

***Stanislaus County Employees'
Retirement Association***



ELECTRONIC DATA SECURITY POLIC

Policy 1009

January 28, 2011

In addition to complying with Stanislaus County's Computer Security – end user policy, found in Tab 16 of the County personnel manual, Stanislaus County Employees' Retirement Association (StanCERA) augments the policy with the following:

StanCERA member data is considered the Property of StanCERA and subject to all implied property rights. It may not be shared, distributed, published, disposed of, or otherwise released without explicit direction of the StanCERA Executive Director.

1. Electronic member data

- All electronic member data will reside in Tyler and Arrivos databases;
- Access to member data is limited to authorized StanCERA staff;
- Modification of member data may only be done by authorized StanCERA staff; and
- Any data extracted will be limited, secure and temporary.

At times member data must be extracted and shared, such as: actuarial valuations, yearly audits, death audits, state and federal reporting, and authorized Public Records Act requests. Secure procedures are in place for all such processes which include password security, data encryption and/or secure file transfer protocol (SFTP). Excluding these required functions, identifiable member data will not be transported off StanCERA premises. Identifiable member data is any data that includes Social Security number, birth date, name, or address.

Electronic identifiable member data will not be:

- attached to emails for sharing or distribution outside of StanCERA;
- saved to any transportable media including flash drives and CDs or other external; storage device; or
- saved to any Laptop or portable computer.

Extracted member data will only be stored on the StanCERA network drives. Temporary storage on desktop PCs should be cleared daily or at the end of the project/assignment.

Any deviation of the policy requires prior written authorization of the Executive Director or designee, with notification to the Board of Retirement.

2. PERA Application Security

Access authorizations will be reviewed and verified quarterly.

3. Violation of Policy

An employee who violates this policy will be subject to the appropriate disciplinary action, which may include suspension, demotion, or termination from County employment. In addition, an employee may be subject to civil, and/or criminal prosecution.

A vendor who violates this policy may be subject to termination of relations with StanCERA. Vendors may also be subject to civil, and/or criminal prosecution.

Policy Review

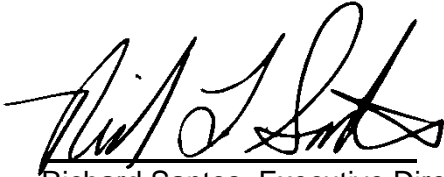
This Board shall review this policy at least every three years.

Policy History

Adopted by the Retirement Board on January 28, 2011.

Amended May 23, 2017.

Reviewed June 10, 2020

A handwritten signature in black ink, appearing to read 'Richard Santos', written over a horizontal line.

Richard Santos, Executive Director

POLICY APPROVAL DATE: January 28, 2011