UNIVERSITY OF NORTHERN COLORADO

PCI DSS 3.1 Point of Sale Physical Terminal Policy

Purpose

This policy outlines the University of Northern Colorado’s policy regarding PCI DSS 3.1 Point of Sale terminals.

Applies To

This applies to all Point of Sale terminals but does not include web based points of sale nor credit card swipe machines. All persons working for or on behalf of the University of Northern Colorado which participate at any level in the processing of credit card data through a Point of Sale.

Acronyms

POS – Point of Sale
PCI DSS 3.1 – Payment Card Industry Data Security Standard version 3.1
CDE – Cardholder Data Environment
CHD – Cardholder Data
SAD – Sensitive Authentication Data
PAN – Personal Account Number
TSC – Technical Support Center
PA-DSS – Payment Application Data Security Standard

Definitions

Point of Sale – A device which transacts a credit card sale.
Cardholder Data Environment – The environment in which cardholder data is processed or stored. This includes both electronic space such as a computer network as well as physical space (including where the network hardware is stored).
Cardholder Data – Data associated with the card, name, PAN, address, etc.
Sensitive Authentication Data – Full track data, track two or three data, PIN data, CVV, CV2, etc.
Personal Account Number – The credit card number
PCI Compliance Officer – The CISO for UNC
Technical Support Center – email: help@unco.edu or phone 970-351-4357 or 800-545-2331

Policy

- All persons working in a CDE will receive annual PCI DSS compliance training.
- All persons working in a CDE will contribute to the security of the CDE by taking the following steps:
    - Wearing an identifying uniform or displaying a token which visibly marks them as authorized to be in the physical environment
    - Challenging any individual in the CDE that is not displaying the identifying uniform or token
    - Be familiar with the work area and equipment
    - Regularly inspect the terminals, network connections, network cables, and areas for suspicious devices or tampering
    - Immediately report any suspicious devices or persons to your supervisor, UNC PD, or to the Office of Information Security (through the TSC), as the situation dictates.
- Do not make any copy of credit card data
- Follow the written procedure for transacting a sale through your POS
- Use the POS only as described by the Payment Application developer
- Report your suspicion of any default user accounts or passwords to your supervisor
- Report any alteration to the CDE that could potentially alter its security to your supervisor
- The POS will have access to only the resources it needs to conduct business
- The POS will be regularly updated, scanned, and patched
- The POS user will have permissions appropriate to their role
- The POS will have unique IDs for each user
- Implement the POS using PCI DSS best practices and following the Payment Applications PCI PA-DSS implementation guide.
- Do not solicit credit card data through insecure methods
- Be familiar with UNC Security Policy including the following:
    - Article 9 – The Information Technology Security Plan
    - UNC’s current PCI DSS policy located on www.unco.edu/it under policies

Revision History

Version	Published	Author	Description
1.0	2015/08/13	Matt Langford	New for PCI DSS 3.1
1.1	2015/09/09	Matt Langford	Minor updates