PCI DSS 3.1 Security Policy

Purpose

This document outlines all of the policy items required by PCI to be compliant with the current PCI DSS 3.1 standard and that it is the University of Northern Colorado's Policy to be compliant with all requirements set forth below.

Applies To

This Policy applies to all PCI environments within the University of Northern Colorado and to all staff, faculty, and students that operate within or in cooperation with a PCI environment.

Definitions

CDE – Cardholder data environment

DSS – Data Security Standards

PA-DSS – Payment Application Data Security Standards

PCI – Payment Card Industry

PAN – Primary Account Number

SAD – Sensitive Authentication Data, includes Full Track Data, PIN/PIN Block, CAV2/CVC2/CVV2/CID

Cardholder Data – PAN, Cardholder Name, Service Code, Expiration Date

Policy

UNC commits to the following actions in regard to each section of PCI-DSS version 3.1:

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

1.1

a. A formal process exists for approving and testing all external network connections and changes to the firewall and router configurations.
b. UNC will, at all times, maintain a current network diagram for PCI environments.
c. Configuration standards include requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.
d. The current network diagram is consistent with the firewall configuration standards.
e. Firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.
f. Firewall and router configuration standards include a documented list of services, protocols and ports necessary for business (for example, hypertext transfer protocol (HTTP), Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols).
g. All allowed insecure services, protocols, and ports necessary, and are security features documented and implemented for each.
h. Firewall and router configuration standards require a review at least every six months.
i. Firewall and router rule sets reviewed at least every six months.
j. Maintain a current network PCI network diagram for each of the PCI environments.
k. Maintain a current dataflow diagram for PCI environments.

1.2

a. Inbound and outbound traffic is restricted to that which is necessary for the cardholder data environment, and the restrictions are documented.
b. All other inbound and outbound traffic specifically denied.
c. Router configuration files are secure and synchronized.
d. Perimeter firewalls are installed between any wireless networks and the cardholder data environment, and are these firewalls configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

1.3

a. Direct connections are prohibited for inbound or outbound traffic between the Internet and the cardholder data environment.
b. Internal addresses are prohibited from passing from the Inte

Information

Information

c. Policies and procedures include coverage for all storage of cardholder data.
d. Processes and procedures include:
A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy.
Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy.
e. All stored cardholder data meets the requirements defined in the data retention policy.

3.2

a. When sensitive authentication data is received and deleted, processes in place to securely delete the data to verify that the data is unrecoverable. The university does not store SAD.
b. The full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance.
c. The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance.
d. The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance.

3.3

a. The PAN is masked when displayed (the first six and last four digits are the maximum number of digits to be displayed).

3.4

a. PAN is rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit logs), by using any of the following approaches:
• One-way hashes based on strong cryptography (hash must be of the entire PAN)
• Truncation (hashing cannot be used to replace the truncated segment of PAN)
• Index tokens and pads (pads must be securely stored)
• Strong cryptography with associated key management processes and procedures.
b. Logical access to encrypted file systems is managed independently of native operating system access control mechanisms.
c. Cryptographic keys stored securely.
d. Cardholder data on removable media is encrypted wherever stored.

3.5

a. Access to cryptographic keys are restricted to the fewest number of custodians necessary.
b. Keys are stored in encrypted format and are key-encrypting keys stored separately from data-encrypting keys.
c. Cryptographic keys are stored in the fewest possible locations and forms.

3.6

a. Cryptographic key procedures include the generation of strong cryptographic keys.
b. Cryptographic key procedures include secure cryptographic key distribution.
c. Cryptographic key procedures include secure cryptographic ke

e. For SSL/TLS implementations:
HTTPS appears as part of the browser Universal Record Locator.
Cardholder data is required only when HTTPS appears in the URL.

f. Industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment.

4.2

a. PANs are rendered unreadable or secured with strong cryptography whenever they are sent via end-user messaging technologies (for example, e-mail, instant messaging, or chat).

b. Policies are in place that state that unprotected PANs are not to be sent via end-user messaging technologies.

Requirement 5: Protect

- Installing a web-application layer firewall in front of publi

8.2

a. In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users:
Something you know, such as a password or passphrase.
Something you have, such as a token device or smart card.
Placing servers containing cardholder data behind proxy servers/firewalls or content caches.
Something you are, such as a biometric.

8.3

a. Two-factor authentication is incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.

8.4

a. All passwords are rendered unreadable during transmission and storage on all system components using strong cryptography.

8.5

a. Proper user identification and authentication management controls are in place for non-consumer users and administrators on all system components, as follows:
Additions, deletions, and modifications of user IDs, credentials, and other identifier objects controlled, such that user IDs are implemented only as authorized (including with specified privileges).
User identity is verified before performing password resets for user requests made via a non-face-to-face method (for example, phone, e-mail, or web).
First-time and reset passwords will set to a unique value for each user, and each user must change their password immediately after the first use.
Access for any terminated users is immediately deactivated or removed.
Inactive user accounts over 90 days old will either be removed or disabled.
Accounts used by vendors for remote access, maintenance or support is enabled only during the time period needed.
Vendor remote access accounts is monitored when in use.
Authentication procedures and policies is communicated to all users who have access to cardholder data.

b. Group, shared, or generic accounts and passwords, or other authentication methods, are prohibited as follows:
Generic user IDs and accounts are disabled or removed.
Shared user IDs for system administration activities and other critical functions do not exist.
Shared and generic user IDs are not used to administer any system components.

c. User passwords are changed at least every 90 days.

d. A minimum password length of at least seven characters is required.

e. Passwords will contain both numeric and alphabetic characters.

9.2

a. Procedures are developed to easily distinguish between onsite personnel and visitors, as follows:

Processes and procedures for assigning badges to onsite personnel and visitors include the following:

Granting new badges.

Changing access requirements.

Revoking terminated onsite personnel and expired visitor badges.

Access to the badge system is limited to authorized personnel.

Badges will clearly identify visitors and easily distinguish between onsite personnel and visitors.

9.3

a. Visitors is authorized before entering areas where cardholder data is processed or maintained.

b. Visitors are given a physical token (for example, a badge or access device) that identifies the visitors as not onsite personnel.

c. Visitor badges will expire.

d. Visitors are asked to surrender the physical token before leaving the facility or upon expiration.

9.4

a. A visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.

b. The visitor log contain the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and is the visitor log retained for at least three months.

9.5

a. Media back-ups are stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.

b. This location's security is reviewed at least annually.

9.6

a. All media is physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).

9.7

a. Strict control is maintained over the internal or external distribution of any kind of media.

b. Controls include the following:

Media is classified so the sensitivity of the data can be determined.
Media that is sent by secured courier or other delivery method that can be accurately tracked.

9.8

a. Logs are maintained to track all media that is moved from a secured area, and management approval obtained prior to moving the media (especially when media is distributed to individuals).

9.9

a. Strict control is maintained over the storage and accessibility of media.
b. Inventory logs of all media properly are maintained and periodic media inventories are conducted at least annually.

9.10

a. Hardcopy materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
b. Containers that store information to be destroyed are secured to prevent access to the contents.
c. Cardholder data on electronic media are rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secu

Information

10.7

b. The policy addresses all PCI DSS requirements.
c. An annual risk assessment process is documented that identifies threats and vulnerabilities, and results in a formal risk assessment.
d. The risk assessment process is performed at least annually.
e. The information security policy is reviewed at least once a