OP 62.09: SECURITY OF CARD PAYMENT DEVICES

PURPOSE

The purpose of this policy is to provide guidance for all university units that process credit/debit card payments (in-person, phone-in, mail-in, etc.) using physical payment devices to ensure the payment devices are secure and regularly inspected to avoid the possibility of tampering.

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 payment card processing privileges, and damage to the reputation of the department and the university.

DEFINITIONS

Card Payment Device – Any hardware used for processing credit/debit card payments including any device that allows for swiping the magnetic stripe on the card, dipping an EMV enabled chip card, use of near field communication (NFC) technology, manually entering cardholder information, etc.

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

All card payment devices used to process credit/debit card payments must be issued to the department by the MSU PCI Council. If the department desires to use a card payment device other than those issued by the council, the department must request and receive approval from

the council before deploying a different device. Approval for using a different card payment device may include additional responsibilities to ensure payments are handled in a manner that complies with all applicable PCI Compliance regulations.

Roles and Responsibilities – Departmental Users
Card payment devices must not be installed, replaced, or returned without guidance and approval from the MSU PCI Council.

Card payment devices issued to the departmental unit must be inspected on a regular basis to look for tampering or substitution. It is recommended that each device be inspected before its first use on any given day. Inspections must be performed by appropriate departmental personnel. Suspicions of tampering must be immediately reported to the MSU PCI Council.

A formal inventory and inspection of all card payment devices must be performed and documented on at least a quarterly basis. Results of the inventory process may be retained in the records of the department.

Roles and Responsibilities – MSU PCI Council
An inventory list of all approved card payment devices will be maintained by the MSU PCI Council.

The inventory list will be updated when devices are deployed, relocated, decommissioned, etc.

The inventory list will be reviewed for accuracy on at least an annual basis.

Training sessions will be provided at least annually to ensure university personnel are trained to be aware of suspicious behavior and to report any tampering or substitution of card payment devices. At a minimum, these training sessions will instruct university personnel in the following areas:

- To be aware of any suspicious behavior taking place in close proximity to card payment devices.
- To obtain MSU PCI Council approval prior to granting any third-party access to card payment devices.
- To obtain guidance, assistance, and/or approval from the MSU PCI Council before installing, replacing, or returning card payment devices.
- To immediately report suspicious behavior and/or indications of device tampering or substitution to the MSU PCI Council.

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