

---

**2006 SALES AND SERVICES – CREDIT CARD SALES PCI COMPLIANCE**

---

Subject: PCI Compliance  
Title: Sales and Services – Credit Card Sales PCI Compliance  
No.: 2006  
Effective: April, 2007  
Revised: January, 2012  
Last Reviewed: January, 2012  
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 as well as the establishment of information security policies, guidelines, and standards. Information Systems and Computing is responsible for the operation of Penn's data networks (PennNet). These offices therefore have the responsibility and authority to ensure that all merchant accounts and any related third party payment processors adhere to the PCI requirements to protect cardholder data throughout the University.

The Senior Business Officer in each School/Center will be responsible for ensuring that a PCI self-assessment is completed each year for every merchant account and certify that, overall, their organization is PCI compliant.

The Treasurer's office is responsible for submitting the annual Report On Compliance (ROC) 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." This policy defines the way in which credit card merchant accounts must protect cardholder data and achieve PCI compliance based on the method that credit cards are processed. This policy is intended to be used in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council at: <https://www.pcisecuritystandards.org/>.

---

**III. PURPOSE**

---

This policy defines the steps that merchant account holders must use to assess and secure credit card data annually in paper and electronic form. It also establishes responsibility and accountability for all steps in the processing of credit card data, self-assessment of the merchant account and the remediation of processes associated with the transmission, storage or processing of credit card data.

Upon completion of the annual assessment and remediation efforts an aggregate self-assessment that includes all university and UPHS merchant accounts will be submitted to our acquiring bank.

## IV. RISK OF NON-COMPLIANCE

---

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

Merchant account holders 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 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 organization (owner) for which the account was set up.

### Credit Card Data

Full magnetic stripe or the PAN (Primary Account Number) plus any of the following:

- Cardholder name
- Expiration date
- Service Code

### OWASP

Open Web Application Security Project (see <http://www.owasp.org>)

### PCI-DSS

Payment Card Industry Data Security Standard.

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, 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

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

## Self-Assessment

The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS. The current version of the SAQ, (posted at <https://www.pcisecuritystandards.org/saq/index.shtml>), is based on the current version of the Payment Card Industry (PCI) Data Security Standard (DSS).

## 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.

---

## 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 (including the entities that comprise the University of Pennsylvania Health System) 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 compliance with these requirements throughout the University's Schools and Centers. To achieve compliance, the following requirements must be met by organizations using credit cards to process payments on behalf of the University
- B. Requirements – Local Programs.
  - i. General Requirements. Organizations using credit cards to process payments must ensure that:
    - a) Their credit card merchant accounts are approved by the Senior Business Officer for the school/center or his/her designee and by the Treasurer's Office.
    - b) Management and employees are familiar with and are adhering to the PCI-DSS requirements of the PCI Security Standards Council at:  
<https://www.pcisecuritystandards.org/>.
    - c) Management and/or designees conduct an annual self-assessment against the requirements and report results to the Office of the Treasurer, Cash Management, signed and certified by the organization's Senior Business Officer.
    - d) All employees involved in processing credit card payments sign a statement that they have read, understood, and agree to adhere to Computer Security Policy, Incident Response Policy (see section VIII.D – References) and this policy. This PCI confidentiality and non-disclosure statement can be found on the Treasurer's web site at:  
<http://www.finance.upenn.edu/treasurer/cashman/ccprocessing.shtml>
    - 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 either the Treasurer's Office, ISC Information Security or the Office of Audit, Compliance and Privacy (OACP). 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. **Methods of Processing.** Only the following methods for processing are allowable.
  - a) Point of Sale (POS) processing using dedicated phone lines for both card present and card not present (received by mail, phone or fax) transactions.
  - b) Web-based processing using a PCI-compliant service provider approved by the Treasurer's Office (See Appendix A – Payment Processors) such that the credit card number is NOT entered into a web page of a server hosted on PennNet.
  - c) PCI-compliant lock-box processing in which credit card data is not stored or transmitted on PennNet.
  - d) Use of alternative methods may be approved, on a case-by-case exception basis, by the Treasurer's Office, and only after review and approval by ISC Information Security. All approved exceptions will be listed in the approved vendor list of Appendix A.
  
- iii. **Specific Requirements.** Organizations using the methods in VII.B.ii.a through VII.B.ii.c must also comply with requirements in the PCI-DSS Sections 2, 3, 4 and 6, including but not limited to the following critical requirements:

	Point of Sale (POS)	*Web-based	Lock-box	Approved Alternatives
i. Securely dispose of sensitive cardholder data when no longer needed. Secure destruction may be via shredding, pulping, or for electronic media 3x wipes using secure deletion utility.	X			X
ii. Neither the full contents of any track for the magnetic stripe nor the three-digit card validation code may be stored in a database, log file, or point of sale product.	X			X
iii. Displays of cardholder data may only show the last four digits of the account number.	X			X
iv. Account numbers in databases, logs, files, backup media must be secure, for example by encryption or truncation.	X			X
v. Transmissions of sensitive cardholder data over public networks must be encrypted in accordance with the PCI standards.				X
vi. Sensitive cardholder data may not be sent via unencrypted e-mail.	X	X	X	X
vii. All servers and workstations involved in transmission or storage of credit card data must use and regularly update anti-virus software.				X

viii. Software development processes must use industry accepted best practices and incorporate current security precautions throughout the software development lifecycle.		X		X
ix. Web applications must utilize commonly accepted security guidelines, such as OWASP.		X		X
x. Server-side controls must be implemented to prevent SQL injection and other bypassing of client side-input controls.		X		X
xi. Access to cardholder data must be restricted to users with a need to know.	X	X	X	X
xii. Each person with computer access to cardholder data must use a unique ID.				X
xiii. Physical security controls must be in place to prevent unauthorized access to facilities, computing equipment or media (electronic or paper) housing cardholder data.	X			X
xiv. Employees with access to cardholder data must sign an agreement verifying that they have read and understood the security policies and procedures.	X	X	X	X
xv. Criminal background and credit checks must be performed on employees with access to account numbers. This includes any staff who receive or process more than an individual credit card through a point of sale terminal at a given time.	X	X	X	X
xvi. Third party vendors (see approved vendor list in Appendix A) with access to cardholder data must be contractually obligated to comply with the PCI standards.		X	X	X
xvii. Security incidents must be reported to ISC's Information Security in accordance with Information Security's Incident Response Policy ( <a href="http://www.upenn.edu/computing/policy">http://www.upenn.edu/computing/policy</a> ).	X	X	X	X

**\*Web-Based** as specified in the above table shall mean using a PCI-compliant service provider approved by the Treasurer's Office such that the credit card number is NOT entered into a web page of a server hosted on the Penn network

**C. Compliance**

- I. **Self-Assessment:** The PCI-DSS Self-Assessment Questionnaire must be completed by the merchant account owner annually and anytime a credit card related system or process changes.
- II. **Notification:** The Office of the Treasurer will notify all merchant account owners in the Fall that they have to fill out and resubmit the self-assessment each Spring, signed by both the merchant account owner and the organization's Senior Business Officer or his/her designee. Each year, The

Office of the Treasurer will communicate a detailed compliance schedule to Senior Business Officers.

- III. **Remedy:** Any systems or processes that do not meet the current version of the requirements must be modified to meet the requirements.
- IV. **Report On Compliance:** Upon completion of remediation efforts across the university's schools and centers, the Treasurer's office will submit the annual report on compliance to our acquiring bank.
- V. **Financial Implications:** The merchant account owner shall bear the costs associated with ensuring compliance with this policy and the requirements 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 or legal fees.
- VI. **Responsibility:** Responsibility for compliance with this policy lies with the merchant account owner and the organization's senior business officer.
- VII. **Time Frame:** All merchant account owners are required to complete a self-assessment by March 1 annually.
- VIII. **Enforcement:** Compliance with this policy will be enforced by the Office of Audit, Compliance and Privacy. OACP is responsible for monitoring compliance of participating organizations by collecting and reviewing annual self-assessments and vulnerability scanning reports on the PCI compliant network.
- IX. **Review:** ISC Information Security is responsible for reviewing the security policy annually and for conducting an appropriate awareness and training program.

#### D. References

- PCI Data Security Standards (<https://www.pcisecuritystandards.org>)
- [Computer Security Policy](http://www.isc-net.upenn.edu/policy/approved/20100308-computersecurity.html) (<http://www.isc-net.upenn.edu/policy/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 minimize the number of vendors 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 contract or in an amendment of their contract.

### Payment Processors

CyberSource

PayPal (formerly Verisign's) Payflow Link with exception only (Processor of choice is CyberSource)

### Application Vendors

Sallie Mae

Harris Publishing

Apply Yourself

Public Interactive

Pacific World

Tickets.com (Exception that requires PCI compliant hosting environment)

Micros

IC Verify

JSA Technologies

Jump TV

Tender Retail and McGann Software

Kintera

Get active / Convio