Yosemite Community College District Policies and Administrative Procedures **No. 6-8065**

Policy

6-8065 Payment Card Industry Compliance

Yosemite Community College District will comply with the Payment Card Industry Data Security Standards necessary to remain compliant and appropriately certified and will ensure that appropriate business practices and procedures as well as information security technology is implemented to retain certification and safeguard payment card data.

Whenever the District enters into a contract for the purchase, development, procurement, maintenance or use of any electronic or information technology, for the purposes of e-commerce functionality, the vendor shall certify that it complies with the requirements of Payment Card Industry (PCI) and its related regulations.

I. Definitions:

a. Payment Card Industry Data Security Standards (PCI-DSS): a set of standards established by the Payment Card Industry Security Standards Council to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

b. Cardholder Information Security Program (CISP): a program designed to ensure that all merchants that store, process, or transmit cardholder data, protect it properly by adhering to the Payment Card Industry (PCI) Data Security Standard.

c. Cardholder Information: any personally identifiable data associated with a cardholder or a payment card, for example, an account number, expiration date, name, address, social security number, Card Validation Code CVC 2 (MasterCard), Card Verification Value CVV2 (VISA), Card Member ID (Discover) or CID – Card Identification Number (American Express) (e.g., three – or four-digit value printed on the front or back of a payment card).

d. Point of Sale Terminal (POS-T): electronic retail payment device which (1) reads a customer’s bank’s name and account number when a bank card or credit card is swiped (passed through a magnetic stripe reader), (2) contacts the bank and (if funds are available) transfers the customer approved amount to the seller’s account, and (3) prints a receipt.

e. Credit Card: a plastic card issued to concede to the holder, upon presentation to authorized stores or service providers, products or services on credit.

f. Debit Card: a plastic card that may be used for purchasing goods and services or for obtaining cash advances for which payment is made from existing funds in a bank account.

g. “Need to Know”: access to the information must be necessary for the conduct of one’s official duties.

Adopted: July 9, 2014
Revision Adopted: December 11, 2020
Last Reviewed: December 11, 2020

Administrative Procedure

6-8065 Payment Card Industry Compliance

I. Procedures for Processing Payment Card Information:

a. Administrators of College Departments who need to accept payment cards and/or obtain a physical terminal to either swipe or key transactions through a point of sale terminal (POS-T) must request approval from the Chancellor or designee.

b. College and Central Services personnel assigned to process payment card transactions must receive training on the process to report and include those transactions in the District financial system.

c. College and Central Services personnel who accept payment cards must receive training on understanding the requirements of and compliance with the PCI-DSS standards.

d. College and Central Services personnel who accept payment cards must store only essential information. Each of the following must not be stored: the Card Validation Code, the PIN, and the full contents of any track from the magnetic stripe or chip associated with the card.

e. All media used for payment cards must be destroyed when retired from use. All hardcopy must be shredded using secure cross-cut shredded method prior to disposal.

f. Exceptions to this procedure may be granted only after a written request from the College or Central Services department has been reviewed and approved by the Chancellor or designee.

g. The Senior Director of Information Technology or designee will authorize access for positions that require specific levels of data access. For employees who do not need to have access to payment card account numbers, the numbers will be masked to protect account information.

h. Under no circumstances may payment card information be obtained or transmitted by e-mail, through campus mail or wireless networks. Payment card data transmission is permissible by fax.

i. Any changes to systems housing account information must only be performed when

i. Thorough testing has taken place to ensure adequacies of controls
ii. Functionality testing with module custodians and/or functional exports has taken place
iii. Change control processes have been followed

II. Procedures for PCI Data Storage and Destruction:

a. Hardcopy containing cardholder data shall be destroyed immediately after processing using secure cross-cut shredded method prior to disposal.

b. All electronic media containing cardholder information shall be labeled and identified as confidential.

c. An inventory of media containing cardholder information shall be performed quarterly.

d. Audit logs for system housing cardholder data shall be readily available for a period of 90 days. After 90 days, logs can be archived but must be maintained for one year.

e. Electronic backup media containing cardholder data shall be secured/encrypted and stored in a secure environment. Retention and destruction of electronic backup media is defined by Yosemite Community College District (YCCD) data retention program.

III. Procedures for Using Third Party and External Vendors:

a. Use of third party service providers for the purpose of payment card processing must be reviewed and approved by Chancellor or designee and the Senior Director of Information Technology or designee.

b. External service providers must be PCI-DSS compliant and provide current, certified proof of compliance upon request.

c. Contracts with external vendors must include language that requires vendors to demonstrate compliance with PCI-DSS if relevant to the services provided by the vendor. Contracts with external vendors must contain language that requires notification of any changes in PCI compliance status.

IV. General PCI Security Procedures:

a. Each employee with access to cardholder data electronically must have a unique password.

b. In accordance with the YCCD Information Security Program, cardholder data must not be stored on servers, local hard drives or external (removable) media including USB Flash drives and optical media unless encrypted and otherwise in full compliance with PCI-DSS.

c. All personal computers/workstations/laptops or other devices which handle payment card transactions must automatically have their screens locked after no more than ten (10) minutes of inactivity.

d. For a paper media (e.g. paper receipts, forms, and faxes), cardholder information should not be stored, unless approved for appropriate business purposes and access is limited to individuals with a business need to know. Cardholder data should be "blacked" out on paper media, and disposed of properly (e.g. cross-cut shredded) when no longer needed for business purposes.

V. College and Central Services Department Administrators Need to Ensure:

a. Only authorized personnel have access to payment card applications and data.

b. Payment card account numbers are properly secured and safeguarded.

c. Colleague accounts are properly reconciled with any discrepancies brought to the attention of Central Services Fiscal Services immediately. To maintain proper segregation of duties and minimize the risk of fraud, the individual administering Colleague shall not be the same individual that initiates, authorizes and processes the transactions.

d. Central Services Fiscal Services shall be notified immediately of any changes in a department’s card processing environment; including using the account for a new purpose, adding a new card acceptance technology or channel, or adding or customizing a payment application.

VI. The YCCD Central Services Fiscal Services Department will:

a. Provide training to ensure College and Central Services staff are accepting and processing payment cards in compliance with PCI-DSS standards.

b. Work with College department(s) and Central Services staff to create and test payment card applications before implementation.

c. Work with external vendors to ensure compliance with policies, practices, and procedures for accepting payment cards at the college.

d. Work together with Information Technology to complete the PCI-DSS Self-Assessment annually.

e. Verify annually that payment card applications are PCI-DSS compliant and, if applicable, on the Payment Application Best Practice (PABP) list.

VII. The YCCD Central Services Information Technology Department will:

a. Approve installation, modifications, and removal of all network hardware devices throughout the District.

b. Identify compliant application software or service providers with the required functionality to meet college business needs.

c. Ensure all physical network devices (e.g., routers, switches, wireless access points, and firewall configurations) and/or applications are properly secure.

d. Ensure all systems processing payment card transactions are segmented into the proper VLAN which properly segments and isolates all PCI traffic.

e. Perform approved scans on end user’s desktops/laptops to identify potential unsecure payment card information which violate the District Information Security Standard.

f. Arrange for an approved third-party company to conduct annual penetration tests and vulnerability scans on all systems processing payment card transactions and resolve any issues immediately.

g. Implement any and all identified precautions needed to safeguard all District payment card transactions in accordance with PCI-DSS.

h. Work together with Fiscal Services to complete the PCI-DSS Self-Assessment annually and coordinate with external scan vendor(s) quarterly to ensure PCI-DSS compliance.

i. If required, coordinate with approved PCI-DSS QSA vendors to verify PCI-DSS compliance.

VIII. Requirements for Breach Notification:

a. Any breaches, actual or suspected, of this procedure or any of the PCI-DSS standards shall be reported immediately to the Chancellor or designee and the Senior Director of Information Technology or designee.

b. In the event that a breach is suspected, the PCI-DSS Incident Response Plan will be followed until the incident is cleared or the plan has been followed through to completion.

Procedure Last Revised: ~~July 9, 2014,~~ December 11, 2020
Last Reviewed: December 11, 2020