PCI DSS 3.1 Data Manager Guidance

Purpose

This document details the type of knowledge, data, and environment that a PCI DSS 3.1 Data Manager would be expected to understand and provide.

Applies To

This applies to all persons who manage the data coming into or out of the Cardholder Data Environment. All persons working for or on behalf of the University of Northern Colorado which participate in managing data coming into or out of the Cardholder Data Environment.

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 –

into a POS or credit card terminal. The customer should either be present or giving authorization over the phone.

Responsibility for transporting, storing and processing

It is your responsibility to understand how credit card data must be stored, processed or transported. If, for example, you are still receiving CHD via mail because a customer is not aware of a change in how we solicit that information you must understand, secure and document the entire process that surrounds the reception, storage and transport of that data. In this situation we are required to place that mail into a secure storage container owner or Data Manager and IM&T. The CDE must be maintained and managed so that systems cannot be moved or removed without informing all parties. This means that all changes must be reported including replacement of computers, terminals, any device which is plugged into a network jack, etc.

POS devices should ONLY be used for transactions

POS devices cannot be used to conduct any other form of business. Any unnecessary connectivity not only introduces risks from external systems but additionally creates connections to our primary network. This could mean that large portions of the UNC network could then fall under PCI DSS compliance rules. This means that POS systems should have no internet access, they shouldn’t connect to any shares on the network, or get email. They should only be connected to systems essential for business.

POS updated and scanned

Data Managers should be aware of what operating systems they are running, how they are getting updates, if they have anti-virus/malware running, and get confirmation that they are being tracked in a compliant manner by the IM&T team. The Data Manager should understand and inform themselves when their software needs a version upgrade or patching.

POS best practices

You should be aware of PCI DSS best practices which is included in the annual training. Data Managers should know what their 3rd party payment application vendor recomis 1.(n)19( )-10(t)-22(h)19u822(3