UNIVERSITY of NORTHERN COLORADO

PCI DSS 3.1 Policy for Point of Sale Managers at UNC Template

Purpose

This document defines the University of Northern Colorado's policy regarding PCI DSS 3.1 for POS Managers in <INSERT NAME OF DEPARTMENT/BUSINESS/ORG> at UNC. This document applies to any persons managing an environment which transacts business by receiving or processing credit card information.

Applies To

This Guideline applies to all students, faculty, staff, or third parties that manage a POS system or a PCI environment at UNC.

Definitions

PCI – Payment Card Industry
DSS – Data Security Standard
POS – Point of Sale
PCI Environment – Any system, computer, or physical area that supports, interacts with, or is physically located in an area that is in contact with credit cards or credit card numbers.
CHD – Card Holder Data

Guidelines

POS Managers shall do the following:

1. When implementing any new technology regarding credit cards you must contact the IM&T team to inform them of the impact to current PCI DSS compliance.
2. When implementing any new process regarding credit cards you must contact the IM&T Office of Information Security with an update regarding the change in process.
3. When implementing any new policy regarding credit cards you must contact the IM&T Office of Information Security with an update regarding the change in policy.
4. As the manager of the POS it is your responsibility to do the following:
    a. Ensure you understand (in concert with IM&T) your responsibilities regarding the POS including the following:
        i. Management of the encryption keys, if applicable

ii. Management of the secure deletion of card holder data

iii. Management of the relationship with your vendor

iv. Coordination of POS updates

v. Management of retention of card holder data

b. Ensure that all the POS roles are appropriate for the users they are assigned to.

c. Maintain the POS roles and users by giving the minimum permissions needed to complete the assigned tasks.

d. Maintain the POS roles and users by removing roles and users as needed.

e. Ensure that employees are not writing down credit card numbers unless it is covered in a specific process and is PCI DSS compliant.

f. Ensure that any card holder data that is on paper is secure at all times.

g. Write a procedure for the handling of all written card holder data.

h. Enforce the password rules for PCI DSS compliance for your POS as follows:

i. Password must be changed every 90 days

ii. At minimum passwords should be at least 7 characters long

iii. All passwords must at least as complex as containing both alpha and numeric characters

iv. All individuals must submit a new password that is different than the last four used

v. Repeated access attempts should result in the lockout of the account after 6 attempts

vi. Once an account is locked out there must be a minimum of 30 minutes wait time or the account can be unlocked by an administrator

i. The POS should require authentication after 15 minutes without use.

j. Ensure that any access to the credit card database is authenticated.

k. Ensure that access to your facility is adequately controlled.

l. Ensure that your employees and authorized persons can be clearly distinguished visually from non-employees and non-authorized persons.

m. Physically secure all card holder data.

n. Track all access to card holder data.

o. Ensure that card holder data is destroyed at the end of its defined retention period

p. Define what your data retention policy is.

q. Define what your data disposal policy and process are.

r. Do not circumvent data protection measures

Revision History

Version	Published	Author	Description
1.0	2014/06/20	Matt Langford	Original publication.
1.1	2015/06/22	Matt Langford	Minor Updates