University of Maryland
Mandatory Payment Card Procedures

Payment Card Industry
Data Security Standard (PCI DSS) Version 4.0

Content

Revisions/Approvals

Ver. #	Changes Approved By	Ver. date	Reason
1.0	CH	9/2020	Compliance Requirements for Payment Card Transactions
2.0	AA	8/30/21	University of Maryland Mandatory Payment Card Procedures
3.0	AA	6/14/22	Updates to Procedures
4.0		2/7/24	Updated to include new 4.0 requirements

Annual Review

In compliance with PCI DSS requirements, this document 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 UMD Merchants.

Purpose

To establish the requirements for the acceptance and processing of credit card payments and for the protection of Cardholder Data (CHD) supplied to the University or any Third-Party Service Provider acting on behalf of the University in accordance with the Payment Card Industry Data Security Standard (PCI DSS). This document and any supporting documents mentioned herein represent the University of Maryland's mandatory procedures with respect to payment cards to:

- Prevent loss or disclosure of sensitive customer information including payment card data.
- Reduce the risks associated with the administration of payment card data by units. ● Ensure proper internal controls and compliance with PCI DSS.
- Establish requirements to protect personal information.
- Comply with federal and state laws related to securing personal information.

Scope & Applicability

The University of Maryland Mandatory Payment Card Procedures applies to all faculty, staff, students, organizations, third-party vendors, or individuals acting on behalf of the University, systems, and/or networks involved with handling CHD or can impact the security of the University's Cardholder Data Environment (CDE), including the University System of Maryland and the University of Maryland Center for Environmental Science. This includes transmission, storage, and/or processing of payment card data, in any form on behalf of University of Maryland.

Authority

The University of Maryland policies fall within a greater hierarchy of laws, statutes, and regulations. The State of Maryland allows the University of Maryland to accept payments. The State of Maryland's Treasurer's Office has delegated the authority to manage the University of Maryland to the President who has delegated PCI compliance to the Vice President of Finance and Chief Financial Officer. As a part of that management, the University must maintain and implement these Mandatory Payment Card Procedures.

Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges for the University, along with fines imposed on and damage to the reputation of the unit and the institution.

Mandatory Procedures

The University of Maryland may allow acceptance of payment cards as a method of payment for goods and services upon written approval from the University of Maryland's Payment Card Industry (PCI) Compliance Operations Committee. The University of Maryland requires all units that accept payment cards to do so only in compliance with the PCI DSS and in accordance with this document, the University of Maryland Mandatory Payment Card Procedures, and other supporting documents.

All units of the University of Maryland that receive or expect to receive payments resulting from a credit or debit card transaction must comply with these Mandatory Procedures. Furthermore, each unit must develop and maintain internal written procedures for their unit with respect to storing, processing, and transmitting cardholder data. Internal written procedures must acknowledge at minimum that:

1. Units are prohibited from using payment methods that have not been authorized by the PCI Compliance Operations Committee.
2. Units seeking contracts with third party service providers that process, transmit, store or otherwise connect to payment card information must have pre-approval from the PCI Compliance Operations Committee, and contracts must include the applicable PCI Compliance Operations Committee approved PCI language. Third parties will be required to confirm their compliance with the current version of the PCI DSS and provide an annual Attestation of Compliance signed by a Qualified Security Assessor or Internal Security Assessor (QSA). Units are required to obtain the AOC from the third party.
3. Units are prohibited from typing or entering cardholder data on behalf of the customer through the use of any workstation/laptop/iPad/smartphone/computer keyboard.
4. Units are prohibited from communicating or accepting cardholder data via email, fax, chat, social media, texting, instant messenger, or other messaging technologies.
5. Units should follow approved unit procedures for the appropriate method of responding to and securely destroying cardholder data.
6. Units with active processing equipment should maintain an updated inventory list, inspect equipment at least monthly and document log inspections. Inspection logs should be kept for at least three years in alignment with document retention policies. Units should refer to their unit PCI procedures for specific guidelines.
7. Unit procedures must be reviewed annually by the unit and the PCI Compliance Operations Committee.
8. Units must comply with annual PCI training requirements and ensure training is part of the onboarding process for new hires involved in the payment card process prior to interacting with payment cards in any capacity.
9. Units are prohibited from using a photocopier to copy cardholder data.
10. Units must adhere to the PCI DSS and UMD Cardholder Data Security Standards for all UMD network infrastructures and IT elements that are involved with the transmitting or processing of cardholder data.
11. Units are prohibited from processing credit cards using the UMD wireless network.

Units accepting payment cards will need to provide written acknowledgement of their PCI responsibilities and security requirements (PCI DSS and University of Maryland Data Security Policies) to the PCI Compliance Operations Committee as a prerequisite to accepting credit Cards as a method of payment. This agreement may be updated from time to time as requirements change. Failure to follow the requirements of the agreement may result in disciplinary action and/or criminal action including, but not limited to, revocation of the ability to accept card payments.

Purchases or rental of payment card terminals, including mobile applications, must meet PCI DSS standards.

All purchases and rentals of terminals used to process payments must be coordinated through the PCI Compliance Operations Committee – only devices and locations that have been approved and are tracked by the PCI Compliance Operations Committee may be used in any way associated with payment card processing.

Units may only accept payment card brands authorized by the State of Maryland Treasurer's Office and agree to operate in accordance with the contract(s) the State of Maryland holds with its Service Provider(s) and the Card Brands. This is to ensure that all transactions are in compliance with the Payment Card Industry Data Security Standards (PCI DSS), Federal Regulations, NACHA (National Automated Clearing House Association) rules, service provider contracts, and University of Maryland policies regarding security and privacy that pertain to credit card transactions.

All payments received must be directed into a State of Maryland approved bank account.

Accounting entries to record the receipt of the payment will be linked directly into the UMD's Kuali Financial System, whenever possible, to ensure timely recording of transactions and expedite the prompt reconciliation of general ledger and bank accounts.

Prohibited Methods of Accepting Credit Cards

Any solution not approved by the PCI Compliance Operations Committee is prohibited for accepting credit card payments. A solution includes but is not limited to terminals/devices, websites, payment gateways and Processors. ***Use of payment aggregators including, but not limited to, Stripe, Square, PayPal, or Venmo are strictly prohibited unless otherwise approved by the PCI Compliance Operations Committee.***

Payment Card Data Retention and Disposal

Units are required to establish internal controls and procedures to secure personal information. ● Retention periods must be limited to that which is required for business, legal, and/or regulatory purposes and units must have a process in place to review the need for any stored paper records on a quarterly basis. All data must be treated as confidential.

- 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.
- Units must limit access to all cardholder data to employees who require the information for completing job duties and periodically review roles to ensure data access is limited to only employees who require access to complete their job duties.
- Units should limit the recording of payment card numbers on paper to circumstances where the need to do so is unavoidable. All paper containing payment card numbers must be properly secured in a locked office, cabinet or other area that is only accessible by authorized personnel. All paper containing payment card numbers must be destroyed by the close of business, but no later than 24 hours after the payment is processed. See below for requirements on cardholder data disposal.
- Units must not store any cardholder data electronically in any format outside of the payment

processing systems that are approved by the PCI Compliance Operations Committee. ● Electronic storage of Primary Account Number (PAN) and/or Sensitive Authentication Data (SAD) even if encrypted is prohibited.

- ● Storage of sensitive authentication data (SAD) such as CVV or CSC, is never permitted and must be rendered completely unreadable immediately.
- ● After the designated retention period:

- ○ Hard-copy documentation must be crosscut shredded, incinerated, or pulped 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).

Refer to Standard for Protecting Sensitive Information (IT-4) for additional information.

Enforcement

All UMD Merchants are subject to periodic audit. Any UMD 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.

Incident Response Procedures

An incident is defined as a suspected or confirmed data compromise in which there is a potential to impact the confidentiality or integrity of payment card data. A data compromise is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted payment card data is collected, processed, stored, or transmitted.

Unit should report an actual or suspected PCI security related incident to the IT contact for their unit as soon as possible so the matter can be investigated and resolved. If an IT contact is not available, the incident should be reported to soc@umd.edu and the Division of IT's Security Operations Center will manage reporting and tracking.

Interpretations

The authority to interpret these Mandatory Payment Card Procedures rests with the UMD's PCI Compliance Operations Committee.

Exclusions

These Mandatory Payment Card Procedures should be followed at all times. If a situation arises that justifies or needs more internal discussion to determine if a one-time exception is an option, this should be discussed with the UMD's PCI Compliance Operations Committee so the situation can be reviewed***. Any and all exceptions to these Mandatory Payment Card Procedures must be approved in writing by the PCI Compliance Operations Committee (pcicompliance@umd.edu).***

Definitions

- Card Brands – American Express, Discover, JCB, MasterCard or Visa.
- Cardholder – Someone who owns and benefits from the use of a membership card, particularly a credit card.
- Cardholder Name – The name of the Cardholder to whom the card has been issued. ● 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.
- Payment Cards – Credit and debit cards issued by one of the five Card Brands. ● CAV2, CVC2, CID, or CVV2 data – The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions. ● Database – A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets. ● Disposal – CHD must be disposed of in a certain manner that renders all data unrecoverable (cross cut shredding, Incineration, or UMD approved shredding vendor or disposal service ● Expiration Date – The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
- Magnetic Stripe (i.e., track) data – Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Units may not retain full magnetic-stripe data after transaction authorization.
- Merchant – Any individual or unit that accepts credit cards bearing the logos of any of the five Card Brands as a method of payment for goods and/or services on behalf of the University. ● Merchant Department – Any department or unit (can be a group of departments or a subset of a department) which has been approved by the (institution) to accept credit cards and has been assigned a Merchant identification number.
- MID – Merchant ID - Unique ID associated with each UMD 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 – 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 Point of Contact – An individual within the department who has primary authority and responsibility within that department for credit card transactions.
- PIN/PIN block Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message. ● PCI DSS – Payment Card Industry Data Security Standard – 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. The Standard is an information security standard for organizations that handle branded credit cards from the major card brands: VISA, MasterCard, Discover, American Express and JCB. It is mandated by the card brands but administered by the Payment Card Industry Security Standards Council (PCI SSC). https://www.pcisecuritystandards.org

- PCI SSC – Payment Card Industry Security Standards Council made up of five Card Brand members that set the standards to enhance CHD security.

- 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 payment card information (credit and/or debit) on behalf of the University of Maryland, or that provides services that control or could impact the security of the CDE. A third party can include any vendor, contractor, or business partner.
- Units – Schools, divisions, academic departments, non-academic units, etc. that are accepting credit card payments in the name of the University of Maryland.

Supporting Documents

UMD Cardholder Data Security Standards
Standard for Configuration of Routers and Firewalls on Networks Processing Cardholder Data (IT 6)
Standard for Vendor Supplied Defaults & Parameters on Networks Processing Cardholder Data (IT-7)
Standard for Protection of Cardholder Data (IT-8)
Standard for Encrypted Transmission of Cardholder Data (IT-9)
Standard for Managing Vulnerabilities within Networks Processing Cardholder Data (IT-10) Standard for Access Control on Networks Processing Cardholder Data (IT-11)
Standard for Monitoring of Networks Processing Cardholder Data (IT-12)
Standard for Testing of Networks Processing Cardholder Data (IT-13)
UMD Data Classification Standards
Sending Credit Card Information Over Email FAQ
Payment Card Industry Compliance

Card Brand Rules

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