ADMINISTRATIVE POLICY

Policy Title:	Credit Card Security Policy
Policy Subtitle/Subject	Maintain Credit Card Security
Responsible Executive(s) (RE)	Senior Vice President and Chief Operating Officer
Responsible Office(s) (RO)	Controller's Office
Primary Point of Contact from RO	Garrett Platner
Contact Information (email and phone)	gplatner@tulane.edu 504-314-2666
Date Proposed	7/2/24
Reviewed	
Last Updated	10/15/24
Effective Date	

Permanent	Temporary
X	

1.0 POLICY STATEMENT

All Tulane University departments/units that collect, process, transmit and/or store cardholder data must comply with all the requirements of the latest version of the Payment Card Industry Data Security Standard (PCI DSS).

Departments that anticipate payment card (i.e. debit or credit card) acceptance for goods and/or services must be approved by the PCI Compliance team which is comprised of members from the Controller's Office and the Division of IT. The provisions of this policy also apply to all existing University departments that have previously been approved for payment card processing. Departments that use third party vendors to accept payment cards are also subject to compliance requirements of this policy,

this includes vendors providing goods and/or and services on campus, and other entities or organizations that process payment cards.

2.0 PURPOSE AND SCOPE

The University designates the Controller's Office (CO) as responsible for setting up and maintaining oversight of all merchant accounts. Departments are not authorized to independently establish relationships with credit card processors. It is understood that merchant accounts support processing both deposits and "negative" deposits to the university bank account.

3.0 APPLICABILITY OF THIS POLICY

The University has a fiduciary responsibility to protect our customers' payment card information. Cardholder data is of high value to malicious individuals because the information can be used for fraudulent purposes. Therefore, we must ensure that appropriate safeguarding measures are in place to protect cardholder data and continuously demonstrate PCI DSS compliance.

The PCI DSS is a set of comprehensive requirements for enhancing cardholder data security, which is intended to help organizations proactively protect cardholder data and was developed by the founding payment brands (i.e. Visa, Mastercard, Discover, American Express, and JCB) of the Payment Card Industry Security Standards Council. All payment card activity on behalf of Tulane University, at the University, or using Tulane University resources must comply with the PCI DSS. Failure to comply may result in fines, legal liability, reputation damage and loss of business.

4.0 WEBSITE ADDRESS FOR THIS POLICY

https://policy.tulane.edu/policy-library

5.0 CONTACTS

PCI Committee tulanepci@tulane.edu	Garrett Platner gplatner@tulane.edu 504-314-2666		

6.0 CONTENTS

7.0 DEFINITIONS

Acquirer - Also referred to as "acquiring bank" or "acquiring financial institution". Entity that initiates and maintains relationships with merchants for acceptance of payment cards.
Approved Scanning Vendor (ASV) Company approved by the PCI Security Standards Council to conduct scanning services to identify common weaknesses in system configuration.

Business Need-to-Know - When an employee's access rights are granted to only the least amount of data and privileges needed to perform a job.

Cardholder Data - At a minimum, cardholder data contains the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, service code, and/or other sensitive authentication data.

Cardholder Data Environment (CDE) - Area of computer system network that processes cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

Data Breach - A data breach is an incident in which sensitive data may have potentially been viewed, stolen, or used by an unauthorized party.

Malware - Malicious software designed to infiltrate a computer system with the intent of stealing data, or damaging applications or the operating system. Such software typically enters a network during many business approved activities such as via email or browsing websites.

Merchant - A University department approved to accept payment cards at a given location as payment for goods and/or services or receipt of donations.

Merchant ID Number (MID) - A unique number that identifies the University department approved to accept payment cards.

Payment Card Application - Any hardware, software, or combination of hardware and software that aid in the processing, transmitting or storing of cardholder data as part of authorization or settlement. Examples include: point of sale (POS) devices, e-commerce shopping carts, web-based payment applications and third party (vendor) provided systems.

Payment Card Industry Data Security Standard (PCI DSS) - PCI DSS is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands. The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. The PCI DSS may be accessed at: https://www.pcisecuritystandards.org/.

Self-Assessment Questionnaire (SAQ) - A validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. There are multiple types of the PCI DSS SAQ to meet various payment card processing scenarios. Each unique version of the PCI DSS SAQ includes a Self-Assessment Questionnaire and Attestation of Compliance, which must be completed annually by the merchant and/or service provider as appropriate. The Tulane University PCI Compliance Team will assist you in the selection and completion of the SAQ for your merchant location.

Payment Card Processing - The processing, transmitting and/or storing of cardholder data, i.e. acceptance of credit or debit cards.

Primary Account Number (PAN) - Unique number for credit and debit cards that identifies the cardholder account.

Qualified Security Assessor Company (QSAC) - A company approved by the PCI Security Standards Council to validate an entity's adherence to PCI DSS requirements.

Service Provider - A business entity that provides various services to merchants. Typically, these entities store, process, or transmit card data on behalf of another entity (such as a merchant) OR are managed service providers that provide managed firewalls, intrusion detection, hosting, and other IT-related services.

Vulnerability Scan - A software tool that detects and classifies potential weak points (vulnerabilities) on a computer network.

Card Present Transactions - Transactions are considered "card present" if the Card Verification Value (CVV)1 is submitted at the time of the transaction. The CVV1 is contained only when using the magnetic stripe, chip, or contactless payment methods and is not the three-digit or four-digit verification code seen on the card (aka. CVV2, CVC2) that is more commonly known. Therefore, such transactions require that

the physical card must be presented at the time of the payment and the payment data entered by swiping, inserting (Europay, MasterCard, and Visa (EMV)), or tapping (Near Field Communication (NFC)) the card.

Card Not Present Transactions - Transactions are considered "card not present" if the CVV1 is not submitted at the time of the transaction because the physical card is not presented. Payments made over the telephone or Internet or sent via mail fall into this category.

8.0 POLICY AND PROCEDURES

8.1 Card Present Transactions

If your department accepts in person payments, follow the departmental procedures listed.

- Attach any/all form(s) where payment card information is requested (if applicable)
- Only approved merchant employees can process credit card transactions and/or handle cardholder information.

8.2 Card Handling Policies

- Review Card Security
    - Confirm the card is valid. The card may not be used after the last day of the expiration month embossed on the card.
    - Only the actual card/account holder should be using the card. (Ask for Picture ID)
    - Does the customer's current signature match the signature on the back of the card? Compare the signatures and make sure that the signed name is not misspelled or otherwise obviously different.
    - Does the signature panel on the card look normal? Check to be sure that it has not been taped over, mutilated, erased, or painted over. Obvious physical alterations to the card could indicate a compromised card.
    - Does the account number on the front of the card match the number on the back of the card and the terminal receipt display? If the numbers do not match, or if they are covered or chipped away, this could indicate an altered card.
    - Does the name on the customer receipt match the embossed name on the front of the card? If the name is different, this could indicate an altered card.
- Risks of Keyed Transactions
    - Manually keying in the card account information carries a higher risk of fraud since many of the built-in card security features cannot be accessed. If the magnetic stripe, chip, or contactless are unusable, or if you choose to process transactions manually, follow these steps:
        - Key the transaction and expiration date into the terminal
        - Ask the cardholder to sign the paper receipt and compare the signature
- Report Suspected Card Fraud
    - If you suspect the card is fraudulent, report it following the security breach steps outlined in the "Other Considerations" section.

- Retain the signed merchant copy of the swipe machine-generated receipt and return the other copy to the cardholder.
    - Place the merchant copy of the receipt in a secure location until the end of day batch process has been run.
- Oversight of the payment card terminal (NOTE: *PCI DSS has physical security requirements.)*
    - Periodically log the information into the (*required*) **Merchant Device Inventory and Tampering Checklist** while checking the machine daily to determine if it has been tampered with or exchanged (i.e. verify stickers have not been removed and re-affixed, same model, same serial number, etc.). These logs may be requested at any time to ensure compliance with the policy.
    - Report any tampering as a security breach per the steps outlined in the "Other Considerations" section.
    - When possible, keep the machine in a locked area when not in use or after hours.

8.3 Card Not Present Transactions

Transactions are considered "card not present" if the CVV1 is not submitted at the time of the transaction because the physical card is not presented. **Payments made over the telephone or Internet, or sent via mail or fax fall into this category. Manual entry of payment data is considered card-not-present even if the card is present.**

8.3.1 Mailed Payments

If your department accepts mailed in payments, follow the departmental procedures below.

- At least two people should be responsible for opening the mail and processing any payment transactions. If possible, these staff members should alternate days. The transaction(s) must be processed within one business day from when the user has access to the cardholder information.
- Bundle together all payment requests and attach a cover sheet with the date, count of requests, and initials of the person opening the mail.
- Hand over the bundle to the person responsible for entering the payment(s).
- Process the payments using the approved departmental method (i.e. hosted payment application, terminal, etc.) and print out two copies of the receipt.
- The portion of the form containing the payment card information must be destroyed after the transaction has been processed in an approved PCI manner. Options for acceptable destruction include removing and cross-cut shredding or rendering it unreadable on the form (i.e. hole-punch through the card number, expiration date, and security code). Obscuring CHD (writing/scribbling over the card number) is NOT an acceptable disposal method for cardholder data. Proper disposal requires physical destruction as defined by the PCI DSS.
- Return a copy of the receipt to the customer via the approved departmental method which is *{mail / fax / scan / email}*. Retain the other copy in a secure location to use if a refund is later issued.
- Place the merchant copy of the receipt in a secure location until the End of Day batch process runs.

8.3.2 Telephone Payments

If your department accepts telephone payments, follow the departmental procedures below.

- All telephone payments should be entered into the payment terminal or application during the call. If not possible, the transaction(s) must be processed within one business day from when the

user has access to the cardholder information. Do not accept payment information via a voicemail/phone message.
- If payment data must be written down, it should be recorded on your department's credit card authorization form and processed during or immediately after the call has concluded. The portion of the form containing the payment card information must be destroyed in an approved PCI manner. Options for acceptable destruction include removing and cross-cut shredding, or rendering it unreadable on the form (i.e. hole-punch through the card number, expiration date, and security code). Obscuring CHD (writing/scribbling over the card number) is NOT an acceptable disposal method for cardholder data. Proper disposal requires physical destruction as defined by the PCI DSS.

8.3.3 Fax Payments

Tulane does not accept payments via fax.
- Cardholder data cannot be transmitted via fax for any University purposes.
- If a credit card number is received via fax for University purposes, the document should be destroyed using a cross-cut shredder and the sender notified that this payment process cannot be accepted.

8.3.4 E-Mail Payments

Tulane does not accept payments via email.
- Cardholder data cannot be transmitted via email for any University purposes.
- If a credit card number is transmitted via e-mail, the file should be immediately deleted and removed from the deleted emails folder. The message cannot be handled in any other way. The sender should be notified that this payment process cannot be accepted. IT must be notified to securely remove the email from the system.

8.3.5 Online Payments

If your department accepts online payments, follow the departmental procedures below.
- All online payments must be processed only by the customer. Technical resources such as networks, workstations, servers, and other resources owned, managed, or otherwise the responsibility of Tulane cannot be brought into any cardholder data environment.
- Payments entered into an online application using data received in-person, on the telephone, or via a paper form (i.e. fax, mail) must be handled according to the procedures defined in each relevant section above.
- Payments entered into an online application using data received in-person, on the telephone, or via a paper form (i.e. fax, mail) must be handled according to the procedures defined in each relevant section above.

8.4 Back-Office Procedures

8.4.1 Refunds

Refund processing policies are described below:
- Refunds must be issued using the same mode of processing that was used for the original transaction.

- Refunds must be issued to the same payment card number that was used for the original transaction.
- If the card holder can provide documentation that the original payment card account number has been closed, the department may issue a refund to another payment card the cardholder has.
- The refund amount may only be up to the amount of the original transaction.
- No individual should be processing payments and refunds, however if the department has insufficient personnel to implement such segregation of duties then the refund must be approved by a supervisor or department head by signing the refund receipt attached to the original transaction receipt.

8.4.2 Chargeback/Dispute Process

A chargeback is a processed credit card transaction that is reversed (charged back) to a merchant because the customer or customer's bank finds something wrong with the transaction. The Merchant Services team will notify you via e-mail of your recent chargeback/dispute. It is the responsibility of your department to provide supporting documentation of such. All chargeback documentation for Visa, MasterCard, American Express, and Discover cards, should be received and sent electronically.

It is imperative that your department maintain accurate record keeping and documentation accordingly.

8.4.3 Record Retention

Need to know Louisiana's laws regarding this.

9.0 CONSEQUENCE OF VIOLATING THE POLICY

Violation of this policy may result in disciplinary action, up to and including termination and/or criminal prosecution.

APPENDIX I

Systems Configuration

Work with the Division of IT and/or your technical contact in your department to ensure that:

- Anti-virus software is implemented and updated regularly on all systems and devices. This is to protect the workstation.
- Vendor operation system and application patches are installed in a timely manner.
- Data detection and data encryption software are implemented to ensure that all confidential data is identified, secured or deleted. This is to protect the workstation.
- If external vendors or third-parties need access to service any third-party applications or software, access should only be granted for the time needed to complete the necessary task and then immediately disabled.

APPENDIX II

Other Considerations

Directing cardholders to kiosks/workstations to enter CHD is prohibited.

Many departments use third-party payment systems or gateways for online payment card processing. Customers should be directed to complete payments online using their own personal device. If you are specifically directing people to use computer labs, kiosk machines, or other public-use computers to make payments, this can inadvertently bring these devices into PCI scope. Therefore, DO NOT direct customers or offer payment card entry on any device that has not been properly secured or approved by the PCI Compliance Team.

Suspected breach of security or fraud

Follow the process below in the event of a credit card security breach or incident:

- Notify your supervisor and the PCI Compliance Team via email at [PCI TEAM EMAIL] immediately.

- Follow guidelines in Tulane's Emergency Response Plan outlined here: https://tulane.app.box.com/s/r9spno75zlhvyfi7p55omr1h64yjnzlg/file/1278938301462