Cybersecurity Program

I. Purpose

A. This policy establishes general guidelines and a framework for organizational cybersecurity to ensure sufficient governance and management as well as sufficient procedures are in place to safeguard SJCERA informational assets and member data in alignment with industry standards such as the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF") and Special Publication ("SP") 800-53 Rev 5 Security and Privacy Controls or Information Systems and Organizations.

B. SJCERA Trustees as well as appointed officers and designated employees ("Staff") have a fiduciary responsibility to protect the fund and to assess and reduce security risk ensuring the confidentiality, integrity, and availability of SJCERA's information systems and data. Without proper oversight, unauthorized access could result in the breach of systems, exposure of sensitive data such as Personal Identifiable Information ("PII") and Protected Health Information ("PHI"), financial loss, reputation damage, or impact to fiduciary roles.

II. Scope

A. This policy applies to all information systems, employees, vendors, contractors, and partners that access or manage SJCERA's systems and data. The policy covers both internal and external cybersecurity risks.

III. Governance and Accountability

A. Board of Retirement (the "Board")
The Board of Retirement shall oversee the cybersecurity program, as well as instruct Staff to provide regular reports on cybersecurity risks to the San Joaquin County Employees' Retirement Association and related infrastructure (the "System"). The Board shall ensure alignment between SJCERA cybersecurity initiatives and organization goals through delegation and instruction to Staff.

Additionally, the Board shall, through consultation with Staff, ensure sufficient resources are allocated in order to maintain cybersecurity maturity and compliance with industry standards.

B. Chief Executive Officer (the "CEO")
The CEO shall implement the Board-approved cybersecurity policy and may delegate such implementation to Staff and outside vendors as appropriate.

C. Assistant Chief Executive Officer (the "ACEO")

The ACEO shall develop and maintain the Board-approved cybersecurity program, while following appropriate industry standard guidelines. The ACEO shall also provide the Board with quarterly reports in closed session on the cybersecurity posture of the System and incident responses. The ACEO shall be responsible for coordinating with the IT Manager, external auditors, and vendors on cybersecurity program management and risk reporting to the Board.

D. IT Manager

The IT Manager is responsible for daily cybersecurity operations including vendor management and communications. The IT Manager shall manage security awareness programs and ensure compliance with cybersecurity policies for System stakeholders.

The IT Manager shall conduct regular risk assessments and penetration testing of the System to identify vulnerabilities. The IT Manager shall also review San Joaquin Countywide Information Security Policies annually to ensure SJCERA meets or exceeds County policies and procedures. The IT Manager shall make additional policy and procedure update recommendations to the ACEO as needed, no less than once per annum.

IV. Cybersecurity Program Components

Staff, as designated and defined above shall be responsible for the following duties in coordination with the IT Manager, external auditors, and vendors as listed below:

A. Identify (Asset Management and Risk Assessment)

1. Maintain an updated inventory of all IT assets, including hardware, software, and data repositories.

2. Develop and document a risk management process to identify, prioritize, and assess cybersecurity risks.

3. Identify critical business functions and information requiring protection (e.g., member records, pension payments).

4. Establish roles and responsibilities for cybersecurity-related tasks.

B. Protect (Safeguard Systems and Data)

1. Implement access control policies based on least privilege and need-to-know principles.
2. Use multi-factor authentication (MFA) for remote access and privileged accounts.
3. Ensure all devices, systems, and software are patched and up-to-date.
4. Encrypt sensitive data at rest and in transit.
5. Establish controls and procedures to ensure PII is safeguarded throughout the organization.
6. Develop and implement cybersecurity awareness training for all employees.

C. Detect (Monitoring and Incident Detection)

1. Deploy intrusion detection and prevention systems (IDPS) for network monitoring.
2. Implement Security Information and Event Management (SIEM) systems to analyze and detect anomalous activity.
3. Conduct regular audits and vulnerability scans to identify potential threats.
4. Monitor vendor access and ensure third-party systems comply with SJCERA's security policies.

D. Respond (Incident Management)

1. Maintain an Incident Response Plan (IRP) that outlines procedures for identifying, managing, and mitigating cyber incidents.
2. Establish a communication protocol for internal and external stakeholders during incidents.
3. Conduct regular incident response drills to test the effectiveness of the IRP.
4. Report significant incidents to the Board and, if necessary, to regulatory authorities.

E. Recover (Resilience and Restoration)

1. Maintain up-to-date backups of critical systems and data, stored securely offsite.
2. Develop a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
3. Conduct regular tests of recovery procedures to ensure operational readiness.
4. Review and update recovery plans after incidents or changes in the environment.

F. Third-Party Risk Management

1. Ensure all third-party vendors comply with SJCERA's cybersecurity policies and are contractually obligated to report security incidents.
2. Conduct regular assessments of vendor security practices.
3. Include cybersecurity clauses in all new vendor agreements.

G. Monitoring, Reporting, and Continuous Improvement

1. Provide the Board with regular updates on the cybersecurity program, including key metrics and significant incidents.
2. Conduct annual assessments using NIST's Cybersecurity Framework to identify areas for improvement.
3. Engage external auditors for independent cybersecurity evaluations.
4. Foster a culture of continuous improvement to adapt to emerging threats and technologies.

V. Policy Review

A. Staff shall review this Policy at least once every three years to ensure that it remains relevant, appropriate, and in compliance.

VII. History

12/13/2024 Adopted by Board of Retirement

Certification of Board Adoption:

12/13/2024

Clerk of the Board Date