FP-36: Credit Card Policy

I. Credit Card Acceptance and Processing

In the course of doing business at East Tennessee State University it may be necessary for a department or other unit to accept credit cards or checks for payment and gather data from the payer. These payments can be for goods or services, study abroad travel costs, or registration fees for camps or conferences. All personal pay partner accounts are prohibited for payment of ETSU fees, registrations, services or products. An online store can be created to assist departments in the collection of these payments and information.

A uStore website can be established where the department can sell products or services, collect registration fees for camps or conferences, or collect travel costs for study abroad programs. The UStore can also gather needed information from the buyer, student, or registrant. These transactions are commercially secure and utilize a centralized process.

Departments may be able to participate in an existing UStore for the university or may require their own departmental UStore. If a unique UStore needs to be established, a new merchant account for the purpose of accepting and processing credit cards at the University will be requested for ETSU's credit card processor. This is determined on a case by case basis. Any fees associated with the acceptance of the credit card in that unit, can be charged to the unit.

Any department accepting credit cards on behalf of the University or related foundation must designate an individual within the department who will have primary authority and responsibility within that department for credit card transactions. This individual it referred to as the Site Manager. The department should also specify a back-up, or person with secondary responsibility, should matters arise when the site manager is unavailable. Specific details regarding processing and reconciliation will depend up on the method of credit card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and are also available by contacting the Office of Financial Services. Annual reviews will be conducted with each department to discuss updates and any environmental changes with credit cards due to security threats if any, and protection methods evolving rapidly throughout the year.

Sales of tangible property may require the department to charge and remit Tennessee state sales tax. Sales of goods and services may also be identified as Unrelated Business Income (UBI) under Federal Internal Revenue Service regulations which require retention of a portion of the revenue to pay the associated federal tax. The determination of online sales tax and UBI tax is made in Financial Services.

Procedure for initiating and maintaining an online payment site:

Interested departments or units should contact the Financial Information Systems to begin the process of accepting credit cards. Steps include:

1. Completion of a TouchNet Marketplace - New Online Payment Site/Product/TouchNet Ready Partner form.
2. Completion of training.

3. Review the University's "Policies for Credit card Processing and Security", including ensuring ongoing compliance with all requirements of the policy.

II. Credit Card Data Security Policy

This policy addresses Payment Card Industry (PCI) Data Security Standard (DSS) that are contractually imposed by the major credit card brands on merchants that accept these cards as forms of payment. The policy covers the following specific areas contained in the PCI standards related to cardholder data: collecting, processing, transmitting, sorting and disposing of cardholder data.

Procedures must be documented by authorized departments and be available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

A. Cardholder data collected are restricted only to those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access to review the list monthly to ensure that the list reflects the most current access needed and granted.
B. Cardholder data, whether collected on paper or electronically, are protected against unauthorized access.
C. All equipment used to collect data is secured against unauthorized use in accordance with the PCI Data Security Standard.
D. Physical security controls are in place to prevent unauthorized individuals from gaining access to the personal computers, rooms, and cabinets that store the equipment, documents and electronic files containing cardholder data.
E. The Office of Information Technology is responsible for PCI compliance for the electronic payment gateway (currently TouchNet) and all other centrally administered servers that process, store or transmit cardholder data. Individual departments are held responsible for PCI compliance for all departmental procedures, applications, point of sale devices and departmentally administered servers that process, store or transmit cardholder data. Additionally, these procedures, applications and systems should comply with Office of Information Technology policies, and any applicable distributed information technology unit standards. All controls, including firewalls and encryption, should be documented and verified.
F. Email should not be used to transmit credit card or personal payment information, nor should it be accepted as a method to supply such information. In the event that it does occur, disposal as outlined in section II.i. below is critical.
G. No database, electronic file, or other electronic repository of information will store credit/debit card numbers, the full contents of any track from the magnetic stripe or the card-validation code.
H. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited, to the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants, and portable external hard drives.

I. Cardholder data should be destroyed immediately following the required retention period. The maximum period of time the data may be retained is 15 months. A regular schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data it kept beyond the record retention requirements. Paper documents should be shredded in a cross-cut shredder. Before disposal or repurposing, computer drives should be sanitized in accordance with the University Electronic Data Disposal Policy.

III. Responding to a Security Breach

Refer to the Personal Information Security Breach Policy in the event of a breach or suspected breach of security.

If warranted, the Office of Financial Services will alert the merchant bank, the payment card associations, Internal Audit, General Counsel, and the Executive Vice President. A suspected breach may be reported to East Tennessee State University by the processing bank or/and outside party. In that case, the Financial Services Department will notify the campus merchant involved in the suspected breach and the relevant steps outlined in the Personal Information Security Breach Policy should be executed. A detailed incident response plan will be maintained by the Financial Services Department.

IV. Sanctions

Failure to meet the requirements outline in this policy will result in suspension for the physical and, if appropriate, electronic payment capability with credit cards for affected units. Additionally, if appropriate, any fines and assessments which may be imposed by the affected credit card company will be the responsibility of the impacted unit.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

V. Other Related Policies

FP-32 Identity Theft Prevention Policy

East Tennessee State University Web Privacy Statement

VI. Definitions

Cardholder data any personally-identifiable data associated with a cardholder. Such data include account number, expiration date, name, address, social security number, Card Validation Code, Card Verification Value, Card Identification Number, or Card Member ID.

Merchant Department any department or unit (can be a group of departments or a subset of a department) which has been approved by East Tennessee State University to accept credit cards and has been assigned a Merchant identification number.

PCI-DSS Payment card Industry Data Security Standards

Site Manager an individual within the department who has primary authority and responsibility within that department for credit card transactions.

Touchnet Gateway the only approved gateway for processing credit card transactions per the University policy.

uStore online payment website where departments sell products or services, collect registration fees for camps or conferences, or collect travel costs for study abroad programs. The website can gather needed information from the buyer, student, or registrant.