SamCERA Portable Electronic Device Policy

For purposes of this policy, the term "Portable Electronic Devices" generally refers to electronic tablets, such as an iPad, but also includes any other electronic device such as a laptop or cellular phone which is utilized for the purpose of conducting SamCERA business and/or accessing SamCERA's network or applications.

Purpose and Scope:

This policy is intended to set forth the authorization and limitations of use of Portable Electronic Devices by SamCERA Board Members.

This policy does not cover SamCERA staff utilizing Portable Electronic Devices to conduct SamCERA business. As County employees, SamCERA staff members' use of such devices is subject to compliance with the County's IT security policies, which are consistent with this policy with respect to required security measures.

The policy incorporates modern cybersecurity best practices, including multi-factor authentication (MFA) requirements, encryption standards, Mobile Device Management (MDM), and secure remote access controls.

Background:

SamCERA Board packet material is extensive. The copying, delivering, and producing of such materials can be expensive and, in any event, is not in line with SamCERA's environmental policies and practices. In addressing these concerns, SamCERA now makes its monthly Board packet materials available in electronic format. SamCERA facilitates the offsite access and usage of electronic versions of these and other documents by allowing Board members to use Portable Electronic Devices to retrieve, store, edit, and read such materials.

Portable Electronic Devices are a security risk because they may contain private, confidential, or sensitive SamCERA information including, but not limited to, SamCERA member information and non-public investment information. Portable Electronic Devices are more vulnerable to viruses and cybersecurity threats due to potential gaps in virus protection and outdated software. Unauthorized peripheral devices, such as USB drives, may also pose a risk. In addition, because such devices are portable, they are at increased risk for loss, theft, or other unauthorized access and are more likely to be connected to non-SamCERA networks or devices which may, in turn, provide an avenue for unauthorized users to gain access to the device and SamCERA's or the County's network or applications. Consequently, this policy includes enhanced security measures such as mandatory encryption, regular security updates, endpoint detection and response (EDR), and Zero Trust Network Access (ZTNA) protocols.

Policy:

1. To the extent that Board Members desire to utilize a Portable Electronic Device to conduct SamCERA business, such devices must be issued by SamCERA, or in the case of a Board Member who is also a County employee, through a County-issued device in accordance with the County's IT security policies. Board Members may not access SamCERA's non-public information such as confidential investment reports and information or confidential member information, or otherwise conduct confidential SamCERA business on Portable Electronic Devices that are personally-owned or provided to the member by an organization/employer other than SamCERA or the County.
2. For Board Members who are County employees, the use of any County-issued Portable Electronic Device must comply with the County's IT security policies as such policies may be amended or developed from time to time including, but not limited to, the County's Information Technology Security Policy, Portable Computing Policy, Virus Protection and Patch Management Policy, and Remote Access Policy.
3. Board Members understand that their authorization to: a) periodically use Portable Electronic Devices and software provided by SamCERA and/or b) connect to SamCERA's or the County's network is limited to, and for the sole purpose of, conducting SamCERA business. Board Members further understand that they have no expectation of privacy with regard to their use of SamCERA-issued devices or their use of SamCERA's or the County's network.
4. SamCERA-issued devices are not solely assigned to individual Board Members but are resources to be used on an as needed basis and may be rotated amongst Board Members in accordance with SamCERA's business needs.
5. SamCERA-issued devices are not for the personal use of each Board Member. Board Members will not permit anyone else including, but not limited to, the Board Member's family and/or associates, to use SamCERA-issued Portable Electronic Devices.
6. Board Members may not download or install any software onto any SamCERA-issued devices without prior authorization by the SamCERA CEO or Retirement Technology Officer (RTO).
7. Board Members who have an assigned SamCERA-issued device are responsible for the security of the device as well as all associated equipment and data. Board Members must report any lost or stolen Portable Electronic Devices used to conduct SamCERA business to the CEO or RTO as soon as discovered. Board Members using SamCERA-issued devices should regularly install security updates as they become available and such devices will occasionally be required to be returned to SamCERA for routine maintenance, to confirm

that proper security updates have been installed, and to ensure that they are being used only in a manner that is consistent with this policy.

8. To the extent that a Board Member needs their SamCERA-issued Portable Electronic Device to remotely access the SamCERA network, such access will only be allowed through remote access systems maintained by SamCERA.