E-Commerce: Electronic Protection of Credit Card Holder Information Policy

Effective Date: June 2008
Updated: August 2009

Policy Statement
This policy defines the requirements for systems and technologies that utilize, capture, and store credit card information in support of e-commerce for the University.

Reason for the Policy
The University uses e-commerce to conduct business which must adhere to the mandatory security standards and control requirements for protecting cardholders’ information.

Primary Guidance to Which This Policy Responds
This policy responds to the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS requirements for enhancing payment account data security was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the adoption of consistent comprehensive industry-wide compliance requirements.

Responsible University Office & Officer
The office of Columbia University Information Technology Security is responsible for the maintenance of this policy, and for responding to questions regarding this policy. The Chief Information Security Officer (CISO) is the responsible officer.

Revision History
This policy was established in March 2008. This policy was updated in August 2009 to include provision for web front-ends (i.e., website or webpage) using credit card information in support of e-commerce for the University.

Who is Governed by This Policy
This policy applies to individuals, schools, departments, centers, institutes, and programs (“University Departments”) that sell goods, services, information, or gifts and accept credit cards as a form of payment.

Who Should Know This Policy
Senior business officers, department administrators, all finance and administrative staff who accept credit cards as a form of payment; all technical staff that support business units which accept credit cards as a form of payment.

Exclusions & Special Situations
None
**Policy Text**

The University Departments must not capture, store, and transmit credit card information on CU servers or network. Therefore, to enable credit card processing, university departments must outsource their e-commerce systems and technologies that utilize, capture, and store credit card information to a PCI compliant vendor or company which has been independently certified by a company on the Payment Card Industry’s list of Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs).

University Departments may provide an SSL encrypted web front-end (i.e., website or webpage) for the initial part (e.g., item to be purchased, quantity, email address, billing/shipping information, phone number, transaction total or partial total) of the e-commerce transaction. This provision requires that prior to entering any payment information (i.e., card number, type of card, CVV number, expiration date) the cardholder is securely re-directed to the website of an approved PCI compliant third party e-commerce vendor located outside of Columbia University’s systems and network, to facilitate the transaction. All third party e-commerce vendors must be reviewed by Procurement Services (see Appendix B for an approved list). See illustration below.

---

![Diagram of e-commerce transaction](image_url)

The consumer visits e-commerce site hosted at Columbia and selects items for purchase (#1 above). Prior to entering any payment information (i.e., card number, type of card, CVV number, expiration date), the cardholder is re-directed to the website of an approved PCI compliant third party e-commerce vendor via a secure communication (i.e., SSL) (#2 above).
Do not create a website that captures, stores, and transmits the customer’s credit card information on any Columbia University system.

Credit card information (partial or full) must not be captured, stored, and transmitted at any point on any of the University computers.

If unauthorized e-commerce related equipment that captures, stores, and transmits credit card information is discovered in the University, the University reserves the right to disable the machine(s) in question.

The e-commerce web front-end that is hosted at Columbia University must comply with the specific technical and review/recertification requirements available from CUIT (Appendix A) and Merchant ID related requirements from the Office of Treasurer.

**Responsibilities**

Individuals, schools, departments, centers, institutes, and programs (“University Departments”) that sell goods or services and accept credit cards as a form of payment are responsible for implementing appropriate managerial, operational, physical, and technical controls for compliance with this policy and PCI DSS technical requirements. Senior Business Officers in University Departments are responsible for ensuring that the technical set-up for an e-commerce website is compliant with PCI DSS technical requirements and related University policies.

Failure to abide by this policy may be subject to disciplinary action and/or sanctions up to, and including discharge or dismissal in accordance to Columbia University policy and procedures.

Additionally, intentional negligence that results in breach of confidentiality of personal information that is protected by law, acts, or regulations, can also result in criminal prosecution. Penalties for non-compliant to PCI DSS requirements include fines up to $500,000 per incident if data is compromised.

**Definitions**

*CVV number* - The CVV (Card Verification Value) or CVN (Card Verification Number) or CID (Card Identification Number) is the three digit (or four digits on AmEx) security code that is printed, not imprinted, on a Visa, MasterCard, AmEx or Bankcard. This number is never transferred during card swipes and should only be known by the cardholder, the person holding the card in their hand.

*Electronic commerce* - commonly known as e-commerce or eCommerce, consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks.

*Payment Processor* - Third-party merchant services provider who handles the work associated with processing of credit card transactions between merchants, credit card issuers, and merchant account providers.
**Payment Gateway** - The service that automates the payment transaction between the shopper and merchant; it is usually a third-party service that is actually a system of computer processes that process, verify, and accept or decline credit card transactions on behalf of the merchant through secure Internet connections. The payment gateway is the infrastructure that allows a merchant to accept credit card and other forms of electronic payment gateways used for Internet transactions, it may also be called an IP payment gateway.

**SSL** - Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. SSL creates a secure connection between a client and a server. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message.

**Contacts**
For questions or comments:
Columbia University Information Technology
   Email: security@columbia.edu
   Telephone: 212-854-1919

**Cross References to Related Policies**

See the University Policy Library for the “Credit Card Merchant Identification/ID (MID) Setup and Maintenance Policy”

For CUIT Security Policies, see the University Administrative Policy Library, CU Information Technology section:

http://www.columbia.edu/cu/administration/policylibrary/responsible_office/cuit.html

See the “Data Classification” policy for related information.

For more information, see the PCI Security Standards Council

https://www.pcisecuritystandards.org/