SECURED WORKPLACE POLICY

Responsible Manager: LACERA's Privacy Officer

Original Effective Date: April 1, 2018 **Last Updated:** March 7, 2018

Mandatory Review: April 1, 2020 (Biennially)

Approval Level: Board of Retirement (BOR)

---

1 PURPOSE

The purpose of the Secured Workplace Policy ("Policy") is to establish LACERA's minimum requirements and parameters for securing sensitive and confidential information under its physical control.

The goals of this policy are to:

- Mitigate potential security breaches; and
- Create employee awareness about the importance of securing sensitive and confidential information such as Protected Health Information (PHI) and Personal Identifiable Information (PII).

2 LEGAL AUTHORITY

This Policy is created as part of LACERA's fiduciary responsibility to all of its members. Also, LACERA is obligated to secure all sensitive and confidential personal information and medical information of members and staff under various Federal and State laws, including but not limited to:

- The Health Insurance Portability and Accountability Act (HIPAA), as a plan sponsor,
- County Employees Retirement Law of 1937 (CERL)
- Federal and State Privacy and Data Breach laws

3 SCOPE

The term "secured workplace" refers to any physical location where sensitive and/or confidential information is handled or stored by LACERA's employees, temporary agency staff, board members, and contractors (authorized individuals). These physical locations include, but are not limited to, cubicles, offices, work areas, shelves and storage areas, and other LACERA office locations.

4 POLICY STATEMENT

4.1 Protection of Sensitive and/or Confidential Information

At all times, sensitive and confidential information is to be protected from misuse, loss, unauthorized access, unintended modification, disclosure, and/or removal.

When in use, such materials are to remain in the exclusive possession and control of authorized individuals and used only for the originally intended and authorized use. Reasonable security measures must be followed, such as keeping these materials in a secured location and protected from unauthorized examination or access. Sensitive documents should not be left unattended on printers, fax machines, or copiers or any other areas where they might be accessible to other parties.

When not in use, confidential and sensitive documents should be stored in a secured storage space. This includes a locked drawer, cabinet, or specific room such as an office, storage room, or records room.

Only authorized and accountable individuals should control the access to secured work and storage spaces.

Any known or suspected violation of this policy should be reported to management immediately, and appropriate steps should be taken to correct or mitigate any negative impact.

4.2 Enforcement and Consequences of Noncompliance

4.2.1 The Privacy Officer (PO), the PO's designee, or the interim PO as appointed by the Chief Executive Officer, is responsible for:

a. Enforcing the provisions of the Secured Workplace Policy and ensuring that all divisions comply with it;

b. Notifying management of any new local or national-level regulations that apply to the Policy;

c. Periodic monitoring and auditing of the Policy;

d. Providing management and staff with any guidance on the Policy, including defining reasonable security measures; and

e. Investigating possible violations of the Policy and advising on any corrective actions when necessary.

4.2.2 Each Division Manager is responsible (subject to the Privacy Officer's concurrence) for:

a. Developing division procedures that ensure the Secured Workplace Policy is properly managed and adhered to within the division;

b. Ensuring that employees are properly trained on divisional procedures;

c. Providing staff with the tools they need to keep their workspaces secure. For example, ensuring that all desks have lockable drawers, or provide lockable storage areas so employees can lock up printed documents that may contain confidential data;

d. Enforcing compliance with the Secured Workplace Policy, including imposing appropriate consequences for policy non-compliance. Examples of enforcement measures include, but are not limited to, periodic inspections..

4.2.3 If a division is not in full compliance with LACERA's Secured Workplace Policy, the Division Manager will prepare a Secured Workplace Compliance Plan, subject to the approval of LACERA's Privacy Officer. This plan lays out remediation steps and an estimated date of completion. Steps listed should include immediate mitigation measures that are to be implemented until permanent security measures are established.

4.2.4 Each employee's manager is responsible for ensuring the employee is in compliance with the Policy. Any employee found not to be in compliance with the Policy or an approved Secured Workplace Compliance Plan will be counseled and/or provided refresher training regarding the policy as deemed necessary by the manager. Continued noncompliance will be subject to disciplinary action, in accordance with the Progressive Discipline guidelines, up to and including termination of employment, depending on the severity of the incident.

The following serve as examples of possible violations:

a. Keys and lock combinations are accessible by unauthorized parties;

b. Sensitive documents are left unattended in plain sight;

c. LACERA-issued equipment such as key cards, ID badges, or any digital devices are not secured; and

d. Sensitive documents are left unattended on equipment, such as printers, fax machines, or copiers.

4.3 Definitions

4.3.1 Authorized and Accountable Individuals: LACERA employees, temporary agency staff who have been approved to access specific data types, board members, and contractors (with the exception of maintenance and cleaning contractors, whether employed by LACERA or the Office of the Building)

4.3.2 HIPAA: Health Insurance Portability and Accountability Act, a 1996 Federal law that restricts access to individuals' private medical information

4.3.3 Secured Work Space: Work space that can be locked to prohibit entry

4.3.4 Unsecured Work Space: An open work space that cannot be locked to prohibit entry

4.3.5 Secured Storage Space: Storage that can be locked to prohibit entry

4.3.6 Unsecured Storage Space: Storage space that cannot be locked to prohibit entry

4.3.7 Security: Protecting information from unauthorized disclosure or intelligible interception

4.3.8 Reasonable Security Measures: Security tools and practices established by a Division Manager or above, and approved by LACERA's Privacy Officer, based on a careful consideration of costs, risks, and benefits

4.3.9 Sensitive and Confidential Information: Includes but not limited to all LACERA-related data, storage media in any format, medical files such as those protected under the HIPAA Privacy Rule or medical records maintained by Disability Retirement Services and Disability Litigation, Social Security numbers, information not attainable through the Public Records Act, etc. The following are the primary categories of Sensitive and Confidential Information:

a. **PHI**: Protected Health Information as defined by HIPAA or other similar laws

b. **PII:** Personal Identifiable Information, including member records

c. **Security Information:** Information required to access other sensitive or confidential information, or LACERA's assets

d. **Proprietary Information:** Information that is considered a valuable asset to LACERA that requires protection from unauthorized access to preserve its value

e. **Privileged Information:** Information that LACERA is entitled by law to protect from disclosure, such as attorney–client communications and legal work products

4.3.10 Secured Workplace Compliance Plan. This plan is prepared by Division Management when a division is found to be noncompliant with LACERA's Secured Workplace Policy. This plan is subject to the approval of LACERA's Privacy Officer. This plan lays out remediation steps and an estimated date of completion. Steps listed should include immediate mitigation measures that are to be implemented until permanent security measures are established.

5 HISTORY

5.1 Approvals

As the scope of this Policy applies to all LACERA staff and has an organization-wide effect, the following approval is required.

5.1.1 Recommended by OOC:

5.1.2 Approval by BOR:

5.2 Current Status

5.2.1 Original Effective Date: April 1, 2018

5.2.2 Last Updated: March 7, 2018

5.2.3 Mandatory Review: April 1, 2020 (Biennially)

5.3 Versions

5.3.1 There are no prior versions to date.