COLUMBIA UNIVERSITY
CREDIT CARD ACCEPTANCE AND PROCESSING POLICY

Effective Date: August 31, 2009
Latest Revision: **March 28, 2017**

Policy Statement
This policy establishes the requirements for the acceptance and processing of credit card payments and for the protection of Cardholder Data in accordance with the Payment Card Industry Data Security Standards (PCI DSS).

Reasons for the Policy
The reason for this policy is to set the standard for protecting Cardholder Data supplied to the University or any Third Party Service Provider acting on behalf of the University.

Primary Guidance to which this Policy Responds
This policy responds to the applicable PCI DSS requirements and University policies relevant to the protection of Cardholder Data. This policy does not supersede any Card Brand rules or federal or state law.

Responsible University Office
The Office of the Treasurer

Revision History
This policy was established in August 2009
Revision(s): July 9, 2012; August 28, 2013; October 31, 2016
Latest revision: March 28, 2017

Who is Governed by this Policy
All internal University personnel who handle Cardholder Data or can impact the security of the CU Merchant's Cardholder Data Environment are governed by this policy.

Who Should Know this Policy
All University personnel and any Third Party Service Provider acting on behalf of the University who handle Cardholder Data or can impact the security of the CU Merchant's Cardholder Data Environment should know this policy.

Exclusions and Special Situations
None.

Policy Text
Columbia University acknowledges the importance of its data security and regulatory responsibilities and has established a framework to protect Cardholder Data. All processes, operational procedures and related technologies used for accepting credit cards must comply with the PCI DSS and relevant University policies.

- CU Merchant IDs (MIDs) can only be obtained through the Office of the Treasurer.
- CU Merchant environments must be validated and approved by the CUIT-PCI Security Group via the Merchant Security Review Form prior to going live and prior to implementing any changes to existing CU Merchant environments.

    - CU Merchants must document and maintain a current diagram illustrating the CU Merchant's Cardholder Data Environment (CDE). The diagram must include all data flows, POS devices, network devices, servers, computing devices, applications and any other component or device located within or connected to the CU Merchant's CDE and must be attached to Merchant Security Review Forms for validation by the CUIT-PCI Security Group.
- CU MID requests must be approved by the Senior Business Officer of the department requesting a new MID or updates to an existing MID.
- CU Merchants are expected to protect Cardholder Data (CHD) and prevent any unauthorized use.
- CU strictly prohibits CHD and Sensitive Authentication Data (SAD) from being captured, stored, processed, or transmitted on University servers or networks with the following exceptions:
    - ***Transmission of encrypted CHD*** is permitted through a PCI validated Point-to-Point Encryption (P2PE) Solution (see Approved Methods of Accepting Credit Cards).
    - ***Storage*** of paper forms and digital images of CHD is permitted only when CHD is rendered unreadable (*see Data Retention/Storage*).
- Credit card processing via Wi-Fi is prohibited.
- If a P2PE solution is implemented, the CU Merchant must provide documentation confirming the solution was implemented with all controls in the P2PE Instruction Manual provided by the P2PE solution provider.
- Roles and responsibilities associated with credit card processing must be assigned and acknowledged.
- Individuals with access to the CU Merchant CDE have completed all required training.
- All Third Party Service Providers (TPSPs) that may affect the security of a CU Merchant's CHD or could have an impact on the CU Merchant's CDE must be approved through University Procurement Services prior to requesting a new CU MID or being associated with an existing CU MID.

University Approved Methods of Accepting Credit Cards

- Point-of-Sale (POS) (face-to-face) / Card-Present:
    - Stand-alone terminal with dial-up connection to a dedicated phone line (*IP/Internet connections are prohibited for stand-alone terminals*)
    - Handheld terminal enabled with Cellular connection (*mobile phone card readers are prohibited*)
    - P2PE Solution listed on the PCI Council's List of PCI P2PE Validated Solutions.
- Mail order/telephone order (MOTO) / Card-not-Present:
    - University approved software and hardware only
- E-Commerce / Card-not-Present:
    - Outsource all e-commerce functions and technology support to a University approved PCI compliant vendor
    - University developed websites

Additional information is provided in the attached appendices.

Data Retention/Storage

- Electronic storage of Primary Account Number (PAN) and/or Sensitive Authentication Data (SAD) *even if encrypted* is prohibited, with the following exceptions:
    - Storage of CHD is only permitted in the form of paper documents and/or digital images of such paper documents and must adhere to the following:
        - Documentation containing the full PAN may only be securely stored in

paper form and only until authorization, at which point the full PAN must be rendered unreadable with no more than the first six and/or last four digits visible (411111*****1111) before the document is imaged and scanned for digital storage

    - Storage of SAD is never permitted and must be rendered completely unreadable immediately.
- All paper records must be stored in a safe, secure and monitored area with access limited to select personnel on a "need to know" basis only.
- All digital records must be saved to a secure file location on a drive with limited and monitored access to select personnel on a "need to know" basis only.
- Retention periods must be limited to that which is required for business, legal, and/or regulatory purposes per Columbia University Records Retention Policy and Merchant must have a process in place to review the need for any stored paper records on a quarterly basis.
- After the designated retention period:
    - Hard-copy documentation must be crosscut shredded, incinerated, or pulped either by the merchant or through a contract with an Information Security Office approved-vendor, per the University's Sanitation and Disposal of Information Resources Policy, such that there is reasonable assurance the hard-copy documents cannot be reconstructed.
    - Digital images of documentation must be rendered unrecoverable (e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).

Merchant Responsibilities

Responsibilities include but are not limited to the following:

- Required training must be completed by all individuals with access to the CU Merchant CDE, first upon hire or upon assuming a new role that requires such access, then on an annual basis thereafter, for as long as the individual has access to the CU Merchant CDE.
- Assign roles and responsibilities to individuals with access to the CU Merchant CDE to ensure appropriate internal controls and compliance with PCI DSS and Columbia's related policies.
- Maintain chain of custody records for all equipment that has direct physical interaction with CHD.
- Maintain current list and location of MIDs, terminals and authorized users, operating procedures, data flow diagrams, staff training and equipment inspection logs available for review upon request.
- Review transactions prior to settlement and ensure all open batches are settled daily, and reconcile all account activity (including fees) at least monthly.
- Maintain copies of TPSP documentation indicating which PCI DSS requirements will be met by the TPSP and which will be the responsibility of the CU Merchant.
    - Obtain proof of TPSP's PCI DSS compliance on an annual basis.
- Take immediate action to respond to a suspected or confirmed security compromise of the CU Merchant CDE or any CU Merchant CHD by notifying individuals identified in below section "Responding to a Suspected Credit Card Security Breach."

More information is available on the CU Merchant Services Website.

Enforcement

CU Merchants are subject to periodic audit. Any CU Merchant in violation of PCI DSS or University policies can result in the termination of the Merchant's ability to accept credit cards as a method of payment. Individuals may also be subject to disciplinary action.

Responding to a Suspected Credit Card Security Breach
Anyone with knowledge or suspicion that the CU Merchant CDE or any CU Merchant CHD has been compromised in any way must immediately report the incident to each of the following:

- Immediate supervisor
- Senior Business Officer
- Red Flag Program Administrator: id_security@columbia.edu
- Office of the Treasurer: creditcards@columbia.edu or the Associate Treasurer, Global Treasury Operations
- CUIT: pcisecurity@columbia.edu or the Director, Network Computer Security

CU Merchant must also take immediate steps to preserve all business records, logs and electronic evidence.
The Office of the Treasurer will coordinate with the Office of General Counsel and other appropriate departments to determine if notification laws are applicable and will notify the acquiring bank of any suspected or confirmed compromise The Incident Response Plan will be tested annually.

Annual Policy Review
In compliance with PCI DSS requirements, this policy will be reviewed at least annually and updated as needed to reflect changes to industry standards and/or business objectives and to address new or evolving threats to CU Merchants.

Contacts
OFFICE OF THE TREASURER
creditcards@columbia.edu
Associate Treasurer, Global Treasury Operations
Assistant Director, PCI Compliance & Merchant Account Services

CUIT PCI SECURITY
pcisecurity@columbia.edu

Definitions

- Card Brands – American Express, Discover, JCB, MasterCard or Visa.
- CHD – Cardholder Data - At minimum, consists of the full PAN but may also include the full PAN with cardholder name, expiration date, or service code.
- CDE – Cardholder Data Environment - The people, processes and technology that capture, store, process or transmit CHD or SAD, including any system components that may affect the security of such data.
- Credit Cards – Credit and debit cards issued by one of the five Card Brands.
- CU Merchant – Any individual/school/department that accepts credit cards bearing the logos of any of the five Card Brands as payment for goods and/or services on behalf of the University.
- MID – Merchant ID - Unique ID associated with each CU Merchant account used for transaction processing and billing.
- Payment Application – Software application that stores, processes, or transmits CHD as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties.
- PAN – Primary Account Number – and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account, and consists of 16 to 19 digits.
- PCI SSC – Payment Card Industry Security Standards Council made up of five Card Brand

members that set the standards to enhance CHD security.

- PCI DSS – Payment Card Industry Data Security Standards – provides a baseline of technical and operational requirements designed to protect CHD which applies to all entities that store, process or transmit CHD or SAD and/or are involved in credit card processing.
- SAD – Sensitive Authentication Data - Security related information used to authenticate cardholders and/or authorize credit card transactions, includes full track data, equivalent data on the chip, three- or four-digit code (e.g., CVV2), or Personal identification number (PIN) entered by cardholder during a card present transaction, and/or encrypted PIN block present within the transaction message.
- TPSP – Third Party Service Provider – business entity that is not a Card Brand and is directly involved in the processing storage or transmission of CHD, or that provide services that control or could impact the security of the CDE.

Cross References to Related Policies

- INFORMATION TECHNOLOGY (CUIT)
  - Acceptable Usage of Information Resources Policy
  - Business Continuity And Disaster Recovery Policy
  - Data Classification Policy
  - Electronic Data Security Breach Reporting and Response Policy
  - Email Usage Policy
  - External Hosting Policy
  - Information Resource Access Control and Log Management Policy
  - Information Security Charter
  - Information Security Risk Management Policy
  - Internet Domain Name Policy (Replacing Columbia Domain Name Policy)
  - Network Protection Policy
  - Registration And Protection Of Endpoints Policy
  - Registration And Protection Of Systems Policy
  - Sanitization And Disposal Of Information Resources Policy
- OFFICE OF GENERAL COUNSEL
  - Identity Theft Prevention Policy
  - Records Retention Policy

Related Links

For more information on PCI Security Standards, refer to: https://www.pcisecuritystandards.org/
For more information on CU's Merchant Services refer to: Merchant Services Website

Card Brand Rules

- American Express Merchant Reference Guide - U.S.
- Discover Merchant Rules
- JCB Merchant Requirements
- MasterCard Merchant Rules
- Visa Merchant Rules

Resources

- Merchant Security Review Form
- Device Inventory Log
- Device Inspection Form
- Merchant Manual

Appendix A: Compliance Requirements for Point-of-Sale (POS) (face-to-face) / Card-Present Merchants

All card-present CU Merchants must adhere to the following and to all relevant University policies and procedures, including but not limited to all equipment setup procedures and training requirements, prior to going live.

- All equipment must be ordered through the Office of the Treasurer.
- Do not allow unannounced service visits or accept unannounced installs, replacements or upgrades (for hardware or software) without checking with the Office of the Treasurer.
- All default and administrator passwords must be changed from the default password prior to processing any transactions.
- POS Terminals must only be connected via a dedicated dial-up phone line.
    - IP connections are prohibited with the exception of Point-to-Point Encryption (P2PE) Solutions.
    - Connection to Wi-Fi is prohibited.
- P2PE solutions must be listed on the PCI Council's List of PCI P2PE Validated Solutions, all other P2PE solutions are not permitted unless prior approval from CUIT PCI Security Group.
- Ensure POS terminal is EMV chip enabled and is on the List of PCI Approved PTS Devices.
    - If it is not, contact The Office of the Treasurer to update your equipment.
- Maintain an up-to-date list of all POS terminals/devices that includes the following:
    - Make, model of terminal/device.
    - Location of terminal/device (for example, the address of the site or facility where the device is located).
    - Terminal/device serial number or other unique identifier.
- Limit access to terminals to authorized individuals only.
- Maintain an up-to-date list of all individuals with access to each terminal.
- Perform daily inspections of each POS terminal/device that has direct access to CHD within the CU Merchant CDE and keep monthly logs of inspections as back up.
    - Look for broken terminals, swapped terminals, tampered labels on the terminals, changes to terminal connections, hidden cameras on or near the terminal, addition of unfamiliar electronic equipment connected to the terminal, overlays of skimming and key-logging hardware on terminals.
- Document procedures for periodic inspection of terminal/devices.
- Secure all POS terminals/devices during non-business hours.
- During business hours, secure terminals/devices with locking stands, cable trays, and other securing mechanisms.
    - Position any PIN entry devices so there is no capability of recording or viewing PINs entered by customers.
- Review transactions daily for any unauthorized transactions.
- Transaction receipts are required and Merchant copies must be retained (in paper or digital image form) for a minimum of two (2) years (or such longer period as the Card Brand Rules or federal or state law may require).
    - Transaction receipts must be stored in a safe, secure area and organized in chronological order by transaction date.
- Ensure all personnel for card-present Merchants have been provided additional training to be aware of attempted tampering or replacement of devices.
    - Personnel must report any suspicious behavior, tampering or substitution of devices immediately per the Responding to a Suspected Credit Card Security Breach section in the Credit Card Acceptance and Processing Policy.

- Any unused terminals must follow the below protocol for proper disposal:
    - Call the customer service number provided on the terminal to have them walk you through deprogramming the terminal and clearing the installed software.
    - Mail terminals to the following address and reference "Columbia University - Credit Card Terminal Program" on the package:

      Chris Massaro
      Chief Operating Officer
      Monmouth Wire & Computer Recycling
      3250 Shafto Road
      Tinton Falls, NJ 07753
- Refund policy must be posted in clear view of the cardholder at the time of checkout, or printed on customer receipts.
- When outside personnel and TPSPs are using CU Merchant terminals, CU Merchant must ensure the following:
    - Agreements approved by University Procurement Services are in place that require the TPSP and outside personnel to adhere to the same level of requirements covered in this Appendix.
    - CU Merchant must obtain confirmation in writing from the TPSP that all outside personnel operating on CU Merchant equipment have completed adequate PCI training provided by the TPSP.

Appendix B: Compliance Requirements for Mail order/telephone order (MOTO) / Card-not-Present Merchants

All card-not-present CU Merchants must adhere to the following and to all relevant University policies and procedures, including but not limited to all software setup procedures and training requirements, prior to going live.

- Authorization forms used to collect CHD must never collect security code (CVC2, CAV2, CVV2, CID).
- All MOTO transactions should be submitted securely, through one of the following methods:
    - University approved payment gateway by authorized users only.
    - Stand-alone point-of-sale (POS) dial-up connection only, terminal provided by The Office of the Treasurer.
        - POS processing must also adhere to Appendix A of the Columbia University Credit Card Acceptance and Processing Policy.
- CHD must never be left over voicemail or emailed.
- Each user performing MOTO transactions must use their own unique login ID and password provided by Treasury. Unique login credentials must never be shared. Periodic audits are conducted against the IPs of user logins and user activity; any shared user IDs found may be immediately disabled without notice.
- Any computer used to process MOTO transactions must be hard wired to a Columbia University network jack and connected to the Citrix Server.
    - Computers cannot be connected to any wireless networks, nor plugged into a wireless router.
- Computers used to process MOTO transactions cannot have any wireless devices installed and must not be a laptop (i.e. no wireless keyboards or mice, no wireless card).
    - CU Merchants must physically inspect their cardholder data environment to check for rogue wireless access points quarterly.
- Firewall with inbound and outbound blocking must be installed with:
    - Default deny set (note that windows XP firewall does not block outbound traffic)
    - No port should be open unless absolutely required by a business application running on the system and is approved by CUIT PCI Security.
- Absolutely no remote access (via remote desktop, GoToMyPC, etc.) allowed to any system used to access any payment gateway for credit card payment processing. CUIT/Local IT must ensure the following settings are in place on all computers used for transaction processing:
    - RDP and HTTP (Microsoft-HTTPAP 2.0) must be disabled.
    - The following registry values must be set to true (1)
        1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\RequireSecuritySignature.
        2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\EnableSecuritySignature.
- Refund policy must be clearly displayed on all mail order forms.
- Refer to the Registration And Protection Of Endpoints Policy for additional requirements.
- When outside personnel and TPSPs are processing MOTO transactions on behalf of the CU Merchant, the CU Merchant must ensure the following:
    - Agreements approved by the Office of Procurement are in place that require the TPSP and outside personnel to adhere to the same level of requirements covered in this Appendix.
    - CU Merchant must obtain confirmation in writing from the TPSP that all outside personnel with access to the CU Merchant account have completed adequate PCI training provided by the TPSP.

Appendix C: Compliance Requirements for E-Commerce / Card-not-Present Merchants

All card-not-present e-commerce CU Merchants must adhere to the following and to all relevant University policies and procedures, including but not limited to, all e-commerce setup procedures and training requirements, prior to going live.

- Merchants must obtain a payment gateway account from Treasury when requesting a new CU MID.
- E-Commerce Merchants must never capture, store, process or transmit CHD on any CU network or server.
- When using a payment application, the applications must be listed on the PCI Council's List of Validated Payment Applications; no other applications are permitted.
- Merchants must provide an encrypted web front-end using the current PCI DSS recommended cryptographic protocol for the initial part of the e-commerce transaction (e.g., item to be purchased, quantity, email address, billing/shipping information, phone number, transaction total or partial total).
- All online payment forms where CHD is captured must originate from a University approved PCI compliant TPSP.
    - 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 a University approved PCI compliant TPSP located outside of University systems and network to facilitate the payment transaction through a secure payment form.
    - The entirety of the payment form must be served and managed by the University approved PCI compliant TPSP and access to manage any part of the payment form by any University employee is prohibited.
- Enable security features on payment gateway accounts used for E-Commerce:
    - *HTTP Referrers* - Only accept transactions from a pre-approved list of websites. Although this adds additional steps to implement, this action will help prevent fraudulent users from submitting transactions from their website, claiming to be you.
    - *Server Side Code* - All sensitive merchant data, including transaction amount and API interface credentials, should be placed in server side code, rather than placing hidden value fields on an HTML form. API interface credentials must not be visible within the view page source HTML by right clicking within the webpage. This will reduce the ability for malicious users to edit and use this data for their own fraudulent purposes.
    - *Address Verification Service (AVS)* - Service that compares the customers billing address to what their bank has on file.
    - *Card Verification Value (CVV or CVC2)* - This refers to the 3 or 4 digit value that is intended to confirm that the buyer has the physical card in their possession at the time they are completing the purchase.
- Refund policy, privacy policy & contact information must all be clearly posted on Merchant site.