TEMPLE UNIVERSITY

POLICIES AND PROCEDURES

Title:	Credit Card Handling and Acceptance
Policy Number:	05.20.17
Issuing Authority:	Office of the Vice President of Finance and Treasurer
Responsible Officer:	Vice President of Finance and Treasurer
Date Created:	November 8, 2006
Date Last Amended/Reviewed:	November 2022
Date Scheduled for Review:	January 2024
Reviewing Offices:	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 acceptance and/or processing privileges.

Definitions

1. Credit card payment can be accepted either via:
    a. Secure website (e-mail is not acceptable)
    b. In person (never permitted for student tuition payments).
    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 requirements within this policy are derived from all applicable statutes, regulations or credit card association rules including the following:

    a. 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. Personally Identifiable Information (PII) is information that can be used by others to steal one's identity or to engage in fraudulent financial activity. 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

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. This request will include a copy of the department's procedures in accordance with those as outlined in this policy and incorporate information about the vendor being used for payment processing. Upon approval, the Bursar will issue credit card merchant numbers. 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 during the processing of any transaction, or who retain, store and/or safeguard or dispose of PII.

1. Only university employees are permitted to handle PII as defined under this policy and in accordance with the procedures outlined below.

2. 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 are required to participate in training.

3. 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 related data. There should be no outstanding or unexplained items resulting from these checks.

4. 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 are available from the Bursar's Office.

5. PII (defined above) 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.

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

7. 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.

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

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

10. 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) to ensure that its system meets all university security requirements before it may accept and process any credit card payments.

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

12. Failure to follow these policies may result in the loss of credit card processing privileges upon review of 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 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 Treasurer.

Communications and Training

Departments/units that 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. **History:**

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

   Last amended:

   Approved by the president on November 8, 2006
   Amended to better reflect university policy in January 2018.
   November 2022: Updated to reflect current Bylaws and job titles.

   Reviewed By:

   Offices of Ethics & Compliance, University Counsel, and University Secretary.

2. **Cross References:**

   Gift Acceptance Policy #05.60.01

   University Petty Cash Handling

   Comprehensive Information Security Program #04.72.11

   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