UNIVERSITY of NORTHERN COLORADO

PCI DSS 3.1 Policy for Data Disposal at UNC Template

Purpose

This document defines the University of Northern Colorado's policy regarding PCI DSS 3.1 retention of card holder data for<INSERT NAME OF DEPARTMENT/BUSINESS/ORG> at UNC.

Applies To

This Guideline applies to all students, faculty, staff, or third parties that work in 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

I. The duration of card holder data retention is as follows:

1. Card holder data can be stored for a period no longer than <This is in regards to storing the full card number, the retention period should only be as long as absolutely necessary. If you retain ANY form of cred card numbers I recommend a retention of no longer than 90 days (30 days or less is best) and you must justify why you need to retain it that long. If you never retain any sort of card holder data please replace this with (Card holder data is not stored by <INSERT NAME OF DEPARTMENT/BUSINESS/ORG> at UNC)>
2. Card data is stored for the following business reason(s):
<This should be your business reason for retaining card holder data. If you do not store card holder data you may remove #2>

II. The card holder data will be secured as follows:

1. Card holder data is secured encrypted by the PA-DSS certified application, if applicable.
2. Physical card holder data is stored securely, if applicable.

3. Card holder data is destroyed after the defined retention period.

III. UNC does not store Sensitive Authentication Data

IV. Users and managers with elevated privileges which allow access to card holder data via computer must comply with the following:

1. All users must have a unique ID.
2. In addition to a unique ID you must have a second form of authentication, such as a password, passphrase, token, smart card, or biometric scanner.
3. Passwords must be changed every 90 days.
4. Passwords must conform to the UNC password policy.
5. Individuals must submit a new password that is different from the last four passwords.
6. The account must lock out after 6 failed attempts and.
7. The account must lock out for a minimum of 30 minutes or until reset by an administrator.
8. A session that has been idle for 15 minutes must require users to reauthorize.
9. All access to any database containing card holder data is authorized.

V. Access to secure areas where card holder data are stored must be restricted to authorized personnel only.

1. Only persons with a business need should have access to areas where card holder data are stored.
2. Personnel need to be able to be physically distinguished from those who do not have access. (Uniforms, badges, etc.)
3. A log needs to be kept regarding access to the secure areas where card holder data is kept.

VI. An accurate record must be kept regarding the possession of all card holder data.

1. The possession of card holder data must be logged and the responsible party must sign for the data.
2. Placement of card holder data into a secure location must be logged and the responsible party must sign in the data.
3. Removal of card holder data from a secure location must be logged and the responsible party must sign out the data.
4. Secure transport of the card holder data must be logged.
5. Delivery of the card holder data must be logged.
6. Destruction of card holder data must be logged.

UNIVERSITY of NORTHERN COLORADO

Revision History

Version	Published	Author	Description
1.0	2014/06/18	Matt Langford	Original publication.
1.1	2015/06/22	Matt Langford	Minor Updates