Coast Community College District
BOARD POLICY
Chapter 6
Business and Fiscal Affairs

BP 6905 Payment Card Industry Data Security Standards Compliance

References:
PCI DSS v3.2.1, PCI Security Standards Council

The District shall maintain compliance with the current version of the Payment Card Industry ("PCI") Data Security Standards ("DSS"). Any College or department that stores, processes, or transmits cardholder data in exchange for goods and services is responsible for facilitating the District's compliance and related responsibilities. "Cardholder data" is defined as the full Primary Account Number (PAN) on its own; or, the PAN in combination with any of the following: cardholder name, expiration date, or service code. Cardholder data applies only to payment cards bearing the VISA, MasterCard, American Express, Discover, or JCB logos.

Approved Methods of Payment Processing

Payment card processing must be done using a Merchant Identification (MID) number provided by the District's Credit Card Processor Heartland/TouchNet or other compatible partner with District-approved point of sale software. MID numbers will be assigned to a member of the associated College/business unit's management who will be responsible with facilitating the District's compliance with the PCI DSS for that MID.

Payment card processing must be performed in one of the approved payment channel types listed below which conforms with the associated PCI Security Administrative Procedure. These payment channel types include:

- In Person: card-present transaction through approved point-of-interaction devices.
- Mail Order/Telephone Order ("MOTO"): card-not-present transaction through approved third-party virtual terminals
- eCommerce: card-not-present transactions through an approved third-party payment page.

Cardholder data storage is not permitted after authorization of a credit card transaction. In the event that physical cardholder data is received (related to In Person or MOTO), destruction must occur immediately. Electronic storage of cardholder data is not permitted under any circumstances. This includes, but is not limited to, storage of cardholder data in e-mail or on District shared drives.

Maintaining Compliance

The Vice Chancellor, Administrative Services will facilitate an annual risk assessment

process with the College Vice Presidents of Administrative Services and the Executive Director Information Technology to identify critical assets, threats, and vulnerabilities related to currently approved payment channels. The results of the risk assessment must be formally documented and used to update applicable Board Policies and Administrative Procedures.

The College Directors of Business Services are responsible for ensuring College business unit management will maintain the following documentation:

1. Process specific procedures (e.g., payment processing, destruction, etc.)
2. Evidence of security awareness training for all applicable staff
3. Inventory of point-of-interaction devices (if applicable)

The District Information Technology Department will implement and maintain applicable technical security controls associated with approved payment channels or identified during the annual risk assessment process.

District Administrative Services will maintain a list of all applicable security controls in the form of a Prioritized Approach Tool provided by the PCI Security Standards Council ("SSC").

Annual Attestation of Compliance

On an annual basis the District will attest to compliance with the PCI DSS per the guidance of the PCI SSC. This assessment will be facilitated by Administrative Services leveraging appropriate District and College resources and using the guidance of the appropriate PCI SSC provided Self-Assessment Questionnaire ("SAQ"). Completed SAQ(s) must be signed by Vice Chancellor Administrative Services and provided to applicable stakeholders (e.g., acquiring bank, payment brands, etc.)

Exceptions identified during the annual assessment process must be tracked using the PCI Prioritize Approach Tool and assigned to appropriate individuals for timely remediation. The PCI Compliance Lead will track remediation and report status to the Vice Chancellor Administrative Services.

Exceptions

Exceptions to this Policy must be approved by the Vice Chancellor, Administrative Services, documented, and included in compliance, maintenance, and attestation processes described previously. College PCI Business Leads and associate business unit(s) will be responsible to monitor the cost of additional security controls needed to meet and maintain compliance beyond approved payment channels.

Adopted February 5, 2020