Status Draft PolicyStat ID 18110305

San Bernardino County Employees' Retirement Association

Origination	11/2/2017
Last Approved	1/6/2022
Effective	8/6/2025
Last Revised	1/6/2022
Next Review	8/3/2028
Area	General
Applicability	SBCERA systemwide

SBCERA Technology Assets

POLICY NO. 019

I. PURPOSE

To establish clear standards for the proper use and security of SBCERA technology assets and access to SBCERA's secured networks and systems by both SBCERA staff and trustees.

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 applies to all technology assets owned, operated, leased, or contracted by SBCERA.

IV. DEFINITIONS

- Technology Assets: All hardware, software, data, and related resources used by Trustees and Staff under IS Dept. oversight.
- Data: Any electronic file or information.
- Personal Use: Non-official use during non-work time with minimal cost.
- Inappropriate Use: Any use violating SBCERA policy, law, or regulation.
- Mobile Device: Portable devices for SBCERA use or access.

- Confidential Information: Any sensitive, proprietary, or personally identifiable information.

V. GENERAL POLICY GUIDELINES

This policy establishes the standard security measures and expectations for SBCERA's technology assets. The Information Services (IS) Department maintains additional procedures and guidelines to support the secure operation of these assets and to protect SBCERA's networks, data, and systems. The Chief Executive Officer (CEO) or their designee is authorized to adjust these measures as necessary to address emerging threats or operational needs, ensuring the ongoing security of SBCERA's technology environment.

1. **Ownership**
   All SBCERA technology assets and data are SBCERA property. Use of SBCERA e-mail, software, and hardware must comply with licensing, copyright, and relevant laws. Assets and data may be subject to inspection, search, or disclosure under law.
2. **Issuance**
   Assets are issued for business needs. Staff and Trustees must secure and return assets upon separation. Assets will be repurposed or disposed of in accordance with applicable policies and guidelines
3. **Liability**
   Users are responsible for safeguarding assigned assets and any stored data, ensuring protection from inappropriate use or compromise.
4. **Asset Types**
   Technology assets potentially available for assignment will be grouped into the following categories including but not limited to notebooks, printers, monitors, peripherals, desktop phones, cellular phones, tablets, desktops, and hybrids (notebook and tablet combinations). Due to security and administration concerns, assets will be limited to select manufacturers and models, unless a specific business need requires an alternative selection. This limitation ensures SBCERA can properly secure and administer all technology asset.
5. **Security**
   All assets must have appropriate security controls, including authentication, encryption, and, where applicable, multi-factor authentication. Lost or compromised assets must be immediately reported for sanitization or access termination.
6. **Replacement / Damage / Loss**
   Damaged or outdated assets may be replaced. Negligence resulting in loss or damage may result in reimbursement obligations.
7. **Authorized Purposes**
   Assets are for official SBCERA business. Limited personal use is permitted if it:
   - Occurs during non-work time,
   - Incurs no significant cost,
   - Does not interfere with duties or security,
   - Does not violate any policy or law.
8. **Personal Use**
   Personal use is a privilege, not a right, and may be further restricted by necessary policies, procedures, guidelines, and management.
9. **Privacy & Monitoring**

There is no expectation of privacy. SBCERA reserves the right to monitor, access, and disclose communications or data on SBCERA systems. Any personal or business use of SBCERA systems may be subject to disclosure under the California Pubic Records Act.

10. **Network & Internet**
    Access to SBCERA's network must use approved secure solutions. Internet and cellular usage is monitored and managed by the IS Department to protect network integrity. Bandwidth and access may be restricted based on business needs.

11. **Telephone & Email**
    Business calls and e-mails may be monitored, recorded, and disclosed as public records where required by law. Personal call on SBCERA phones must be minimal and necessary.

12. **Proper Representation**
    Trustees and Staff shall ensure that personal use does not present the appearance of acting in an official SBCERA capacity or imply SBCERA endorsement.

13. **Prohibited Uses**
    Prohibited activities include, but are not limited to:

    - Sending or storing large non-business files.
    - Streaming or subscribing to non-business services.
    - Personal use of social media (except business approved).
    - Installing unauthorized software or hardware.
    - Using assets for outside employment or political activity.
    - Accessing, transmitting, or storing illegal or offensive material.
    - Misusing assets for unauthorized system access or misrepresentation.

VI. SECURING CONFIDENTIAL INFORMATION

Confidential information must be stored and transmitted securely, using only SBCERA authorized devices and secure methods. Transport and handle confidential data with care, following IS Department guidelines. PII must never be sent in an unsecured manner.

VII. CONNECTION TO SBCERA NETWORKS

Devices connecting to SBCERA networks must:

- Use approved secure access solutions.
- Be IS Department-managed or specifically approved.
- Meet all security requirements.
- Be subject to audit.
- Have access restricted to authorized users and resources.

VIII. ENFORCEMENT

The SBCERA Information Services Department oversees compliance, in consultant where

needed with Human Resources and the CEO. Violations may lead to disciplinary action, loss of access, termination, or legal penalties, as applicable.

Approval Signatures

Step Description	Approver	Date
HR Final Review & Distribution	Iliana Torres	3/2/2022
	Iliana Torres	3/2/2022

Applicability

SBCERA, SBCERA Internal