

MISSISSIPPI STATE UNIVERSITY CREDIT/DEBIT CARD PROCESSING

PURPOSE:

Mississippi State University entities processing credit card payments must take appropriate measures to prevent loss or disclosure of customer information including credit card numbers. Failure to comply with requirements imposed by the Visa Cardholder Information Security Plan (CISP) and MasterCard Site Data Protection Program (SDP) may result in financial loss for many customers, fines imposed on the university, suspension of credit card processing privileges and damage to the reputation of the unit and the university. The purpose of this policy is to provide requirements and guidance for all credit/debit card processing activities for Mississippi State University.

SCOPE:

This policy applies to:

- All units and employees of Mississippi State University who accept credit/debit card payments for University business or handles any credit card information for any purpose.
- All external organizations under contract to provide outsourced services for credit/debit card processing for University business.
- Any other person or organization using the MSU technology infrastructure for credit/debit card acceptance.

POLICY:

a. The approval process for all credit/debit card processing activities will be as follows:

- The Controller and Treasurer must approve all credit/debit card processing activities at Mississippi State University before a unit enters into any purchase arrangements for software and/or equipment. This requirement applies regardless of the transaction method used (e.g. e-Commerce, Point of Sale (POS) device or swipe terminals).
- All technology implementation (including approval of authorized payment gateways) associated with the credit/debit card processing must be approved by the Controller and Treasurer prior to entering into any arrangements for purchase of software and/or equipment.
- Sensitive cardholder data (account number) must not be stored in any form on MSU computers or networks without approval of the Controller and Treasurer. In cases where exceptions are approved, all data must be stored in an approved encrypted form and protected using approved security standards.

b. Units approved for credit/debit card processing activities must maintain the following standards:

- All employees involved in accepting or handling credit card information for any purpose must attend appropriate training as determined by the Controller and Treasurer.
- Paper documents containing credit/debit card numbers must be maintained in a secure location. These documents must be destroyed as soon as practical after use to reduce the chance of loss or theft.
- Access to credit/debit card processing systems and related information must be restricted to authorized personnel.

c. Periodic audits will be performed on each unit responsible for credit/debit card processing to ensure compliance with this policy and the associated procedures.

d. All credit/debit card processing must maintain compliance with Visa and MasterCard's *Payment Card Industry Data Security Standard (PCIDSS)*. Information regarding these standards may be reviewed at <https://sdp.mastercardintl.com>. A copy can be obtained from the Office of the Controller and Treasurer.

REVIEW:

This policy will be reviewed as needed by the University Controller and Treasurer with any modifications submitted to the Vice President for Finance and Administration.

RECOMMENDED BY:

/s/ Wayne Bland
Wayne Bland
Controller and Treasurer

10-19-05
Date

/s/ C. Ray Hayes
C. Ray Hayes
Vice President for Finance and Administration

11-22-05
Date

REVIEWED BY:

/s/ Don Zant
Don Zant
Director of Internal Audit

11-23-05
Date

/s/ Charles L. Guest
Charles L. Guest
General Counsel

12-01-05
Date

APPROVED BY:

/s/ Charles Lee
Charles Lee
President

01-24-06
Date

OP 62.08
1/24/2006