Non-LACERA Managed Devices (Bring Your Own Device (BYOD)) Acceptable Use Policy (Applicable to LACERA Trustees)

Adopted: Board of Retirement, December 6, 2023
Board of Investments, December 13, 2023

Non-LACERA Managed Devices (Bring Your Own Device)
Acceptable Use Policy (Applicable to LACERA Trustees)

Authorizing Manager: Chaitanya Errande, Information Security Officer

Effective Date: 12/13/2023 **Last Updated:** November 2023

Mandatory Review: November 2024 (Every Year)

Approval Level: Board of Retirement and Board of Investments

I. Purpose

The purpose of this policy is to promulgate standards for the use of technological accounts and devices that are not owned or managed by LACERA that are used by Trustees to conduct LACERA business.

II. Scope / Applicability

LACERA does not require Trustees to use their own personal accounts and devices to conduct LACERA business. LACERA accounts and devices are available to all Trustees. This Policy applies to LACERA Trustees ("Trustees") who wish to Bring Your Own Device and use their own accounts (BYOD). BYOD allows authorized Trustees to conduct LACERA business using their own personal technological accounts and devices.

LACERA encourages Trustees, to use LACERA issued accounts and devices to conduct LACERA business given the risks associated with the use of BYOD and to protect LACERA's member and business information as well as their own; nonetheless, if Trustees opt not to do so and to continue the use of BYOD, they should follow the standard procedures and protocols set forth in this Policy.

III. Legal Authority

This Policy is based on the paramount fiduciary duty of Trustees and the Boards under Article XVI, Section 17 of the California Constitution, and other authority, to administer the fund consistent with the duty of loyalty to members and their beneficiaries and consistent with the duty of prudence to "discharge their duties with respect to the system with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent person acting in a like capacity and familiar with these matters would use in the conduct of an enterprise of a like character and with like aims." This Policy is based on best and prudent practices for the use of your own personal technological devices to conduct LACERA business.

Both the Board of Investments (BOI) and the Board of Retirement (BOR) may promulgate policies, procedures, and charters, including policies regulating the use by Trustees of LACERA devices and personal devices used for LACERA business, as needed for the purpose of LACERA administration to further their fiduciary duty under Article XVI,

III. Legal Authority (Continued)

Section 17 of the California Constitution, the County Employees Retirement Law of 1937 (CERL), the California Public Employees' Pension Reform Act of 2013 (PEPRA), and other governing laws, regulations, and case authority.

IV. Definitions

For the purpose of this Policy, the terms below are defined as follows:

Acceptable Use: The application of best practices that ensure LACERA resources, including information, accounts, and devices, are protected, and the use is limited to conducting authorized LACERA business by Trustees.

Authorized User(s): A Trustee authorized to use a BYOD by the Board of Retirement or Board of Investments.

BYOD (Bring Your Own Device): A non-LACERA managed personal computing platform, mobile device, communication, accounts, or storage system. (Examples of communications include, but are not limited to, email, SMS, social media).

LACERA Communication Systems and Resources: Any data, services, account, or device owned by LACERA. (Examples of LACERA resources include but are not limited to LACERA email, LACERA issued mobile devices such as phones, tablets, laptops, Internet of Things (IOT), LACERA data and applications).

Security Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a BYOD or the information the BYOD system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use.

LACERA Trustees/Trustees: Members of the Board of Retirement and/or Board of Investments.

V. Policy

LACERA recognizes that Trustees may wish to use their BYOD to use, transmit and receive LACERA data, e-mails, and resources. This Policy provides standards and guidance for Acceptable Use of BYOD to access LACERA resources and services.

1) LACERA Trustees shall employ reasonable physical security measures to prevent a BYOD from being lost or stolen, and to prevent unauthorized access and use, including having a passcode on their BYODs.
2) Trustees shall exercise due care with members' Personally Identifiable Information (PII), Personal Health-related Information (PHI) and any other sensitive information, including emails and disability claim information, located in

VI. Policy (Continued)

a BYOD device or account. Such sensitive information shall not be stored on any BYOD beyond the date of the business need.

3) LACERA Trustees shall only use a BYOD in accordance with Acceptable Use.
4) Any BYOD must be password or biometric protected. Password complexity should adhere to a minimum of 12 characters including at least 1 Capital letter, 1 number, and 1 special character (@,#, $, * ...) on data encryption and logins and at least 8-digit pins where number pins are required for login.
5) Screen locking and screen timeout should be enabled on any BYOD to be no more than 15 minutes.
6) Trustees may request LACERA to leverage various device control tools to manage and monitor access from a BYOD to protect the security and prevent the misuse of LACERA resources. Actions that may be taken include but are not limited to:
    a. Deleting or remotely wiping LACERA data and LACERA applications from personally owned devices due to:
        i. Lost or stolen devices.
        ii. Change in Trustee status.
        iii. Violation of, or changes to LACERA policies and procedures.
        iv. Any other circumstances that may put LACERA resources and member data at risk.
    b. Tracking of connections to and usage of LACERA resources.
    c. Investigating potential breaches and/or misuse of all LACERA related communications, information, or other collected data.
7) If requested, LACERA will only exercise control over LACERA resources on the BYOD platform. Personal email and member communications of all types in the personal email are out of scope to the extent obtained in a capacity other than that of a LACERA Trustee.
8) BYOD should be updated with the most current operating system by the Trustee by following recommended updates by the software manufacturer of all installed software and the device manufacturer.
9) LACERA Trustees shall immediately report any known security incidents involving their BYOD to the Board Chair and LACERA's CEO. Trustees are expected to cooperate with LACERA on any investigations that follow.
10) Trustees are expected to comply with requests where a BYOD is subject to search according to criteria provided by the Legal Office and produce LACERA records on such devices when needed in response to Public Records Act requests, subpoenas, or litigation discovery.
11) LACERA is not liable for the loss, theft, or damage of any BYOD except as would otherwise be covered due to official use.
12) LACERA will be promptly notified if a BYOD is subject to any litigation or a Public Records Act request.
13) LACERA resources on a BYOD must be completely removed before Trustees decide to terminate ownership of their devices.

V. Policy (Continued)

Non-Compliance

If an authorized Trustee fails to follow appropriate security standards, their respective boards reserve the right to rescind the Trustees authorization to use BYOD under a 2/3 vote of the members present, or if less than two-thirds of the members of the Board are present, unanimous vote of those present.

VI. References

These references are intended to help explain this Policy and are not an all-inclusive list of security standards. The following information complements and supplements this Policy:

Related Information:

- LACERA Privacy and Confidentiality Policy
- LACERA End-User Security Policies & Standards Manual

NIST (National Institute of Standards and Technology) SP 1800-22, BYOD for standards and framework.

VII. Version History

Policy Issue Date: December 13, 2023

Policy Effective Date: December 13, 2023

VIII. Policy Reviews /Approval

This Policy is a Board approved Policy and shall be reviewed one year after the original effective date and each year thereafter.

Review Level: Board of Retirement and Board of Investments

Periodic Review Timeframe: Every year