oversight.

3. Staff must ensure the factual accuracy of all AI content they produce or publish and must not create or share false or misleading information using AI systems.

D. Transparency and Explainability

1. SJCERA shall maintain documentation that explains the purpose, logic, and outcomes of AI systems, to the extent possible and appropriate.

2. Members have the right to know when AI is used in interactions that affect them and to request clarification or human review.

E. Risk Management

1. Prior to adoption, all AI technologies shall undergo a risk assessment to evaluate potential legal, ethical, operational, and reputational impacts.

2. AI systems shall be regularly evaluated for accuracy, fairness, and unintended consequences.

3. Risk assessments of AI systems must be performed, documented, and retained for audit purposes.

F. Procurement and Vendor Requirements

1. Third-party vendors supplying AI capabilities must meet SJCERA's standards for privacy, security, and ethical AI practices.

2. Contracts must include provisions for audit rights, transparency, and system explainability.

3. AI vendors must disclose whether their models were trained on copyrighted or sensitive data.

G. Ethical Considerations

1. AI shall not be used in ways that result in discriminatory, biased, or unfair treatment of individuals or groups.

2. Staff shall review any input to, and outputs from, AI systems for potential biases.

H. Intellectual Property

1. Staff shall respect copyright, trademark, and intellectual property rights when using AI systems.

2. For any questions or concerns about potential copyright infringement, contact the Legal Division.

## V. AI System Development and Integration

A. When developing or integrating AI systems:

1. Adopt a Risk-Based Approach: Employees must integrate a risk management process aligned with the NIST AI Risk Management Framework (AI RMF), ensuring early and continuous identification, assessment, and mitigation of risks related to safety, fairness, reliability, and operational impact.

2. Ensure Cross-Disciplinary Collaboration: SJCERA must establish and maintain collaboration between technical teams, legal counsel, and subject matter experts to ensure AI systems are developed with a comprehensive understanding of both technical performance and member impact.

3. Prioritize Resilience: Employees must design AI systems with built-in safeguards, robust testing protocols, and continuous monitoring mechanisms to ensure reliable and secure performance as technologies and conditions evolve.

4. Maintain Flexibility: SJCERA must implement modular, adaptable AI system architectures that support efficient updates and integration of future innovations without requiring full system replacements.

## VI. Compliance and Enforcement

A. AI System Development and Integration

1. Violations of this Policy may result in administrative and disciplinary action, up to and including contract termination or termination of employment.

## VII. Law Prevails

A. In the event a conflict between this Policy and the County Employees Retirement Law, the Public Employees' Pension Reform Act, or other applicable state or federal law arises, the law shall prevail.

## VIII. Policy Review

A. Staff shall review this Policy at least once every three years to ensure that it remains relevant, appropriate, and in compliance. Any revisions or amendments to this Policy must be approved by the Board in accordance with the bylaws.

## IX. History

12/12/2025 Policy adopted by the Board

**Certification of Board Adoption:**

12/12/2025

Clerk of the Board Date