THE UNIVERSITY OF TENNESSEE

System-wide Policy: FI0311 - Credit Card Processing	
Version: 3	**Effective Date: 11/01/2017**

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: 3	**Effective Date: 11/01/2017**

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.
   a. This includes non-electronic methods (taking payments with an imprinter or payment information on paper forms), face-to-face electronic methods (using 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).
2. Outsourcing General Policy: Departments and units may elect to outsource credit card transaction processing. This option transfers most of the risk to the third party service provider. However, outsourcing does not remove the responsibility for verifying and maintaining protection from the outsourcing department or unit, nor does it eliminate the requirement of completing an annual PCI Self-Assessment Questionnaire (SAQ). Approval for credit card transaction processing must follow the merchant approval process (see section labeled Merchant Approval Process). Contracts/agreements must include language requiring the third party to comply with all appropriate PCI DSS requirements and provide proof of compliance annually.

Scope

3. This policy specifically addresses all credit/debit card processing by and for the University of Tennessee. All electronic and non-electronic methods mentioned above apply and are subject to this policy. This remains true of any payments, whether handled directly by the university, on university-owned systems, or handled by third parties on the university's behalf.
4. This policy applies to all students, faculty, staff, and others, referred to as users, while accessing, using, or handling the University of Tennessee's applicable

information technology resources. All users are required to be familiar with and comply with this policy.

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

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

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

a. Deposit or transmit all credit **or debit** card payments 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
b. Assure that outsourced electronic payment processing and cardholder information handling is provided by only those processors who have been approved by the Treasurer's Office.
c. Assure that a central, secure server managed by the campus/institute information technology office is used when a certified outsource provider is not feasible.
d. Attend PCI training annually, staying informed of responsibilities.
e. 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).
f. Notify the CIO when changes occur to system resources (i.e., new PCI systems, addition to PCI firewall zone, etc.).
g. 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.

h. Reconcile and verify credit card transactions in the normal accounting reconciliation process as required by FI0115 - Reconciling and Reviewing Departmental Ledgers.
i. Notify the CIO immediately of any suspected security breaches.
j. Notify Treasurer's Office of any changes to approved credit card transaction processes.
k. Complete appropriate PCI SAQ annually and maintain PCI DSS compliance.
l. Maintain internal policies and procedures to meet PCI requirements.
m. Cover all costs associated with PCI DSS compliance, as well as any fines, fees, and remediation expenses associated with a security breach.

6. **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 CDE and ensure that departmental computing resources used to process, transmit, or store payment data are placed in the environment designated for this purpose.

7. **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. 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.
   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. Provide annual PCI training for all departments/merchants as part of UT's formal security awareness program and keep records of attendance.
   e. Send regular PCI security reminders to all departments/merchants as part of UT's formal security awareness program.
   f. Approve any change to credit card processes and communicate decision with the Treasurer's Office.

8. **Audit and Consulting Services**

   Audit and Consulting Services must:

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

9. **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. Perform internal vulnerability scans at least quarterly on applicable PCI systems.
f. Perform internal vulnerability scans after significant changes (i.e., new systems, changes in network topology, firewall rule changes, etc.) regarding applicable PCI systems.
g. Coordinate quarterly external PCI scans on applicable PCI systems.

10. **Treasurer's Office**

The Treasurer's Office must:

a. Establish the merchant response process and collect the responses to the PCI SAQ.
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 Audit and Consulting Services.
g. Maintain and validate the PCI DSS compliance documentation.
h. Initiate and manage all communication with the university's credit card processor.

Merchant Approval Process

11. 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. Additionally, once the approved form has been accepted by the Treasurer's Office, the requesting department must develop and submit credit card processing procedures to Audit and Consulting Services for review (See FI0310 - Receiving and Depositing Money, as well as Point-of-Sale/Internet Credit/Debit Card Processing Procedures for Departments). Audit and Consulting Services 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 Consulting Services, the Treasurer's Office will request a merchant number from the appropriate credit card processor and notify the department accordingly.

Requirements

12. **Credit Card Number Storage Requirements**
    a. The department or unit should never transmit or store any credit card numbers on any system, personal computer, or e-mail account that has not been explicitly authorized by this policy.
    b. The Card Security Code, e.g., a three- or four-digit number on the back of the credit card, must not be stored after the initial transaction is approved. MasterCard, Visa, and Discover credit, as well as debit cards, have a three-digit Card Security Code, called the "CVC2" (card validation code), "CVV2" (card verification value), and "CID" (card identification number), respectively.
    c. Credit card numbers should only be stored in one location to minimize the monitoring and cost of compliance. One exception for storing in multiple locations would be electronic backups of secured/registered servers.
    d. Departments/merchants may only use devices and systems approved by the Treasurer's Office. Departments/merchants must not use personally-owned systems or mobile phones (university issue or personal) for receiving, processing, or storing credit card data.
    e. All systems that handle, process, or store credit card numbers must be registered with the CIO.

Outsource Requirements - Third Party Service Provider

13. Departments and units may elect to outsource 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 from the department or unit, nor does it eliminate the requirement of completing an annual PCI SAQ. Approval for credit card transaction processing must follow the standard approval process. Contracts must include language that the third party is required to comply with all appropriate credit card company security requirements and annually complete the PCI SAQ.

Noncompliance with Policy

14. 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.

PROCEDURES

Knoxville:	http://budget.utk.edu/fiscal-policy/
Health Science Center:	https://uthsc.policymedical.net/policymed/home/index?ID=de47aa28-16aa-408b-9c96-cb04f232964f&
Institute of Agriculture:	https://ag.tennessee.edu/Pages/UTIApolicies.aspx
Martin:	http://www.utm.edu/departments/finadmin/procedures.php
Chattanooga:	http://www.utc.edu/business-financial-affairs/fiscalpolicies.php

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)

FOR MORE INFORMATION:

Justin Holt (865) 974-2493 jholt11@utk.edu