



Policy 2.2 Credit Card Merchant Accounts

Responsible Official: VP for Finance
Administering Division/Department: Cash Operations
Effective Date: June 01, 2008
Last Revision: February 06, 2009

Policy Sections:

1. Overview
2. Applicability
3. Policy Details
4. Definitions
5. Related Links
6. Contact Information
7. Revision History

Overview

To provide general guidelines regarding credit card merchant accounts.

Applicability

All employees.

Policy Details

2.2.1 Establishment of Departmental Credit Card Merchant Accounts

All University departments wishing to establish either an internet or terminal credit card merchant account must request this account through the Cashier's Office. Please note there are initial start-up fees to set up these accounts. The procedure for establishing a new merchant account is as follows:

1. Go to the [Emory Finance Division website](#) and sign in.
2. Under Operating Areas, go to Cashier Operations.
3. Under Credit Card Processing, click the "Go" button and then click the "Apply Now" button.
4. Fill out the application in its entirety. Print the application, and have all concerned parties sign the application including the department head.
5. Forward the application to the [Cashier's Office](#) for processing (101 B. Jones Center).

At the beginning of the new fiscal year (September) all departments with established merchant accounts or using credit cards in the normal course of their business are required to renew and update their application for merchant account status. Fill out the renewal application, sign, print and return it to the Cashier's Office. Failure to do so will result in a loss of credit card merchant user privileges.

2.2.2 Credit Card Security Standard Procedures

It is the policy of the University that all departments or other campus entities that accept credit cards in the normal pursuit of business do so in a secure manner as set forth by the [Payment Card Industry \(PCI\) Data Security Standard](#). It is the responsibility of the Department Head to ensure all sensitive data such as credit card numbers, PIN numbers, validation codes, social security numbers, etc. are protected against fraud, unauthorized use or other compromise. Security standards that are in place include but are not limited to:

- Ensure your credit card processing terminal is truncating the credit card account number so that only the last 4 digits of the account number are visible. If it is not truncating, you will be required to purchase a new encoder. Please call the [Cashier's office](#) to place an order.
- All documentation that contains sensitive information such as credit card numbers, expiration dates,

social security numbers or other confidential information must be kept at all times in a secure area such as a locked file cabinet, desk drawer or office. Distribute keys and/or combinations only to designated individuals. Replace or rekey locks that have been suspected of compromise, or in the event of termination or transfer of designated employees.

- Only designated persons should handle sensitive information. Restrict access to sensitive areas to the fewest number of people. Dual control is recommended for access to restricted areas.
- Do not store credit card numbers on your desktop computer. If you receive credit card information via email, print a copy of the email and then delete the email from your account.
- If you receive credit card information via fax machine, the machine should be located in a secure area.
- If you receive credit card information via telephone or mail order, do not write information on anything other than an approved form to be used for such purposes.
- In all cases, once the credit card number has been processed, use a black magic marker pen or other implement to mask the credit card number on the document. Leave the last four digits exposed for future reference.
- Do not store credit card validations codes. Do not store PIN verification numbers. Do not store the full contents of any track from the magnetic stripe on the back of a card.
- Retain credit card data for a minimum of 18 months, after which amount of time it is recommended the data be destroyed.

2.2.3 Chargebacks and Disputed Transactions

Disputed or rejected transactions are charged back to the individual department accounts.

2.2.4 Compliance

Departments who are consistently non-compliant with the policies of the University risk revoking their right to establish credit card account for their department. This definition and any subsequent action is at the discretion of Finance management.

2.2.5 Transaction Fees

Departments are charged a percentage on every transaction as a fee from the credit card companies. They show up per transaction or monthly, depending on the card type.

Definitions

Credit card transactions: Allowing customers to purchase goods or services using a credit card either at a terminal or online

Related Links

- Current Version of This Policy: <http://policies.emory.edu/2.2>
- [Best Practices:](http://www.finance.emory.edu/external/polprod/creditcards.cfm) (http://www.finance.emory.edu/external/polprod/creditcards.cfm)
- [PCI Security Standards Council:](http://www.pcisecuritystandards.org) (http://www.pcisecuritystandards.org.)
- [Higher Education and PCI Compliance: Definitions, Challenges, and Actions:](http://www.finance.emory.edu/external/polprod/documents/HigherEdandPCICompliance.pdf) (http://www.finance.emory.edu/external/polprod/documents/HigherEdandPCICompliance.pdf)
- [PCI Compliance for Higher Education Best Practices Checklist:](http://www.finance.emory.edu/external/polprod/crdtcardcompl.cfm) (http://www.finance.emory.edu/external/polprod/crdtcardcompl.cfm)
- [Student Financial Services:](http://www.emory.edu/studentfinancials/index.shtml) (http://www.emory.edu/studentfinancials/index.shtml)
- [Finance Department:](http://www.finance.emory.edu) (http://www.finance.emory.edu)

Contact Information

Subject	Contact	Phone	Email
Credit Card Merchant Accounts	Student Financial Services	404-727-6095	student.financials@emory.edu

Revision History

- Version Published on: Mar 31, 2007 (Sub-sections 2.2.3, 2.2.4 and 2.2.5 were added to the current policy.)
- Version Published on: Mar 31, 2007 (Original Publication)