Status Active PolicyStat ID 19188192

Origination	10/2025	Chapter Lead	Brooke Quinones: HR Admin
Last Approved	10/2025	Policy Area	Chapter 3 General Institution
Effective	10/2025		
Last Revised	10/2025		
Next Review	10/2031		

AP 3737 Information Security Payment Card Industry Requirements

1. PURPOSE AND SCOPE

SBCCD adheres to the requirements of the Payment Card Industry Data Security Standard (PCI). The following additional requirements are
mandatory for systems that store, process, or transmit cardholder data. References to the relevant PCI section numbers are in parentheses after each requirement:

2. ACCESS CONTROL

i. Implementation of an automated access control system (7.1.4).

ii. The access control system must cover all (PCI) system components (7.2.1).

iii. The access control system must assign privileges based on job classification and function (7.2.2).

iv. The access control system must be set to a default “deny all” setting (7.2.3).

v. Render all passwords unreadable during transmission and storage on all systems components using strong cryptography (8.4).

vi. Set the lockout duration to a minimum of 30 minutes or until the administrator enables the user ID (8.5.14).

vii. Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users (8.5.16).

3. PHYSICAL SECURITY

i. Video cameras must be used to monitor individual physical access to areas where credit card data is

stored, processed, or transmitted.

ii. Physical access to publicly accessible network jacks must be restricted. Network ports for visitors should not be enabled unless network access is explicitly authorized by District IT or college Technology departments.

iii. Physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines must be restricted to those authorized to work with cardholder data.

iv. All media containing cardholder data must be physically secured. Media back-ups must be stored in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. These locations must be reviewed at least annually.

A. Internal or external distribution of any kind of media must be strictly controlled.
B. Media containing cardholder data must be classified so sensitivity of the data can be determined.
C. Secure couriers or other delivery methods that can be accurately tracked must be used.
D. Appropriate IT management must approve any and all media that is moved from a secured area (especially when media is distributed to individuals).

v. Storage and accessibility of media must be strictly controlled. Inventory logs of media must be maintained and inventoried at least annually.

vi. Media containing credit card data must be destroyed when it is no longer needed for business or legal reasons. a) Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.

vii. Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

4. LOGGING AND MONITORING

i. Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

ii. Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting servers.

iii. Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

5. INTERNALLY DEVELOPED SYSTEMS CHANGE CONTROL

- Development/test and production environments must be separate.
- Separation of duties between development/test and production environments.

- Production data (live PANs) are not used for testing or development.
- Removal of test data and accounts before production systems become active.
- Change control procedures for the implementation of security patches and software modifications must include the following:
    - Description of the impact of the change.
    - Documented change approval by authorized parties.
    - Functionality testing to verify that the change does not adversely impact the security of the system.
    - Back-out procedures.

6. NETWORK SECURITY

- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
- Firewall and router configurations must restrict connections between untrusted networks and any system components in the cardholder data environment. An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.
- Prohibit direct public access between the Internet and any system component in the cardholder data environment. Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment
- Implement a demilitarized zone (DMZ) to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. Limit inbound Internet traffic to IP addresses within the DMZ.
- Install a firewall at each Internet connection and between any DMZ and the internal network zone.
- Do not allow internal addresses to pass from the Internet into the DMZ.
- Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
- Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)
- Place system components that store cardholder data (such as a database) in an internal network zone.
- Where feasible, implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)
- Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises.
- Never send unprotected primary account numbers (PANs) by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).
- Use strong cryptography and security protocols to safeguard sensitive cardholder data during

transmission over open, public networks, including the following:

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to:
  - The Internet.
  - Wireless technologies, including 802.11 and Bluetooth.
  - Cellular technologies, for example, Global System for Mobile Communications (GSM), and Code Division Multiple Access
  - (CDMA).
  - ◈ General Packet Radio Service (GPRS).
  - ◈ Satellite communications.

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.pdf

Approval Signatures

Step Description	Approver	Date
Approved per Level 3 process in AP 2410	Brooke Quinones: HR Admin	10/2025