Status **Active** PolicyStat ID **17257878**

Origination	12/2024	Chapter Lead	Nohemy Ornelas: Chapter 3(CC),4&5
Last Approved	12/2024	Policy Area	Chapter 3 General Institution
Effective	12/2024	References	Non CCLC
Last Revised	12/2024		
Next Review	12/2034		

AP 3728 Information Security Physical Security

1. PURPOSE AND SCOPE

   All San Bernardino Community College District (SBCCD) information systems must be properly protected from potential physical and environmental threats to ensure the confidentiality, integrity, and availability of the data contained within. This Administrative Procedure describes physical access methods, visitors, data center security, and media disposal.

   This is one of a series of information security Administrative Procedures maintained by the District Information Technology (IT) department designed to protect SBCCD information systems.

   Please refer to AP-3725–Information Security Program Overview for information on the assets' applicability and application to employees and external parties.

2. PHYSICAL SECURITY

   All SBCCD technology locations will employ security control measures to prevent unauthorized physical access, damage, or interference to the premises and information.

   a. Physical Security Responsibilities

      i. The Campus Police departments manage perimeter security for the colleges and District offices. This group has physical keys to buildings and a master badge allowing access to all facilities.

      ii. District IT is responsible for the data center at each location. District IT approves access to the District IT- data centers.

b. Access Cards and Visitors to SBCCD Data Centers

District IT offices and secure areas are protected by entry controls designed to allow only authorized personnel to obtain building access. Authorized individuals may be issued an Employee, Temporary, or Visitor badge that enables electronic access to exterior doors and authorized internal doors. Additional authorization may be required for access to some doors.

Employees and visitors to SBCCD District IT facilities must clearly display ID badges at all times. Employees must be alert for unknown persons without badges, or employees not displaying badges.

District IT visitors must be provided with a badge or keycard that expires and identifies the person as a non-employee. SBCCD personnel must escort visitors. Visitors may be required to surrender badges after leaving the facility or at the date of expiration.

c. Data Center Access

The District IT and College data centers are critical processing facilities that must be protected by defined security perimeters with appropriate security access controls.

All persons who do not have a badge that requires access to the data center must be escorted by an employee whose badge is authorized to access the data center. Approval is required from the District IT and/or college management prior to any access to this area.

An authorized District IT employee is responsible for making sure that visitors entering a SBCCD data center are properly logged. It is mandatory that all visitors check in with District IT reception or college Technology departments, and visitors to a SBCCD data center must sign in and sign out with District IT and/or college Technology Department reception so that the entry and purpose of the visit can be tracked for auditing and security purposes.

For data center visitors, the reception log must note the name, date, company, purpose of visit, any escorting employee, and both sign-in and sign-out times. Spot checks of the log may be performed by District IT and/or college Technology departments and matched against the audit trail of door accesses from the keycard badging system. Reception area visitor logs must be retained for three months.

For audit and compliance purposes, the District IT management and/or college Technology department management will review those authorized to access an SBCCD data center at least quarterly to ensure that the privileges of employees or vendors who no longer need access to the data center have been removed. Records of these reviews will be maintained for audit purposes.

d. Equipment Maintenance and Environmental

District IT and college Technology departments must ensure that all utilities (e.g.

UPS, generator) and other equipment is monitored in accordance with manufacturer specifications and correctly maintained to ensure the availability, integrity and confidentiality of information contained within it.

The typical data center should have dry pipe water fire suppression, HVAC units, environmental protection, redundant UPS systems, and an exterior backup diesel generator.

Only authorized maintenance personnel are allowed to perform repairs. All repairs or service work must be documented. Documentation records must be maintained by District IT and/or college Technology departments.

Computer room personnel must be trained in the use of any automatic fire suppression systems, the use of portable fire extinguishers and in the proper response to smoke and fire alarms.

Smoking, drinking, and eating in computer processing rooms is prohibited.

e. Media Disposal and Destruction

District IT and/or College Technology Departments must ensure that electronic information storage devices (e.g., hard drives (spinning, ssd, m.2, etc.), tapes, USB sticks, removable hard disks, floppy disks, CD's and DVD's) are disposed of in a manner commensurate with their information classification.

All electronic storage devices must be wiped by a process such that data on the storage device cannot be recovered by individuals and/or technology.

External firms responsible for disposing of any type of SBCCD information must be held to any standards specified by contract. This includes confidentiality agreements and adequate security controls.

All Data Owners must ensure that media containing Restricted data is destroyed when it is no longer needed for business or legal reasons.

Employees must use proper destruction methods when disposing of SBCCD information. Paper copies of sensitive information must be shredded or incinerated. Users of the information are responsible for disposing of it in secure disposal containers or using another proper destruction method.

f. Payment Card Industry (PCI) Requirements

Refer to AP 3737 Information Security - Payment Card Industry Requirements (PCI)

g. Policy Enforcement

Any person found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including loss of access rights or termination of employment.

References:
NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
HIPAA Security Rule 45 C.F.R. §§ 164.310(a)(2)(ii), 164.310(a)(2)(iii)
PCI DSS Requirements and Security Assessment
Procedures: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
PCI DSS Quick Reference Guide Version
3.0 https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3.pdf

Approval Signatures

Step Description	Approver	Date
Approved per Level 2 process in AP 2410	Kelly Goodrich: PPAC Support	12/2024