Point-of-Sale/Internet Credit/Debit Card Processing Procedures for Departments

Procedures: Point-of-Sale/Internet Credit and Debit Card Processing for Department

Effective: Date

1. General Statement

The University of Tennessee's 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. Department has targeted Date to begin offering customers the opportunity to Describe product or service the customer will pay for with credit and debit cards.

2. Point-of-Sale Processing System

Describe what type of equipment will be used for the credit and debit card point-of-sale system, the transactions that will be processed, and name of the processor. Using this type of machine, the credit card information is captured and transmitted via the phone line to the processor for authorization/approval. Each day, at a predetermined time, all approved transactions are submitted to the processor for batch settlement. Employee 1 in department releases the batch and **generates a daily batch release report** detailing transactions processed by the department. Employee 1 must process the deposits received within three business days as specified in University Policy FI0310. 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. Processor that processes the transaction and the software are compliant with the Payment Card Industry Data Security Standards. Using this software, the credit card information is captured via the Internet and transmitted electronically to the processor for authorization/approval. Each day, at 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. Employee 1 must process the deposits received within three business days as specified in University Policy FI0310. 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 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 and debit card sales system with the sales/inventory/registration system information. Describe what the staff member does and the reports he or she generates.

Upon reconciliation of the daily transaction register provided by the credit and 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: 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 or 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 processes all point-of-sale transactions securely using the point-of-sale system from vendor which is compliant with Payment Card Industry Data Security Standards. Only the last four digits of card numbers are displayed on any printed material or credit card devices, including reports and receipts. Cardholder numbers are not stored electronically. All reports and receipts with cardholder information are secured in a locked cabinet. The department secures all point-of-sale devices by procedure, e.g., locked in cabinet. Describe the department's written procedure for assigning responsibility and securing mobile point-of-sale devices. Department trains all employees who handle cardholder information on privacy and confidentiality and performs background checks on all employees. The point-of-sale merchant is the leading provider of trust services, including authentication, validation, and payment needed by the Payment Card Industry Data Security Standards. Describe how paper records are destroyed securely.

I**nternet Sales**

Third-party vendors,software vendors, and credit card processors have been certified as complying with Payment Card Industry Data Security Standards. Only the last four digits of card numbers are displayed on any printed material or electronic devices, including receipts and reports. All transactions are securely processed using software over a secure sockets layer (SSL) connection (a protocol for encrypting information over the internet). 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.

7. Implementing and Revising the Procedures

Department is responsible for implementing these procedures and will discuss this document with all related personnel before implementation. Department may revise the procedures as deemed necessary, which will be approved by the Director. Department will review the policy at least

annually for content and accuracy. Any significant changes to the procedures 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.