Credit Card Acceptance and Processing Policy

Effective Date: August 31, 2009
Latest Revision: August 28, 2013

Policy Statement
This policy sets requirements for the acceptance and processing of credit and debit cards (credit cards) and the secure storage of credit cardholder data.

Reasons for the Policy
The purpose of this policy is to document control procedures and requirements to ensure that cardholder data supplied to the University is secure and protected in accordance with University Policies and the Payment Card Industry Data Security Standards (PCI DSS).

Primary Guidance to Which This Policy Responds
Columbia University Registration and Protection of Systems Policy and the Payment Card Industry Data Security Standard (PCI DSS).

Responsible University Office
The Office of the Treasurer

Revision History
This policy was established in August 2009.
Revision: July 9, 2012
Latest revision: August 28, 2013

Who is Governed by this Policy
This policy applies to all individuals, schools, departments, centers, third party contractors, institutes, and programs that accept donations or sell goods, services, or information, and accept credit cards as a form of payment on behalf of Columbia University.

Who Should Know This Policy
All senior business officers, department administrators and financial and administrative staff whose businesses accept credit cards as a form of payment are required to know this policy.

Exclusions and Special Situations
Exceptions may be granted for offices that are located off campus with the written approval of the Office of the Treasurer. If approved, exceptions will be subject to annual review.

Policy Text
A University Department accepting credit cards is a credit card merchant. To accept credit card payments, the merchant must obtain a Columbia University merchant ID (CU MID) which is a unique number that identifies the merchant for reference and billing purposes.
University Departments may ONLY obtain a CU MID by contacting the Office of the Treasurer creditcards@columbia.edu and complying with specific requirements.

A CU MID will only be issued to University Departments that comply with this policy and all related security policies and of which the Departments' senior business officer acknowledges technical and operational responsibilities associated with credit card acceptance.

Merchants are expected to protect cardholder data and to prevent their unauthorized use.

There are several approved University methods to accept credit cards, including e-commerce, in person using a standalone dial up terminal, in person via web based virtual terminal, or via a Point of Sale (POS) terminal connected to the internet.

**Internet transactions**

University Departments accepting credit cards via e-commerce must adhere to the criteria in the *CU REGISTRATION AND PROTECTION OF SYSTEMS POLICY*. The policy provides that University Departments must not capture, store or transmit cardholder data on Columbia servers or networks.

For merchants processing credit cards using a web based virtual terminal and/or web based POS virtual terminal with the use of peripherals, transactions are permitted only from a local machine on campus using University approved software.

**Cardholder Data**

Cardholder data refers to any information printed, processed, transmitted or stored in any form on a credit card. Cardholder data elements include the following:

- Primary Account Number (PAN)
- Cardholder Name (1)
- Service Code (1)
- Expiration Date (1)
- Full Magnetic Stripe Data (3)
- CAV2/CVC2/CVV2/CID
- PIN/PIN Block

(1) These data elements must be protected if stored in conjunction with the PAN. Sensitive authentication data must not be stored after authorization (even if encrypted).

(3) Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.
Data Retention

- Electronic storage of cardholder data is prohibited by CU Policy.

- All paper record retention of cardholder data must be kept to a minimum. If you must store paper records (transaction receipts, credit card slips, order forms, and hard copy reports) for valid business reasons, either the PAN must be rendered unreadable (retaining only the first 6 or last 4 digits) or the records must be stored in a safe, secure and monitored area for a maximum of seven years. After the designated retention period, the paper records must then be securely destroyed according to the University's Records Retention Policy.

- Sensitive authentication data must never be stored after authorization (even if encrypted).

Merchant Responsibilities

- Comply with University policies and procedures to safeguard credit card and other personally identifiable or sensitive information.

- Ensure that cardholder data is treated as confidential and access is restricted to a need to know basis.

- Ensure functional segregation of duties between employees who process credit card transactions and chargebacks with those who balance and reconcile the transactions.

- Ensure credit card transactions and chargebacks are validated daily.

- Ensure all University employees or contractors acting on behalf of Columbia University, involved with accepting credit cards (including any IT employees) complete annual compliance training.

- Comply with all annual University and PCI DSS self assessment reporting requirements. 

  Immediate steps must be taken to preserve all business records, logs and electronic evidence.

Contacts

Office of the Treasurer
Associate Treasurer - Cash Management and Operations 212-854-9685
Email: creditcards@columbia.edu

Cross References to Related Policies

Information Technology Policies: http://www.columbia.edu/cu/administration/policylibrary/responsible_office/cuit.html including:
  - Columbia University Registration and Protection of Systems Policy
  - Electronic Data Security Breach Reporting and Response Policy
  - Email usage and Retention Policy
  - Data Classification Policy
  - The Records Retention Policy: http://policylibrary.columbia.edu/records-retention-policy
For more information on PCI, refer to https://www.pcisecuritystandards.org/.

All processes for accepting credit cards must comply with PCI DSS. The standards globally govern all merchants and organizations that store, process and/or transmit credit card data.