The University of Delaware Payment Card Program

[**1.0 Overview**](#_heading=h.30j0zll) **[3](#_heading=h.30j0zll)**

[1.1 Applicability](#_heading=h.1fob9te) [3](#_heading=h.1fob9te)

[1.2 Authority](#_heading=h.3znysh7) [3](#_heading=h.3znysh7)

[1.3 Compliance and Exceptions](#_heading=h.2et92p0) [4](#_heading=h.2et92p0)

[1.3.1 Compliance Requirements](#_heading=h.tyjcwt) [4](#_heading=h.tyjcwt)

[1.3.2 Compliance Exceptions and Reporting](#_heading=h.3dy6vkm) [4](#_heading=h.3dy6vkm)

[1.3.3 Managing Noncompliance](#_heading=h.1t3h5sf) [4](#_heading=h.1t3h5sf)

[**2.0 Merchant Management**](#_heading=h.4d34og8) **[6](#_heading=h.4d34og8)**

[2.1 Application to Accept Payment Cards](#_heading=h.2s8eyo1) [6](#_heading=h.2s8eyo1)

[2.2 Merchant IDs](#_heading=h.17dp8vu) [6](#_heading=h.17dp8vu)

[2.3 Ongoing Management of Merchants](#_heading=h.3rdcrjn) [6](#_heading=h.3rdcrjn)

[2.3.1 Attestations of Compliance](#_heading=h.26in1rg) [7](#_heading=h.26in1rg)

[**3.0 Third-Party Management**](#_heading=h.lnxbz9) **[8](#_heading=h.lnxbz9)**

[3.1 Types of Third-Parties and Relationships](#_heading=h.35nkun2) [8](#_heading=h.35nkun2)

[3.1.1 Acquirers](#_heading=h.1ksv4uv) [8](#_heading=h.1ksv4uv)

[3.1.2 Payment Processors](#_heading=h.44sinio) [8](#_heading=h.44sinio)

[3.1.3 Service Providers](#_heading=h.2jxsxqh) [8](#_heading=h.2jxsxqh)

[3.1.4 Merchants](#_heading=h.2jxsxqh) [9](#_heading=h.2jxsxqh)

[3.2 Managing Third Parties](#_heading=h.z337ya) [9](#_heading=h.z337ya)

[3.2.1 Contracting with Third Parties](#_heading=h.3j2qqm3) [9](#_heading=h.3j2qqm3)

[3.2.2 Ongoing Management of Third Parties](#_heading=h.1y810tw) [10](#_heading=h.1y810tw)

[**4.0 Operations Management**](#_heading=h.4i7ojhp) **[11](#_heading=h.4i7ojhp)**

[4.1 Processing Activities](#_heading=h.2xcytpi) [11](#_heading=h.2xcytpi)

[4.1.1 Acceptable Payment Methods](#_heading=h.1ci93xb) [11](#_heading=h.1ci93xb)

[4.1.2 In-Person (Card Present) Payment Requirements](#_heading=h.3whwml4) [11](#_heading=h.3whwml4)

[4.1.3 Online Payment Requirements](#_heading=h.2bn6wsx) [12](#_heading=h.2bn6wsx)

[4.1.4 Mailed Payment Requirements](#_heading=h.qsh70q) [13](#_heading=h.qsh70q)

[4.1.5 Telephone Payment Requirements](#_heading=h.3as4poj) [13](#_heading=h.3as4poj)

[4.1.6 Faxed Payment Requirements](#_heading=h.1pxezwc) [14](#_heading=h.1pxezwc)

[4.1.7 Handling Payment Information Received through Insecure Channels](#_heading=h.49x2ik5) [14](#_heading=h.49x2ik5)

[4.2 Employee Management](#_heading=h.2p2csry) [15](#_heading=h.2p2csry)

[4.3 Data Management](#_heading=h.147n2zr) [16](#_heading=h.147n2zr)

[4.4 Cardholder Data Environment (CDE) Management](#_heading=h.3o7alnk) [17](#_heading=h.3o7alnk)

[4.5 Assessment](#_heading=h.23ckvvd) [18](#_heading=h.23ckvvd)

[4.6 Incident Response](#_heading=h.ihv636) [18](#_heading=h.ihv636)

[**5.0 Roles and Responsibilities**](#_heading=h.32hioqz) **[19](#_heading=h.32hioqz)**

[5.1 Treasury Services](#_heading=h.1hmsyys) [19](#_heading=h.1hmsyys)

[5.2 Unit Head Responsibilities](#_heading=h.41mghml) [19](#_heading=h.41mghml)

[5.3 Employee Responsibilities](#_heading=h.2grqrue) [20](#_heading=h.2grqrue)

[5.4 Information Technologies](#_heading=h.vx1227) [20](#_heading=h.vx1227)

[**6.0 Supporting Documents**](#_heading=h.3fwokq0) **[21](#_heading=h.3fwokq0)**

[**7.0 Contact Information**](#_heading=h.1v1yuxt) **[22](#_heading=h.1v1yuxt)**

[**Appendix A: Glossary**](#_heading=h.4f1mdlm) **23**

# 1.0 Overview

The University of Delaware accepts payment cards for certain transactions, including goods, services, and gifts. In doing so, the University and its units accept the responsibility to protect its customers’ data.

In order to accept payment cards, the University and its units must demonstrate and maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS) and with other applicable laws, regulations, and policies (“PCI compliance”).

The University’s Payment Card Program establishes institutional standards, including requirements and procedures, for managing University merchants, processing activities, the CDE, third parties, and PCI compliance.

All units that accept payment cards may do so only with prior approval from the Treasury department and only in accordance with the requirements of this Payment Card Program and the PCI DSS. All payment solutions must be PCI validated point to point encryption (P2PE) as found here: <https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement?return=%2Fassessors_and_solutions%2Fpoint_to_point_encryption_solutions>

## 1.1 Applicability

The Payment Card Program applies to all aspects of the University’s acceptance of payment cards. This includes

* all units accepting payment cards for transactions
	+ all University merchants
	+ all units acting as service providers
	+ all units outsourcing processing activities
* all individuals who come into contact with cardholder data
* all third parties engaged in processing activities on behalf of the University
* all cardholder data in any form (paper or electronic)
* all payment card processing activities
* the University’s cardholder data environment (CDE; all systems, services, and networks involved in processing activities).

This Payment Card Program applies in conjunction with other University policies and other laws, regulations, and external policies. For example, units are also subject to cash management policies and accounting responsibilities.

This Payment Card Program will be updated at least annually and in keeping pace with legal, regulatory, and technological changes.

## 1.2 Authority

The Office of the Vice President for Finance and Deputy Treasurer has authority over processing activities and PCI compliance for the University.

Treasury Services is charged with administering PCI policy—including this Payment Card Program—and PCI compliance across the institution.

## 1.3 Compliance and Exceptions

*PCI compliance* at the University of Delaware includes compliance with:

* this Payment Card Program
* the Payment Card Industry Data Security Standard (PCI DSS)
* the policies of the individual payment brands
* applicable P2PE Instruction Manuals (PIMs)
* other applicable laws, regulations, and policies.

### 1.3.1 Compliance Requirements

Each unit is responsible for its own PCI compliance to the extent that it is engaged in processing activities. Each unit is also responsible for ensuring the PCI compliance of any third parties it has engaged for processing activities. Units may only engage with third parties that are approved by Treasury Services.

Unit heads are primarily responsible for the PCI compliance of their units. Employees are responsible for adhering to unit security plans and operational procedures.

Each unit must develop a PCI security plan. This plan—which will be based on this Payment Card Program and the unit’s particular needs—will outline which security controls the unit will implement and how they will be implemented. Tools and resources are available to assist unit in the security planning process.

Compliance must be reported as described in Section 2.3.1.

Treasury Services engages a Qualified Security Assessor (QSA) on a routine basis to assess institutional PCI compliance, identify gaps, and recommend remediation actions.

### 1.3.2 Compliance Exceptions and Reporting

Exceptions to security controls and standard procedures must be justified by operational or technical needs and must be approved by the unit head and Treasury Services.

Treasury Services and the IT Security Office will work in an advisory capacity to assist units in finding alternatives to security controls that cannot be administratively, operationally, or technically implemented.

### 1.3.3 Managing Noncompliance

Every employee is responsible for reporting instances of fraud or noncompliance, including:

* processing payment cards using unauthorized or insecure methods, systems, or services
* improper recording, storage, or disposal of payment information
* fraudulent processing activities.

Units and employees should report known noncompliance to Treasury Services.

Treasury Services will assess noncompliance and, in collaboration with campus partners and appropriate authorities, take appropriate steps to remediate noncompliance or otherwise resolve issues. It is always better to fix noncompliance before it becomes an issue.

Unit heads are responsible for ensuring the remediation of noncompliant items as may be observed during routine operation or discovered during assessments and updating Treasury Services on the status of remediation efforts.

Individuals found to have engaged in noncompliant behaviors may be subject to disciplinary action, suspension or termination of employment, and/or legal action.

Some violations may constitute criminal offenses under local, state, or federal laws.

Units are responsible for the costs of noncompliance related to their processing activities. These costs may include

* fines and penalties imposed by the payment card industry
* monetary costs associated with remediation, assessment, forensic analysis, fraudulent activity, or legal fees
* suspension or termination of their merchant account and their authorization to accept payment cards.

# 2.0 Merchant Management

University entities desiring to accept payment cards must receive approval from Treasury Services prior to engaging in processing activities.

Units may be approved as *University merchants*, which are directly responsible for processing payment cards. Alternatively, units may be approved to accept payment cards with processing activities wholly outsourced to *third party merchants* (see Section 3.1.4).

## 2.1 Application to Accept Payment Cards

The opening of a new merchant account for the purpose of accepting and processing payment cards is done on a case by case basis. Any fees associated with the acceptance of payment cards in that department will be charged to the individual merchant.

To begin the process of accepting payment cards, interested unit heads should:

1. Review policy documentation to understand your PCI compliance responsibilities:
	1. Payment Card Program
2. Submit application materials to Treasury Services (cashcontrol@udel.edu).
	1. Unit Application to Accept Payment Cards
	2. Unit Payment Card Plan

## 2.2 Merchant IDs

Treasury Services provisions and issues *Merchant IDs (MIDs)* to units to facilitate payment card acceptance and accounting.

Each unit is responsible for all activity and costs associated with its MID. This includes bearing costs of processing and any costs associated with noncompliance.

All University merchants must use a unique, University-issued MID for their processing activities. Multiple MIDs may be issued to differentiate processing activities based on payment method.

Units engaging third party merchants may rely on third party MIDs with the approval of Treasury Services.

## 2.3 Ongoing Management of Merchants

Merchants are responsible for managing their processing activities on an ongoing basis.

1. Merchants must maintain a Unit Payment Card Plan describing the security controls in place to protect cardholder data and the CDE. Changes made to approved processes must be reviewed by Treasury.
2. Merchants must maintain operational procedures describing the unit’s processing activities, including how employees are expected to handle payment cards (see Section 4.0).
3. Merchants must notify Treasury Services of changes affecting cardholder data or the CDE, including changes in processing activities, systems, or services.

### 2.3.1 Attestations of Compliance

The University must attest institutional PCI compliance to its acquirers on an annual basis.

Each unit must attest its PCI compliance to Treasury Services on an annual basis in support of institutional attestations. Units will be issued accounts and login credentials for the CardPointe Reporting Dashboard to complete the following attestation activities:

1. Completion and submission of applicable *PCI DSS Self-Assessment Questionnaires (SAQs)* based on unit processing activities.
	1. SAQ A: To be completed by University merchants who conduct online transactions.
	2. SAQ P2PE: To be completed by University merchants who directly enter payments using point-to-point encrypted (P2PE) payment terminals.
	3. Other SAQs as may be appropriate.
2. Submission of, and attestation of compliance with, the Unit Payment Card Plan.
3. Submission of copies of employee attestations.

All employees who handle cardholder data must annually attend PCI training and attest to their PCI compliance responsibilities.

# 3.0 Third-Party Management

The University may contract with PCI-compliant third parties, including merchants and service providers, to assist with (and, in some cases, completely outsource) processing activities.

Treasury Services oversees the engagement of third parties.

**Units may engage with approved third parties to assist with processing activities.**

* Treasury Services maintains a list of approved third parties whom units may engage.
* Units may request approval for new third parties by contacting cashcontrol@udel.edu.
* Units may not engage third parties without Treasury Services’ prior written approval.
* Any changes to payment processing card holder data flow must be approved by Treasury Services prior to change.

**PCI compliance responsibilities change when third parties are involved.** The University and its units are responsible for

* Ensuring their own PCI compliance as it relates to their processing activities
* Ensuring the PCI compliance of any third parties involved in those processing activities
* Documenting the boundaries of responsibility for PCI compliance.

## 3.1 Types of Third-Parties and Relationships

### 3.1.1 Acquirers

*Acquirers* are specially designated entities that process payment card transactions for merchants.

The University must attest to each of its acquirers annually regarding the status of its PCI compliance with respect to transactions processed by that acquirer. The University also follows up with its acquirers to remediate issues of noncompliance or provide compensating controls.

### 3.1.2 Payment Processors

*Payment processors*: entities engaged by the University to handle payment card transactions on its behalf. Payment processors may also be referred to as “payment gateways.”

Units may engage approved payment processors to assist with processing activities.

Treasury Services maintains a list of approved payment processors.

Third party payment card applications or services must be processed through approved payment processors. To request integration of a third party payment application or service to an approved payment processor, contact cashcontrol@udel.edu.

### 3.1.3 Service Providers

*Third-party service provider*: any third party directly involved in the processing, storage, or transmission of cardholder data on the University’s behalf. Service providers generally include any non-merchant entity that has the ability to affect the security of a transaction.

University merchants may engage an approved third-party service provider to assist with processing activities.

As a University merchant, the unit is responsible for PCI compliance for all processing activities in which it is involved. The unit is also generally responsible for ensuring the third-party service provider’s PCI compliance.

The current boundaries of responsibility and future changes between the University and the third party must be clearly documented.

### 3.1.4 Merchants

*Third-party merchant*: any third party engaged in accepting payment cards for transactions on the University’s behalf using a non-University merchant account.

Units may engage an approved third-party merchant to outsource some or all processing activities.

**Outsourcing some processing activities**

Where a unit outsources some, but not all, processing activities to a third-party merchant:

* the unit is still directly involved in some processing activities
* the unit acts as a service provider to the third-party merchant
* the unit is not a University merchant.

As a service provider, the unit is responsible for PCI compliance for all processing activities in which it is still involved. The unit is also generally responsible for ensuring the third-party merchant’s PCI compliance. Agreements with third parties should include language recognizing the third party is wholly responsible in the event of a data breach.

The boundaries of responsibility between the University and the third party must be clearly documented.

**Outsourcing all processing activities**

Where a unit outsources all processing activities to a third-party merchant:

* the unit is not directly involved in any processing activities
* the unit does not act as a service provider
* the unit is not a University merchant.

Because it isn’t a service provider or a University merchant, the unit isn’t directly responsible for any processing activities. The unit is still responsible for ensuring the third-party merchant’s PCI compliance and the corresponding PCI language in the third-party agreement.

## 3.2 Managing Third Parties

### 3.2.1 Contracting with Third Parties

To protect the University from financial, legal, and other liabilities, third parties must be vetted and engaged according to written agreements.

1. Contracts must be reviewed and approved by Treasury Services.
2. The contract must require the third party, as well as any subcontractors involved in processing activities, to comply with the PCI DSS and provide proof of such compliance on a routine basis. Third parties must also supply a card holder data flow diagram. Any changes to this diagram must be approved by the university prior to changes being made or language in the contract holding them responsible for any changes made to the data flow diagram.
3. Boundaries of responsibility between each third party and the University must be documented.

### 3.2.2 Ongoing Management of Third Parties

Third party merchants and service providers must provide proof of their PCI compliance on an annual basis. Units that engage their own third party under the approval of Treasury Services are responsible for requesting proof of that third party’s PCI compliance and providing such documentation to Treasury Services on an annual basis.

1. All third parties providing payment card services must be PCI DSS compliant.
	1. Third party PCI DSS compliance must be verified prior to beginning a new engagement.
	2. Third party PCI DSS compliance must be verified on at least an annual basis.
2. Third party engagements must be subject to written and executed agreements.
	1. Agreements must require the third party’s compliance with PCI DSS.
3. Treasury Services will maintain a list that documents all approved third parties.

# 4.0 Operations Management

## 4.1 Processing Activities

All departments authorized to accept payment card transactions must have their card handling procedures documented and made available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis. Changes in approved business processes must be reviewed by Treasury Services in a timely manner

**Processing activities must be carried out using approved P2PE solutions. Use of methods or solutions not approved by Treasury Services constitutes a violation of policy and is likely to result in noncompliance.**

### 4.1.1 Acceptable Payment Methods

**All payment methods and solutions require the prior written approval of Treasury Services**; the University vets processing activities, systems, and services to verify their PCI compliance and security. Use of an unapproved method or payment solution constitutes a violation of policy and may result in unit and institutional noncompliance.

**The following methods are approved only when using approved payment solutions:**

1. In person (card present) payments
2. Online payments
3. Mailed payments
4. Telephone payments
5. Faxed payments (not preferred; single-function analog fax machines only)

**The following methods are prohibited from use:**

1. Emailed payments
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 payments (via IP and/or multi-function fax machines)

Of note, emerging technologies have made it easier to electronically process payment card transactions through the use of applications and mobile devices (including smartphones, tablets, and laptops). The ability to process transactions in this manner does not necessarily guarantee that they are PCI compliant or sufficiently secure. **Use of methods or solutions not approved by Treasury Services constitutes a violation of policy and is likely to result in noncompliance.**

### 4.1.2 In-Person (Card Present) Payment Requirements

Card present transactions are those in which the cardholder presents the physical payment card to a University merchant to render payment.

1. Payments must be processed in an approved and compliant manner.
	1. Payments must be processed using a solution approved by Treasury Services.
		1. Cardholder data must never be directly entered into a workstation or unapproved device.
	2. Employees must 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. Ensure the actual card/account holder is using 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).
2. Cardholder data should not be recorded or stored (see Section 4.3).
	1. Payments must be processed immediately (during the transaction) whenever possible.
	2. If cardholder data must be processed at a later date, it may be written in paper form, stored in a locked safe, processed as soon as possible, and securely destroyed via cross-cut shredding immediately after processing.

### 4.1.3 Online Payment Requirements

Online payments may only be accepted through an approved payment processor.

To request a payment form and integration, or to request approval for new third parties, contact support@arrowpayments.com or cashcontrol@udel.edu.

1. Payments must be processed in an approved and compliant manner.
	1. Payments must be processed using a solution approved by Treasury Services.
		1. Online payment forms must be managed by an approved payment processor.
		2. Online payment forms must never be used by University merchants to directly enter payment information at the point of sale.
		3. University merchants must not provide, or instruct customers to use, public workstations or unapproved self-service kiosks to enter payment information.
			1. Customers should be instructed to submit payment information using their personal device.

### 4.1.4 Mailed Payment Requirements

Payments may be accepted by mail. University merchants should be aware that the acceptance of paper forms containing cardholder data introduces additional security responsibilities.

1. Payments must be processed in an approved and compliant manner.
	1. Payments must be processed using a PCI validated P2PE solution approved by Treasury Services.
		1. Mailed payments must be sent to an official University address.
		2. Cardholder data must never be directly entered into a workstation or unapproved device.
	2. Mailed payments must be processed using dual control.
		1. At least two people should be responsible for opening mail and logging payment requests.
2. Cardholder data should not be recorded or stored (see Section 4.3).
	1. Payments must be processed immediately (during the transaction) whenever possible.
	2. If paper forms containing cardholder data must be processed at a later date, they must be stored in a locked safe, processed as soon as possible, and securely destroyed via cross-cut shredding immediately after processing.

### 4.1.5 Telephone Payment Requirements

University merchants may accept payment information during live telephone calls, provided that special controls are in place to protect cardholder data and limit the scope of the CDE.

1. Payments must be processed in an approved and compliant manner.
	1. Payments must be processed using a PCI validated P2PE solution approved by Treasury Services.
		1. Telephone payments must be submitted via an approved telephone number.
		2. Cardholder data must never be directly entered into a workstation or unapproved device.
2. Cardholder data should not be recorded or stored (see Section 4.3).
	1. Payments must be processed immediately (during the live telephone call or immediately after the call ends) whenever possible.
	2. If cardholder data must be processed at a later date, it may be written in paper form, stored in a locked safe, processed as soon as possible, and securely destroyed via cross-cut shredding immediately after processing.
	3. Cardholder data submitted via voicemail must not be processed.
		1. In the event that a customer submits cardholder data via voicemail, securely delete the voicemail. You may also contact the customer to notify them that the payment cannot be processed and that their payment information has been securely deleted. (Payment information may be processed during a live telephone call).
		2. Do not promote voicemail as a means of submitting payments.

### 4.1.6 Faxed Payment Requirements

The University does not recommend fax as a channel for accepting payment information. However, if a University merchant elects to accept faxed payments, **such payments may only be accepted via analog, single-function fax machines**. Payments submitted through IP and/or multi-function (e.g., combination fax and copy machines) fax machines are noncompliant and must not be processed.

1. Payments must be processed in an approved and compliant manner.
	1. Payments must be processed using a PCI validated P2PE solution approved by Treasury Services.
		1. Faxed payments must be sent to an approved University fax machine.
		2. Cardholder data must never be directly entered into a workstation or unapproved device.
	2. Faxed payments must be processed using dual control.
		1. At least two people should be responsible for retrieving faxes and logging payment requests.
2. Cardholder data should not be recorded or stored (see Section 4.3).
	1. Payments must be processed immediately (during the transaction) whenever possible.
	2. If paper forms containing cardholder data must be processed at a later date, they must be stored in a locked safe, processed as soon as possible, and securely destroyed via cross-cut shredding immediately after processing.
3. Fax machines used for processing activities must be secured.
	1. The fax machine must have an analog output (use of IP fax machines is prohibited).
	2. The fax machine must be single function (use of multi-function fax machines is prohibited).
	3. The fax machine must be located in a physically secure location, inaccessible to the public.

### 4.1.7 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.*

University merchants must not promote these methods as valid payment channels and should discourage customers from submitting payment information through these media. Any payment information received through these channels must be immediately and securely destroyed.

1. University merchants must never process payments submitted through insecure channels.
2. 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, and request that payment information be submitted through an alternate, compliant channel (see example wording below)
	3. securely destroy any messages or documents containing cardholder data (including messages in trash folders).
3. University merchants must not promote insecure payment channels (e.g., email, fax, voicemail, and instant messaging).

Responding to cardholder data received via an insecure channel:

Thank you for contacting {DEPARTMENT 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, 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.*

## 4.2 Employee Management

University merchants are responsible for authorizing and overseeing the activity of all employees involved in processing activities. Treasury Services provides training and other resources to help employees and University merchants understand how to accept payment cards in a secure and compliant manner.

1. Payment cards must be handled only by authorized employees.
	1. Processing activities must be limited to appropriate employees based on their job duties.
	2. Employees must be assigned unique accounts or other identifiers for processing activities. These identifiers must not be shared.
2. Employee authorization for processing activities must be managed.
	1. Access authorizations must be reviewed and recertified at least annually.
	2. Access must be promptly revoked when an employee leaves the unit.
3. Employees must complete institutional PCI compliance training before interacting with payment cards or the CDE and annually thereafter.
4. Employees must annually attest to their understanding of compliance with payment card policies and procedures. Training and results must be kept for audit purposes.

## 4.3 Data Management

In order to process payments, University merchants may accept cardholder data and other payment information as may be necessary. Each University merchant is responsible for protecting the data entrusted to it by its customers.

1. Cardholder data must be protected against unauthorized access.
	1. Physical security controls must be in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents, or electronic files containing cardholder data.
	2. Cardholder data in electronic form must be encrypted prior to transmission.
		1. Cardholder data must be encrypted at the entry device (e.g., a payment terminal) using a PCI validated P2PE solution.
2. Retention, storage, and destruction of cardholder data must be managed.
	1. Cardholder data must never be recorded or stored in electronic format.
		1. Paper forms containing cardholder data must never be scanned or otherwise digitized.
	2. Cardholder data may be recorded and stored in paper format only in select circumstances:
		1. When unable to process in-person payments immediately
		2. When unable to process mailed payments immediately
		3. When unable to process telephone payments immediately
		4. When unable to process faxed payments immediately
	3. Cardholder data in paper format must be
		1. processed as soon as possible (in no case more than two business days after receipt)
		2. stored only if absolutely necessary, and only in a locked safe accessible only to authorized employees
		3. securely destroyed via cross-cut shredding immediately after processing.
	4. Paper forms may be retained for non-processing purposes only if the portion containing cardholder data has been securely destroyed.
	5. Sensitive Authentication Data must never be recorded or stored in any format. Sensitive Authentication Data includes:
		1. the contents of the magnetic stripe
		2. the three or four-digit CVV or CVV2
		3. the PIN or PIN block.
3. The Primary Account Number must never be printed unless truncated (e.g., first six or last four digits only).
4. Cardholder data must never be requested or accepted via insecure channels (see Section 4.1.7).

## 4.4 Cardholder Data Environment (CDE) Management

The Cardholder Data Environment comprises all of the systems, services, and networks over which the University conducts its processing activities.

The CDE is managed under the direction of Treasury Services.

**Any methods, systems, and networks involved in processing activities are brought into scope and must be PCI compliant.** Unauthorized modification of the CDE (for example, by transmitting cardholder data using unapproved networks or equipment) may bring the University into noncompliance and constitutes a violation of University policy.

Where practical, the University will reduce the scope of its CDE through administrative, operational, and technical controls.

1. Cardholder data and processing activities must be restricted to only the systems, services, and networks approved as part of the CDE.
	1. Treasury Services will issue or oversee the procurement of PCI validated P2PE equipment.
	2. Payments must never be processed using workstations or unapproved devices.
2. Access to the CDE—and to the data, systems, and services therein—must be restricted to only authorized and properly trained employees and third parties.
	1. Maintenance activities, including maintenance access, must be documented and approved.
3. Equipment must be periodically inventoried.
4. Equipment must be physically secured.
	1. Equipment must be kept in a secured and restricted area where practical.
5. Equipment must be periodically inspected for tampering or substitution.
	1. Inspections must be documented using a UD PCI Device Inventory and Tampering Checklist Form.
	2. Verify the serial/model number on the device sticker matches the serial/model number displayed electronically on the device.
	3. 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.
	4. Verify that no foreign object (unfamiliar electronic equipment, device, keypad overlay, wire, or cable) is connected to or placed near the device.
	5. Verify that there are no modifications (pry marks, or bent, broken, or stressed seams) to the device.
	6. Evidence of tampering or substitution must be immediately reported to the unit head, Treasury Services, and the IT Security Office.
6. Systems that process unencrypted cardholder data must be explicitly approved by Treasury Services and require additional protection requirements.
7. Equipment must be securely decommissioned and disposed.
	1. Requests to dispose of processing equipment must be submitted to Treasury Services at cashcontrol@udel.edu.

## 4.5 Assessment

Routine risk assessments are a vital step in protecting cardholders and the University. These assessments—and the University’s authorization to accept payment cards—depends upon the support of each unit engaged in such acceptance.

A formal risk assessment process must be implemented to periodically (no less than annually) analyze and document current threats and vulnerabilities to the CDE.

## 4.6 Incident Response

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

In the event of a breach or suspected breach of security, the department or unit must immediately notify Treasury Services and the IT Security Office to begin execution of the Tier II Incident Response Plan. Unit should treat a breach or suspected breach as evidence until IT security can complete an inspection. Unit should not delete files or turn machines off until instructed to do so by IT security.

The Incident Response Plan should be reviewed and tested at least annually.

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.

# 5.0 Roles and Responsibilities

## 5.1 Treasury Services

Treasury Services is responsible for administering payment card policies, including this Payment Card Program, and processing activities across the University.

Treasury Services’ responsibilities under policy include:

1. Act as the institutional point of contact for the University’s acquirer and service providers as well as PCI-related assessors and the payment brands.
2. Administer the University’s Payment Card Program.
3. Administer and enforce PCI compliance activities.
4. Administer the University’s CDE, including approving, inventorying, issuing, and maintaining PCI-compliant systems and equipment for use by University merchants.
5. Administer University merchants, including approval, provisioning of merchant IDs, inventorying, attestation, and training.
6. Oversee the engagement of third parties.
7. Manage exceptions to this policy, including documentation, approval, and annual review.
8. Investigate incidents and violations affecting cardholder data or the CDE.
9. Routinely brief the Vice President for Finance and Deputy Treasurer on the status of processing activities and PCI compliance across the institution.
10. Monitor regulatory and technological developments to inform University merchants of changes and update this policy as appropriate.

## 5.2 Unit Head Responsibilities

Unit heads are responsible for their unit’s processing activities and PCI compliance.

Unit heads’ responsibilities under policy include:

1. Assume responsibility for their unit’s PCI compliance.
2. Act as the unit point of contact for Treasury Services, third parties, and other stakeholders.
3. Develop, implement, and maintain unit PCI security plans and business procedures to ensure unit processing activities are PCI compliant.
4. Oversee employee activity, including limiting processing activities to only authorized employees and ensuring those employees complete PCI-related security and awareness training and attestation.
5. Manage relationships with approved third parties, including obtaining and providing to Treasury Services written documentation of third parties’ PCI compliance on an annual basis.
6. Support institutional PCI compliance assessments and remediation of noncompliance.
7. Assume all costs associated with their merchant account, including equipment costs, banking fees, and costs associated with noncompliance.
8. Promptly notify Treasury Services of changes affecting cardholder data or the CDE, including changes in employment, processing activities, systems, or services.
9. Report suspected or observed violations of the PCI DSS or University policy to Treasury Services and to the IT Security Office.

## 5.3 Employee Responsibilities

Employees are responsible for complying with University policy and PCI requirements in the course of conducting processing activities.

Employees’ responsibilities under policy include:

1. Understand and comply with policies and procedures related to processing activities.
2. Handle payment cards and cardholder data only as authorized.
3. Protect cardholder data and personally identifiable information as required by laws, regulations, and policies.
4. Complete PCI-related security and awareness training and attestation.
5. Report suspected or observed violations of the PCI DSS or University policy to Treasury Services and to the IT Security Office.

## 5.4 Information Technologies

IT, as a custodian of the CDE and given its expertise in security and risk management, is responsible for assisting in the management of PCI compliance.

IT’s responsibilities under policy include:

1. Assist Treasury Services in reviewing and interpreting security requirements under applicable laws, regulations, and policies, including the PCI DSS.
2. Investigate violations of security in accordance with University incident response policies and procedures.
3. Under the direction of Treasury Services and as a custodian of the University’s IT resources, manage the technological infrastructure supporting the University’s CDE.
4. Monitor technological developments, trends, and changes in laws and regulations and recommend updates to policies, standards, procedures, and guidelines as appropriate.

# 6.0 Supporting Documents

Unit Application to Accept Payment Cards

Unit PCI Security Plan

Unit PCI Security Plan Attestation Form

UD PCI Device Inventory and Tampering Checklist (Single)

UD PCI Device Inventory and Tampering Checklist (Multiple)

# 7.0 Contact Information

For questions about the UD Payment Card Program, contact:

University of Delaware Treasury Services

Office of the Vice President for Finance and Deputy Treasurer

220 Hullihen Hall

Newark, DE 19716

302-831-2107

cashcontrol@udel.edu

# Appendix A: Glossary

The PCI Security Standards Council maintains a [Glossary of Terms, Abbreviations, and Acronyms](https://www.pcisecuritystandards.org/document_library) that contains additional, pertinent information.

* **Cardholder:** Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.
* **Cardholder Data:** At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.
* **Cardholder Data Environment (CDE):** The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
* **CAV2, CVC2, CID, or CVV2 data:** The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.
* **Expiration Date:** The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
* **Magnetic Stripe (i.e., track) data:** Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
* **Merchant Department:** Any department or unit (can be a group of departments or a subset of a department) which has been approved by the (institution) to accept payment cards and has been assigned a Merchant identification number.
* **Payment Card Industry Data Security Standards (PCI DSS):** The security requirements defined by the Payment Card Industry Security Standards Council and the five major payment card brands: Visa, MasterCard, American Express, Discover, and JCB.
* **Primary Account Number (PAN):** Number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account and includes a check digit as an authentication device.
* **PIN/PIN block:** Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
* **Secure Destruction:** Cardholder data must be disposed of in a certain manner that renders all data irrecoverable. Cardholder data in paper form must be destroyed using a cross-cut shredder. Cardholder data should not be stored in electronic format; however, electronic media that contain cardholder data must be sanitized in accordance with the PCI DSS.
* **Sensitive Authentication Data:** Additional elements of payment card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
* **Service Code:** The service code that permits where the card is used and for what.