# Instructions

Review each section and update as follows:

* 1. 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.
	2. For those that do apply, modify or replace the example steps included so that the steps reflect your actual departmental procedures.

UMB DEPARTMENT Payment Card Procedures

DEPARTMENT NAME

Date REvised:

Contents

[Instructions 0](#_Toc470706616)

[I. Procedure Statement 3](#_Toc470706617)

[II. Purpose 3](#_Toc470706618)

[III. To Whom this Policy Applies 3](#_Toc470706619)

[IV. Overview 3](#_Toc470706620)

[V. Payment Card Procedures 4](#_Toc470706621)

[Card Present Transactions 4](#_Toc470706622)

[Card Not Present Transactions 6](#_Toc470706623)

[Back Office Procedures 9](#_Toc470706624)

[V. Systems Configuration 10](#_Toc470706625)

[VI. Other considerations 10](#_Toc470706626)

[Responding to CHD sent through email 10](#_Toc470706627)

[Suspected breach of security or fraud 11](#_Toc470706628)

[Annual PCI Compliance 11](#_Toc470706629)

[VII. Effective Date and Approval 11](#_Toc470706630)

***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 UMB 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 UMB or our constituents.

# **III. To Whom this Policy Applies**

All individuals with responsibility, authority, and stewardship over payment card transactions on behalf of UMB. 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 UMB for goods or services should designate a full time employee who will have primary authority and responsibility for payment card and/or ecommerce transaction processing within that department. This role is titled “PCI Coordinator.” Personnel changes in this role must be reported to the PCI Compliance Committee. This individual will be responsible for the department complying with the security measures established by the Payment Card Industry and UMB policies. In addition, they are responsible for ensuring that employees takes the annual PCI training. **Please note that students are only allowed to handle cardholder data (CHD) if they are employees of UMB.**

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

The UMB PCI Compliance Committee will review the departmental Payment Card Procedures as part of the compliance review cycle. The PCI Compliance Team will provide training on PCI Compliance at least annually. PCI Coordinators are responsible for ensuring new staff are trained and familiar with UMB policies and procedures. All staff handling payment card information must also annually (as part of the annual training requirement) review the departmental Payment Card procedures and acknowledge their understanding.

Departmental procedures should be reviewed, signed and dated by the PCI Coordinator for the Merchant Account on an annual basis indicating compliance with the UMB [PCI Policy](https://www.umaryland.edu/policies-and-procedures/library/financial-affairs/policies/viii-9908a.php) and [Procedure](https://www.umaryland.edu/policies-and-procedures/library/financial-affairs/procedures/financial-services/payment-card-industry-data-security-standards-compliance-and-payment-card-transactions.php). Upload departmental procedures indicating the most recent review date to the CampusGuard Central Portal <https://cg.central.campusguard.com/portal>

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

* Segregation of duties
* Deposits
* Reconciliation procedures
* Physical security
* Information disposal
* Data retention
* Incident response

# **V. Payment Card Procedures**

Departmental procedures and controls are reviewed by the PCI Compliance Committee.

## ***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. Clearly in order 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.

1. Attach any/all form(s) where payment card information is requested (if applicable)
2. Only approved staff should be handling credit card transactions.
3. Card Handling Guidelines
	1. Review Card Security
		1. Is the card valid? The card may not be used after the last day of the expiration month embossed on the card.
		2. Only the actual card/account holder should be using the card. Request ID.
		3. Does the customer's signature on the charge form (i.e. receipt) 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.
		4. 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.
		5. 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.

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.

* 1. Risks of Keyed Transactions
		1. Whenever possible, the cardholder should initiate the transaction. However, in certain circumstances when the card cannot be read, a UMB employee may need to manually key the information.
		2. 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
			+ Obtain an imprint of the card (NOTE: *This can help prove that the card was actually in hand when the transaction was completed. If an impression of the card is taken, there will need to be a data retention policy for that stored paper, a secure place to store the data, and a proper destruction plan for when that data no longer needs to be kept.)*
			+ Ask the cardholder to sign the paper receipt and compare the signature (Note: *Compare the signature to the one on the back of the card to validate the person using the card. If the card is not signed, the card brands deem the card not valid to be used and the transaction can be denied*).
	2. Report Suspected Card Fraud
		1. If you suspect the card is fraudulent, report it following the [security breach](#Breach) steps defined below.
1. Retain the signed merchant copy of the swipe machine-generated receipt and return the other copy to the cardholder.
2. Place the merchant copy of the receipt \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ until the [End of Day batch process](#EOD) has been run.
3. 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*)
	1. Log information into the (*required*) [Swipe Terminal Inventory Sheet](https://www.umaryland.edu/media/umb/af/sa/Swipe-Terminal-Inventory-Sheet.xlsx) and periodically check 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.).
	2. Report any tampering as a [security breach](#Breach) per the steps defined below.
	3. Keep the machine in a locked area when not in use or after hours.

List 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 fall into this category.

A payment should be processed within one business day of receiving the payment and the CHD should be destroyed by the close of business, but no later than 24 hours after processing the payment. The preferred method for destruction is cross-cut shredding. Alternatives may be used as long as the CHD is unreadable and destroyed. Examples include punching holes through the card number, expiration date, and security code for CHD that is documented on a form. Writing over the CHD with a black marker is NOT an acceptable method for destroying CHD.

Mailed 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.

Examples include:

(Modify the template to detail your department procedures for mailed payments).

1. At least two people should be responsible for opening the mail and logging any payment requests onto the [Payments Tracking Form](https://www.umaryland.edu/media/umb/af/sa/Telephone-Mail-Payment-Card-Processing-Tracking-Form.docx). If possible, these staff members should alternate days.
2. Bundle together all payment requests and attach a cover sheet with the date, count of requests, and initials of the person opening the mail.
3. Hand over the bundle to the person responsible for entering the payment(s).
4. Process the payments using the approved departmental method (i.e. hosted payment application, terminal, etc.) and print out two copies of the receipt.
5. 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.
6. Return a copy of the receipt to the customer via the approved departmental method which is *{mail / fax / scan / email}*. Retain the other copy *{\_\_\_here\_\_\_\_\_\_}* to use if credit is later issued.
7. If necessary, forward the payment confirmation to the event coordinator or person responsible for the class.
8. Place the merchant copy of the receipt \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ until the [End of Day batch process](#EOD) has been run.

Individuals responsible for opening and distributing the mail (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.

Examples include:

(Modify the template to detail your department procedures for telephone payments).

1. 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.
2. If payment data must be written down, it should be logged on the [Telephone Payments Form](https://www.umaryland.edu/media/umb/af/sa/Telephone-Mail-Payment-Card-Processing-Tracking-Form.docx) 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 is NOT recommended as it is not always effective.
3. 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.

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, per UMB Procedure:

1. Operational Unit personnel are prohibited from submitting online payments on behalf of customers.
2. Customers must initiate and submit their own online payments.
3. List all online application URLs:

Individual(s) with responsibilities in managing online application and/or processing payments and refunds (include backup personnel as well):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Other Payment Methods Confirmation:

Payment cards cannot be accepted via email, fax, instant messenger, or similar messaging technologies that are identified under [Section II.B in the UMB Procedure](https://www.umaryland.edu/policies-and-procedures/library/financial-affairs/procedures/financial-services/payment-card-industry-data-security-standards-compliance-and-payment-card-transactions.php). If a payment is received via an unsecured method, such as email, the recipient should delete the payment information and reply to the sender. In the response the recipient should tell the sender that payments cannot be accepted by *[ ]* *(insert method)* and list the acceptable payment methods.

Please confirm that your department does not accept payments by the methods described herein by including your signature and current date on the lines below:

## Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Back Office Procedures

**End of Day Batch Process:**

Include the steps below that you follow to settle all transactions at the end of each day per your payment processor.

* Step 1 (*please include the details of each step here)*
* Step 2
* Staple the settlement sheet in front of the sales receipts and store in a secure location (i.e. a locked safe or locked drawer).
* Do not retain cardholder data.

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Reconciliation process:**

All departments are required to

Close out and settle their payment card terminals or web-based applications daily. The three reconciliations listed in this section are required. These reconciliations must be performed at least once per calendar month. Operational Units may decide to reconcile more frequently as needed. A sample reconciliation template is available [here](https://www.umaryland.edu/financialservices/forms/).

* + - * 1. Sales must be reconciled with payments processed. This ensures that payments have been processed for all sales. Compare the sales report with the batch report.
				2. The batch report must be reconciled with the amount funded. This ensures that the payments processed have been funded by the merchant bank. Compare the batch report with the merchant bank activity.
				3. The merchant bank activity must be reconciled to the general ledger activity in the UMB financial system. This ensures that the transactions are posted in the UMB financial system. Compare the merchant bank activity statement with the UMB financial system general ledger report.

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Document Retention:**

A payment should be processed within one business day of receiving the payment and the CHD should be destroyed by the close of business, but no later than 24 hours after processing the payment. The preferred method for destruction is cross-cut shredding. Alternatives may be used as long as the CHD is unreadable and destroyed. Examples include punching holes through the card number, expiration date, and security code for CHD that is documented on a form. Writing over the CHD with a black marker is NOT an acceptable method for destroying CHD.

Sales and reconciliation records must be retained for a minimum of three (3) years or until audited, whichever is longer.

Keep in mind that other federal or state regulations that may dictate longer retention periods. Additionally, for records that are grant-/contract-related, the grant/contract documents may dictate the record retention requirements. See the Sponsored Programs Administration website for further record retention guidance http://www.umaryland.edu/spa/award-management/record-retention/.

Physical access to data records is restricted to staff with a need to know.

For all payment documentation all steps below are required:

* Label all files containing reconciliation/settlement documentation and note the destruction date clearly. No confidential data should be retained.
* Be sure to log any movement of the files until they are destroyed in accordance with [UMB Data Retention-Archival Policy](https://www.umaryland.edu/policies-and-procedures/library/information-technology/policies/x-9907a.php).

# **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
	1. “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
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:

1. Immediately notify the employee’s supervisor and the Operational Unit PCI Coordinator.
2. If fraud is suspected, contact Change Management Advisory Services.
3. If the suspected activity involves computers (hacking, unauthorized access, etc.), also contact the Operational Unit’s IT support team and immediately notify the Center of Information Technology Services (CITS).

## **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.

# **VII. Effective Date and Approval**

The procedures herein are 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:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Department Manager

Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Department VP

Title

Date Approved: *{DATE}*

Date Revised: *{DATE}*