2006 SALES AND SERVICES – CREDIT CARD SALES PCI COMPLIANCE

Effective: June 2016
Revised: June 2016
Last Reviewed: May 2017
Resp. Office: The Office of the Treasurer

I. AUTHORITY AND RESPONSIBILITY

The Treasurer's office is responsible for issuing credit card merchant accounts and for overseeing policies and procedures regarding payment processing and adherence to information security policies, guidelines and standards. Information Systems and Computing (ISC) is responsible for the operation of Penn's data networks (PennNet). The Treasurer's Office has the responsibility and authority to ensure that all merchant accounts and any related third-party payment processors adhere to the Payment Card Industry (PCI) requirements to protect cardholder data throughout the University.

The Senior Business Leader(s) in conjunction with the merchant account owners in each School/Center will be responsible for ensuring that their merchant account(s) are PCI Compliant on a daily basis.

The Treasurer's office is responsible for submitting the annual Attestation of Compliance (AOC) to our acquiring bank.

II. EXECUTIVE SUMMARY

The Payment Card Industry (including VISA, Master Card, AMEX, Discover and other major card issuers) has established important and stringent security requirements to protect credit card data. These are called the PCI Data Security Standards or "PCI-DSS." These standards define the way in which credit card merchant accounts must protect cardholder data and achieve PCI compliance based on the method by which credit cards are processed. This policy is intended to be used in conjunction with the complete PCI-DSS standards as established and revised by the PCI Security Standards Council at: https://www.pcisecuritystandards.org/.

III. PURPOSE

This policy defines the responsibilities that merchant account owners and Senior Business Leaders have in assessing and validating compliance with PCI-DSS standards. It also establishes responsibility and accountability in the processing of credit card data, conducting the ongoing self-assessment of the merchant account and undertaking any remediation of processes associated with the transmission, storage or processing of credit card data.

Upon review of the PCI self-assessments and any necessary remediation efforts by merchant account owners, the Treasurer's Office will then complete and submit the annual AOC to the University's acquiring bank that includes all University merchant accounts.

IV. RISK OF NON-COMPLIANCE

Without adherence to the PCI-DSS standards and this policy, the University would be in a position of unnecessary reputational risk and financial liability.

Departments who fail to comply are subject to:

a) Any fines imposed by the payment card industry
b) Any additional monetary costs associated with remediation, assessment, forensic analysis, fraudulent card activity or legal fees
c) Suspension of the merchant account.

V. DEFINITIONS

Merchant Account

A relationship set up by the Treasurer's office between the University and a bank in order to accept credit card transactions. The merchant account is tied to a general ledger account to distribute funds appropriately to the School/Center (owner) for which the account was set up.

For purposes of the PCI DSS, a merchant is defined as any School/Center that accepts payment cards bearing the logos of any of the five members of the PCI Security Standards Council (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payments 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 service providers.

Merchant Account Owner

As defined by Penn: point of contact for the School/Center's merchant account. This person is responsible for the completion of the Self-Assessment Questionnaire in Coalfire One in conjunction with the Senior Business Leader. This should be a full time, exempt Penn employee approved by the Senior Business Leader.

Cardholder Data

At a minimum, cardholder data consists of the full Primary Account Number (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.

PAN

Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called Account Number.

Payment Card Industry Data Security Standard (PCI-DSS)

The PCI-DSS is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council (PCI-SSC), including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

PCI Security Standards Council (PCI-SSC)

The security standards council defines credentials and qualifications for assessors and vendors as well as maintaining the PCI-DSS.

Approved Scanning Vendor (ASV)

A Company approved by the PCI-SSC to conduct external vulnerability scanning services.

Penetration Test

Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the environment (external testing) and from inside the environment.

PCI Self-Assessment Questionnaire (SAQ)

The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate ongoing compliance to the PCI-DSS. The University currently uses Coalfire One, a third-party tool created by Coalfire, to automate the Self-Assessment Questionnaire (SAQ) process.

For information see:

http://www.coalfire.com/Documents/DataSheets/DS_SAQ_CoalfireOne.jpg

Authorized users who have already set up their merchant accounts through the Treasurer's Office can access the system at: https://idp.coalfire.com/account/signin

VI. SCOPE

This policy applies to all persons who come in contact with credit card data. It applies to any computing devices owned or leased by the University of Pennsylvania that store, transmit, or process credit card data over the Penn network (PennNet). It also applies to all third parties who process credit card data on behalf of a University-issued merchant account. The use of a PennCard as a debit card (PennCash) is not within the scope of this policy.

VII. STATEMENT OF POLICY

A. Penn requires that Schools/Centers using credit cards to process payments on behalf of the University to comply with the requirements and obligations set forth in Sections B and C below. If you are establishing a merchant account for the University of Pennsylvania Health System (UPHS), you must refer to the UPHS PCI policy [hyperlink].

B. Requirements.

i. General Requirements. Schools/Centers using credit cards to process payments must ensure that:

a) Their credit card merchant accounts are approved by the Senior Business Leader for the School/Center and by the Treasurer's Office. A new credit card merchant account should not be requested without a full understanding of the responsibilities and alternatives of accepting funds on behalf of the University. Approval will generally be given only to those who have an anticipated annual credit card sales volume of approximately $100,000 unless otherwise documented and approved by the Treasurer's Office.

b) Management and employees who process or have access to credit card data are familiar with and are adhering to the applicable PCI-DSS requirements of the PCI Security Standards Council and have taken the annual University PCI course located in Knowledge Link.
c) Senior Business Leaders in conjunction with the merchant account owners conduct an ongoing self-assessment against the PCI-DSS standards in Coalfire One.
d) All employees involved in processing credit card payments shall acknowledge electronically a statement that they have read, understood, and agree to adhere to Computer Security Policy, Incident Response Policy (see section D. – References) and this policy.
e) Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of credit card data must be brought to the attention of and be approved by the Treasurer's Office. This includes both internal processes and those of approved third party vendors (See Appendix A) whose applications or software store or process credit card data on the University's behalf.

ii. The Treasurer's Office requires any third parties processing credit card payments on behalf of the University must be approved by the Treasurer's Office in accordance to Appendix A.

iii. Approved SAQ validation Types. Only the following SAQ validation types highlighted in Table 1 below are allowed:

a) SAQ A
b) SAQ B

Use of any alternative SAQ Validation types must be approved, on a case-by-case exception basis, by the Treasurer's Office.

Table 1

SAQ Validation Type	Description	# of Questions v3.1	ASV Scan Required v3.1	Penetration Test Required v3.1
*A	Card not present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage.	14	NO	NO
B	Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage.	41	NO	NO
A-EP	E-Commerce merchants redirecting to a third party website for payment processing, no electronic cardholder data storage.	139	YES	YES
B-IP	Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage.	83	YES	NO
C	Merchants with payment application systems connected to the internet: No e-commerce or electronic cardholder data storage.	139	YES	YES

C-VT	Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage.	73	NO	NO
P2PE	Merchants only using hardware payment terminals in a PCI SSC listed P2PE Solution: No e-commerce or electronic cardholder data storage.	35	NO	NO
D-MER	All other SAQ-eligible merchants.	326	YES	YES

***SAQ A as specified in the above table shall mean using a PCI-compliant service provider approved by the Treasurer's Office (see Appendix A) such that the credit card number is NOT entered into a web page of a server hosted on the Penn network.**

C. Compliance

I. **Training**: All merchant account users, individuals involved in any way with the processing of credit/debit card transactions to accept/refund money for products or services on behalf of the University are responsible for taking annually the University Payment Card Industry - Data Security Standards Workforce Education course located in Knowledge Link.

II. **Notification:** The Treasurer's Office will notify departments of any upcoming trainings, changes to Coalfire One and other PCI-DSS related updates.

III. **Self-Assessment:** The PCI-DSS Self-Assessment Questionnaire (SAQ) must be maintained by the merchant account owner and updated anytime a credit card related system or process changes/added.

IV. **Remediation**: Any systems or processes that do not meet the current version of the PCI-DSS requirements must be remediated to meet PCI-DSS standards. Merchant account owners are responsible for remediation and the Treasurer's Office is responsible for the final approval of the SAQ in Coalfire One.

V. **Attestation of Compliance**: Upon completion of remediation efforts across the University's Schools and Centers, the Treasurer's office will submit the annual AOC to our acquiring bank.

VI. **Financial Implications**: The department shall bear the costs associated with ensuring compliance with this policy and the PCI-DSS standards as well as any fines imposed by the payment card industry for non-compliance and any additional monetary costs associated with remediation, assessment, forensic analysis, fraudulent card activity or legal fees.

VII. **Review**: ISC Information Security is responsible for reviewing the Computer Security Policy and Information Security Incident Response Policy (listed in reference D) annually. The Treasurer's Office is responsible for reviewing the Credit Card Sales PCI Compliance policy annually and for conducting an appropriate awareness and training program.

VIII. **Responsibility**: Responsibility for compliance with this policy lies with the merchant account owner and the School/Center's Senior Business Leader.

IX. **Enforcement**: Compliance with this policy will be enforced by the Treasurer's Office. The Treasurer's Office will be monitoring compliance of participating Schools/Centers by reviewing self-assessments in Coalfire One.

D. References

- PCI Data Security Standards: (https://www.pcisecuritystandards.org)
- Computer Security Policy: http://www.upenn.edu/computing/group/npc/approved/20100308-computersecurity.html

- Information Security Incident Response Policy: http://www.net.isc.upenn.edu/policy/approved/20070103-secincidentresp.pdf)

APPENDIX A - APPROVED VENDOR LIST

The intent of the Treasurer's Office is to standardize the vendor relationships that handle credit card data on behalf of the University. The below vendors and their associated processing formats have been approved for use by merchant account owners across the University and have included PCI compliant language in their contracts or in an amendment of their contracts. Any additional vendor relationships must be requested by the Senior Business Leader and must be approved by the Treasurer's Office before any negotiations are started. Third Party relationships will only be considered for accounts with signification transaction volume.

Acquiring Bank
Bank of America

Point-of-Sale (POS) Hardware Devices (Treasurer's Office will handle the ordering of any devices)
Bank of America devices
- FD130
- FD410

E-Commerce Payment Processors
CyberSource