Coast Community College District
ADMINISTRATIVE PROCEDURE
Chapter 6
Business and Fiscal Affairs

AP 6905 Payment Card Industry Data Security Standards Compliance

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

Authority

The Vice Chancellor, Administrative Services is responsible for administering and amending (subject to ratification by the Board), as needed, this Procedure.

Definition

This Procedure defines the proper handling of credit card information, credit card reading devices, and PIN Transaction Security Devices used by the District. This Procedure is in conformance with the guidelines set forth within the Payment Card Industry Data Security Standards ("PCI-DSS") as well as good business practices related to the handling of credit card information, and represents the District's conformity to compliance requirements.

Responsibilities

It is the responsibility of all District employees who handle credit card transactions to ensure that credit card information, including cardholder data and Primary Account Number ("PAN"), and related devices adhere to:

Data Handling

1. Data will be treated as confidential.
2. Data that is not absolutely necessary in order to conduct business will not be retained in any format (e.g., paper or electronic).
3. District employees will not accept, request, or retain credit card data via e-mail or other electronic means.
4. If District employees receive credit card data in an email, they will contact the IT Help Desk immediately to have the message removed from District computers and the District email system. The employee also will notify the sender of the email that the District does not accept credit card information via email and that it should not be attempted again. The employee will not notify the sender using the Reply function in the email as this may inappropriately transmit credit card information.
5. District employees will not store any card-validation code (i.e., the three- or four-digit code) used to validate a card-not-present transaction, personal identification number ("PIN") or encrypted PIN block.
6. Account numbers will be masked if and when displayed (i.e., no more than the first six and last four digits of the credit card numbers).

7. District employees will notify District Fiscal Services before any new PIN Transaction Security Devices are placed in service.
8. District employees will review the PCI certification of every PIN Transaction Security Device in use annually and request replacement devices for any which are no longer certified. Devices must conform and be authorized for use by Heartland or other District contracted payment servicer. The list of certified devices is available at: https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php.
9. Physical access to records will be restricted to employees with a "business-need-to-know." Means such as locked file cabinets and restricted file rooms, as well as restricted distribution of such records, will be used.
10. The District will not maintain the credit card PAN data and will remove all credit card PAN information in a PCI_DSS approved manner.
11. If such data is shared with any external service provider, District Administrative Services will implement procedures to manage service providers with whom cardholder data is shared or that could affect the security of cardholder data, as follows:
    a. A list of providers is maintained;
    b. A written agreement is executed and retained which defines the provider's responsibility related to the security of this information;
    c. Any new service provider will be thoroughly vetted by departmental management, District Administrative Services, and others, as appropriate, before engagement to ensure that the provider can meet these requirements.
    d. Every service provider's PCI-DSS compliance status is reviewed on an annual basis. Instances of non-compliance are reported to the District Administrative Services personnel for assistance in determining appropriate follow-up actions.

College Procedures

(A) Device Inspection

Inventory and inspections of all PIN Transaction Security Devices are to take place at regular intervals, with no more than three months passing between inspections. Employees receive training on how to properly perform device inspections and to recognize signs of tampering. If signs of tampering or damage are found, appropriate steps are taken according to the incident response plan.

(B) System Configuration at the College Level

College Administrative Services will ensure, through working with the Information Technology Department and others, as needed, that all applicable requirements are followed, including, but not limited to:

- Anti-virus software will be implemented, updated, and run at regular intervals.
- Vendor patches will be installed on a timely basis.
- Access will be granted to systems only on a "business-need-to-know" basis.

- If external vendors need remote access to service District third-party software, their access will be granted only for the time needed to do the necessary task(s) and then will be immediately disabled.

(C) Processing

- College Administrative Services will make the refund policy available to all customers.
- No cash advance transactions are authorized.
- No cash back is authorized at the time of the original sale.

Ratified February 5, 2020