

Policy for PCI Compliant Network Devices

Purpose

This policy outlines how all PCI DSS environments need to connect to the university network.

Applies To

This Policy applies to all PCI environments with devices connected to the network.

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 terminal that allows for credit card transactions.

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

UNIVERSITY OF NORTHERN COLORADO

Policy

All PCI environments and devices at the University of Northern Colorado must connect to a PCI DSS compliant network. Analog connections are no longer considered compliant. All current analog connected devices must be converted to digital before December 15th 2015.

Revision History

Version	Published	Author	Description
1.0	2015/10/08	Matt Langford	Original publication.