

**<<Department Name>>**

**Departmental Payment Card Procedures**

The following template is being provided to guide in the documentation of departmental procedures. Sections not applicable to how the department operates should be deleted and specific procedures relevant to the department should be added.

# **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 Radford University Payment Cards 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 the department for handling or processing payment card transactions. These procedures should supplement other University policies and procedures that are in place to minimize the potential for loss of sensitive data belonging to either Radford University or our constituents.

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

All persons with responsibility, authority, and stewardship over payment card transactions on behalf of the department. 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 Radford University must designate a Merchant Payment Card Coordinator. The Merchant Payment Card Coordinator must be a full time employee within the department who has primary authority and responsibility for payment card and/or ecommerce transaction processing within the department. This Merchant Payment Card Coordinator will serve as the primary contact regarding payment card processing for the department. Any changes to the person filling this role should be reported to the University Bursar. This individual will be responsible for the department complying with the security measures established by the Payment Card Industry and Radford University policies. In addition, the Merchant Payment Card Coordinator is responsible for ensuring that any employee who handles payment card transactions takes the annual PCI training and signs the Payment Card Security and Confidentiality Agreement. Only approved/trained staff should be handling credit card transactions.

Departments may only use the services of vendors which have been approved by the Associate Vice President for Finance & University Controller (AVPF & UC) to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order, or internet-based. The Merchant Payment Card Coordinator must review the departmental Payment Card Procedures at least annually as part of the compliance review cycle. All changes and/or revisions must be approved by the Department Head. The Controller’s Office will provide access to training on PCI Compliance. 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 Head on an annual basis indicating compliance with Radford University’s Payment Card Policy.

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

* Segregation of duties
* Deposits
* Reconciliation/settlement procedures
* Physical security (including directions for periodically inspecting devices that capture payment card data through direct physical interaction with the payment card (i.e. card swipe or dip) at the point of sale and how to report suspected tampering.)
* Access security including proper handling and protection of user IDs and passwords.
* Information disposal
* Data retention
* Point of Sale/Cash register procedures (if applicable)
* Completion and delivery of Cashier Transmittal forms.
* Incident response (Reporting of suspected breach of security or fraud)

# **V. Summary of Departmental Oversight and Activity**

\*Must be updated annually

**Department Head Name**:

**Merchant Payment Card Coordinator’s Name**:

**Payment Card data is correctly collected/processed through the following means**:

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.*

 Are In Person Card Present Payments Accepted: \_\_\_ Yes \_\_\_ No

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.*

Are Payments Accepted via mail: \_\_\_ Yes \_\_\_ No

Are Payments Accepted via telephone: \_\_\_ Yes \_\_\_ No

Are Payments Accepted via online: \_\_\_ Yes \_\_\_ No

Are Payments Accepted via fax: \_\_\_ Yes \_\_\_ No

Are Payments Accepted via e-mail: \_\_\_ Yes \_\_\_ No

I hereby certify the appropriate means of payment card data collection/processing is properly identified as stated above and I have read the University Policies related to Payment Cards, Fees and Funds Handling:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Merchant Card Payment Card Coordinator Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Department Head Date

# **VI. Overview of Activity**

Brief Description of the activities for which payment cards are accepted:

List of location(s) where cardholder data is collected:

List all equipment that is used for payment card processing to include the following:

* Computers (include asset tag number, make, model, serial number, and assigned custodian).
* Point of Sale/Swipe Terminals (include asset tag number, make, model, and serial number).
* Fax Machine (include make, model, serial number).
* Other (specify): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (include any identifying information similar to above).

List of all third party service providers involved in payment card processing including payment gateways and merchant processors.

List of all locations where payment card data is stored, whether electronic or physical, to include the following:

* Business justification for storing the payment card data.
* Security precautions and practices taken to protect the payment card data.
* Names/titles of all persons who have access to the payment card data.
* Retention period and methods used to destroy the payment card data.

# **VI. Procedures**

\*Sections not applicable to how your department processes may be deleted.

**Method of Payments**

1. In Person Payments:

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 (Reference appendix if applicable)
2. 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.
		3. 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.
		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.
		6. 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.
	2. Risks of Keyed Transactions
		1. 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
			* Ask the cardholder to sign the paper receipt and compare the signature
	3. Report Suspected Card Fraud
		1. If you suspect the card is fraudulent, report it following the security breach steps defined below.
3. Retain the signed merchant copy of the swipe machine-generated receipt and return the other copy to the cardholder.
4. Place the merchant copy of the receipt \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ until the End of Day batch process has been run.
5. 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*) *Card Reader Tamper Inspection Log* 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 per the steps defined below.
	3. 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):

* Primary:
* Backup:

<<Add Departmental specific procedures here>>:

1. Mailed in Payments:

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

1. At least two people should be responsible for opening the mail and logging any payment requests onto the *Receipt Mail Log*. 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 to use if credit is later issued.
7. If necessary, forward the payment confirmation other applicable parties.
8. Place the merchant copy of the receipt \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ until the End of Day batch process has been run.

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

* Primary:
* Backup:

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

* Primary:
* Backup:

<<Add Departmental specific procedures here>>:

1. Telephone Payments

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

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 *(optional)* **Telephone Payments Form** 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):

* Primary:
* Backup:

<<Add Departmental specific procedures here>>:

1. Fax Payments

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

1. 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.
2. Use of a multi-function printer / fax machine can increase the PCI scope and is prohibited, a plain paper, dial up fax is recommended.
3. 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.
4. 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.
5. The receipt must only contain that portion of the account number allowed in the current PCI Data Security Standards, i.e. last four digits.
	1. The merchant copy must be attached to the fax and filed in the designated place for later reconciliation.
	2. The customer copy may be faxed, mailed, or emailed to the customer (optional).

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

* Primary:
* Backup:

<<Add Departmental specific procedures here>>:

1. Online Payments

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

1. 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.
2. 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.
3. 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):

* Primary:
* Backup:

<<Add Departmental specific procedures here>>:

**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…………………….

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

* Primary:
* Backup:

**Reconciliation process:**

All departments are required to:

1. Close out and settle their payment card terminals or web-based applications daily.
2. Reconcile transactions on their Daily Settlement Reports against their \_\_\_\_\_\_\_\_\_\_ 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 as requested.

All refunds should be processed …………………..

If any consumer disputes (chargebacks) are received, the notice should be sent immediately to the University Bursar with a copy of the original transaction and an explanation of why the money should not be returned.

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

* Primary Preparer:
* Backup Preparer:
* Primary Reviewer:
* Backup Reviewer:

**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.

**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.

**Inspection of Equipment**

Regularly inspect (*specify timeframe*) credit card processing equipment to ensure there is no evidence of tampering and document inspections in a log (see Appendix ?). Inspections must check for the following:

1. Serial number(s) match
2. Model number(s) match
3. Any tamper evident stickers are intact
4. Foreign objects are not attached
5. No evidence of pry marks or bent, broken, or stressed seams
6. Anything unusual

**Responding to Cardholder Data sent through e-mail:**

Any open communication system such as email or chat programs are not considered secure for the transmission of any payment card information. If payment information is sent 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 name)*. We appreciate your correspondence, 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.

**Person Log:**

List of all persons involved in the handling of payment card transactions and their role. Documentation must be maintained verifying that each person has read the Radford University *Payment Card Policy/Procedure* and all payment card procedures as well as attended annual required training. This information may be maintained in a separate log but must include all applicable information.

# **VI. Reporting Suspected Security Events or Fraud**

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

1. Immediately notify your supervisor, merchant card payment coordinator, department head, University Controller, and the Information Security Officer.
2. If the suspected activity involves computers (hacking, unauthorized access, etc.) make sure you contact itsecurity@radford.edu.

If you are unsure, but suspect fraud related to payment card activities, you should report in compliance with the University’s [*Fraud, Waste and Abuse Policy*](https://www.radford.edu/content/dam/departments/administrative/policies/GeneralPoliciesandProcedures/GEN-PO-1003_FraudPolicy.pdf).

# **VII. Annual PCI Compliance**

1. If applicable, 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 policies herein are effective {DATE}. This policy shall be reviewed and revised annually.

Approved:

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

Merchant Card Payment Coordinator

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

Department Head

Date Approved: {DATE}

Date Revised: {DATE}