Central Connecticut State University

CCSU Procedures for In-Person Credit Card Transactions

Revision Date: 12/19/16	Effective Date: Spring 2017
Approved by: CFO and CIO	Approved on date: December 2016

Policy Statement

It is necessary for some departments to accept credit cards as part of their responsibilities. Whenever possible the credit cards should be processed via the University's online payment portals. These procedures do not apply if the payments are made online by the Payer (card holder or account owner) through the University's contracted eCommerce vendor, currently Nelnet's Commerce Manager, and the eCommerce vendor processes the transaction through to the University's financial institution with no intermediary handling of funds by the university.

To obtain an online payment portal for eCommerce that accepts both credit cards and eChecks, submit the following information by email to the Bursar:

1. Department name
2. Contact name / phone / email
3. Function / purpose
4. Existing website
5. Banner Index
6. Names of users in the Department
7. Miscellaneous data fields needed (for example, university affiliation, t-shirt size, hotel, etc.)

When this is not feasible credit cards may be accepted in person, provided approval has been granted by the Chief Financial Officer and Chief Information Officer. In order to meet Payment Card Industry Data Security Standards (PCI-DSS) departments that accept credit cards in person shall adhere to the standards and procedures outlined in this policy.

Definitions

1. **Credit Card Processing Equipment** – This includes the credit card terminal as well as the cellular modem used to connect the terminal to the internet.

2. **Cellular Modem** – A device that allows equipment to be connected to the internet via a cellular network.

Roles, Responsibilities and Standards

1. **Approval to Accept Credit Cards in Person:**
   No department may start accepting credit cards without prior approval of the Chief Financial

Officer and Chief Information Officer or their designee. Individuals with access to process credit card payments must read and sign the PCI Compliance Statement Form. An original (or copy) of the signed form must be sent to the Chief Financial Officer.

2. **Approved Department List:**
   The Chief Financial Officer or designee shall keep a list of all departments that have been approved to accept credit cards.

3. **Approved Credit Card Processing Equipment List:**
   The Chief Information Officer or designee shall keep a list of approved credit card processing equipment. This list will include the manufacture and model of the equipment. The equipment on this list will meet all PCI-DSS requirements. If a department needs to replace equipment, the supervisor needs to contact the Director of Technical Services to get the appropriate replacement equipment.

4. **Purchasing Credit Card Processing Equipment:**
   Only the CIO or designee shall purchase credit card processing equipment.

5. **Deployed Credit Card Processing Vehicles:**
   The Chief Information Officer or designee shall keep a list of approved credit card processing hardware and software. For hardware, this list will include the manufacture, model, locations, and serial number or other unique identifier of the equipment. For software, this list will include the vendor, contact information, software version, and installation locations.

6. **Configuration of Credit Card Processing Equipment and Software:**
   All credit card process equipment shall be configured by the vendor. University personnel shall not make any changes to the equipment, except for members of the Information Technology department at the direction of the vendor.

7. **Authorized Employees:**
   Each department that accepts credit cards in person shall keep a list of employees who are authorized to use and have access to the credit card processing equipment and software. This list shall be reviewed by the department annually for accuracy and submitted to the Chief Financial Officer annually on or before June 30th each year.

General Requirements

1. **Credit Card Processing Requirements:**
   Credit cards cannot be accepted over the phone. The card must either be present to perform the transaction or the transaction must be performed through approved online channels only by the cardholder.

2. **Credit Card Security:**
   Card numbers shall not be written down to be processed at a later time or date. Additionally,

employees shall not ask card holders for the card's personal identification number (PIN).

3. **Credit Card Processing Equipment Security:**
When not in use, the credit card processing equipment shall be kept in a secured location such as a locked drawer or cabinet. Only authorized employees shall have access to the secured location. Lost or stolen equipment shall be reported within 24 hours of identification of missing item to the police department, Chief Financial Officer and Chief Information Officer or designees.

4. **Network Connections:**
Credit card processing terminal shall only be connected to the cellular modem it was deployed with. Under no circumstances should the terminal be connected to the University's network. Under no circumstances should any equipment other than the processing terminal be connected to the cellular modem.

5. **Procedure Documentation:**
Each department that accepts credit cards must have documented procedures on the processing of the credit cards and be annually reviewed. An up-todate copy of these procedures will be submitted to the Chief Financial Officer or designee on an annual basis by June 30th.

6. **Employee Training:**
Authorized employees must be trained in the department's documented procedures on how to process credit cards.

7. **Enforcement:**
The Chief Information Officer, Chief Financial Officer, or their designee may revoke a department's permission to accept credit cards for policy or procedure violations. Additionally, payment card industry violations can results in fines. These fines will be charged back to the offending Department. For more information on PCI Security Standards, please visit https://www.pcisecuritystandards.org

Related Regulations, Policies & Procedures, and Forms

Official PCI Security Standards Council Site	https://www.pcisecuritystandards.org/
BOR Draft Standard STND-004	Payment Application, Point of Sale Security
Compliance Statement Form	CCSU Payment Card Industry (PCI) Compliance Statement Form