

# Trinity University

## Credit Card Handling Policy and Procedures

---

### POLICY

---

#### Policy Statement

The establishment of control measures for credit card transactions is necessary to maintain proper security over credit cardholder information. Trinity University Credit Card Handling Policy requires each Department be approved as a credit card processing merchant and each method of processing credit transactions be approved by the Business Office. A credit card merchant is defined as a department or other entity which processes credit transactions.

Department requirements for credit card processing include the following:

- Business Office approval before entering into any contracts or purchases of software and/or equipment. This requirement applies regardless of the transaction method or technology used (e.g. e-commerce or point-of-sale device).
- University Information Technology Security Office approval of all technology implementation, including approval of authorized payment gateways.
- Comply with procedures for safeguarding cardholder information and secure storage of data. This pertains to ALL transactions initiated via the telephone, over the counter, mail order, Internet, etc.
- Complete an annual security self-assessment questionnaire provided by the Business Office and report the results to the Business Office to ensure compliance with this policy and associated procedures. This is a supplemental questionnaire that will be used by the Business Office and ITS to complete [SAQ C Version 1.2 Oct 2008](#)
- Compliance with [Payment Card Industry \(PCI\) Data Security Standards \(link Version 1.2 Oct 2008\)](#)

Periodic reviews of safeguarding and storage of cardholder information will be conducted by the Business Office. Credit card handling procedures are additionally subject to audit by Internal Audit, external audit or charge card review firms. In addition, the University Information Technology Security Office will periodically conduct an assessment of security controls in place to protect technology implementations, including but not limited to periodic network-based vulnerability scans. Departments not complying with approved safeguarding, storage and processing procedures may lose the privilege to process credit card transactions.

#### Who Should Know This Policy

Any department chair or Department administrator with responsibilities for managing university credit card transactions, and those employees who are entrusted with handling credit cards and credit card information must be familiar with, understand, and comply with this policy

## Responsibilities

**Department** – Submits a request to establish credit card accounts with an approved merchant service provider (see page 4 for details).

**Credit Card Handling Supervisor** – Ensures the following standards are maintained:

- Keep secure and confidential all cardholder numbers and information. Credit card receipts should typically be treated the same as you would treat cash. The Department will be responsible for any losses due to poor internal or inadequate controls.
  - Sensitive cardholder data (i.e., full account number, type, expiration, and track (CVC2/CVV2) data, cannot be stored in any fashion on computers or networks.
  - Credit card numbers must **NOT** be transmitted in an insecure manner, such as by e-mail, unsecured fax, or through campus mail. Lock bags available from the University Cashier must be used instead of campus mail.
  - All documentation containing card account numbers must be maintained in a “secure” environment limited to dependable, trustworthy and accountable staff. Secure environments include locked drawers, file cabinets in locked offices, and safes.
  - All documentation containing card account numbers must be destroyed in a manner that will render them unreadable after their useful life ( <sup>1</sup> **no more than** 18 months) has expired. Records reaching their expiration date **must** be **securely** sent to Purchasing to be destroyed by an outside vendor in order to provide verifiable destruction dates.
- Restrict access to credit card data and processing to appropriate and authorized personnel.
  - Background checks must be performed prior to the hiring of any new positions with unrestricted access to cardholder information.
  - Require all personnel involved in credit card handling to attend card security training at least every two years.
- Establish appropriate segregation of duties between credit card processing, the processing of refunds, and the reconciliation function. Supervisory approval of all card refunds is required.
- Perform an annual self assessment to ensure compliance with this policy and associated procedures, and report the results of this assessment to the Business Office.
- Notify the University Information Security Administrator’s office in Information Technology Services prior to implementation of any technology changes affecting transaction processing associated with the credit card accounts by submitting a *Payment Card Change/Termination Request form* to the Business Office.

**Credit Card Handlers and Processors (within each Department)** –

- Agree not to disclose or acquire any information concerning a cardholder’s account without the cardholder’s consent.

- <sup>2</sup> Good business practice dictates the retention of authorizations for no longer than 18 months for response to copy requests and chargebacks. In the event that a chargeback occurs for which there is no supporting documentation the department will absorb the cost of the chargeback.
- E-commerce and Departments using third-party software, including cash register systems are prohibited from storing complete payment card numbers on University computers at any time.
- Agree to resolve chargebacks related to credit card disputes or rejected sales.
- Other (external) campus credit card processors must securely store and transmit information using at least 128 bit encryption, and provide certification attesting to Payment Card Industry Data Security Standards compliance.

#### **Business Office –**

- Review and approve the establishment of new department credit card accounts and/or processors.
- Administer the process of obtaining new Merchant I.D. numbers.
- Conduct periodic reviews of existing Departments regarding safeguarding and storage of cardholder information.
- Provide periodic training on the secure storage and disposal of all non-e-commerce credit card paper transaction records in conjunction with University cash handling policies.
- Require all personnel involved in credit card handling to complete a *Statement of Payment Card Industry Compliance* which will become a part of their permanent record filed in Human Resources. Signed statements will be initiated by the Business Office as part of the training process.
- Communicate with departments regarding chargebacks related to credit card disputes or rejected sales.
- Provide an annual report to the University Information Security Administrator in Information Technology Services of all departmental credit card accounts and associated transaction volumes.
- Collaborate with the University Information Security Administrator in Information Technology Services to complete the security self assessment questionnaire.

#### **University Information Security Administrator in Information Technology Services –**

- Review and approve implementation of any technology changes and payment gateways associated with credit card transactions processing.
- Conduct periodic reviews for compliance with Payment Card Industry Data Security Standards.
- Collaborate with the Business Office to complete the security self assessment questionnaire.

### **Establishing New Credit Card Department Account**

In order to accept credit cards in return for goods/services, Departments must read and sign the Payment Card Agreement and complete the Request to Process Payment Cards form and return the documents to the Business Office, NH 141. Upon approval, the Business Office will establish new credit card accounts (Merchant I.D. numbers) with an authorized merchant service provider. If at any time you have a question or concern about accepting credit cards, please contact the Business Office for assistance (see page 5 for contact information).

It will take approximately three weeks for Merchant I.D. numbers to be requested and set up. A training session for you and your staff will then be scheduled by the appropriate personnel.

### **Accounting for Transactions**

The daily net sales settle electronically into the appropriate university bank account, usually within 48 hours. It is the responsibility of the Departments to close out credit card batches daily and submit accounting information within three working days of the batch close date through the University Cashier. Contact the cashier at extension 7395 for more detailed information.

It is the Department's responsibility, in cooperation with the Business Office, to reconcile the settlement amount in the general ledger account to the credit card receipts on a regular basis, but no less than monthly. Departments will have two months to clear any outstanding credit card transactions that appear on the monthly bank reconciliation after which they will be written off to miscellaneous income.

Each Department receives a monthly statement directly from the authorized merchant service provider. These statements provide a listing of each batch submitted for reconciliation purposes. It is the Department's responsibility to verify that this information is correct.

### **Information Security Incident Response Policy**

Current ITS policies and procedures <http://iraa.trinity.edu/iraa/x500.xml> ensure timely and effective handling of any breaches in security related to digital processing. It is important that any digital breach in security of credit cardholder information be reported immediately to [infosec@trinity.edu](mailto:infosec@trinity.edu).

All non-digital breaches in security should be reported immediately to the Credit Card Handling Supervisor and the Business Office. If a breach is discovered after normal business hours contact Campus Security.

## **Additional Information**

**E-COMMERCE.** Electronic commerce transactions must be processed using either TouchNet or CBORD, as these are the only university approved e-commerce providers.

**FEES.** Each transaction is subject to assessment, discount and per item fees charged by Visa, MasterCard, Discover, and American Express.

Additional fees may be assessed by the authorized merchant service provider, based on a competitive bid process. Examples include fees for transaction processing, chargebacks and supplies. Please contact the Business Office for current information.

### **MERCHANT SERVICE PROVIDERS (Credit Card Processors)**

Wells Fargo Merchant Services  
Bank of America Merchant Services  
American Express Merchant Services  
Discover Merchant Services

## **CONTACTS**

### Merchant ID(s) & Credit Card Statements

Patsy Gottardy, Business Office  
E-mail: [pgottard@trinity.edu](mailto:pgottard@trinity.edu)  
Extension: 7661

---

### University Information Security

Stephen Perez - Information Technology  
Services, University Information Security  
Administrator  
E-mail: [sperez@trinity.edu](mailto:sperez@trinity.edu)  
Extension: 7619

### TouchNet

John Sonnen - Information Technology  
Systems, Director of Enterprise Systems  
E-mail: [jsonnen@trinity.edu](mailto:jsonnen@trinity.edu)  
Extension: 8878

Owen Kaltenbacher – Information  
Technology Systems, Senior Application  
Administrator  
E-mail: [okaltenb@trinity.edu](mailto:okaltenb@trinity.edu)  
Extension: 7442

## **PAYMENT CARD INDUSTRY GUIDELINES**

[Visa Departments Card Management Guide](#)

[MasterCard International Rules Manual](#)

[Payment Card Industry Data Security Standard](#)

[American Express Merchant Policy](#)

[Discover Merchant Policy](#)

Trinity University gratefully acknowledges permission granted by The University of Iowa to use their Credit Card Handling Policy and Procedures as a template.

<sup>1</sup>Updated: April 7, 2010 – previously stated: (18 months)

<sup>2</sup>Updated: April 7, 2010 – previously stated: Credit card authorizations must be kept for 18 months for response to copy requests and chargebacks

**TRINITY UNIVERSITY**

**STATEMENT OF PAYMENT CARD INDUSTRY COMPLIANCE**

I understand that in my capacity as \_\_\_\_\_  
(Job Title)

I will have access to confidential credit card numbers and information. I acknowledge that access to this information is necessary for me to perform my job duties for the University. Likewise, I understand that it is against University policy for me to disclose this information to anyone who does not have specific need relating to the performance of my duties and the University’s business to know the information.

To protect consumer credit card numbers and information and comply with industry standards, I agree to:

- NOT store sensitive cardholder data (i.e., full account number, type, expiration, and track data) in any fashion on computers or networks.
- NOT transmit credit card numbers in an insecure manner, such as by e-mail, unsecured fax, or through campus mail.
- Store all documentation containing card account numbers in a “secure” environment limited to dependable, trustworthy and accountable staff. Secure environments included locked drawers, file cabinets in locked offices, and safes.
- Destroy all documentation containing card account numbers in a manner that will render them unreadable after their useful life (18 months) has expired.
- Attend card security training at least every two years.
- Obtain supervisory approval of all credit card refunds
- Notify the University Information Technology Security Office prior to implementation of any technology changes affecting transaction processing associated with a merchant account.

I affirm that I received the appropriate credit card security training and have read and understood the Trinity University Credit Card Handling Policy and Procedures.

I understand that if I violate these standards of confidentiality or this Statement of Compliance, I may be subject to immediate dismissal from my position and, may violate certain applicable federal and state laws for which I may have personal responsibility/liability.

**Departments may lose the privilege to serve as a credit card merchant if these standards are not upheld.**

Employee Name: \_\_\_\_\_

Department: \_\_\_\_\_

Employee Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Supervisor Name: \_\_\_\_\_

Supervisor Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Return completed form to:**

**Pasty Gottardy – Business Office  
Northrup 141-S**

cc: Office of Human Resources

Revised: March 2009

# Trinity University

## Payment Card Agreement

Department Name: \_\_\_\_\_

This document with attachments specifies the agreement between Trinity University Business Office (hereafter referred to as Business Office) and university departments (hereafter referred to as Department) to give Departments the ability to accept credit cards from customers as an accepted form of payment for goods or services.

Section I:	Process Description
Section II:	General Rules, Regulations and Guidelines for Departments
Section III:	Attachments
Section IV:	Contacts
Section V:	PCI-DSS Committee Members
Section VI:	Glossary of Terms

### Section I: Process Description

- Trinity University has negotiated a university-wide contract for Department credit card processing.
- Cards accepted are VISA, MasterCard, Discover, and American Express.
- Electronic ticket capture is the transmission of sales to the credit card processor through the use of electronic equipment. The preferred methods for processing credit card sales include PC software, cash register systems, and internet processing. Credit card terminals approved by the PCI-DSS (Payment Card Industry-Data Security Standards) Committee may be used on a select basis (see section V, page 4 for contact information).
- Department sales information is transmitted electronically to the authorized merchant service provider. The provider receives authorization and payment from the cardholder's bank. Funds are then deposited into a University bank account.
- A Department requests approval to become a credit card merchant from the Business Office. Upon approval, the Business Office establishes new merchant accounts with each authorized merchant service provider.
- The merchant service provider issues monthly statements to each Department for reconciliation purposes. To become a credit card merchant, a Department or campus organization must complete the ***Trinity University Request to Process Payment Cards*** form at the end of this document. The application contains contact information, department location, general ledger account numbers for revenue/fees, equipment and processing method desired.

- The Department must complete a *Trinity University Payment Card Change/Termination Request* in the event of any changes in the information provided on the original application form. The Payment Card Change/Termination Form is also included at the end of this document.
- The Department **must** batch out sales at the end of each day and must submit accounting information via a Trinity University Cash Transmittal (deposit slip) within three working days of the credit card batch close date through the University Cashier.
- The Department must reconcile their daily sales to the report generated when the daily sales are batched out, to the university general ledger account, and to the monthly statement provided by the merchant service provider.
- Departments must contact the Business Office in the event that they will be making any changes to their method of processing after initial set up. Examples include changing from terminal based processing to processing through PC software, through a web site, or terminals built into cash registers. All such changes must be approved by the Business Office and the University Information Security Administrator in Information Technology Services.
- If a Department experiences a “hacking” incident concerning their credit card operations, or suspects such an incident has occurred, the University Information Security Administrator must be contacted immediately. Call 999-7401 or after hours call Help Desk 7409 (select the emergency option, and ask the attendant to contact the University Information Security Administrator on call).
- **COMPLETE CARDHOLDER CREDIT CARD ACCOUNT NUMBERS ARE NOT TO BE STORED IN ANY ELECTRONIC FILE IN ANY CAPACITY.** If necessary, the *last four digits (only)* of the account number may be captured.

## Section II: General Rules, Regulations and Guidelines for Departments

All face-to-face transactions should have the payment card present and **require** an authorized signature from the cardholder. Always verify the card is valid and signed. Compare signatures and check for ID where possible and feasible.

If it is not a face-to-face transaction, some other method must be used for securing the payment (i.e. mail in form with credit card information and signature, fax in signature, etc.). Request a signed authorization form and obtain a signature of the cardholder as often as possible.

Departments may accept card numbers via phone, secured fax, and U.S. mail. **DO NOT ASK FOR CARD INFORMATION OR SOLICIT CARD INFORMATION VIA E-MAIL.**

Departments must keep all card numbers and information secure and confidential. No sensitive card information (full account number, type, expiration date, or track data) can be stored on any computer database or server.

Departments agree not to disclose or acquire any information concerning a cardholder's account without the cardholder's consent. Departments will not sell, purchase, provide disclose or exchange card account information or any other transaction information.

Departments will keep an original copy, imaged copy or a microfilm copy of each credit card transaction for no less than 18 months. All credit card documentation containing card account numbers must be maintained in a secure environment limited to dependable, trustworthy and accountable staff. Secure environments include locked drawers, file cabinets in locked offices, and safes. Credit card receipts should be treated the same as you would treat cash. After 18 months, these materials must be destroyed in a manner that will render them unreadable. Departments will be responsible for any losses due to poor internal controls.

A cash advance or withdrawal from your Department to a cardholder, or to yourself, is **not authorized**. Departments may not accept money from a cardholder and subsequently prepare a credit draft for the purpose of creating a credit to the purchaser's account. The terminal may only be used for transactions related to purchases of Trinity University goods and services.

Departments agree that the sales draft represents a bona fide, newly created transaction involving the merchandise and/or services itemized on the sales draft. A customer should not be charged before merchandise is shipped. In the case of an intangible product (i.e. registration) process the charge to the customer when registration confirmation is sent.

Departments are required, in good faith, to maintain a fair policy for the exchange and return of **merchandise**, and for resolving disputes over merchandise and/or services purchased with a payment card. If a transaction is for non-returnable, non-refundable merchandise, this must be indicated on all copies of the sales draft before the cardholder signs it. ***A copy of your return policy must be displayed in public view.***

Departments will give proper credit for returns and adjustments by performing the proper function on the terminal. Under no circumstances should any card refund or adjustment be paid to a cardholder in cash. If cash is refunded and the cardholder files a dispute, your department will bear the loss of income from the transaction.

All fees associated with processing of credit card transactions will be paid by the Department.

Refer to the attachments in Section III for additional documentation on Payment Card Industry Standards.

This Agreement shall not become effective until approved by the Office of Fiscal Affairs and will remain in full force until terminated by either party by giving written notice to the other party.

I understand the above Payment Card Agreement and by signing below agree to abide by the rules and regulations stated herewith and the attachments listed below.

Printed name: \_\_\_\_\_  
(Department chair or administrator)

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

### **Section III: Attachments**

Trinity University Credit Card Handling Policy and Procedures

VISA Merchants Card Management Guide:

[http://usa.visa.com/download/merchants/card\\_acceptance\\_guide.pdf](http://usa.visa.com/download/merchants/card_acceptance_guide.pdf)

MasterCard International Rules Manual: <http://www.mastercard.com/us/merchant/support/rules.html>

Payment Card Industry Data Security Standard: <https://www.pcisecuritystandards.org>

American Express Merchant Policy:

[https://www209.americanexpress.com/merchant/singlevoice/USEng/FrontServlet?request\\_type=navigate&page=merchantPolicy](https://www209.americanexpress.com/merchant/singlevoice/USEng/FrontServlet?request_type=navigate&page=merchantPolicy)

Discover Information Security & Compliance: <http://www.discovernetwork.com/fraudsecurity/disc.html>

### **Section IV: Contacts**

Patsy Gottardy, Business Office

E-mail: [pgotard@trinity.edu](mailto:pgotard@trinity.edu)

Extension: 7661

Owen Kaltenbacher, Information Technology Services - TouchNet

E-mail: [okaltenb@trinity.edu](mailto:okaltenb@trinity.edu)

Extension: 7442

Stephen Perez, Information Technology Services – University Information Security Administrator

E-mail: [sperez@trinity.edu](mailto:sperez@trinity.edu)

Extension: 7619

### **Section V: PCI-DSS Committee Members**

#### Business Office

Mary Jump, Chair

Brad Melton

Judy Noland

Azmin Victoria

#### Tiger Card Office

Jerry Ferguson

#### Fiscal Affairs

Jennifer Gilmore Adamo

#### Information Technology Services

Fred Zapata

Stephen Perez

## Section VI: Glossary of Terms

**PCI-DSS:** Payment Card Industry-Data Security Standards – Includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The comprehensive standard is intended to help organizations proactively protect customer account data.

Consolidates and defines the standards for protecting cardholder information across all associations:

- Visa
- MasterCard
- American Express
- Discover

Failure to become PCI compliant can result in fines, higher discount rates, and/or loss of privileges to process credit card transactions.

**Merchant Service Provider:** Also referred to as the credit card processor. This is a third party vendor that processes credit card payments from the cardholder to the seller's bank account. A list of merchant service providers currently under contract with Trinity University can be found on page 5 of the Credit Card Handling Policy and Procedures.

**Credit Card Merchant:** A university department or other entity, such as a campus organization, which processes credit transactions.

**Batch out Sales:** To close out or settle credit card transactions. Batching out sales completes the data entry process and transmits transactions to the merchant service provider. Additional fees may be assessed for failing to batch out sales daily.

# Trinity University Request to Process Payment Cards

Department: \_\_\_\_\_  
 Campus address: \_\_\_\_\_  
 Contact: \_\_\_\_\_  
 E-mail: \_\_\_\_\_  
 Tel: \_\_\_\_\_  
 Fax: \_\_\_\_\_

For Business Office Use Only	
Merchant ID (s):	
MC/VISA:	MID:
AMEX:	TID:
Discover:	DID:
ID(s) Received on:	
Date Submitted to ITS:	

GL Account # for deposits: \_\_\_\_\_ GL Account # for fees/chargebacks: \_\_\_\_\_

*You will automatically be set up to accept MasterCard, VISA, Discover, and American Express (if available for options you will be using)*

Estimated annual credit card sales volume: \$ \_\_\_\_\_  
 Estimated credit card average sales amount: \$ \_\_\_\_\_  
 Percent of credit card sales:  
     Over the counter: \_\_\_\_\_ Telephone/Mail: \_\_\_\_\_ Web: \_\_\_\_\_

***Describe transaction processing methods: software vendor (TouchNet, CBORD), credit card terminals, or other (If other, provide detailed explanation in the box provided below or attach a separate sheet. All third party vendors selected for credit card processing must be a TouchNet ready partner).***

Identify method used for securing documentation containing cardholder information:  
 Locked drawers                      Locked file cabinets                      Safe

Anticipated number of staff who will need access to TouchNet to process E-Commerce transactions:  
 Attach a list of all staff that will be authorized to process credit card sales on their personal computers.

Anticipated number of point of sale terminals needed (if applicable):  
**NOTE:** *Each terminal will need a shared or dedicated phone line.*

Cash register interface with credit cards?                      Yes                      No  
**NOTE:** You must send the software specifications for your cash register system to the Business Office to verify compatibility with existing credit card software.

***Describe Department goods/services offered by accepting credit cards***

***Departmental authorization (VP required):***

Printed name: \_\_\_\_\_  
 Signature: \_\_\_\_\_

Date: \_\_\_\_\_

***Please return the completed form to: Mary Jump – Business Office – Northrup 141-V***

Business Office Approval: \_\_\_\_\_ Date: \_\_\_\_\_  
 Fiscal Affairs Approval: \_\_\_\_\_ Date: \_\_\_\_\_  
 ITS Approval (Security Administrator): \_\_\_\_\_ Date: \_\_\_\_\_

# Trinity University Payment Card Change/Termination Request

Department: \_\_\_\_\_

Campus address: \_\_\_\_\_

Merchant I.D. Account #:

MC/VISA \_\_\_\_\_

AMEX \_\_\_\_\_

DISCOVER \_\_\_\_\_

Business Office Use Only	
Merchant ID (MID)	_____
Terminal ID (TID)	_____
Datawire ID (DID)	_____
Submitted to ITS on:	_____

\_\_\_\_\_ Change department information

\_\_\_\_\_ Terminate department account

**Check all boxes containing a change and indicate new information**

\_\_\_\_\_ Contact: \_\_\_\_\_

\_\_\_\_\_ Telephone: \_\_\_\_\_

\_\_\_\_\_ E-mail: \_\_\_\_\_

\_\_\_\_\_ Fax: \_\_\_\_\_

\_\_\_\_\_ Dept. Account # for deposits: \_\_\_\_\_

\_\_\_\_\_ Dept. Account # for fees/chargebacks: \_\_\_\_\_

**Credit Card processing method/equipment**

\_\_\_\_\_ Credit Card terminal

\_\_\_\_\_ Cash Register

\_\_\_\_\_ PC Software

\_\_\_\_\_ TouchNet

**Department Goods/Services offered by accepting credit cards:**

Departmental authorization: Name: \_\_\_\_\_  
(please print)

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Please return the completed form to:**

Name: \_\_\_\_\_ Department: \_\_\_\_\_

Business Office approval: \_\_\_\_\_ Date: \_\_\_\_\_