THE OHIO STATE UNIVERSITY

# PCI Requirements
## Office of Business and Finance
**Issued July 2015**

This document provides supplemental information to be used in conjunction with the Payment Card Compliance policy to assist merchants and individuals who handle, process, support or manage payment card processing.

## Definitions

Attestation of Compliance (AoC) - A report prepared by a PCI.

Internet Protocol (IP) Address - A unique number used to represent every computer in a network. The format of an IP Address is four sets of numbers separated by dots (e.g. 10.10.10.123)

Level 1 Service Provider - A vendor that provides access to the internet and to applications to facilitate the transfer and/or storage of payment card information. The following link provides a complete list of PCI Compliant Level 1 Service Providers: http://www.visa.com/splisting/searchGrsp.do

Primary Account Number (PAN) - The 16 digit card number.

PIN Entry Device (PED) - Terminal that allows entry of a customer's PIN.

Personal Identification Number (PIN) - Personal number used in debit card transactions.

Report of Compliance (RoC) - PCI Report prepared by a Qualified Security Assessor to verify a merchant's compliance with the PCI DSS.

SAQ, Self-Assessment Questionnaire - There are eight SAQs listing the PCI Data Security Standards that apply to each method of processing payment cards. OSU's pre-approved processing methods use SAQ A and SAQ B.

## Processing Methods and Associated Requirements

**Processing Methods and Associated Requirements**

The Ohio State University requires all individuals handling, processing, managing or supporting the systems that process payment cards to comply with the current version of the Payment Card Industry (PCI) Data Security Standards (DSS). Listed below are processing methods pre-approved by the university and methods requiring review and approval by OSU's PCI Committee and/or OSU's PCI Qualified Security Assessor (QSA).

I. Pre-approved payment card processing methods and associated requirements are listed below.
   A. Phone line or Cellular terminal
      1. Purchase or rent an approved terminal.
      2. Meet the PCI standards listed in SAQ B.
      3. Complete PCI Training and PCI Manager Training on Carmen or the Wexner Center's Net Learning prior to establishing an account.
      4. Complete the monthly terminal inspection checklist provided by the Office of Financial Services unless an alternative schedule is pre-approved by the university QSA. The purpose of the inspection is to prevent tampering or unapproved replacement of the terminal. Maintain such checklist for internal audit and the annual PCI assessment.
      5. Complete annual Enterprise Risk Assessment or Risk Assessment provided by the Office of the OCIO.
      6. Meet annually with the QSA if required.
   B. e-Commerce – Outsourcing Payment Process to Approved Level 1 Third Party Vendor.
      1. Select a Level 1 Third Party Vendor listed on the Visa Global Registry of Service Providers or the MasterCard Compliant Service Provider List. Alternatively, the merchant may use a third

party vendor who has completed an annual Attestation of Compliance (AoC) prepared by a PCI QSA.
2. Meet the PCI standards listed in SAQ A.
3. Complete PCI Training and PCI Manager Training on Carmen or the Wexner Center's Net Learning prior to establishing an account.
4. Only customers may enter their cardholder data on the payment website.
5. e-Commerce website must redirect payments using an I-Frame implementation.
6. Third Party Vendor must sign the PCI Agreement with Third Party Vendors or otherwise substantially agree to the terms thereof. This must be submitted to the Office of Financial Services prior to processing payments. This agreement must be maintained by the Merchant Manager for the annual PCI assessment.
7. Merchant must verify the Third Party Vendor maintains PCI compliance and the merchant must monitor the annual renewal date of compliance. If a Third Party Vendor's compliance expires, the vendor must be terminated unless a vendor has been granted an extension by the PCI Council.
8. Complete annual Enterprise Risk Assessment or Risk Assessment provided by the Office of the OCIO and submit to the Office of Financial Services prior to the QSA assessment.
9. Meet annually with the QSA if required.

II. Processing Methods requiring approval by OSU PCI Committee and/or QSA

A. There are six methods of processing payments using e-commerce. Each requires review and/or approval by the PCI Committee and/or QSA. If the PCI Committee determines the potential merchant will need to obtain approval from the QSA, the merchant must engage the services of the QSA to review and approve the processing method and implementation.
B. Complete PCI Training and PCI Manager Training on Carmen or the Wexner Center's Net Learning prior to establishing an account.
C. Meet the PCI standards listed in the relevant SAQ listed below:
   1. SAQ A-EP – transmitting and processing transactions using a Level 1 third party service provider listed on the Visa Global Registry of Service Providers or the MasterCard Compliant Service Provider List. This method does not use a pre-approved I-Frame implementation.
   2. SAQ B-IP – transmitting and processing transactions using a payment card terminal with IP connectivity.
   3. SAQ C – transmitting and processing payments on the internet using the university's network and/or related software.
   4. SAQ C-VT – transmitting and processing transactions using a dedicated computer terminal securely connected to a PCI approved third party vendor's online gateway. Access to e-mail, file servers or websites is strictly prohibited.
   5. SAQ D – transmitting, processing and storing cardholder data on the university's network.
   6. SAQ P2PE – transmitting, processing, and/or storing cardholder data using PCI approved Point-to-Point Encryption.
D. Complete annual Enterprise Risk Assessment or Risk Assessment provided by the Office of the OCIO and submit to the Office of Financial Services prior to the QSA assessment.
E. Meet annually with the PCI QSA and pass the assessment.
F. Contact the Office of Financial Services for further information regarding the process for review and approval.

III. PCI Committee and QSA Review and Approval of e-Commerce Methods

A. Merchants who would like to process using an e-Commerce method that is not pre-approved, must have the payment card process reviewed and/or approved by the PCI Committee and/or the QSA.
B. The PCI Committee consists of representatives from units that have managers experienced with processing payment cards using e-Commerce and the related PCI standards that must be met. Current members are:

Advancement – Roland Kreml, kreml.1@osu.edu
Athletics – Troy Henley, henley.4@osu.edu
Extension and Agriculture – Cindy Buxton, buxton.65@osu.edu
Office of Financial Services – Carole Fallon, fallon.82@osu.edu
Office of the Chief Information Officer – David McCartney, mccartney.89@osu.edu
Student Life – Helios Yu, yu.166@osu.edu and Meredith Krisher, krisher.4@osu.edu
Wexner Medical Center – Jamie Nelson, Jamie.nelson@osumc.edu

C. The PCI Committee will convene to review a merchant's request to process using e-Commerce.
   1. Contact the Office of Financial Services to request a form to be completed and to schedule a meeting with the PCI Committee. fallon.82@osu.edu or 292-7792
   2. The following information must be provided prior to review by the Committee.
      a. SAQ method of processing requested
      b. Data Flow Diagram - this is a diagram to illustrate the initial processing of the payment card and the flow of the payment card data to vendors part of the payment card process.
      c. Verification the third party vendor(s) are on the Visa Global Registry of Service Providers http://www.visa.com/splisting/searchGrsp.do or the MasterCard Compliant Service Provider List http://www.mastercard.com/us/company/en/docs/SP_Post_List.pdf
      d. Network diagram, if applicable.

D. The PCI Committee will determine if the merchant request will require the QSA to review and approve the requested e-Commerce method of processing. The merchant will need to engage the services of the QSA and provide documents and information requested by the QSA.

IV. Data Retention

A. Merchants must keep record of the following data for two years
   1. Monthly Terminal Inspection Check lists
   2. Tracking of individuals who have completed PCI Training and PCI Manager Training
   3. Record of the payment card transaction

V. Incident Response Reporting Security Incidents

A. Protecting cardholder data is everyone's responsibility. Known, suspected, and alleged incidents involving lost, disclosed, stolen, compromised, or misused cardholder data must be reported immediately to the following individuals:
   1. Supervisor and merchant manager.
   2. The merchant manager must report any such incident immediately to the following departments:
      a. Office of the Chief Information Officer by phone to 614-688-5650 AND e-mail to security@osu.edu
      b. In the case of the Wexner Medical Center, to OSUWMC by email at issecurity@osumc.edu.

B. This security incident report must not disclose cardholder data.

C. The Office of the Chief Information Officer and/or the Wexner Medical Center Security will immediately notify the Office of Financial Services by e-mailing the Director of Risk, Doug Huffner at huffner.7@osu.edu and his assistant, Donna Loychik at loychik.1@osu.edu

## Requirement Details

I. PCI Training

A. Training is required for individuals who handle, process, manage or support the systems that process payment card transactions. Training is offered on Carmen and Wexner Center's Net Learning. For instructions on Carmen, go to https://ocio.osu.edu/itsecurity/training.

B. Manager Training is also required for Merchant Managers. https://ocio.osu.edu/itsecurity/training

C. Training for individuals who do not have a name.#, will be available in manual format at the following website. http://u.osu.edu/treasurer/treasury/paymentcardsandpci/

II. Monthly Terminal Inspections

A. Complete monthly terminal inspections if merchant is using a payment card terminal unless an alternative schedule is pre-approved by the QSA.

B. Maintain monthly terminal inspection check list for the annual PCI assessment.

III. Risk Assessments - Enterprise Risk Assessment or OCIO Risk Assessment

A. Merchants associated with units that complete Enterprise Risk Assessments must complete an annual assessment and provide documentation to the PCI assessor.

B. Merchants not part of an Enterprise Risk Assessment must complete the Office of the Chief Information Officer's Risk Assessment if processing using one of the pre-approved payment processing methods.

IV. Background checks on personnel considered for hire

A. Merchant managers must perform applicable background checks, within the limits of local law and in accordance with Background Check policy, on individuals considered for hire who will have access to cardholder data in physical or electronic format.
B. Background checks are not required if individuals will have access to one card number at a time such as store cashiers in a supervised setting.
C. It is strongly recommended that any current employee or personnel who have access to more than one payment card number at a time have a background check within the limits of local law and in accordance with Background Check policy.

V. Fax, e-mail, scanning and other technologies to send cardholder data are prohibited.
A. Cardholder data may not be faxed, e-mailed, scanned or sent by end-user messaging technologies unless written approval is obtained from the PCI Committee and/or the QSA.
B. If a customer e-mails, faxes, or sends cardholder data, the following steps must be taken:
1. Notify the customer the transaction cannot be processed. Notification may be done by calling the customer and requesting they provide the number over the phone. Alternatively, notify the customer by separate e-mail that does not include the payment card number and request the payment card number by phone. E-mail, fax, and other messaging technologies are not secure nor authorized methods to transmit cardholder data;
2. Delete the email with the payment card data.
3. If the customer sent cardholder data by fax, cross-cut shred the fax immediately.

VI. Shredding and destroying cardholder data and terminal devices
A. Cardholder data must be destroyed when it is no longer needed for business or legal reasons and must be cross-cut shredded.
B. A payment card terminal must be shredded using an approved vendor when no longer needed.
C. If a third party vendor is used to destroy cardholder data or terminal devices, the vendor must be a Level 1 service provider on the approved PCI list or be approved by NAID, National Association Information Destruction. Shred-it, 614-231-7470 and Royal Document Destruction, 614-751-9731.
D. The data destruction service provider must sign the PCI Agreement with Third Party Vendors or otherwise substantially agree to the terms thereof.

VII. CVV2 or PIN
A. Do not write down or store the three or four digit CVV or CVV2 on the front or back of a card or the PIN in physical or electronic format.

VIII. Imprint device that slides across the payment card is not permitted unless written approval is obtained by the PCI Committee and/or the QSA.
A. Do not use an imprint device to process cardholder payments as they display the full 16 digit card number on the customer and merchant copy.
B. In the event of an emergency, the merchant has two options:
1. Rent a cellular phone terminal to process payments; or
2. Write down the payment card number and expiration date and securely store the information in a locked drawer or locked cabinet. Process the payment card when the terminal or e-Commerce system is operational.

IX. Mask all except the last four digits of the payment card
A. Terminals, computers, and receipts may display or print no more than the last four digits of the payment card numbers.

X. Forms with 16 digit payment card numbers
A. Mail-in payment forms must be designed to have the payment card number at the top or bottom of the form. After the card number is processed, the portion of the form with the card number should be cut off and destroyed in a cross-cut shredder. If the form is kept, it must be securely stored in a locked cabinet or locked office. The customer's signature and other information must be retained.
B. Forms with 16 digit card numbers must not be scanned unless prior written approval is obtained from the QSA.

XI. Mail
A. Cardholder data may be mailed by US postal service, however, secure procedures must be documented and followed to insure only staff with a business need-to-know have access. Once the

transaction is processed, the cardholder data must be cross-cut shredded or stored in a locked cabinet or locked office.

B. No cardholder data may be sent by campus mail.

XII. Moving or transferring cardholder data

A. Any transfer of cardholder data from a secure area is only permitted after administrative approval. It must be transferred by a secure courier or delivery method that can be accurately tracked.

B. Campus mail is not an approved method of transfer.

XIII. Restrict access based on a business need-to-know

A. Access to physical or electronic cardholder data must be restricted to individuals whose job requires access.

XIV. Restrict physical access to electronic or physical data

A. Establish procedures to restrict access to cardholder data in physical or electronic form.

B. Visitor sign-in logs, escorts, and other means must be used to restrict access to documents, servers, computers, and media.

C. The unit must establish password protection on computers and authentication procedures if applicable.

XV. Secure the data

A. Hard copy or media containing cardholder data must be stored in a locked cabinet or locked office.

XVI. Classify cardholder data as confidential

A. All retained cardholder data should be clearly identified as confidential.

B. The data must be securely stored in a locked cabinet or locked office as soon as processing is completed.

XVII. Internal and external scans and penetration testing

A. If applicable, complete successful quarterly internal and external scans and yearly penetration tests.

XVIII. Assign a unique ID and require authentication for each person with computer access to cardholder data or online merchant statements

A. A unique ID must be assigned to each person with computer access to cardholder data. This includes access to the university's merchant processor's online service.

B. User names and passwords may not be shared.

## Resources

**Office of Financial Services for Payment Card Forms and Information** http://u.osu.edu/treasurer/

## For More Information, Contact

Office of Financial Services, 614-292-7792, http://u.osu.edu/treasurer/

## History

Issued: 07/01/2015 version 1.0