Section 3.9 PCI DSS Information Security Policy
Issued: March 2010
Replaces: July 2008

I. PURPOSE

The purpose of this policy is to establish guidelines for processing charges on Credit 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. 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 information in a physical or electronic format using university resources. All computers and electronic devices, including wireless devices, involved in processing payment card data are governed by PCI DSS. This includes, but is not limited to; servers, computers, cashiering systems, workstations, and point of sale terminals that process, transmit, or store credit card information.

III. POLICY

Southern Illinois University's preferred method for acceptance of credit card payments is through the State of Illinois contract. Any unit wishing to process credit 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 credit 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 computing resources and Cardholder Data should be limited to only those individuals whose job requires such access. PCI Standard 7
B. Any job position that requires access to Cardholder Data or the Cardholder Data Environment will be considered security sensitive. Criminal and credit 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 employees who have access to Cardholder Data or who are involved in credit card processing must attend 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 unencrypted email or any other unsecured transmission method. PCI Standard 4.2
E. A self-assessment questionnaire (SAQ) must be completed annually by each merchant. The SAQ is a validation tool intended to assist with self evaluating compliance with PCI DSS.
F. Each merchant must conduct an annual risk assessment to identify threats and vulnerabilities. PCI Standard 12.1.2
G. Wireless technology should be implemented only after careful evaluation of the need for the technology against the risk.

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. Credit card transactions should be processed in accordance with the respective campus guidelines and the PAN should be redacted to include no more than the last four digits. PCI Standard 3.3. In addition, any Sensitive Authentication Data should never be stored. 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

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. All POS terminals must be PCI DSS compliant.
D. Reports printed from POS terminals should not include the full PAN.

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 credit card information.
B. Firewalls should be installed and maintained to control computer traffic between the Cardholder Data Environment and all untrusted networks. 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. 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 http://usa.visa.com/.
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 8.5
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
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 a wireless analyzer 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 credit card payments. Additionally, fines may be imposed by the affected credit 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 12.9

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 sensitive data. PCI DSS defines a series of best practices for handling, transmitting, and storing sensitive data.
B. *Cardholder Data:* Includes cardholder name, primary account number, expiration date, and service code.
C. *Cardholder Data Environment:* Includes the area of a computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.
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., CVV2 and CVC2 data)), full magnetic stripe, and PIN / PIN Block. Sensitive authentication data must not be stored after authorization. PCI Standard 3.2
E. *Merchant:* Any person or department accepting money for goods or services. Includes conference registrations, memberships, fees, etc.
F. *Credit Card:* Any payment card, including debit cards, which is issued by one of the major credit card associations (e.g. Visa, MasterCard, Discover)
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. 1.2

I. *POS:* Point of Sale

J. *PAN:* Primary Account Number

CHART 1

	Data Element	Storage Permitted	Protection Required
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	Yes
	Service Code	Yes	Yes
	Expiration Date	Yes	Yes
Sensitive Authentication Data	Full Magnetic Stripe Data	No	N/A
	CAV2/CVC2/CVV2/CID	No	N/A
	PIN/PIN Block	No	N/A

Glenn Poshard, President

3-5-2010
Date