Status Active PolicyStat ID 17258513

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 3734 Information Security Security Network Security

1. PURPOSE AND SCOPE

   The objective of this Administrative Procedure is to describe controls required to protect District information and systems. Network infrastructure must be configured securely in order to protect District systems and maintain network integrity and availability. Effective network security will reduce potential vulnerabilities and help to enforce secure access to District information and technology.

   This is one of a series of information security Administrative Procedures designed to protect District information systems. The District Information Technology (IT) department has a district-wide fiduciary responsibility to set, maintain, and ensure the provisions of this regulation. District IT accomplishes this through collaborative engagement with the campus Technology Services departments.

   a. Applicability of Assets

      This Administrative Procedure applies to all electronic assets that are owned or leased by the District, including but not limited to:

      - Servers
      - Network Infrastructure
      - Mobile Devices
      - Infrastructure as a Service or IaaS

   b. Applicability

      This Administrative Procedure applies to all full-time and part-time regular academic and classified employees, , such as short-term (temporary) staff, substitutes,

professional experts, Federal Work Study students, and student help, who are employed by, and volunteers who assist the District for meeting the needs of students.

c. Applicability and Related Documents

This Administrative Procedure applies to all external parties, including but not limited to District business partners, vendors, suppliers, service providers, and other third-party entities with access to District networks and system resources.

d. References and Related Documents

Please refer to the Information Security Administrative Procedures for additional information references, and definitions.

2. NETWORK SECURITY

District IT has primary responsibility for District network and security. District IT in collaboration with the college technology departments manages and administers campus infrastructure and network components. Senior Technology Support Specialists, supervised by the District Director Technology Services are the operational managers of district and campus firewalls and network equipment.

a. General Network Controls

System configuration standards are in place for critical network and server components that are managed by District IT and campus technology departments. Standards must address known security vulnerabilities and industry best practices and provide specifications for “hardening” the native operating system or platform from known security weaknesses.

District IT must maintain appropriate network documentation, including a high-level network diagram specifically noting inbound and outbound network connections. This must include wireless network components and show connections to all networks, any cardholder data Payment Card Industry (PCI) locations, and wireless networks.

Network diagrams and configuration details must not be disclosed to unauthorized parties unless identifying IP addresses and names have been removed. The data classification level for sanitized (IP addresses, server names, and other identifying elements removed) diagrams is Internal. Unsanitized network diagrams have a data classification of Restricted. Refer to the Administrative Procedure 3726: Information Security - Data Classification for classification requirements.

Only necessary and secure services, protocols, services/daemons, etc., should be enabled as required for the function of the system. For any required services, protocols, or services/daemons that are insecure, appropriate security features must be enabled. For example, secure technologies such as SSH, S-FTP, SSL, or IPsec VPN should be used to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.

Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be unsecure must be maintained by District IT or college Technology Services.

Vendor-supplied defaults must be changed before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

System security parameters must be configured to prevent misuse. All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers, must be removed.

Publicly accessible network jacks should be restricted to authorized systems.

b. External Connections and Firewalls

District IT management or campus technology management must approve all new external connections, inbound or outbound, to the District's internal network. All connections into and out of the internal network must be documented, managed, and internally coordinated.

Firewalls must be deployed to restrict inbound and outbound connections to the District's network.

New network connections requested to be allowed through District firewalls must be approved by District IT management or college Technology Department management and require a business case justification.

Ad-hoc modification of firewall rules can jeopardize the security of the District's network. Established change control procedures must be followed for all firewall changes.

Where technically possible, firewall rules should be tested prior to implementation.

A review of all firewalls and routers must be completed every six (6) months. This activity must include a review of the specific ports/services/protocols allowed into the environment and proper documentation of the review.

For specific processes and procedures, refer to AR 3731: Internally Developed Systems- Change Control and Firewall Security Departmental Procedures.

c. Wireless Security

Wireless connectivity is provided as a convenience for staff and students utilizing wireless implementation at SBCCD colleges and sites. Either a student or staff SSID must be entered to gain access. Refer to Wireless Security Departmental Procedures for additional information on using wireless services.

Any other permanent wireless network implementations must be approved by

District IT.

Wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings, must be changed prior to implementation.

District IT and college Technology Departments will test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.

i. Wireless Environments and PCI

Whenever possible, cellular networks must be used for wireless transmission of cardholder data.

Firewalls are installed between wireless networks and the cardholder data environment and configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

For wireless environments connected to the cardholder data environment or transmitting cardholder data, vendor defaults must be changed. This includes but is not limited to default wireless encryption keys, passwords, and SNMP community strings.

d. Encryption

Encryption scrambles sensitive information that is stored or transmitted electronically. Cryptographic solutions must adhere to international export laws or any applicable legal or regulatory controls. Encryption must be used at the District in the following situations.

i. Passwords

All passwords must be encrypted and unreadable. This includes password files for users, firewalls, routers, operating systems, applications, databases, and web servers. Password or credential files stored on third-party platforms must also be encrypted.

ii. Restricted Data

AP 3726: Information Security-Data Classification describes how data is categorized based on its sensitivity, need for confidentiality, or value to the District. Data classified as Restricted is the most sensitive category. Its unauthorized disclosure may violate regulations or standards, such as PCI, or contractual agreements with third parties or service providers.

Restricted data may exist in applications, databases, or files. Various access controls protect data when in its original location, but when copied, reproduced, or transmitted, the original protections are lost. However, the classification and level of protection for a data element must travel with it regardless of its location or format.

Storing Restricted data on unencrypted removable devices, personal drives, or various types of USB storage may expose sensitive or confidential data to unauthorized disclosure and is against District regulations. If transporting or storing restricted data, it must be on a removable device; users must work with District IT or campus IT to ensure the data is secure.

If Restricted data is copied from its original location (e.g., to other files, removable devices, or on backup media), it must be encrypted. If sent via e-mail or other transmission means on public networks, it must be encrypted. Refer to the Encryption Departmental Procedures for specific encryption methods and procedures.

iii. Remote Administrator Access

Remote access by security, system, or firewall administrators to perform maintenance or troubleshoot problems presents a greater security risk due to the elevated privileges these individuals possess. System Administrators must connect securely using the SSL VPN to ensure that communications with District networks from a remote location are over an encrypted channel. This includes any non-console administrative access. Two-factor authentication is required where technically feasible.

iv. Key Management

Key management procedures must be documented for all processes and procedures involving encryption keys, especially if used for cardholder data. PCI DSS requirements mandate strong keys, secure key distribution and storage, periodic key changes, and other requirements. Please refer to the Encryption Departmental Procedures for detailed information.

e. Scanning and Vulnerability Management

District IT and college Technology Departments must be informed of information security issues and vulnerabilities applicable to District computing systems. When security issues are identified, District IT is responsible for notifying appropriate personnel, including system and network administrators/technicians and college Technology Directors.

The primary method for identifying new threats as they arise will be through vendor and security Internet mailing lists. The District will identify and assign a risk ranking to newly discovered security vulnerabilities. As appropriate, platform hardening standards must be updated to reflect measures required for protection from any newly discovered vulnerability.

The District performs quarterly external vulnerability scans on critical systems and networks in scope for PCI compliance. External vulnerability scans are performed by an Approved Scanning Vendor (ASV) as designated by the Payment Card Industry Security Standards Council (PCI SSC).

The District performs internal vulnerability scans on a periodic (at least semi-annual) basis or after any significant network changes. Penetration tests must be performed at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include both network-layer and application-layer tests.

An annual process is in place to identify threats and vulnerabilities that result in a formal risk assessment.

f. Network Time Protocol (NTP)

   All critical system clocks and times must be configured to acquire, distribute, and store a consistent time. All District production systems must be configured to use one of the internal NTP servers to maintain time synchronization with other systems in the environment. Internal NTP servers will be configured to request time updates from the Internet site http://time.nist.gov. Client systems able to retrieve time settings from the NTP server will be limited through Access Control Lists (ACL). The NTP system will always run the latest available version of the software.

g. Payment Card Industry (PCI) Requirements

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

Approval Signatures

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