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 NKU Governance, Risk and Compliance 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 OIT Governance, Risk, and Compliance via email (GRC@nku.edu) to complete the required paperwork (NKU Merchant Application), 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 PCI Security Standards Council website (https://www.pcisecuritystandards.org). Requests should be directed to NKU OIT Governance, Risk and Compliance, and the NKU Merchant Application should be completed and submitted to GRC@nku.edu to obtain a merchant number. At the time of application, departments can discuss the best option for the area.

This policy addresses Payment Card Industry Data Security Standard (PCI DSS) that are contractually imposed by the major card brands on merchants who accept these cards as forms of payments.

II. ENTITIES AFFECTED

This policy applies to all Northern Kentucky University 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**

The NKU OIT Governance, Risk and Compliance (GRC@nku.edu) 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.
Information Technology Infrastructure
The Information Technology Infrastructure team is responsible for regularly monitoring and testing the NKU network. The Information Technology Infrastructure team will cooperate with NKU OIT Governance, Risk and Compliance in accordance to the University's compliance with the PCI DSS technical requirements and 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 by NKU OIT Governance, Risk and Compliance 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 (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 is stored.
5. Cardholder data is not to be processed, stored, or transmitted using the University's general data or voice networks unless NKU OIT Governance, Risk and Compliance has verified 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 is 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 is deleted or destroyed before it is disposed. 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

The NKU OIT Governance, Risk and Compliance team 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. Attendance information will be maintained for record-keeping purposes.

IX. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

Billing, Receipt Handling, & Deposits policy: https://inside.nku.edu/content/dam/policy/docs/Policies/BillingReceiptHandlingandDeposits.pdf


IT Incident Response policy: https://inside.nku.edu/content/dam/policy/docs/Policies/InfoSecurityIncidentResponse.pdf

NKU Merchant Application: https://inside.nku.edu/merchantservices/application.html


REVISION HISTORY

<table>
<thead>
<tr>
<th>REVISION TYPE</th>
<th>MONTH/YEAR APPROVED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision</td>
<td>April 14, 2020</td>
</tr>
<tr>
<td>Revision</td>
<td>April 5, 2019</td>
</tr>
<tr>
<td>Revision</td>
<td>February 9, 2016</td>
</tr>
<tr>
<td>Revision</td>
<td>March 31, 2015</td>
</tr>
<tr>
<td>New Policy</td>
<td>August 13, 2012</td>
</tr>
</tbody>
</table>
# CREDIT CARD PROCESSING AND SECURITY

## PRESIDENTIAL APPROVAL

<table>
<thead>
<tr>
<th>PRESIDENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
</tr>
<tr>
<td>Ashish K. Vaidya</td>
</tr>
</tbody>
</table>

## BOARD OF REGENTS APPROVAL

<table>
<thead>
<tr>
<th>BOARD OF REGENTS (IF FORWARD BY PRESIDENT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ This policy was forwarded to the Board of Regents on the <em>Presidential Report (information only).</em> Date of Board of Regents meeting at which this policy was reported: 5/13/2020.</td>
</tr>
<tr>
<td>☐ This policy was forwarded to the Board of Regents as a <em>Presidential Recommendation (consent agenda/voting item).</em></td>
</tr>
<tr>
<td>☐ The Board of Regents approved this policy on 8/3/2020. (Attach a copy of Board of Regents meeting minutes showing approval of policy.)</td>
</tr>
<tr>
<td>☐ The Board of Regents rejected this policy on 8/3/2020. (Attach a copy of Board of Regents meeting minutes showing rejection of policy.)</td>
</tr>
</tbody>
</table>

## VICE PRESIDENT AND CHIEF STRATEGY OFFICER

| Signature | Date 8/3/2020 |
|-----------|
| Bonita Brown |
| Bonita J. Brown |