Section 3.9 PCI DSS Information Security Policy
Issued: November 2017
Replaces: June 2016

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, that processes, transmits, or stores Cardholder Data or Sensitive Authentication Data in a physical or electronic format using university resources. 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 should be performed for any person prior to assignment of duties that include access to Cardholder Data or the Cardholder Data Environment. Background checks 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
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 annually. Computer and network support staff are subject to annual training requirement. PCI Standard 12.6

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 by each merchant or merchant group. The SAQ is a validation tool intended to assist with self evaluating compliance with PCI DSS.
F. Each Merchant must maintain an inventory of system components (hardware and software) that are in scope for PCI DSS PCI Standard 2.4
G. Each merchant must conduct a formal documented risk assessment annually and upon significant changes to the environment to identify critical assets, threats and vulnerabilities. PCI Standard 12~~.1~~.2
H. Wireless technology should be implemented only after careful evaluation of the need for the technology against the risk.
I. 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 annually and after any changes to ensure operating effectively. PCI Standard 11.3.4

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. In addition, access to cardholder data should be restricted to a "need to know" basis. PCI Standard 7
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 first six and the last four digits. PCI Standard 3.3. 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 3.1 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 POS terminal.
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 POS terminals must be PCI DSS compliant.
E. Reports printed from POS terminals should not include the full PAN.
F. Ensure POS terminals and other devices that capture payment card data via direct physical interaction with the card are protected from tampering and substitution. PCI Standard 9.9

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. Firewalls 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

C. Sensitive Authentication Data should not be stored and PAN should be masked when displayed to include no more than the first six and last four digits. PCI Standards 3.2 and 3.3 (see Chart 1)
D. Monitor PCI DSS compliance status for all service providers at least annually. PCI Standard 12.8.4. This includes ensuring that all third party payment applications are PA DSS approved and 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/. Ensure that all service providers acknowledge in writing to customer that they are responsible for the security of cardholder data the 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 service provider. PCI Standard 12.8.5
E. Each merchant is responsible for assigning someone to ensure proper user authentication and password management, including addition, deletion, and modification of user ID's. PCI Standard 8.1.2 Vendor-supplied defaults for system passwords should not be used. PCI Standard 2
F. Sensitive Authentication Data must be encrypted during transmission over networks that are easily accessed by malicious individuals. PCI Standard 4
G. Deploy anti-virus software on all systems commonly affected by malicious software, particularly personal computers and servers. PCI Standard 5 Perform periodic evaluations for systems not considered to be commonly affected by malicious software to confirm such systems continue to not require anti-virus software. PCI Standard 5.1.2
H. Develop and maintain secure systems and applications by installing the latest vendor supplied security patches. PCI Standard 6
I. Assign a unique identification number to each person with computer access within the cardholder environment. PCI Standard 8
J. Physical access to data or systems that house Cardholder Data should be restricted. PCI Standard 9
K. Implement logging mechanisms to track and monitor all access to network resources and Cardholder Data. PCI Standard 10
L. Regularly test security systems and processes using methods such as network vulnerability scans and penetration testing. PCI Standard 11. Test for the presence of wireless points by using methods such as a wireless analyzer, network access control, or deploying a wireless Intrusion Detection System/Intrusion Prevention System. PCI Standard 11.1

IV. SANCTIONS

Merchants not complying with this policy may lose 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 people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.
D. *Sensitive Authentication Data:* Includes Card Validation Code (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 (magnetic stripe or equivalent on a chip), and PIN / PIN Block used to authenticate cardholders and/or authorize payment card transactions. Sensitive authentication data must not be stored after authorization. PCI Standard 3.2
E. *Merchant:* For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard, or Visa) as payment for goods and/or services.
F. *Payment Card:* Any credit card or debit card or other payment device, which is issued by one of the major credit card associations (e.g. Visa, MasterCard, Discover, American Express, JCB International).
G. *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.
H. *Payment Application Data Security Standards (PA DSS):* PA DSS is a set of standards designed to assist software vendors in developing secure payment applications that comply with PCI DSS requirements. A list of validated payment applications is listed on the PCI SSC website, https://www.pcisecuritystandards.org/. This policy is based upon PCI DSS v. 3.2.
I. *POS:* Acronym for "Point of Sale". Hardware and/or software used to process payment card transactions at merchant locations.
J. *PAN:* Acronym for "Primary Account Number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
K. *Account Data:* Account Data consists of Cardholder Data and/or Sensitive Authentication Data.
L. *System Components:* Any network devices, servers, computing devices, or applications in or connected to the Cardholder Data Environment.

CHART 1

	Data Element	Storage Permitted	Render Data Unreadable
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data [1]	Full Track Data[2]	No	Cannot store per requirement 3.2
	CAV2/CVC2/CVV2/CID[3]	No	Cannot store per requirement 3.2
	PIN/PIN Block [4]	No	Cannot store per requirement 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.