UNIVERSITY OF
NORTHERN COLORADO

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 – 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

Guidance

If your policy does not match this guidance document an exception will need to be provided to the PCI Compliance Officer. This exception must describe why any alteration to the guidance needed to occur, what is done to mitigate any resulting security risk or compliance failure, and the plan to address that exception going forward.

Training
Every year beginning in August and ending in September the IM&T department will issue at least two annual PCI DSS training sessions for users and managers. This will cover any changes from the previous standard and covers information that all personnel operating in a PCI environment are expected to know. If your department transacts credit card payments you are required to receive PCI DSS training on at least an annual basis. All departments are free to seek alternate training but should document when the training took place, who presented the training, and who all attended. This information will be needed by the PCI Compliance Officer for their annual audit.

Securing the CDE
All Cardholder Data Environments must be secured. This means locking the area when not in use and/or securing the computers, terminals, printers, and peripheral devices when they are not in use. All CDEs must implement some program which visually identifies persons who are permitted to operate within the CDE. This can take the form of a uniform, a badge that or other physical token which must be worn at all times while in the CDE. Visitors who are authorized but do not directly report to the CDE management should also be identified in some visual manner such as a recognizable token that they must display at all times. This token must be different than the one belonging to "regular" CDE operators. The physical security policies should be documented and reviewed annually. Your policy should outline what measures you take to identify authorized personnel and guests as well as what to do when an unauthorized individual or equipment is detected in the CDE.

Inspecting equipment and reporting
A regular inspection of all CDE equipment should be performed by both the Data Manager and employees. Instructions specific to your equipment inspection should be easily available to you and your employees. A clear reporting path should be laid out in case a suspicious device or tampering is discovered. We suggest that any suspicious computer or network device is first reported to management and then to the TSC to be routed to the IM&T Security Team.

We do not copy credit card data
It is UNC's policy that at no time do we copy in any way any credit card data. If the current process includes this activity it must be immediately remediated. Acceptable alternatives include directly inputting customer information into a web POS interface or entering the data directly

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 as it arrives. That storage area must be secure and only authorized persons should be able to access it. All access must be documented and periodically reviewed. When the mail is retrieved you must document who took possession and how it was secured for transport. When it arrives for processing the processor must document their reception of that information. The form must be secure until it is processed and then it should be destroyed in a PCI DSS compliant manner. This process must be recorded and documented. Paper must be cross-cut shredded, pulped, or incinerated.

A few security details about what secure storage and destruction looks like
A safe is acceptable as is a locked drawer in a locked office so long as the office and drawer are locked at all times that the office is not occupied. It is our responsibility to securely destroy all PCI DSS sensitive documents which would require, at minimum, the use of a cross cut shredder. All process documentation should be made available on request to the PCI DSS auditor either internal or external.

Procedure for using the POS or processing credit card transactions
This should be a step by step document that describes your process for receiving and processing credit card transactions either through the terminal or whichever process your business system uses. This procedure should focus on the standard everyday operation but should include any contingency process if there is a terminal or processing failure. You should reference the payment application's documentation to ensure you are using it in a PCI DSS compliant manner.

The CDE belongs to the business owner
Remember that the CDE is ultimately the responsibility of the business owner or department manager. Your technical support team has experience in PCI DSS compliant networking and implementation but day to day use and management must be owned by the functional area director or Data Manager. This includes the definition of the roles within the application as well as the addition, removal and change of any employees. The Data Manager must understand when the environment is not configured in a PCI DSS compliant manner and understand what the requirements are for compliant passwords and changing default passwords.

Changes to the environment
Data Managers need to be aware of any changes to the CDE and that all such changes need to be communicated to all stake holders. In the UNC environment that typically includes the business

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 recommends in their best practices documentation.

Do not solicit credit card data through insecure methods
You must not solicit (or transmit) credit card data through insecure communication channels. These include insecure web interfaces, email, IM or texts or other communication channels that are not explicitly required by the payment application. You should not solicit mail in paper forms from your customers. This is insecure and places UNC at high risk. While traversing the USPS it is generally trusted but once those forms hit the UNC internal mail system they enter an insecure environment. In addition this forces the receiving department to take so many extra measures to ensure the safety of the form that we are better off asking for another method of payment. See the section above titled: Responsibility for transporting, storing and processing

Managing encryption keys
Data Managers will need to understand the impact that changing encryption keys has on their environment, how their application works, and how they want to manage their encryption keys. IM&T will partner with Data Managers to help you understand encryption key crypto periods, acceptable cyphers, split control, key management, retirement and rotation.

Data Retention Policy

UNC is working on some guidelines that delve deep into this topic but at a high level this includes defining how long you are required to retain data. IM&T highly recommends that we choose less than 30 days for retention for any CHD. The longer the period the more enticing that data store is for bad actors and the worse the breech would be if it did happen. The Data Manager is responsible for setting their policy regarding retention and should outline the duration, reason, and method of data destruction. This policy should also include how you are going to dispose of any hardware. That plan should discuss how any equipment will be cleansed or destroyed.

Reporting suspected or known breeches
Incidents should be reported immediately to the Office of Information Security through the TSC. Enough detail should be provided so that we can engage the right teams but additional details should be reserved for the Computer Incident Response Team Manager. It is essential to control information at that critical point so that an investigation can be pursued if needed.

Documentation review
Documentation must be reviewed annually. These reviews must be documented. We recommend a revision history similar to the one at the end of this document.

Maintain a security conscious environment
Encourage people who work in a CDE to keep up to date on credit card scams and good security practices. IM&T has a cybersecurity module in Skill Soft and hosts a number of awareness events every year as well as security related CETL sessions and technical talks.

Revision History

Version	Published	Author	Description
1.0	2015/08/01	Matt Langford	New for PCI DSS 3.1
1.1	2015/08/13	Matt Langford	Included links to policy items
1.2	2015/09/03	Matt Langford	Language clarification
1.3	2015/09/09	Matt Langford	Language clarification