FINANCE
CONTROLLER

December 20, 2019

Subject: Compliance Requirements for Payment Card Transactions

Purpose

The purpose of this guidance is to promote the protection of payment card transactions and cardholder data in accordance with the Payment Card Industry Data Security Standard (PCI-DSS). Credit and debit cardholder data information is regulated information that must be appropriately secured.

Requirements

University of Maryland College Park (the University) is required to be compliant with the Payment Card Industry (PCI) Data Security Standards and is committed to providing a secure environment to protect against both loss and fraud related to cardholder information. This compliance includes securely processing, storing, transmitting and disposing of credit card and debit cardholder information. Failure to comply with the PCI-DSS standards may result in fines, loss of ability to process payment cards, and reputational damage to the University. Any department that must securely store payment card information will be required to pay for the necessary security enhancements and appropriate security technology to maintain PCI compliance.

Applicability

PCI compliance requirements apply to faculty, staff, students and external entities that intend to use the University's network. Cardholder data is designated as regulated data per the Information Security Policy. University offices and members of the University community involved in processing payment card transactions are responsible for protecting such data, and for following the information security practices and policies set forth herein, including those referenced under the Related Information section below.

Governance

The PCI Governance Committee (the Committee) is responsible for arranging or approving PCI certified approved payment card acceptance services, and for approving payment card

procedures. University offices may not collect, process, store, transmit or display payment card information without advance approval from the Committee. The Committee initially includes representatives from the Office of the Controller, Division of IT, Athletics, Dining, and Transportation Services to include perspectives from both policy and practical implementation. Once the initial requirements are met, the Committee will consist of the Office of the Controller and Division of IT.

PCI-DSS Guidelines

- The Office of Student Financial Services and Cashiering is responsible for issuing all Merchant Identification accounts (MIDS).
- Do not store credit card numbers on any computer, server, or database. This includes Excel spreadsheets.
- Treat payment card receipts like you would cash.
- Keep payment card data secure and confidential.
- Restrict access to cardholder data to business need-to-know.
- Documents containing cardholder data should be kept in a secure environment (i.e. safe, locked file cabinet, etc.).
- Cardholder data must be transmitted securely (i.e. using point-to-point encryption (P2PE).
- Email, chat or instant messaging is not an approved way to transmit credit card numbers.
- Fax transmittal of cardholder data is permissible only if the receiving fax is located in a secure environment. We should eliminate the use of a FAX processing for credit cards
- Photocopies are not permitted for use to copy credit card numbers.
- Credit card receipts and supporting documentation containing card numbers should be kept for two years, but no longer.
- "Sanitize" account numbers on paper documents by using a redacting pen (Sharpie Pens are not PCI compliant) or using a (generally called cross-cut shredders) which dissect documents in two directions, leaving tiny paper fragments.
- Paper receipts should be destroyed so that account information is unreadable and cannot be reconstructed.
- Manual credit/debit card swipes or imprinters are not authorized for use.
- Technology changes that affect payment card systems are required to be approved by the PCI Governance Committee prior to being implemented.
- Any new systems/software that process payment cards are required to be approved by the PCI Governance Committee prior to being purchased.
- Computer systems that process payment cards must utilize a firewall.
- Use and regularly update antivirus software.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Assign a unique ID to each person with computer access.
- Computer systems that process payment cards must have the ability to monitor and track access to network resources and cardholder data.

- Report all suspected or known security breaches to the Controller's Office and the IT Security Office.

These guidelines apply to all payment card transactions whether conducted in person, via telephone, mail, internet, or through a university-approved third-party vendor on behalf of a unit.

Departments are required to use the following:

A. Nelnet eCommerce: exceptions need to be approved by the PCI Committee.
B. 3rd party Web systems that will keep your department's credit card process out-of-scope.
C. Point-2-Point Encryption (P2PE) technology for terminals and point of sale (POS) devices (please consult with Office of the Controller for a list of approved devices).

Responsibilities

Authorized Users and Card Processors – University offices with a business need to process payment card transactions must contact the Office of the Controller in advance of accepting any payments to obtain a merchant identification account, training, and the appropriate University-approved secure payment processing method(s).

External Users – Any University office that manages or contracts with external users, including but not limited to tenants, caterers, business establishments, volunteer organizations, or event organizers that intend to use external payment card services, must also contact the Office of the Controller to request a review and approval. The Office of the Controller and the Division of Information Technology Information Security Office will work together to ensure the external payment card service is acceptable to the University.

Terminology

- Cardholders - The individual person to whom a payment card is issued and who pays for products or services using that card
- Cardholder Data - The main data covered by PCI DSS. Consists of the PAN, cardholder name, card expiration date, and sometimes service code.
- Card Verification Code or Value – Refers to either: (1) magnetic-stripe data, or (2) printed security features
    - CAV - Card Authentication Value (JCB payment cards)
    - CVC - Card Validation Code (MasterCard payment cards)
    - CVV - Card Verification Value (Visa and Discover payment cards)
    - CSC - Card Security Code (American Express)
    - CID - Card Identification Number (American Express and Discover payment cards)
    - CAV2 - Card Authentication Value 2 (JCB payment cards)
    - CVC2 - Card Validation Code 2 (MasterCard payment cards)

    - CVV2 - Card Verification Value 2 (Visa payment cards)
- Card Brands – Credit and debit cards include, but are not limited to those issued by Visa, MasterCard, Discover, Diners Club, and American Express. *Note - The Terrapin Express Card is not a Payment Card.
- Merchant - The entity that receives payments from cardholders for products or services.
- Nelnet eCommerce - PCI compliant payment gateway utilized through Student Financial Services and Cashiering
- PAN - Acronym for "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.
- PCI - Acronym for "Payment Card Industry."
- PCI DSS - Acronym for "Payment Card Industry Data Security Standard." A standard maintained by the PCI SSC that provides controls over the environment of an organization that stores, processes or transmits cardholder data or sensitive authentication data.
- PIN - Acronym for "personal identification number." Secret numeric password is known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user-provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.
- Point-to-Point Encryption (P2PE) - is a combination of secure devices, applications, and processes that encrypt data from the point of interaction, whether it is a card swipe or dip until the data reaches the secure decryption environment.
- POS - Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.
- Primary Account Number - The card number printed on the front of the card.
- Service provider - a business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).
- Settlement - Payment of the outstanding balance owed by the issuer to the acquirer, and later the merchant.
- Cardholder Information: Any information pertaining to a credit or debit card, including but not limited to card number, cardholder name, card verification (CVC, CVV or CID) number (appearing on the back of most cards), expiration date, personal identification number (PIN), password, etc...

Effective Date: January 1, 2020

If you have any further questions, please contact pcicompliance@umd.edu