VENTURA COUNTY EMPLOYEES' RETIREMENT ASSOCIATION

STAFF TECHNOLOGY USE AND MOBILE DEVICE POLICY

I. Policy

The Ventura County Employees' Retirement Association (VCERA) relies on mobile devices to provide staff with the ability to conduct business both on and off site. The purpose of this document is to ensure appropriate use of both VCERA-owned Mobile Devices and Personal Devices (when such devices are used for VCERA business), support of VCERA devices and to identify expectations for replacement of VCERA-owned devices should loss or damage occur.

II. Purpose

This policy is intended to set forth the authorization and limitations of use of VCERA Mobile Devices and Personal Devices that have County of Ventura email and VCERA data present or accessible.

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 with offsite access. The electronic version is created to allow staff to use Mobile Devices to retrieve, store, edit and read the electronic board agenda packet.

2) Mobile Devices and personal devices are a potential security risk due to loss, theft, or other unauthorized access, and may contain confidential or privileged VCERA information, including, without limitation, private member and beneficiary information, member health records, as well as confidential and proprietary information of alternative investment managers.

3) Personal Devices may be more vulnerable to malware, viruses and other such threats because the user may not regularly use virus protection software and other safeguards available to VCERA's computers.

4) Personal Devices may be more vulnerable to unauthorized access because the user is required to manually configure passwords or security codes on their device(s).

5) Email, data and other written communications by VCERA staff discussing or otherwise conducting VCERA business, constitutes public records that may be subject to inspection unless protected from disclosure under the California Public Records Act. If personal devices are used for official communications, VCERA staff will be required to review their emails for communications responsive to a Public Records Act request for VCERA business information in a timely manner to enable VCERA to respond to such requests, pursuant to the California Supreme Court decision in City of San Jose v. Superior Court 2 Cal.5th 608.

III. Scope

These guidelines apply to VCERA staff.

IV. Definitions

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

6) "Mobile 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, eReaders, iPads and any other mobile device capable connecting to the Internet, VCERA and County of Ventura networks, email and data.

7) "Associated Equipment" is defined to include charging cables, accessories and other peripheral devices used in conjunction with "Mobile Devices."

8) "Personal Device" is defined to include laptops, smartphones, tablets, eReaders, iPads or any Mobile Device that is personally owned but capable of connecting to the Internet, VCERA and County of Ventura networks, email and data.

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

V. Objectives

10) Device Assignment - Mobile Devices will be provided staff whose job functions, as deemed by the Retirement Administrator, require access to County email, data and VCERA Board Meeting materials, outside the office or beyond normal working hours. Acquisition, assignment and use will be governed by this policy.

11) Appropriate Use – Mobile Device usage is entrusted to staff and will be governed by VCERA's Chief Technology Officer. 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 and County-owned Mobile 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.

12) Mobile Device Management (MDM) – To ensure controls are in place to protect VCERA, the County and member data, Mobile Devices are to be 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 mobile computing devices (laptops, Windows tablets, etc.) are to be encrypted with full disk encryption as supported by County of Ventura – IT Services. Mobile devices are encrypted by default when locked.

14) Personal Devices – Staff may be permitted access to County or VCERA resources from a Personal Device. Users must be aware that when a County or agency email profile is created on their Personal Device, it creates a connection to Office 365. VCERA data that is on Personal Devices that connect to the County network and 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 or County email profile loaded on the Personal Device.

15) County of Ventura and VCERA WiFi

County of Ventura WiFi

The County of Ventura offers separate WiFi networks to staff, business partners and vendors. These networks are available in VCERA offices and serve different purposes and have separate controls in place to regulate and ensure appropriate use. If staff attempts to connect to an unauthorized network from a VCERA owned device, the device will be blocked and dropped from all County WiFi networks.

VCWiFi – This network is for staff access only while using County/VCERA owned devices which includes laptops, iPads, some desktop computers and VCERA-issued smartphones, if any.

NCWiFi – This network is intended for business partners such as consultants, visitors, contractors, etc. This is NOT to be used by staff or from County/VCERA owned devices.

VCERA WiFi Networks

VCERA has WiFi networks that are separate and distinct from the WiFi provided by the County of Ventura. Use of VCERA WiFi is restricted to use of Trustee devices, VCERA-issued Mobile Devices, staff Personal Devices, contractors and approved guests. Usage is as follows:

VCERA-Board – This network is intended for use by Trustees and Senior Staff Mobile Devices. This network is monitored to ensure only approved devices are connecting.

VCERA-Contractor – This network is intended for use by hired Contractors and designed

VCERA Staff upon approval by the Chief Technology Officer and/or Retirement Administrator. This network is monitored to ensure only approved devices are connecting.

VCERA-Staff – This network is intended for use by Staff to connect Personal Devices and is to be used in accordance with this policy. Should a device be vaguely named or flagged as compromised or exceeding acceptable resource usage, it will be blocked from connecting.

VCERA-Guest – This network is intended for use by business partners such as consultants, visitors, contractors, etc. This is NOT to be used by staff or from County/VCERA owned devices.

VI. Guidelines

16) Privacy - Staff understand that their authorization to use VCERA assigned Mobile Devices is for the primary purpose of conducting VCERA business. Staff further understand that they have no expectation of privacy regarding their use of such devices, as between the user and VCERA.

17) Mobile Device Agreement and Separation - Users issued VCERA-owned Mobile Devices and associated equipment are responsible for safeguarding the VCERA asset 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. Staff are required to sign the VCERA Mobile Device Agreement upon acquisition of Mobile Device equipment governed by this policy.

    Staff will return all assigned Mobile Devices and associated equipment prior to or upon separation of VCERA service and remove all personal accounts, data and passwords. Staff 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 Mobile Device or its associated equipment not be returned, staff may be responsible for reimbursing VCERA the costs agreed upon in the VCERA Mobile Device Agreement.

18) Security Patching, Upgrades, Routine Maintenance or Repair - Staff understand that VCERA may require assigned Mobile Devices be returned to the office for security patching, upgrades, or routine maintenance or repair; this is to ensure that devices are being used only in a manner consistent with this policy. Staff 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 or Personal Device, configured with County of Ventura email or VCERA data be lost or stolen, staff must report this loss to the Chief Technology Officer immediately.**

    Staff who have an assigned Mobile Device are responsible for the security of the device, all associated equipment and all data and must sign the VCERA Mobile Device Agreement upon receipt of the device. Staff must report any lost or stolen device or data immediately to the Chief Technology Officer. The purpose of this is primarily to protect VCERA, County or member data, and secondarily to attempt to recover the asset.

All users are responsible for backing up any personal data stored on the assigned Mobile Device.

20) Password/Security Code - All VCERA assigned Mobile Devices must use, at a minimum, a four-digit security code or 8-character password for access. Personal Devices that have County of Ventura email or VCERA data on them, MUST be configured at a minimum, with a four-digit security code or password for access.

21) Auto-Lock - All VCERA assigned Mobile 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 that have County of Ventura email or VCERA data on them, must automatically lock after a maximum of 10 minutes of inactivity and require entry of a security code or password to unlock for use.

22) Management Software - Assigned Mobile Devices may have management software installed for enforcing policies, deploying updates and new software, and identifying device location. staff understand such software may not be tampered with, uninstalled or disabled.

23) County of Ventura Email and VCERA Data on Personal Devices - Personal Devices configured with County of Ventura email or VCERA data are subject to remote wiping of business email and data or the entire contents of the device. Staff understand that 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 both the Staff Technology Use and Mobile Device Policy and the VCERA Mobile Device Agreement at least once every three (3) years to ensure that it remains relevant and appropriate and present to the Board for approval.

VIII. Policy History

The Chief Technology Officer last reviewed this policy on March 24, 2021. The Board last reviewed and approved this policy on March 29, 2021. This policy replaces and supersedes the *Ventura County Employees' Retirement Association Mobile Device Policy*, originally adopted on June 18, 2012 and last revised on June 26, 2019.