VENTURA COUNTY EMPLOYEES' RETIREMENT ASSOCIATION

MOBILE DEVICE POLICY

I. Definitions

1) For purposes of this policy, "mobile devices" are defined to include laptops, cellular phones, tablets, Kindles, eReaders, iPads or any other mobile device capable connecting to the Internet to access VCERA and County of Ventura email and data.

II. Purpose and Objectives

2) This policy is intended to set forth the authorization and limitations of use of Ventura County Employees' Retirement Association (VCERA) mobile devices and personal devices that have County of Ventura email and VCERA data present.

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

III. Scope

4) These guidelines apply to all Board and staff members.

IV. Background

5) Board packet material is extensive. The copying, delivering and producing of the packet material is expensive and not in line with environmental practices of VCERA. VCERA makes available an electronic PDF version of the monthly board packet and provides offsite access and usage of the electronic version by allowing Board and staff members to use mobile devices to retrieve, store, edit and read the electronic board packet.

6) Mobile devices are a security risk because, they are at risk for 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 (HIPPA data), as well as confidential and proprietary information of alternative investment managers.

7) Personal mobile 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 desktop computers.

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

9) Email and other written communications by VCERA Board and staff members discussing or otherwise conducting VCERA business constitute public records that are subject to inspection unless protected by the California Public Records Act from disclosure. If personal devices are used for official communications, as the California Supreme Court concluded in the 2017 *City of San Jose v. Superior Court* decision, VCERA Board and staff members will be required timely to respond to requests for their email communications regarding VCERA business in response to any California Public Records Act requests for such communications.

V. Guidelines

10) Privacy: Board and staff members understand that their authorization to use VCERA assigned mobile devices are for the primary purpose of conducting VCERA business. Board and staff members further understand that they have no expectation of privacy with regard to their use of such devices.

11) Security Patching, Upgrades, Routine Maintenance or Repair: Board and staff members understand that VCERA could require that assigned devices be returned to the office for, security patching, upgrades, routine maintenance or repair, to ensure that devices are being used only in a manner that is consistent with these policies. Board and staff 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.

12) Loss or Theft and Data Backups: Board and staff members who have an assigned mobile device are responsible for the security of the device, all associated equipment and all data. Board and staff members must report any lost or stolen device or data, to the Chief Technology Officer as soon as discovered. All users are responsible for backing up personal data stored on the assigned mobile device. Should a personal device, configured with County of Ventura email or VCERA data be lost or stolen, users must inform the Chief Technology Officer immediately.

13) 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 mobile devices that have County of Ventura email or VCERA data on them, must use, at a minimum a four-digit security code or password for access.

14) Auto-Lock: All VCERA assigned mobile devices must automatically lock after a maximum of 10 minutes of inactivity and require entry of a security code or password to unlock for use. Personal mobile 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.

15) Management Software: Assigned mobile devices may have management software installed for enforcing policies, deploying updates and new software, and identifying device location. Board and staff members understand such software may not be tampered with, uninstalled or disabled.

16) County of Ventura Email and VCERA Data on Personal Devices: Personal mobile 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 mobile device. Board and staff members understand that every attempt will be made to contact the user before this occurs, but in the event of a significant security breach or threat, this may not be possible.

17) Return Prior to Separation: Board and staff members will return all assigned mobile device(s) prior to separation of VCERA service and remove all personal accounts, data and passwords. Board and staff members will be required to provide user account information should personal account and passwords not be removed from the device.

VI. Process Review

18) The Chief Technology Officer will review the 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.

VII. Process History

19) The Chief Technology Officer last reviewed this policy on June 26, 2019. The Board last reviewed and approved this policy on July 1, 2019. The Board previously approved this policy on June 1, 2018. The Board originally adopted this policy on June 18, 2012.