Michigan Technological University
Information Technology

PCI DSS Credit Card Guidelines

Introduction

Michigan Tech accepts credit cards to provide a convenient way to handle business transactions such as conference registration, the purchase of course materials, or the purchase of meals at a campus dining facility. Credit cards must be processed in compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements. The purpose of this document is to establish basic guidelines for accepting, processing, and storing or transmitting cardholder data to ensure PCI DSS compliance.

Guidelines

- Assignment of user privileges to Cardholder Data is to be based on individual job classification and function. The least amount of access necessary to perform job responsibilities is to be granted.
- Any job position that requires access to stored Cardholder Data will be considered security sensitive. Departments are to perform applicable background checks on potential employees who will have access to systems, networks, or cardholder data.
- Personnel involved in credit card processing, transmitting, or storing must attend card security training every year.
- Any person processing credit card information must agree not to disclose or acquire any information concerning a cardholder's credit card account without the cardholder's consent. Employees must sign and acknowledge that they have read and understood University and departmental payment card data security policies and procedures.
- Sensitive cardholder data (full account number, card type, expiration, PIN, and card-validation code (three-digit or four-digit value printed on the front or back of the card) is NOT stored in any way.
- Credit card numbers should never be stored on a personal computer.
- Email, unsecured fax, or campus mail are never to be used to transmit credit card numbers.
- All records that include cardholder data, including physical security of paper and electronic media (including computers, removable electronic media, receipts, reports, faxes, etc.) are to be in a secure environment. Secured environments include locked drawers and safes, with limited access to only individuals who are processing the credit card transaction. Departments must conduct an inventory of media as well as maintain inventory logs and audit trails of all paper and electronic media.
- Any cardholder information in paper format (recording, writing down or storing cardholder information) is to be kept at a minimum. Processing is performed as soon as possible and the credit card number is immediately blacked out to the last four digits. In addition, any Sensitive Cardholder Data should be masked.

- Stored credit card information and merchant receipts will be retained according to the respective campus data retention policy (no longer than 18 months) so long as there is a business, legal and/or regulatory purpose.
- Departments will notify IT regarding any technology changes affecting transaction processing.
- Network vulnerability scans shall be performed on machines that are involved in the processing of credit/debit cards on at least a quarterly basis and after any significant change in the network.

Credit Card Processing Procedures

With the help of IT, each department that processes, stores, or transmits cardholder data, must complete an annual self-assessment questionnaire to ensure PCI DSS compliance. For specific requirements, please visit https://www.pcisecuritystandards.org.

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