MERCY UNIVERSITY

Policy Name:	Payment Card Industry Data Security Standards (PCI DSS) Policy		
Associated Form(s):	N/A	**Policy Number**:	2020-12
Reviewed:	Non-Academic Policy Review Committee	**Approved:**	December 22, 2020
Approval Authority:	President Timothy L. Hall	**Adopted:**	December 23, 2020
Responsible Executive(s):	1. Chief Information Officer 2. Director, Internal Audit	**Revised:**	N/A
Responsible Office(s):	1. Information Technology 2. Internal Audit	**Contact(s):**	1.Director of IT 2. Director of Internal Audit

I. Purpose of this Policy

This policy provides information to ensure compliance by Mercy University (the "University") with the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS is a set of comprehensive requirements for enhancing payment account data security, developed by the founding payment brands of the PCI Security Standards Council (PCI SSC) – American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. This policy represents the University's commitment to complying with PCI DSS to prevent loss or disclosure of cardholder information. Further details about PCI can be found at the PCI Security Standards Council Web Site https://www.pcisecuritystandards.org/

Questions regarding this policy should be directed to the Director, Internal Audit.

II. Reason for the Policy

The reason of this policy is to protect cardholder information of students, parents, donors, alumni, customers, and any other individual or system and network, that utilizes a credit card to transact business with the University. Cardholder information includes primary account numbers (PAN), cardholder name, expiration data, service code, and authentication code.

III. Requirements

To accept credit card payments, the University must prove and maintain compliance with PCI DSS. This policy provides the requirements for processing, transmitting, storage and disposal of cardholder data of payment card transactions, to reduce the institutional risk associated with the administration of credit card payments and to ensure proper internal controls are in place.

The University requires all merchants (i.e., University department) that accept payment card payments to do so only in compliance with PCI DSS and this policy and procedures. No student organizations or clubs can be merchants. If a student organization or club is seeking to charge for a good or service, please reach out to Assistant Dean of Student Affairs for assistance. All money collected from fundraisers or dues must be deposited directly into a University account. No organizational money should ever be deposited into a personal banking account.

All University merchants are prohibited from accepting funds via PayPal, Venmo, Square or other methods which requires funds to flow through a personal bank account(s).

PCI compliance is an ongoing daily process activity, not a one-time event. All employees, who in any manner, is part of the acceptance of cardholder data, will be required to be complete annual training and sign a PCI Security Awareness Training & Confidentiality Agreement.

IV. Merchant Responsibilities

A merchant is defined as a campus unit or department that accepts credit and debit payment cards as payment for goods, services, information, or gifts. There may be one or more employees, referred to as Merchant Department Responsible Persons (MDRP) (refer to Section 5), within a merchant that is responsible for accepting payment.

Merchant responsibilities are as follows:

- All merchants must follow the PCI DSS standards and this policy.
- All merchants are prohibited from accepting funds via PayPal, Venmo, Square or other methods which requires funds to flow through a personal bank account.
- No merchant accepting payment cards will store cardholder data, whether in hard copy or electronic format.
- All payment devices that process credit cards must be stored in a locked space with limited access when not in use. To the extent possible, they should only be accessible to the MDRP's.
- University IT infrastructure will have up-to-date security measures in firewall configurations, network administration, and other areas that could affect PCI compliance.
- MDRP's must keep a monthly log certifying the results of their inspection of any signs of tampering with terminals/devices.

V. Merchant Department Responsible Person (MDRP) Duties

Any merchant accepting payment card and/or electronic payments on behalf of the University for gifts, goods or services must designate an individual (staff or faculty member) within that department who will have primary authority and responsibility for e-commerce and payment card transaction processing, transmitting, storage and disposal on behalf of the University. This individual(s) is referred to as the Merchant Department Responsible Person (MDRP). All MDRP's will be trained upon hire, complete annual training and must sign the PCI Security Awareness Training & Confidentiality Agreement prior to performing that work.

1.1. TRANSMITTING CHECKLIST

- Payment cards may be accepted in the following manner:
  - In-person with physical credit card present.
  - Hard-copy postal mail.
  - On-line payments hosted by a third-party organization such as CashNet, Blackbaud Merchant Services or Blackboard Transact.
  - Over the phone – If a cardholder requests an employee to enter in the cardholder number on their behalf, first have the MDRP suggest making the payment online by the cardholder. If they are having difficulty suggest using a different browser, different credit card or restarting their computer. In the rare instance that a credit card number has to be entered by an MDRP, please use extra caution in not writing

the number down before entering it online or repeating the number back to them. In all situations, have the cardholder repeat the payment information to you.

- Payment cards *may not* be accepted in the following manner:
  - In an email, text message, chat box or fax. If received in any of these fashions, dispose of the information immediately and let the individual know that payment cannot be accepted in that fashion.
- MDRP's must maintain strict control over the internal and external distribution of any kind of media that contains cardholder data.
- Material sent to constituents with a designated area for written cardholder data, to be returned to the University, must be handled safely and appropriately destroyed, after business use. (Every effort should be made to eliminate the area for written cardholder data on appeals, instead noting a secure means to make a credit card payment on a secure online form or by check).
- In the rare instance that an agent of the University is offered payment card information during an off-site visit, the agent will direct the constituent to the online site to make payment. If that is not possible, a transmittal form can be filled out, properly secured by the agent, and returned to the appropriate MDRP immediately.

1.2. PROCESSING CHECKLIST

- Cardholder data received for manual processing (mail, hand delivered) must be processed on the same day it is received, or no more than one business day later. Cardholder data in written form must be disposed of immediately after the business purpose has been served.
- Physical security controls must be in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents or electronic files containing card holder data.
- If cardholder data must be shared, only for a business purpose, mask the primary account number (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed).

1.3. STORAGE CHECKLIST

- The University does not store authorized cardholder data in hardcopy or electronic form in any of its online systems, or portable devices such as flash drives, phones, laptops, iPads and such or physically in hard copy format. Any prior cardholder data authorization forms, or hard copies or soft copies, that have been stored, must be disposed off immediately.
- Cardholder data that has been collected but has not yet been processed, in addition to mail that has been received, must be stored in a secure location (i.e., locked room or cabinet).

1.4. DISPOSAL CHECKLIST

Cardholder data must be disposed of in a certain manner that renders all data unrecoverable. This includes hard copy documents and any electronic media including computers, hard drives, magnetic tapes and USB storage devices.

- The approved methods of disposal for hardcopy media is crosscut shredding or placing it in secure shred boxes around campus.
- The approved methods of disposal for electronic media is a secure wipe program, industry accepted standards for secure deletion or physically destroying the media until its is deemed unrecoverable.

2. SECURITY PROGRAM TRAINING AND ATTESTATION

All MDRP's with physical and logical access to cardholder data at the University, whether employees, third-parties, contractors, temporary employees, and/or other staff members, etc. must be trained on their role in safeguarding cardholder data, at the time of hiring and annually. MDRP's must be trained on device tampering. Common methods of tampering are adding card skimmer hardware to a swipe machine, unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings. Training should cover how to verify someone claiming to be a service or repair person before allowing them access to processing or swiping devices, not installing, or replacing devices without verification first, being wary of suspicious behavior such as unknown persons unplugging or opening devices, and reporting suspicious behavior or device tampering to the correct personnel.

Along with required training, MDRP's must read this policy and sign the PCI Security Awareness Training & Confidentiality Agreement, attesting to have received annual training and reading the policy. The Agreements will be managed and maintained by Internal Audit.

It will be the responsibility of each merchant to inform Internal Audit of any changes to the MDRP's in their departments.

3. CONTROLS AND AUDITS PERFORMED BY IT, MERCHANT, AND INTERNAL AUDIT

The University will maintain an up-to-date inventory of all devices that capture payment card data. The University will protect card present processing devices from being tampered with or being substituted:

- IT will maintain a list of all devices that capture card data (IP address, make, model, serial number or asset tag number and location of device) and ensure that the list of devices is updated when devices are added, relocated, or decommissioned. Also, IT will ensure that all Point of Sale (POS) devices have updated patches and antivirus with up to date logging.

- IT will verify and collect PCI DSS Compliance Certificates or PA-DSS Validation Certificate (POS systems) on all service providers within the relevant Merchant Department on an annual basis.
- Each merchant will physically secure all devices that capture payment card data. MDRP's must perform a monthly visual inspection of devices to ensure that nothing appears tampered with or damaged and keep a log of the inspection results. Examples of signs that a devise might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, changes to the serial number or other external markings.
- A yearly physical inspection of devices will be performed, documented, and retained by Internal Audit. Internal Audit will also collect and maintain the annual PCI Security Awareness Training & Confidentiality Agreement, to be completed annually by each MDRP.

4. SECURITY BREACH

An "incident" is defined as a suspected or confirmed data compromise. A data compromise is any situation where there has been unauthorized access to a system or network were prohibited, confidential or restricted data is collected, processed, stored, or transmitted; payment card data is prohibited data. A data compromise can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.

Information Security Incident Types:

- Accident: An incident with nonhuman natural causes, such as weather or mechanical failure. This includes power outages, fire, floods, hardware failure, and similar events.
- Error: An incident caused by a human because of a mismatch between the intended and the effective results of a task.
- Lost / Stolen / Not Returned: An incident where an asset is unaccounted for. This includes missing computing devices, storage media, or other information assets including non-electronic information assets such as paper reports.
- Unauthorized Access: An incident where an individual gains logical or physical access without permission to a network, system, application, data, or other resource.
- Denial of Service: An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This category includes both being the victim of and participating in the DoS.
- Malicious Code: An incident with successful installation of malicious software such as virus, worm, Trojan horse, or other code based malicious entity that infects an operating system or application. This does NOT include malicious software that has been successfully quarantined by antimalware software.

- Improper Usage: An incident where a person violates acceptable computing use policies. This category includes DMCA violations.
- Scans/Probes/Attempted Access: An incident with any activity that seeks to access or identify a system, open ports, protocols, service, or any combination for later exploit. This activity does not result in a compromise or denial of service.
- Investigation: Used to track unconfirmed incidents that are potentially malicious or anomalous and are deemed by the reporting individual to warrant further review.
- Exercise / Network Defense Testing: An incident caused by exercises and approved testing of internal or external information system defenses. This includes information security assessments, vulnerability scans, penetration tests, or similar activities.

Common indicators of data breaches are as follows:

- Unsuccessful logon attempts.
- Unexplained modifications or deletion of data.
- System crashes.
- Poor system performance.
- Anti-virus programs malfunctioning or becoming disabled suddenly.

In the event of a breach or suspected breach of security immediately reach out to your supervisor and the **Mercy University Helpdesk 914-674-7526** and/or Chief Information Officer (CIO). Additionally, the following steps should be taken:

1) Do not log onto the machine.
2) Do not change passwords.
3) Do not modify systems files
4) Do not switch the suspected compromised device off.
5) Do unplug the machine from a network connection cable, if the ability to do so exists.
6) Be on high alert and monitor all e-commerce applications.

Please establish an incident log and record all actions related to the incident with accurate date, time, and details of actions performed; This includes:

a. Access to system(s) by Employees to determine whether an incident occurred (who performed the tasks, exactly what actions were taken, what account[s] were used, etc.)
b. Any software utilized to perform any analysis or troubleshooting
c. Any communications with any individual or organization regarding the incident
d. Any steps taken to secure the affected device(s) and establish and maintain a chain of custody to preserve evidence

5. INCIDENT RESPONSE PLAN

One of the guidelines from the PCI Security Standards is that the University create a Security Incident Response Team and document an incident response plan (PCI IRP).

The Response Team consist of CIO, CFO, Internal Audit and Security personnel in Information Technology Department including and not limited to *Dir, Technical Services; Dir, of IT; Dir, Digital Technologies*

The PCI IRP is:

1) MDRP immediately notifies Supervisor of any suspected or confirmed breach.
2) Supervisor makes determination and immediately informs IT Helpdesk and CIO.
3) Information Technology will investigate to determine if breach occurred.
4) Information Technology will notify the Response Team if a breach has occurred.
5) Response team will notify payment brands (MasterCard, Visa, JB, Discover and American Express) in the event of a compromise.
6) The Response Team will resolve the problem to the satisfaction of all parties involved.
7) The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future.

Please refer to Mercy University Incident Management Plan for detailed steps.

6. SERVICE PROVIDERS

IT Security maintains a list of service providers and the services that they provide. In the agreement with the service providers, it states that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the University. IT will validate, annually, that all service providers are PCI compliant.

Appendix:

BEST PRACTICES FOR MERCHANTS ACCEPTING PAYMENT CARDS

We understand that complying with PCI DSS may be difficult and confusing for some departments. If you have identified a business need that requires you to accept credit/debit card payments, we recommend that you review this set of high-level best practices:

1) If you don't need it, don't store it!
   - Many offices retain cardholder data (CHD) "just because". This includes paper and forms. Once the transaction has been processed, destroy the CHD on the form. This may require a redesign of your departmental form to save other relevant information that may be needed – consider moving the CHD to the bottom where it can be properly removed and shredded, while maintaining the other information.
2) Do not just ball it, destroy it!
   - Balling up a hardcopy document with CHD and tossing it into the garbage or recycling bin is not considered appropriate disposal of CHD. The proper way to destroy is to put it into a crosscut type shredder or a or placing it in secure (locked) shred boxes.
3) "Self-help" customer service is the right choice!
   - Many merchants at the University use third party payment systems, like CashNet and Blackboard, to help facilitate online payments. Many times, if a cardholder has a tough time entering their payment online, they may ask for assistance via a phone call, email, etc. As much as possible, we should try not to enter credit card information on behalf of the cardholder. In the rare instance that a credit card number must be entered by an MDRP, please use extra caution in not writing the number down before entering it online or repeating the number back to them. In all situations, have the cardholder repeat the payment information to you.
4) Clean desk policy
   - Don't leave any CHDout in the open, on your desk or anywhere it is easily accessible by a non-authorized person. At the end of the night, and temporarily being away from your desk, it is always your responsibility and duty to safeguard CHD.
5) Electronic storage of CHD
   - Do not copy or type CHD, even temporarily, onto spreadsheets or other programs. Even if you don't save the document, an image or file of the data is stored on the hard drive.
6) Never email CHD!
   - Employees should never use email as a manner of transmitting CHD
   - Should a customer email their credit card information, reply to the sender, deleting the CHD and say "for their protection and the protection of Mercy University, policies dictate that credit card information shall not be accepted via email. Please use one of our accepted method of processing your information (in-person or online)".
7) Don't let unauthorized personnel access to confidential CHD or access to payment processing devices.

8) Document desk procedures

- Write out what your procedures are in the role of handling confidential data. Include such items as receipt or processing procedures, disposition, and destruction of CHD. Storage and transfer of forms to other offices.