Instructions

1. Items in **bold-underline** indicate optional documents that you may need to create.
2. Items in *{bracketed-italics}* indicate an item that needs to be filled in with the appropriate steps or wording that correctly describes the process in your department.
3. Review each section and update as follows:
    a. For those that do not apply to the department, i.e. you do not accept payments via fax, simply sign and date to indicate that this has been reviewed and confirmed.
    b. For those that do apply, modify or replace the example steps included so that the steps reflect your actual departmental procedures.

FLORIDA INTERNATIONAL UNIVERSITY

{Merchant Location Name} - Payment Card Procedures

{DEPARTMENT NAME}

8/17/2021

Contents

{DEPARTMENT NAME} Payment Card Procedures

I. Procedure Statement

Per the Payment Card Industry Security Standards Council (PCI SSC), each department that handles payment card information must have documented procedures that are consistent with the University's Payment Card Processing policy, and cover the processes for complying with the current version of the Payment Card Industry Data Security Standards (PCI DSS).

II. Purpose

The intent of these procedures is to provide guidance to departments that are responsible for handling or processing payment card transactions from customers for goods and/or services provided. These procedures should supplement other internal procedures that are in place to minimize the potential for loss of sensitive data belonging to either Florida International University (FIU) or our constituents.

III. To Whom this Policy Applies

All individuals with responsibility, authority, and stewardship over payment card transactions on behalf of FIU. All persons who handle payment card transactions assume the responsibility for following the procedures outlined below.

IV. Overview

Any department accepting payment cards on behalf of FIU for goods and/or services should designate a primary contact, usually a full time employee, within that department who will have primary authority and responsibility for payment card and/or ecommerce transaction processing within that department. This should be the department manager. Any changes to the person filling this role should be reported to the PCI Compliance Team. This individual will be responsible for the department complying with the security measures established by the Payment Card Industry and FIU's policies. In addition, they are responsible for ensuring that any employee who handles payment card transactions is properly vetted through the Merchant Employee e-form process. **Please note that students are only allowed to handle cardholder data (CHD) if they are employees of FIU**.

Departments may only use the services of vendors which have been approved by the FIU PCI Compliance team to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order, or internet-based.

The FIU PCI Compliance Team will review the departmental Payment Card Procedures at least annually as part of the compliance review cycle. Any relevant procedural changes and/or revisions will be published on the Office of the Controller's webpage and/or directly communicated to all merchants. The PCI Compliance training is available online and must be completed at least annually, and as new staff that will be responsible for cardholder data are hired. All staff handling payment card information must also annually review the departmental Payment Card procedures and acknowledge their understanding through the employee statement of understanding. The annual employee requirement is completed through the Merchant Employee e-form process.

Departmental procedures should be reviewed, signed and dated by the merchant location's primary contact on an annual basis indicating compliance with the University's Payment Card Processing Policy. These procedures also must be submitted to the PCI Compliance Team.

Departmental procedures must thoroughly describe the entire transaction process and will include, but are not limited to, the following:

- Business Operation Overview
- Segregation of duties
- Deposits
- Reconciliation procedures
- Physical security
- Disposal of CHD
- Data retention
- Cash register procedures (if applicable)
- Incident response

V. Payment Card Procedures

Departmental procedures and controls are to be reviewed by the staff and the PCI Compliance Team.

Business Operation Overview:

{Include an explanation of type of revenue(s) generated by your merchant account(s)}

Card Present Transactions

Transactions are considered "card present" if the Card Verification Value (CVV)1 is submitted at the time of the transaction. The CVV1 is contained only on the magnetic stripe and is **not** the three-digit verification code (aka. CVV2, CVC2) that is more commonly known. Therefore such transactions require that the physical card must be presented at the time of the payment and the payment data entered by swiping, inserting (Europay, MasterCard, and Visa (EMV)), or tapping (Near Field Communication (NFC)) the card.

In Person Payments

If your department does **not** accept in person payments, please confirm this by including your signature and current date on the lines below:

Name: _____ Date: _____

If your department accepts in person payments, please follow the departmental procedures listed.

A. Attach any/all form(s) where payment card information is requested (if applicable)
B. Only approved merchant employees can process credit card transactions and/or handle cardholder information.
C. Card Handling Guidelines

a. Review Card Security
    i. Is the card valid? The card may not be used after the last day of the expiration month embossed on the card.
    ii. Only the actual card/account holder should be using the card. (Ask for Picture ID)
    iii. Does the customer's signature on the charge form match the signature on the back of the card? Compare the signatures and make sure that the signed name is not misspelled or otherwise obviously different.
    iv. Does the signature panel on the card look normal? Check to be sure that it has not been taped over, mutilated, erased, or painted over. Obvious physical alterations to the card could indicate a compromised card.
    v. Does the account number on the front of the card match the number on the back of the card and the terminal receipt display? If the numbers do not match, or if they are covered or chipped away, this could indicate an altered card.
    vi. Does the name on the customer receipt match the embossed name on the front of the card? If the name is different, this could indicate an altered card.
b. Risks of Keyed Transactions
    i. Manually keying in the card account information carries a higher risk of fraud since many of the built-in card security features cannot be accessed. If the magnetic stripe on the back of the card is unreadable, or if you choose to process transactions manually, follow these steps:
        - Key the transaction and expiration date into the terminal
        - Ask the cardholder to sign the paper receipt and compare the signature
c. Report Suspected Card Fraud
    i. If you suspect the card is fraudulent, report it following the security breach steps outlined in the "Other Considerations" section.
d. Retain the signed merchant copy of the swipe machine-generated receipt and return the other copy to the cardholder.
e. Place the merchant copy of the receipt in a secure location until the end of day batch process has been run.
f. Oversight of the swipe machine (NOTE: *PCI DSS Requirement 9.9 requires that all swipe terminals must be periodically checked and those checks must be logged*)
a. Periodically log the information into the (*required*) **Merchant Device Inventory and Tampering Checklist** while checking the machine daily to determine if it has been tampered with or exchanged (i.e. verify stickers have not been removed and re-affixed, same model, same serial number, etc.).
b. Report any tampering as a security breach per the steps outlined in the "Other Considerations" section.
c. Keep the machine in a locked area when not in use or after hours.

- Upload a list that contains the individuals responsible for handling in-person payments (include backup personnel as well):

Card Not Present Transactions

Transactions are considered "card not present" if the CVV1 is not submitted at the time of the transaction because the physical card is not presented. **Payments made over the telephone or Internet, or sent via mail or fax fall into this category.**

Mailed in Payments

If your department does **not** accept mailed in payments, please confirm that by including your signature and current date on the lines below:

Name: _____ Date: _____

If your department accepts mailed in payments, please follow the departmental procedures below.

A. At least two people should be responsible for opening the mail and processing any payment transactions. If possible, these staff members should alternate days. The transaction(s) must be processed within one business day from when the user has access to the cardholder information.
B. Bundle together all payment requests and attach a cover sheet with the date, count of requests, and initials of the person opening the mail.
C. Hand over the bundle to the person responsible for entering the payment(s).
D. Process the payments using the approved departmental method (i.e. hosted payment application, terminal, etc.) and print out two copies of the receipt.
E. The portion of the form containing the payment card information must be destroyed after the transaction has been processed in an approved PCI manner. Options for acceptable destruction include removing and cross-cut shredding, or rendering it unreadable on the form (i.e. hole-punch through the card number, expiration date, and security code). Writing over the cardholder data (CHD) with a black marker is NOT recommended as it is not always effective.
F. Return a copy of the receipt to the customer via the approved departmental method which is *{mail / fax / scan / email}*. Retain the other copy in a secure location to use if a refund is later issued.
G. Place the merchant copy of the receipt in a secure location until the End of Day batch process runs.

Individual(s) responsible for opening and distributing the mail (include backup personnel as well):

_____

_____

Individual(s) with responsibility for mailed or faxed in payments (include backup personnel as well):

_____

_____

Telephone Payments:

If your department does **not** accept telephone payments, please confirm this by including your signature and current date on the lines below:

Name: _____ Date: _____

If your department accepts telephone payments, please follow the departmental procedures below.

A. All telephone payments should be entered into the payment terminal or application during the call. If not possible, the transaction(s) must be processed within one business day from when the user has access to the cardholder information. Do not accept payment information via a voicemail/phone message.
B. If payment data must be written down, it should be recorded on your departments credit card authorization form and processed immediately after the call has concluded. The portion of the form containing the payment card information must be destroyed in an approved PCI manner. Options for acceptable destruction include removing and cross-cut shredding, or rendering it unreadable on the form (i.e. hole-punch through the card number, expiration date, and security code). Writing over the CHD with a black marker is NOT recommended as it is not always effective.
C. If the department uses a payment application a validated point to point encrypted (P2PE) solution must be used when entering cardholder data and each person taking telephone payments must have a unique login; shared logins are explicitly forbidden in the PCI DSS.

Individual(s) with responsibility for telephone payments (include backup personnel as well):

_____

_____

Fax Payments:

If your department does **not** accept fax payments, please confirm this by including your signature and current date on the lines below:

Name: _____ Date: _____

If your department accepts fax payments, please follow the departmental procedures below.

A. The fax machine must be located in an area not accessible to the public during the day and moved to a secure location if left turned on at night.
B. Use of a multi-function printer / fax machine can increase the PCI scope for the department so should be avoided if possible; a plain paper, dial up fax is recommended.

C. Faxes with payment information must be immediately distributed to the individual responsible for key-entering the information into the approved swipe device or payment application.
D. The payment card information must be removed and cross-cut shredded or rendered unreadable (hole-punch through the card number, expiration date and security code) after the transaction has been processed. If the payment data can be removed from the bottom of the page and destroyed, the top portion may be retained.
E. The receipt must only contain that portion of the account number allowed in the current PCI Data Security Standards, i.e. last four digits.
    a. The merchant copy must be attached to the fax and filed in the designated place for later reconciliation.
    b. The customer copy may be faxed, mailed, or emailed to the customer (optional).

Individual(s) with responsibility for telephone payments (include backup personnel as well):

_____

_____

Online Payments:

If your department does **not** accept online payments, please confirm this by including your signature and current date on the lines below:

Name: _____ Date: _____

If your department accepts online payments, please follow the departmental procedures below.

A. Consumer-initiated, online payments do not fall into departmental PCI scope, but the application itself and any online payments entered by staff are the responsibility of the department.
B. If the department uses a payment application, each person entering payments online must have a unique login; shared logins are explicitly forbidden in the PCI DSS.
C. Payments entered into an online application using data received in-person, on the telephone, or via a paper form (i.e. fax, mail) must be handled according to the procedures defined in each relevant section above.

Individual(s) with responsibility for online payments (include backup personnel as well):

_____

_____

Back-Office Procedures

Refunds:

Refund processing guidelines are described below:

1. Refunds must be issued using the same mode of processing that was used for the original transaction.
2. Refunds must be issued to the same payment card number that was used for the original transaction.
3. If the card holder can provide documentation that the original payment card account number has been closed, the department may issue a refund to another payment card the cardholder has.
4. The refund amount may only be up to the amount of the original transaction.
5. No individual should be processing payments and refunds, however if the department has insufficient personnel to implement such segregation of duties then the refund must be approved by a supervisor or department head by signing the refund receipt attached to the original transaction receipt.

All refunds should be processed and entered into *{describe your department's refund process here}.*

Individual(s) responsible for processing refunds (include backup personnel as well):

_____

_____

End of Day Batch Process:

Include the steps below that you follow to settle all transactions at the end of each day:

- Step 1 (*please include the details of each step here)*
- Step 2
- Staple the settlement sheet in front of the sales receipts and
  Either store in a secure location (i.e. a locked safe or locked drawer) until the information is uploaded as supporting documentation to the journal entry in PeopleSoft Financials.

Individual responsible for closing out all daily transactions (include backup personnel as well):

_____

_____

Journal Entries:

Merchant Services implemented an interactive training that will assist your department's designated journal contacts in creating journal entries related to payment (debit and credit) card activity in PeopleSoft Financials. The Merchant Journal Training provides resources that will further facilitate the recording process

Individual responsible for closing out all daily transactions (include backup personnel as well):

_____

_____

Reconciliation process:
All departments are required to perform reconciliations of their merchant activity. Include the steps below that you follow to reconcile:

1. Step 1: Close out and settle your payment card terminals or web-based applications daily (Some locations have auto-batch enabled).
2. Step 2: Reconcile transactions on their Daily Settlement Report(s) against their *{enter report name here}* report to assure that they have received credit for all processed transactions. Reconciliations of your revenue must be performed and the documentation must be available for review if requested.
3. Step 3: The approved designated journal contacts in your department must record the journal entries in PeopleSoft Financials in accordance to the guidelines noted in the Merchant Journal Training.

Chargeback/Dispute Process
A chargeback is a processed credit card transaction that is reversed (charged back) to a merchant because the customer or customer's bank finds something wrong with the transaction.

The Merchant Services team will notify you via e-mail of your recent American Express related chargeback/dispute. It is the responsibility of your department to contact American Express to dispute their claim and provide supporting documentation of such. All chargeback documentation for Visa, MasterCard, and Discover cards, should be received and sent electronically. This can be achieved by enrolling in Bank of America Merchant Services tool, **Dispute Manager** within Clientline.

It is imperative that your department maintain accurate record keeping and documentation accordingly.

Individual(s) responsible for reconciliation and chargeback/dispute process (include backup personnel as well):

_____

_____

Record Retention

All merchant locations are required to adhere to the State of Florida's general records schedule GS1-SL. The item numbers below can be located within the GS1-SL schedule:

- Signature Authorization Records (Item #300): This record series consists of forms authorizing individuals to sign purchase orders, credit cards/receipts, or paychecks, to accept packages requiring a signature, or to sign off on other types of agency business.
  RETENTION: 1 fiscal year after obsolete or superseded
- Receipt/Revenue Records: Detail (Item #365): This series consists of records documenting specific receipts/revenues collected by an agency through cash, checks, electronic transfers,

credit and debit cards, or other methods. The series may include, but is not limited to, records such as cash collection records and reports, cash receipts books, cash register tapes, deposit transfer slips, EFT notices, credit and debit records receipt ledgers, receipt journal transactions and vouchers, refund records, bad check records, and other accounts receivable and related documentation. Retention is based on Section 95.11(2), Florida Statutes, and Statute of Limitations on contracts, obligations, or liabilities.
RETENTION: 5 fiscal years

- Payment Card Sensitive Authentication Data (Item #395): This record series consists of elements of a customer's payment card data that are used to authenticate a financial transaction using that payment card (e.g. credit card, debit card). Sensitive authentication data includes those elements defined as such by the Payment Card Industry Security Standards Council in their Data Security Standard. Requirements and Security Assessment Procedures(Version 1.2, October 2008 or subsequent edition) and includes full magnetic stripe data (also known as full track, track, track 1, track 2, magnetic-stripe data); three-digit or four digit card verification code or value; and personal identification number (PIN) or encrypted PIN block.
  RETENTION: Destroy immediately upon completion of the transaction.

Keep cardholder data storage to a minimum by following the data retention policy, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
- Data that is not absolutely necessary in order to conduct business will not be retained in any format. All data will be treated as confidential.
- Specific retention requirements for cardholder data
- Processes for secure deletion of data when no longer needed
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.
- Physical access to data records is restricted to staff with a need to know.

For all payment documentation, regardless of the inclusion of CHD, all steps below are required:

- Label all files containing reconciliation / settlement documentation, include an indicator if confidential data is included, and note the destruction date clearly.
- Be sure to log any movement of the files until they are destroyed in accordance with FIU's **Record Retention and Disposition Policy**.

Individual(s) who maintain the log (include backup personnel as well):

_____

_____

VI. Systems Configuration

Work with the Division of IT and/or your technical contact in your department to ensure that:

- Anti-virus software is implemented and updated regularly on all systems and devices

- Vendor operation system and application patches are installed in a timely manner.
- Data detection and data encryption software are implemented to ensure that all confidential data is identified, secured or deleted.
- If external vendors or third-parties need access to service any third-party applications or software, access should only be granted for the time needed to complete the necessary task and then immediately disabled.

VII. Other Considerations

Directing Cardholders to Kiosks/Workstations to enter CHD is prohibited

Many departments use third-party payment systems or gateways for online payment card processing. Customers should be directed to complete payments online using their own personal device. If you are specifically directing people to use computer labs, kiosk machines, or other public-use computers to make payments, this can inadvertently bring these devices into PCI scope. Therefore, DO NOT direct customers or offer payment card entry on any device that has not been properly secured or approved by the PCI Compliance Team.

Responding to CHD sent through email

Any open communication system such as email or chat programs are not considered secure for the transmission of any payment card information. If a customer should send their payment information to the department via email, the following steps should be taken:

1) Click "Reply" on the email
2) Delete the payment card data from the original portion of the email.
3) In your response, Copy and paste the following
    a. "Thank you for contacting (*insert department or name)*. We appreciate your business, however as part of our compliance effort with the Payment Card Data Security Standard and our practice to protect all of our customers' Personally Identifiable Information, we cannot process the payment that you have sent through email. We ask that you use one of the following approved methods for making your payment:
        - Online - www.xxxxxxxxxx.edu
        - Mail – mailing address
        - Phone – xxx-xxx-xxxx
        - Fax – xxx-xxx-xxxx
4) Then promptly delete the original email and empty the trash.

Suspected breach of security or fraud

Follow the process below in the event of a credit card security breach or incident:

- Notify your supervisor and the PCI Compliance Team via email at pcicompliance@fiu.edu immediately.

PCI Compliance Team Contact List

Katherine Cochran
Email Address: kcochran@fiu.edu
Contact Number: 305-348-3888

Jose Zubimendi
Email Address: jzubimen@fiu.edu
Contact Number: 305-348-1139

Helvetiella Longoria,
Email Address: helve@fiu.edu
Contact Number: 305-348-3591

Oriana Estevez
Email Address: omangarr@fiu.edu
Contact Number: 305-348-2557

Alexandra Mirabal
Email Address: aimiraba@fiu.edu
Contact Number: 305-348-9060

Vendor Contact List

Please add to and/or revise the vendor contact list below with any third part vendor(s) involved in your merchant process/environment. This information is crucial in the event of a data breach as the vendor will need to be contacted.

Vendor Name	Customer Service Helpdesk #	Representative Name	Email Address and/or Phone Number
Clientline	1-800-285-3978		
CyberSource	1-866-501-7958		
Bluefin/PayConex	1-800-675-6573		

Annual PCI Compliance

1) Collect an Attestation of Compliance (AOC) from any service providers with whom cardholder data is shared, or that could affect the security of your customers' cardholder data.
2) Review departmental policies and procedures to ensure that they are current and accurate.
3) Complete the Self-Assessment Questionnaire (SAQ) that has been assigned.

VIII. Effective Date and Approval

The procedure herein is effective *{DATE}*. This procedure shall be reviewed and revised, if necessary, annually to become effective at the beginning of the fiscal year, unless otherwise noted.

Approved By:

_____
{Merchant Location's Primary Contact Name}
{Title}

_____
{Department VP/Finance Manager Name}
{Title}

Date Approved: *{DATE}*
Date Revised: *{DATE}*