CREDIT CARD PROCESSING AND SECURITY

POLICY NUMBER: RESERVED FOR FUTURE USE
RESPONSIBLE OFFICIAL TITLE: SENIOR VICE PRESIDENT FOR ADMINISTRATION AND FINANCE
RESPONSIBLE OFFICE: ADMINISTRATION AND FINANCE
EFFECTIVE DATE:2/9/2016
SUPERSEDES POLICY DATED: 3/31/2015

I. POLICY STATEMENT

The purpose of this policy is to establish guidelines and a process for the initiation and approval of all forms of credit card payment in accordance with and compliance to Payment Card Industry Data Security Standards (PCI DSS).

University departments may accept credit cards as a form of payment for goods and services provided, after receiving advance written approval from the Merchant Services Manager 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 cards and obtain a physical terminal to either swipe or key transactions through a data capture machine, need to contact the Merchant Services Manager and complete the required paper work to obtain a merchant number (see Attachment A). Any fees associated with the acceptance of the credit cards in each department, will be charged to that department.

Departments wishing to engage in electronic commerce must use a certified PCI DSS compliant payment gateway as indicated on PCI Security Standards.org website (https://www.pcisecuritystandards.org). Requests should be directed to the Merchant Services Manager and Attachment A should be completed and filed with Student Account 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 Data Security Standards (PCI DSS) 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 Data Security Standards related to cardholder data: collecting, processing, transmitting, storing and disposing of cardholder data.

II. ENTITIES AFFECTED

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

III. AUTHORITY

This purpose of this policy is to enforce the Payment Card Industry Data Security Standards and any state or federal laws applying to the acceptance, processing or transmitting of card holder data; the securing of card holder data; or the reporting procedures required in the case of a breach of card holder data.

IV. DEFINITIONS

Cardholder: The individual to whom a credit 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 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 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 DSS: Payment Card Industry Data Security Standards is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI DSS defines a series of requirements and best practices for handling, transmitting and storing sensitive data.

V. RESPONSIBILITIES

Merchant Services Manager
The Merchant Services Manager or designee is responsible for the periodic reviews of departmental procedures and practices in connection with credit card receipt transactions. Results will be reported to Internal Audit. All issues of non-compliance will be reported immediately to the Vice President for Administration and Finance.

Information Technology Infrastructure
Information Technology Infrastructure team is responsible for regularly monitoring and testing the NKU network. Information Technology Infrastructure team will cooperate with the Merchant Services Manager in accordance to 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 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.

Compliance

The Vice President for Administration and Finance and/or the Associate Vice President for Finance will terminate credit 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. COMMITTEE

A committee made up of staff from Human Resources, Internal Audit, Comptroller's Office, Business Auxiliary Services, General Counsel, Information Technology, Purchasing and any other departments deemed necessary by the Merchant Services Manager shall be convened on an ad hoc basis for purposes of addressing issues relating to this policy or any changes required.

VII. PROCEDURES

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 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 disks, floppy disks, USB flash drives, personal digital assistants, 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.

X. TRAINING

The Merchant Services Manager will conduct annual training with all existing merchant departments or any that foresee the need to accept credit cards in the near future. This training typically takes place in June/July of each year.

XII. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

NKU Incident Response Plan

NKU Merchant Application

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
New Policy	2/9/2016

Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	
Choose an item.	