POLICY NO. 021

PURPOSE:

To provide guidelines for the appropriate use, access, ~~and~~ disclosure, and protection of Personally Identifiable Information ("PII") in SBCERA's possession related to members, beneficiaries and other related persons of record; members of the public; SBCERA employees and Board of Retirement trustees; and participating employers.

BACKGROUND:

PII means information in any format that could reasonably be used to identify a person, including, but not limited to, name, address, e-mail address, Social Security number, birth date, or any other combination of information, including personnel, medical, financial, or similar files protected by the right to privacy under applicable law.

Certain PII may be considered "Sensitive PII," which is information that, if disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, such as Social Security numbers, financial account information, or medical information.

The policy is intended to strike an appropriate balance between the objectives of open government and the protection of the privacy rights of individuals.

GUIDELINES:

~~There are a number of~~ Federal and California laws ~~that~~ addressing privacy and security ~~issues that~~ significantly impact SBCERA's handling of PII. In the absence of any provision of applicable law to the contrary, SBCERA employees ~~must~~ shall handle PII in accordance with the following guidelines. SBCERA Legal Services shall be consulted ~~in the~~when ~~determination~~ determining ~~of~~ whether to disclose or withhold PII based ~~upon the application of~~on these guidelines and ~~state and federal~~applicable law.

1. PII shall not be disclosed to any~~one~~ person or entity ~~for any reason~~ unless: there is ~~a~~ written authorization ~~by~~ from the individual whose privacy interest is at stake; SBCERA receives an order of a court of competent jurisdiction; the disclosure is required under the California Public Records Act; or the disclosure ~~or it~~ is necessary for the administration of the system, including but not limited to benefit administration, member services, compliance with legal obligations, or any other authorized operational function.

   Access to and use of PII shall be limited to the minimum amount necessary to perform assigned job duties or fulfill a legitimate business purpose.

~~1.~~

2. All SBCERA vendors, partner agencies, or other third parties~~, subject to contractual terms~~, who may have access to or are exposed to PII maintained by SBCERA~~,~~ shall be required to execute a non-disclosure/confidentiality agreement or be subject to equivalent confidentiality and data protection provisions within applicable contractual agreements, and comply with all data protection and security requirements as defined within such agreements.~~.~~

~~2.~~3. SBCERA employees may utilize technology tools, including automated or artificial intelligence-based systems, to assist in the processing or analysis of information; however, PII must not be entered into, transmitted to, or exposed through external systems or tools unless explicitly authorized and appropriate safeguards, including de-identification or redaction, are in place in accordance with SBCERA policies, procedures and applicable law.

CONSEQUENCES:

The deliberate or negligent mishandling or misuse of PII by an SBCERA employee is considered misconduct and may subject the employee to discipline, up to and including termination, or Board action.

Unauthorized access, including a data breach, or improper disclosure of PII shall be reported immediately to the Chief Executive Officer, Chief Counsel, Chief Information Officer, and SBCERA Board, and, depending on the severity of the breach and if required by law, to the affected person(s). Upon discovery of the unauthorized access or disclosure, SBCERA and/or its vendor shall take prompt corrective action to mitigate any associated risks or damages ~~involved,~~ and take any further action as required by applicable law. Employees are expected to report suspected or actual unauthorized access of disclosure of PII in accordance with this policy.