Section 3.9 PCI DSS Information Security Policy
Issued: May 2024
Replaces: January 2021

I. PURPOSE

The purpose of this policy is to establish guidelines for processing charges on Payment Cards to protect against the exposure and possible theft of account and personal cardholder information that has been provided to the University, and to comply with the Payment Card Industry Data Security Standards (PCI DSS) requirements which became effective June 30, 2005, and as amended. The University must adhere to these standards to limit its liability and continue to process payments using Payment Cards.

The University has established a PCI DSS Task Force. The Task Force will be responsible for documenting, analyzing, monitoring and distributing all policies and procedures required under PCI DSS.

II. SCOPE

This policy applies to all University units, employees, contractors, consultants, and other workers. This policy is applicable to any party, including University Related Organizations, which processes, transmits, or stores Cardholder Data or Sensitive Authentication Data or could impact the security of the Cardholder Data Environment. All computers and electronic devices, including wireless devices, involved in processing Payment Card transactions are governed by PCI DSS. This includes, but is not limited to; servers, computers, cashiering systems, workstations, virtual machines, payment application and point of sale terminals that process, transmit, or store Cardholder Data or Sensitive Authentication Data.

III. POLICY

Southern Illinois University's preferred method for acceptance of Payment Cards is through the State of Illinois contract. Any unit wishing to process Payment Card transactions should contact their respective Bursar's office. After authorization by the Bursar's Office, a specialized Merchant Number will be established. The unit will work with the PCI DSS Campus Committee Representatives for integrating the payment mechanism to the State of Illinois' contracted vendor's system.

Any internal or external parties involved with the acceptance and processing of Payment Cards for payment of goods and services must ensure that PCI DSS compliance is maintained. To help meet the Payment Card Industry requirements, the following is required:

General Requirements

A. Access to System Components and Cardholder Data should be limited to only those individuals whose job requires such access. PCI Standard 7 All access to the Cardholder Data Environment should be disabled promptly when an individual terminates or no longer requires access. PCI Standard 9.3
B. Any job position that requires access to Cardholder Data or the Cardholder Data Environment will be considered security sensitive. Background checks or other types of employee screening should be performed for any person prior to assignment of duties that include access to Cardholder Data or the Cardholder Data Environment. Background checks or other types of employee screening are not required for those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction. PCI Standard 12.7.1
C. All personnel who have access to the Cardholder Data Environment or who are involved in Payment Card processing must complete card security training upon hire and at least once every

12 months. Computer and network support staff are subject to annual training requirement. PCI Standard 12.6.3

D. Primary Account Number (PAN) should never be transmitted via unprotected end-user messaging technologies such as email, instant messaging, SMS, chat or any other unsecured transmission method. PCI Standard 4.2
E. A self-assessment questionnaire (SAQ) must be completed annually for each merchant or merchant group. The SAQ is a validation tool intended to assist with self evaluating compliance with PCI DSS.
F. An inventory of system components (hardware and software) that are in scope for PCI DSS must be maintained. PCI Standard 12.5.1
G. A formal documented targeted risk analysis should be performed periodically and upon significant changes to the environment and reviewed at least once every 12 months to identify critical assets, threats and vulnerabilities. PCI Standard 12.3.1
H. Wireless technology should be implemented only after careful evaluation of the need for the technology against the risk.
I. Personnel accessing cardholder data via remote access technologies are prohibited from copying, moving and storing cardholder data onto local hard drives and removable electronic media unless explicitly authorized by your campus PCI DSS Campus Committee Representative. PCI Standard 3.4.2

In Office Processing Requirements

Cardholder Data provided over the phone or through the mail is generally documented in hard copy. The following requirements pertain to the hard copy. If the transaction is subsequently processed using a Point of Sale (POS) terminal or through Web, it will also be subject to those requirements.

A. Physical cardholder information must be locked in a secure area, and limited to only those individuals that require access to that data. PCI Standard 9.4. In addition, access to cardholder data should be restricted to a "need to know" basis. PCI Standard 7.2.
B. Payment Card transactions should be processed in accordance with the respective campus guidelines and the PAN should be redacted to include no more than the bank identification number (BIN) and the last four digits. PCI Standard 3.4.1. In addition, any Sensitive Authentication Data should never be stored after authorization (even if encrypted). PCI Standard 3.2 (See Chart 1)
C. Stored credit card information will be retained according to the respective campus data retention policy. Cardholder Data storage should be kept to a minimum and retention time limited to that which is required for a business, legal and/or regulatory purpose. PCI Standard 3.2.1. The payment card data retention policy can be found in your respective campus' Guidelines.

Point of Sale Terminal Processing Requirements

A. Cardholder Data should not be stored on the POI devices.
B. Do not print the entire PAN on either the department copy or customer copy of any receipts or reports.
C. Do not print the card expiration date on the department copy or customer copy of any receipt.
D. All POI devices must be PCI DSS compliant.
E. Reports printed from POS terminals should not include the full PAN.
F. Ensure POI devices that capture payment card data via direct physical interaction with the card are protected from tampering and unauthorized substitution. PCI Standard 9.5.1

Web Payment Processing & Electronic Storage Requirements

A. Approval by the PCI DSS Campus Committee Representatives (CCR) is required before implementing software and installing equipment that processes, transmits or stores Payment Card information.
B. Network Security Controls should be installed and maintained to control computer traffic between the Cardholder Data Environment and all untrusted networks, as well as traffic into and out of more sensitive areas within an entity's internal trusted network. PCI Standard 1.4.1. Sensitive Authentication Data should not be stored and PAN should be masked when displayed to include no more than the BIN and last four digits. PCI Standards 3.4.1. (see Chart 1)
C. Monitor PCI DSS compliance status for all third-party service providers at least once every 12 months. PCI Standard 12.8.4. This includes ensuring that all service providers are on the Visa list of approved service providers. This list can be found on Visa's website at https://usa.visa.com/splisting/splistingindex.html. Ensure that all third-party service providers acknowledge in writing to customer that they are responsible for the security of cardholder data the third-party service provider possesses or otherwise stores, processes or transmits on behalf of SIU. PCI Standard 12.9 Document the PCI DSS requirements managed by each third-party service provider. PCI Standard 12.8.5
D. Assign someone to ensure proper user authentication and password management, including addition, deletion, and modification of user ID's. PCI Standard 8.2.4 Vendor-supplied defaults for system passwords should not be used. PCI Standard 2.2.2
E. Sensitive Authentication Data must be encrypted during transmission over networks that are easily accessed by malicious individuals. PCI Standard 4.2.1
F. Deploy anti-malware software on all system components at risk from malware, particularly personal computers and servers. PCI Standard 5.2.1 Perform periodic evaluations for systems not considered to be commonly affected by malicious software to confirm such systems continue to not require anti-malware software. PCI Standard 5.2.1
G. Develop and maintain secure systems and software by installing the latest vendor supplied security patches. PCI Standard 6.3.3
H. Assign a unique identification number to each person before granting access to system components or cardholder data. PCI Standard 8.2.1
I. Physical access to data or systems that store, process, or transmit Cardholder Data should be restricted. PCI Standard 9
J. Enable audit logs for all system components and Cardholder Data. PCI Standard 10.2.1
K. Regularly test security systems and networks using methods such as vulnerability scans and penetration testing. PCI Standard 11. Test for the presence of wireless access points by using methods such as a wireless network scans, physical/logical inspections of system components, network access control, or deploying a wireless Intrusion Detection System/Intrusion Prevention System. PCI Standard 11.2.1
L. If possible, network segmentation should be used to isolate the Cardholder Data Environment from the remainder of the University's network. If segmentation is used, perform penetration testing at least once every 12 months and after any changes to ensure operating effectively. PCI Standard 11.4.1 and 11.4.2 and 11.4.3

IV. SANCTIONS

Non-compliance with this policy may result in the loss of the privilege to accept Payment Card payments. Additionally, fines may be imposed by the affected payment card company. Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary actions, suspension, termination of employment and/or legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

V. REPORTING A SUSPECTED BREACH

In the event of a suspected breach, contact your CCR immediately. If a breach is confirmed, the Incident Response Plan will be followed. PCI Standard 12.10

VI. DEFINITIONS AND RESOURCES

A. *Payment Card Industry Data Security Standard (PCI DSS):* PCI DSS is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding Cardholder Data to reduce credit card fraud. PCI DSS defines a series of best practices for processing, transmitting, and storing Cardholder Data and Sensitive Authentication Data.

B. *Cardholder Data:* At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

C. *Cardholder Data Environment:* The system components, people, and processes that store, process or transmit cardholder data or sensitive authentication data, including any system components that may not store, process or transmit cardholder data/sensitive authentication data but have unrestricted connectivity to system components that store, process, or transmit cardholder data/sensitive authentication data.

D. *Card Verification Code:* Also referred to as the Card Validation Code or Value, or Card Security Code. For PCI DSS purposes, it is the three- or four-digit value printed on the front or back of a payment card. May be referred to as CAV2, CVN2, CVV2, or CID according to the individual Participating Payment Brands. For more information, contact the Participating Payment Brands.

E. *Sensitive Authentication Data:* Security-related information used to authenticate cardholders and/or authorized payment card transactions. This information includes but is not limited to card validation verification codes (e.g., three-digit or four-digit value printed on the front or back of a payment card (e.g., CAV2/CVC2/CVV2/CID)), full track data (from magnetic stripe or equivalent on a chip), and PIN and PIN Block.

F. *Service Code:* Three-digit or four-digit value in the magnetic-strip that follow the expiration date of the payment card on the track data. It is used for various things, such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.

G. *Merchant:* For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any PCI SSC Participating Payment Brand as payment for goods and/or services. A merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or services providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

H. *Network Security Controls*: Firewalls and other network security technologies that act as network policy enforcement points. NSCs typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules.

I. *Payment Card:* Any payment card form factor that bears the logo of any PCI SSC Participating Payment Brand.

J. Payment Card Form Factor: Includes physical payment cards as well as devices with functionality that emulates a payment card to initiate a payment transaction. Examples of such devices include, but are not limited to, smartphones, smartwatches, fitness bands, key tags, and wearables such as jewelry.

K. *PCI DSS Campus Committee Representatives (CCR):* The Bursar and designated Information Technology representative at each respective campus location. For purposes of this document, the term Bursar includes the Comptroller at the School of Medicine.

L. *POS:* Acronym for "Point of Sale System". Hardware and/or software used by merchants to accept payment from customers. May include POI devices, PIN pads, electronic cash registers, etc.
M. *POI:* Acronym for "Point of Interaction," the initial point where data is read from a card.
N. *PAN:* Acronym for "Primary Account Number." Unique payment card number (credit, debit, or prepaid cards, etc.) that identifies the issuer and the cardholder account.
O. *PIN Block*: A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain the PAN (or a truncation thereof) depending on the approved ISO PIN Block Format used.
P. *Account Data:* Account Data consists of Cardholder Data and/or Sensitive Authentication Data.
Q. *System Components:* Any network devices, servers, computing devices, virtual components, or software included in or connected to the Cardholder Data Environment, or that could impact the security of the Cardholder Data Environment.

Approved:

Daniel Mahony, President

5/21/2024

Date

CHART 1	Data Element	Storage Permitted	Render Data Unreadable
Cardholder Data	Primary Account Number (PAN)	Yes, but kept to a minimum (PCI Standard 3.2)	Yes (PCI Standard 3.5)
	Cardholder Name	Yes, but kept to a minimum (PCI Standard 3.2)	No
	Service Code	Yes, but kept to a minimum (PCI Standard 3.2)	No
	Expiration Date	Yes, but kept to a minimum (PCI Standard 3.2)	No
Sensitive Authentication Data [1]	Full Track Data[2]	Cannot be stored after authorization (PCI Standard 3.3.1)	Yes, data stored until authorization is complete must be protected with strong cryptography (PCI Standard 3.3.2
	Card Verification Code	Cannot be stored after authorization (PCI Standard 3.3.1)	Yes, data stored until authorization is complete must be protected with strong cryptography (PCI Standard 3.3.2
	PIN/PIN Block [4]	Cannot be stored after authorization (PCI Standard 3.3.1)	Yes, data stored until authorization is complete must be protected with strong cryptography (PCI Standard 3.3.2

[1] Sensitive Authentication Data must not be stored after authorization (even if encrypted).

[2] Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

[3] The three-or-four-digit value printed on the front or back of a payment card.

[4] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.