THE OHIO STATE UNIVERSITY

Payment Card Compliance, 5.15

University Policy

Applies to: Individuals who handle, process, support, or manage payment card transactions received by the university.

Responsible Office

Office of Business and Finance

POLICY

Issued: 03/01/2007
Reviewed: 06/01/2018

The Ohio State University requires those who handle, process, support, or manage payment card transactions received by the university to comply with the current version of the Payment Card Industry (PCI) Data Security Standards (DSS).

Purpose of the Policy

To provide the university with clear and manageable steps to protect customer cardholder data and to protect the university from a cardholder breach by complying with PCI DSS.

Definitions

Term	Definition
Cardholder data	More than the last four digits of a customer's 16 digit payment card number, cardholder name, expiration date, CVV2/CVV*, or PIN.
Card verification value (CVV2 or CVV)	A three digit number on the back or four digit number on the front of a payment card. PCI does not permit the CVV2/CVV to be stored on paper, electronically, or by any other means.
Data Security Standards (DSS)	Established by the card brands and the PCI Security Standards Council for payment card security. Merchants must refer to the current and applicable provisions of the DSS: pcisecuritystandards.org/
e-Commerce	Method of processing electronic payments primarily on the Internet.
Merchant	University unit that accepts Visa, MasterCard, American Express or Discover payment cards using the university's merchant processor(s). A merchant is assigned a merchant account number by the Office of Financial Services.
Merchant manager	University employee responsible for the PCI compliance (e.g., PCI DSS, PCI training, maintaining documents for PCI audit, etc.) of a merchant account(s) designated by the dean/VP.
PCI Committee	University committee charged with establishing the university PCI Requirements, reviewing merchant requests; chaired by Office of Financial Services.
PCI Payment Application, PA-DSS approved (Software)	Payment Application Data Security Standard's (PA-DSS) approved software sold, distributed, or licensed which stores, processes, or transmits cardholder data as part of authorization or settlement. This includes customized, pre-installed, and "off-the-shelf" software. The following link provides a complete list of PCI approved payment applications: pcisecuritystandards.org/
Payment Card Industry (PCI) Security Standards Council	Visa, MasterCard, American Express, and Discover have formed a council to establish Data Security Standards (DSS) for the industry. Please see the following link for their website: pcisecuritystandards.org/
Payment card(s)	Includes credit and debit cards bearing the logo of Visa, MasterCard, American Express and Discover used to make a payment.
Qualified Security Assessor (QSA)	PCI assessor certified and listed on the PCI Security Standards Council's list of QSAs: pcisecuritystandards.org/approved_companies_providers/qsa_companies.php
Third party vendor (also called "third party service provider")	Business entity directly involved in transmitting, processing, or storing of cardholder data or which provides services that control or could impact the security of cardholder data.
Virtual payment terminal	Web-browser-based access to a third party service provider website to authorize payment card transactions, when the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card.

Applies to: Individuals who handle, process, support, or manage payment card transactions received by the university.

Policy Details

I. Scope
   A. This policy sets the requirements for **merchants** using a payment card terminal as well as merchants processing or sending transactions using **e-Commerce**.
      1. Terminal transactions include face-to-face transactions via phone line or cellular terminals. In some cases, a terminal's keypad may be used to enter card-not-present transactions where **cardholder data** was received via postal mail or over the phone.
      2. e-Commerce transactions include the following:
         a. Links on university websites redirecting customers to another payment website;
         b. IP-connected terminals processing payments on the Internet;
         c. Point of sale transactions at a computer cash register using **PCI payment applications** including point of sale software on a computer to transmit, process, or store cardholder data;
         d. Use of **third party vendor's virtual payment terminal** to transmit, process, or store cardholder data; or
         e. Transactions transmitted, processed, and stored on the university network.
   B. This policy requires each merchant to use pre-approved payment processing methods listed in the university PCI Requirements, be approved by the university **PCI Committee** (chaired by the Office of Financial Services), or be approved by the university's external **Qualified Security Assessor (QSA)**.
   C. Merchants using third party vendors must comply with the current PCI regulations and university PCI Requirements.

II. Background
   A. The cardholder industry formed the **Payment Card Industry (PCI) Security Standards Council** which includes Visa, MasterCard, American Express, and Discover.
   B. The PCI Security Standards Council developed **Data Security Standards (DSS)** to assure consumers that using **payment cards** is a secure method to process payments.
      1. The PCI DSS include controls for handling payment cards, internet security, and reporting of a breach of cardholder data.
      2. The PCI DSS are mandated by the payment card brands and by contract with the university's merchant processor for a merchant to accept payment cards.
   C. The focus of the PCI DSS is to protect against payment card fraud in e-Commerce and terminal-based transactions. Cardholder data in physical or electronic form must be protected. The following processes can result in unacceptable internet accessibility of customer cardholder data. Unless the merchant has obtained approval from the university PCI Committee and/or the university QSA, these processes must be avoided if they include cardholder data:
      1. Basic functions including and not limited to faxing; e-mailing; scanning payment forms; maintaining spreadsheets, receipts, or documents in electronic form; and using messaging technology, must be avoided if they include cardholder data.
      2. All merchants and individuals processing payment cards must comply with PCI DSS and additionally with university PCI Requirements.
   D. In the event of a breach of cardholder data, the university's merchant processor is authorized on behalf of the cardholder companies to assess the merchant any fine levied by the cardholder companies as well as the costs of investigation, remediation, customer notification, payment card monitoring, and customer card re-issuance.

III. Accountability
   A. It is the responsibility of all individuals to whom this policy applies to be informed of and follow the requirements under this policy and any associated documents to protect cardholder data.
   B. Employees who violate this policy may be subject to disciplinary action, including and not limited to termination of employment and/or potential criminal prosecution under applicable federal, state, and local laws.

Applies to: Individuals who handle, process, support, or manage payment card transactions received by the university.

C. Other individuals to whom this policy applies who violate this policy are subject to appropriate sanctions, including but not limited to termination of the relationship and/or potential criminal prosecution under applicable federal, state, and local laws.

PROCEDURE

Issued: 03/01/2007
Reviewed: 06/01/2018

I. Designating Merchant Managers
   A. College/VP units processing payment card transactions must have a designated **merchant manager** before a merchant account may be established.
   B. The dean/VP must designate the merchant manager.

II. Establishing Or Making Changes To A Merchant Account
   A. Establishing merchant accounts
      1. The merchant manager must approve the establishment of any merchant account.
      2. To establish a merchant account and accept payment cards, a unit must complete a Merchant Set-up form and submit it to the Office of Financial Services.
         a. The Office of Financial Services will review the Merchant Set-up form and complete set-up of pre-approved payment processing methods.
         b. Requests to use another payment processing method must be reviewed by the Office of Financial Services and approved by the PCI Committee or external QSA. Documents and card data flow diagrams are required.
      3. Before establishing a merchant account, the merchant manager must document that all individuals who handle, process, support, or manage payment card transactions have completed PCI training.
      4. Units must comply with the PCI DSS, university PCI Requirements, and university Information Security Standard to establish a merchant account and accept payment cards.
   B. Changes to an existing merchant account
      1. Proposed changes must be reviewed and approved by the PCI Committee and, if applicable, the external QSA. Documents and card data flow diagrams are required for review by the committee or the QSA.
      2. Examples of changes include and are not limited to: purchasing software, selecting a new third party vendor, or changing the configuration of an e-Commerce implementation.
      3. Changing to use a pre-approved payment method does not require review and approval.

III. PCI Training
   A. All individuals who handle, process, support, or manage payment card transactions received by the university must complete the university PCI training upon hire and annually thereafter. Training requirements are addressed in the university PCI Requirements.
   B. Additionally, IT directors and designated staff involved in payment card e-Commerce processing must also comply with the university Information Security Standard.

IV. 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; and
         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.

V. Data Retention

Applies to: Individuals who handle, process, support, or manage payment card transactions received by the university.

A. Merchants must keep records of the payment card transaction in accordance with the university Records Retention Schedule but are not required to retain cardholder data.
B. The PCI Security Standards Council does not permit the **CVV2/CVV** to be stored on paper, electronically, or by any other means.

VI. Audit By QSA
A. Merchants will be audited annually by an external QSA.
B. Merchant managers must maintain required documentation in preparation for the audit including and not limited to verification of staff training, contract documents, and other required data based on the current version of PCI DSS.

VII. Additional Operational Requirements
A. Merchants, merchant managers, and individuals who handle, process, support, or manage university payment card transactions must additionally follow the university PCI Requirements as established by the PCI Committee.

Responsibilities

Position or Office	Responsibilities
Dean/VP	Designate the college/unit merchant manager.
Individuals who handle, process, support, or manage payment card transactions	1. Comply with PCI DSS and university PCI requirements. 2. Be informed of and follow the requirements under this policy and any associated documents to protect cardholder data. 3. Complete PCI training upon hire and annually thereafter. 4. Immediately report any known, suspected, or alleged incidents involving lost, disclosed, stolen, compromised, or misused cardholder data to the supervisor and merchant manager without disclosing cardholder data. 5. Comply with the university Information Security Standard.
IT directors and designated staff	1. Complete PCI training upon hire and annually thereafter. 2. Comply with the university Information Security Standard. 3. Immediately report any known, suspected, or alleged incidents involving lost, disclosed, stolen, compromised, or misused cardholder data immediately to the supervisor and merchant manager without disclosing cardholder data. 4. Follow the university PCI Requirements for all merchant operations.
Merchant (unit accepting cardholder payments)	1. Use pre-approved payment processing methods listed in the university PCI Requirements, be approved by the university PCI Committee, or be approved by the university's external QSA 2. Comply with current PCI DSS and university PCI requirements 3. Protect cardholder data 4. Immediately report any known, suspected, or alleged incidents involving lost, disclosed, stolen, compromised, or misused cardholder data to the supervisor and merchant manager without disclosing cardholder data. 5. Keep records of the payment card transaction in accordance with the university Records Retention Schedule. 6. Complete a Merchant Set-up form and return it to the Office of Financial Services to establish a merchant account. 7. Follow the university PCI Requirements for all merchant operations, including records of the payment card transaction. 8. Participate in annual audits by an external QSA.
Merchant manager	1. Comply with PCI Data Security Standards and university PCI Requirements. 2. Approve the establishment of any merchant account in the college/VP unit. 3. Document that all individuals who handle, process, support, or manage payment card transactions have completed PCI training prior to establishing a merchant account. 4. Protect cardholder data. 5. Immediately report known, suspected, and alleged security incidents to the Chief Information Officer by phone and Security Group by email, or OSUWMC if Medical Center by email as appropriate without disclosing cardholder data. 6. Maintain required documentation in preparation for the audit by external QSA.

Applies to: Individuals who handle, process, support, or manage payment card transactions received by the university.

Position or Office	Responsibilities
Office of Financial Services	1. Assign account numbers to merchants. 2. Chair the PCI Committee. 3. Review all Merchant Set-up forms and complete set-up of pre-approved processing methods. 4. Review requests to use payment processing methods other than pre-approved methods and take to the PCI Committee or external QSA for approval. 5. Protect cardholder data. 6. Establish (and maintain) the university PCI Requirements.
PCI Committee	1. Establish the university PCI Requirements. 2. Review merchant requests. 3. Approve requests to use payment processing methods other than pre-approved methods. 4. Review and approve proposed changes to existing merchant accounts. 5. Protect cardholder data.

Resources

Office of Financial Services for Payment Card Forms and Information

The following forms, documents, and trainings may be accessed at: busfin.osu.edu/treasurer/pci-compliance

- Merchant Set-up Form
- PCI Requirements
- PCI Training
- PCI Manager Training
- Other information about payment cards

Other University Policies and Standards, policies.osu.edu/

- Records Retention Schedule, library.osu.edu/documents/records-management/general-schedule.pdf
- Institutional Data policy, go.osu.edu/idp
- Information Security Standard, go.osu.edu/infosec-iss

Other Information

External Websites:

- PCI Security Standards Council website, pcisecuritystandards.org
- Third Party Vendors, visa.com/splisting/searchGrsp.do
- Glossary of PCI terms, pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3.pdf

Contacts

Subject	Office	Telephone	E-mail/URL
PCI Compliance	Office of Business and Finance, Office of Financial Services	614-292-7792	BF-treasury-mgt@osu.edu busfin.osu.edu/treasurer/pci-compliance
Enterprise Security	Office of the Chief Information Officer, Enterprise Security	614-292-2020	security@osu.edu
Data Security, Wexner Medical Center	Wexner Medical Center, IT Help Desk	614-293-3861	issecurity@osumc.edu

History

Issued:	03/01/2007	
Revised:	08/01/2009	
Revised:	07/03/2013	
Revised:	07/15/2014	
Revised:	07/01/2015	"Credit Card" renamed "Payment Card Compliance"
Reviewed:	05/16/2016	
Edited:	05/01/2017	Policy section only
Reviewed:	06/01/2018	