***NOTE: This template should be used by University units to document their internal procedures for handling payment card transactions. Make appropriate changes to ensure that it reflects your unit’s operations. Pay special attention to* *highlighted sections.***

Unit Payment Card Plan

Type Unit Name Here

Type Unit Name Here is approved by Treasury Services as a University merchant, allowing us to accept payment cards for our transactions.

To maintain our merchant status and support PCI compliance, our unit maintains this Unit Payment Card Plan, documenting how we accept and process payment cards.

This plan will be updated annually as part of our unit’s ongoing PCI compliance efforts.

[**1.0 Merchant Overview**](#_heading=h.30j0zll) **[2](#_heading=h.30j0zll)**

[1.1 Merchant IDs](#_heading=h.1fob9te) [2](#_heading=h.1fob9te)

[1.2 Acceptable Payment Methods](#_heading=h.3znysh7) [2](#_heading=h.3znysh7)

[1.3 Third Parties](#_heading=h.2et92p0) [3](#_heading=h.2et92p0)

[**2.0 Unit Management**](#_heading=h.tyjcwt) **[4](#_heading=h.tyjcwt)**

[2.1 Employee Authorization and Training](#_heading=h.3dy6vkm) [4](#_heading=h.3dy6vkm)

[2.2 Data Retention and Disposal](#_heading=h.1t3h5sf) [4](#_heading=h.1t3h5sf)

[2.3 Device Inspection](#_heading=h.4d34og8) [4](#_heading=h.4d34og8)

[2.4 Report Fraud and Noncompliance](#_heading=h.2s8eyo1) [5](#_heading=h.2s8eyo1)

[2.5 Back Office Procedures](#_heading=h.17dp8vu) [5](#_heading=h.17dp8vu)

[2.5.1 End of Day Batch Process](#_heading=h.3rdcrjn) [5](#_heading=h.3rdcrjn)

[2.5.2 Reconciliation Process](#_heading=h.26in1rg) [5](#_heading=h.26in1rg)

[**3.0 Processing Procedures**](#_heading=h.lnxbz9) **[6](#_heading=h.lnxbz9)**

[3.1 In-Person (Card Present) Payment Procedures](#_heading=h.35nkun2) [6](#_heading=h.35nkun2)

[3.2 Online Payment Procedures](#_heading=h.1ksv4uv) [7](#_heading=h.1ksv4uv)

[3.3 Mailed Payment Procedures](#_heading=h.44sinio) [7](#_heading=h.44sinio)

[3.4 Telephone Payment Procedures](#_heading=h.2jxsxqh) [8](#_heading=h.2jxsxqh)

[3.5 Faxed Payment Procedures](#_heading=h.z337ya) [8](#_heading=h.z337ya)

[3.6 Handling Payment Information Received through Insecure Channels](#_heading=h.3j2qqm3) [9](#_heading=h.3j2qqm3)

[**4.0 Compliance Activities**](#_heading=h.1y810tw) **[10](#_heading=h.1y810tw)**

[4.1 Attestation](#_heading=h.4i7ojhp) [10](#_heading=h.4i7ojhp)

[4.2 Assessment](#_heading=h.2xcytpi) [10](#_heading=h.2xcytpi)

[4.3 Incident Response](#_heading=h.1ci93xb) 10

# 1.0 Merchant Overview

## 1.1 Merchant IDs

We have been issued the following Merchant IDs for our processing activities:

|  |  |
| --- | --- |
| **MID** | **Purpose** |
|  |  |
|  |  |
|  |  |

## 1.2 Acceptable Payment Methods

All payment methods and solutions require the prior written approval of Treasury Services.

**Our unit accepts payment cards via the following methods:**

|  |  |  |
| --- | --- | --- |
| **Method** | | **Description (purpose and method)** |
| ☐ | In-person (card present) |  |
| ☐ | Online |  |
| ☐ | Mailed |  |
| ☐ | Telephone |  |
| ☐ | Faxed |  |
| ☐ | Other (describe) |  |

**\*\*NOTE\*\* The following payment methods are PROHIBITED:**

1. Emailed credit card numbers
2. Direct entry into workstations
3. Use of any non-PCI Validated Point to Point Encrypted (P2PE) solutions
4. Use of unapproved mobile devices
5. Use of unapproved self-service terminals or kiosks
6. Faxed credit card numbers (via IP and/or multi-function fax machines)

## 1.3 Third Parties

Type Unit Name Here engages the following third parties to assist with our processing activities with the approval of Treasury Services:

|  |  |  |
| --- | --- | --- |
| **Third party** | **Description of services** | **Contact information** |
|  |  |  |
|  |  |  |
|  |  |  |

On an annual basis, our unit will request proof of the above third parties’ PCI compliance and provide such documentation to Treasury Services.

# 2.0 Unit Management

## 2.1 Employee Authorization and Training

Employees will be authorized to process payment cards according to legitimate business needs. Employees will be issued and/or use unique, non-shared accounts for all card processing activities. Access and authorizations will be reviewed and recertified annually.

Employees are required to complete institutional PCI compliance training and attest that they understand their responsibilities before they may begin handling payment cards or cardholder data. Training and results must be kept for audit purposes.

## 2.2 Data Retention and Disposal

Cardholder data will be recorded only when necessary, retained only until payment is processed, and securely disposed of immediately after processing:

1. 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.
2. Cardholder data will never be stored in electronic form.
3. Cardholder data in paper form
   1. will be stored in a locked safe accessible only to authorized employees
   2. will be processed as soon as possible
   3. will be cross-cut shredded immediately after processing
   4. will not include CVV code or cardholder PIN.

## 2.3 Device Inspection

Payment card terminals or similar devices will be inventoried and inspected for tampering or substitution and documented <indicate frequency> using the UD PCI Device Inventory and Tampering Checklist Form:

1. Verify the serial/model number on the device sticker matches the serial/model number displayed electronically on the device.
2. Verify tamper evident stickers or seals covering screw holes or seams on the device have not been removed, re-affixed or altered in any way.
3. Verify that no foreign object (unfamiliar electronic equipment, device, keypad overlay, wire, or cable) is connected to or placed near the device.
4. Verify that there are no modifications (pry marks, or bent, broken, or stressed seams) to the device.

Each Unit is required to keep a log with the date of inspection and inspector’s signature. These logs should be kept for 3 years for audit purposes.

Evidence of tampering or substitution must be immediately reported to the unit head, Treasury Services, and the IT Security Office.

## 2.4 Report Fraud and Noncompliance

Employees should report signs of fraud and insecure or questionable activities to the unit head and/or Treasury Services.

* Fraudulent processing activities (e.g., use of stolen or altered cards).
* Processing payment cards using unauthorized or insecure methods, systems, or services.
* Improper recording, storage, or disposal of payment information.

## 2.5 Back Office Procedures

### 2.5.1 End of Day Batch Process

Type Unit Name Here’s procedures to settle all transactions at the end of each day are as follows:

1. Step 1 (please include the details of each step here)
2. Step 2
3. Staple the settlement sheet in front of the sales receipts and
   1. Either store in a secure location (i.e. a locked safe or locked drawer) until morning
   2. Or deliver to Treasury Services, who is responsible for GL entries.

### 2.5.2 Reconciliation Process

1. Close out and settle their payment card terminals or web-based applications daily.
2. Reconcile transactions on their Day 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 filled in a secure location and available for review by Treasury Services.

All refunds should be processed and entered into by Treasury Services.

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

# 3.0 Processing Procedures

## 3.1 In-Person (Card Present) Payment Procedures

Type Unit Name Here’s procedures for accepting in-person payments are as follows:

1. Confirm the transaction amount.
2. Verify the cardholder and payment card prior to processing the payment.
   1. Inspect the expiration date on the card (the card may not be used after the last day of the expiration month embossed on the card).
   2. Ask for ID to ensure the actual card/account holder is using the card. Please note: customers are not required to show ID if the cardholder’s signature is on the back of the card.
   3. Ensure the customer's signature on the charge form matches 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. Check to be sure that the card has not been taped over, mutilated, erased, or painted over.
   5. Verify the account number on the front of the card matches the number on the back of the card and the terminal receipt display (mis-matched, covered or chipped numbers could indicate an altered card).
   6. Verify the name on the customer receipt matches the embossed name on the front of the card (mismatched names could indicate an altered card).
   7. If you suspect the card is fraudulent, report it as per Section 2.4.
3. Process the payment using a university-owned PCI validated P2PE payment terminal.
   1. Never enter cardholder data directly into a workstation or unapproved device.
   2. If payment must be processed at a later date,
      1. record the payment information in paper form
      2. store the paper in a locked safe accessible only to authorized employees
      3. process the payment as soon as possible
      4. cross-cut shred the paper immediately after processing.
4. Print two copies of the receipt.
   1. Have the cardholder sign the merchant copy of the receipt.
   2. Return the customer copy of the receipt to the cardholder.
   3. Place the merchant copy of the receipt \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ until the End of Day batch process has been run.

## 3.2 Online Payment Procedures

Online payments must be customer-initiated and must not be entered online by Type Unit Name Here staff on behalf of a customer—i.e., **never use online payment forms to directly enter payment information at the point of sale**. Transactions entered by unit staff on behalf of a customer must be processed according to telephone payment procedures.

Instruct customers to submit payments using their personal device. Never provide—and never instruct customers to use—public workstations or unapproved self-service kiosks to enter payment information.

To correct issues with online payment services, contact your software application support team, [support@arrowpayments.com](mailto:support@arrowpayments.com), or [cashcontrol@udel.edu](mailto:cashcontrol@udel.edu).

## 3.3 Mailed Payment Procedures

Customers may mail payment requests to [approved address].

Type Unit Name Here’s procedures for accepting mailed payments are as follows:

1. Log mailed payments upon receipt.
   1. At least two people should be responsible for opening the mail and logging any payment requests. If possible, these staff members should alternate days.
   2. The receipt of mailed in payments should be recorded on a locked spreadsheet, with specific personnel with access to password to eliminate editing of the spreadsheet. Only the customer’s name, date of payment receipt, and last 4 digits of the card should be recorded on the spreadsheet. It is strictly prohibited to save the full card number and/or CVV in any electronic format.
   3. Bundle together all payment requests and attach a cover sheet with the date, count of requests, and initials of the person opening the mail.
   4. Hand over the bundle to the person responsible for entering the payment(s).
2. Process the payments immediately (in no case later than 2 business days after receipt) using a payment terminal.
   1. Never enter cardholder data directly into a workstation or unapproved device.
   2. If payment must be processed at a later date, store the payment requests in a locked safe and process the payment as soon as possible.
   3. Cross-cut shred the portion of the form containing the payment card information immediately after the transaction has been processed.
3. Print two copies of the receipt.
   1. Return a copy of the receipt to the customer via the approved departmental method which is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   2. Place the merchant copy of the receipt \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ until the End of Day batch process has been run.
      1. Retain \_\_\_\_\_\_\_\_\_\_\_\_\_to use if credit is later issued.

## 3.4 Telephone Payment Procedures

Type Unit Name Here’s procedures for accepting telephone payments are as follows:

1. Accept telephone payments only during live telephone calls.
   1. Do not process payment information submitted via voicemail. If you receive a voicemail containing payment information, follow the steps in Section 3.6 to respond.
2. Process the payments immediately (during the call if possible) using a PCI validated P2PE payment terminal.
   1. Never enter cardholder data directly into a workstation or unapproved device.
   2. If payment must be processed at a later date,
      1. record the payment information in paper form
      2. store the paper in a locked safe accessible only to authorized employees
      3. process the payment as soon as possible
      4. cross-cut shred the paper immediately after processing.
3. Print two copies of the receipt.
   1. Return a copy of the receipt to the customer via \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   2. Place the merchant copy of the receipt \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ until the End of Day batch process has been run.
      1. Retain \_\_\_\_\_\_\_\_\_\_\_\_\_to use if credit is later issued.

## 3.5 Faxed Payment Procedures

Type Unit Name Here will only accept faxed payments via an analog, single-function fax (no document scan or copy functionality) machine kept in a locked office.

Type Unit Name Here’s procedures for accepting faxed payments are as follows:

1. 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.
2. Process the payments immediately (in no case later than 2 business days after receipt) using a PCI validated P2PE payment terminal.
   1. Never enter cardholder data directly into a workstation or unapproved device.
   2. If payment must be processed at a later date, store the payment requests in a locked safe and process the payment as soon as possible.
   3. Cross-cut shred the portion of the form containing the payment card information immediately after the transaction has been processed.
3. Print two copies of the receipt.
   1. Return a copy of the receipt to the customer via \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   2. Place the merchant copy of the receipt \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ until the End of Day batch process has been run.
      1. Retain \_\_\_\_\_\_\_\_\_\_\_\_\_to use if credit is later issued.

## 3.6 Handling Payment Information Received through Insecure Channels

End-user messaging technologies—such as email, fax\*, voicemail, and text messaging—are not secure methods for transmitting payment information, and their use may potentially expose cardholder data and bring the University’s general network into scope. **These methods are prohibited for handling cardholder data. Never process a payment using these methods.**

*\*Faxed payments are insecure if accepted through an IP or multi-function fax machine.*

In the event that a customer submits cardholder data through an insecure channel:

1. Do not process the payment.
2. Notify the customer that the transaction cannot be processed as submitted (see example wording below).
   1. Remove any copies of cardholder data from your message prior to replying.
   2. Request that payment information be re-submitted via an approved method.
3. Securely destroy any messages or documents containing cardholder data (including messages in trash folders).

Responding to cardholder data received via an insecure channel:

Thank you for contacting Type Unit Name Here. 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, voicemail, etc.}. We ask that you use one of the following approved methods for making your payment:

* Online - {department website URL}
* Mail – {department mailing address}
* Phone – {department phone number}
* Fax – {department fax number}

*Delete the cardholder data from your message prior to responding, and delete the original message after replying, including your email’s Trash or Deleted folder.*

# 4.0 Compliance Activities

## 4.1 Attestation

The unit head will attest to Type Unit Name Here’s PCI compliance annually. Attestation activities include

1. completing applicable Self-Assessment Questionnaires (SAQ) at the instruction of Treasury Services
2. submitting a copy of this plan as documentation of our unit’s processing activities
3. submitting Attestations of Compliance (AOCs) from any service providers with whom cardholder data is shared, or that could affect the security of our customers’ cardholder data.

## 4.2 Assessment

Type Unit Name Here will support institutional risk assessment efforts as requested. Primarily, this means ensuring the accuracy of our unit’s SAQ responses and this payment card plan on at least an annual basis.

## 4.3 Incident Response

In the event of a suspected breach of security, employees must immediately and confidentially notify the unit head, Treasury Services and the IT Security Office. All evidence must be preserved until the IT Office has determined if a breach has occurred, scope of the breach, and forensic evidence has been gathered. This information is treated with confidentiality. Any and all communication to be handled by the Incidence Response Team.

IT maintains the Tier II Incident Response Plan, which includes procedures for responding to incidents affecting cardholder data or the CDE.

All staff members who process payment cards must aware of the signs of an incident, including

* evidence of tampering with, or substitution of, equipment
* unauthorized access to, or disclosure of, cardholder data.