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 –

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