Operating Instruction 7.3.17.1 Operating Instructions for Payment Card Acceptance, Processing, and Security

Part 1. Purpose
To ensure that a safe and secure environment is created and maintained for sensitive payment data (whether electronic or other form).

These operating instructions outline the general requirements for colleges, universities, and the system office related to establishing and maintaining procedures and controls for payment card processing compliant with Payment Card Industry Data Security Standard (PCI DSS).

Part 2. Definitions
A comprehensive glossary of terms and related definitions may be found at: PCI Glossary. The definitions below are those most likely to be useful to the reader of these operating instructions.

Payment Card Industry Data Security Standards (PCI DSS)
A set of global data security standards designed to protect payment card account numbers. Any payment card (credit, debit, prepaid, stored value, gift or chip) bearing the logo of one of five payment brands is required to be protected as prescribed by the standards. The brands are: American Express, Discover, JCB, MasterCard and Visa. PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If the PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply. Storage includes any type of paper or electronic recording.

Acquiring bank (or "acquirer")
A member of a bankcard association or a vendor that seeks and maintains a contractual relationship for payment card processing with merchants to accept the prescribed payment cards. For example, the state of Minnesota has a contractual relationship with an acquiring bank and the system colleges and universities use this contract for processing students' on-line tuition and fee payments.

Cardholder
A non-consumer or consumer customer to whom a payment card is issued or any individual authorized to use the payment card.

Cardholder data
The card's primary account number (PAN), a service code consisting of a three or four digit number in the magnetic strip on the rear of the card, the cardholder's name, and the expiration date of the card.

E-Commerce
Payment card transactions requiring use of a merchant website. Actual cardholder data entry generally occurs on a third-party payment card processing website, but the cardholder transfer from the merchant site to the processing site is seamless. Contrast with point-of-sale transactions where the cardholder is typically present with the payment card.

M**erchant**
An individual or organization, whether private or public, which provides goods or services, where payment options include customer use of a payment card. Each college or university may have multiple merchants. For example, two auxiliary locations on campus that accept payment cards but through different merchant agreements with different acquiring banks will qualify as two separate merchants for purposes of applying these operating instructions.

Point-of-Sale
A common form of payment card transaction where the cardholder and payment card are generally present at a merchant site (the "point-of-sale"). Card data is generally processed via keypad or through swipe of the card such that cardholder data is read electronically.

Transactions
Transactions to which PCI standards may be applicable include over-the-counter transactions, mail-in, fax and phone orders, internet (e-commerce) orders, sales draft requests, chargebacks and refunds.

Part 3. Campus Responsibilities

It is the responsibility of each college and university to establish and maintain written procedures applicable to payment card processes where payment cards are accepted on campus. Procedures must be compliant with PCI security standards and consistent with these instructions.

Subpart A. PCI standards

PCI DSS define requirements into six broad groupings or principles:

1. Build and maintain a secure network
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks

6. Maintain an information security policy (Board Policy 5.23 Security and Privacy of Information Resources and supporting procedures represent the primary source of system information security policy.)

- Full text documentation may be found at: PCI Security Standards
- Understanding the Intent of the Requirements Navigating PCI DSS
- Operating Instructions 5.23.1.10 Payment Card Technical Requirements

Subpart B. System standards
In developing its policy and procedure, each college, university, and the system office will need to address the following issues.

1. Define campus management for all payment card acceptance.
2. Include PCI compliance language in all relevant contracts.
3. Establish general procedures for current operations.
4. Adopt data security measures.
5. Meet documentation requirements.
6. Develop an incident response plan.

Part 4. Define Campus Management for all Payment Card Acceptance
If the system office, college, or university allows the addition of new merchants, it shall establish requirements for becoming a merchant that include, at a minimum:

Subpart A. Review and approval process
A procedure addressing the review and approval process governing the new merchant payment card acceptance structure. The procedure must include:

1. the formal merchant set-up requirements including an application and approval process;
2. the name and title of the campus-designated merchant approval officer with delegated authority to make the approval decisions;
3. a schedule of estimated costs for start-up processing and on-going maintenance;
4. a description of the minimum data processing and handling control requirements the merchant shall be able to meet. These should include adequate segregation of duties (for example, transaction processing, cash receipt and refunds), periodic reconciliations, oversight and review, and physical security. This should also address data safeguards from transaction initiation through secure storage and disposal or erasure of retained data.

Subpart B. Management responsibilities
The procedure must define merchant (or department) versus central campus management responsibilities and delineate how costs associated with both the establishment of the new merchant account and the associated compliance obligations are funded.

Subpart C. Merchant's role
The procedure must define the merchant's role for self-assessment, compliance documentation requirements, responsibilities for scanning if required, changes in PCI DSS requirements and/or remediation responsibilities in the event issues surface through self-assessment efforts, etc.

Subpart D. Additional requirements
Additional requirements may be necessary for a compliant merchant application and processing environment at the college or university. Examples would be unique merchant applications, unusual physical or other security considerations, etc.

Part 5. Include PCI Compliance Language Relevant to All Contracts
Colleges and universities shall include PCI compliance language in all relevant contracts. If the services sought under an RFP or procured under a contract involve the storage, processing or transmittal of payment card account numbers, the RFP and subsequent contract must address PCI responsibilities.

- PCI Guidance for Drafting Contracts
- PCI Amendment Template

Part 6. Establish General Procedures for On-going Operations
College and universities shall establish compliant procedures for continuing operations. These may vary by payment card transaction to comply with relevant data needs, documentation and compliance requirements.

Subpart A. Procedures common to all transaction types
1. Establish and follow merchant procedures addressing segregation of duties, reconciliations, physical security and disposal of cardholder data, as applicable.
2. Establish and follow basic cardholder data security steps regarding data acquisition, cardholder consent, physical and electronic security, limiting employee access, etc.
3. Adhere to training requirements, both initial and refresher.

Subpart B. Transactions where card is present (over-the-counter)
1. Establish cardholder requirements related to signature, transaction copy, ID check, etc.
2. Effectively safeguard data by printing last four digits of card number only and establishing procedures to secure data at every step: short-term storage and disposal (for example, until after reconciliation is complete), batching and reconciliation, etc.
3. Plan a secure back-up processing method, in the event processing terminal is not functioning, including additional or different security measures to be taken.

Subpart C. Transactions where card is not present (mailed, faxed or phoned)

1. Ensure internal payment reporting which supports accounting and reconciling needs but does not contain cardholder data (last four digits of card number may be included).
2. Ensure adequate physical security (for example, restricted access to fax machine, mail processing, phone conversations, etc.).
3. Process transactions promptly and safeguard secure storage of documents containing necessary cardholder data.
4. Enforce secure document disposal in accordance with campus retention and destruction policy (for example, applicable term plus one month but not to exceed six months subject to differing requirements imposed by law, regulation or contract on transactions).
5. Use adequate batch processing procedures.

Subpart D. E-commerce transactions

1. Limit processing to PCI DSS compliant third-party providers.
2. Ensure payment card data is not stored on campus servers or networks without approval by the chief information officer.
3. Comply with System and campus User ID and Password requirements.
4. Use only systems and technologies meeting all required security protocols.
5. Conduct quarterly vulnerability scans as required and implement remediation efforts on a timely basis.

Subpart E. Acquiring bank chargebacks and sales draft transactions

1. Identify responsible office on campus for control of timely and accurate response to requests for information in support of a questioned or disputed transaction
2. Responsible office will coordinate timely and complete response.
3. Maintain duplicate support material, including clear documentation of submission data.
4. Ensure secure storage of supporting material (if cardholder data is included), followed by secure destruction upon resolution of sales draft or chargeback transaction.

Part 7. Adopt Data Security Measures

Each college and university shall adapt physical and IT security measures sufficient to satisfy payment card processing requirement contained within PCI DSS. Board Policy 5.23 Security and Privacy of Information Resources and supporting procedures represent the primary source of system information security policy. Each college and university shall implement local policies and procedures as necessary to address additional security needs that are unique to the campus environment.

Part 8. Documentation Requirements

PCI DSS imposes a compliance approach using one of several self-assessment questionnaires (SAQ). The specific questionnaire is determined by the processing environment and related

level of risk. System institutions are classified as [Level 2, 3 or 4] merchants by acquiring banks. Each college and university shall establish a self-assessment process using the appropriate SAQ. It is up to each college and university to determine the degree to which each campus merchant is responsible for this self-assessment. At a minimum, each campus shall document:

a. ongoing self-assessment using the appropriate SAQ;
b. annual campus merchant compliance status (tied to year-end financial statement review) including accurate documentation of any compensating controls and, if applicable, a plan to achieve full compliance if current status is noncompliant;
c. campus merchant change request and update reporting (requirement to report any proposed changes in processing and proposed steps necessary to address any changes in compliance requirements - this should be approved by the campus merchant approval officer); and
d. quarterly network scans (report results and remediation steps and timeline if applicable).

Part 9. Develop an Incident Response Plan

Each college and university shall outline a process for reporting a breach in security to the campus merchant approval officer and the chief financial officer.

Date of Adoption: 08/30/10
Date of Implementation: 08/30/10
Date of Last Review: 02/10/17

Date and Subject of Revision:

02/10/17 - Reviewed as part of the five year review cycle.

No additional HISTORY.