CREDIT CARD PROCESSING AND SECURITY

POLICY NUMBER: ADM-CCARDPROCSEC
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: CHIEF FINANCIAL OFFICER-VICE PRESIDENT FOR ADMIN. & FINANCE
RESPONSIBLE OFFICE: INFORMATION TECHNOLOGY
EFFECTIVE DATE: UPON PRESIDENTIAL APPROVAL – 8/13/2012
MOST RECENT REVIEW: 2/8/2024
NEXT REVIEW DATE: PREVIOUS REVIEW PLUS FOUR (4) YEARS – 2/8/2028
BOARD OF REGENTS REPORTING (CHECK ONE):
☐ PRESIDENTIAL RECOMMENDATION (CONSENT AGENDA/VOTING ITEM)
☒ PRESIDENTIAL REPORT (INFORMATION ONLY)

I. POLICY STATEMENT

The purpose of this policy is to establish guidelines and processes for the initiation and approval of all forms of credit card payment in accordance with and compliance to Payment Card Industry Data Security Standard (PCI DSS). For PCI Standards related to technical specifications, please contact the Northern Kentucky University (NKU) Information Security Governance, Risk and Compliance Team within NKU's Office of Information Technology (NKU OIT).

University departments may accept credit cards as a form of payment for goods and services provided. However, departments must first receive approval from NKU OIT Governance, Risk and Compliance and the Office of the Comptroller in accordance with NKU's Billing, Receipt Handling & Deposits policy, and follow 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 device must contact NKU's Comptroller's Office (859-572-5263) to complete the required paperwork, receive approval, and obtain a merchant number. 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 the PCI Security Standards Council website. Requests should be directed to NKU's Comptroller's Office (859-572-5263) to obtain a merchant number.

The NKU Governance, Risk and Compliance Team (GRC@nku.edu) must be consulted by any department pursuing payment processing to ensure that all University compliance requirements and standards are met.

II. ENTITIES AFFECTED

This policy applies to all NKU faculty, staff, students, organizations, individuals, systems, or devices involved in the processing, transmitting, or storage of cardholder data on behalf of NKU. The scope includes any credit card activities conducted at all NKU campuses and locations.

III. AUTHORITY

The purpose of this policy is to enforce the Payment Card Industry Data Security Standard (PCI DSS) and any state or federal laws applying to the acceptance, processing, or transmitting of cardholder data; the securing of cardholder data; or the reporting procedures required in the case of a breach of cardholder 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).

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 Standard (PCI DSS) 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

NKU Governance, Risk and Compliance Team
The NKU OIT Governance, Risk and Compliance (GRC@nku.edu) Team or designee is responsible for the periodic reviews of departmental procedures and practices in connection with credit card receipt transactions. The periodic reviews will be conducted no less than once annually. Results will be reported to the NKU Internal Audit department. All non-compliance issues will be reported immediately to the Chief Financial Officer and Chief Information Security Officer.

Office of Information Technology (NKU OIT)
NKU OIT will cooperate with NKU's Governance, Risk and Compliance Team in accordance with the University's compliance with PCI DSS technical requirements and will verify the security controls of systems authorized to process credit cards, as detailed in the NKU IT PCI Standards.

Heads of Departments and Activities
Department heads are responsible for documenting departmental procedures and for ensuring that credit card activities comply with this policy. Departments may be held responsible for any fines levied against the University that result from noncompliance by the department.

Compliance
The Vice President of Administration and Finance/Chief Financial Officer 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 Chief Financial Officer.

VI. COMMITTEE

A PCI Council composed of staff from Human Resources, Internal Audit, Comptroller's Office, Business Auxiliary Services, General Counsel, Information Technology, Procurement, and any other departments deemed necessary 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, are protected against unauthorized access.
3. All equipment used to collect data is secured against unauthorized use in accordance with the PCI Data Security Standard (PCI DSS).
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 are stored.
5. Cardholder data are not to be processed, stored, or transmitted using the University's general data or voice networks. Exceptions or alternative solutions will be reviewed by NKU OIT Governance, Risk and Compliance to verify that the technical controls, including firewalls and encryption, are in accordance with the PCI Data Security Standard (PCI DSS). University wi-fi is not secured for the transmission of cardholder data and is expressly forbidden to be used for that purpose.
6. Cardholder data are expressly forbidden to be sent via end-user messaging technologies, such as email, text message, and instant messenger.

7. Databases do not store credit card numbers, 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 are forbidden to 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 are deleted or destroyed before disposal. Paper documents should be cross-cut shredded and destroyed when no longer needed for business or legal reasons in accordance with 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.

VIII. TRAINING

Annual training with existing merchant departments or any that foresee the need to accept credit cards in the near future takes place with NKU's required annual compliance training program. Additional training opportunities will be provided as needed or upon request. Attendance information will be maintained for audit purposes.

IX. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

Billing, Receipt Handling, & Deposits policy

Information Security policy

Information Security Incident Response policy

NKU Merchant Application

Records Management policy

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
Revision	February 8, 2024
Revision	April 14, 2020
Revision	April 5, 2019
Revision	February 9, 2016
Revision	March 31, 2015
New Policy	August 13, 2012

CREDIT CARD PROCESSING AND SECURITY

PRESIDENTIAL APPROVAL

PRESIDENT

Signature Cady Short-Thompson *Date* 2/8/24

Cady Short-Thompson

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☐ This policy was forwarded to the Board of Regents on the ***Presidential Report (information only)***.
Date of Board of Regents meeting at which this policy was reported: _____/_____/_____.

☐ This policy was forwarded to the Board of Regents as a ***Presidential Recommendation (consent agenda/voting item)***.

- ☐ The Board of Regents approved this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing approval of policy.)
- ☐ The Board of Regents rejected this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

SECRETARY TO THE BOARD OF REGENTS

Signature *Date*

Tammy Knochelmann