

**BOARD OF RETIREMENT**

**POLICY FOR THE USE AND DEPLOYMENT  
OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES**

**Purpose and Scope:**

Artificial Intelligence is rapidly developing and will inevitably be utilized by SamCERA and its contractors, consultants, and vendors in a multitude of capacities including, but not limited to, member services, investment management, and administrative operations. The use and deployment of AI will significantly affect the administration of retirement systems and their investment of funds, likely creating efficiencies and enhancing decision-making but also raising issues of privacy, ethics, and accountability.

Pursuant to Article XVI, Section 17 of the California Constitution, the Board retains sole and exclusive fiduciary responsibility for the assets and administration of the retirement system. Use of AI must be consistent with this duty and this policy therefore establishes the Board's guiding principles for the adoption, oversight, and governance of AI. The purpose of this Policy is to ensure that SamCERA's use of AI is responsible, secure, and ethical. This Policy will be reviewed annually and updated as technology, applicable law, and industry best practices evolve.

This Policy applies to all SamCERA officials and employees as well as to SamCERA's contractors, vendors, and consultants, and any other parties providing services or working on SamCERA's computer or network systems, or otherwise handling any SamCERA information. This Policy applies to all SamCERA – owned or operated systems, devices, and networks, and to any use of AI in connection with SamCERA business, regardless of platform or device.

**Definitions:**

For the purposes of this policy, the terms below have the following definitions:

Artificial Intelligence ("AI") - Machines or computer systems capable of performing tasks that typically require human intelligence. These tasks include reasoning, learning, perception, and natural language understanding.

AI Agent - An autonomous entity that perceives its environment through sensors and acts upon that environment using actuators to achieve specific goals. AI agents can range from simple programs to complex systems that interact intelligently with humans and environments.

Generative Artificial Intelligence ("Generative AI" or "GenAI") – A subset of AI that uses algorithms or models to create novel content such as text, images, videos, or other media based on patterns learned from training data. It generates new outputs rather than just analyzing or classifying data.

Large Language Model (“LLM”) – A foundation model in AI that is trained on massive datasets of text to understand and generate human-like language. LLMs like OpenAI’s GPT (Generative Pre-Trained Transformer) can perform diverse language tasks including generation, summarization, conversation, and more.

Confidential Information – Information that is not publicly available and that is possessed by SamCERA or concerns SamCERA’s business operations. Such information may be oral, written, or electronic and includes, but is not limited to, the following:

1. Member Records & Sworn Statements: Cal. Gov’t Code § 31532 specifically provides that, “Sworn statements and individual records of members shall be confidential and shall not be disclosed to anyone except insofar as may be necessary for the administration of this chapter or upon order of a court of competent jurisdiction, or upon written authorization by the member.”
2. Personally Identifiable information (“PII”): PII refers to any information that can be used on its own, or combined with other data, to distinguish or trace an individual’s identity. This includes, but is not limited to, common identifiers such as first or last names, dates of birth, Social Security numbers, street addresses, email addresses, and member records.
3. Protected Health information (PHI): PHI refers to individually identifiable information that relates to a person’s health condition, treatment, or payment for care (including health insurance information). Per HIPAA’s Privacy Rule, PHI includes information of persons who are living or who have been deceased for less than 50 years. PHI does not include health information about an employee that is held in SamCERA’s employment records in its role as an employer, or SamCERA’s member records in its role as a retirement plan administrator; nonetheless, such information is private and should be protected.
4. Security Information: Information required to access other Confidential Information, or SamCERA’s assets, such as SamCERA operations, systems architecture and applications, and facilities.
5. Proprietary Information: Information that is considered an asset to SamCERA that requires protection from unauthorized access to preserve its value, such as proprietary or confidential financial information regarding SamCERA’s investments and investment managers that is protected from disclosure under the law.
6. Privileged Information and Information Exempt from Disclosure under the Public Records Act: Information that SamCERA is allowed or required by law to protect from disclosure, including, but not limited to, attorney-client communications and attorney work product, pending litigation and claims, personnel records, drafts, information

showing the deliberative process (which would expose an agency's decision making process in such a way as to discourage candid discussion within the agency and thereby undermine the agency's ability to perform its functions), and official information (disclosure of which is against the public interest, due to the necessity for preserving the confidentiality of the information outweighing the necessity for disclosure in the interest of justice).

## **Guiding Principles:**

### **Data Privacy and Security**

Staff shall ensure that Confidential Information is not entered into any open or unsecured AI systems and may not be utilized by any SamCERA service providers to train their LLMs or operate their AI systems. When necessary, Confidential Information may be used in closed, secure AI systems procured by SamCERA or its vendors, and approved by the CEO in consultation with appropriate staff, that satisfy SamCERA's cybersecurity and vendor risk management standards. Security assessments must be conducted before deployment of any AI tool to ensure that Confidential Information is not exposed or otherwise likely to enter the public domain. AI must be used in compliance with all statutory confidentiality requirements including, but not limited to, Cal. Gov. Code § 31532, which protects the confidentiality of member and beneficiary records. AI must also be used in compliance with all existing policies and best practices, including SamCERA's internal practices regarding separation of information, such as firewalls and ethical walls.

### **Ethical Foundations and Accountability**

AI may be used to assist SamCERA officials and employees but may never displace the fundamental judgment of the Board or its staff. All AI deployments must be consistent with ethical standards of honesty, fairness, and avoidance of conflicts of interest. The ultimate responsibility for decisions rests with people, not machines and SamCERA personnel remain accountable for any action taken with the assistance of AI. Particular attention must be paid to address the potential for bias or disparate impact on members and beneficiaries, as well as inaccurate, misleading, or fabricated content (known as "hallucinations"). Where AI is used to support decisions relating to benefits eligibility, disability determinations, investments, finance, or other SamCERA operations, a human reviewer must confirm and be responsible for the output before any action is finalized.

### **Transparency**

Staff must ensure that AI tools used in member service, benefit determination, investment analysis, or administrative operations are explainable and auditable. Outputs should be capable of being reviewed and understood by non-technical decision-makers, so that neither staff nor the Board are asked to rely on "black box" recommendations without context. If members interact directly with AI Agents, such as chatbots or automated responses, they must be informed that they are communicating with AI and given the option of speaking with a human representative.

### Procurement and Contracting Standards

Contracts with third-party service providers that utilize AI in their business operations should include explicit provisions requiring compliance with this policy (including, but not limited to, its data privacy and security principles) and all applicable laws. Consistent with SamCERA's procurement policies, contracts for the provision of AI services to SamCERA must provide audit rights, reporting obligations, performance standards, and termination provisions in the event of non-compliance.

### Compliance with Laws and Regulations

All users of AI must comply with applicable laws, regulations, and ethical guidelines governing intellectual property, data security, and privacy.

### Training

Staff using AI tools must receive training to understand both the capabilities and limitations of the AI technologies that they utilize or oversee, and also to ensure compliance with the principles set forth in this Policy. The CEO will ensure periodic educational sessions for the Board so trustees remain informed about developments in AI and its relevance to pension administration and investment management.