MONTANA STATE UNIVERSITY BILLINGS

Administrative Services
Policies & Procedures

Policy Number: 246.1
Policy: Payment Card Industry (PCI)
Effective Date: 1/2015
Revision Date: 11/2023
Approved by: Business Services Director

PROCEDURE:

I. Payment Card Industry Data Security Standard (PCI or PCI DSS) Compliance

A. Introduction and Purpose:

This policy is a supplement to the Safeguarding Customer Information policy. Specifically this policy will detail the handling of Card Holder Data (CHD) on campus, how we accept CHD, how we process, and how we store the information as a University. Included in the policy will be training for employees with CHD access. Service Provider requirements will be addressed. This policy will not address specific IT related issues regarding PCI DSS.

B. Policy:

1.Employees, PCI requirement 12.6:

a. All employees with access to CHD data must be trained annually.

b. Supervisors in departments that accept CHD must meet the training requirements regardless of their CHD access.

c. New employees with CHD access need to participate in the training after hire.

2. Service Providers, PCI requirements 12.8:

a. All third party service providers must be PCI DSS compliant.

b. A list of all third party service providers must be kept.

c. All contracts with service providers handling CHD must include language that requires PCI compliance and continuance. All contracts must be approved by the Business Services Director.

3. CHD Materials Access:

a. Access to sensitive CHD materials and storage areas need to be kept secure per PCI requirement 9.5.

b. Materials must be secured by in safes, file cabinets, locked rooms or storage areas with limited access to those personnel.

c. Establish and follow retention procedures for CHD per PCI requirement 9.8.

4. CHD Acceptance Devices (Credit Card Machines and POS Systems), PCI requirement 9.9:

a. Secure devices that capture and transmit CHD.

b. Inspect these devices for tampering or substitution.

c. Document location and identity of the devices used to accept credit cards.

d. Report any suspected tampering or substitutions to the CIO, Business Services Director or the Vice Chancellor of Administration.

e. The square and other card readers/devices that attach to portable systems (laptops, cell phones, iPads, etc.) are not approved for use.

5. Protect stored CHD, PCI requirement 3.2 and 3.3.

a. Do not retain the full mag stripe information.

b. Do not retain pin number.

c. PAN must be masked if retained.

d. CHD must be stored in a locked desk, cabinet or storage area. Video surveillance is recommended.

e. Only Business Services will store for long term any paper media related to CHD.

f. Forward any CHD for processing to Business Services.

g. Shred CHD when the business purpose has expired.

6. Access to the CHD on a need to know basis, PCI requirement 7.1.

a. Only those employees with a business need should have access to the CHD.

b. Access should be assigned based on their role within the University.

7. CHD Daily Processing requirements.

a. Do not accept CHD from an email or FAX.

b. Do not enter into any computer CHD, all documents leave hidden files when deleted.

c. Do not enter CHD into a third party software system for a customer.

d. Under certain circumstances you may take credit cards over the phone.

e. Under certain circumstances you may process CHD received via postal or express mail services.

f. Secure your terminals, devices and CHD storage areas when not attended.