Michigan Technological University
Information Technology

Credit Card Acceptance and Processing Procedures

Introduction

Michigan Tech accepts credit cards for many payments of goods and services. Credit card payments must be processed in compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements, which are intended to limit exposure and/or theft of personal cardholder information.

Michigan Tech must adhere to these standards in order to retain our ability to accept credit card payments. Departments not complying with approved safeguarding, storage, processing, and administrative procedures will lose the privilege of processing credit cards. In addition, each department engaged in credit card processing may be held responsible for any financial losses due to poor internal or inadequate controls or negligence/neglect in adhering to the PCI Standard.

Purpose

The purpose of this procedure is to establish and define requirements for collecting, storing, processing and transmitting credit card data to ensure proper control and integrity of data as well as to facilitate compliance with PCI DSS requirements. These standards are designed to assist Michigan Tech in the safekeeping of cardholder information, which in turn reduces the chances of security breaches, fraud, and potential financial losses.

Scope

This procedure applies to all University employees, faculty, students, contractors, guest, consultants, temporary employees, and any other users who accept donations or sell goods, services, or information, and accept credit cards as a form of payment.

All computers and electronic devices used for processing payment card data are governed by PCI DSS. This includes servers that store payment card numbers, workstations that are used to enter payment card information, and computers or credit card swipe devices through which payment card information may be transmitted.

Definitions

Payment Card Industry Data Security Standard (PCIDSS) is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that hold, process, or pass cardholder information.

Cardholder Data is any personally identifiable data associated with a cardholder. Examples include but are not limited to: account number, expiration date, card type, name, address, social security number, and Card Validation Code (e.g., three-digit or four-digit value printed on the front or back of a payment card referred to as CVV2 or CVC2).

Merchant ID (MID) is a unique number that identifies each department for accounting purposes.

Point of Sale (POS) is a computer or credit card terminal that either runs as a standalone system or connects to a server at the University or at a remote off site location.

E-commerce occurs when the authorization and settlement of a transaction are processed through a computer over the Internet. Typically the card is not present and the customer is offsite with respect to the merchant.

Department Responsibilities

Departments are responsible for knowing and complying with PCI DSS and University policies to safeguard credit card and other personally identifiable or sensitive information. Departments must also follow established procedures to ensure that cardholder information is handled and stored securely.

This applies to all transactions regardless of the type of transaction (phone, in-person, mail, web, etc.).

Establishing Payment Card Services

Any University department wishing to accept credit cards for goods or services must first contact it-Information Technology Services and Security (ITSS) will work with departments to determine a solution that best fits the department's needs in terms of credit card processing.

Once a solution has been chosen, ITSS will request a MID from Accounting. In order to accept credit card payments, departments must first have a MID.

All transactions that involve the transfer of credit card information must be performed on systems approved by ITSS and will include a compliance and security review. Approval MUST be obtained prior to entering into any contracts or purchases of software and or equipment relating to credit card processing. This requirement applies regardless of the transition method of technology used.

Merchants may NOT set up their own banking relationships for payment card processing. Payment card revenue MUST be deposited into designated University bank accounts. PayPal accounts are not University-approved bank accounts.

There are several approved University methods to accept credit cards, including e-commerce, in person via web based virtual terminal, or via a Point of Sale (POS) terminal connected to the Internet.

E-Commerce Transactions

Touchnet is the University's primary credit card processing application and to the extent possible, is to be used for all credit card transactions. This type of transaction begins when the customer purchases a product, registers for an event, or makes a donation, etc. through a payment application website. In this situation, the customer is not present for the sale.

Touchnet offers a variety of solutions that have been configured to meet the PCI Data Security Standards. ITSS will work with Departments to determine the appropriate solution.

Point of Sale Transactions

Some departments may have specialized software or a Point of Sale (POS) system for processing credit cards. Payments may be processed with the cardholder present or cardholder NOT present by mail, telephone, or fax order per the department's business operational needs. The credit card transaction process begins when the customer purchases a product and their card is swiped or entered into a point-of-sale system.

Paper and Credit Card Terminal Transactions

The University has phased out paper processing of credit card information due to the amount of work required to be PCI DSS compliant. To the extent possible, the use of physical credit card terminals have also been phased out. Both processes have been replaced by Virtual Cashiering Stations, a web based payment form that enables departments to accept telephone, fax, and mail payments for all major credit cards. The functionality is the same as a stand-alone credit card processing terminal however has more security features enabled.

Processing Transactions

Specific details regarding processing and reconciliation will depend upon the method of credit card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established. Only authorized individuals can process credit card transactions.

Card Swipe

If the credit card is present it may be swiped. This method is generally the least expensive and eliminates the need to manually enter the credit card number.

Manual Key Entry

If the credit card is not present, the credit card information may be entered manually. Information required to enter manually will be the credit card number, expiration date, amount to be charged, CVV code and the billing zip code. The CVV and billing zip code will ensure a lower rate for processing the transaction.

Daily Settlements

Systems must be closed out daily and reconciled to the daily activity to ensure all transactions are correct. The daily Batch Settlement Report is generated when the system is closed each day. The bank charges a higher processing fee for any transactions that are not settled daily.

Security of Cardholder's Information

Cardholder information is obtained either by the cardholder being present (credit card present) or by transmitting cardholder information (telephone, Internet, etc.). All individuals authorized to accept credit card payments must securely process, store and dispose of credit card data in order to adhere to the Payment Card Industry (PCI) Data Security Standards (DSS).

Credit card numbers must be masked to protect account information for all users except those who have a legitimate business need. The first six or last four digits are the maximum number allowed to be displayed.

If any card information is written down while performing the transaction, that information must be shredded once the transaction has been completed. If credit card information is obtained and recorded for future use (example: periodic billing for partial payments), the information must be secured and not accessible to unauthorized individuals (safe, locked file cabinet, etc.), as well as other PCI requirements such as logging and auditing of access to data. The information once used is to be properly destroyed.

It is not permissible to transmit or obtain credit card information by email, Wireless Devices, PDAs, Instant messaging, Chat applications or other unsecure methods unless otherwise approved by IT. If email containing cardholder data is received, immediately delete the email and notify the sender that the University does not accept cardholder data via email and that the transaction will not be processed. In the response, give the customer a list of alternative methods of sending their card information (mail, phone, or secured fax). If you reply to the original email, make sure you remove any card information before sending the message. Also, be sure to delete the message from your email inbox, sent box, and deleted box.

Report any suspected exposure (to unauthorized parties) or loss of cardholder data to IT immediately.

This includes lost or stolen files with credit card numbers, electronic loss of data, databases infected with viruses and any other loss or potential loss.

For further reference please see Credit Card Processing Guidelines.

If you have any questions please call IT Help at 487-1111 or email it-help@mtu.edu.

END OF DOCUMENT
Rev 9/20/16