

**Administration and Department**

**Payment Card Procedures**

**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 department and the University.

**PCI DSS**

The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express 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)

In order to accept credit card payments, The University of Southern Mississippi must prove and maintain compliance with the Payment Card Industry Data Security Standards. The University of Southern Mississippi Payment Card Security Policy and additional supporting documents provides the requirements for processing, transmission, storage and disposal of cardholder data of payment card transactions in order to reduce the institutional risk associated with the administration of credit card payments by university departments to ensure proper internal control and compliance with the Payment Card Industry Data Security Standard (PCI-DSS).

**Procedures**

In the course of doing business at The University of Southern Mississippi, including affiliated organizations, it may be necessary for a department or other unit to accept payment cards. The University of Southern Mississippi requires all departments that accept payment cards to do so only in accordance with the PCI DSS and the following procedures.

## 1. Card Acceptance and Handling

The opening of a new merchant account for the purpose of accepting and processing payment cards is done on a case by case basis. Any department requesting a new merchant account must adopt the University’s approved solution for maintaining compliance. Any costs (e.g. equipment, device management, encryption, processing fees, etc.) associated with the acceptance of payment cards in a department, will be charged to the department.

* 1. Interested departments should contact the Director of Student Financial Services to begin the process of accepting payment cards. Steps include:
		1. Completion of an “Application for Department Merchant Account”
		2. Approval by the Tax Compliance Office to accept payments on behalf of the University for goods or services.
		3. Read and sign-off on the University Payment Card Security Policy and supporting documents.
		4. If applicable, email itbilling@usm.edu to request information and approval for E-Commerce (online payments via the University’s approved internet processor).
	2. Any department accepting payment cards on behalf of the institution must designate an individual within the department who will have primary authority and responsibility within that department for payment card transactions. This individual is referred to as the Merchant Department Responsible Person or MDRP. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the MDRP is unavailable.
	3. Specific details regarding processing and reconciliation will depend upon the method of payment card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and are also available by contacting Business Services.
	4. All service providers and third party vendors that provide payment card services must be PCI-DSS compliant and approved by the Merchant Services/PCI Committe. Departments who contract with third-party service providers must maintain a list that documents their service providers and:
		1. Ensure contracts include language that states the service provider or third party vendor is PCI complaint and will protect all cardholder data.
		2. Annually audit the PCI compliance status of all service providers and third-party vendors. A lapse in PCI compliance could result in the termination of the relationship.

## 2. Payment card Data Security

All departments authorized to accept payment card transactions must have their card handling procedures documented and made available for periodic review. Departments must have the following components in place within their procedures and ensure that these components are maintained on an ongoing basis.

***PROCESSING AND COLLECTION***

* 1. Access to cardholder data (CHD) is restricted to only those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access to CHD and review the list monthly to ensure that the list reflects the most current access needed and granted.
	2. Equipment used to collect cardholder data is secured against unauthorized use or tampering in accordance with the PCI DSS. This includes the following:
		1. Maintaining a list of devices and their location;
		2. Periodically inspecting the devices to check for tampering or substitution;
		3. Training for all personnel to be aware of suspicious behavior and reporting procedures in the event of suspected tampering or substitution.
	3. Email must never be used to transmit payment card or personal payment information, nor should it be accepted as a method to supply such information. In the event that it does occur, disposal as outlined below is critical. If payment card data is received in an email then:
		1. The email should be replied to immediately with the payment card number deleted stating that "The University of Southern Mississippi does not accept payment card data via email as it is not a secure method of transmitting cardholder data".
		2. Provide a list of the alternate, compliant option(s) for payment.
		3. Delete the email from your inbox and also delete it from your email Trash.
	4. Fax machines used to transmit payment card information to a merchant department must be standalone machines with appropriate physical security; receipt or transmission of payment card data using a multi-function fax machine is not permitted.

***STORAGE AND DESTRUCTION***

* 1. Cardholder data, whether collected on paper or electronically, is protected against unauthorized access. Never store the Primary Account Number (PAN), expiration date, track data, security codes, and PIN number post authorization.
	2. Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents or electronic files containing cardholder data.
	3. No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe, or the card-validation code.
	4. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants and portable external hard drives.
	5. Cardholder data should not be retained any longer than a documented business need; after which, it must be deleted or destroyed using a PCI DSS-approved method of destruction. The maximum period of time the data may be retained is six months. A regular schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the required retention period.

## 3. Responding to a Security Breach

In the event of a breach or suspected breach of security, the department or unit must immediately contact the University Help Desk and execute The University of Southern Mississippi Information Security Incident Response Plan.

## 4. Sanctions

Failure to meet the requirements outlined in this policy may result in suspension of the physical and, if appropriate, electronic payment capability with payment cards for affected unit(s). In the event of a breach or a PCI violation, the payment card brands may assess penalties to the University’s bank which will likely then be passed on to the University. Any fines and assessments imposed on the University will be the responsibility of the impacted unit. A one-time penalty of up to $500,000 per card branch per breach can be assessed as well as on-going monthly penalties.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University of Southern Mississippi will carry out its responsibility to report such violations to the appropriate authorities.

**Definitions**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **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, JCB
 |
|  |  |
| **Cardholder** | Someone who owns and benefits from the use of a membership card, particularly a payment card. |
|  |  |
| **Card Holder 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:* Cross-cut shredding, Incineration, Approved shredding or disposal service
 |
|  |  |
| **Merchant 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. |
|  |  |
| **Merchant Department Responsible Person****(MDRP)** | An individual within the department who has primary authority and responsibility within that department for payment card transactions. |
|  |  |
| **Third Party Vendor** | Third-party vendors are classified into two categories for the purposes of these procedures. * Third-party vendors who contract to do business with and accept credit/debit payments on behalf of a university merchant. The payments accepted by these third-party vendors must be deposited to the university’s bank account. Examples of this type of third-party vendor include the ticket system for athletics and the Arts. These third-party systems are used to meet the specific needs of certain university merchants. Guidelines governing this type of third-party vendor are contained within this manual.
* Third-party vendors who contract to do business as a location on University property. Examples of this type of third-party vendor include the university bookstore provider (Barnes & Noble) and the University food services (Aramark). While these vendors are outside the scope of this policy, it is imperative the initiating department ensures these third-party contracts with the University address compliance with PCI
 |
| **Database** | A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets. |