AMERICAN UNIVERSITY WASHINGTON, D.C.

University Policy: Cardholder Data Security

Policy Category: Financial Services

Subject: Protecting covered data in support of the Payment Card Industry (PCI) Data Security Standards

Office Responsible for Review of this Policy: Office of Finance and Treasurer

Procedures & Guidelines:

Related University Policies: Data Classification Policy, Computer Use & Copyright Policy, IT Security Policy and Records Retention and Disposal Policy.

I. SCOPE

This policy applies to all American University faculty, staff, students, and organizations that handle electronic or paper documents associated with credit or debit card receipt transactions or accept payments in the form of credit or debit cards. The scope includes any credit or debit card activities conducted at all American University campuses and locations.

II. Policy Statement

This policy addresses Payment Card Industry (PCI) Security Standards that are contractually imposed by Visa, Master Card, Discover, and American Express, on merchants that accept these cards as forms of payment. American University recognizes the Office of Finance and Treasurer as the sole authority to assign credit card Merchant ID's and to contract with credit card processors and merchant banks.

The policy covers the following specific areas contained in the PCI Data Security Standards (DSS) related to cardholder data: collecting, processing, transmitting, storing and disposing of cardholder data. The PCI Security Council defines cardholder data as:

Full magnetic stripe or the Primary Account Number (PAN) plus any of the following:
- Cardholder name
- Expiration date
- Card Verification Value (CVV)

All departments wishing to accept, store, transmit or process cardholder data must complete Part I of the Payment Acceptance Activity Clarification (PAAC) form outlining the purpose and description of the business process and submit to Treasury Operations. Once Part I has been received by Treasury Operations, the PCI Review Committee may conduct further review of the proposal. Upon approval, Part II of the PAAC form must be completed by the requesting unit describing specific merchant detail such as card brands, hardware required, website URL and the dollar and projected transaction volume. Treasury Operations will

coordinate with the Processor to issue the new Merchant ID number for the purpose of processing card transactions in accordance with the objectives set forth in this policy.

Departments must acknowledge in writing on the Confidentiality Agreement regarding cardholder data that they have reviewed the policies and procedures outlining the handling of cardholder data prior to being assigned a Merchant ID by Treasury Operations. Departments seeking final authorization must ensure that the following objectives, meant to meet the spirit of the PCI-DSS requirements, are met:

1. Access to cardholder data collected is restricted only to those users who need it to perform their jobs.

   Access to areas where cardholder data is processed must be tightly restricted. Methods must be established to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder information is accessible.

   If necessary, visitor access to such areas should be controlled through physical audit trails (such as sign in sheets) or department issued guest badge and/or access device, which must be surrendered upon exit.

2. Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment or documents containing cardholder data.

   This includes physically securing all paper and electronic media (e.g., payment terminals, computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder information. Appropriate measures must be taken to secure cardholder information during transfer of such cardholder information by authorized individuals within the office environment.

3. Computer access (account authorization and creation) to systems that are used to collect, process, store or transmit cardholder data must meet PCI-DSS and University logical access controls in accordance with OIT's Logical Access Policy. Please contact the OIT Help Desk for details of all logical access requirements.

4. Cardholder data, whether collected on paper or electronically, must be protected against unauthorized access. Do not store the full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.), the card-validation code (3 or 4 digit value printed on the front or back of a payment card (CVV2, CVC2 data)) or the PIN Verification Value (PVV).

   a. PAN Information must not be stored in an electronic spreadsheet, database, or other file format.

   b. Portable electronic media devices must not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact

disks, USB flash drives, smart phones, tablet computers, and portable external hard drives.

c. Cardholder data should *never* be received or sent via email or voicemail.

d. Credit card data must be truncated anywhere it is stored (including data on printed receipt forms, portable media, backup media, in logs, and data received from or stored by wireless networks). PCI-DSS permits storing the first six and/or the last four digits of the PAN, but never the Card Verification Value (CVV). Any retained paper documents that contain cardholder data must have such data redacted in accordance with PCI Standards. If a University department utilizes recurring payments, a PCI-Compliant third party Service Provider must be used to store full-track cardholder data.

5. All cardholder data must be destroyed upon authorization.

   Paper documents must be cross cut-shredded. Any materials containing cardholder data must be rendered unreadable prior to discarding, scanning, imaging or storing. The transfer of paper documents containing cardholder data should only be done using an approved secured carrier or other delivery method that can be accurately tracked. Retired computer drives must be erased, degaussed, or physically destroyed in accordance with University's Records Retention and Disposal Policy.

6. All equipment used to collect data must be secured against unauthorized use in accordance with the PCI- DSS.

   Point of sales systems, cash registers, workstations, or applications where cardholder data is processed, stored or transmitted must be verified by the Office of Information Technology (OIT) and the University's Qualified Security Assessor (QSA) as compliant with the PCI-DSS.

7. An approved QSA must validate Service Providers as PCI-DSS compliant.

   It is incumbent on the requesting department to execute the proper due diligence prior to engagement with a third party Service Provider. The Treasury Office will facilitate the audit of campus Service Provider (third party) compliance status at least annually.

8. Software that is classified as a payment application such as PayPal or Official Payments must be validated in accordance with the Payment Application Data Security Standards (PA-DSS).

   The specific version number must be listed on the PCI Security Standards Council web site as a Validated Payment Application.

9. All individuals with access to cardholder data must attend Security Awareness training at least annually. Training should include but is not limited to the Reducing Your Digital Risk: Payment Card Industry module located in the University's AsuccessfulU catalog,

email bulletins, PCI DSS videos and on-campus seminars with updates on managing cardholder data security.

III. DEFINITIONS

Cardholder: The customer to whom a credit card or debit card has been issued or the individual authorized to use the card.

Cardholder data: All personally identifiable data about the cardholder gathered as a direct result of a credit or debit card transaction (e.g. account number, expiration date, etc.).

Card-validation code: The three-digit value printed on the signature panel of a payment card used to verify card-not-present transactions (the four-digit code located on the front of American Express cards). On a MasterCard payment card this is called CVC2. On a Visa payment card this is called CVV2.

Credit or Debit Card Receipt Transactions: Any collection of cardholder data to be used in a financial transaction whether by phone, facsimile, paper, card presentation or electronic means.

Database: A structured electronic format for organizing and maintaining information that can be easily retrieved. Simple examples of databases are table or spreadsheets.

Encryption: The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key. Use of encryption protects information from unauthorized disclosure between the encryption process and the decryption process (the inverse of encryption).

Firewall: Hardware and/or software that protect the resources of one network from users from other networks. This includes local firewalls on a computer that is handling cardholder data.

Magnetic Stripe Data (Track Data): Data encoded in the magnetic stripe used for authorization during a card present transaction.

Network: A network is defined as two or more computers connected to each other so they can share resources.

Payment Acceptance Activity Clarification form: A Treasury Operations form, with two parts, created to request a merchant ID. The requesting AU department must include the business process/purpose of the transaction for credit card acceptance.

Processor: The entity or payment gateway that processes the credit card transaction from the point of sale (AU Merchant) to the credit card issuer and ultimately to settlement in AU's depository bank.

Qualified Security Assessor: A Qualified Security Assessor (QSA) is a data security firm that has been trained and is certified by the PCI Security Standards Council to perform on-site security assessments for verification of compliance with PCI DSS.

Service Provider: A business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data.

Additional information can be found at:
https://www.pcisecuritystandards.org/security_standards/glossary.php

IV. RESPONSIBILITIES

Heads of departments and activities: Department heads are responsible for completing Part 1 of the Payment Acceptance Activity Clarification form. Additionally, documenting departmental procedures and providing appropriate training for personnel as well as ensuring that credit and debit card activities are in compliance with this policy. Departments will be responsible for any fines levied against the University that result from noncompliance by the department. Individuals tasked with handling or having access to cardholder data should have received appropriate HR in-processing background checks which include but are not limited to employment history, criminal record, credit history, and reference checks.

PCI Review Committee: The PCI Review Committee is composed of a group of AU Finance staff members appointed to review and approve departmental requests for merchant ID's. The committee will coordinate any need for QSA review.

Office of Finance & Treasurer: The Treasury Operations Office is responsible for the periodic reviews of departmental procedures and practices in connection with credit and debit card receipt transactions. Results will be reported to the Associate Vice President of Finance and Assistant Treasurer.

Office of Information Technology (OIT): The Office of Information Technology is responsible for regularly monitoring and testing the American University network. The OIT in partnership with the QSA will coordinate the University's compliance with the PCI DSS technical requirements and verify the security controls of systems authorized to process credit cards.

V. COMPLIANCE

The Associate Vice President of Finance and Assistant Treasurer may terminate credit and debit card collection privileges for any department not in compliance with this policy.

V. SIGNATURE, TITLE AND DATE OF APPROVAL

This policy needs to be signed by the appropriate officer (listed below) before it is considered approved.

This document was approved and signed by

Donald Myers
CFO, Vice President and Treasurer

on December 16, 2013