Policy 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.

Applies To:

This policy applies to all credit card merchants at Ohio State 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.

Explicit Policy Requirements: (Items for which non-compliance will result in a policy Exception):

The following items are explicitly defined in the policy and should be considered as policy requirements; items which if not followed, will result in policy "exceptions."

Ref #	Description	Page	Para
1	• 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.	1	I. B.
2	• 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.	1	II.
3	• Departments are not permitted to transmit, process, or store credit card information on University computer systems or the Internet.	1	II.
4	• 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.	1	II.
5	• Departments not complying with approved safeguarding and processing procedures may lose the privilege to serve as a credit card merchant.	1	II.
6	• To set up a credit card terminal account, the department must contact the Office of Financial Services prior to set up. • To set up Internet or use software or a wireless terminal, the department must complete a Credit Card Merchant Agreement and Request Form.	2	I.

Ref #	Description	Page	Para
7	• The Office of Financial Services will make transaction entries daily to the GL based on the chartfield designated by a department. • It is the department's responsibility to reconcile the settlement amount in the GL to the credit card receipts and to the statements issued by the credit card processor on a regular basis, but no less than monthly. • When customer's 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.	2	II.
8	• 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.	2	III.A.
9	• 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.	3	III.B
10	• 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.	3	III. C.
11	• **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.	3	III.D.
12	• Access to physical or electronic cardholder data must be restricted to individuals whose job requires access.	3	III.E.
13	• A unique ID must be assigned to each person with computer access to credit card information. User names and passwords may not be shared.	3	III.F.

Ref #	Description	Page	Para
14	• 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.	3	III.G.
15	• 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.	4	III.H.
16	• There must be appropriate segregation of duties between personnel handling credit card processing, the processing of refunds, and the reconciliation function.	4	III.I.
17	• 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.	4	III.J.
18	• 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.	4	III.K.
19	• Imprint machines are not permitted to process credit card payments as they display the full 16-digit credit card number on the customer copy.	4	III.L.
20	• 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 and the Office of the Chief Information Officer. This report must not disclose by fax or e-mail credit card numbers, three or four digit validation codes, or PINs.	4	III.M.

Summary of Potential Policy Exceptions:

- Departments are transmitting, processing, and/or storing credit card information on university computer systems or the Internet.
- The department has set up a credit card terminal account without contacting the Office of Financial Services prior to set up.
- The department set up Internet or use software and/or a wireless terminal without completing a Credit Card Merchant Agreement Request Form.
- Charge cards are accepted for more or less than the amount of the purchase.
- Customers are receiving sales drafts with the full 16 digit credit card number printed on it.
- Credit card numbers are sent via e-mail or fax.
- The department is storing (electronically or physically) CVV, CVV2, or PIN codes.

- Full or partial credit card numbers and 3 or 4 digit validation codes are being faxed and/or e-mailed.
- The department does not have an adequate segregation of duties in the handling of credit cards, processing of refunds, and the reconciliation function.
- Departments are not performing applicable background checks on potential employees who have access to systems, networks, or cardholder data.
- Suspected exposed, stolen, or misused credit card information is not immediately reported to the Office of Financial Services and the Office of the Chief Information Officer.
- Credit card merchants are not complying with Payment Card Industry standards.
- When cardholders visit university online sites, they are not redirected to a PCI approved third party site.
- The department does not reconcile the settlement amount in the GL to the credit card receipts and to the statements issued by the credit card processor on a regular basis and/or is not completing the reconciliations in a timely manner.
- The department does not research and respond to a customer dispute within the designated time period and/or does not correct the chargeback, if needed.
- The department does not maintain a department information security policy.
- The department has not established policies and procedures for physically and electronically safeguarding cardholder information and/or has not established procedures to prevent access to cardholder data in physical or electronic form.
- Departments are not completing the "Responsibilities of Credit Card Handlers and Processors" form for all personnel involved in credit card transactions.
- Signatures on charge cards do not agree to the draft.
- Expiration dates are not verified.
- The department does not adequately secure the merchant copy of the sales draft if it has the full 16 digit credit card number printed on it.
- Access to physical or electronic cardholder data is not restricted to individuals whose job requires access.
- Unique ID numbers are not assigned to each person with computer access to credit card information.
- User names and/or passwords are shared.
- Terminals and computers do not mask 12 of the 16 digits of the credit card number.
- The department is using imprint machines to process credit card payments.

Policy Areas of Potential Student Life Interpretations and/or Follow-up with Business & Finance:

The following items are potential areas of policy interpretation, left to the discretion of Student Life:

Ref #	Description	Page	Para
	• **Are Dining cashiers required to complete background checks?** Per	4	III. J.

Ref #	Description	Page	Para
	policy, they appear to be exempt.		
	• **Are cashiers verifying signatures?** Does any SL unit include this in training or encourage this practice?	3	III. D.
	• **Are adequate segregation of duties in place?**	4	III. I.

Areas of Consideration for Defining as "Reasonable" in the ICS:

Ref #	Description	Page	Para
1	• **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. Need to define what job duties would require access to cardholder data.	3	III.E.

Potential Training Topics:

Training - Fiscal and Business Officers and IT Directors and their staff must complete annual PCI training.

- Institutional Data Policy
- Business Responsibilities
- Business Expenditures
- Understand & Prevent Fraud
- Internal Controls
- Cash Handling
- Identity Theft Red Flags
- Earnings Operations at OSU
- Deposits
- Managing OSU Records
- Background Checks