VENTURA COUNTY EMPLOYEES' RETIREMENT ASSOCIATION

TRUSTEE TECHNOLOGY USE & MOBILE DEVICE POLICY

I. Policy

The Ventura County Employees' Retirement Association (VCERA) provides Board members with VCERA-owned devices and County of Ventura email to securely conduct VCERA business. The purpose of this document is to identify the requirements to use VCERA-owned devices and County of Ventura email to ensure device and data security. This policy will also outline the appropriate use and support of VCERA-owned devices and set forth expectations for replacement should loss or damage occur.

The use of Personal Devices (excluding Personal Smartphones) and personal email addresses are not permitted or supported to conduct VCERA business. Should an exception be required, for limited use of a Personal Device, written approval by VCERA's Retirement Administrator or Chief Technology Officer is required.

Board members that have devices owned and supported by another County of Ventura agency and a County of Ventura email are permitted to use their County-owned device.

II. Purpose

This policy is intended to set forth the authorized use of VCERA-owned devices and County of Ventura email that may have VCERA data present or accessible, as well as the limited use of Personal Smartphones and Personal Devices.

This policy is not intended to address usage of USB sticks, DVDs, CDs, external hard drives, or other forms of portable data storage.

1) VCERA provides electronic versions of board and committee materials which are accessible via County of Ventura email, SharePoint and/or secure online agenda management software.

2) To protect member confidentiality and privileged VCERA data, VCERA-owned devices and County of Ventura email are provided to all Board members to ensure secure storage and transmission of sensitive and confidential information. These security protections cannot be mandated for Personal Devices, resulting in potential security risk due to loss, theft, or unauthorized access due to user control over manual configuration of passwords or security codes, or other VCERA security practices.

3) Email, data and other written communications by VCERA Board members discussing or otherwise conducting VCERA business, constitute public records that may be subject to inspection unless protected from disclosure under the California Public Records Act. If

Personal Devices or Personal Smartphones are used for official communications, VCERA Board members will be required to review their emails and report to VCERA in a timely manner all VCERA business-related communications responsive to a Public Records Act request to enable VCERA to respond to such requests, pursuant to the California Supreme Court decision in City of San Jose v. Superior Court (2017) 2 Cal.5th 608.

III. Scope

These guidelines apply to VCERA Board members.

IV. Definitions

For purposes of this policy the following key terms are defined as follows:

4) "VCERA-owned Device" is defined as any portable device owned and issued by VCERA, with Internet capabilities, that can leave the VCERA office. This may include laptops, smartphones, tablets, iPads and any other mobile device capable of connecting to the Internet, broadband networks and VCERA and County of Ventura networks, email, and data.

5) "Associated Equipment" is defined to include charging cables, accessories and other peripheral devices used in conjunction with "VCERA-owned Devices."

6) "Personal Device" is defined to include laptops, tablets, eReaders, iPads or any mobile device (except for Personal Smartphones) that is personally owned and can connect to the Internet, VCERA and County of Ventura guest wireless networks, email and data.

7) "Personal Smartphone" is defined to include iPhone or Android smartphones not owned by VCERA or the County of Ventura and can connect to the Internet, broadband networks and VCERA and County of Ventura guest wireless networks.

8) "Mobile Device Agreement" is defined as the signed agreement between VCERA and Board members documenting assignment of VCERA-owned devices, associated equipment and replacement costs should a device be lost or damaged due to neglect.

V. Objectives

9) Device Assignment – VCERA-owned devices will be furnished to all Board members, however those that have a County of Ventura owned device are permitted to use this device in lieu of a VCERA-owned device. The purpose of the device is to provide access to VCERA email, data and board meeting materials, outside the office or beyond normal working hours. Acquisition, assignment, and use will be governed by this policy.

10) Appropriate Use – To protect both VCERA and the County of Ventura (to the extent VCERA data is stored on County servers), controls are in place to ensure appropriate use. VCERA-owned devices contain data that may be legally "discoverable", i.e., subject to disclosure

under the Public Records Act and to discovery under the civil litigation or criminal discovery rules, within the limits defined by law.

11) Password Protection – To prevent unauthorized access to sensitive and confidential data, email and VCERA and County of Ventura networks, all VCERA-owned devices are configured with a password and inactivity lock-out, governed by VCERA cybersecurity practices. These settings cannot be altered or disabled.

12) Mobile Device Management (MDM) – To ensure controls are in place to protect VCERA, the County of Ventura and member data, VCERA-owned devices are enrolled in MDM software. MDM has controls in place to monitor and prohibit unauthorized use, app installation, content, etc. on VCERA-owned devices. MDM software cannot be uninstalled by the user and requires location services to be enabled.

13) Mobile Device Encryption – All VCERA-owned devices are encrypted with full disk encryption as supported by County of Ventura – IT Services. VCERA-owned devices are encrypted by default.

14) Personal Smartphones – Board members may be permitted access to VCERA email, data and board materials from a Personal Smartphone. Users must be aware that when a VCERA email is connected to their Personal Smartphone, it creates a connection to Office 365. VCERA email or data that is on a Personal Smartphone that connects to Office 365 may be subject to disclosure under the Public Records Act or discovery under civil litigation or criminal discovery rules, within limits defined by law. Additionally, upon departure from VCERA (resignation, retirement, termination, death, etc.), a data wipe may be initiated, to remove the VCERA email loaded on the Personal Smartphone.

15) Personal Devices and Personal Email – The use of Personal Devices and personal email addresses are not permitted or supported to conduct VCERA business. Should an exception be required, for limited use of a Personal Device only, written approval by VCERA's Retirement Administrator or Chief Technology Officer is required. There is no exception for the use of personal email addresses.

VI. Guidelines

16) Privacy – Board members' authorization to use VCERA-owned devices is for the primary purpose of conducting VCERA business. Board members may have no expectation of privacy regarding their use of such devices, as between the user and VCERA.

17) Mobile Device Agreement and Separation – Board members issued VCERA-owned devices and associated equipment are responsible for safeguarding the device and may be responsible for the replacement cost of the device or associated equipment if it is lost or damaged due to neglect or misuse. Board members are required to sign the VCERA Mobile Device Agreement upon acquisition of VCERA-owned devices governed by this policy.

Board members will return all assigned VCERA-owned devices and associated equipment prior to or upon separation of VCERA service and remove all personal accounts, data and passwords. Board members will be required to provide user account information if personal account and passwords are not removed from the device prior to its return. Should a VCERA-owned device or its associated equipment not be returned, Board members may be responsible for reimbursing VCERA the costs agreed upon in the VCERA Mobile Device Agreement.

18) Security Patching, Upgrades, Routine Maintenance or Repair – VCERA may require assigned VCERA-owned devices to be returned to the office for security patching, upgrades, or routine maintenance or repair; this is to ensure that devices are kept current with security practices and are being used only in a manner consistent with this policy.

    Board members are responsible for immediately contacting the VCERA Chief Technology Officer should any suspected malicious activity or breach of passwords occur. If deemed necessary, the device must be surrendered to the Chief Technology Officer for further review.

19) Loss or Theft and Data Backups – Should a VCERA-owned device, Personal Device or Personal Smartphone, configured with VCERA email or data be lost or stolen, Board members must report this loss to the VCERA Chief Technology Officer immediately.

    All users are responsible for backing up any personal data stored on the assigned VCERA-owned device.

20) Password/Security Code – All Personal Devices and Personal smartphones that have VCERA email or data on them, MUST be configured at a minimum, with a four-digit security code or password for access.

21) Auto-Lock – All VCERA-owned devices must automatically lock after a maximum of 15 minutes of inactivity and require entry of a security code or password to unlock for use. Personal Devices and Personal Smartphones that have VCERA email or data on them, must automatically lock after a maximum of 15 minutes of inactivity and require entry of a security code or password to unlock for use.

22) Management Software – Assigned VCERA-owned devices may have management software installed for enforcing policies, deploying updates and new software, and identifying device location. Such software may not be tampered with, uninstalled or disabled.

23) VCERA Email and Data on Personal Devices or Personal Smartphones – Personal Devices or Personal Smartphones configured with County of Ventura email or data are subject to remote wiping of business email and data or the entire contents of the device. Every attempt will be made to contact the user before such action is taken, but in the event of a significant security breach or threat, this may not always be possible.

VII. Process Review

VCERA staff will review the Trustee Technology Use and Mobile Device Policy at least once every three (3) years to ensure that it remains relevant and appropriate and present to the Board for approval. VCERA staff will review the VCERA Mobile Device Agreement at least once every three (3) years to ensure that it remains relevant and consistent with the most recently approved Trustee Technology Use and Mobile Device Policy.

VIII. Policy History

The Board last reviewed and approved this policy on March 25, 2024. The Board previously reviewed and approved this policy on March 29, 2021.