

## **BUSINESS POLICY LETTER**

TO: All Members of the University Community 2009:06

DATE: February 2009

### **CREDIT CARD PROCESSING AND SECURITY POLICY (Supersedes 2008:05)**

---

#### **I. SCOPE**

This policy applies to all Ferris State University faculty, staff, students, organizations and individuals who, on behalf of the University, handle electronic or paper documents associated with credit or debit card receipt transactions or accept payments in the form of credit or debit cards. The scope includes any credit or debit card activities conducted at all Ferris State University campuses and locations.

#### **II. POLICY STATEMENT**

University departments may accept credit and debit cards as a form of payment for goods and services provided, after receiving advance written approval from the Director of Business Operations in accordance with the Billing, Receipt Handling and Deposits Policy and following the objectives set forth in this policy.

Departments, who need to accept credit/debit cards and obtain a physical terminal to either swipe or key transactions through a data capture machine, need to contact the Director of Business Operations and complete the required paper work to obtain a merchant number(see Attachment A).

Departments wishing to engage in electronic commerce should use TouchNet's electronic payment gateway. Requests should be directed to the Director of Business Operations and Attachment A should be completed and filed with the Business Operations to obtain a merchant number.

This policy addresses Payment Card Industry (PCI) Security Standards that are contractually imposed by VISA and MasterCard on merchants who accept these cards as forms of payments. The policy covers the following specific areas contained in the PCI Security Standards related to cardholder data: collecting, processing, transmitting, storing and disposing of cardholder data.

Procedures must be documented by authorized departments and be available for periodic review. Departments seeking final authorization must ensure that the following objectives are met:

1. Access to cardholder data collected is restricted only to those users who need it to perform their jobs.

2. Cardholder data, whether collected on paper or electronically, is protected against unauthorized access.
3. All equipment used to collect data is secured against unauthorized use in accordance with the PCI Data Security Standard.
4. Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets where the equipment or documents containing cardholder data is stored.
5. Cardholder data is not processed, stored or transmitted using the University's network unless the PCI Compliance Officer and IT have verified the technical controls, including firewalls and encryption, are in accordance with the [PCI Data Security Standard](#).
6. Databases do not store credit/debit card number, the full contents of any track from the magnetic stripe or the card-validation code.
7. 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.
8. Cardholder data is deleted or destroyed before it is disposed. Paper documents should be shredded, and computer drives erased, degaussed, or physically destroyed in accordance with the University's Information Security Guidelines referenced within the Information Security Policy.
9. Credit card terminals are physically secured and batch/transmitted on a daily basis.

### **III. DEFINITIONS**

Cardholder: The individual to whom a credit card or debit card has been issued or the individual authorized to use the card.

Cardholder data: All personally identifiable data about the cardholder gathered as a direct result of a credit or debit card transaction (e.g. account number, expiration date, etc.).

Card-validation code: The three-digit value printed on the signature panel of a payment card used to verify card-not-present transactions. On a MasterCard payment card this is called CVC2. On a Visa payment card this is called CVV2.

Credit or Debit Card Receipt Transactions: Any collection of cardholder data to be used in a financial transaction whether by facsimile, paper, card presentation or electronic means.

Database: A structured electronic format for organizing and maintaining information that can be easily retrieved. Simple examples of databases are table or spreadsheets.

Encryption: The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key. Use of encryption protects information from unauthorized disclosure between the encryption process and the decryption process (the inverse of encryption).

Firewall: Hardware and/or software that protect the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet must have a firewall to prevent outsiders from accessing its own private data resources.

Magnetic Stripe Data (Track Data): Data encoded in the magnetic stripe used for authorization during a card present transaction.

Network: A network is defined as two or more computers connected to each other so they can share resources.

PCI: **Purchasing Card Industry Standard** is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

#### **IV. RESPONSIBILITIES**

**Director of Business Operations**: The Director of Business Operations or a designated appointed official is responsible for the periodic reviews of departmental procedures and practices in connection with credit and debit card receipt transactions. Results will be reported to the Associate Vice President for Finance. All issues of non-compliance will be reported immediately to the Associate Vice President for Finance.

**Information Technology Systems (ITS)**: The Information Technology Systems Office is responsible for regularly monitoring and testing the Ferris network. ITS will cooperate with the PCI Compliance Officer in accordance the University's compliance with the PCI Standard technical requirements and verify the security controls of systems authorized to process credit cards.

**Heads of departments and activities**: Department heads are responsible for documenting departmental procedures and for ensuring that credit and debit card activities are in compliance with this policy. Departments will potentially be responsible for any fines levied against the University that result from noncompliance by the department.

#### **V. COMPLIANCE**

The Vice President for Administration and Finance and/or the Associate Vice President for Finance will terminate credit and debit card collection privileges for any department not in compliance with this policy.

Failure to meet the requirements outlined in this policy will result in suspension of physical and or electronic payment capability for the affected departments. Additionally, fines may be imposed by the affected credit card company, beginning at \$500,000 for the first violation, from each card company.

Persons in violation of this policy are subject to the full range of sanctions up to and including termination. Some violations may constitute criminal offenses under local, state and federal laws. The University will report such violations to the Vice President for Administration and Finance and/or the Associate Vice President for Finance.

## **VI. OTHER RELATED POLICIES**

Billing, Receipt Handling and Deposits Policy; Consolidated Billing Policy; Information Security Policy; Proper Use of Information Resources, Information Technology, and Networks Policy.

Rick Christner  
Interim Vice President for  
Administration and Finance

Contact Office: Associate VP for Finance