OP 62.10: SAFEGUARDING CARDHOLDER DATA (CHD)

PURPOSE

The purpose of this policy is to provide guidance for all credit/debit card processing activities to ensure cardholder data is safely and securely handled at the university.

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 credit 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 credit 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Expiration Date – The date on which a card expires and is no longer valid.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.

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

Mississippi State University classifies sensitive cardholder information as "Category I Data". Per the university's Information Security Program: "*Category I data refers to data protected specifically by law or by Mississippi State University policy. Examples of category I data include data covered by HIPAA, FERPA, donor, employee, or sensitive research data, Social Security identification numbers, payment card data …*". Due to the extremely sensitive nature associated with Category I Data, it is imperative that the following policy requirements are enforced with regard to sensitive cardholder information.

Electronic Media

Sensitive cardholder information may not be stored in any form on university computers, networks, or other electronic media. If sensitive cardholder information is found to be electronically stored on any university equipment, the department/employee must notify the MSU PCI Council immediately. The council will work with departmental employees to ensure sensitive cardholder information found on electronic media is rendered unrecoverable via a

secure wipe program (in accordance with industry-accepted standards for secure deletion), or by physically destroying the media in compliance with current PCI DSS requirements.

Sensitive cardholder information may never be transmitted using electronic messaging technologies such as email, instant messenger, etc.

Physical Media (i.e. paper documents)
As a general rule, paper documents containing sensitive cardholder information may not be retained and stored. All paper documents containing sensitive cardholder information must be destroyed in a PCI DSS-compliant manner immediately after the card transaction is completed.

Under certain circumstances, it may be necessary to retain sensitive cardholder information on paper documents for a short period of time (30 days or less). In order to store paper documents containing sensitive cardholder information, the following criteria must be met:

- Written approval must be received from the MSU PCI Council allowing the unit to physically store documents containing sensitive cardholder information. Exceptions to the "30-day rule" will be reviewed and approved on a case by case basis.
- Documents will be physically secured in a location only accessible by individuals needing access to conduct their job responsibilities. A list of stored documents must be maintained, and a periodic inventory review must be conducted at least quarterly.
- The department will develop, implement, and maintain control procedures to ensure the list of individuals with physical access to documents containing sensitive cardholder information is accurate and up to date, and access is limited to only those who need access to perform their job responsibilities. These control procedures must be reviewed on at least a quarterly basis to ensure documents containing sensitive cardholder information are being properly stored, secured and destroyed in a timely fashion.

As a general rule, physical documents containing sensitive cardholder information should not be transported between buildings on or off campus. In the event it becomes necessary to transport documents containing sensitive cardholder data, internal control procedures must be put in place to ensure transportation was successfully completed, all documents were delivered, and no sensitive cardholder data was compromised during the process. Should the documents require transport, the documents must be secured at all times and control / ownership must be tracked and documented.

For all departments that handle payment card data, reference to this policy must be included in the departmental procedures and staff 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