

**Department Payment Card**

**Responsibilities**

**Purpose:**

Each department that handles credit and debit card information must have written procedures tailored to its specific organization that are consistent with the University’s Administration and Department Procedures and PCI-DSS. Departmental procedures are reviewed, signed and dated by the department head on an annual basis indicating compliance with the University’s Payment Card Security Policy. These procedures are submitted to and approved by the Dean or Vice President, and the Merchant Services/PCI Committee.

This document is intended to provide assistance in the development of the departmental procedures required by the PCI-DSS. Departmental procedures should describe the entire transaction process and include, but are not limited to, the following:

* Segregation of duties
* Deposits
* Reconciliation procedures
* Physical security
* Disposal
* Cash register procedures (if applicable)

**Responsibilities**

* Any department accepting payments on behalf of the University for goods or services must have received approval from the Tax Compliance Office prior to receiving a merchant account.
* Departments should designate an employee within the department who will have primary authority and responsibility for payment card and/or ecommerce transaction processing within that department. Responsibilities include:
	+ Departmental compliance with the security measures established by the payment card industry and university policies.
	+ Ensuring any employee who handles cardholder data completes the annual training and signs an acknowledgement indicating their understanding of and adherence to the policies.
	+ Completion of the annual PCI-DSS Self-Assessment Questionnaire (SAQ)
	+ Completion of the Annual Merchant Survey

Any changes in this designee must be communicated to the Director of Student Financial Services immediately.

* Department Head must review and sign the completed PCI DSS Self-Assessment Questionnaire (SAQ) and Merchant Survey on an annual basis.
* Departments may NOT place orders for new or replacement payment card terminals. If the payment card processor recommends a replacement terminal, the department may NOT accept one before contacting University Business Services first. All terminals are procured through the University Business Services office.
* University Business Services will obtain merchant numbers for Visa, MasterCard, Discover, and American Express (if the department chooses to accept). All payment card equipment and terminals will be obtained and programmed by the University Business Services for the department. Equipment costs will be billed to the department.
* Departments may only use the services of vendors which have been approved by the Merchant Services/PCI Committee to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order or internet based
* Departments must notify University Business Services of software upgrades and changes related to credit card processing.
* Departments using POS systems must provide all outward facing IP addresses used in the processing and/or transmitting of credit card data for external scanning.
* Payment card numbers must not be transmitted in an insecure manner, such as by e-mail or chat, unsecured fax, or through campus mail. Similarly, payment card data must not be stored insecurely in any form, such as paper forms or received faxes.
* University employees must not direct any cardholder to a general purpose computer to make a payment
* University employees must not enter cardholder data (CHD) into a general purpose workstation for a customer.
* Sensitive cardholder data [i.e., full account number, expiration date, PIN, and card-validation code] must never be stored in any University system or personal computer after the payment has been authorized.
* The entire payment card number must not be printed on either the merchant copy or customer copy of any receipts; it is permissible to include the first six and last four digits only. Old documents containing the entire card number should be cross-cut shredded or all but the last four digits punched out with a hole-punch.
* All documentation containing card numbers must be stored in a secure environment until processed. Secure environments include locked drawers and safes, with limited access to only individuals who are authorized to handle the payment card data. Processing should be done as soon as possible and the payment card number should immediately be destroyed as described above.

* All media used to store payment card data must be destroyed in a PCI-compliant manner when it is no longer needed for business or legal reasons. Please see below for the options for proper disposal.
	+ Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.
	+ Storage containers used for materials that are to be destroyed must be secured.
	+ Cardholder data on electronic media must be rendered unrecoverable (e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).
* Limit access to system components and cardholder data to only those individuals whose job requires such access
* Employees who handle or have access to cardholder data are required to participate in annual payment card security training provided by Business Services/iTech.
* Units using third-party software, including POS systems, are prohibited from storing complete payment card numbers on university computers at any time.
* Units using third-party software, including POS systems, must keep documentation of all agreements and configurations related to the software for audits or in case of an emergency.

In case of a suspected compromise or theft of credit card data:

* Immediately contact the iTech Helpdesk by phone (601.266.4357) or by email (helpdesk@usm.edu)
* Execute the University’s Security Incident Response Plan