OP 62.08: CREDIT / DEBIT CARD PROCESSING

PURPOSE

The purpose of this policy is to provide guidance to Mississippi State University departments that process credit/debit card payments for university business.

In order to accept credit and debit card payments, Mississippi State University must maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS). The DSS was created to protect cardholder data to reduce payment card fraud and identity theft. Mississippi State University must take appropriate measures to prevent loss or disclosure of customer information including payment card numbers. Failure to comply with PCI DSS requirements may result in financial loss for customers, fines imposed on the university, suspension of payment card processing privileges, and damage to the reputation of the department and the university.

DEFINITIONS

Cardholder Data (CHD) – Those elements of payment card information that are required to be protected. At a minimum, cardholder data consists of the full Primary Account Number (PAN). It can also be comprised of the full PAN plus any of the following: Cardholder Name, Expiration Date, and the Service Code.

Primary Account Number (PAN) – Unique numeric code of 14 or 16 digits embossed on a bank, debit, or credit card and encoded in the card's magnetic strip and/or microchip. The PAN identifies the issuer of the card and the specific cardholder account.

Cardholder Name – The name of the Cardholder to whom the card has been issued.

Expiration Date – The date on which a card expires and is no longer valid. The expiration date is embossed, encoded and/or printed on the card.

Service Code – The three or four-digit value that defines where the card can be used and for what purposes. The Service Code is encoded in the track and/or chip data, and is not visibly printed anywhere on the card.

Sensitive Authentication Data – Additional elements of payment card information that are required to be protected but never allowed to be stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data, and PIN/PIN block. These security-related elements are used to authenticate the cardholder and/or authorized transactions.

Magnetic Stripe (aka. track data) – Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during an in-person transaction. Entities may not retain full magnetic-stripe data after transaction authorization regardless of success or failure of the transaction.

CAV2, CVC2, CID, or CVV2 data – The three- or four-digit value printed on or to the right of the signature panel, or on the face of a payment card; used to protect data integrity of the card and/or reveal potential counterfeiting. This code is often requested in ecommerce transactions as an additional measure to validate the payment card.

PIN/PIN block – Personal Identification Number entered by cardholder during an in-person transaction, or the encrypted block of data present within the transaction message.

Sensitive Cardholder Information – For purposes of this policy, the term "sensitive cardholder information" refers to Cardholder Data (CHD) and/or other Sensitive Authentication Data.

Third Party Solution: To better comply with the requirements of the Payment Card Industry (PCI) standards, Mississippi State University has contracted with a third party payment card processor to provide a safe, secure, and PCI-compliant environment in which to process credit/debit card payments. The third party solution provides a registered product that is divided into two separate systems: one is used to process Student Accounts Receivable payments and the other to process payments for other departments, divisions, and entities on and off campus.

MSU PCI Council: The MSU PCI Council (also referred to as "the council") is led by the Office of the Controller and Treasurer and comprised of members from the Office of the Controller and Treasurer, Information Technology Services and, when necessary, other university departments. The council is responsible for ensuring the university is properly adhering to all PCI DSS requirements and regulations.

SCOPE

This policy applies to all units and employees of Mississippi State University who accept credit/debit card payments for university business or handle sensitive cardholder information for any purpose. This policy also applies to third party contractors, affiliates and any other individuals who accept credit/debit card payments for university business or handle sensitive cardholder information for any purpose.

POLICY

1. All credit/debit card payments must be processed using MSU's third party solution unless an exception is approved by the PCI Council.
2. Any effort to implement new systems and/or business practices that involve credit/debit card processing must receive approval from the PCI Council prior to implementation. This includes payments processed online, over the phone, through the mail, face to face or using an outsourced, third party service provider who processes payments on behalf of the university. To avoid unnecessary project delays, it is recommended the council be engaged as soon as possible in the process.

3. Departmental units approved for credit/debit card processing activities must adhere to all university policies and procedures regarding credit/debit card payments and current PCI DSS regulations.
4. All individuals involved in accepting, processing, or handling sensitive cardholder information for any purpose must participate in training as provided by the PCI Council.
5. Individuals must not be permitted access to credit/debit card processing systems and/or sensitive cardholder information unless their job responsibilities specifically require such access.
6. Requests for access to MSU's third party solution will be submitted to the PCI Council for review and approval. The council will provide access to the third party solution on an as needed basis, and notify the department when access rights are granted. Access will be limited to only those functions required for the individual to conduct their job responsibilities. When an individual leaves their position, the department must notify the council within one week so that the access to the third party solution can be removed.
7. When using an approved, alternate payment processing solution (i.e. not MSU's third party solution), the department will provide individuals access to the solution on an as needed basis. Access will be limited to only those functions required for the individual to conduct their job responsibilities. The department will develop, implement, and maintain control procedures to ensure system access is reviewed on a regular basis, access is limited to only individuals who need access to perform their jobs responsibilities, and access is limited to only those functions required for the individuals to conduct their job responsibilities. Access for terminated individuals or those who have left their position will be removed within one week of their departure from that role.
8. Periodic audits will be performed to ensure all units comply with all policies and procedures associated with processing credit/debit card transactions at the university.
9. For all departments that handle payment card data, reference to this policy must be included in the departmental procedures and training program.

REVIEW

This policy will be reviewed every four years or as needed by the Controller and Treasurer with any modifications submitted to the Vice President for Budget and Planning.

REVIEWED BY:

/s/ Kevin Edelblute — 05/09/2017
Assistant Vice President and Controller and Treasurer — Date

/s/ Don Zant — 05/09/2017
Vice President for Finance — Date

/s/ Timothy N. Chamblee — 05/19/2017
Assistant Vice President and Director Institutional Research and Effectiveness — Date

/s/ Joan Lucas — 05/22/2017
General Counsel — Date

APPROVED BY:

/s/ Mark Keenum — 06/05/2017
President — Date