# Departmental Payment Card Handling Guidelines

[Department – Merchant Name]

**Purpose**

|  |
| --- |
| **GUIDANCE:** Collection and processing of card payments must be conducted in compliance with standards established by the **Payment Card** Industry Security Standards Council (PCI SSC), W&M Payment Card Policy & Procedures, and the guidelines outlined in this document. Departments are responsible for ensuring all processes, procedures, and technologies follow the security standards dictated by the PCI DSS and as approved by Financial Operations, Information Technology, and the PCI Committee.  This document provides the required business guidelines departments must follow. As such, these guidelines may either be used as a template to create departmental procedures or incorporated into existing procedures. All departments must have procedures documented and available for staff reference/training. In addition, the PCI Committee, Internal Audit or external auditors may ask to review these procedures. Departments are responsible for reviewing their procedures annually and/or updating as requirements change. |

[Suggested opening paragraph]

These card handling procedures document how credit card payments are handled for the merchant called [name of merchant]. These procedures are in accordance with the standards established by the **Payment Card** Industry Security Standards Council (PCI SSC) and [W&M Payment Card Policy & Procedures](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/index.php). [Merchant name] is responsible for ensuring all processes, procedures, and technologies follow the security standards dictated by the PCI DSS and as approved by Financial Operations, Information Technology, and the PCI Committee.  In addition, if [name of merchant] has not had any transactions in the past 12 -18 months, [name of merchant] will be terminated.

**Business Process - Accepting and Handling Card Payments**

**[**Insert summary of your business operations to include a brief overview of all systems/processes used in credit card processing.] Appendix A depicts the credit card data flow.

**User Access and Physical Security:**

|  |
| --- |
| **GUIDANCE:** Access to cardholder data (CHD) and equipment used to collect CHD must be limited to only those individuals whose job requires such access. Access to Point of Sale (POS) systems and any associated payment card devices is also restricted based on job responsibilities and must be tracked using the [**PCI DSS Security Awareness Program Roster**](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/paymentcardforms/pci-awareness-roster.xlsx). . If using an online system, must be able to view list of employees, their access and roles.  Devices that capture payment card data via direct physical interaction with the card should be physically secured and protected from tampering and substitution. Devices include card swipe terminals, Bluefin devices and approved single-use ipads. This includes daily inspections of the device surface to detect tampering and training personnel to be aware of suspicious activity. Departments must keep a log of all equipment inspections by documenting each inspection on the [W&M PCI Quality Control Checklist](file:///C:\Users\btflem\Box\PCI-CampusGuard\Final%20Docs\W&M%20pci-quality-control-checklist%20(D1).xlsx). User access to sensitive areas that store, process, or transmit cardholder data is restricted based on individual job function. ***Devices should be secured at all times whether locked in an office or a drawer when not in use*** to prevent tampering. |

[Suggested language]

Access to cardholder data (CHD) in [TouchNet and/or Clover Flex devices] is limited to only those individuals whose job requires access and authorized by the merchant/backup merchant manager. Access to CHD is restricted based on job responsibilities and must be tracked using the [**PCI DSS Security Awareness Program Roster**](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/paymentcardforms/pci-awareness-roster.xlsx).

.[TouchNet] The merchant manager requests access to TouchNet for each departmental user by submitting an IT ticket at [https://support.wm.edu](https://support.wm.edu/). The request must identify the role. (See Appendix A for TouchNet roles.) All logins to TouchNet are unique to the user and passwords are never shared. Only the merchant manager, designated W&M Bank Reconciliation Accountants, and IT Administrators have access to TouchNet/[merchant uStore/uPay site name]. The merchant manager reviews access annually as well as when personnel leave the department. All terminations are reported to IT for modifications in TouchNet access and recorded on the [**PCI DSS Security Awareness Program Roster**](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/paymentcardforms/pci-awareness-roster.xlsx).

[CloverFlex] The merchant manager/back-up merchant manager requests access to the Clover Flex device(s) using the [**Clover Flex Access/Termination Request**](https://forms.office.com/Pages/ResponsePage.aspx?id=Prw8uR1mWECGk6iXuSS413Hx59163WRHolslCcm0qllUNDJIWjZKU0FSMjJOQTQ2Q1pJWUNEREdDUC4u). All logins to the Clover Flex are unique to the user and PIN numbers are never shared. All terminations are reported using the same form. All information is also recorded on the Employee Access Log.

[Other Approved Systems/Devices – detail how access is granted/terminated for each employee.] The merchant manager/back-up merchant manager monitors access to any other approved systems/devices used to enter credit card data. [Explain how access is granted/terminated and tracked.]

**Annual Training:**

|  |
| --- |
| **GUIDANCE:** In accordance with PCI DSS Requirement 12.6.1, all users within the department authorized to handle card payments will complete the annual W&M Payment Card Industry DSS training. Employees will access this training through Cornerstone; students and volunteers will access it through Blackboard. This annual PCI DSS training is intended to promote employee awareness of technical and operational requirements to protect cardholder data. Upon hire, the department’s business process owner will notify the PCI Committee (pci@wm.edu) of any new staff required to complete training through Blackboard. Merchant Managers will direct all employees to Cornerstone for training. In addition, any new staff member is required to complete W&M Payment Card Security & Confidentiality Agreement, W&M Security Education and Awareness Training and the W&M Payment Card Industry training. Departments are responsible for tracking the initial completion as well as the annual completion of the agreement and training for each member using the [**PCI DSS Security Awareness Program Roster**](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/paymentcardforms/pci-awareness-roster.xlsx).  . |

[Suggested language]

The merchant manager and all department users who work in [TouchNet/CloverFlex or other approved system] complete the following training annually:

* W&M Payment Card Industry Training
* W&M Security Education and Awareness Training
* Merchant Manager training (merchant managers/back-up only)
* Payment Card Security & Confidentiality Agreement
* Department Card Handling procedures
* All associated policies and procedures as referenced on the W&M website for Payment Card Handling

Annual training including the acknowledgement of the W&M Payment Card Security & Confidentiality Agreement is tracked in Cornerstone for employees and in Blackboard for students/volunteers. The Merchant Manager is responsible for tracking all training using the [**PCI DSS Security Awareness Program Roster**](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/paymentcardforms/pci-awareness-roster.xlsx).

and reviewing the list annually to ensure each employee/team member has completed the training. The merchant manager is also responsible for providing training on the departmental procedures and usage of [TouchNet/Clover Flex/other approved system]. New hires who require access to [TouchNet, CloverFlex, other approved system] must complete all training, as outlined above, prior to using.

**Payment Card Devices or Other Approved Devices:**

|  |
| --- |
| **GUIDANCE:** Purchase of payment card devices, including mobile applications, must be coordinated through Financial Operations – Cashier’s Office. The Cashier’s Office will order the payment card devices, track and distribute to each merchant. Any other device used to accept payment cards must be approved by the PCI Committee, IT and Procurement. If necessary, certain approved devices may need to be configured by Information Technology. Only approved and tracked devices and locations may be used in any way associated with payment card processing. All devices must meet PCI DSS standards.   * The department is responsible for ensuring that only authorized staff have access to the device and are properly trained. * Devices must be [inventoried](file:///C:\Users\btflem\Box\PCI-CampusGuard\Final%20Docs\W&M%20pci-quality-control-checklist%20(D1).xlsx) with Financial Operations – Cashier’s Office and must be maintained in a secure location. * Other approved devices (i.e., Bluefins or single-use ipad) must be inventoried by the department and must be maintained in a secure location. * Sharing or transfer of wireless devices between departments is not allowed without proper approval from Financial Operations. * Hardwired devices ***may not be moved and plugged into a different network jack*** without approval and coordination from IT. * It is the department’s responsibility to coordinate efforts with Financial Operations or Information Technology to ensure that terminals/devices are updated with the most recent software version to reduce processing errors, etc. (For example, all approved single-use ipads must be taken to Information Technology for software updates, yearly.**)**   Departments may use request to use a Loaner card terminal through the Cashier’s Office. It can be used on a temporary basis to accept in-person card payments at specified times as agreed upon on the application, see [Merchant Payment Card Loaner Program](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/merchantpaymentcardloanerprogram/index.php). The loaner device must be kept in a secured location/locked when not in use. Use of loaner device follows the same processing procedures for in-person payments as outlined within this document. A loaner device is checked for tampering and the [W&M PCI Quality Control Checklist](file:///C:\Users\btflem\Box\PCI-CampusGuard\Final%20Docs\W&M%20pci-quality-control-checklist%20(D1).xlsx) is completed. |

[Suggested language]

[Merchant name] uses the Clover Flex payment device as issued by the Cashier’s Office.

* The merchant/backup merchant manager requests access for each team member based on job responsibilities.
* Each user has a unique PIN assigned to login. PINs are not shared.
* Devices are inventories and inspected [daily/weekly] by a team member. Results of the inspection is log in the W&M PCI Quality Control Checklist.
* Clover Flex is secured at all times. During non-business hours the device is locked [where]. [Detail where device is stored when no one is at the desk.]

[Merchant name/department area] uses an [approved device, name device] to enter [donations/ticket sales] on behalf of the customer. [These approved single-use ipads are configured by Information Technology.]

* The merchant/backup merchant manager configures the PIN access code per ipad.
* [Single-use ipads/Bluefins] are inventoried and inspected [daily/weekly] by a team member. Results of the inspection is log in the W&M PCI Quality Control Checklist.
* [Single-use ipad/Bluefin] is secured at all times. During non-business hours the device is locked [where]. [Detail where device is stored when no one is at the desk.]

**Online Card Services**:

|  |
| --- |
| **GUIDANCE:**  Usage of online card services must be coordinated through Financial Operations. Only approved vendors and associated payment providers may be used. All vendors/payment providers must meet PCI DSS standards. Each department is responsible for ensuring that only authorized staff have access to the online card service and are properly trained.     * Merchants using an online card service (TouchNet uStore/uPay, Authorize.net, Blackbaud Merchant Services or other approved vendor) must only handle payment card transactions that have been processed through the vendor. Merchants may not process face-to-face transactions where they enter information into a website for a customer as this is not compliant with PCI DSS and violates W&M compliance. If exceptions are needed, please contact the PCI Committee for an authorized solution. * Do not use group, shared, or generic IDs, passwords, or other authentication methods. Use unique IDs for each user, with unique passwords for each. The longer the password, the better. Default or generic IDs on all systems that store, process, or transmit CHD must be removed or disabled. * **Never** direct a payer to a specific computer or offer to enter payment card data into a website on their behalf. Advise the individual to use “any internet enabled device” to complete the transaction on their own. |

[Suggested language]

[Merchant name] uses [system name, i.e., the integrated TargetX/TouchNet uPay]. [Software name] is an approved W&M ecommerce solution.

* [Merchant name] only handles payment card transactions that have been processed through the [software name]. Merchant personnel DO NOT process face-to-face transactions where card information is entered directly into a website for a customer, as this is not compliant with PCI DSS and violates W&M compliance. [If an approved solution has been granted, detail here.]
* Each authorized user has a unique login/password. The merchant manager requests users to be setup in [system - how]. Each user creates their own password.
* [Merchant name] does NOT direct a payer to a specific computer or offer to enter payment card data into a website on their behalf. Team members may advise the individual to use “any internet enabled device” to complete the transaction on their own.

**Batch Settlement:**

|  |
| --- |
| **GUIDANCE:** Payment Card Devices must be settled no less frequently than daily. It may be prudent, given the level of activity, to settle batches on a more frequent basis. The department must maintain all signed receipts and card swipe device Batch Total Settlement Reports for the designated timeframe as established by the Library of Virginia. Refer to the [W&M Deposit and Cash Receipting Procedures](https://www.wm.edu/offices/financialoperations/cashiering/forms/index.php) for additional guidance. |

[Suggested language for Clover Flex]

Clover Flex is closed out daily. If necessary, based on volume, a batch may be closed/settled during the day. [merchant name] has access to all receipts and closeout reports via the Clover Flex dashboard.

**Banner Cashiering:**

|  |
| --- |
| **GUIDANCE:** Banner cashiering sessions are closed daily, settled and processed each night. At 8:00 AM EST, a batch for each merchant is closed for the previous day’s activity and sent to the credit card processor. Funds are posted to Bannerbased on the departments’ merchant account ID and index provided to Financial Operations on the W&M Payment Card Application. Departments will establish and maintain appropriate segregation of duties between card processing, processing of refunds, and the reconciliation of payment card transactions. Each department is responsible to reconcile sales transactions to their general ledger no less than monthly. |

[Suggested language if General Ledger integration w/Banner]

[Merchant] [system, i.e., TouchNet uPay/uStore] has a General Ledger integration to Banner. Funds are posted to Bannerbased on the merchant account ID and index provided to Financial Operations on the W&M Payment Card Application. The W&M Bank Reconciliation Accountant reconciles monies received at the bank with [system/TouchNet] and Banner each business day. The Merchant Manager is contacted with any issues of reconciliation or General Ledger Exceptions.

**Disputes and Chargeback:**

|  |
| --- |
| **GUIDANCE:** Financial Operations – Cashiering will receive and report chargebacks and transaction disputes to the department. (If departments receive any dispute or chargeback directly please notify the Cashier’s Office immediately upon receipt.) Departments can either accept or reject the chargeback. If rejected, the department will provide supporting documentation to justify that the transaction is valid. Failure to respond within the allocated timeframe will result in a loss to the department. Prompt attention to these matters is a priority. It is the department’s responsibility to develop appropriate internal controls to mitigate risks related to chargebacks. |

[Suggested language]

The merchant/backup merchant manager works with the Cashier’s Office on any reported disputes or chargebacks. If notified of either, the merchant/backup merchant manager will investigate the charge and provide all supporting information to the Cashier’s Office. If needed, the merchant/backup merchant manager will make the final decision on accepting the chargeback or continue the dispute process.

**Equipment & Use Overview:**

|  |
| --- |
| **GUIDANCE:** Physical Equipment: an inventory of equipment, if applicable, must be kept detailing the following information. |

[Suggested Language if using Clover Flex or others devices; N/A for online systems if no face-to-face]

The following is an inventory of the device(s) used:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Equipment Type | Equipment Name | Device ID | Serial Number | Location/Physical Security | Purpose of Use | |  |  |  |  |  |  | |  |  |  |  |  |  | |  |  |  |  |  |  | |

**Physical Security Procedures**:

|  |
| --- |
| **GUIDANCE:**   1. Upon hire, staff are trained to comply with standards established by the PCI DSS, W&M Mary Payment Card Policy, and the operational procedures of the department. In addition, staff are also trained to be aware of methods in which devices can be tampered with or replaced. Training includes the following:    1. Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.    2. Be aware of suspicious behavior. For example, attempts by unknown persons to unplug or open devices.    3. Do not alter or attempt to troubleshoot devices. Troubleshooting support is provided by Financial Operations/vendor. 2. At the start of each day (prior to use), the device surfaces are checked to detect tampering or substitution. Using the [W&M PCI Quality Control Checklist](file:///C:\Users\btflem\Box\PCI-CampusGuard\Final%20Docs\W&M%20pci-quality-control-checklist%20(D1).xlsx), verify that the device has not been swapped with a fraudulent device by performing the following steps:    1. Compare the serial number and model number listed on the device to that included on the Device Security Review Sheet.    2. Review the tamper evident stickers on the surface of the device and make sure it is intact.    3. Inspect the device and review for foreign objects (i.e. skimmers), unexpected attachments or cables plugged into the device, pry marks, broken or stressed seams.    4. If you notice anything unusual or suspect that the device has been tampered with or substituted, contact Financial Operations at [pci@wm.edu](mailto:pci@wm.edu).    5. When mobile devices are changing hands between department users, an **additional tamper check must be performed by the responsible party upon return.** |

[Suggested language]

1. Upon hire, all team members are trained to comply with standards established by the PCI DSS, W&M Mary Payment Card Policy, and the operational procedures of this department. In addition, team members are also trained to be aware of methods in which devices can be tampered with or replaced.

Training includes the following:

* 1. Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. All visitors are logged using the Visitors Log.
  2. Be aware of suspicious behavior. For example, attempts by unknown persons to unplug or open devices.
  3. Do not alter or attempt to troubleshoot devices. Troubleshooting support is provided by Financial Operations/vendor.
  4. Review of the [Clover Flex Tampering](https://www.eu.clover.com/gb/help/get-help-for-a-tampered-device/?device=FS34J11SImA6W8UGOUgeS).

1. At the start of each day (prior to use), a team member checks the device surfaces to detect tampering or substitution. Using the [W&M PCI Quality Control Checklist](file:///C:\Users\btflem\Box\PCI-CampusGuard\Final%20Docs\W&M%20pci-quality-control-checklist%20(D1).xlsx), verify that the device has not been swapped with a fraudulent device by performing the following steps:
   1. Compare the serial number and model number listed on the device to that included on the Device Security Review Sheet.
   2. Inspect the device and review for foreign objects (i.e. skimmers), unexpected attachments or cables plugged into the device, pry marks, broken or stressed seams.
   3. If you notice anything unusual or suspect that the device has been tampered with or substituted, contact Financial Operations at pci@wm.edu.
   4. When mobile devices are changing hands between department users, an **additional tamper check must be performed by the responsible party upon return.**

**Payment Card Processing Procedures**

|  |
| --- |
| **GUIDANCE:** Departments must document how orders/transactions are received. If a method is not applicable, state that the department does not accept cards in this manner. |

1. **IF: Mail Order – The department receives mail orders and credit card information is returned on the form.** 
   1. Process mail orders via swipe device
   2. Shred mailed in form containing CHD with a cross-cut
2. **IF: Fax Order – The department receives orders via fax at xxx-xxx-xxxx which is located xxxx. This fax machine is secured (how). NOTE:** Fax machine must be a stand-alone. It cannot be part of the all-in-one copiers.
   1. Process faxed order via swipe device
   2. Shred faxed order form containing CHD with cross cut shredder
3. **IF: Phone Order – The department will accept credit card orders via phone.**
   1. Credit card information will be taken and entered directly into credit card swipe device [or other approved device]. No numbers or information will be written down.
   2. Confirmation Number will be given to customer once card is accepted.
   3. Phone orders **MUST NOT** be entered into an online form/website. Contact the PCI Committee ([pci@wm.edu](mailto:pci@wm.edu)) for any exceptions. [Alter this bullet if department has an approved device to be used in conjunction with a website.]
4. **IF: Email Order - N/A – W&M does not accept credit card numbers sent in via email.** 
   1. The credit card payment will NOT be processed. If numbers are received via email a response will be sent to the customer.
   2. The response will be a separate email – not a response to the original email, indicating the policy and procedure for sending credit card information.
   3. The email will be permanently deleted from email in box and trash.
5. **IF: In Person – The department accepts credit card payment in person.** 
   1. Request card from cardholder for processing. Ensure card is signed, if not, request ID.
   2. Process transaction via swipe device ONLY. Online forms/website **CANNOT** be used unless approved by PCI Committee.
   3. Have customer sign merchant copy/receipt.
   4. Verify signature matches back of card. Ask for photo ID from any customer without a signature on back of card.
   5. Give card and receipt to customer.
6. **IF: Online Orders** 
   1. Online orders are received via the approved system (for example, TouchNet).
   2. Department individuals **CANNOT** submit orders on behalf of the customer. [If department has an approved device, alter this item to detail what approved device is used.]
   3. Department individuals with authorized access to system will fulfill orders on a daily basis.

**Refund Procedures:**

|  |
| --- |
| **GUIDANCE:** Clear disclosure of return, refund, and cancellation policies can help to prevent potential cardholder disputes/chargebacks.  Visa/MasterCard will support refund policies provided they are clearly disclosed to cardholders. Departments using an online system must communicate refund/return/cancellation policy either in the sequence of pages before final checkout with a click to accept button or checkbox on the checkout screen / location with electronic signature. |

1. The department’s refund policy is [state refund policy].
2. Procedures to refund a credit card transaction are included in the user manual for the [device name] devices and[system name].

**Incident Response Procedures:** An incident is defined as a suspected or confirmed data compromise in which there is a potential to impact the confidentiality or integrity of payment card data.  A data compromise is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted payment card data is collected, processed, stored, or transmitted. In the event of a suspected or confirmed incident:

1. Call theChief Information Security Officer at 221-1822 or email [abuse@wm.edu](mailto:abuse@wm.edu) with a description of the incident.
2. Do NOT turn off the PC.
3. Disconnect the network cable connecting the PC to the network jack. If the cable is secured and you do not have the key to the network jack, simply cut the network cable.
4. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
5. Assist the Response Team as they investigate the incident.

Revisions/Approvals

| Ver. # | Changes By | Ver. date | Reason |
| --- | --- | --- | --- |
|  | Bonnie Fleming | 11/4/2020 | Guidelines updated. |
|  | Bonnie Fleming | 8/31/2021 | Guidelines updated. |
|  | Bonnie Fleming | 3/16/2022 | Guidelines updated to include language for approved devices (i.e., approved single-use ipads). |
|  | Kelly Johnson | 9/26/2022 | Purpose to include termination clause. [PCI DSS Security Awareness Program Roster](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/paymentcardforms/pci-awareness-roster.xlsx) replaces Access Log where it was mentioned. |
|  | Bonnie Fleming | 5/8/2023 | Added data flows. |

## Appendix A - Data Flow

|  |
| --- |
| **GUIDANCE:** Select the data flow(s) that represent your business process(es). Delete those that do not apply. |

A picture containing text, diagram, screenshot, design

Description automatically generated

A diagram of a payment method

Description automatically generated with low confidence

A picture containing text, screenshot, online advertising, operating system

Description automatically generated

A picture containing text, screenshot, diagram, design

Description automatically generated