



OBJECTIVE

To define the policy and procedures for the acceptance of credit cards by merchants affiliated with the university. For the purpose of this policy, a merchant is defined as a department or entity affiliated with the university.

POLICY

Applies to: All credit card merchants at the university.
Issued: 03/2007
Revised: 08/2009

I. Acceptance of credit cards

- A. The university accepts credit card payments as a convenient service for customers. Departments may accept VISA, MasterCard, Discover, American Express, and debit cards with a VISA or MasterCard logo.
- B. Each department that accepts credit cards for payment must be approved by the Office of Financial Services and where applicable approved by the Office of the Chief Information Officer before entering into any contract, purchase, acquisition, or replacement of equipment, software, Internet provider, or wireless device related to credit cards.

II. Data Security standards

- Credit card merchants at the university are required to follow strict procedures to protect customers' credit card data. The credit card companies (including Visa, MasterCard, Discover, and American Express) have developed standards which credit card merchants must follow called Payment Card Industry (PCI) Data Security Standards (DSS). All merchants must comply with the [PCI standards](#).
- 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. Exceptions to this policy must be reviewed and approved in writing by the OSU PCI Committee. Contact Treasury Management at 292-6261 for information.
- 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.

PROCEDURE

Applies to: All credit card merchants at the University.
Issued: 03/2007
Revised: 08/2009

Note: Responsibilities and procedures for establishing and managing credit cards are complex. This policy provides basic information. Detailed and technical information including systems specifications, contract and liability information is provided in [The Office of Financial Services Credit Card Merchant Policy/Credit Card Handling Responsibilities and Procedures Policy](#). It is recommended that both documents be reviewed in conjunction with each other. The Office of Financial Services is available to provide assistance and address questions as needed.

I. Setting up a Credit Card Account

- A. To set up a credit card terminal account, please refer to the [Financial Resources Manual](#) available on the Office of Financial Services website.
- B. To set up Internet or use software or a wireless terminal, complete a Credit Card Merchant Agreement and Request form. The form may be accessed through the [Financial Resources Manual](#) available on the Office of Financial Services website.

II. Accounting for Transactions

- A. The Office of Financial Services will make transaction entries daily to the General Ledger based on the Chartfield (chart of accounts) designated by a department.
- B. It is the department's responsibility to reconcile the settlement amount in the general ledger to the credit card receipts and to the statements issued by the credit card processor on a regular basis, but no less than monthly.
- C. When customers dispute a charge, departments will be notified via email regarding any disputed charge card sale. It is a department's responsibility to research and respond within the designated time period, including correcting the chargeback if needed.

III. Credit Card Data Security

- A. Fiscal Officers and Systems Managers are required to 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 PCI requirements.
- B. 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.
 - C. Supervisors including deans, fiscal officers, and systems managers must communicate [The Office of Financial Services Credit Card Merchant Policy/Credit Card Handling Responsibilities and Procedures and Policy](#) to their staff, and maintain the “Responsibilities of Credit Card Handlers and Processors” form for all personnel involved in credit card transactions, which is found in the policy.
 - D. All personnel involved in credit card transactions shall do the following:
 - 1. Charge cards shall be accepted for no more than the amount of purchase.
 - 2. The signature on the charge card, if available, must agree to the draft.
 - 3. The expiration date on the credit card must be verified.
 - 4. In the case of face-to-face credit card transactions, the customer receives the copy of the sales draft that has only four (4) digits of the credit card number. The department retains the other copy and must securely lock these drafts if the draft has the full 16-digit credit card number printed on it.
 - 5. Credit card numbers should not be sent via e-mail or fax.
 - E. Access to physical or electronic cardholder data must be restricted to individuals whose job requires access.
 - F. A unique ID must be assigned to each person with computer access to credit card information. User names and passwords may not be shared.
 - G. Storing (electronically or physically) a Card Verification Value Code (CVV or CVV2), or Personal Identification Number (PIN) number is prohibited. This is a three or four digit number found on the back of most credit cards, except for American Express cards where it can be found on the front of the card.



- H. 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.
- I. There must be appropriate segregation of duties between personnel handling credit card processing, the processing of refunds, and the reconciliation function.
- J. Departments must 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.
- K. Terminals and computers must mask 12 of the 16 digits of the credit card number, usually the first 6 digits and the last 4 digits of the credit card number.
- L. Imprint machines are not permitted to process credit card payments as they display the full 16-digit credit card number on the customer copy.
- M. If an employee suspects that credit card information has been exposed, stolen, or misused this incident must be reported immediately to the Office of Financial Services (292-7568) and the Office of the Chief Information Officer 247-2020. This report must not disclose by fax or e-mail credit card numbers, three or four digit validation codes, or PINs.

IV. Merchant Fees

- A. The fees charged by the credit card companies are based on a variety of factors including the type of card the customer presents. To obtain the lowest rate for credit card terminal transactions the merchant should refer to the [Financial Resources Manual](#) available on the Office of Financial Services website.
- B. Please contact Treasury Management for current fees to process credit card transactions.

V. To Accept Buck ID

- A. Go to the [Buck ID](#) website.
- B. A dual processing terminal will be required to process credit cards and Buck ID cards.



RESOURCES

[Office of Financial Services](#)

Treasury Management
Riverwatch Tower, Suite B
364 W. Lane Ave.
Columbus, OH 43201-4340
Phone: (614) 292-6261
Fax: (614) 292-7568

The Office of the CIO Security Group

Phone: 247-2020 or 688-5650

E-mail to security@osu.edu

[Financial Resources Manual](#) on Office of Financial Services web site