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)

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card verification value (CVV2 or CVV)</td>
<td>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.</td>
</tr>
<tr>
<td>Cardholder data</td>
<td>More than the last four digits of a customer's 16-digit payment card number, cardholder name, expiration date, CVV2/CVV, or PIN.</td>
</tr>
<tr>
<td>Data Security Standards (DSS)</td>
<td>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/</td>
</tr>
<tr>
<td>e-Commerce</td>
<td>Method of processing electronic payments primarily on the Internet.</td>
</tr>
<tr>
<td>Exception</td>
<td>Any violation of or noncompliance with a university policy issued by the Office of Business and Finance (Business and Finance).</td>
</tr>
<tr>
<td>Health System</td>
<td>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.</td>
</tr>
<tr>
<td>Merchant</td>
<td>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.</td>
</tr>
<tr>
<td>Merchant manager</td>
<td>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.</td>
</tr>
<tr>
<td>Payment card</td>
<td>Includes credit and debit cards bearing the logo of Visa, MasterCard, American Express, and Discover used to make a payment.</td>
</tr>
<tr>
<td>Payment Card Industry (PCI) Security Standards Council</td>
<td>Visa, MasterCard, American Express, and Discover have formed a council to establish Data Security Standards (DSS) for the industry. See pcisecuritystandards.org/ for their website.</td>
</tr>
<tr>
<td>PCI Committee</td>
<td>University committee charged with establishing the PCI Requirements, reviewing merchant requests; chaired by Financial Services.</td>
</tr>
<tr>
<td>PCI Payment Application, PA-DSS approved (software)</td>
<td>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 &quot;off-the-shelf&quot; software. The following link provides a complete list of PCI approved payment applications: pcisecuritystandards.org/</td>
</tr>
<tr>
<td>Qualified Security Assessor (QSA)</td>
<td>PCI assessor certified and listed on the PCI Security Standards Council’s list of QSAs: pcisecuritystandards.org/approved_companies_providers/qsa_companies.php</td>
</tr>
<tr>
<td>Third-party vendor</td>
<td>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.”</td>
</tr>
<tr>
<td>Unit</td>
<td>College or administrative unit.</td>
</tr>
</tbody>
</table>
Payment Card Compliance

University Policy

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

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

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

<table>
<thead>
<tr>
<th>Position or Office</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| 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. |
| 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 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. |
Payment Card Compliance

University Policy

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

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
- Information Security Standard, [go.osu.edu/infosec-iss](http://go.osu.edu/infosec-iss)
- Institutional Data, [go.osu.edu/idp](http://go.osu.edu/idp)

Financial Services Payment Card Forms and Information, [busfin.osu.edu/treasurer/pci-compliance](http://busfin.osu.edu/treasurer/pci-compliance)
- Merchant Set-up Form
- PCI Requirements
- PCI Training
- PCI Manager Training
- Other payment card information


External Websites
- PCI Security Standards Council website, [pcisecuritystandards.org](http://pcisecuritystandards.org)

Contacts

<table>
<thead>
<tr>
<th>Subject</th>
<th>Office</th>
<th>Telephone</th>
<th>E-mail/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data security, Health System</td>
<td>Health System IT Help Desk</td>
<td>614-293-3861</td>
<td><a href="mailto:issecurity@osumc.edu">issecurity@osumc.edu</a></td>
</tr>
<tr>
<td>Enterprise security</td>
<td>Enterprise Security, Office of the Chief Information Officer</td>
<td>614-292-2020</td>
<td><a href="mailto:security@osu.edu">security@osu.edu</a></td>
</tr>
<tr>
<td>PCI Compliance</td>
<td>Financial Services, Office of Business and Finance</td>
<td>614-292-7792</td>
<td><a href="mailto:BF-treasury-mgt@osu.edu">BF-treasury-mgt@osu.edu</a> busfin.osu.edu/treasurer/pci-compliance</td>
</tr>
</tbody>
</table>
Applies to: Individuals who handle, manage, process, or support payment card transactions received by the university

History

<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issued</td>
<td>03/01/2007</td>
<td></td>
</tr>
<tr>
<td>Revised</td>
<td>08/01/2009</td>
<td></td>
</tr>
<tr>
<td>Revised</td>
<td>07/03/2013</td>
<td></td>
</tr>
<tr>
<td>Revised</td>
<td>07/15/2014</td>
<td></td>
</tr>
<tr>
<td>Revised</td>
<td>07/01/2015</td>
<td>“Credit Card” renamed “Payment Card Compliance”</td>
</tr>
<tr>
<td>Reviewed</td>
<td>05/16/2016</td>
<td>Policy section only</td>
</tr>
<tr>
<td>Edited</td>
<td>05/01/2017</td>
<td>Policy section only</td>
</tr>
<tr>
<td>Reviewed</td>
<td>06/01/2018</td>
<td>Minor revision. Number removed from title.</td>
</tr>
<tr>
<td>Revised</td>
<td>06/21/2019</td>
<td>Minor revision.</td>
</tr>
<tr>
<td>Revised</td>
<td>07/01/2020</td>
<td>Minor revision.</td>
</tr>
</tbody>
</table>