(1) 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: 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.

(2) Procedures

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 must request approval from the Senior Vice President for Business and Administrative Services or his/her designee.

b. Department personnel assigned to process payment card transactions must receive training on the process to report and include those transactions in the College's financial system.

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

d. Department personnel who accept payment cards must store only essential information. The Card Validation Code or the PIN Number must not be stored nor should the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) be stored.

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

f. Exceptions to this procedure may be granted only after a written request from the department has been reviewed and approved by the Senior Vice President for Business and Administrative Services or his/her designee.

g. The Vice President of Information Technology or his/her 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

(3) The following steps must be adhered to for all data storage and destruction:

a. Hardcopy containing cardholder data shall be destroyed immediately after processing.
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 monthly.
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 Columbus State Community College's (CSCC's) data retention program.

(4) Use of third party service providers for the purpose of payment card processing must be reviewed and approved by Senior Vice President for Business and Administrative Services or his/her designee and the Vice President for Information Technology.

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

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

(7) In accordance with the College's Information Security Program, cardholder data should not be stored on servers, local hard drives or external (removable) media including floppy discs, CDs, and thumb drives unless encrypted and otherwise in full compliance with PCI-DSS.

(8) All Personal Computers/workstations/laptops which process payment card transactions must automatically have their screens locked after no more than fifteen (15) minutes of inactivity.

(9) For 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. shredded) when no longer needed for business purposes.

(10) 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 Business Services immediately. To maintain proper segregation of duties and minimize the risk of fraud, the individual administering Colleague is not the same individual that initiates, authorizes and processes the transactions.
d. Business Services is 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.

(11) The Business Services Department will:

a. Provide training to ensure College staff for accepting and processing payment cards in compliance with PCI-DSS standards.
b. Work with College department(s) 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. Verify annually that payment card applications are PCI-DSS compliant and, if applicable, on the Payment Application Best Practice (PABP) list.

(12) The Division of Information Technology will:

a. Approve installation, modifications, and removal of all network hardware devices throughout the College.
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 away from non-payment card processing systems.
e. Perform approved scans on end user's desktops/laptops to identify potential unsecure payment card information which violates the College's Information Security Standard.

f. Perform penetration tests and vulnerability scans on all systems processing payment card transactions and resolve any issues immediately.

g. Implement any and all precautions needed to safeguard the College's payment card transactions in accordance with PCI-DSS.

h. Complete the PCI-DSS Self Assessment yearly and coordinate with external scan vendor(s) quarterly to ensure PCI-DSS compliance.

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

(13) 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.

(14) The Privacy and Security Addendum must be signed by all external vendors that store, transmit, or use cardholder information.

(15) Any breaches, actual or suspected, of this procedure or any of the PCI-DSS standards shall be reported immediately to the Senior Vice President for Administrative Services or the Vice President for Information Technology.

New Procedures