UNIVERSITY of NORTHERN COLORADO

PCI DSS 3.1 Policy for Mobile Point of Sale Users at UNC

Purpose

This document defines the University of Northern Colorado's policy regarding PCI DSS 3.1 for Mobile point of sale (POS) Users at UNC.

Applies To

This document applies to any persons operating in an environment which receives or processes credit card information via a mobile POS device.

Definitions

Point of Sale (POS) Device - any device that is used to process a credit card.

Mobile POS Device - any device that is used to process a credit card that is capable of being used in multiple locations and that is not connected directly via phone line or direct network connection. This includes devices that use wireless, cell or network not present transactional modes.

PCI DSS - Payment Card Industry Data Security Standards.

PCI PA-DSS - Payment Card Industry Payment Application Data Security Standards.

PCI Compliant 3rd Party Vendor - A 3rd party vendor for payment card processing which has provided the University proof that it is compliant with PCI PA-DSS or DSS as needed.

PCI Compliant Network - A PCI compliant network means that the network conforms to best practices and any and all standards set by PCI.

PCI DSS 3.1 POS Policy

The University does not solicit credit card numbers via insecure methods.

- UNC does not ask for credit card numbers to be sent via the mail
- UNC does not ask for credit card numbers to be sent over email

The University does not create any non-secure copy of credit card numbers including but not limited to: text files, unencrypted database entries, paper copies, email, instant messaging, text messaging, etc.

The University destroys any copy of credit card data that it receives unsolicited in these formats by crosscutting (or pulping) hardcopy and secure deleting electronic copies.

The University does not store any credit card data and all third party processors are PCI PA-DSS and/or DSS compliant. All third party applications implemented as per the instructions given by the PCI PA-DSS compliant third party vendor.

All UNC PCI environments are segmented into their own PCI compliant network.

All UNC staff, faculty or students working in a PCI environment are given, at minimum, yearly training on PCI compliance and their specific responsibilities as it relates to PCI compliance and good security practice.

PCI DSS 3.1 Policy for Mobile Points of Sale

The responsibility of a Mobile POS User for the University is as follows:

- The User has read and understands the PCI DSS 3.1 POS Policy.
- The User has read and understands Article 9 of the University Regulations.
- The User has received PCI training within the last year.
- The User has received training on the use of the device and understands how to operate it in a safe and secure manner.

Revision History

Version	Published	Author	Description
1.0	2014/06/20	Matt Langford	Original publication.
1.1	2015/03/16	Matt Langford	Format and content update
1.2	2015/05/27	Matt Langford	Adjusted for DSS 3.1