MIDWESTERN STATE UNIVERSITY

Operating Policies & Procedures Manual

# University Operating Policy/Procedure (OP)
# OP 14.17: Payment Card Processing

**Approval Authority:** University President
**Policy Type:** University Operating Policy and Procedure
**Policy Owner:** Vice President for Administration and Finance and Chief Information Officer
**Responsible Office:** ~~Controller~~Assistant Vice President, Financial Services
**Next Scheduled Review:** 05/01/2029~~4~~

## I. Policy Statement

Midwestern State University ("MSU" or "University") seeks to protect the interests of the University and its customers by establishing strong internal business controls and standard revenue collection methods throughout the University.

## II. Reason for Policy

The purpose of this Operating Policy/Procedure (OP) is to ensure compliance with the Payment Card Industry Data Security Standard and to protect the cardholder information of patrons that utilize a credit card to transact business with MSU.

## III. Application of Policy

This policy establishes policy and procedures for acceptance of payment cards by University departments for sales and services.

## IV. Definitions

For purposes of this OP:

**Payment Card -** A payment card supports cashless payment for goods and services. Examples include, but are not limited to, credit cards, debit cards, and charge cards.

**Merchant -** Each department processing payment card transactions is referred to as a Merchant.

**Merchant ID -** A Merchant ID is a unique number used to identify the department and card type. The University Business Office will request the required merchant identification number from the payment card processor and provide them to the Merchant.

**Payment Card Industry Data Security Standards (PCI DSS)** - PCI DSS is a single approach to safeguarding sensitive data for all types of payment cards. The Standards are a result of collaboration between Visa and MasterCard and are designed to create common industry security requirements.

To download the PCI DSS, go to: https://www.pcisecuritystandards.org/

**Payment Card Application** - Payment Card Applications can be hardware, software, or a combination of hardware and software which aid in the processing of payment cards. Examples include Point of Sale (POS) devices, web applications/forms which collect or process payment cards, or third-party systems which process payment card transactions.

**Payment Card Processor** - A payment card processor offers merchants online services for accepting payment online including credit card, debit card, direct debit, bank transfer, and real-time bank transfers.

**PCI DSS Self-Assessment Questionnaire (SAQ)** - The PCI DSS SAQ is a validation tool intended to assist a Merchant and service provider(s) in self-evaluating their compliance with PCI DSS.

To download a PCI DSS SAQ, go to: https://www.pcisecuritystandards.org/

**PCI DSS Data Network** - A secure firewalled network within MSU's network, developed according to the PCI DSS standard, for the hosting of computers, servers, or storage which process payment card transactions and data.

**Service Provider/Vendor** – As used in this policy is a 3rd party payment card processor.

## V. Procedures and Responsibilities

### A. Payment Card Processor

1. Payment Card Processor. All payment card transactions must go through Midwestern State University's (MSU) payment card processor, currently Heartland Payment Systems.

   Any exceptions to the use of this standard processor must be approved by the University Vice President for Administration and Finance, the ~~Controller~~Assistant Vice President, Financial Services, the Chief Information Officer, and the ~~Chief~~ Information Security Officer.

   Current Exceptions for 3rd Party Service Provider/Vendors:

   **Stripe**: Processes payments for Athletics ticketing, University Advancement donations made through Gravyty, and the Fain College of Fine Arts event tickets~~.~~

   ~~**Rydin**: Processes payments for the MSU Police Department ticketing system.~~

2. Methods of Processing. MSU processes payment cards both physically and online. Merchants that want to begin processing payment cards, ***must*** use one of the following MSU-approved processing methods:

   a. Online
   This is done through MSU's online e-commerce solution Touchnet Marketplace. Any exception to this MUST be reviewed and approved by the Business Office.

   b. In Person
   Payments may be made in person with campus merchants.

3. Acceptable Vendors. If using a third-party software, the software must connect through the University e-commerce solution Touchnet Marketplace. Any exception to this must be reviewed and approved by the Business Office. Only PCI DSS-compliant vendors may be used. All software contracts and purchase orders must include non-disclosure and/or confidentiality statements. Proof of compliance must be:

   a. a written agreement from the service providers acknowledging they are responsible for the security of cardholder data the service providers possess; and

   b. sent to the Business Office.

**B. Establishing and Maintaining Payment Card Services**

1. Establishing Accounts. Merchant IDs will not be issued until the Merchant meets **all** of the following requirements.

   a. Complete and submit to the Business Office:
   - Policy Certification
   - PCI DSS Awareness online training

2. Maintaining Accounts. Merchant IDs may be revoked if the Merchant does not meet **all** of the following requirements. The Business Office will reach out to all merchants during the Fall of every year to request updates on each of these in order to comply with PCI DSS certification regulations for the University.

   a. Complete the PCI DSS Self-Assessment Questionnaire (SAQ) annually or **upon any change** to the hardware, software, or payment card processing methodology and submit to the Business Office;

   b. Complete the MSU Merchant Application & Update as requested by the Business Office, or **upon any change** to the hardware, software, or payment card processing methodology and submit to the Business Office;

   c. Complete required PCI DSS Awareness online training annually. Training is required for:

- Any employees who process payment cards or have access to sensitive payment card information received by their department for payment card transactions
- Supervisors of the above employees
- Departmental Business Managers whose department accepts credit card payments
- Others who oversee payment card operations in a department;

d. Complete Policy Certification annually. Required by the same individuals listed in Section V.B.2.c of this OP; and

e. Continued compliance with this OP, PCI DSS, and MSU IT Security Policies.

## C. Authority and Responsibility

1. The Business Office is responsible for:

   a. issuing a payment card Merchant ID and for overseeing the policies and procedures on payment processing;

   b. negotiating payment card processing and related services on behalf of any MSU department;

   c. performing monthly reconciliation on the bank account, to which payment card receipts are credited;

   d. determining if the charges have been assessed against the bank account in accordance with the pending procurement document(s) during the account reconciliation process;

   e. assisting merchants with resolving discrepancies related to payment card charges with the MSU payment card processor;

   f. verifying that all Merchants are in compliance with MSU policies and current PCI DSS financial controls in regards to protecting cardholder data; and

   g. the revocation of a Merchant ID that fails to comply with the PCI DSS and/or this OP.

2. The Information Technology Department is responsible for:

   a. the operations and maintenance of the MSU data networks, as well as, the establishment of IT security policies and standards in compliance with PCI DSS, federal, state, and local regulations;

   b. developing and maintaining an MSU PCI DSS Data Network for the hosting of computers, servers, and online storage engaged in processing or storage of payment card transactions;

c. assisting any Merchant in assessing its payment card processes, applications, and migration to a PCI DSS-compliant solution for the processing of payment cards;

d. verifying that all Merchants are compliant with the current PCI DSS technical requirements; and

e. annual collection of information to monitor service 3rd party service provider/vendor PCI DSS compliance status.

3. The Merchant is responsible for:

a. all requirements outlined above in Section V.B.2 of this OP;

b. developing a system and procedure to monitor and analyze security alerts and information and distribute these alerts to the appropriate personnel;

c. developing and maintaining departmental policy and procedures for physical inspection of payment card equipment, including frequency and methods of inspection and submitting this policy to the Business Office annually or as requested;

d. verifying that their software, hardware, applications, or other devices, products, etc. and associated processes for processing payment cards meets PCI DSS requirements - assistance from the Business Office and the MSU IT Department may be needed;

e. maintaining and safeguarding all payment card processing equipment according to the PCI DSS standard. The equipment must be able to produce receipts (merchant and/or customer) that masks all but the last four digits of the cardholder's card number;

f. contacting the payment card processor regarding defective payment card processing equipment. The Merchant should return the equipment directly to the payment card processor, provided the payment card processor has instructed the Merchant to return the equipment. The Merchant should obtain a comparable replacement directly from the payment card processor;

g. contacting the Business Office to relocate its purchased payment card processing equipment (media) or dispose of the equipment in accordance with the PCI DSS standard and relevant MSU Operating Policies when the Merchant discontinues the acceptance of payment cards. Purchased equipment should be returned to the payment card processor. Before any payment card processing equipment is transferred to another department or returned to the leasing company, verify all payment card data has been securely removed. If the equipment will be disposed of, all payment card data must be securely removed, or the storage device must be destroyed to prevent unauthorized access to the data;

h. maintaining a record retention and disposal policy in accordance with OP 02.34: Records Management Policy, to keep information storage to a minimum, that information will be used for business and regulatory purposes only, and that information will comply with OP 44.11: Information Resources Use and Security Policy (Contact the University Librarian at the Moffett Library at (940) 397-4173 for records retention guidance); and

i. responding to card brand chargebacks, disputes, sales draft retrieval requests or other requests from the issuing bank or cardholder within the specified time period providing proper documentation, or determining that the chargeback, dispute or other request is legitimate and should stand as is.

## VI. Related Statutes, Policies & Procedures and Websites

Payment Card Industry – Data Security Standards Form

## VII. Responsible Offices

Questions or comments regarding this Policy should be directed to:

Vice President for Administration & Finance
vpaf@msutexas.edu
Extension 4117

Business Office
bus.office@msutexas.edu
Extension 4101

Chief Information Officer
cio@msutexas.edu
Extension 4647

Chief Information Security Officer
ciso@msutexas.edu
Extension 4680

## VIII. History

20 May 2022: OP 14.08: Payment Card Processing is a new policy recommended during an internal audit review by the Texas Tech University System in February 2022 regarding PCI compliance. Adopted and approved by MSU Interim President James Johnston.

__/__/2025: Renumbered from OP 14.08: Payment Card Processing to OP 14.17: Payment Card Processing, and adopted and approved by MSU President Stacia Haynie.

_____
Stacia Haynie, President

Midwestern State University

Date Signed: _____