**Payment Card Processing**

**Department:**

**Date:** 24 January 2018

**General Information**

Hardware:

Third-party vendors:

Processors:

**Required Documentation**

Departmental procedures: Information detailing how credit cards are accepted, processed, and documented.

Quality Control Check List: Credit cards terminals periodically inspected to verify make, model, and serial numbers; additionally, a surface inspection preformed to identify attempted tampering or unexpected attachments.

PCI DSS Security Awareness Roster: Comprehensive list of everyone authorized to process payment cards.

**Processing**

*Describe in detail the procedures for accepting and processing each payment method and the system and/or hardware used to complete the transaction.*

Card present:

Phone:

Mail:

Online:

**Refunds**

*Describe in detail how a refund is processed, the system or hardware used, and personnel permitted to perform refunds.*

**Deposits**

*Describe in detail the steps for documenting deposits.*

Network File locations:

Deposit Certificate Log(s):

Deposit Transmittal Form (DTF):

Deposit Certificate Number Range:       to

**Security Incident**

*An ‘incident’ is defined as a suspected or confirmed ‘data compromise’. A ‘data compromise’ is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted data is collected, processed, stored or transmitted; Payment Card data is prohibited data. A ‘data compromise’ can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.*

In the event of a suspected or confirmed incident:

1. Contact the Response Team by sending an email documenting the incident to:

**howdysjw@jmu.edu and e-commerce@jmu.edu**.

1. The Response Team will immediately coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident.
2. If the incident involves a payment station (PC used to process credit cards):
   1. Do NOT turn off the PC.
   2. Disconnect the network cable connecting the PC to the network jack.
3. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
4. Assist the Response Team as they investigate the incident.

**Financial Procedure 4125 - Payment Cards**

**.100 General**

Prior to implementation and use, initial payment card activity at James Madison University must be approved by the Assistant Vice President for Finance.

Once authorized to sell merchandise or rent university facilities by the Assistant Vice President for Finance, departments are required to comply with Virginia Retail Sales and Use Tax Collection requirements.

* Contact the Cash & Investments Office for specific procedures prior to initiating any sales/rentals.

Additional procedures for payment card activity for Local/Agency Fund accounts are included in Section 3045, "Local/Agency Funds".

**.200 Control Responsibilities**

* All James Madison University departments, affiliates, and vendors must maintain compliance with the current version of the Purchase Card Industry – Data Security Standards (PCI-DSS)
* Departments will request PCI-DSS Security Awareness Training through the University Business Office for all new employees (including students) who have been designated to handle any aspect of payment card processing.
  + Background checks must be completed for all employees who process payment cards, have payment card system logins, or in any way interact with cardholder data.
* Only a minimum number of employees whose job responsibilities requires access to cardholder data should have such access.
* Departments shall complete the appropriate Self-Assessment Questionnaire in coordination with the University Business Office on an annual basis
* Departments shall ensure appropriate security controls are in place related to payment card transactions:
  + All payment card refunds are required to be placed back on the same payment card as used in the original sale. In cases where the original card has since closed, the department is required to contact the University Business Office at 8.4674 for further instruction in how to proceed with the refund process.
  + All employees given access to payment card information shall have completed PSI DSS Security Awareness training within the past twelve months.
  + Supervisors shall request background checks for student employees through Student Work Experience Center (SWEC). For all Faculty and Staff, the background check is done automatically through Human Resources during the OnBoard process.
  + Once PCI-DSS Security Awareness Training has been completed, submit the staff terms of agreement for the trainee to the University Business Office.
  + Departments are not permitted to store cardholder data.
    - All post-authorization payment card information is required to be destroyed in a PCI-compliant manner, such as cross-cut shredder or outsourced service.
    - All customer and merchant receipts shall only show truncated card numbers - the first six and last four digits are allowed.
* Departments currently accepting payment cards are required to maintain the following documentation.
  + Departmental Procedures- written documentation of department specific payment card policies.
  + PCI-DSS Security Awareness Roster- a list of all individuals within the department who can interact with cardholder data.
  + Quality Control Check List- used to document the inspection of payment card terminals.

**Notes:**

* All payment handling operations are subject to review and/or audit by the University Business Office as well as the university's internal and external auditors. The University Business Office surveys university departments regularly to identify all payment collection points. If the controls are inadequate, corrective action will be taken.
* When a department wants to expand upon current services offered by a vendor, the department must contact the University Business Office for a PCI Review in order to determine how the system changes will impact James Madison University’s PCI Scope.
* James Madison University has committed to reducing our PCI Scope; as such any new or existing vendor’s application that would increase the university’s PCI scope is prohibited.

**.210 University Business Office**

* The University Business Office shall provide PCI-DSS Security Awareness Training to all university employees who interact with cardholder data upon hire, reoccurring annually thereafter.
* The University Business will coordinate with JMU IT to provide and maintain a secure cardholder data environment that complies with the current PCI-DSS.
* The University Business Office works with JMU’s Security Advisor to assign departmental Self-Assessment Questionnaires.
* The University Business Office initiates annual completion of Self-Assessment Questionnaire.

**.300 Processing Procedures**

**.310 Assistant Vice President for Finance**

* Authorize departments to sell goods and services in accordance with Commonwealth regulations.
* Approve exceptions to daily requirements as appropriate.

**.320 University Business Office**

* Provide departments who currently accept payment cards the appropriate deposit transmittal forms and instructions.
* Monitor and audit departmental payment card processing.
* Update departmental staff on PCI-DSS compliance changes.
* Provide departments with a sequence of numbers to be used for Deposit Certificate numbers.
* Coordinate with Wells Fargo to establish merchant identification numbers for departments who have been authorized to accept payment cards.
* Assist departments in acquiring appropriate payment card processing equipment or implementing approved online payment sites.
* Assist in resolving problems encountered in monthly reconciliation process of payment card transactions.
* Perform scheduled and unscheduled audits.
* Payment card chargebacks (when the bank retrieves funds from the university's local bank account due to a customer disputed payment card charge)- the University Business Office will complete all paperwork associated with the chargeback and coordinate with the department and the customer in order to reimburse the chargeback.

**.330 Departments**

* Once a department has been approved to process payment cards, the University Business Office will obtain merchant numbers for Visa, MasterCard, Discover, and American Express (if applicable).
* All payment card equipment and terminals will be obtained by the University Business Office for the department. Equipment costs will be billed to the department the following month.
* Departments are responsible for contacting the University Business Office in regards to any terminal issues or error messages that may appear on the terminal. Departments are not permitted to order new equipment or replace existing payment card terminals. If the payment card processor recommends a replacement terminal, the department shall contact the University Business Office for guidance.
* When applicable to job responsibilities, departments will request access to online transaction management sites through the University Business Office.
* Departments shall ensure proper separation of duties exists, payment handling, record keeping, and reconciliations should be assigned to different staff members. If the size of the department makes proper separation of duties impossible, a second person must verify reconciliations of funds received and accounts maintained.
* Departments will prepare Deposit Transmittal Forms daily based on deposits of funds received the previous business day.
  + The department will obtain the payment card version for the Deposit Transmittal Form from the University Business Office. This payment card version is not available online.
  + The department will obtain a unique Deposit Certificate (DC) number from the department’s log for each payment card Deposit Transmittal Form.
  + This form must be delivered to Financial Reporting at MSC 5715 within three business days for keying into the university finance system. See section .400 for correct preparation instructions.
* Processing payment card information received in an email is strictly prohibited. Respond to all emails which include payment card information by deleting the payment card information and including instructions for re-submission through an approved method.
* Retain all necessary documentation- merchant copy receipts, batch reports, copy of deposit transmittal forms, monthly reconciliations.
* The department must reconcile their departmental budget monthly comparing the university finance system reports to departmental records.

**.400 Forms Preparation and Submission**

* Deposit Transmittal Form (DTF): This form is required to transmit deposit information and expenditure credit items for Treasurer of Virginia revenue items for input to the Financial Information System.
  + The payment card version of the Deposit Transmittal Form is only available from the University Business Office and is not available online.
  + The original payment card version of the Deposit Transmittal Form is sent to the Financial Reporting Office at MSC 5715. The department must keep a copy for departmental files.
  + When depositing payment card transactions, the Deposit Transmittal Form must be delivered to Financial Reporting within three business days, after the deposit date.
* Following are instructions for preparation of the FIS Deposit Transmittal Form. Enter information in the following categories ONLY.

|  |  |
| --- | --- |
| DC #: | Enter the Deposit Certificate number on the Deposit Transmittal Form using a sequence of numbers provided by the University Business Office. |
| Prepared By: | Name of the person completing the form, initial beside typed name. |
| Dep. Date: | Enter the date the deposit is being made. |
| Date: | Enter the date the form is prepared. |
| Phone/E-Mail: | Phone number and/or e-mail address of the preparer. |
| Bank Code: | Enter TV for Treasurer of Virginia deposits. (Consult Financial Procedures Manual section 3045.300, "Local/Agency Funds" for deposits to Dept. ID#’s starting with an 8.) |
| MSC: | Enter the MSC of the preparer. |
| Bank Acct.: | Enter CH03 for Treasurer of Virginia payment card deposits. All payment card deposits, and ONLY payment card deposits, are CH03. |
| Amount: | Enter and verify the total amount of the deposit, if completed electronically this total is automatically calculated. |
| Line Count: | This field will automatically populate. |
| Explanation: | Indicate any additional facts related to the origin and/or the nature of the deposit. The batch settlement confirmation number may be listed here. |
| Payment Cards: | Only option available on the payment card version of the Deposit Transmittal Form. |
| Discover/MasterCard/Visa: | Select if the deposit is for Discover/MasterCard/Visa transactions. The deposit will arrive from FNBO (First National Bank of Omaha). |
| American Express: | Select if the deposit is for American Express. The deposit will arrive from American Express. |
| Dept. ID #: | Enter the six-digit department identification number. Refer to Section 2010, "Department Numbers" Numerical Listing. |
| Account #: | Enter the six-digit revenue source code. Refer to Section 2020, "Revenue Account Codes and Definitions". |
| Description of Deposit: | Indicate the origin and/or nature of the deposit. |
| Amount: | Summarize the receipts by revenue account codes and Dept. ID#’s and enter the amount for each code. For unidentified items, list each amount collected separately. Payment Card amounts must be recorded, by day, on a separate Deposit Transmittal form. These amounts should not be included with cash and check receipts. |
| D/C: | Enter a "C" if the deposit is a credit to Dept. ID # - enter a "D" if the deposit is a Debit to the Dept. ID. |
| Total: | Enter and verify the total amount of the deposit, if completed electronically this total is automatically calculated. |

*Notes for payment card deposit preparation:*

1. Payment card terminal sales are batched once, daily for every payment card machine in the department.
2. If the deposit you are making has refunds included in the total, list the sales on the deposit transmittal as a "C" credit and the refunds as a "D" debit to get a "net" total.
3. The department is required to utilize clientline.net for all Visa, MasterCard, and Discover transactions and americanexpress.com for American Express transactions (if applicable) on a daily basis to retrieve actual deposit dates and deposit totals. All departments have been given access to these sites for their respective merchant numbers. Step by step procedures or access to these sites can be obtained by contacting the Compliance Specialist in the University Business Office at 8-4674. By using these sites correctly, James Madison University ensures it is in compliance with the Commonwealth of Virginia’s CAPPS manual which states:
   * “There MUST BE A ONE-TO-ONE MATCH between the deposit entry that posts to the Treasurer's bank account and the deposit total reported in Cardinal. The AMOUNTS MUST BE THE SAME regardless of the method of input to Cardinal. DEPOSITS MUST BE SEGREGATED BY TYPE so that different types of deposit activity are not commingled on a deposit form (i.e., cash deposits should be separated from credit card receipts). Each type of deposit activity noted below must be reported on a separate deposit form, using a separate DC number.

**.410 Deposit Certificate Sequencing**

Treasurer of Virginia Deposit Certificate numbers are obtained through the University Business Office. The department should maintain an Excel spreadsheet of these numbers to keep track of the DC numbers used, deposit date, amount, and card type deposit. The department must only use the numbers within their sequence and restart the sequence each July 1. If a department runs out of numbers within their designated sequence within the fiscal year, contact the University Business Office for another set of numbers—do not go past your designated numbers or reuse DC numbers.

**.500 Deposit Reconciliation**

A monthly written reconciliation comparing revenue deposited- to university FIS reports is required. Auxiliary Enterprises accounts (Nos. 3xxxxx) are reconciled by comparing the department's internal records to university monthly FIS reports. Educational and General Accounts (Nos. 1xxxxx) are reconciled by comparing revenue transaction documents to University monthly FIS reports.

**.520 Who Should Perform the Reconciliation?**

Departments accepting payment cards are responsible for reconciling their FIS Monthly detail reports as described in Financial Procedures Manual Section 3035. The individual responsible for preparing the deposit should not be assigned this responsibility.

**.530 Reconciliation Differences:**

If differences other than timing differences are encountered, contact the University Business Office to determine the proper adjustment. For transaction research assistance, contact [e–commerce@jmu.edu](mailto:e–commerce@jmu.edu).