Policy: Credit Card Handling Policy and Procedures

I. PURPOSE

This policy sets forth requirements to be followed by employees, associates, affiliates, and other individuals (including students) and provides guidance for the compliance with industry standards for credit card processing.

II. 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.

III. DEPARTMENT REQUIREMENTS FOR CREDIT CARD PROCESSING INCLUDE THE FOLLOWING:

A. 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).

B. University Information Security Administrator (in Information Technology Services) approval of all technology implementation, including approval of authorized payment gateways.

C. Attend card security training before beginning to process credit card transactions and at least once every year. Once training is completed, credit card handler and processor will be provided with a Statement of Payment Card Industry Compliance.

D. 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.

E. 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 Information Technology Services (ITS) to complete SAQ D Version 2.0 Oct 2010.

F. Compliance with Payment Card Industry (PCI) Data Security Standards

Periodic reviews of safeguarding and storage of cardholder information will be conducted by the Business Office.

---

1 Updated: March 29, 2012 — previously stated SAQ C Version 1.2 Oct. 2008
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 Administrator 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.

IV. 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.

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

- Keep secure and confidential all cardholder data 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.

  - Create and maintain Office Procedures for Handling Credit Card Data (Office Procedures) specific to the Department. Return signed forms to the Business Office. Review and update Office Procedures annually.¹
  - Require all personnel involved in credit card handling to read and sign the department’s Office Procedures.²
  - Ensure the department does not store or retain credit card numbers after processing.³
  - Ensure credit card transactions are only conducted on secure computers or other authorized devices.⁴

- Sensitive cardholder data (i.e., full account number, type, expiration, and track (CVC2/CVV2) data, CANNOT be stored in any fashion (paper, computers or networks, etc.).⁵

- Credit card numbers must NOT be transmitted in an unsecure 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. E-mails received containing credit card numbers should not be accepted. The credit card number should be deleted and then a response may be sent to inform the individual that for their security, the University does not accept credit card information through e-mail. The e-mail should then be deleted and emptied from the Trash Folder.

- The University Records Retention Policy requires that all credit card receipts be retained for 7 years in a “secure” environment with access limited to dependable, trustworthy and accountable staff and MUST NOT CONTAIN CREDIT CARD #, EXPIRATION DATE, SECURITY CODE OR OTHER CARD HOLDER DATA. Secure environments include locked drawers, file cabinets in locked offices, locked

---

¹ Added March 29, 2012
² Added March 29, 2012
³ Added March 29, 2012
⁴ Added March 29, 2012
⁵ Added March 29, 2012
⁶ Added March 29, 2012
⁷ Added March 29, 2012
storage facilities, and safes.\(^8\)

- If credit card information is collected or submitted on an intake form, the credit card number must be cut off and destroyed by cross cut shredder immediately after transaction is complete. The form can then be retained for 7 years in a secure environment.\(^9\)

- All credit card receipts must be destroyed in a manner that will render them unreadable after 7 years. Records reaching their expiration date must be destroyed by a cross cut shredder, and their destruction documented OR the records may be securely sent to the Trinity University Warehouse to be destroyed by an outside vendor in order to provide verifiable destruction dates.\(^10\)

**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 individuals, and transfer or promotion of current employees to positions with unrestricted access to cardholder information.\(^11\)

- Background checks must be performed on all individuals (faculty, staff, students, volunteers) involved in credit card handling prior to beginning work.\(^12\)

- Contact Human Resources at extension 7507 or humanresources@trinity.edu to schedule a background check.\(^13\)

- Require all personnel involved in credit card handling to attend card security training once every year. Limit access to system components and cardholder data to only those individuals whose job requires such access.\(^14\)

- Maintain an updated list of authorized credit card processing personnel, authorized computers or other media (forms, wireless hand held units, computers, etc.).\(^15\)

- 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.

- Ensure that annual training is attended by all employees and managers involved in the processing of credit cards.

- 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.

---

\(^8\) Added March 29, 2012
\(^9\) Added March 29, 2012
\(^10\) Updated: March 29, 2012 – previously stated: All documentation containing card account numbers must be destroyed in a manner that will render them unreadable after their useful life (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.
\(^11\) Updated: March 29, 2012 – previously stated: Background checks must be performed prior to the hiring of any new individuals, transfers or promotions of current employees for positions with unrestricted access to cardholder information.
\(^12\) Added March 29, 2012
\(^13\) Added March 29, 2012
\(^14\) Updated: March 29, 2012 – previously stated: Require all personnel involved in credit card handling to attend card security training at least every two years.
\(^15\) Added March 29, 2012
Credit Card Handlers and Processors (within each Department)

- Please note that Student Organizations must have a faculty or staff sponsor and a general ledger account.
- Agree not to disclose or acquire any information concerning a cardholder’s account without the cardholder’s consent.
- 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 providers 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. Read and sign the Department Office Procedures for Handling Credit Card Data.
- Attend card security training before beginning to process credit card transactions and at least once every year. Once training is completed, credit card handler and processor will be provided with a Statement of Payment Card Industry Compliance.
- Read and sign the Department Procedures for Handling Credit Cards.

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 and required annual 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 personnel 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.

---

16 Added March 29, 2012
17 Updated: March 29, 2012 – previously stated: 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.
18 Added March 29, 2012
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 SAQ (security self-assessment questionnaire).

Establishing New Credit Card Department Account

In order to accept credit cards in return for goods/services, department personnel involved 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 110. 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 questions or concerns about accepting credit cards, please contact the Business Office for assistance at extension 7336.

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 department 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 University 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 each department’s responsibility to verify that this information is correct.

Information Security Incident Response Policy

Current ITS policies and procedures 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 dsec@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, TUPD (Trinity University Police Department) should be contacted at extension 7070.

---

19 Updated: March 29, 2012 – previously stated: Infosec@trinity.edu
20 Updated: March 29, 2012 – previously stated: Campus Security
ADDITIONAL INFORMATION

<table>
<thead>
<tr>
<th>E-COMMERCE</th>
<th>Electronic commerce transactions must be processed using either TouchNet or CBORD, as these are the only university approved e-commerce providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEES</td>
<td>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.</td>
</tr>
</tbody>
</table>
| MERCHANT SERVICE PROVIDERS (Credit Card Processors) | - Wells Fargo Merchant Services  
- American Express Merchant Services  
- Discover Merchant Services |

CONTACTS

PCI-DSS Training Requests

Azmin Victoria, Sr. Accountant  
Business Office  
E-mail: avictori@trinity.edu  
Extension: 8006

Merchant ID(s) & Credit Card Statements

Annissa Hernandez, Accountant  
Business Office  
E-mail: aherna10@trinity.edu  
Extension: 7336

University Information Security

Stephen Perez,  
University Information Security Administrator  
Information Technology Services  
E-Mail: sperez@trinity.edu  
Extension: 7619

John Sonnen,  
Director of Enterprise Systems  
Information Technology Services  
E-mail:jsonnen@trinity.edu  
Extension: 8878

Owen Kaltenbacher,  
Senior Application Administrator  
Information Technology Services  
E-mail: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.