



Responsible University Administrator:	Vice President for Finance and Administration
Responsible Officer:	Director of Student Financial Services
Origination Date:	4/1/2016
Current Revision Date:	N/A
Next Review Date:	7/1/2017
End of Policy Date:	N/A
Policy Number:	ADMA-BUS-009
Status:	Effective

Payment Card Security Policy

Policy Statement

Accepting payments by credit or debit card is very convenient and one of the most recognized methods of payment. If utilized safely, it can enhance the revenue stream of a unit/ department. By being approved to use this method, each unit/department is responsible for the associated risks of fraud and identity theft.

Reason for Policy/Purpose

This document and additional supporting documents represents The University of Southern Mississippi's policy to prevent loss or disclosure of customer information including payment card data. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the unit and the university.

Who Needs to Know This Policy

The University of Southern Mississippi Payment Card Security Policy applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems and networks involved with payment card handling. This includes transmission, storage and/or processing of payment card data, in any form (electronic or paper), on behalf of The University of Southern Mississippi.

Website Address for this Policy

www.usm.edu/institutional-policies/policy-adma-bus-009

Definitions

Payment Card Industry Data Security Standards (PCI DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Payment card Brands: Visa, MasterCard, American Express, Discover, and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org)
Cardholder	Someone who owns and benefits from the use of a membership card, particularly a payment card.
Cardholder Data (CHD)	Those elements of payment card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.
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 or printed on the card.
Service Code	The service code that permits where the card is used and for what.
Sensitive Authentication Data	Additional elements of payment card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
Magnetic Stripe (i.e., track) data	Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
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 verify card- not-present transactions.

PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Disposal	CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices,(Before disposal or repurposing, computer drives should be sanitized in accordance with the (Institution’s) Electronic Data Disposal Policy). The approved disposal methods are: <ul style="list-style-type: none"> • Cross-cut shredding, Incineration, Approved shredding or disposal service
Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by the (institution) to accept payment cards and has been assigned a Merchant identification number.
Database	A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets.

Policy/Procedures

In order to accept credit and debit card payments, The University of Southern Mississippi must prove and maintain compliance with the Payment Card Industry Data Security Standards (PCI-DSS). The University of Southern Mississippi Payment Card Security Policy and additional supporting documents provide the required guidance for processing, transmission, storage and disposal of cardholder data. This is done in order to reduce the institutional risk associated with the handling of payment card data and to ensure proper internal control and compliance with the PCI-DSS.

It is the policy of The University of Southern Mississippi to allow acceptance of payment cards as a form of payment for goods and services upon written approval from the university Merchant Services/PCI Compliance Committee. The University of Southern Mississippi requires all departments that accept payment cards to do so only in compliance with the PCI DSS and in accordance with the procedures outlined in this policy document, The University of Southern Mississippi “Administration and Department Procedures” and other supporting documents.

Review

The Director of Student Financial Services is responsible for review of this policy annually.

Forms/Instructions

Annual Merchant Survey Renewal
Department Policy Template

Appendices

N/A

Related Information

Administration and Department Procedures
Information Security Incident Response Plan
Department Payment Card Responsibilities

History

New policy instituted in 2016.


Amendments: N/A

Authorization

Title: Payment Card Security Policy

Policy number: ADMA-BUS-009

RECOMMENDED BY:



Responsible University Administrator

7-26-16

Date

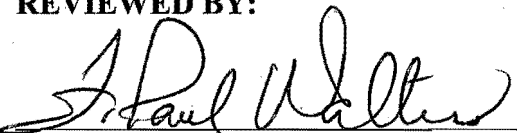


Responsible University Officer

7.26.16

Date

REVIEWED BY:



Director of Compliance and Ethics

7/29/16

Date




Office of General Counsel

29 JUL 2016

Date

APPROVED:



President

8.1.16

Date