Coastal Carolina University - Payment Card Procedures v3.2

DEPARTMENT NAME: _____

DATE REVISED: _____

Contents

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 Coastal Carolina University 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 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 Coastal Carolina University or our constituents.

III. To Whom this Policy Applies

All individuals with responsibility, authority, and stewardship over payment card transactions on behalf of Coastal Carolina University. 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 Coastal Carolina University for goods or services should designate 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 Treasury Accountant in Financial Services. This individual will be responsible for the department complying with the security measures established by the Payment Card Industry and Coastal Carolina University policies. In addition, they are responsible for ensuring that any employee or contractor who handles payment card transactions takes the annual online PCI training, signs the training acknowledgement, and, if applicable, undergoes the appropriate background check before any access is granted. **Please note that students are only allowed to handle cardholder data (CHD) if they are student employees of** Coastal Carolina University**.**

Departments may only use the services of vendors which have been approved by Financial Services to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order, or internet-based. The department will be responsible for all processing fees, encryption monthly fees, and the expense of any approved credit card processing equipment.

The Coastal Carolina University PCI Compliance Team will review the departmental Payment Card Procedures at least annually as part of the compliance review cycle. All changes and/or revisions will be published on the Financial Services web page and will be effective when issued. The PCI Compliance Team will provide online training for PCI Compliance at least annually, and as new staff are hired. All staff

handling payment card information must also annually review the departmental Payment Card procedures and acknowledge their understanding.

Departmental procedures should be reviewed, signed and dated by the Department Manager on an annual basis indicating compliance with Coastal Carolina University's Payment Card Policy. These procedures also must be filed in their department's PCI Compliance folder.

Any departmental procedures should thoroughly describe the entire transaction process and will include, but are not limited to, the following:

- Segregation of duties
- Deposits
- Reconciliation procedures
- Physical security
- Information disposal
- Data retention
- Cash register procedures (if applicable)
- Incident response

V. Payment Card Procedures

All departmental procedures and controls are to be reviewed by Financial Services and the PCI Compliance Team. These generic departmental procedures should be followed as a starting point.

Card Present Transactions

Transactions are considered "card present" if the CVV1 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. To then be a card present transaction, the physical card must be presented at the time of the payment and the payment data entered by swiping, inserting (EMV), or tapping (NFC) the card.

In Person Payments

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

Name: _____ Date: _____

If your department accepts in person payments, please detail the departmental procedures below.

A. Attach any/all form(s) where payment card information is requested (if applicable)
B. Only approved staff and student employees should be handling credit card transactions.
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.
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, the customer must provide another form of payment.

c. Report Suspected Card Fraud
   i. If you suspect the card is fraudulent, report it following the security breach steps defined below.

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 place until the end of day batch process has been run to prepare a deposit form to be delivered daily to Office of Student Accounts (if payments are not automatically interfaced).
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. Log information into the **Inspection Log** for each terminal to record periodic checks the machine 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.). This **Inspection Log** for each terminal should be filed in the department's PCI Compliance folder.
   b. Report any tampering as a security breach per the steps defined on page 9.
   c. Keep the machine in a locked area when not in use or after hours.

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 detail the departmental procedures below.

A. At least two people should be responsible for opening the mail and logging any payment requests onto a **Payments Tracking Form** *(recommended)*. If possible, these staff members should alternate days.
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 or white out 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 place to use if credit is later issued.
G. If necessary, forward the payment confirmation to the event coordinator or person responsible for the class.
H. Place the merchant copy of the receipt in a secure place until the end of day batch process has been run to prepare a deposit form to be delivered daily to Office of Student Accounts (if payments are not automatically interfaced).

Individuals 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 that by including your signature and current date on the lines below:

Name: _____ Date: _____

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

A. All telephone payments should be entered into the payment terminal or application during the call if possible. Do not accept payment information via a voicemail/phone message.
B. If payment data must be written down, it should be logged on a **Telephone Payments Form** *(recommended)* and processed immediately after the call has concluded. 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 CHD with a black marker or white out is NOT recommended as it is not always effective.
C. If the department uses a payment application, each person taking telephone payments must have a unique login; shared logins are explicitly forbidden in the PCI DSS standards.
D. Place the merchant copy of the receipt in a secure place until the end of day batch process has been run to prepare a deposit form to be delivered daily to Office of Student Accounts (if payments are not automatically interfaced).

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

_____

_____

Fax Payments:

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

Name: _____ Date: _____

If your department accepts fax payments, please detail 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).
F. Place the merchant copy of the receipt in a secure place until the end of day batch process has been run to prepare a deposit form to be delivered daily to Office of Student Accounts (if payments are not automatically interfaced).

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

_____

_____

Online Payments:

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

Name: _____ Date: _____

If your department accepts online payments, please detail 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.
D. Place the merchant copy of the receipt in a secure place until the end of day batch process has been run to prepare a deposit form to be delivered daily to Office of Student Accounts (if payments are not automatically interfaced).

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

_____

_____

_____

Reconciliation process:

All departments are required to:

1. Close out their payment card terminals or web-based applications daily (if not automatic).
2. Reconcile transactions on their Daily Settlement Reports against their general ledger reports to assure that they have received credit for all processed transactions. Reconciliations must be performed at least monthly, preferably on the last business day of the month. These are to be filed in a secure location and available for review by Financial Services.

If any consumer disputes (chargebacks) are received, the notice should be sent immediately to the Treasury Accountant in Financial Services with a copy of the original transaction and an explanation of why the money should or should not be returned.

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

_____

_____

Document Retention:

Keep cardholder data storage to a minimum by implementing data retention and disposal policies, 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.
- Note the name, contents, and location in the *(optional)* **Document Retention Log**.
- Be sure to log any movement of the files until they are destroyed in accordance with Coastal Carolina University's **Record Retention and Disposition Policy**.

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

_____

_____

_____

_____

V. Systems Configuration

Work with the Information Technology department to ensure that:

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

VI. Other considerations

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 client should send their payment information to the department, 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:

In the event of a security breach/incident, follow formally assigned duties and responsibilities.

1) Notify your supervisor immediately.
2) If you are unsure, but suspect fraud related to payment card activities, you should contact the Controller in Financial Services.
3) If the suspected activity involves computers (hacking, unauthorized access, etc.) make sure you contact your Local IT Support Person and immediately notify ITS Security.

Annual PCI Compliance:

1) Ensure all staff and student workers handling credit card transactions complete annual online PCI Compliance training and file proof of training in your departmental PCI Compliance folder.
2) Review departmental policies and procedures to ensure that they are current and accurate.
3) Complete/assist with the annual Self-Assessment Questionnaire (SAQ) that has been assigned.

VII. Effective Date and Approval

The policies herein are effective _____. This policy shall be reviewed and revised, if necessary, annually to become effective at the beginning of the fiscal year, unless otherwise noted.

Approved:

_____
Department Manager
Title

_____
Department VP
Title

Date Approved: _____

Date Revised: _____