Section 3.0 FINANCIAL AND ADMINISTRATIVE OVERSIGHT

3.7 INFORMATION SECURITY POLICY

Adopted: July 14, 2026

Purpose

This policy establishes the governance framework for managing cybersecurity risks and safeguarding the confidentiality, integrity, and availability of the System's information, technology assets, and business operations. The LACERS Board of Administration ("Board") recognizes that information security is an important component of enterprise risk management and essential to maintaining public trust and confidence in the System. Therefore, LACERS' information security measures comply with the requirements of the California Consumer Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA), relevant California Civil Codes governing data breach reporting and notification, and 2 CFR § 200.79 regarding Personally Identifiable Information (PII).

I. Scope

This policy applies to the LACERS Board, staff, and any individuals who access, develop, manage, or maintain LACERS information systems, networks, software applications, websites, or related resources on behalf of LACERS and its stakeholders. It is the responsibility of all users of LACERS systems to safeguard the organization's technology and information assets, including:

- Computer hardware and related components
- System software
- Application software
- Artificial intelligence
- Communications network hardware and software

II. Policy Guidelines

A. Information Security Program (ISP). LACERS shall maintain an ISP designed to protect organizational information and technology resources from unauthorized access, misuse, disclosure, disruption, or loss. The ISP will align its security practices with applicable governmental standards and LACERS-recognized cybersecurity frameworks and will support, at a minimum, the following objectives:

- Perform ongoing risk assessments and implement measures to reduce identified vulnerabilities.
- Ensure robust threat detection, incident response, and recovery capabilities, along with organizational readiness for these activities.
- Provide ISP-specific training for LACERS staff.
- Establish onboarding, compliance, monitoring, and reporting requirements for LACERS staff, visitors, and vendors.

Section 3.0 FINANCIAL AND ADMINISTRATIVE OVERSIGHT

B. Governance and Oversight. Designated information technology and information security personnel are responsible for the daily administration of security controls, the conduct of risk assessments, the execution of monitoring activities, and the communication and coordination of incident response functions. Executive management is responsible for implementing and administering the ISP. The Board shall provide governance and oversight of information security risk management by reviewing periodic reports on material risks, significant security incidents, and the status of mitigation activities. This policy shall be subject to periodic review to ensure it meets industry best practices for public pension plans.

C. Confidential and Sensitive Information. LACERS shall implement reasonable safeguards to protect all confidential and sensitive information. Such information may be found in any medium, whether oral, written, or electronic. It includes the following:

- **Personal Information** – Non-public information that is identifiable to an individual. Examples include demographic information, such as an individual's age, social security number, or personal contact information; health information, such as an individual's medical history; or certain benefit elections, such as a member's contingent beneficiaries.
- **Security Information** – Information that could negatively impact the security or operational integrity of LACERS if disclosed without authorization. Examples include details about LACERS' information technology systems, security controls, and financial accounts.
- **Privileged Information** – Information that is legally protected from mandatory disclosure, such as attorney-client communications and investment due diligence materials.

These safeguards include controlling who may access the information, how it is collected, used, stored, shared, and ultimately disposed of. Access to confidential information is restricted to authorized personnel and shall be accessed, used or disclosed only to the extent necessary to support LACERS' operational needs and in accordance with all applicable laws. Individuals who are granted access to sensitive information are responsible for ensuring it is not improperly disclosed, accessed, or misused.

D. Third-Party Service Providers. LACERS acknowledges that third-party vendors, consultants, contractors, administrators, and other service providers can introduce information security risks when they access pension systems or data. Therefore, LACERS shall require these third parties to accept appropriate contractual provisions concerning information security protections and implement necessary security measures. These may include

confidentiality commitments, cybersecurity and data-protection obligations, incident-reporting requirements, and, when applicable, requirements for providing evidence of adequate security controls or compliance practices.

E. Incident Response. LACERS shall maintain procedures for identifying, reporting, responding, mitigating, and recovering from information security incidents and cyber threats. All personnel and contract service providers must adhere to the following requirements:

- **Incident identification and reporting** – All suspected or confirmed cyber incidents must be reported immediately to the designated information security personnel, and a description of the incident and the scope of affected data must be provided. If the incident involves a third-party vendor that has access to pension system data, LACERS may suspend vendor access if necessary to prevent further compromise.
- **Containment** – Affected systems or accounts will be isolated, and suspected credentials must be revoked or reset. Remote connections or data flows may also be suspended until security is assured.

F. Eradication and System Restoration. Unauthorized access mechanisms and exploited vulnerabilities must be removed, and systems shall be restored using verified clean backups and tested to ensure they are free of compromise. Enhanced monitoring will remain in place during post-restoration stabilization.

G. Communication and Notification. LACERS Executive team and Board shall be notified promptly of confirmed incidents. If a cyber incident compromises Member data, Members' notifications must be coordinated with the legal and communications teams. LACERS shall ensure vendors meet their own legal notification obligations.

- **Post-Incident Review** – LACERS shall complete an after-action report summarizing the incident, impact, responsive activities, and areas for improvement. Identified gaps or weaknesses will be addressed through updated controls, policies, and training.

III. Compliance

All individuals governed by this policy are required to adhere to LACERS' information security standards, requirements, and administrative procedures. Non-compliance with this policy may result in disciplinary action, contractual remedies, or other corrective measures permitted under applicable law.