Western Michigan University
Payment Card Policies and Procedures

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

Purpose ................................................................. 2
PCI DSS ........................................................................ 2
Visa Cardholder Information Security Plan (CISP) .............................................. 2
MasterCard Site Data Protection Program (SDP) .................................................. 2
Scope/Applicability ............................................................ 2
Policy ........................................................................... 3
Procedures ...................................................................... 4
Card Acceptance and Handling ........................................................................ 4
Payment Card Data Security ........................................................................... 5
  Processing and Collection ........................................................................... 5
  Storage and Destruction ............................................................................ 5
Risk Assessment ......................................................................................... 6
Incident Response ....................................................................................... 6
Policy and Training ...................................................................................... 6
Sanctions ................................................................................................. 6
Supporting Documents ................................................................................ 7
Glossary ..................................................................................... 7

Confidential Property of Western Michigan University © 2017
Purpose
This document and additional supporting documents represents Western Michigan University’s policy 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.

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, Western Michigan University must prove and maintain compliance with the Payment Card Industry Data Security Standards. The Western Michigan University’s Payment Card Policy 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 departments and to ensure proper internal control and compliance with the Payment Card Industry Data Security Standard (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 Payment Card Industry Data Security Standard (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 Western Michigan University Payment Cards Policy applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of Western Michigan University.
Policy

It is the policy of Western Michigan University to allow acceptance of payment cards as a form of payment for goods and services upon written approval from the Office of the Vice President of Business and Finance. Western Michigan University requires all departments that accept payment cards to do so only in compliance with the PCI DSS and in accordance with this policy document, the Western Michigan University payment card procedures, and other supporting documents.

Merchant requests should be forwarded to the Cashiering Office for final approval and implementation. Entities accepting payment cards will acknowledge their responsibilities, as well as the security requirements (Payment Card Industry Data Security Standard and institutional Data Security Policies) that must be followed. Failure to follow the requirements of the agreement may result in the revocation of your ability to accept card payments.

Entities must accept only payment cards authorized by the Cashiering Office and agree to operate in accordance with the contract(s) Western Michigan University 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 rules, service provider contracts, and Western Michigan University policies regarding security and privacy that pertain to electronic transactions. Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
- Data that is not absolutely necessary in order to conduct business will not be retained in any format. All data will be treated as confidential.
- Specific retention requirements for cardholder data
- Processes for secure deletion of data when no longer needed
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.
- Physical access to data records is restricted to staff with a need to know.

Cardholder data (CHD) received via end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is never to be used to process a payment. Follow approved departmental procedures for the appropriate method of responding to and securely destroying the cardholder data.

All Processing Equipment is to be obtained via the Cashiering Office. Exceptions to this policy will be limited and will require a justification (including reason why the available central processing systems will not work for your area) to be submitted and approved by the PCI Committee and the Office of the Vice President for Business and Finance in advance of any equipment or system purchase.
All payments received must be directed into a Western Michigan University Approved Bank Account. The type and nature of the electronic transaction (e.g., ACH, Credit Card, Point of Purchase, wire, etc.) will dictate where the transaction will be deposited. Accounting entries to record the receipt of the payment will be linked directly into the university’s general ledger system (GLOW) whenever possible, to ensure timely recording of transactions and expedite the prompt reconciliation of general ledger and bank accounts.

**Procedures**

In the course of doing business at Western Michigan University, including affiliated organizations, it may be necessary for a department or other unit to accept payment cards. Western Michigan University requires all departments that accept payment cards to do so only in accordance with PCI DSS and the following procedures.

**1. Card Acceptance and Handling**

The opening of a new merchant account for the purpose of accepting and processing payment cards is done on a case by case basis. Any fees associated with the acceptance of the payment card in that department could be charged to the individual merchant.

1. Interested departments or merchants should contact Liana Fox and/or the Cashiering Office to begin the process of accepting payment cards. Steps include:
   1.1. Completion of an “Application to become a Merchant Department”
   1.1.2. Completion of training
   1.1.3. Review and acknowledgement of the “Western Michigan University Payment Card Policies and Procedures”, including proof of ongoing compliance with all requirements of the policy

1.2. Any department accepting payment cards on behalf of the institution or related foundation must designate an individual within the department who will have primary authority and responsibility within that department for payment card transactions. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the primary is unavailable.

1.3. Specific details regarding processing and reconciliation will depend on the method of payment card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and are also available by contacting the Cashiering Office.

1.4. All service providers and third party vendors providing payment card services must be PCI DSS compliant. Departments who contract with third-party service providers must maintain a list that documents all service providers and:
   1.4.1. Ensure contracts include language stating that the service provider or third party vendor is PCI complaint and will protect all cardholder data.
   1.4.2. Annually audit the PCI compliance status of all service providers and third-party vendors. A lapse in PCI compliance could result in the termination of the relationship.
2. Payment Card Data Security

All departments authorized to accept payment card transactions must have their card handling procedures documented and made available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

**PROCESSING AND COLLECTION**

2.1. Access to cardholder data (CHD) is restricted to only those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access to CHD and review the list annually to ensure that the list reflects the most current access needed and granted.

2.2. Equipment used to collect cardholder data is secured against unauthorized use or tampering in accordance with the PCI DSS. This includes the following:
   - 2.2.1. Maintaining an inventory/list of devices and their location;
   - 2.2.2. Periodically inspecting the devices to check for tampering or substitution;
   - 2.2.3. Training for all personnel to be aware of suspicious behavior and reporting procedures in the event of suspected tampering or substitution.

2.3. Email must never be used to transmit payment card or personal payment information, nor should it be accepted as a method to supply such information. In the event that it does occur, disposal as outlined below is critical. If payment card data is received in an email then:
   - 2.3.1. The email should be replied to immediately with the payment card number deleted stating that “Western Michigan University does not accept payment card data via email as it is not a secure method of transmitting cardholder data”.
   - 2.3.2. Provide a list of the alternate, compliant option(s) for payment.
   - 2.3.3. Delete the email from your inbox and also delete it from your email Trash.

2.4. Fax machines used to transmit payment card information to a merchant department must be standalone machines with appropriate physical security; receipt or transmission of payment card data using a multi-function fax machine is not permitted.

**STORAGE AND DESTRUCTION**

2.5. Cardholder data, whether collected on paper or electronically, is protected against unauthorized access.

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

2.7. No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe, or the card validation code.

2.8. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants, and portable external hard drives.

2.9. Cardholder data should not be retained any longer than that defined by a legitimate business need. CHD must be destroyed immediately following the required retention period using a PCI DSS-approved method of destruction. A
regular schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the required retention period.

3. Risk Assessment
Implement a formal risk assessment process in which current threats and vulnerabilities to the institution’s network and processing environment, including staff, are analyzed. Risk assessments must be conducted annually. Information Technology should conduct the risk assessment of the infrastructure and threats; departments that accept payment cards should also conduct an assessment of their physical environments and assess risks to the payment environment. Address all threats with mitigation tasks, timelines and/or acceptance statements. Prepare and maintain documented output from the risk assessment exercise(s).

4. Incident Response
In the event of a breach or suspected breach of security, the department or unit must immediately execute the Western Michigan University Information Security Incident Response Plan [http://wmich.edu/it/policies/incidentresponse](http://wmich.edu/it/policies/incidentresponse). The plan must include notifications, staff requirements, and handling procedures. If the suspected activity involves computers (hacking, unauthorized access, etc.), immediately notify OIT Help Desk. The Incident Response Plan should be reviewed and tested at least annually.

5. Policy and Training
Ensure policy and procedure documentation governing cardholder data exists and that it covers the entirety of the PCI DSS. Document users’ acknowledgement of understanding and compliance with all policies and procedures annually. Ensure training on the PCI DSS and overall information security is provided to all staff members with access to cardholder data and/or the processing environment upon hire, and at least annually thereafter.

6. Sanctions
Failure to meet the requirements outlined in this policy may result in suspension of the physical and, if appropriate, electronic payment capability for the affected merchant(s). In the event of a breach or a PCI violation the payment card brands may assess penalties to the Institution’s bank which will likely then be passed on to the Institution. Any fines and assessments imposed will be the responsibility of the impacted merchant. A one-time penalty of up to $500,000 per card brand per breach can be assessed as well as on-going monthly penalties.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment and any legal action. Some violations may constitute criminal offenses under local, state, or federal laws. Western Michigan University will carry out its responsibility to report such violations to the appropriate authorities.
Other Supporting Documents

- **Link to be added at a later date** - Appendix 1 - PCI Payment Card Security Incident Response Plan
- **Link to be added at a later date** - Appendix 2 - PCI Application for New Payment Card Merchants
- **Link to be added at a later date** - Appendix 3 - PCI Annual Merchant Survey
- **Link to be added at a later date** - Appendix 4 - PCI Payment Card Best Practices

Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>Cardholder</td>
<td>Someone who owns and benefits from the use of a membership card, particularly a credit card.</td>
</tr>
<tr>
<td>Card Holder 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>Primary Account Number (PAN)</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>Cardholder Name</td>
<td>The name of the Cardholder to whom the card has been issued.</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>Service Code</td>
<td>The service code that permits where the card is used and for what.</td>
</tr>
<tr>
<td>Sensitive Authentication Data</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>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. Entities may not retain full magnetic-stripe data after transaction authorization.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------</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-present 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>Disposal</td>
<td>CHD must be disposed of in a certain manner that renders all data unrecoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices, (Before disposal or repurposing, computer drives should be sanitized in accordance with Western Michigan University’s Electronic Data Disposal Policy). The approved disposal methods are: • Cross-cut shredding, Incineration, Approved shredding or disposal service</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 Cashiering Office to accept credit cards and has been assigned a Merchant identification number.</td>
</tr>
<tr>
<td>Merchant Department Responsible Person (MDRP)</td>
<td>An individual within the department who has primary authority and responsibility within that department for credit card 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>
</tbody>
</table>