Status **Active** PolicyStat ID **17257736**

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 3727 Information Security Access Control

1. PURPOSE AND SCOPE

   The objective of this Administrative Procedure is to provide internal controls for access to the San Bernardino Community College District (SBCCD) sites, information, and applications. This administrative procedure (AP) is part of a series of APs governing the secure use and access of Information Technology Systems and Services.

   Access controls may be physical (such as locks and badges), administrative (such as the AP to safeguard passwords), or technical (protections enforced by software settings or privileges). These controls are designed to allow or restrict the ability to view, update, or delete information within the SBCCD networks and systems or paper documents.

   a. Applicability of Assets
      The scope of this AP includes all electronic assets owned or leased by SBCCD.
      i. Assets may include but are not limited to:
      ii. Desktop and Laptop computers
      iii. Mobile Devices
      iv. Servers
      v. Network Infrastructure
      vi. Electronic Media
      vii. Mobile Computing Devices

   b. Applicability
      This AP applies to all SBCCD employees, including consultants, contractors, temporary employees, and volunteers.

c. Applicability to External Parties
This AP applies to all external parties, including but not limited to SBCCD business partners, vendors, suppliers, outsourced service providers, and other third-party entities with access to SBCCD networks and system resources.

2. ACCESS CONTROL

a. Access Control Principles
There are three basic access control principles at the SBCCD:

i. All information is made available only to those with a legitimate “need-to know”. Access is provided on this basis, guided by job requirements and data classification.

ii. Access controls for SBCCD systems will be provided in a manner that promotes individual accountability. Audit trails and monitoring of access establishes accountability and allows for follow-up of access violations and security breaches.

iii. Users with the highest levels of privilege on a computer system will be restricted to the least privileges necessary to perform the job.

b. Authentication to District Systems
Authentication is the verification of a user's identity. All individuals require identification (ID) prior to gaining access to secured SBCCD facilities or systems such as server rooms, cash handling rooms and other areas where security is in the interest of the District.

Internal (SBCCD personnel) and external (non-personnel) users must provide a valid and unique user ID in order to authenticate to the network. In addition to a unique ID, the authentication method must include at least one of the following:

i. A password or passphrase;

ii. Token device or smart card; or

iii. Biometric.

If the new user is a contractor or non-employee, the user ID will be identifiable as such by its naming convention.

Group, shared, or generic accounts do not provide accountability and are not to be used for network or application authentication. Some exceptions may apply to this requirement, such as a system account that is required for server or network processing or an account that is to be used by departments that would be used as an official communications account.

Physical access to secured facilities requires that SBCCD users possess appropriate access badges or credentials in order to enter all sites. Some areas, such as computer rooms, may require additional access levels, cards or keys. Refer to the AP-3728: Information Security - Physical Security for specific information.

c. Authorization to Applications
Addition, modification, and deletion of user IDs and other credentials must be controlled. Data Owners (or their designees) have the responsibility for making security decisions about applications that process data for which they are responsible.

Assuming the role of the Data Owner may require:

i. Approving and re-certifying access by users to systems or data they control, or

ii. Classifying data belonging to the application system they manage (determining the level of confidentiality or classification that should be assigned to an application's data, which will dictate its level of protection).

Access to certain functions may be provisioned automatically based on job position. Otherwise, the appropriate IT department, as authorized by Data Owners, must approve all new accounts. Each request for access must contain written and/or electronic evidence of approval by the Data Owner, District IT, or college Technology Services. Extension authorizations for contractor accounts must be applied by District IT or college Technology Services to provide an audit trail.

Access requests must specify access either explicitly or via a “role” that has been mapped to the required access. Outside of initial standard network access provided based on the job position of the users, access to additional applications or capabilities is discretionary and must be both requested and approved by the Data Owner. For additional access, users should submit an access request.

Departmental security administrators, as defined below, may set up access for some applications. District IT will pass the request on to the relevant team to set up access.

Remote access is not automatically provided to all users and must be requested and approved. Refer to the AP-3730: Remote Access for additional information.

The District IT or college Technology Services departments will maintain for a minimum of six (6) years logs or other documentation of all access request approvals, user account creations, modifications, and deletions.

3. SECURITY ADMINISTRATORS

The appropriate District IT or college Technology Services department is responsible for administering overall system access within SBCCD, and so may request information from appropriate managers or administrators, such as who has access to their applications, and the procedures that they have put in place to provision them.

Some users (in District IT, college Technology departments, or business departments) may

have a higher level of access privilege in order to administer systems or applications. They may have the ability to add, modify, or delete other users for the applications they control. To maintain system access to District-owned or developed software, District IT or the college Technology departments shall be provided an Administrative Account that will be used for recovery and auditing elevated access periodically.

Systems administrators and network technicians, under management supervision, have a responsibility to maintain appropriate access controls for the applications they maintain in order to protect information from unauthorized access. The number of administrators should be tightly controlled and limited to as few as necessary.

Security administrators should have their accounts set up with the proper access and log in with their accounts to conduct any privileged access. A log should be kept to review any privilege access and changes, and a report should be delivered and reviewed periodically each year by the Security Director and college Technology Directors. Security administrators should only use their privileged accounts to carry out administrative tasks that require privileged access. A non-privileged account should be used to perform routine tasks.

4. PASSWORDS

Users of the SBCCD computer systems will be provided with one or more unique accounts and associated passwords.

Users are accountable for work performed with the account(s) issued to them and are responsible for the confidentiality of their passwords. Passwords must be difficult to guess and kept private, and users must not disclose their passwords to anyone.

The following rules apply to password composition:

i. Must not be left blank when a new account is created. New passwords must not be the same for all users;

ii. Must have a minimum length of eight (8) characters;

iii. Must contain both numeric, special, and alphabetic characters /be alphanumeric and contain one upper case letter;

iv. New passwords must be changed immediately upon first use;

v. New passwords must not be the same as the four previously used passwords or used within a one-year period, and Passwords must be changed at least every 90 days (some passwords within IT are exempt from this requirement).

If a user requests a password reset via phone, email, web, or other non-face-to-face method,

Administrators who can reset passwords must verify the user's identity, such as by providing personal information, before changing the password.

5. ACCOUNT LOCKOUT

Accounts will be locked after six (6) invalid login attempts. Once an account is locked, an

authorized District IT or college Technology department staff, automated recovery system or authorized student services representative is required to reset the account after the user's identity has been verified. The lockout duration will be set to a minimum of 30 minutes or until an administrator enables the account.

Faculty classroom/lab workstations have a session idle time of 30 minutes after which the session will be locked. With the exception of some system accounts, all other user accounts have a session idle time of 15 minutes, after which the session will be locked.

6. EMERGENCY ACCOUNTS

   An Emergency Account / User ID will be established when access is needed to diagnose or correct a problem. The request to create the Emergency ID must be made through the appropriate college Technology Director, District IT manager, or administrator. The ID will be enabled only for a 24-hour period unless a specific time period is requested.

   Upon completion of the work, the requestor must inform the appropriate college Technology Director or District IT manager so that the ID can be disabled.

7. TERMINATION OF ACCESS PRIVILEGES

   Supervisors are responsible for notifying Human Resources if personnel will be leaving SBCCD or, in some cases, those who are placed on administrative or extended leave . HR will contact District IT and other Security Administrators as required so that access may be removed. Access must be disabled immediately upon notification or at the end of the last day of work.

8. REVIEW OF ACCESS

   A bi-annual audit of computer resource authorizations to confirm that access privileges remain appropriate will be conducted by appropriate IT staff. After an additional sixty (60) days, inactive accounts will be purged. These requirements may not apply to certain specialized accounts (e.g., Windows Administrator, root). Student accounts maybe be exempt and regulated by the District established provisioning process.

   District IT and/or college Technology departments, working with HR, may periodically validate employment and may immediately suspend users who are on leave of absence or extended disability. At least annually, IT will request that Data Owners verify continued access by users with access to their applications. District IT, college Technology departments, and/or external auditors will periodically review security administration procedures for specific applications and may employ monitoring tools to audit and verify access controls.

9. PAYMENT CARD INDUSTRY REQUIREMENTS

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

References:

PCI DSS Requirements and Security Assessment Procedures:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
PCI DSS Quick Reference Guide
Version3.0: https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3.pdfNIST
SP 800-53 Rev. 4 AC-2, IA Family

HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)

Approval Signatures

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