Status **Active** PolicyStat ID **17258043**

Origination	12/2024
Last Approved	12/2024
Effective	12/2024
Last Revised	12/2024
Next Review	12/2034

Chapter Lead	Nohemy Ornelas: Chapter 3(CC),4&5
Policy Area	Chapter 3 General Institution
References	Non CCLC

AP 3730 Information Security Remote Access

1. PURPOSE AND SCOPE

   The objective of this Administrative Procedure is to control access to the San Bernardino Community College District (SBCCD) information and systems when connections are made to those systems from a remote location.

   This is one of a series of information security Administrative Procedures maintained by the Technology and Educational Support Services department designed to protect SBCCD information systems.

   Please refer to AP-3725-Information Security Overview for applicability of assets application to staff, and external parties.

2. REMOTE ACCESS

   All connections into and out of the internal network must be documented and managed by District IT and/or college Technology departments. Remote access is not automatically provided to all personnel and must be requested and approved as described below. The exception to this is access to the Student Information System (SIS) through the Colleague Self-Service and WebAdvisor using an Internet browser. Access to these systems is authorized for both employees and students, based on their job function and role, using assigned credentials and passwords.

   Users must use established remote access mechanisms or gateways to District systems. Aside from the Colleague Self-Service and WebAdvisor, SSL VPN is used to gain access to SBCCD systems.

Remote access to District financial systems requires two-factor authentication and is granted based on the employee's job function and role, using assigned credentials and passwords.

Remote access is prohibited from any public or shared computer or Internet kiosk. This would include public computers provided for open use in a library, hotel, conference center, or any location that provides open access to a computer.

Users may not establish new remote access systems or methods unless approval has been granted, as noted below.

All remote access will be audited annually by District IT management and/or college Technology department management.

a. Request for Remote Access

   Users create service desk tickets to request remote access. Refer to the AP-3727 Information Security - Access Control for further information.

b. Approvals for Remote Access

   General remote access: For college employees, remote access must be approved by the college President or designee. For District Services employees, remote access must be approved by the Chief Technology Officer and Technology and Educational Support Services or designee.

   New remote access methods: District IT must approve any new remote access method or system.

c. Access Controls for Remote Connections

   Remote access sessions will be automatically disconnected after 30 minutes of inactivity. Personal firewall software must be installed on all SBCCD or employee-owned computers with direct connectivity to the Internet that are used to access a District network. Anti-virus software must also be installed and must include the most recent software updates and virus profiles.

   Any remote access connection that has been established for a vendor, business partner, or other third party for purposes of support must be immediately deactivated once no longer in use by the appropriate IT staff.

d. Transmission Over Networks

   If SBCCD Restricted data is to be transmitted over any communications network, it must be sent only in encrypted form. Networks include SBCCD email mail systems, connections using the Internet, and supplied SBCCD remote access systems. All such transmissions must use software encryption approved by the District IT department. For further information, refer to the AP-3726 Information Security—Data Classification.

e. Payment Card Industry Considerations

SBCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI). Where cardholder data is present, remote access to those systems must incorporate two-factor authentication. This refers to network-level access originating from outside the SBCCD network to the SBCCD network by employees and third parties.

Personnel accessing cardholder data via remote-access technologies are prohibited from copying, moving, and storing cardholder data onto local hard drives and removable electronic media unless explicitly authorized by the Vice Chancellor of Technology and Learning Services for a legitimate business need.

3. REGULATION COMPLIANCE

The SBCCD IT team will verify compliance with this policy through various methods, including but not limited to periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate asset owner.

a. Exceptions

Any exception to this regulation must be approved in advance by the college president or designee for college employees or the Chief Technology Officer for the District employees.

b. Non-Compliance

An employee found to have violated this regulation may be subject to disciplinary action, up to and including termination of employment.

4. RELATED STANDARDS, POLICIES, AND PROCESSES

Please review the following regulations and guidelines for details of protecting information when accessing the network via remote access methods and acceptable use of SBCCD's network:

- Administrative Procedure 3720 Electronic Communications

Reference:
NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)
Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

Approval Signatures

Step Description	Approver	Date

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