10.11 Use and Security Acceptance of Credit Card Numbers/Cardholder Data

Purpose

To ensure that The University of Northern Iowa acknowledges its obligation to provide appropriate security for processing of credit card payments and cardholder data in its domain of ownership and control. Furthermore, the University recognizes its responsibility to remain compliant with all state and federal laws and regulations on the acceptance of credit cards as a form of payment. Also, Moreover, the University recognizes its responsibility to comply with the Payment Card Industry Data Security Standard (PCI DSS) requirements issued by the Payment Card Industry Security Standards Council. (PCI Council).

Scope

This policy applies to all faculty, staff, and students as well as any other individuals or entities who process credit cards as a form of payment at the University of Northern Iowa. This policy applies to all cardholder data, even if stored without the use of an IT resource. Further, this policy applies to all IT resources that store, process, or transmit cardholder data. Securing and protecting cardholder data from misuse or malicious activity and maintaining compliance with the PCI DSS is the responsibility of those who manage systems as well as those who use them. Effective security is a team effort involving the participation and support of every member of the University community who accesses and uses cardholder data.

This policy is not applicable to university procurement cards issued to University of Northern Iowa (UNI) employees and administered by the Office of Business Operations (OBO).

Definitions

Availability - A loss of availability is the disruption of access to or use of information or an information system.
1. Confidentiality - A loss of confidentiality is the unauthorized disclosure of information.
   Integrity - A loss of integrity is the unauthorized modification or destruction of information.
2. Cardholder data - Confidential or identifying information found on a credit card, such as cardholder name, primary account number, expiration date, service code, and any validation codes (CVV/CVC).
3. “Unit” or “units” - The term “unit” or “units” shall refer to UNI departments, schools, programs, activities, or offices.

Policy Statement

UNI is committed to ensuring the privacy and proper handling of cardholder data that it collects and maintains from students, faculty, staff, patrons, and other individuals conducting business with the University. Faculty, staff, students, or anyone else accessing cardholder data must protect the data from
a loss of availability, confidentiality, or integrity. Units wishing to process credit cards for payment must
be approved by OBO prior to accepting credit cards for payment and use approved methods for
handling cardholder data. All systems, electronic or paper-based, processing credit card payments must
be secured sufficiently to protect the availability, confidentiality, and integrity of the cardholder data.

Whereas the confidentiality of cardholder data is of chief importance, measures necessary to protect
the confidentiality of cardholder data are superior to the availability of credit card payment systems.

Units not complying with this policy may lose the privilege to process credit card payments and may be
responsible for any losses, including costs of fines and remediation imposed by the PCI Council and/or
UNI’s acquiring bank, occurring due to their action or inaction. Individuals who knowingly violate this
policy and/or in any way compromise the availability, confidentiality or integrity of cardholder data may
be subject to appropriate disciplinary action and/or sanctions.

As required by the PCI DSS, the University shall maintain and follow a comprehensive set of policies,
procedures, and guidelines for the processing of credit card payments. These documents shall
be updated regularly as advances in technology and changes to the PCI DSS occur, as well as having the
full force and effect of this policy.

**Procedures**

**Office of Business Operations Responsibilities**

OBO shall be primarily responsible for the enforcement of this policy and will maintain a collection of
cardholder data-related policies and procedures, and standards.

In accordance with PCI DSS, OBO shall establish several required committees of relevant University
personnel, including individuals designated by the Chief Information Officer (CIO). These committees will
review and approve required policies and procedures, conduct an assessment of compliance with this
policy, verify compliance with the PCI DSS, conduct official reviews pertaining to PCI DSS, maintain
appropriate segregation of duties, and assign responsibility for the operations of UNI’s credit card
payment processes. Each committee shall be required to meet annually and as needed, and annually at
a minimum.

OBO shall provide training annually and as needed, and annually at a minimum, to comply with the PCI
DSS. OBO shall maintain a list of covered units or individuals.

In the event of non-compliance with this policy, OBO shall have the authority to revoke the privilege of
any unit or individual to process credit card payments until an official review is conducted as required by
PCI DSS and OBO has determined acceptable operating procedures have been established in the unit.

**Information Technology Services Responsibilities**

The CIO shall designate individuals to administer, monitor, secure, and maintain information systems
needed for the processing of cardholder data; these individuals are considered to have access to
cardholder data. The responsibilities of Information Technology personnel include performing ongoing
information risk assessments and audits to ensure that information systems meet PCI DSS requirements.

The CIO and designated staff shall have the authority to select the technological solutions used by UNI to meet the PCI DSS. As required by PCI DSS, in the event that the availability, confidentiality, or integrity of the cardholder data is in question, the CIO or staff designated designee shall have the authority to remove the ability of any unit or individual to process credit card payments until an official review is conducted or the threat to the availability, confidentiality, or integrity of cardholder data has been remediated.

**Covered Units - Responsibilities**

All units accepting credit cards as a form of payment in any manner, including staff with access to cardholder data, must adhere to this policy. Individuals responsible for the units covered by this policy are responsible for assuring their unit’s compliance with the policy. Units covered by this policy must:

1. Consult with OBO on the acceptance or utilization of credit cards.
2. Accept credit cards only with approval from OBO.
3. Never store cardholder data on University computers or electronic systems at any time.
4. Receive instruction and approval from OBO to store cardholder data on paper-based records.
5. Utilize information systems approved by OBO to process credit card payments.
6. Follow all policies, procedures, and guidelines provided by OBO for credit card operations; refer to OBO web page for additional information.
7. Utilize IT resources approved by OBO to process credit card payments.
8. Purchase required equipment and supplies for credit card payments with the assistance of OBO.
9. Receive instruction and approval from OBO to store cardholder data on paper-based records.
10. Never store cardholder data on University IT resources at any time.
11. Purchase required equipment and supplies for credit card payments with the assistance of OBO.
12. Follow all policies, procedures, and guidelines provided by OBO for credit card operations; refer to OBO web page for additional information.
13. Utilize IT resources approved by OBO to process credit card payments.
14. Purchase required equipment and supplies for credit card payments with the assistance of OBO.
15. Receive instruction and approval from OBO to store cardholder data on paper-based records.
16. Never store cardholder data on University IT resources at any time.
17. Purchase required equipment and supplies for credit card payments with the assistance of OBO.
18. Receive instruction and approval from OBO to store cardholder data on paper-based records.
19. Never store cardholder data on University IT resources at any time.
20. Follow all policies, procedures, and guidelines provided by OBO for credit card operations; refer to OBO web page for additional information.
21. Utilize IT resources approved by OBO to process credit card payments.
22. Purchase required equipment and supplies for credit card payments with the assistance of OBO.
23. Receive instruction and approval from OBO to store cardholder data on paper-based records.
24. Never store cardholder data on University IT resources at any time.
25. Purchase required equipment and supplies for credit card payments with the assistance of OBO.
26. Receive instruction and approval from OBO to store cardholder data on paper-based records.
27. Never store cardholder data on University IT resources at any time.

**Usage of Terms**

**ACQUIRING BANK** – An acquiring bank is the bank or financial institution which processes credit or debit card payments on behalf of a merchant.
AVAILABILITY – Availability is the ability to assure that systems work promptly and service is not denied to authorized users. A loss of availability is the disruption of access to or use of information or an information system.

CONFIDENTIALITY – Confidentiality ensures that confidential information is only disclosed to authorized individuals. A loss of confidentiality, for the purposes of this policy, is the unauthorized disclosure of information.

CARDHOLDER DATA – Confidential or identifying information found on a credit (or debit) card, such as cardholder name, primary account number, expiration date, service code, and any validation codes (CVV/CVC).

INTEGRITY – Integrity is the appropriate maintenance of information and systems. A loss of integrity is the unauthorized modification or destruction of information.

3. being followed.

IT RESOURCE – IT resource may include computers, software, servers, network utilization, storage utilization, virtual machine capacity, tablets, phones, multimedia devices, storage devices, wireless spectrum, and any other in-demand resource managed by IT staff.

UNIT or UNITS – The term “unit” or “units” shall refer to UNI departments, schools, programs, activities, or offices.

Office of Business Operations, Information Technology Services, and the Senior Vice President for Administration and Financial Services, Finance & Operations, University Council, approved June 2012

President’s Cabinet, President and Executive Management Team, approved July 9, 2012.