**Internal Credit/Debit Card Processing
Policies and Procedures for**

**University of Tennessee Merchants**

**Merchant:** DBA

**Effective:** Date

**Reviewed:** Date

**Revised:** Date

1. General Statement

2. Point-of-Sale Processing System

3. Internet Credit Card Processing System

4. Reporting Deposits to the University Depository

5. Voids, Returns, and Chargebacks

6. Protection of Credit Card Information

7. Implementing and Revising the Procedures

# 1. General Statement

The University of Tennessee’s Merchant/Department recognizes credit and debit card sales as a way to provide an additional service to its List Types of Customers for the department. In providing such a service, it is advantageous to have the capability to process credit and debit card (check cards issued by well-established credit card companies) transactions. This document provides procedures for processing such transactions with a point-of-sale and/or Internet processing system, which offers our customers the opportunity to Describe product or service the customer will pay for with credit and debit cards. This document also contains internal policies for the processes.

# 2. Point-of-Sale Processing System

Describe what type of equipment, including make and model, will be used for the credit and debit card point-of-sale (POS) systems, the type of transactions that will be processed (e.g., face-to-face, phone, fax), and the name of the processor. Using the type of machine, the credit card information is captured and transmitted via the phone line to processor for authorization/approval. Each day, at a predetermined time, all approved transactions are submitted to processor for batch settlement. Employee 1 in department releases the batch and **generates a daily batch release report** detailing transactions processed by the department and must process the deposits received within three business days as specified in University Policy FI0310, *Credit Card Processing*. Employee 1 reconciles the daily batch release report to the daily transactions. Employee 2 must reconcile the daily batches with the IRIS ledgers.

# 3. Internet Credit Card Processing System

Describe how the department will manage or implement a secure Internet site using software. Describe the type of transactions (credit cards, debit cards, electronic funds transfer, automated clearinghouse) and what software is being used, etc. Our approved processor and the software are certified compliant with the Payment Card Industry Data Security Standards. The customer is redirected to the payment site prior to entering any cardholder data. Using this software, the credit card information is captured via the processor’s site and is transmitted electronically by the processor for authorization/approval. Each day, a predetermined time, all approved transactions are submitted to the processor for settlement. Employee 1 in department releases the batch and **generates a daily batch release report** detailing transactions processed by the department and must process the deposits received within three business days as specified in University Policy FI0310*, Receiving and Depositing Money*. Employee 1 reconciles the daily batch release report to the daily transactions. Employee 2 must reconcile the daily batches with the IRIS ledgers.

# 4. Reporting Deposits to the University Depository

Transactions will occur in the point-of-sale and/or Internet system on a real-time basis, meaning the customer’s credit card account will be charged upon completion of the transaction. However, department will use a “batch method” of settling daily credit card transactions with the university depository. Describe what your department does. Settlement will occur at the beginning of each business day at specify time for transactions successfully completed the previous day. The software provided by the university depository allows the reporting and batch processing of daily transactions.

The following procedures should be followed:

Employee 1 reconciles the daily transaction register provided by the credit/debit card sales system with the sales/inventory/registration system information. Describe what the staff member does and the reports he/she generates.

Upon reconciliation of the daily transaction register provided by the credit/debit card sales system, Employee 1 from department will release the transactions to the depository for settlement.

Employee 1 prepares the deposit (as with normal operations) using the IRIS deposit document, as described in Policy FI0310. The deposit from credit and debit cards will be remitted as part of the normal deposit routine within three business days.

Employee 1 will remit deposits along with other transactions to the Bursar’s Office (or central cashier) within three business days of the funds’ receipt, with the exception of holidays and days of administrative closing.

Deposits for the department will be credited to the following cost center(s) or WBS element(s): cost center(s) or WBS element(s).

Employee 2 will perform a monthly reconciliation of daily batch totals to the departmental ledger(s).

The basic rule for division of duties is that the employee who performs the monthly reconciliation should not handle money or process any daily transactions.

# 5. Voids, Returns, and Chargebacks

**Voids**

No opportunity will be available for the customer or department personnel to void a credit card transaction. Once the customer successfully completes the transaction, he or she may not reverse or cancel it, and department staff may not void any successfully completed transactions from the point-of-sale system. If voids are allowed, describe the process, how voids are authorized, and who authorizes.

**Returns**

In certain cases, it may be necessary for a customer to receive payment refunds. Director of department will approve in writing all refunds, returns, and like credits. After Director has approved a return, he/she will send a memo to the Bursar’s Office (or central cashier). The Bursar’s Office (or central cashier) will determine whether the customer has outstanding university debts before any refund is issued. Refunds will be debited to department’s cost center(s) or WBS element(s).

*Note: If the credit is processed online, describe which employee performs the credit and the procedures that are followed.*

**Chargebacks**

A chargeback occurs when a merchant is required to issue credit to a cardholder's account. The merchant is billed by its acquiring bank, which has been billed initially by the card issuer. This may happen for a number of reasons, but most often a cardholder disputing a transaction triggers a chargeback. If chargebacks occur, describe the process, steps taken to find the correct account, who makes the correction to the account, and who authorizes.

# 6. Protection of Credit Card Information

**Point-of-Sale**

The department securely processes all point-of-sale transactions using the point-of-sale system from vendor which is compliant with Payment Card Industry Data Security Standards. The point-of-sale vendor is a leading provider of trust services, including authentication, validation, and payment needed by the Payment Card Industry Data Security Standards. The department does not retain the full content of any track from the card’s magnetic stripe or the personal identification number (PIN), or encrypted pin block after authorization, and under no circumstances is the card verification code (CVC, CVV) ever stored. In addition, the primary account number (PAN) is masked and only the last four digits of card numbers are displayed on any printed materials or credit card devices, including reports and receipts. Leaving media of any kind unsecured for viewing, copying, or scanning is strictly prohibited.

The department secures all point-of-sale devices by procedure, e.g., locked in cabinet, locked office, etc.. Describe the department’s procedure for assigning responsibility and securing mobile point-of-sale devices. The POS system is periodically inspected for tampering or substitution. This includes verification of terminal serial number and review of any unwarranted attachments. Personnel will be trained to be aware of and identify tampering. Any signs of tampering or substitution of devices will be immediately reported to the Treasurer’s Office or the UTSA ISO.

Department trains all employees who handle cardholder information on privacy and confidentiality and performs background checks on all employees.

**Internet Sales**

All transactions are securely processed using software over a connection using a protocol for encrypting information over the Internet and department is no longer using SSL nor early TLS (older than v1.1). Software vendor is a leading provider of trust services, including authentication, validation, and payment needed by websites to conduct trusted and secure electronic commerce and communications over Internet protocol (IP) networks. State where the credit card data resides and how it is protected. Describe any other protection mechanisms and how paper and electronic records are destroyed securely.

Department will never instruct a customer to use any UT-owned device (e.g., computers in a lab or library setting) for making credit card payments for our products or services. Customers will be instructed to pay on a non-university owned device, unless this was part of the processes approved by the Treasurer’s Office.

**Additional Polices for Protecting Credit Card Information**

Strict control of all media pertaining to credit card processing is maintained at all times with regards to internal or external distribution of all media. All media is classified as “moderate” and will be secured as such. Media includes, but is not limited to, computers, point-of-sale terminals, other removable electronic media, paper receipts, paper reports, and faxes. Media leaving the merchant area will be sent via secured courier or other delivery method that can be accurately tracked, and management will approve by signature prior to moving it.

Only approved critical technologies are allowed and users are required to have complete understanding and acknowledgement of their proper uses prior to the necessary explicit authorization by management. Inventory logs are maintained to provide strict control of storage and accessibility. The inventory list includes the make, model, location, and the explicitly authorized users of the device and is updated when devices are added, relocated, decommissioned, or when authorized users change.

All reports and receipts with cardholder information are secured in a locked cabinet with limited access. Once transactions have been approved via processor and the receipt has been printed, all card number and personal information is shredded using a cross-cut shredder. Describe how stored paper records are securely destroyed (e.g., Records Management, Shred-It, etc.).

Cardholder numbers are never stored electronically. Any cardholder data that is received electronically will be immediately deleted and the Recycle Bin/Trash will be immediately emptied. To ensure data is not recoverable, a secure eraser/sanitization application will be run immediately.

Cardholder data is never sent via text, chat, or other end-user messaging technologies. Credit card payments are never asked for nor accepted via email. Should a customer email their card information to a merchant representative, the email will be deleted immediately and the email Deleted Items/Trash will be immediately emptied. The customer will be sent a new email (not a reply to the original message) saying that the email containing credit card information has been deleted and payments cannot be accepted via email; and the customer will be given alternative methods for making payments.

Cardholder data will be restricted to merchant representatives on a need-to-know basis. Access rights are granted to privileged users to the least privileges necessary to perform job responsibilities. The privileges will be assigned based on role-based access control (i.e., job classification and function). Once an employee no longer needs the access, or when the employee has been terminated, access will be immediately revoked.

Audit logs and security event logs are reviewed daily by describe processes. These reviews are performed in accordance with the university’s policies and risk management strategy. Any follow up to exceptions and anomalies is performed by describe processes. All audit logs are retained for at least one year and a minimum of the last three month’s logs will be available immediately for analysis.

Department follows the university’s *PCI DSS Vulnerability Scanning Standards* with regards to all internal and external scanning. Scans are performed at least quarterly and after any significant change to the network. All hosts subjected to the scans must pass each scan.

Department follows the university’s *PCI DSS Penetration Testing Standards*. Penetration tests are performed at least annually and after any changes to segmentation controls or methods.

In the event of any suspected data breach, Department will follow UT’s PCI Incident Response Plan, found on UT’s PCI Compliance website.

# 7. Implementing and Revising the Procedures

Department is responsible for implementing these procedures and will discuss this document with all relevant personnel before implementation. Department may revise the procedures as deemed necessary, which will be approved by Director. Department will review the policy at least annually for content and accuracy. Any significant changes to the procedures and/or environment will be reviewed with the campus/institute Chief Business Officer and the Treasurer’s Office before implementation. The procedures are intended to supplement Policies FI0310 and FI0311. University policy will prevail in any discrepancies created by these procedures.

Department will stay involved in the university’s security awareness program. This means all employees processing credit card payments will take part in the annual security awareness training. Employees will also regularly review all policies and procedures.