Status **Active** PolicyStat ID **10838832**

San Bernardino County Employees' Retirement Association

Origination	11/2/2017
Last Approved	1/6/2022
Effective	1/6/2022
Last Revised	1/6/2022
Next Review	1/5/2025
Area	General
Applicability	SBCERA systemwide

SBCERA Technology Assets

POLICY NO. 019

I. PURPOSE

The purpose of this policy is to provide guidance as to the appropriate use of technology assets and their access to the organization's secured networks and systems.

II. BACKGROUND

San Bernardino County Employees' Retirement Association (SBCERA) utilizes a complex array of interconnected technology assets in order to carry out its mission. SBCERA Staff (Staff) make use of these assets in order to provide service to its membership, plan sponsors, and other stakeholders. Assets may also be made available to the Board of Retirement (Board) members (Trustees) to assist in carrying out their fiduciary duties.

III. SCOPE

This policy covers all technology assets owned and/or operated by, leased to, or under contract with SBCERA.

IV. DEFINITIONS

- **Technology Assets:** All tangible and intangible assets owned, leased, operated, maintained, housed within, paid for, or otherwise used by Trustees and Staff; and where general oversight is within the responsibility of the SBCERA Information Services Department (IS Dept.). Assets include but are not limited to computer hardware, software, licensing, accessories, peripherals, data storage, electronics, telephones, mobile capable devices, Video Teleconference (VTC) Systems, networking equipment/components, cables and office equipment/supplies, Local

Area Networks (LAN), Wide Area Networks (WAN), wireless networks, cellular services, system and/or accounts, cloud-based networks and services, and electronic mail (e-mail).

- **Data:** Any intangible electronic file including but not limited to documents, e-mails, voicemails, pictures, music, and videos.
- **Personal Use**: Activity that is conducted for purposes other than accomplishing official SBCERA or otherwise authorized activity.
- **Non-work Time:** The time when staff are not performing an activity for or under direction of SBCERA. Examples of non-work time include off-duty hours such as lunch periods, authorized breaks, before or after a workday, weekends, or holidays and only if the technology asset(s) would normally be available to the staff member.
- **De Minimis Additional Expense:** The expense incurred when SBCERA is already providing equipment, supplies, or services and the use creates only limited additional amounts of electricity, ink, toner, or paper. Wear and tear from normal use is also considered a de minimis additional expense.
- **Inappropriate or Prohibited Use:** The use of SBCERA technology assets in a way that is forbidden by SBCERA policies, procedures, and/or State or Federal regulations.
- **Mobile Device:** Any device comprised of mobile hardware and/or software components allowing the device to be portable and capable of operating, executing, and providing services and applications. A mobile device may be an SBCERA technology asset, or a device supplied by a Trustee, Staff, Vendor, or Advisor.
- **Confidential Information:** All information potentially containing personally identifiable information, medical information, of a proprietary nature, trade secret, deemed sensitive, classified, or within the guidelines of client privilege.

V. GENERAL POLICY GUIDELINES

1. **Ownership**
   SBCERA has ownership and oversite of all technology assets owned or acquired by the organization and that is in use by Trustees or Staff. At any time SBCERA may require assets be returned, disposed of, or inspected. All data stored on an asset provided by SBCERA is the property of SBCERA. Trustees and Staff forfeit all rights to privacy and the personal data residing within an SBCERA technology asset.
   Staff members and Trustees using an SBCERA e-mail address should note all data associated with SBCERA e-mail addresses stored on any personal device is the property of SBCERA; this includes, but is not limited to, all e-mails, attachments, contacts, and calendar events. e-mail addresses not associated with SBCERA remain the property of the individual.
   SBCERA is the sole licensee of the software included with or added to any technology asset. Any copying, modifying, merging, or redistribution of the software by Trustees or Staff is prohibited. Any individual using a technology asset is responsible for complying with all hardware, software, and service provider license agreements, terms of use and applicable State and Federal copyright laws as well as any other intellectual property protections.
   It should also be noted any SBCERA technology asset may be subject to Public Records Act requests as well as confiscation and search per Government Code section 6250 et. seq. Nothing, personal or other should be considered confidential or protected when residing on an SBCERA technology asset, unless specifically identified as such within State or Federal law.

2. **Issuance**
    - SBCERA will issue technology assets based on business need, not personal preference.
    - Staff will be issued such technology assets as deemed necessary for them to fulfil their required job functions.
    - Upon assuming membership on the SBCERA Board, an approved mobile device for agenda management will be issued to each Trustee unless declined.
    - While issued, the security, care, and proper handling of each technology asset and information stored on said asset is the responsibility of each Trustee and Staff Member, respectively.
    - Upon the expiration of a Trustee's or Staff Member's service with SBCERA, all SBCERA technology assets provided to the individual shall be returned to the IS Dept. The asset(s) will be repurposed if still within the expected usefulness lifecycle, or disposed of if outside. The applicable policies and procedures governing the repurposes or disposal of technology assets shall be followed in either case.
3. **Liability**
   Trustees and Staff are solely responsible and liable for data sent by or stored on technology assets within their possession. The users accept responsibility for keeping the assets free from all inappropriate or potentially dangerous files and/or data and taking reasonable safety precautions with all technology assets and any potential confidential information that may be stored within. SBCERA technology assets are only authorized to be used by the Trustee or Staff Member assigned the asset. Group assets such as printers are the responsibility of all with access to said group asset.
4. **Asset Types**
   Technology assets potentially available for assignment will be grouped into the following categories including but not limited to desktops, printers, monitors, peripherals, desktop phones, cellular phones, tablets, laptops, and hybrids (laptop and tablet combinations). Due to security administration concerns, where possible, SBCERA will only make available assets from one manufacturer and in some cases only a single model from each of the categories, unless a specific business need cannot be met by the existing approved asset. This limitation of a single manufacturer per category is to ensure SBCERA can properly secure all potential confidential information that may reside on the technology asset.
5. **Asset Security**
   SBCERA technology assets including but not limited to servers, switches, desktops, and mobile devices, may have restricted security access enabled. Access to the asset will require the Trustee or Staff Member to provide a password, an authentication device such as a smart card, token, or physical recognition such as a fingerprint. Where applicable, two-factor authentication may be required to access the asset, and/or additional security may be required to access further data or applications.
   For security purposes, where possible SBCERA mobile devices will be wiped or otherwise rendered useless after limited number of failed attempts to gain access to the asset. Internal devices will "lock out" the user after a specific number of failed attempts, requiring IS Staff to "unlock" the device. SBCERA is not responsible for any loss, cost, or harm resulting from this action.

Mobile Devices such as laptops, tablets, and cell phones may have advanced security features such as VPN, connection policies and tracking enabled. These features are to help protect the device and the data stored within.

6. **Replacement / Damage / Loss**
    - Replacement of technology assets may take place from time to time due to wear and tear, damage, usage needs, technology updates, or changes to security requirements.
    - Technology assets may be covered by an extended protection plan. All technical, warranty, or repair issues shall be reported to the IS Dept. The Chief of IS or designee, shall, if applicable, notify the appropriate protection plan provider on any request for service.
    - Theft or loss of, or damage to an SBCERA technology asset must be reported immediately to the CEO or Chief of IS. In any of these instances the asset shall be locally or remotely sanitized (if capable), rendered useless (if capable), or otherwise have its access terminated for the purpose of removing or rendering inaccessible any sensitive or confidential data, and/or its access thereto.
    - The reimbursement for any technology asset due to theft, loss, or damage will be the sole responsibility of the issued user if it is determined that the user acted with negligence or recklessness regarding the care and safeguarding of said asset.
      Authorized Purposes
      Trustees and Staff may use technology assets for authorized purposes only. As set forth below, limited personal use of technology assets by Trustees and Staff during non-work time is considered an "authorized use" of technology assets, when such use:
    - Involves de minimis additional expense to SBCERA;
    - Is performed on the Staff Member's non-work time;
    - Are of reasonable duration and frequency;
    - Does not reduce productivity or interfere with the mission or operations of SBCERA;
    - Does not reduce the overall life cycle of the technology asset;
    - Does not reflect adversely on SBCERA; and
    - Does not violate any SBCERA policy, State or Federal law, or the ethical standards set forth by the organization.

7. **Business Use**
   SBCERA provides computing devices, networks, electronic information systems, and other technology assets to meet the mission and goals of the organization to provide services to the membership, plan sponsors, and other stakeholders. All technology assets are procured and configured solely to provide Trustees and Staff the means by which to meet these objectives.

8. **Personal Use**
   Limited personal use of technology assets is a privilege, not a right. Trustees and Staff have no inherent right to personal use of SBCERA technology assets. SBCERA provides the opportunity to Staff to use technology assets for personal use in an effort to create a more supportive work environment. However, this policy does not create a right to use SBCERA technology

assets for non-SBCERA purposes; nor does the privilege extend to modifying such assets, including loading personal software or making configuration changes. Additionally, the personal use of an SBCERA technology asset has the following restrictions:

- Trustees and Staff must be authorized to use technology assets for official SBCERA business before it is available for limited personal use.
- Managers, supervisors, and designated staff may further restrict personal use based on the needs of the organization/department or specific issues with inappropriate use.

9. **Privacy Expectations**
   Trustees and Staff do not have any right to, nor expectation of privacy while using any SBCERA technology asset including Internet or e-mail services. Furthermore, the use of SBCERA technology assets, for whatever purpose, should not be viewed as private, or anonymous. While using technology assets, usage may be monitored or recorded.

10. **Internet / Cellular Usage**
    SBCERA pays for a specific amount of bandwidth, which allows for the exchange of e-mails, phone calls, online research, the performance of certain job duties, remote access, virtual meetings, and the ability for the membership and plan sponsors to use SBCERA's online services. To protect SBCERA's networks and to ensure all business needs are met, the IS Dept. monitors and controls internet access. Due to this, internet usage from within SBCERA may be granted, denied, throttled, filtered, or time restricted. Additionally, Staff may have varying levels of access based on job need.
    Issued mobile devices will be Wi-Fi enabled by default, and at Board direction or CEO discretion, may have cellular carrier coverage (if capable). Given the number of mobile devices, all cellular enabled mobile devices will maintain a subscription with the same carrier network and data plan; except where a lack of coverage requires a different cellular carrier. The IS Dept. reserves the right to control the download speeds of any device deemed to be using excessive amounts of the allotted shared data to ensure all devices can maintain a reasonable download speed where applicable.

11. **Telephone Calls**
    Telephone calls made from SBCERA's phone system may be monitored or recorded for legitimate business purposes such as providing training, instruction or protection against abusive calls. As there is no distinction within the phone system between business or personal calls, all calls shall be handled with the knowledge the conversation is not private.
    SBCERA issued cellular phones will be subject to all State and Federal regulations. The ability to delete and/or recover any form of communication from said phones will be determined by the carrier's retention policies. SBCERA will not request early "permanent deletion" of any communication that took place on an SBCERA-issued cellular phone, nor will SBCERA attempt to block any valid public, law enforcement, or judicial request for communications stored on the cellular devices, or recoverable from the carrier if deleted.

12. **Electronic Mail (e-mail)**
    The e-mail systems' primary use is for SBCERA business-related purposes; and all messages sent, received, or stored are treated as such. SBCERA has the capability and reserves the right to access, review, copy, and delete any messages stored on the e-mail systems. Trustees and Staff should be aware that messages deleted are not immediately removed from e-mail systems and are subject to applicable record retention settings. SBCERA e-mail is like written

memoranda, and the public may have a right to see and obtain a copy of the messages on the SBCERA e-mail systems.

13. **Proper Representation**
    - Trustees and Staff shall ensure that personal use does not present the appearance of acting in an official SBCERA capacity.
    - The appearance of acting in an official SBCERA capacity includes endorsement or sanction of personal activities.
    - Disregard of section 14 may result in loss of use of technology assets, as well as other sanctions imposed in other SBCERA policies.

14. **Inappropriate Uses**
    The following is considered inappropriate use of SBCERA technology assets and is prohibited unless otherwise stated within this policy. Additional activities not list may also be determined as inappropriate based on applicable Federal, State, Local, and Organization laws, policies, and procedures.
    - Sending, receiving, or storing, greeting cards, videos, music, sounds, games, or other large file attachments that may hinder the performance of the network or other assets (e.g., servers, storage systems, network switches, applications, disaster recovery systems, cloud systems). Staff Members providing communications such as the Communications Section are exempt from this prohibition when performing official SBCERA business, unless the Chief of IS deems such actions are detrimental to the SBCERA network and/or system performance and security.
    - Subscribing to internet services that automatically download non-SBCERA business related data (e.g., sports scores, music, or other continuous data streams), unless approved by the Chief of IS.
    - Searching or using social media sites and applications for personal use including but not limited to Facebook, WhatsApp, Twitter, Instagram, Snapchat, Reddit, Pinterest, and TikTok. The use of LinkedIn for limited personal use is acceptable. Staff Members providing communications such as the Communications Section are exempt from this prohibition when performing official SBCERA business.
    - Loading personal software onto a technology asset or making configuration changes including but not limited to computer games, personal health programs, and messaging applications, unless the application/program has been approved by the IS Dept.
    - Installation of any applications or the purchase of any equipment resulting in a cost to SBCERA is prohibited unless approved by the CEO and the application(s) promote SBCERA's mission.
    - Making personal long distance telephone calls, except:
        a. In an emergency.
        b. Brief calls to locations that can only be reached during standard business hours (e.g., car repair shop, doctor).
        c. Brief calls to arrange transportation, or to check in with significant other or dependent.

- Using technology assets as a staging ground or platform to gain unauthorized access to other systems.
- Creating, copying, or transmitting chain letters or other mass mailings, regardless of the subject matter.
- Intentionally or unlawfully misrepresenting your identity or affiliation in electronic messaging communications.
- Opening or downloading any attachment from non-SBCERA owned or approved e-mail accounts or instant messaging service (e.g., Gmail, Yahoo, AOL, Hotmail, Whatsapp, or MSN mail).
- Clicking on any Hyperlink within an e-mail or dialog box from non-SBCERA owned or approved e-mail accounts or instant messaging service (e.g., Gmail, Yahoo, AOL, Hotmail, Whatsapp, or MSN mail).
- Causing congestion on the network by such things as the propagation of chain letters, junk e-mails, and broadcasting inappropriate messages to groups or individuals.
- Creating, copying, or transmitting any material or communication that is illegal or offensive to fellow staff or to the public, such as hate speech, or material that ridicules others based on race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- Viewing, downloading, storing, transmitting, or copying materials that are sexually explicit or sexually oriented, related to gambling, illegal weapons, terrorist activities, or any other prohibited activities.
- Using technology assets for any outside employment, businesses activities, or non-profit activity (e.g., selling real estate, preparing tax returns for a fee, maintaining an online business, etc…).
- Engaging in any outside fund-raising activity, endorsing any product or service, or participating in lobbying or prohibited partisan political activity (e.g., expressing opinions about candidates, distributing campaign literature), except as such may be specifically permitted under Board General Policy 016 – Solicitation Policy
- Acquiring, reproducing, transmitting, distributing, or using any controlled information including computer software and data, protected by copyright, trademark, privacy laws, other proprietary data or material with other intellectual property rights beyond fair use, or export-controlled software or data.

VI. SECURING CONFIDENTIAL INFORMATION

Confidential information presents certain risks to the organization. SBCERA technology assets may contain such confidential information. The loss, compromise, or misuse of said technology assets may expose members' personal information and / or other confidential information to unauthorized persons. General oversight and direction for the securing of confidential information residing within an SBCERA technology asset will be the responsibility of the IS Dept., unless otherwise directed by the Board or CEO.

- Technology assets will contain only enough confidential information to permit SBCERA staff,

Trustees, applications, and systems to support SBCERA's mission.

- When traveling with confidential information, the following steps must be followed:
    a. The person in possession of confidential information must be aware of the type, reasonable amount, and location at all times.
    b. The only approved medium for transportation of confidential information outside of approved mobile devices are SBCERA supplied Federal Information Processing Standard (FIPS) Compliant devices.
    c. Users MUST take all reasonable precautions to protect any device containing confidential information for which they have been provided or given access to.
- Should the need arise to transmit confidential information over an unsecured channel such as e-mail, the confidential information MUST be secured using an IS Dept. approved method. Any password, encryption key, or similar information needed to view the confidential information cannot be part of the same transmission as the confidential information.
- No Personally Identifiable Information (PII) should ever be transmitted in an unsecured manner. Safeguards and requirements for handling Personally Identifiable Information (PII) can be found within applicable internal SBCERA policies and procedures.

Exception: Due to the nature and types of confidential information used by the various departments, as well as many laws and regulations governing SBCERA, each department may need to retain and make accessible more confidential information than otherwise deemed permissible by this policy, or corresponding procedures. Each Department Chief with the approval of the CEO may implement confidentiality requirements for certain data elements within their business which potentially supersede applicable sections of this policy or corresponding procedures. However, if doing so creates security risk, said risk must be mitigated to industry acceptable standards.

VII. CONNECTION TO SBCERA NETWORKS

A Cybersecurity breach is an ever present risk to the organization. SBCERA has assets that connect to its networks and systems from internal and external locations. Additionally certain vendors and approved third party entities may request to connect to its networks for limited durations. Said connections must be approved, secured, monitored, and controlled by the IS Dept. As such the following requirements must be met prior to any asset or authorized device establishing a connection to any SBCERA networks, or systems.

1. The request for Vendors or third-party entities to access SBCERA secured networks must be made to and approved by the IS Dept.
2. Only assets that are part of SBCERA device management solution are allowed access to the secured networks and systems except when vendors or third parties have been granted limited duration access or an asset has been provided access for a specific task.
3. The device must meet SBCERA security policies and procedures .
4. The user/operator must be identified by name and contact information provided to the SBCERA IS Dept.
5. All non-SBCERA devices with access to the secured networks must have security that restricts

access to the device based on at least one of the following authentication methods.

- Multi-Factor Authentication (preferred)
- Something you know (e.g. a password)
- Must be complex (if capable)
- Must be a minimum of eight (8) characters in length
- Something you have (e.g. a smart card)
- Something you are (e.g. a fingerprint)

1. The user/operator must be given a copy of and become familiar with this policy and any applicable connection procedures.
2. All devices with access to SBCERA's secured networks are subject to a software audit at any time to ensure no program is in operation that could compromise the security and integrity of SBCERA's secured networks.
3. Only one non-SBCERA issued asset shall be approved per user for limited duration access.
4. Only the approved resource(s) can be accessed by the Trustees, Staff Members, Vendor(s), or third party entities.
5. Access rights to the SBCERA secured networks are nontransferable and restricted to the approved user and device(s).
6. Any Trustees, Staff Members, Vendors, and third party entities remotely connecting to SBCERA's secured networks, must use an IS Dept. approved connection method.

VIII. MONITORING AND ENFORCEMENT

The SBCERA IS Dept. maintains general oversight of all technology assets and their acceptable uses, except where otherwise directed by the Board or the CEO. Any unauthorized or inappropriate use of technology assets will be reported to the CEO. Should the unauthorized or inappropriate use be carried out by an SBCERA staff member, the CEO will determine appropriate action(s) including but not limited to the loss or limitation of the Staff Member's privilege of limited personal use, or use of the asset in totality, and/or discipline up to and including termination. Should the unauthorized or inappropriate use be carried out by an SBCERA Trustee, the CEO shall notify the Board Chair of the situation. Should the unauthorized use be carried out by the CEO, the matter shall be reported to the Chief Counsel, who shall consult with the Board Chair to determine what action, if any, is appropriate. Any unauthorized or inappropriate use may result in disciplinary action, and all may face criminal penalties or financial liability, depending on the severity of the misuse.

Approval Signatures

Step Description	Approver	Date

HR Final Review & Distribution	Iliana Torres	3/2/2022
	Iliana Torres	3/2/2022

Applicability

SBCERA, SBCERA Internal