BUSINESS POLICY

TO: All Members of the University Community 2016:07

DATE: February 2016

Credit Card Processing and Security Policy
(Supersedes Policy 2009:05 & 2012:12)

Contents

Section 1 – 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.

Section 2 – 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 Student Financial Services in accordance with the Cash 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 Student Financial Services 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 Student Financial Services and Attachment A should be completed and filed with the Student Financial Services to obtain a merchant number. When they apply there will be a discussion to determine the best option for the area.

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. Cardholder data is not to be sent via end-user messaging technologies. (E-mail, text message, instant messenger, etc.)

7. Databases do not store credit/debit card number, the full contents of any track from the magnetic stripe or the card-validation code. Reports must mask the card number to the first six or last four digits only.

8. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact discs, USB flash drives, mobile communication devices and portable external hard drives.

9. Cardholder data is deleted or destroyed before it is disposed. Paper documents should be cross-cut shredded and destroyed when it's no longer needed for business or legal reasons in accordance to University Records Management Policy. Computer drives must be erased, degaussed, or physically destroyed in accordance with the University's Information Security Guidelines referenced within the Information Security Policy.

10. Credit card terminals are physically secured and batch/transmitted on a daily basis.

11. In the event of a compromise to customer credit card numbers or to a card processing device, departments will notify the Director of Student Financial Services immediately, who will then report the incident to appropriate law enforcement, the merchant bank, the cardholder and various card associations as needed.

Section 3 – 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: **P**urchasing **C**ard **I**ndustry 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.

Section 4 – Responsibilities

Director of Student Financial Services

The Director of Student Financial Services or designee 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 Services (ITS)

The Information Technology Services 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.

Section 5– Compliance

The Vice President of Administration and Finance and/or the Assistant Vice President for Finance will terminate the privileges from any departments that are 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 Assistant Vice President for Finance.

Section 6– Other Related Policies

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

Jerry L. Scoby
Vice President for
Administration and Finance

Contact Office: Director of Student Financial Services

Attachment A

CREDIT CARD PROCESSING
APPROVAL/AUTHORIZATION

Description:

Any university area that wants to accept credit card or debit card payments for good/services rendered must be pre-approved in writing by the PCI Compliance Officer.

If a department is considering using any method other than TocuhNet Payment Gateway to process credit and debit card transactions, the systems must be verified for appropriate technical controls in accordance with the Payment Card Industry(PCI) Security Standard prior to receiving final approval for electronic credit card processing from the PCI Compliance Office.

The PCI Compliance Officer will coordinate the appropriate review and provide a report to the Direct of Student Financial Services for final authorization. Any noncompliant issues will be reported immediately to the Assistant VP for Finance

What to do:

Complete page two of this form, then contact the PCI Compliance Officer, in the Student Financial Services Office, to schedule the verification process.

What the PCI Compliance Officer will do:

The PCI Compliance Officer will review at a minimum, the following technical controls:

- Cardholder data is protected by a secure network that includes a firewall configured in accordance with the PCI Data Security Standard.
- Encryption techniques are used to transmit data over public networks, in accordance with the PCI Data Security Standard.
- On-site departmental review of how/where data will be stored.

Ferris State University
Request to Process Credit Cards

Department Name: _____

Physical Campus Address: _____

Contact Name: _____ Contact Phone: _____

Contact Email: _____ Contact Fax: _____

Primary Customer Service Phone Number	
Years/Months in Business	Years Months
Years Under Current Management	Years
Types of Products/Services Sold	
Accept the following card types (check all that apply, rates are competitive)	□ Visa □ MasterCard □ Discover
Estimated Average Purchase Amount	$
Estimated Average Monthly Sales	$
Estimated Occasional Higher Ticket Amounts	$
Estimated Number of Monthly Transactions	
Refund Policy (check one)	□ No refund □ Refund in 30 days □ Merchandise exchange □ Other (please explain): _____
Method of processing credit cards (check one)	□ Merchant terminal □ E-commerce site □ Touchnet Ready Partner Application Name Application: _____
Percent of Card Sales (must equal 100%)	_____ card present (over the counter/swipe) _____ card not present (web/keyed)
Seasonal Merchant	□ Yes, active the following months: _____ □ No, transactions 12 months of the year
Date technical review completed and approved with IT (not applicable for merchant terminal processing)	

_____ _____
Department Signature PCI Compliance Officer Approval

_____ _____
Date Date

Return completed form to:
PCI Compliance Officer
1201 S. State St. CSS 101Q
Big Rapids, MI 49307