Montana State University

Effective Date: April 5, 2017

Review Date: April 5, 2020

Updated Date:

Payment Card Industry (PCI) Data Security Program and Standard

Brief Description:

To ensure campus compliance with the Payment Card Industry Data Security Standard (PCI-DSS)

Introduction:

The purpose of this program is to ensure that payment card (credit card) and ecommerce activities are consistent, efficient, and secure to protect the interests of the University and its customers. This standard provides guidance to ensure that campus credit card acceptance and ecommerce processes comply with the Payment Card Industry Data Security Standard (PCI DSS) and are appropriately integrated with the University's financial and other systems.

Scope:

This policy applies to Montana State University as well as its self-supporting operations, contractors, consultants, or agents who, in the course of doing business on behalf of the University, accept, process, transmit, store, or otherwise handle cardholder information in physical or electronic form. This policy also applies to all Montana State University organizations that accept process, transmit, store, or otherwise handle cardholder information in physical or electronic form. This policy applies to all types of credit card activity transacted in person, over the phone, via fax, mail, or the internet. System and device functionalities established for credit card data activities of the university may be used only for credit card data activities of the university, not for personal use.

PCI Security Standards

PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process, or transmit data, are mandatory for their respective stakeholders, and are enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and VISA Inc.

- PCI Data Security Standard: The PCI DSS applies to any entity that captures, stores, processes, or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. Any business activity that accepts or processes payment cards must comply with the PCI DSS.
- PCI Data Security Standard for Merchants and Processors: The PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards. It presents steps that appeal to common sense and mirror best security practices.

Operating Principles

The following operating principles must be used by departments when accepting credit card information in order to process payments for services, purchases, registration, etc.

- All merchant sites and merchant card processors must be authorized and approved by University Business Services**.** This includes approval of the written agreement with the service provider. A written agreement must be made with each service provider.
- Such authorization is required for new credit card acceptance channels / merchant accounts, and any addition or change to an existing channel/account including, but not limited to, the:
    - use of existing credit card acceptance channels / merchant accounts for new purposes
    - alteration of business processes that involve payment card processing activities
    - addition or alteration of payment systems or technologies
    - addition or alterations of relationships with third-party payment card service providers
- All merchant card services offered by the University must be delivered using software, systems, and procedures that are compliant with applicable standards.
- When processing credit card transactions, only the minimum amount of information necessary to verify the identity of the cardholder and the legitimacy of the cardholder authorization should be gathered. For example, manual requests to process a customer's credit or debit card may contain the following elements:
    - Properly signed/executed authorization from the cardholder (unless processing over the telephone as provided for in NACHA guidance on TEL transactions)
    - Credit/debit card account number with expiration date
    - The cardholder's correct billing address
    - Authorization codes (Card Identification Number), if the cardholder is not physically present

Credit Card Merchant Numbers

- All credit card merchant ID numbers must be obtained from University Business Services. Revenue-generating departments are prohibited from obtaining merchant ID numbers directly from the credit card companies or processors.
- Departments must use only University Business Services approved third-party providers to ensure PCI compliance.

Credit Card Acceptance Channels

- Credit card information can be accepted through a Montana State University authorized web application, by telephone, or in person only.
- Credit card information cannot be accepted via email (or similar messaging system), fax, voicemail and should never be emailed from the department.
- If data must be written down, use the standard credit card authorization form found on the University Business Services website under PCI. Print this form out on bright paper, so that staff will know what it is by color.
- Departments are not permitted to capture, transmit, process, or store credit card information on Montana State University computer systems, fax machines, the internet, email (or similar messaging system), or any removable electronic storage device (USB memory stick, hard drive, zip drive, etc.).
- When possible, cashiering sites accepting credit card payments should only use Point of Sale terminals or equipment supplied to the location by the campus' merchant card processor. In all cases, Point of Sale terminals and systems must be configured to prevent retention of the full magnetic strip, card validation code, PIN, or PIN Block cardholder data once a transaction has been authorized.
    - The three- or four-digit validation code printed on the payment card, referred to as the Card Identification Number (CID), must never be stored in any form. The CID number may also be referred to as the CVC2 or CVV2.
    - The full contents of any track data from the payment card's magnetic stripe must never be stored in any form.
    - The personal identification number (PIN) or encrypted PIN block must never be stored in any form.
    - If electronic storage is authorized, the primary account number (PAN) must be rendered unreadable anywhere it is stored.
    - All but the last four digits of any credit card account number must be masked when it is necessary to display credit card data.

Credit Card Information Storage

- Paper records containing credit card data must be secured at all times, e.g., stored in a locked file cabinet or locked room in a secure storage container, if any, used for materials that are to be destroyed. Access to the storage area(s) must be limited to those who need access to the credit card data records.

Credit Card Receipts

- Credit card receipts that go to the customer and University Business Services may only show the last four digits of the credit card number. Also, the credit card expiration date should not appear on the receipt.

Annual Self-Assessment and Periodic Internal Network Scan

- Each department processing payment cards must complete an annual PCI DSS Compliance Internal Assessment Questionnaire.
- Departments must work to resolve any exceptions listed in the questionnaire. Departments must also work with the PCI Working Team to resolve any compensating controls.

Training

- Employees who are expected to be given access to cardholder data shall initially be required to complete PCI DSS Training and then renew that training at least annually.
- Employees shall be required to acknowledge at least annually that they have received training, understand cardholder security requirements, and agree to comply with these requirements.

Definitions:

Cardholder

The customer to whom a payment card has been issued or the individual authorized to use the card.

Cardholder Data

At a minimum, cardholder data consists of the full PAN (primary account number). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

Encryption

The process of converting information into an unintelligible form to anyone except holders of a specific cryptographic key (Use of encryption protects information that is between the encryption process and the decryption process from unauthorized disclosure.).

Merchant or Merchant Department

Any University department or other entity that accepts payment cards bearing the logos of any of the five members of the Payment Card Industry Security Standards Council (American Express, Discover, JCB, MasterCard or VISA) as payment for goods and/or services, or to accept donations.

Payment Card

Any payment card/device that bears the logo of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or VISA, Inc.

Responsibilities:

University Business Services

University Business Services has been delegated the authority by the University to approve all physical payment locations, websites, third party processors, or any channel accepting credit card payments, and will be responsible for verifying that credit card payments are only accepted at approved locations using approved merchant card processors. Additional University Business Services responsibilities include:

- Establishing and maintaining a process for campus departments to accept payment cards.
- Approving Online Credit Card Processing Requests before payment cards can be accepted.
- Verifying that all service providers are listed on the List of PCI DSS Validated Service Providers (VISA's website).
- Verifying the existence of a certification letter from a qualified security assessor.
- Verifying the existence of the service auditor's attestation of compliance AoC.
- For all third-party payment software applications that capture, store, process, or transmit cardholder data as part of an authorization or settlement, verifying, on an annual basis, that the third-party software applications are compliant with applicable payment card requirements.
- Ensuring that each campus department that accepts payment cards completes the PCI DSS Compliance Internal Assessment Questionnaire required by applicable standards on an annual basis.
- Ensuring that only PCI DSS approved POS systems are approved for merchants and maintaining a centralized list of all POS devices.
- Maintaining a central file of all documentation indicating third-party vendor and third-party payment software application compliance with applicable requirements.
- Maintaining the PCI DSS Training and related records of completion.

- Authorizing PCI Network/Account access for employees who have completed PCI training.
- Coordinating with the PCI Working Team, any campus response to a security breach involving cardholder data.
- Updating, maintaining and disseminating campus PCI standards and practices as needed
- Working with ITC and PCI Working Team,
    - Coordinate campus compliance with PCI DSS administrative and technical requirements and verify the security controls of systems authorized to process credit cards.
    - Monitor that PCI DSS Self-Assessments and Attestations of Compliance are completed in a timely manner in accordance with PCI DSS standards.

Merchant Department Responsible Person (MDRP)

Every department or administrative area accepting payment cards and/or electronic payments on behalf of the University for goods, services, or donations (the "merchant department") must designate a Merchant Department Responsible Person (MDRP).

The MDRP must be a management employee with primary authority and responsibility for payment card and ecommerce transaction processing within that department. All MDRPs are responsible for:

- Executing, on behalf of the relevant merchant department, payment card account acquisition or change procedures.
- Ensure that PCI DSS Self-Assessments and Attestations of Compliance are completed in a timely manner in accordance with PCI DSS standards.
- Ensure that all employees handling cardholder data have annual PCI DSS compliance training.
- Ensuring that all employees (including the MDRP), contractors, and agents with access to payment card data within the relative merchant department acknowledge on an annual basis that they have read and understood this standard. These acknowledgements should be submitted, as requested, to University Business Services.
- Ensuring that all payment card data collected by the relevant merchant department in the course of performing University business, regardless of whether the data is stored physically or electronically, is secured according to this standard.
- In the event of a suspected or confirmed loss of cardholder data, immediately notifying ITC and University Business Services. Details of any suspected or confirmed breach should not be disclosed in any email (or similar messaging system) correspondence. After normal business hours, notification shall be made to Montana State University Police at (406) 994-2121.

Employees Handling Credit Card Information

- All employees handling cardholder data must have received initial PCI DSS compliance training within the previous one-year period.
- When employees have access to payment card data, whether accepted via telephone, in person, or through other non-electronic methods, the data must be secured before employees leave their workstations for any purpose.
- When payment card data must be physically transported, the means of physical transport must be secure and trackable, and the transport must be approved in advance by management. Credit card data should never be sent via mail that cannot be accurately tracked (namely, campus mail, regular USPS).
- Payment card data on paper must be cross-shredded as soon as possible after the credit card billing transaction is completed.
- Only employees requiring access to payment card and electronic payment data in order to do their jobs are to be granted such access.
- Perform routine visual inspections of every device, looking for potential signs of tampering. Keep track of any operational difficulties that begin happening on a regular basis. If you notice these or anything out of the ordinary, stop using the device immediately and disconnect it from the POS device or network, but do not power it down. Immediately contact the campus central business office and campus central IT office. Some examples of things to look for include:
    - Damaged or altered tamper seals
    - Missing manufacturer labels
    - Missing screws or screws with damaged heads
    - Incorrect keyboard overlays
    - External wires
    - Holes in the device housing
    - An electronic serial number that does not match the number printed on the bottom of the device
    - A high number of mag-stripe read failures or debit card declines
    - Difficulty inserting a chip and PIN card into the EMV slot
- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace, or return devices without verification.
- Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
- Report suspicious behavior and indications of device tampering or substitutions to appropriate personnel (for example, to a manager or security officer).

Non-Compliance and Exceptions:

Montana State University is contractually obligated to its acquirers to secure all credit card data captured, stored, processed, or transmitted. Failure to adequately secure credit card data resulting in a data breach may result in the following responses from the acquirers and/or card brands:

- Require Montana State University to pay for a forensics team to investigate the breach
- Require Montana State University to notify cardholders of the breach
- Impose implementation of additional expensive technical controls
- Impose costly quarterly security audits from third parties
- Assess fines that may reach hundreds of thousands of dollars or more
- Deny Montana State University the ability to process payment cards

University Business Services may suspend/terminate credit card account privileges of any department or administrative unit not in compliance with this standard or that places the University at risk.