AMERICAN UNIVERSITY WASHINGTON, D.C.

University Policy: Cardholder Data Security

Policy Category: Financial Services

Subject: Protecting cardholder 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: N/A

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, student-employees, and departments 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 transactions accepted on behalf of the University's programs and activities.

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. 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.

This policy establishes a consistent and effective methodology for handling cardholder data within the University to improve cardholder security and privacy to meet PCI-DSS compliance requirements.

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, card verification value (CVV) 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). This value is known as the CVC2 on MasterCard payment cards and the CVV2 on Visa payment cards.

CDSP Confidentiality Agreement: The agreement that is required to be signed by any employee that handles credit cards or credit card information or takes part in the credit card acceptance process in any capacity. This agreement acknowledges that the employee has read and agrees to abide by the policies and procedures set forth in the Cardholder Data Security Policy.

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 (PAAC) 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.

Primary Account Number (PAN): Unique payment card number, typically for credit or debit cards, that identifies the issuer and the particular cardholder account.

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. Policy

A. General Information

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. All departments must receive prior approval from the Office of Finance and Treasurer, as described in this policy, if they want to accept, store, transmit or process cardholder data.

A department must complete a Payment Acceptance Activity Clarification (PAAC) form (located at https://myau.american.edu/finances/Controller/Pages) and submit it to Treasury Operations. This form requests the purpose and description of the business process, specific merchant detail such as card brands, required hardware, website URL, and projected dollar amount and transaction volumes for the project. Once Treasury Operations has received the PAAC form back from the department, the PCI Review Committee may conduct further review of the proposal and require additional information, if needed, for an approval to be made. For approved credit card acceptance projects, Treasury Operations will coordinate with the merchant processor to issue the new Merchant ID number for processing card transactions as well as help facilitate the implementation of the project with the department in accordance with the objectives set forth in this policy.

Due to risk management procedures at the University, if the department is to be utilizing student-employees for credit card operations, additional consideration will be required on behalf of the PCI Review Committee before a decision can be made. Please indicate on the PAAC form if student-employees will take any part in handling, accessing, processing, or refunding credit cards or credit card data as a part of the credit card procedures in your department. Students or volunteers who are not employed by American University are not approved to take part in any aspect of the credit card acceptance process.

Prior to being assigned a Merchant ID by Treasury Operations, departments must have employees taking part in the credit card process sign the CDSP Confidentiality Agreement (located at https://myau.american.edu/finances/Controller/Pages) affirming that they have reviewed the policies and procedures set forth in this policy. (This is part of the annual PCI training that must be completed by all employees who handle credit card data). Departments seeking final authorization must ensure, at approval and on an annual basis, that the PCI-DSS requirements identified in this Policy are met and being followed.

Treasury Operations will notify a department if their credit card acceptance project has been approved.

B. PCI-DSS Requirements

For approved credit card acceptance projects, departments must have in place the following requirements in their procedures and ensure that these requirements are maintained on an ongoing basis:

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

   Access to areas where cardholder data is processed must be tightly restricted through both physical and logical controls. Methods must be established to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder information is accessible. Visitors should not be permitted in areas where credit card machines are stored/used. In the rare instance it is necessary for a visitor or unauthorized user to be in the vicinity of a credit card machine, they must be accompanied by an authorized employee at all times.

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

   In the event that a vendor or business partner needs remote access to AU technology for troubleshooting purposes, the vendor's or business partner's remote access must not exceed one business day.

2. Physical security controls must be 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. Sensitive media must be transferred to offsite storage via a secure method like Iron Mountain. Please consult with the Treasury Operations office before sending any media offsite. It is essential that departments that store paper media keep inventory of all stored media and review this inventory annually.

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 IT policies.

4. Cardholder data, whether collected on paper or electronically, must be protected against unauthorized access. 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) are classified as sensitive cardholder data and are not to be stored. Receipts printed by point-of-sale terminals do not contain full card details and are permitted to be stored with access controls in place.

a. The Primary Account Number (PAN) 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, voicemail, or any other end-user messaging technologies (i.e. instant messaging, chat, SMS, etc.).

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 manually after printing or electronically before printing. It is imperative that when redacting sensitive data with a marker, one must check to ensure that the cardholder information is indeed blotted out. If a University department utilizes recurring payments, a PCI-Compliant third-party Service Provider must be used to store full-track cardholder data.

e. Any media stored (i.e. paper receipts, paper reports, faxes, etc.) must be reviewed annually to ensure that storage is secure.

5. All cardholder data must be destroyed upon authorization. (unless truncated/redacted as stated in 4d.)

   Paper documents must be cross-cut shredded. Any materials containing cardholder data must be rendered unreadable prior to discarding, scanning, imaging, or storing. Storage containers used for materials that are to be destroyed must be secured with lock and key. Retired computer drives must be erased, degaussed, or physically destroyed in accordance with the University's Records Retention and Disposal Policy.

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

   Point-of-sale 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 current version of PCI-DSS.

Treasury Operations maintains an ongoing list of details related to all devices that are a part of the AU cardholder data environment. This list is updated when any new devices are purchased, and it is reviewed for accuracy on a quarterly basis.

Point-of-sale terminal users must complete annual PCI training, which contains details regarding how to maintain proper security around credit card devices and how to check for and report potential tampering or substitution of devices. These procedures should be performed continuously by all point-of-sale terminal users. All suspicious behavior or suspected tampering of credit card devices should be reported to Treasury Operations immediately.

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

   It is incumbent on the department using a third-party provider, to execute the proper due diligence prior to engagement with the Service Provider. The Treasury Office will facilitate the audit of campus Service Provider (third-party) compliance status at least annually. Information is maintained about which PCI DSS requirements are managed by each third-party service provider and which are managed by the entity.

8. Software that is classified as a payment application such as Official Payments or Authorize.net 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. The following rules relate to the acceptable use of technology for credit card payment acceptance:

   Cellular Technology: Acceptable through the use of mobile point-of-sale machines that are provided by AU's credit card processor and connect via cellular service.

   Wireless Technology: Not permitted for credit card use at American University. If mobile payment capability is needed, please inquire about purchasing a mobile point-of-sale machine through Treasury Operations.

   Wired Network Technology: Acceptable for credit card payments that are accepted via network installed PCI compliant point-of-sale terminals.

   Portable Electronic Devices: Portable devices such as laptops, tablets, and smart phones are not permitted for University related credit card transactions.

   Network Installed Computers: Cardholder data must *never* be entered directly into a computer workstation using the computer's keyboard. Please contact Treasury Operations for alternative options that are PCI compliant.

10. All individuals with access to cardholder data must attend Security Awareness training upon hire and at least annually. Training should include but is not limited to the University's PCI Compliance Training Curriculum, email bulletins, PCI DSS videos, and on-campus seminars with updates on managing cardholder data security.

    Departments must notify Treasury Operations when any new staff members are hired that will take part in credit card processing to ensure that proper certification and education can be administered. All employees that take credit cards and their direct supervisors are required to take annual training.

C. Responsibilities & Roles For Compliance

Heads of departments: Department heads are responsible for completing the Payment Acceptance Activity Clarification form. Additionally, they must document departmental procedures, provide appropriate training for personnel, ensure that applicable employees complete the CDSP Confidentiality Agreement, and certify that credit and debit card activities follow 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 that 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 and OIT staff members appointed to review and approve departmental requests for merchant ID's. The committee will coordinate any need for QSA review. The committee reviews the Cardholder Data Security Policy on an annual basis and makes updates depending on any changes in the industry and PCI-DSS standards

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 Assistant Vice President of Treasury and the CFO, Vice President & 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.

D. Enforcement

Failure to meet the requirements outlined in this policy may result in suspension of credit and debit card collection capability for affected departments.

Any employee that violates the requirements found in this policy may result in disciplinary action up to and including termination of employment.

V. EFFECTIVE DATE AND REVISIONS

This Policy is effective July 1, 2017.

This Policy was reviewed or revised July 1, 2019.