THE UNIVERSITY OF TENNESSEE

System-wide Policy: FI0311 - Credit Card Processing	
Version: 4	**Effective Date: 06/12/2019**

FI0311 – Credit Card Processing

Topics:

Objective:

This policy provides the requirements and guidelines for all credit card processing activities at the University of Tennessee, including debit card processing and e- commerce activities. The policy addresses protection against the exposure to and possible theft of account and personal cardholder information and the compliance with credit card company requirements for card information that is stored, processed, or transmitted on the university's information technology resources. The referenced credit card company requirements are known as the Payment Card Industry Data Security Standards (PCI DSS). Compliance with the PCI DSS and this policy is mandatory for all university departments/merchants and entities processing credit, debit, or e-commerce payments directly or indirectly.

System-wide Policy: FI0311 - Credit Card Processing	
Version: 4	**Effective Date: 06/12/2019**

Policy:

General Policy

1. Departments are not permitted to engage in any form of credit card payment processing without seeking and receiving approval as required by this policy.

   This includes non-electronic methods (taking payments with an imprinter or payment information on paper forms), face-to-face electronic methods (using point-of-sale (POS) terminals, iPads, etc., or PC-based payment software to process transactions), or indirect electronic methods (taking payments over the phone, via fax, or via e-commerce equipped websites whether handled directly by university employees and systems, or by a third party).

Scope

2. This policy applies to all University of Tennessee employees, contractors, consultants, temporaries, vendors, other third party workers, and any unit that processes, stores, maintains, transmits, or handles payment card information in a physical or electronic format on behalf of the University of Tennessee enterprise, or in use of the University of Tennessee brand name. This includes any entity that utilizes any part of the University of Tennessee network infrastructure for payment card transaction services. This policy also applies to third parties handling credit card payments on behalf of the University of Tennessee.

   Note: This policy does not apply to UT procurement cards or transactions using your university-issued ID card. For more information on procurement cards, see FI0530 - Procurement Cards.

Responsibilities

3. **University Departments/Units (Merchants)**

University departments with Merchant IDs accepting credit/debit card payments for services or goods must:

a. Transmit all credit **or debit** card deposit information to the campus central cashier within three business days of processing. Deposits must be made intact and include all credit **or debit** card transactions received as addressed in FI0130 (batch reports,T-33, ZK doc)
b. Assure that a central, secure server managed by the campus/institute information technology office is used when a certified outsource provider is not feasible.
c. Attend PCI training annually, staying informed of responsibilities.
d. Provide a list of all PCI systems and devices in their area to the campus Chief Information Officer (CIO), once merchant has been approved (see Merchant Approval Process).
e. Notify the CIO when changes occur to system resources (i.e., new PCI systems, addition to PCI firewall zone, etc.).
f. Assure that computing resources used to process, transmit, or store payment data are placed in the segmented cardholder data environment (CDE) designated for this purpose and provided by the CIO.
g. Reconcile and verify credit card transactions in the normal accounting reconciliation process as required by FI0115 - Reconciling and Reviewing Departmental Ledgers.
h. Notify the CIO immediately of any suspected security breaches.
i. Notify Treasurer's Office of any changes to approved credit card transaction processes.
j. Notify the Treasurer's Office of any personnel changes as it relates to merchant services and PCI compliance.
k. Complete appropriate PCI SAQ annually and maintain PCI DSS compliance.
l. Cover all costs associated with PCI DSS compliance, as well as any fines, fees, and remediation expenses associated with a security breach.

4. **Chief Information Officer for Each Campus or Institute**

The CIO for each campus must:

a. Review annual PCI SAQs for technical accuracy before the SAQs are submitted to the appropriate Chief Business Officer (CBO).
b. Provide hardware, software, and other PCI-compliant technical guidance for the purpose of processing, transmitting, and storing payment data.
c. Support departments/merchants in securing systems processing, transmitting, and storing payment data.
d. Maintain lists of all systems and devices that handle, process, or store credit card numbers.
e. Notify University of Tennessee System Administration Information Security Office (UTSA ISO) immediately of any suspected security breaches before making any changes to system(s).
f. Notify UTSA ISO of any significant changes requiring an additional internal vulnerability scan.
g. Create and maintain a separate, segmented cardholder date environment (CDE) and ensure that departmental computing resources used to process, transmit, or store payment data are placed in the environment designated for this purpose. **Note:** CIO can designate the appropriate personnel to execute the above responsibilities

5. **Chief Business Officer**

The CBO for each campus must:

a. Approve the business need for each department and unit requesting to accept credit cards, recognizing the inherent costs associated with PCI DSS compliance.
b. Distribute, collect and review the accuracy of PCI SAQs annually submitted by each department/merchant, accepting risks on behalf of that campus/institute by the approval of the SAQs once they are submitted to the Treasurer's Office.
c. Monitor the compliance with PCI DSS and this policy of campus payment processing activities conducted by university departments/merchants to ensure they are compliant.

d. Verify, in conjunction with the Treasurer's Office, that annual PCI training has been undertaken by all merchant personnel

Note: CBO can designate the appropriate personnel to execute the above responsibilities.

6. **Office of Audit and Compliance**

Office of Audit and Compliance must:

a. Review departmental policies and procedures for processing credit/debit cards upon initial merchant approval request and periodically, as needed, to validate use.

7. **University of Tennessee System Administration Information Security Office**

The UTSA ISO must:

a. Provide advice and guidance to enable applicable entities to understand and comply with the PCI DSS and industry best practices so that payment information can be safeguarded against theft, inadvertent disclosure, and other types of breaches.
b. Review all proposed technology implementations associated with payment processing prior to applicable entities entering into contracts or equipment/software purchases.
c. Provide annual on-site compliance assessments to review PCI processes and accuracy of PCI SAQs.
d. Investigate suspected security breaches and notify the Treasurer's Office, who contacts the payment card processor as necessary.

Note: Forensic investigations must be carried out by PCI Council-approved PCI Forensic Investigators (PFIs). The department/merchant will be responsible for the costs incurred.

e. Coordinate quarterly external PCI scans on applicable PCI systems.

8. **Treasurer's Office**

The Treasurer's Office must:

a. Initiate and manage all communication with the university's merchants.
b. Approve outsourced electronic payment processors.
c. Approve each department and unit that has submitted a request to accept credit cards (See Merchant Approval Process for more information).
d. Request the merchant number for the department from the appropriate processor.
e. Oversee credit card accounting for each approved department and unit.
f. Verify approval of departmental procedures for processing credit cards by Office of Audit and Compliance.
g. Maintain and validate the PCI DSS compliance documentation.
h. Initiate and manage all communication with the university's credit card processor.
i. Assist with yearly site compliance assessments and review the adequacy of merchant PCI processes and accuracy of PCI SAQs
j. Manage annual PCI SAQ reporting process.

Merchant Approval Process

9. The **Merchant Approval Process** (see attachment) for all credit card processing activities shall be as follows:
   a. The department or unit submits the Point-of-Sale and Internet Sales Approval Form for Departments to accept credit/debit card payments to the CIO and the CBO. The approved request form is submitted to the Treasurer's Office.
   b. The Treasurer's Office will review the approved form and notify the submitting department that the form is acceptable. Once the department or

unit receives approval from the Treasurer, the department seeks the assistance of UTSA ISO for interpretation of and understanding PCI DSS and implementation of electronic credit card processing.

c. Once the approved form has been accepted by the Treasurer's Office, the requesting department must develop and submit credit card processing procedures to Office of Audit and Compliance for review (See FI0310 - Receiving and Depositing Money, as well as Point-of- Sale/Internet Credit/Debit Card Processing Procedures for Departments). Office of Audit and Compliance will forward the approved procedures to the Treasurer's Office for filing and to the CBO for informational purposes.

d. Once the completed and approved Point-of-Sale and Internet Sales Approval Form for Departments has been submitted to the Treasurer's Office and the Point-of-Sale/Internet Credit/Debit Card Processing Procedures for Departments has been reviewed by Audit and Compliance, the Treasurer's Office will request a merchant number from the appropriate credit card processor and notify the department accordingly.

Requirements

10. Credit Card Number Storage
    a. The department or unit should never store any complete primary account number (PAN) in electronic or paper format.

Outsource Requirements - Third Party Service Provider

11. Departments and units may elect to outsource some or all of their credit card transaction processing. This option transfers some of the risk to the service provider. Outsourcing does not remove the responsibility for verifying and maintaining protection for the department or unit or completing the necessary PCI SAQ.
    a. Any vendor doing business for and/or representing the university in any way will be required to provide an AOC (Attestation of Compliance) and signed by a QSA (qualified security assessor) to the Treasurer's office.

b. Contracts/agreements must include language requiring the third-party vendors to comply with all appropriate PCI DSS requirements and provide proof of compliance annually.

Noncompliance with Policy

12. Payment processing capabilities will be suspended for departments and units that fail to meet the requirements outlined in this policy. Additionally, the applicable credit card company may impose significant fines. Departments and units that do not comply with this policy and the associated required procedures are subject to, but not limited to, suspension of merchant privileges, disconnection of network services, and/or confiscation of equipment pending review and approval of such processes, procedures, and/or equipment.

Exceptions

13. Any exception to this policy or the established procedures for implementing this policy must be requested in writing in advance and approved by the Treasurer's office, UTSA CISO, Audit, and Campus CIO.

PROCEDURES

To view links to campus policies and procedures, click here:

https://policy.tennessee.edu/campus-policies-procedures/

Forms

- Point-of-Sale and Internet Sales Approval Form for Departments
- Point-of-Sale/Internet Credit/Debit Card Processing Procedures for Departments

Attachments

- Merchant Approval Process (FI0311-Merchant-Approval-Process-Flow-Chart.pdf)

Additional Information

- University of Tennessee Merchant Services and PCI Compliance Website

FOR MORE INFORMATION:

Justin Holt (865) 974-4100 holt@tennessee.edu