THE OHIO STATE UNIVERSITY

Payment Card Compliance

University Policy

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

Responsible Office **Office of Business and Finance**

POLICY

Issued: 03/01/2007
Revised: 07/01/2020 (minor revision)
Edited: 12/16/2022

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
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.
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.
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 on the PCI Security Standards Council website.
e-Commerce	Method of processing electronic payments primarily on the Internet.
Exception	Any violation of or noncompliance with a university policy issued by the Office of Business and Finance (Business and Finance).
Health System	University Hospital, East Hospital, Brain and Spine Hospital, Richard M. Ross Heart Hospital, Harding Hospital, Dodd Rehabilitation Hospital, Ambulatory Clinics and Services, and Arthur G. James Cancer Hospital and Richard J. Solove Research Institute and Outreach Sites.
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 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 designated by the unit leader.
Payment card	Includes credit and debit cards bearing the logo of Visa, MasterCard, American Express, and Discover used to make a payment.
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. See the PCI Security Standards Council website.
PCI Committee	University committee charged with establishing the PCI Requirements, reviewing merchant requests; chaired by 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 PCI Security Standards Council website provides a complete list of PCI approved payment applications.
Qualified Security Assessor (QSA)	PCI assessor certified and listed on the PCI Security Standards Council's list of QSAs.
Third-party vendor	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. Also commonly referred to as a "third-party service provider."

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

Term	Definition
Unit	College or administrative unit.
Unit leader	Head of college or administrative unit (e.g., dean, senior vice president, president, provost).
Virtual payment terminal	Web-browser-based access to a third-party vendor 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.
Waiver	Permission granted to a unit to operate differently than specified or required by a university policy issued by Business and Finance.

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**. All merchants and individuals processing payment cards must comply with PCI DSS and additionally with PCI Requirements.

1. Terminal transactions include face-to-face transactions. In some cases, a terminal's keypad may be used to enter card-not-present transactions when **cardholder data** was received via postal mail or over the phone. Terminal transactions include payments processed using:

a. IP-connected terminals processing payments on the Internet;

b. 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; and

c. Use of **third-party vendor's virtual payment terminal** to transmit, process, or store cardholder data.

2. e-Commerce transactions include the following:

a. Links on university websites redirecting customers to another payment website; and

b. Transactions transmitted, processed, or stored on the university network.

B. This policy requires each merchant to use pre-approved payment processing methods listed in the PCI Requirements be approved by the **PCI Committee**, 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 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 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 emailing; faxing; maintaining spreadsheets, receipts, or documents in electronic form; scanning payment forms; and using messaging technology, must be avoided if they include cardholder data.

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.

E. 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.

PROCEDURE

Issued: 03/01/2007
Revised: 07/01/2020 (minor revision)

I. Designating Merchant Managers
   A. **Units** processing payment card transactions must have a designated **merchant manager** before a merchant account may be established.
   B. The **unit leader** 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 Financial Services.
         a. 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 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, manage, process, or support payment card transactions have completed PCI training.
      4. Units must comply with the PCI DSS, PCI Requirements, and Information Security Standard to establish a merchant account and accept payment cards.
   B. Making 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 changing the configuration of an e-Commerce implementation, purchasing software, or selecting a new third-party vendor.
      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 PCI Requirements.

IV. Reporting Security Incidents
   A. Protecting cardholder data is everyone's responsibility. Alleged, known, suspected, and incidents involving compromised, disclosed, lost, misused, or stolen cardholder data must be reported immediately to the following individuals:
      1. Supervisor, local IT help desk, and merchant manager.
      2. The Information Security Incident Response Management policy provides guidance on the applicable reporting, investigation, and notification requirements.
      3. The merchant manager must report any such incident immediately to Financial Services by email to merchant@osu.edu, and must additionally notify:
         a. Office of the Chief Information Officer, by phone to 614-688-5650 and email to security@osu.edu; and
         b. In the case of the **Health System**, by email to issecurity@osumc.edu.
   B. This security incident report must not disclose cardholder data.

V. Data Retention
   A. Merchants must keep records of the payment card transaction in accordance with the General 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 electronically, on paper, 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 contract documents, verification of staff training, and other required data based on the current PCI DSS.

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

VIII. **Waivers** to this policy must be approved in advance and documented by the Office of Business and Finance, using the Business and Finance University Policy Waiver Request.

IX. Policy Violations
   A. All policy violations must be tracked as an **exception**.
   B. The university may require successful completion of training.
   C. The university may enforce corrective action, up to and including termination, in accordance with applicable policies or rules.
   D. The university may seek restitution, as appropriate.
   E. Criminal charges may be filed, as appropriate.

Responsibilities

Position or Office	Responsibilities
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 PCI Requirements.
Individuals who handle, manage, process, or support payment card transactions	1. Comply with PCI DSS and 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.
Security coordinators	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 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 PCI Committee, or be approved by the university's external QSA 2. Comply with current PCI DSS and PCI requirements. 3. Protect cardholder data.

Position or Office	Responsibilities
	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 General Records Retention Schedule. 6. Complete and submit a Merchant Set-up form to Financial Services to establish a merchant account. 7. Follow 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 PCI Requirements. 2. Approve the establishment of any merchant account in the 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 the Health System by email as appropriate without disclosing cardholder data. 6. Maintain required documentation in preparation for the audit by external QSA.
PCI Committee	1. Establish the 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.
Unit leader	Designate the unit merchant manager.

Resources

Governance Documents

Financial Code of Ethics, busfin.osu.edu/sites/default/files/financial-code-of-ethics.pdf
Information Security Incident Response Management policy, go.osu.edu\infosec-isirmp
Information Security Standard, cybersecurity.osu.edu/cybersecurity-osu/internal-policies-compliance/security-framework/information-security-standard
Institutional Data policy, go.osu.edu/idp

Financial Services Payment Card Forms and Information, busfin.osu.edu/treasurer/pci-compliance
Business and Finance University Policy Waiver Request, go.osu.edu/busfinpolicywaiverrequest
Merchant Set-up Form busfin.osu.edu/university-business/treasurer/merchant-services
PCI Requirements busfin.osu.edu/sites/default/files/quick-start-guide-pci-requirements.pdf
PCI Training cybersecurity.osu.edu/cybersecurity-osu/training/pci-training

General Records Retention Schedule, library.osu.edu/osu-records-management/retention-schedules

External Websites

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

Contacts

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

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	
Revised:	06/21/2019	Minor revision. Number removed from title.
Revised:	07/01/2020	Minor revision
Edited:	12/16/2022	