TEMPLE UNIVERSITY
POLICIES AND PROCEDURES MANUAL

Title: Credit Card Handling and Acceptance
Policy Number: 05.20.17
Issuing Authority: Office of Financial Affairs
Responsible Officer: Chief Financial Officer and Treasurer

Date Created: November 8, 2006
Date Last Amended/Reviewed: July 3, 2014
Date Schedule for Review: September 2017
Reviewing Office: Bursar's Office

Scope of Policy and Rationale

This policy outlines the university's rules and procedures for the proper handling of credit and debit card transactions, including the responsibilities of university employees who process credit card transactions or maintain cardholder information. These rules and procedures are intended to assure timely handling of credit cards transactions and aid in the safeguarding and proper disposal of credit card information. Failure to follow this policy will result in the loss of credit card processing privileges.

Definitions

1. Credit card payment can be accepted either via the:
    a. Secure website (e-mail is not acceptable)
    b. Over the counter (In-Person)
    c. Telephone
    d. Mail

2. The University may accept any or all of the following credit cards at various locations:
    a. American Express
    b. Discover
    c. MasterCard
    d. Visa

3. Compliance requirement within this policy are derived from the following statutes, regulations or credit card association rules:

    a. Federal Gramm-Leach Bliley Act (GLBA)
    b. Payment Card Industry (PCI) Data Security Standards:
        i. American Express Data Security Program (DSS)
        ii. Discover Data Security (DISC)
        iii. MasterCard Site Data Protection (DSS)
        iv. Visa Cardholder Information Security Program (CISP)
    c. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    d. Federal Educational Rights and Privacy Act (FERPA)

4. Personal Identifiable Information (PII) is information that can be used by others to steal one's identity. This includes:
    a. Cardholder's name
    b. Credit Card number
    c. Cardholder Verification Value (CVV2) – 3 or 4 digit code number generally located on the back of the credit card
    d. Address

Policy Statement

1. Any university department that wishes to accept credit cards as payment for goods and/or services must first submit a written request to the Bursar for approval before credit card merchant numbers are issued. This request will include a copy of the department's procedures as outlined in the Credit Card Handling and Acceptance Procedures, issued by the Bursar's Office, as well as incorporate the use of an authorized vendor. University personnel who receive and/or process credit card information must properly safeguard the data and record the transaction(s). This policy applies to all university personnel who handle PII data during the processing of any transaction, or who retain, store and/or safeguard or dispose of PII data.

2. Only university employees (full or part time) are permitted to handle PII data as defined under this policy and in accordance with the procedures outlined below.

3. Mandatory initial training and subsequent training sessions for system or procedural enhancements will be coordinated by the Bursar's Office. All employees who process or oversee credit card transactions will be required to participate.

4. Budget unit heads, deans, or directors must request that the Human Resources Department perform a criminal background check and credit check before any new or transferring employees are permitted to handle credit card transactions or data. If an existing employee is underperforming, background checks must be completed. There should be no outstanding or unexplained items resulting from these checks.

5. Employees with access to credit card information must sign a credit card security ethics certification to document their understanding and willingness to comply with all university policies and procedures. This certification will be submitted to and maintained by the Bursar's Office. Forms will be made available from the Bursar's Office.

6. PII (Credit card numbers and CVV2) must only be entered into credit card terminals or secure and authorized web applications. Credit card numbers and CVV2 data should not be written down or stored in any technology.

7. All credit card terminals and web applications must be closed out and reconciled on a daily basis. Department are responsible to assure that their cost centers have been credited by the merchant services processor or bank. Furthermore, department are responsible for responding to any disputes, also called chargebacks, within specified time limits (maximum 10-15 days) or fund will be debited automatically from their cost centers.

8. Departments and employees must comply with all requirements of the university's Comprehensive Information Security Program policy (#04.72.11) to protect the integrity and privacy of data within the university's computers, computer systems and networks.

9. Access to PII data must be restricted and all data must be safeguarded from fire and theft.

10. All PII **must** be cross-shredded 120 days after the transaction was processed.

11. Departments using third party vendors' software or systems to process PII or credit card transactions must demonstrate that the vendor is compliant with Payment Card Industry (PCI) Data Security Standards. In addition, the department must have the approval of the Chief Information Security Officer (CISO) that its system meets all university security requirements before it may accept and process any credit card payments.

12. When a university employee suspects the loss or theft of any materials containing cardholder date, they must immediately notify their supervisor, the CISO and University Privacy Officer.

13. Failure to follow these policies may result in the loss of credit card processing privileges as shall be decided by the Bursar.

Roles and Responsibilities

The Bursar is responsible for policy compliance and review.

Exceptions

It is understood that unique situations within individual departments may require permanent exceptions to this policy. Any permanent exception to this policy must be included in a department's written procedures and must be approved by the Bursar and the Chief Financial Officer.

Other unique situations within individual departments may require a limited and/or short-term exception to this policy. Exceptions must be restricted to specific dates or events and must be approved in advance by the Bursar and the Chief Financial Officer.

Communications and Training

Departments/units which accept credit card transactions are responsible for contacting the Manager of Banking Services in the Bursar's Office to arrange training for new employees who will be handling transactions as outlined under this Policy.

Notes

1. **Dates of office enactment and amendments:**

   Approved by the president on November 8, 2006

2. History:

The historical information for the policy is not available as policy was created before a history requirement was created.

Reviewed By:

Bursar, Director of Internal Audits, Chief Information Security Officer, University Privacy Officer

3. Cross References:

Gift Acceptance Policy #05.60.01
University Petty Cast Handling
Comprehensive Information Security Program #04.72.11
Federal Gramm-Leach-Bliley Act (GLBA)
Payment Card Industry (PCI) Data Security Standards:
- American Express Data Security Program (DSS)
- Discover Data Security (DISC)
- MasterCard Site Data Protection (DSS)
- Visa Cardholder Information Security Program (CISP)

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Federal Education Rights and Privacy Act (FERPA)
E-Commerce Policy, Office of the Bursar