UNIVERSITY OF PITTSBURGH POLICY 05-11-02

CATEGORY:	FINANCIAL AFFAIRS
SECTION:	Payment
SUBJECT:	Payment Card Handling and Acceptance
EFFECTIVE DATE:	July 21, 2015
PAGE(S):	4

I. SCOPE

This policy establishes the requirements for the acceptance and management of payment cards in any area of the University where payment cardholder data is collected, stored or transmitted. Use of the term “payment card” shall include, but not be limited to, such terms as credit cards, debit cards, check cards and other similar cards or applications that convey payment information. The University must comply with the Payment Card Industry (PCI) Data Security Standards (DSS) which is required of all merchants and service providers that store, process, or transmit cardholder data and applies to all payment channels, including retail, mail/telephone order, and e-commerce. These standards include controls for handling and restricting payment card information, computer and internet security, as well as the reporting of a payment card information breach. Security requirements for payment cardholder data must be strictly enforced to prevent breaches of personal information, significant fines to the University, and/or loss of reputation or good will.

Failure to follow this policy may result in the loss of payment card processing privileges for the University department or unit and may result in employment action against individual employee(s).

II. POLICY

Obtaining Payment Card Processing Privileges

Only University Departments or Units which have established merchant accounts approved through the Office of Finance are permitted to accept payment card payments.

Any use of third-party payment services to process payments for goods or services by any University Department or Unit is not permitted, unless explicitly approved by the E-Business Resource Group (EBRG).

Any use, including test environment use, of third party vendor software or systems to process payment card information, including internal or hosted solutions outside the Pitt network, must be reviewed and approved by the EBRG. This review and approval must be conducted each time an agreement with a third party vendor is modified or renewed.

Any card processing activity, payment equipment or technology must comply with PCI DSS and must be approved by the EBRG. All electronic based transactions that involve the transfer of payment card information must be performed on software and systems approved by the University.

Payment Card Processing

Payment card processing methods covered under this policy include, but are not limited to, the following:

- Secure website (e-mail is not acceptable)
- Over the counter (in person)
- Telephone provided payment is processed while the cardholder is on the line
- Mail

Only authorized University employees are permitted to handle payment cardholder data. Any person accepting payment card information on behalf of the University must properly safeguard the data and record the transaction.

Payment Card Data Storage and Retention

All payment cardholder data must be stored in locked files, secured within a secured area having limited employee access, or in electronic systems with security controls that protect the integrity and confidentiality of this information. Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. Sensitive authentication data includes the data as noted below:

- The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere)
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions
- The personal identification number (PIN) or the encrypted PIN block

Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:

- The cardholder’s name
- Primary account number (PAN) rendered unreadable - Mask PAN when displayed (the last four digits are the maximum number of digits to be displayed
- Expiration date
- Service code
- Card type
- Authorization reference number

To minimize risk, store only these data elements as needed for business. All copies of payment cardholder information other than the six items noted above must be destroyed 60 days after the transaction is processed.

Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements
- Processes for secure deletion of data when no longer needed
- Specific retention requirements for cardholder data
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention

Control and Reporting

Each Department or Unit processing payment card information is responsible for assuring that all payment card sales are properly recorded in the University’s General Accounting records. The Department or Unit must establish strict internal controls that regularly assess their systems, security, department policies and controls related to University payment card payment processing. These responsibilities will be assigned to an individual such as the Department’s Financial Administrator, Business Office Manager, or Technical Security Officer. All departments or units will be required to comply with guidelines as established by the EBRG from time to time.

ANY EMPLOYEE SUSPECTING LOSS OR THEFT OF ANY MATERIALS CONTAINING PAYMENT CARDHOLDER INFORMATON MUST IMMEDIATELY NOTIFY THEIR SUPERVISOR AND DEPARTMENT HEAD, WHO MUST THEN IMMEDIATELY NOTIFY CSSD IF THE PROBLEM INVOLVES COMPUTER SECURITY, THE

DESIGNATED CUSTOMER SECURITY INFORMATION OFFICER, AND THE UNIVERSITY POLICE.

Terminating Payment Card Use

Departments or Units no longer requiring use of a merchant account or payment card transaction must contact the Office of Finance to terminate their merchant account.

Service Providers

All third party service providers must provide written confirmation that they are responsible for maintaining the privacy and security of any cardholder data as well as any payment card data that they possess or maintain on behalf of the University. Agreements with service providers must include appropriate language as provided by the Office of General Counsel.

Sanctions

Violations of this policy, or other supplemental policies or procedures, will be subject to sanctions up to and including immediate suspension or termination of payment card processing privileges, and the Department or Unit will no longer be permitted as an authorized payment card merchant. Further, violations of this policy may result in disciplinary action for individuals up to and including termination of employment, as well as prosecution under applicable federal, state, and local laws.

University, Departments or Units engaged in payment card processing are directly responsible for any financial loss incurred by the University resulting from a Department or Unit's inadequate controls or insufficient adherence to this Policy. Such financial loss may include the expenses of notifying individual payment card holders of data breaches as well as any fines or penalties levied by the merchant bank or card associations.

III. REFERENCES

The following documents are incorporated by reference into this policy:

PCI Data Security Standards https://www.pcisecuritystandards.org/security_standards/index.php

University of Pittsburgh Policies and Procedures related to Support Services – Computing, Information, and Data such as the following examples:

Policy AO 11, Computer Data Administration (formerly 10-02-04)

Policy AO 10, Computer Access and Use (formerly 10-02-05)

Policy AO 35, University Administrative Computer Data Security and Privacy (formerly 10-02-06)

University of Pittsburgh Customer Information Security Plan (CISP)

EBRG Guideline including the website and its related documentation

PCI Technology Guidelines as issued by CSSD

University of Pittsburgh Record Retention Requirements