UTIA Internal Credit/Debit Card Processing Procedures

Merchant: DBA
Merchant ID: MID

Effective: Date
Last Reviewed: Date **Last Updated:** Date

Objective:
This document describes the appropriate procedures for processing and transmitting credit card payments for Merchant/Department, as a merchant of the University of Tennessee Institute of Agriculture (the Institute). 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.

Scope:
The Institute'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.

Procedures:
P2PE Point-of-Sale Processing System (remove this section if you do not process via POS using P2PE)
Merchant/Department uses a make & model wireless terminal that will be used for the credit and debit card point-of-sale (POS) system(s). This PCI-validated P2PE solution is a combination of secure devices, applications, and processes that encrypt credit card data immediately upon swipe or dip in the payment terminal. The data remains encrypted until it reaches Bluefin's secure decryption environment. Types of transactions that will be processed include face-to-face, phone, or fax using Elavon. Using the make & model, the credit card information is captured and transmitted via cellular service or secured WiFi to Elavon, for authorization/approval. Each day, a predetermined time, all approved transactions are submitted to Elavon for batch settlement and is auto-batched. Employee 1 in the Merchant/Department Business Office 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 UT Policy FI0310, Receiving and Depositing Money. Employee 1 reconciles the daily batch release report to the daily transactions. Employee 2 (possibly the appropriate Budget Director) must reconcile the daily batches with the IRIS ledgers.

Internet Credit Card Processing System (remove section if you do not process via ecommerce)
Describe how the Merchant/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 payment gateway/software is being used, etc. Our approved processor, Elavon, and the approved payment gateway 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 gateway's site and is transmitted electronically 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.

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, Merchant/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 they generate.

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 UT 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.

Voids, Returns, and Chargebacks

Voids

No opportunity will be available for the customer or Merchant/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 Merchant/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. Department Head/Director of department will approve in writing all refunds, returns, and like credits. After Department Head/Director has approved a return, they 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 Merchant/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.

Protection of Credit Card Information

Merchant/Department will follow all policies in the UTIA IT0311 – Payment Card Industry (PCI) Security Policy, as well as UT's Policy FI0311 – Credit Card Processing. The Merchant/Department will go over all PCI policies and procedures with new employees prior to allowing access to process or transmit credit card payments, as well as annually with all employees. All employees will also be required to complete annual PCI training.

Merchant/Department will stay involved in the Institute's security awareness program. This means all employees processing credit card payments will take part in the annual security awareness training, as well as the required PCI training. Employees will also regularly review all policies and procedures.

Merchant/Department will stay aware of Service Provider(s) PCI DSS compliance status by working with the Institute's CISO and using the List of Validated Payment Applications, found at. Applications on this list have been assessed for compliance with the Payment Application Data Security Standard (PA-DSS).

Implementing and Revising the Procedures

Merchant/Department is responsible for implementing these procedures and will discuss this document with all relevant personnel before implementation. Merchant/Department may revise the procedures as deemed necessary, which will be approved by Department Head/Director. Merchant/Department will review the procedures at least annually for content and accuracy. Any significant changes to the procedures and/or environment will be reviewed with the Institute's Chief Information Security Officer, the Institute's Chief Business Officer, and the Treasurer's Office before implementation. The procedures are intended to supplement UT Policies FI0310 and FI0311, as well as the UTIA IT0311 – Payment Card Industry (PCI) Security Policy. University and Institute policies will prevail in any discrepancies created by these procedures.

References:

UTIA Glossary of Information Technology Terms
UTIA IT0311 – Payment Card Industry (PCI) Security Policy
UT Policy FI0310 – Receiving and Depositing Money
UT Policy FI0311 – Credit Card Processing

Approval of Procedures

We have discussed with all relevant staff and/or do approve the *UTIA Internal Credit/Debit Card Processing Procedures* as described in this document. Approval is needed only when original procedures are written or when the procedures are updated. When annual review is done, the Primary Point of Contact will sign and date, as will the CISO.

Name	Title	Signature	Date
Name	Primary Point of Contact for Merchant/Department		
Name	Department Head/Director of Dapartment Name, UTIA		
Name	Budget Director, Unit, UTIA		
Sandra D. Lindsey	Chief Information Security Officer, UTIA		
Timothy P. Fawver	Chief Business Officer, UTIA		