Policy 2.2
Credit Card Merchant Accounts

This policy version was not current at the time of printing. Please see http://policies.emory.edu/2.2 for the current version.

Responsible Official: Vice President for Finance/Chief Finance Officer
Administering Division/Department: Treasury Operations
Effective Date: March 31, 2007
Last Revision: March 28, 2007

Policy Sections:

I. Overview
II. Applicability
III. Policy Details
IV. Related Links
V. Contact Information
VI. Revision History

Overview

Requirements for meeting and maintaining Payment Card Industry Security Standards.

Applicability

All university departmental entities wishing to establish either an internet or terminal credit card merchant account.

Policy Details

2.2.1 Establishment of Departmental Credit Card Merchant Accounts

All university departmental entities wishing to establish either an internet or terminal credit card merchant account must request this account through the Cashier’s Office. The procedure to establish a new merchant account is as follows:

I. Go to the Emory Finance Division website and sign in.
II. Under Operating Areas, go to Cashier Operations.
III. Under Credit Card Processing, click the "Go" button and then click the "Apply Now" button.
IV. Fill out the application in its entirety. Print the application, and have all concerned parties sign the application including the department head.
V. Forward the application to the Cashier’s Office for processing (101 B. Jones Center).

At the beginning of the new fiscal year, 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 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 Emory 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 six months, after which amount of time it is recommended the data be destroyed.

Related Links

- Current Version of This Policy: http://policies.emory.edu/2.2
- Best Practices (http://www.finance.emory.edu/external/polprod/creditcards.cfm)
- PCI Security Standards Council (http://www.pcisecuritystandards.org.)

Contact Information

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Cards</td>
<td>Cash Operations Office</td>
<td>404-727-6094</td>
<td></td>
</tr>
</tbody>
</table>

Revision History

Emory University policies are subject to change at any time. If you are reading this policy in paper or PDF format, you are strongly encouraged to visit policies.emory.edu to ensure that you are relying on the current version.