

The Ohio State University Credit Card Merchant Policy

Credit Card Handling Responsibilities and Procedures

Prologue

Colleges and universities have traditionally had open networks of information that foster the exchange of ideas and information. However, college and university networks have sometimes been invaded by hackers. This can result in security breaches that disclose customers' credit card information. To protect our customers' credit card information, the University's reputation, and to reduce the financial costs associated with a breach of credit card information, The Ohio State University has instituted this Credit Card Merchant Policy.

Background Information

As a result of credit card breaches and the resulting customer distrust in using credit cards as a payment option, the credit card industry has formed a council called the Payment Card Industry Council which includes Visa, MasterCard, American Express, and Discover. This PCI Council has developed Data Security Standards (DSS) to assure consumers that their brands and using credit cards are reliable and secure. These standards include controls for handling and restricting credit card information, computer and Internet security, and reporting of a breach of credit card information.¹ These standards are mandated by the industry in order for a merchant to accept credit card payments.

A credit card merchant is a department or any other entity at the University that accepts credit cards for payment. All merchants at the University are required to use First Data Merchant Services to settle credit card transactions. However, merchants have operated in a decentralized manner in selecting third party vendors and software products to process credit card payments. Merchants have designed and developed their own e-commerce websites, purchased third party software or have internally developed software to process credit card payments. In addition, University merchants have selected third party vendors to electronically transmit and store credit card payments. In 2005, TrustWave, a certified PCI network scanning vendor, determined that 60% of breaches were due to third party error. To reduce the number of credit card breaches, the PCI developed a list of approved third party software and a list of approved processing vendors.²

Although the primary focus of the PCI DSS is on Internet-based sales, there are other services that allow systems to be Internet accessible which may expose cardholder information. Basic functions such as e-mail can result in Internet accessibility of a merchant's network. Therefore, all university credit card merchants, including merchants transmitting via a terminal on a dedicated phone line, must complete an annual self-assessment survey and, if applicable, an internal scan and a remote external scan by our PCI approved vendor.

¹ Please see the link to the PCI DSS (Data Security Standards) at the end of this document.

² Please see links to PCI approved third party software and PCI approved Service Providers" at the end of this document.

The credit card companies through PCI have determined there are four Levels of merchants in the industry. The Ohio State University is a Level 3 which is based on the number of credit card transactions per year. PCI has delegated to First Data Merchant Services the responsibility to ensure that organizations are complying with the assessment and scanning requirements to verify compliance with the Data Security Standards.

In the event of a breach by an individual merchant, First Data Merchant Services is authorized on behalf of the credit card companies to assess the particular merchant any fine levied by the card associations as well as the costs of investigation, remediation, customer notification, and customers' card re-issuance. Further, one merchant breach may result in the card association elevating the University to a Level 1 merchant which requires each merchant at the University to pay for and submit to an outside audit of their credit card operation .

Periodic reviews of merchants will be coordinated by the Office of Financial Services and the Office of the Chief Information Officer. Credit card handling procedures are subject to audit by internal audit or external audit. Departments not complying with approved safeguarding and processing procedures may lose the privilege to serve as a credit card merchant.

Policy Statement

Who Should Know This Policy

Any official or administrator with responsibilities for managing University credit card transactions and those employees entrusted with handling or processing credit card information. This includes fiscal officers and systems managers.

To Whom This Policy Applies

This policy applies to all credit card merchants at the University. It applies to merchants accepting credit card payments using a credit card terminal connected to a data phone line as well as merchants processing or sending transactions over the Internet. Internet transactions include links on OSU websites redirecting customers to another website, use of software including Point-of Sale software on a computer to transmit, process, or store credit card information, use of third party vendor to transmit, process, or store credit card information and use of wireless. The University Credit Card Merchant Policy requires each department that accepts credit cards for payment be approved by The Office of Financial Services and where applicable approved by the Office of the Chief Information Officer

Policy

In general, departments are not permitted to transmit, process, or store credit card information on University computer systems or the Internet. When cardholders visit university online sites they must be redirected to a PCI approved third party site to transmit, process, or store the credit card information.

Alternatively, an OSU department may submit a request to transmit, process, or store credit card information provided all software and third party vendors are PCI approved and additional internal requirements are met. The request must be submitted to the Office of Financial Services and will be reviewed by a technical committee of the University.

General Responsibilities and Requirements

Responsibilities of the Office of Financial Services and the Office of the CIO

- Administer the process of obtaining new merchant accounts
- Communicate the policy and PCI DSS to merchants
- Advise merchants wanting to accept credit card payments via wireless, the Internet, or transmit credit card information via the Internet for batch processing.
- Coordinate periodic reviews of existing merchants to include verification of procedures and computer scans as appropriate.

Responsibilities of Credit Card Merchants

All merchants must comply with the requirements listed in the section below titled “General Responsibilities for all Fiscal Officers and Systems Managers of Credit Card Merchant Accounts”. These responsibilities include PCI requirements and University requirements. In addition, merchants must refer to the specific requirements listed in the “Credit Card Merchant Policy for Terminal and Internet related processing” in this document.

General Responsibilities for all Fiscal Officers and Systems Managers

- **Comply with applicable sections of the Payment Card Industry (PCI) Data Security Standards (DSS).** Comply with the applicable provisions of the current PCI DSS.³
- **New merchants or new purchases** - Approval by the Office of Financial Services and, if applicable, the Office of the Chief Information Officer before entering into any contract, purchase, acquisition, or replacement of equipment, software, Internet provider, or wireless device.
- **Maintain a department information security policy** - In addition to complying with University Computing Security Standards policy, supervisors must establish policies and procedures for physically and electronically safeguarding cardholder information and satisfy the requirements of PCI 12. (Please use the form titled “Responsibilities of Credit Card Handlers and Processors” in this document and make the necessary additions pertaining to your department’s credit card processing arrangement.)
- **Prevent unauthorized access to cardholder data and secure the data** - Establish procedures to prevent access to cardholder data in physical or electronic form including but not limited to the following: hard copy or media containing credit card information must be stored in a locked drawer or office; department should establish password protection on computers; visitor sign-in logs, escorts and other means must be used to restrict access to documents, servers, computers, and storage media. PCI 9.
- **Communicate policy to staff and obtain signatures** - Supervisors including Deans, fiscal officers, and systems managers must communicate this Credit Card Policy to their staff and maintain the “Responsibilities of Credit Card Handlers and Processors” form on page 7 for all personnel involved in credit card transactions. PCI 12.6.
- **Restrict access based on a business need-to-know** - Access to physical or electronic cardholder data must be restricted to individuals whose job requires access. PCI. 7.1
- **Assign a unique ID to each person with computer access** - A unique ID must be assigned to each person with computer access to credit card information. User names and passwords may not be shared. PCI 8.1.

³ Please see the link to the PCI DSS (Data Security Standards) at the end of this document.

- **Transmitting credit card information by e-mail or fax prohibited** – Full or partial credit card numbers and three or four digit validation codes (usually on the back of credit cards) may not be faxed or e-mailed. PCI 4.2.
- **Storing electronically the CVV, CVV2 validation code, or PIN number is prohibited** - Do not store the three or four digit CVV or CVV2 validation code from the credit card or the PIN, personal identification number. PCI 3.2.
- **Segregation of duties** - Establish appropriate segregation of duties between personnel handling credit card processing, the processing of refunds, and the reconciliation function.
- **Background checks** – Perform applicable background checks on potential employees who have access to systems, networks, or cardholder data within the limits of OSU Human Resource policy and local law. If employees have access to one card number at a time to facilitate a transaction, such as store cashiers in a supervised setting, background checks are not required by PCI DSS. PCI 12.7.
- **Mask 12 of the 16 digits of the credit card number** - Terminals and computers must mask the first 6 digits and the last 4 digits of the credit card number. PCI 3.3.
- **Imprint machines are not permitted** – Do not use imprint machines to process credit card payments as they display the full 16 digit credit card number on the customer copy. PCI 3.4
- **Report Security Incident to the Office of Financial Services and the Office of the CIO** - If you know or suspect that credit card information has been exposed, stolen, or misused this incident must be reported immediately to the following departments:
 1. The Office of Financial Services, Attn: Cash Management, by fax to 292-7568
 2. The Office of the CIO Security Group, by e-mail to security@osu.edu and by phone to 247-2020 or 688-5650.

This report must not disclose by fax or e-mail credit card numbers, three or four digit validation codes, or PINs. PCI 12.9.

Specific Responsibilities for all Fiscal Officers and Systems Managers – The table below lists responsibilities for merchants accepting credit card payments using the following methods:

- Credit Card Terminal connected to a data phone line
- Internet related processing including:
 - A. Redirecting customers using a link from an OSU web page to a PCI approved service provider or to another company’s site.
 - B. Point of Sale (POS) software that is PCI approved and approved by the university PCI technical committee.
 - C. Software that is PCI approved and approved by the university PCI technical committee.
 - D. Wireless device and software that is PCI approved and approved by the university PCI technical committee.

Credit Card Merchant Policy for Terminal and Internet related processing

(This includes Internet, Internet-related, software, point-of-sale, and wireless systems.)

In general, departments are not permitted to transmit, process, or store credit card data on University computer systems or the Internet. When cardholders visit university online sites they must be redirected to a PCI approved third party site to transmit, process, or store the credit card data. **(See Case A below)**

Alternatively, an OSU department may submit a request to transmit, process, or store the credit card data provided all third party vendors are PCI approved and additional internal requirements are met. The request must be submitted to the Office of Financial Services and will be reviewed by a technical committee. **(See Case B, C, or D below)**

<p>Credit Card Terminal Merchants: merchants using credit card terminals connected to a data phone line.</p> <p>Fiscal Requirements</p> <ol style="list-style-type: none"> 1. Use terminals that do not print on the customer copy the full 16 digit credit card number. 2. Background checks may be required. PCI 12.7 3. Secure storage of credit card information. <p>PCI Provisions applicable - PCI 3, 7, 9 & 12.</p>	<p>Internet-related Merchants:</p> <p>Case A - Redirecting customers using a link from an OSU web page to a PCI approved service provider or to another company's site.</p> <p>Case B - Point of Sale (POS) software that is PCI approved and approved by the university PCI technical committee.</p> <p>Case C - Software that is PCI approved and approved by the university PCI technical committee.</p> <p>Case D- Wireless device and software that is PCI approved and approved by the university PCI technical committee.</p>
---	---

<p>A. Merchants Redirecting - redirecting customers to PCI service providers⁴ using a link from an OSU computer. (Merchants do NOT transmit, process, or store credit card data on any computer located on a university IP address.)</p>	<p>B. Point of Sale (POS) Merchants - using terminal connected to a computer to transmit, process or store credit card information and using PCI approved service providers ⁴. (Merchant must submit a request to The Office of Financial Services.)</p>
<p>Examples</p> <ol style="list-style-type: none"> 1. OSU hosted web page collects all information except credit card information. (i.e. OSU web page is linked to CyberSource "HOP" Hosted Order Page product. 2. OSU hosted web page is linked to another PCI approved company's site. 	<p>Examples</p> <ol style="list-style-type: none"> 1. Using point of sale software to transmit, process, or store credit card information. 2. Using a terminal connected to a computer to swipe credit card transactions that are "batched" daily and sent via the Internet.
<p>Questions</p> <ol style="list-style-type: none"> 1. Is service provider PCI approved? 2. Is service provider linked to another service provider? If yes, is that provider PCI approved? 3. Does the merchant have access to 16 digit credit card numbers? If yes, this is not permitted. 	<p>Questions</p> <ol style="list-style-type: none"> 1. Is POS software on the PCI list? 2. Is the service provider on the PCI approved list? 3. Is service provider linked to another service provider? If yes, is that provider PCI approved? 4. Does the merchant have access to 16 digit credit card numbers? If yes, this is not permitted.
<p>Fiscal Requirements</p> <ol style="list-style-type: none"> 1. All service providers are PCI approved. 2. Third party contract language applies to all vendors ⁵ 3. No access to 16 digit credit card numbers. 	<p>Fiscal Requirements</p> <ol style="list-style-type: none"> 1. Software is on the PCI list. 2. All service providers are PCI approved 3. Third party contract language - all vendors ⁵ 4. No access to 16 digit credit card numbers. 5. Background checks may be required. PCI 12.7
<p>System Requirements</p> <ol style="list-style-type: none"> 1. Successful external scan 2. Successful internal scan using CIO approved software 3. Comply with university Computing Security Standards⁶ 4. No access to 16 digit credit card numbers 	<p>System Requirements</p> <ol style="list-style-type: none"> 1. Successful quarterly external scan 2. Successful quarterly internal scan using CIO approved software. 3. Comply with university Computing Security Standards⁶ 4. No password access to 16 digit credit card numbers 5. Background checks may be required. PCI 12.7

<p>C. Merchants using Software - using software that is PCI⁷ approved to transmit, process, or store credit card information and using PCI approved service providers ⁴ (Merchant must submit a request to The Office of Financial Services.)</p>	<p>D. Wireless Merchants - using wireless terminals:</p> <ol style="list-style-type: none"> 1. Direct transmission of credit card information to a PCI approved service provider. 2. Indirect transmission via an OSU server to a PCI approved service provider. ⁴ <p>(Merchant must submit a request to The Office of Financial Services.)</p>
<p>Examples</p> <ol style="list-style-type: none"> 1. Purchased software installed on a university computer that transmits to a PCI approved service provider. 	<p>Examples</p> <ol style="list-style-type: none"> 1. Wireless transmission of credit card data using a PCI approved wireless device. 2. Wireless transmission using a PCI approved wireless device and transmitting via an OSU server to a PCI service provider or OSU approved cellular provider.
<p>Questions</p> <ol style="list-style-type: none"> 1. Is software on the PCI list? 2. Is the service provider on the PCI approved list? 3. Is service provider linked to another service provider? If yes, is that provider PCI approved? 4. Does the merchant have access to 16 digit credit card numbers? If yes, see the Fiscal and System Requirements below. 	<p>Questions</p> <ol style="list-style-type: none"> 1. Is wireless device and cellular service on the PCI and OSU approved list?⁷ 2. Is the service provider on the PCI approved list? 3. Is service provider linked to another service provider? If yes, is that provider PCI compliant? 4. If transmitting to an OSU server, does the merchant have access to 16 digit credit card numbers? If yes, see the Fiscal and Systems Requirements below.
<p>Fiscal Requirements</p> <ol style="list-style-type: none"> 1. Software is on the PABP list. 2. All service providers are PCI approved. 3. Third party contract language applies to all vendors.⁵ 4. Merchant policy regarding access to 16 digit credit card numbers approved in writing by the Office of Financial Services. 5. Background checks may be required. PCI 12.7 	<p>Fiscal Requirements</p> <ol style="list-style-type: none"> 1. Wireless device and software is on the PCI list.⁷ 2. All service providers are PCI approved.⁴ 3. Third party contract language applies to all vendors⁵ 4. If transmitting to an OSU server, a merchant policy regarding access to 16 digit credit card numbers must be approved in writing by the Office of Financial Services. 5. Background checks may be required. PCI 12.7
<p>System Requirements</p> <ol style="list-style-type: none"> 1. Pass systems architecture review by OSU technical committee. 2. Survey successfully completed. 3. Successful quarterly external scan. 4. Successful quarterly internal scan using CIO approved software. 5. Comply with university Computing Security Standards.⁶ 6. Merchant policy regarding access to 16 digit credit card numbers and approved in writing by the Office of Financial Services. 7. Background checks may be required. PCI 12.7 	<p>System Requirements</p> <ol style="list-style-type: none"> 1. Pass systems architecture review by OSU technical committee. 2. If transmitting directly to a PCI approved service provider merchant must comply with university Computing Security Standards⁶ 3. If transmitting via an OSU server to a PCI approved service provider the following system requirements must be met: <ol style="list-style-type: none"> a. Survey successfully completed. b. Successful quarterly external scan. c. Successful quarterly internal scan using CIO approved software d. Comply with University Computing Standards.⁶ e. Merchant policy regarding access to 16 digit credit card numbers approved in writing by the Office of Financial Services. f. Background checks may be required. PCI 12.7

⁴Service provider - is a vendor that provides access to the Internet and to applications to facilitate the transmission and/or storage of credit card information. See PCI service provider list at the link at the end of this document.

⁵Third party contract addendum - available at OSU Purchasing Department.

⁶University Computing Security Standards - <http://cio.osu.edu/standards>

⁷PCI approved Software- software installed on an OSU computer and determined by the credit card industry to follow the industry's standards for securing credit card information. See link to PCI payment application/software list at the end of this document

Responsibilities of Credit Card Handlers and Processors

(Supervisors – please copy this section and have all credit card handlers and processors return a signed copy to you. Keep these copies on file.)

As a credit card handler or processor I agree to abide by the provisions in this document. If I need further clarification I will refer to “The Ohio State University Credit Card Merchant Policy” located at http://www.busfin.ohio-state.edu/FileStore/515_CreditCard.pdf

I will NOT do the following:

- 1) Acquire or disclose any cardholder’s credit card information without the cardholder’s consent including but not limited to the full or partial sixteen (16) digit credit card number, three (3) or four (4) digit validation code (usually on the back of credit cards), or PINs (personal identification numbers).
- 2) Transmit cardholder’s credit card information by e-mail or fax.
- 3) Electronically store on a University computer file or server any credit card information.
- 4) Use an imprint machine to process credit card payments. (An imprint machine is a non-electronic portable device that slides over a customer’s credit card and displays the full 16 digit credit card number on the customer copy.)
- 5) Share a computer password if I have access to a computer with credit card information.

I will DO the following:

- 1) At time of employment, agree to complete a background check within the limits of local law.
- 2) Change a vendor-supplied or default password if I have access to a computer with credit card information.
- 3) Password-protect my computer if I have access to credit card information on a computer.
- 4) Escort and supervise all visitors including OSU personnel in areas where cardholder information is maintained.
- 5) Store all physical documents or storage media containing credit card information in a locked drawer, locked file cabinet, or locked office.
- 6) Report immediately a credit card security incident to my supervisor, the Office of Financial Services, and the Office of the CIO if I know or suspect credit card information has been exposed, stolen, or misused.
 - a) Supervisor in writing
 - b) The Office of Financial Services, Attn: Cash Management, by fax, 292-7568
 - c) The Office of the CIO, by e-mail to security@osu.edu and by phone to 247-2020.

(This report must not disclose by fax or e-mail any credit card numbers, three or four digit validation codes, or PIN numbers. It must include a department name and contact number.)

Signature

Date

Print Name

Procedures

Establishing New Credit Card Merchant

In order to accept credit cards a department must complete a "Credit Card Merchant Agreement and Request Form" and return it to the Office of Financial Services. (Please refer to Exhibit 5 on the Office of Financial Services website. http://www.busfin.ohio-state.edu/FileStore/515_CreditCard.pdf. Upon approval, the Office of Financial Services will establish a new merchant account. If at any time you have a question or concern about accepting credit cards, please contact the Office of Financial Services for assistance at 292-7792.

Changes to an Existing Account

Changes to an existing merchant account must be approved by The Office of Financial Services and the Office of the CIO. Examples of changes are: purchasing, selling, or discarding a terminal; purchasing software; selecting a new service provider. Signing a contract with any third party vendor related to credit card processing must be approved by Purchasing and include the "PCI Text for Agreements with Third Party Vendors" available at the OSU Department of Purchasing.

Training

It will take approximately three weeks for merchant numbers to be set up and to obtain the equipment as needed. A "Help training package" will be sent to you by First Data Merchant Services. The current contact number for their "Help Desk" is 800-558-7101 or 800-984-3383.

Accounting for Transactions

On the Credit Card Merchant Agreement and Request Form the chartfield information must be provided by the new merchant. The transactions will be automatically loaded in the general ledger system when the merchant closes out (also known as "batching") the daily transactions. The sales, credits, and merchant fees will electronically settle into the appropriate University account.

It is the merchant's responsibility to reconcile the settlement amount in the general ledger to the credit card receipts and the statement on a regular basis, but no less than monthly. Each merchant receives a monthly statement from First Data Merchant Card Services. These statements provide a listing of the transactions submitted for reconciliation purposes. You may also sign up for on-line account access on My Merchant View by contacting the Office of Financial Services at 292-7792. It is the Merchant's responsibility to verify the account information is correct.

Additional Information

Fees

Each transaction is subject to assessment, discount and per item fees charged by Visa, MasterCard, American Express, and Discover. Additional fees for transaction processing are assessed by First Data Merchant Services based on a competitive bid process. Please contact The Office of Financial Services, 292-7792, for current information.

Definitions and Payment Card Industry (PCI) links

CVV Card Verification Value Code (a.k.a CVV2) - This is a three (3) digit number on the back of a credit card. In the case of American Express, this is a four (4) digit code on the front of the credit card.

DSS (Data Security Standards)- The credit card data security standards are established by the PCI Council. Merchants at The Ohio State University must refer to the current and applicable provisions of the DSS.

<https://www.pcisecuritystandards.org/>

IP Address - Internet Protocol Address is 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. 198.123.123.7)

Merchant - A credit card merchant is a department or entity that accepts credit cards for payment. An OSU merchant is assigned a merchant account number by the Office of Financial Services. This number is also the merchant account number for Visa and MasterCard transactions. Separate merchant account numbers are assigned for American Express and Discover.

PCI Software - PCI software is installed on an OSU computer and determined by the credit card industry to follow the industry's best practices for securing credit card information. This includes customized, pre-installed, and "off-the-shelf" software and wireless devices. The following link provides a complete list of PCI approved Payment Application vendors. <https://www.pcisecuritystandards.org/> (See the tab marked "Quick Link")

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

PED (Pin Entry Device) - Terminal that allows entry of a customer's Personal Identification Number.

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

PCI Council (Payment Card Industry) - The credit card industry, Visa, MasterCard, American Express, and Discover, has formed a Council to establish Data Security Standards (DSS) for the industry. Please see the following link for their website. <https://www.pcisecuritystandards.org/>

PCI Self Assessment Questionnaire - Survey to be completed annually by OSU merchants. The DSS should be referred to for clarification of the questionnaire.. <https://www.pcisecuritystandards.org/>

Payment Gateway - A payment gateway is a type of service provider that transmits, processes, or stores credit cardholder data as part of a payment transaction. They facilitate payment transactions such as authorizations and settlement between merchants or processors, also called endpoints. Merchants may send transactions directly to an endpoint or indirectly using a payment gateway.

Service Provider - A vendor that provides access to the Internet and to applications to facilitate the transfer and/or storage of credit card information. The following link provides a complete list of PCI Compliant Service Providers. (Please note, this list is maintained on Visa's website.)

<http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf>