University of Maryland

Mandatory Payment Card Procedures

Payment Card Industry
Data Security Standard (PCI DSS) Version 3.2
Content

Revisions/Approvals  1

Purpose  2

   PCI DSS  2
   Visa Cardholder Information Security Plan (CISP)  2
   MasterCard Site Data Protection Program (SDP)  2

Scope/Applicability  2

Authority  3

Mandatory Procedures  3

Payment Card Data Retention and Disposal  4

Interpretations  5

Exclusions  5

Glossary  6

Revisions/Approvals

<table>
<thead>
<tr>
<th>Ver. #</th>
<th>Changes By</th>
<th>Ver. date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>CH</td>
<td>9/2020</td>
<td>Compliance Requirements for Payment Card Transactions</td>
</tr>
<tr>
<td>2.0</td>
<td>AA</td>
<td>8/30/21</td>
<td>University of Maryland Mandatory Payment Card Procedures</td>
</tr>
</tbody>
</table>

Confidential
Property of University of Maryland
Purpose

This document and additional supporting documents represent University of Maryland’s mandatory procedures with respect to payment cards:

- To prevent loss or disclosure of sensitive customer information including payment card data. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the unit and the institution.
- To reduce the risks associated with the administration of payment cards by units.
- To ensure proper internal controls and compliance with Payment Card Industry Data Security Standards (PCI DSS).
- To establish requirements to protect personal information.
- To comply with federal and state laws related to securing personal information.

PCI DSS

The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org).

In order to accept credit card payments, the University of Maryland must prove and maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS). The University of Maryland Mandatory Payment Card Procedures and additional supporting documents provide the requirements for processing, transmission, storage, and disposal of cardholder data transactions. This is done in order to reduce the institutional risk associated with the administration of credit card payments by individual units and to ensure proper internal control and compliance with the PCI DSS.

Visa Cardholder Information Security Plan (CISP)

Visa Inc. instituted the Cardholder Information Security Program (CISP) in June 2001. CISP is intended to protect Visa cardholder data - wherever it resides - ensuring that members, merchants, and service providers maintain the highest information security standard. In 2004, the CISP requirements were incorporated into the PCI DSS.

MasterCard Site Data Protection Program (SDP)

The SDP Program, with the PCI DSS as its foundation, details the data security and compliance validation requirements in place to protect stored and transmitted MasterCard payment account data.

Scope/Applicability

The University of Maryland Mandatory Payment Card Procedures applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems, and networks involved with payment card handling, 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 is allowing 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 or designee. As a part of that management, the University will develop and implement the Mandatory Payment Card Procedures.

Mandatory Procedures

It is the belief of the University of Maryland to allow acceptance of payment cards as a form 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 card transaction must comply with the Mandatory Payment Card Procedures issued by the PCI Compliance Operations Committee. Furthermore, each unit must develop formal, written procedures with respect to storing, processing, and transmitting credit cards for their unit. At a minimum:

- Unit procedures need to be reviewed annually by the unit and the PCI Compliance Operations Committee.
- Units are prohibited to enter cardholder data on behalf of the customer through the use of any workstation/laptop/iPad/computer keyboard.
- Units are prohibited from communicating or accepting cardholder data via email, fax, chat, social media, texting, instant messenger, or other messaging technologies.
- Units should follow approved unit procedures for the appropriate method of responding to and securely destroying cardholder data.
- Units are prohibited from using payment methods that have not been authorized by the PCI Compliance Operations Committee.
- Units with active processing equipment should inspect equipment at least monthly and log inspections. Units should refer to their unit PCI procedures for specific guidelines.
- Units seeking contracts with third party service providers that process, transmit or store payment card information must have pre-approval from the PCI Compliance Operations Committee, and contracts must include the applicable 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.
- Units should comply with annual PCI training requirements.
- Units are prohibited from using a photocopier to copy cardholder data.
- Units must adhere to the UMD Cardholder Data Security Standards for all UMD network infrastructures and IT elements that are involved with the transmitting or processing of cardholder data.
- 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. 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.

Purchase or rental of payment card terminals, including mobile applications, must be coordinated through the PCI Compliance Operations Committee – only devices and locations that have been approved and tracked by the PCI Compliance Operations Committee may be used in any way associated with payment card processing. All devices must meet PCI DSS standards.

Units must accept only 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.

**Payment Card Data Retention and Disposal**

Units are required to establish internal controls and procedures to secure personal information.

- Units should limit data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. All data will be treated as confidential.
- Units should 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 not store cardholder data electronically in any format.
- 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.

CHD and sensitive information must be disposed of in such a manner as to ensure it cannot be retrieved and recovered by unauthorized persons. Physical documents containing sensitive information must be cross-cut shredded prior to disposal. Refer to [Standard for Protecting Sensitive Information (IT-4)](https://example.com) for additional information.

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.

Any and all exceptions to these Mandatory Payment Card Procedures must be approved in writing by the PCI Compliance Operations Committee (pcicompliance@umd.edu).
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.
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardholder</td>
<td>Someone who owns and benefits from the use of a membership card, particularly a credit card.</td>
</tr>
<tr>
<td>Cardholder Data (CHD)</td>
<td>Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.</td>
</tr>
<tr>
<td>Cardholder Name</td>
<td>The name of the Cardholder to whom the card has been issued.</td>
</tr>
<tr>
<td>CAV2, CVC2, CID, or CVV2 data</td>
<td>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.</td>
</tr>
<tr>
<td>Database</td>
<td>A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets.</td>
</tr>
<tr>
<td>Disposal</td>
<td>CHD must be disposed of in a certain manner that renders all data unrecoverable. Cross-cut shredding, Incineration, approved shredding or disposal service</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.</td>
</tr>
<tr>
<td>Magnetic Stripe (i.e., track) data</td>
<td>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.</td>
</tr>
<tr>
<td>Merchant Department</td>
<td>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.</td>
</tr>
<tr>
<td>Payment Card Industry Data Security Standards (PCI DSS)</td>
<td>The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands: Visa, MasterCard, American Express, Discover, JCB</td>
</tr>
<tr>
<td>PCI Point of Contact</td>
<td>An individual within the department who has primary authority and responsibility within that department for credit card transactions.</td>
</tr>
<tr>
<td>PIN/PIN block</td>
<td>Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.</td>
</tr>
<tr>
<td><strong>Primary Account Number (PAN)</strong></td>
<td>Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Sensitive Authentication Data</strong></td>
<td>Additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.</td>
</tr>
<tr>
<td><strong>Service Code</strong></td>
<td>The service code that permits where the card is used and for what.</td>
</tr>
<tr>
<td><strong>Third Party</strong></td>
<td>A third party can include any vendor, contractor, and business partner who processes, transmits or stores payment card information (credit and/or debit) on behalf of the University of Maryland, or that could affect the security of cardholder data.</td>
</tr>
<tr>
<td><strong>Units</strong></td>
<td>Schools, divisions, academic departments, non-academic units, etc. that are accepting credit card payments in the name of the University of Maryland</td>
</tr>
</tbody>
</table>