# Payment Card Processing Policy

**Document Number:** RISK-0017 **Date Published(sys):** 4/30/2024

## General Description

### Policy Summary:

Trinity University is committed to compliance with applicable laws, regulations, and standards related to accepting payment cards on campus. This Policy provides standards for the University to accept and process payments from third parties by credit card, debit card, or any card or device other than cash or check (collectively, “Payment Cards”).

### Purpose:

Trinity University is subject to certain Federal, State, and industry rules, regulations, and contractual provisions regarding the processing and handling of Payment Cards and the data associated with those Payment Cards. The goal of this Policy is compliance with laws, rules, regulations and contractual provisions, maintenance of a secure Payment Card processing environment and security of Payment Card data.

### Scope:

All Trinity individuals that process Payment Card transactions on behalf of the University and third parties, vendors, and contractors involved in accepting card payments for or on behalf of Trinity University and/or supporting that activity are responsible for compliance with this Policy and familiarizing themselves with its contents.

### Exceptions:

None

## Policy Content

**All University Departments that process Payment Card transactions for goods and services are d**
**be Merchants under the Payment Card Industry Data Security Standards (PCI DSS). Prior to acce**
**Payment Cards, Departments must:**

**1.) Receive approval from the Business Office for the creation of a Merchant Account,**
**2.) Receive approval from ITS of Security Assessment and Payment Card Equipment. Trinity Univ uses Touchnet as the Third Party Payment Processor or Payment Gateway for all Payment Card transactions. No other Third Party Payment Processor or Payment Gateway may be used without of the University.**
**Best practice is to accept online Payment Card transactions through the University's approved S Provider/Payment Gateway, Touchnet, as opposed to in-person transactions. This reduces the U scope as it pertains to PCI DSS. Only Merchant Departments are able to process Payment Card tr on behalf of the University. Third parties that are approved by ITS for Payment Card transaction p on campus may only process outside of the Trinity network on their own mobile Wi-Fi hotspot. Th approved to accept Payment Card transactions on campus and Service Providers who accept Pa Card transactions on behalf of Trinity University must contractually agree to:**
**1.) Represent and warrant that it is compliant with current Payment Card Industry Data Security S (PCI DSS) and shall remain compliant during the Term of the Agreement, ensuring that the enviro the processing of transactions is done in compliance with current PCI DSS standards;**
**2.) Promptly notify Trinity University of its non-compliance status should become PCI DSS non-c during the Term;**
**3.) Provide Trinity University with a copy of its PCI DSS Certificate of Compliance prio performance of services and annually thereafter;**
**4.) Be liable for the security of the Cardholder Data; and**
**5.) Notify Trinity University of any real or suspected breaches of Cardholder Data immediately up discovery.**

**RESPONSIBILITIES OF MERCHANT DEPARTMENTS PCI DSS Standards: Merchant Departments approved to accept Payment Cards must adhere to current PCI DSS Standards and the policies, guidelines and procedures established by Risk Management with support of the Business Office and ITS, and have the following responsibilities:**
**Background Check: All Trinity individuals that process Payment Card transactions on behalf of the University must have a criminal background check through Human Resources.**
**Training: All Trinity individuals that process Payment Card transactions on behalf of the University must complete PCI DSS online training prior to processing and subsequently at least annually.**
**Point of Contact: Designate a point of contact responsible for the effective implementation and ongoing maintenance for PCI DSS compliance.**
**Annual Updates by Merchant Department Point of Contact: Update the Office Procedures document annually, have each individual that processes Payment Card transactions on behalf of the Merchant Department sign, and upload to the shared PCI DSS Compliance drive.**
**Payment Card Equipment: Approval must be received prior to acquiring Payment Card Equipment or entering into a Contract with a Service Provider, Third Party Payment Processor or Payment Gateway. The Merchant Department maintains a list of updates and periodically inspects Payment Card Equipment/devices for tampering. Any evidence of tampering must be reported to the University Information Security Administrator at adeloss1@trinity.edu or 210-999-7459 immediately upon discovery.**

**Payments/Transactions: If payments are taken other than online, the Payment Card Equipment/devices used must be approved by ITS for Payment Card transaction processing.**
**Record Retention: In accordance with Trinity University Record Retention Policy, allowable Cardholder Data should be checked quarterly for expiration and retained for no longer than 18 months.**
**Disposal: All Cardholder Data (any information contained on a Third Party's Payment Card) shall be immediately cross-cut shredded or disposed of in secure bins through Cintas after payment processing. Order forms with demographic and order information may be retained for legitimate business purposes, but the Cardholder Data shall be redacted and cross-cut shredded.**
**Security Breach: If/when a security breach is discovered or suspected, the Merchant Department must immediately contact the University Information Security Administrator at adeloss1@trinity.edu or 210-999-7459.**

## *Performance Evaluation*

### Consequences of Policy Violation:

The University may be assessed non-compliance penalties by the Acquiring Bank. Any non-compliance fees may be the responsibility of the Merchant Department. Failure to comply with this Policy may result in disciplinary action up to and including termination.

## *Terms & Definitions*

### Terms and Definitions:

| Term: | Definition: |
|---|---|
| Acquiring Bank | A financial institution that maintains the University's bank account and is contracted to process credit and debit card transactions. |
| Cardholder Data | The Primary Account Number (PAN) alone or the PAN plus any of the following:<br>full magnetic strip information, cardholder name, expiration date, or security code. |
| Merchant Account | Account number assigned by the Business Office to a Merchant Department for the purpose of processing Payment Card transactions. |
| Merchant Department | A University Department that is approved by the Business Office and ITS to accept Payment Cards on behalf of the University as payment for goods and/or services. |

| Term: | Definition: |
|---|---|
| Payment Card | Refers to credit cards, debit cards or any other card or device other than cash or check. |
| Payment Card Equipment | Payment Card terminal or machine used to process Payment Card transactions. |
| Payment Card Industry Data Security Standard (PCI DSS) | A set of comprehensive requirements for Payment Card data security established by the PCI Security Standards Council. Compliance with the PCI DSS helps to mitigate vulnerabilities that put Cardholder Data at risk. The PCI DSS standards must be adopted by all merchants, organizations, and entities that accept and process Payment Cards. |
| Service Provider | Any company that stores, processes or transmits Cardholder Data on behalf of another entity. Includes Third Party Payment Processors/Payment Gateway companies. |
| Third Parties | Refers to individuals, companies, merchants, vendors, contractors or other parties that are not Merchant Departments and either pay the University for goods or services or request to conduct Payment Card transactions on the Trinity campus. |
| Third Party Payment Processor or Payment Gateway | A company that offers Payment Card processing software and/or gateway services. |

## *Related Documents*

### Related Documents:

| Document Type: | Document Name: | Document Number: |
|---|---|---|
| Policy | Records Retention Policy | BUSO-0020 |

### Related Content:

PCI Security Standards Council

## *Revision Management*

### Revision History Log:

| Revision #: | Date: | Recorded By: |
|---|---|---|
| v1.0 | 2/20/2024 11:46 AM | Jennifer Gilmore Adamo |

### Vice President Approval:

| Name: | Title: |
|---|---|
| Gary Logan | Vice President for Finance & Administration |