The University of Texas Rio Grande Valley

Policy Number: ADM 10-701
Responsible Executive: Finance and Planning
Originated: 09/01/2015

Handbook of Operating Procedures

CASH AND CREDIT CARD HANDLING AND REPORTING

A. Purpose

The purpose of this policy is to institute controls and standardize cash and credit card management at The University of Texas Rio Grande Valley (UTRGV) to ensure the safe, proper handling of cash and of sensitive information in the processing of credit card transactions.

B. Persons Affected

This policy applies to all employees or students of UTRGV who are responsible for accepting, managing, or in any way assisting with the handling of cash, checks, or credit cards in the name of UTRGV for any purpose.

C. Policy

1. In furtherance of UTRGV's fiduciary responsibilities, it is the policy of UTRGV:
   a. to require departments and employees receive administrative authorization prior to handling cash and credit-card operations;
   b. that employees approved for cash-handling and credit-card functions receive training regarding proper cash handling requirements;
   c. that employees and departments consistently manage the handling, receipting, depositing, and reporting of all cash operations or cash-related activities in a manner that promotes the security of UTRGV assets;
   d. to periodically review and adopt security measures for cash and credit card handling, such as the Payment Card Industry Standards adopted by the institution; and
   e. to adhere to the Payment Card Industry Data Security Standard (PCI DSS) developed and maintained by the Payment Card Industry Security Standard Council (PCI SSC) and adopted by UTRGV, since departments that collect credit card payments for goods and services (including online payments) are considered merchants for the purposes of the PCI DSS.
2. Before a merchant department may receive credit card payments, it must develop and implement adequate security and internal controls that meet PCI DSS standards as well as any security standards required by the Chief Information Security Officer (CISO) or this policy.
3. UTRGV and the payment card industry take the safeguarding of cardholder data seriously. Failure to comply with the requirements of this policy, or adopted PCI standards or UTRGV standards, may result in the revocation of a department's merchant account or, in the case of lost or stolen cardholder data, assessment of fines on the department by the bank. The individual department will be financially responsible for any fines resulting from security breaches that originate from their systems.

4. Treasury is responsible for administering the UTRGV credit-card program and for ensuring that participating departments are provided updates on all rules, procedures, and security standards, including annual or as-needed training in order to satisfy authorization requirements. These responsibilities include:

    a. Coordinating with the merchant bank on the merchant's behalf, including cases of a suspected security breach;

    b. distributing and coordinating the preparation of the annual PCI questionnaire by each merchant;

    c. working closely with both the merchant and UTRGV CISO Office to ensure that all necessary security procedures are in place to ensure protection of sensitive credit card data; and

    d. performing periodic and annual assessments to ensure compliance with the requirements outlined in this policy.

    The University Treasurer, in consultation with the PCI taskforce committee, is responsible for recommending the revocation of the ability to accept credit cards for any merchant department that fails to comply with the PCI DSS or this policy.

5. The UTRGV CISO Office is responsible for approving the configuration of merchants' PCI computer systems. The UTRGV CISO Office team is responsible for performing vulnerability scans of PCI computer systems, and may require configuration changes to eliminate vulnerabilities. This is both in preparation for and in addition to vendor scans required for PCI compliance. Vulnerabilities must be mitigated as soon as practical. To meet UTRGV security needs, the UTRGV CISO Office standards may be stricter than the PCI requirements.

6. The UTRGV CISO will assist merchants in assessing its payment card processes, applications, and migration to a PCI DSS compliant solution and with consultation from Treasury. UTRGV CISO will provide technical assistance to Treasury and verify requirements with the current PCI DSS, to include terminals, workstations, firewalls, and any other network component as part of the card holder data environment.

D. <u>Procedures</u>

1. *Approvals*

    a. All departments that use departmental change funds or accept cash, checks or credit cards in the name of UTRGV for any purpose must obtain prior written approval from the Financial Services – Treasury. The original written approval must be kept on file in Treasury and a copy maintained at the Bursar's Office and the requesting department.

    b. Departments that accept credit cards must complete the merchant credit card setup request form provided by Treasury. The UTRGV CISO Office must approve of the computer system and network that will be used by the department for credit card processing before system/network can be used. For School of Medicine merchants, Treasury will submit a request online via Athena application.

c. Merchant accounts must be in place before credit cards may be accepted. Accounts can be revoked for failure to comply with credit-card processor guidelines or applicable UTRGV policies.

d. A PCI Self-Assessment Questionnaire must be completed and submitted to Treasury for each credit card merchant.

2. *Billing & Mailing of Payments*

a. All employees who initiate contracts, memorandums of understanding, affiliation agreements, interagency agreements, royalty agreements, vendor agreements, invoices, or any other solicitations involving payments to UTRGV must ensure that the agreement or other document instructs the payor to remit payment to the Bursar's Office or by ACH, with the exception of all private-source gifts governed by ADM 10-803 Gifts – Solicitation, Acceptance, Processing, and Acknowledgment. The payment should be made payable to UTRGV and may not be made payable to any individual employee. Departments must coordinate specific billing information through the Accounts Receivable (AR) Department.

b. Each department is required to provide invoice/billing and other relevant information to the Bursar's Office to identify the payment for allocation to the proper account.

3. *Acceptable Methods of Credit Card Payment Processing*

i. In Person – In-person payments may be accepted through a point-of-sale terminal procured through UTRGV's payment card processor.

ii. By Telephone – To accept payments by telephone, a department must establish secure processes in how cardholder data is handled, how data processed for payment, and how data is disposed. These processes must be reviewed and approved by Treasury to ensure that all appropriate data security standards are met, before payments can be accepted.

iii. Online – Online payments may be accepted through UTRGV's online processor solutions, described in Section D.4.k.

iv. By Mail - This payment method requires pre-approval from Treasury.

4. *Responsibilities of Cash Handling and Merchant Departments*

a. Handling and Monitoring Cash

i. The department head for each location where cash is maintained or accepted is responsible for assuring that proper procedures are followed for handling and monitoring cash. All cash received should be recorded and handled under appropriate internal controls. If the department head has appointed a custodian, the custodian of a change fund has shared responsibility for the fund.

ii. Procedures are to include, but are not limited to, ensuring proper segregation of duties exist among staff; maintaining complete documentation and audit trails;

completion of required cash handling training by applicable staff members; conducting random audits; ensuring sequential receipting, and balancing; and completing reports timely and accurately. The documentation of transactions and the balancing of cash at all points of transfer and transport are critical to maintain accuracy and safety of cash transactions.

b. Credit Card Refunds

Credit card refunds cannot be issued for more than the original transaction amount and can only be refunded on the card used for the original purchase within a finite number of days.

c. Security Measures – Cash

i. The department head or their custodian are expected to ensure that adequate security measures are taken for the control of the institutional funds and the safety of all personnel handling cash.

ii. When not in use, cash or related items must be stored in a safe, cash register, locked drawer or locked box. Cash or cash related items should never be left unattended during working hours. All cash operations or processing areas must be secured from entry by unauthorized people. When safes are used, it is recommended that combinations be changed periodically and sent under seal to the UTRGV Police Department.

d. Security Measures – Credit Cards

i. All equipment, software, and business processes must comply with current PCI security standards and standards established by the UTRGV CISO Office. To provide adequate security, the combined efforts of the business and information technology functions within the department or college are necessary.

ii. The design and architecture of computer systems and networks associated with credit card processing, as well as the protocols used to transmit such data, must be approved by the UTRGV CISO Office prior to implementation. Subsequent changes must also be approved prior to implementation.

iii. In addition to completing the initial PCI Compliance Questionnaire during setup, each merchant is required to complete an annual PCI self-assessment questionnaire.

iv. Credit card numbers should only be stored electronically as a last resort, and then only in full compliance with the most recent PCI DSS requirements.

v. Card data should never be transmitted over end user technologies such as email, texting, instant messenger, or any other application.

vi. Individuals who have access to cardholder data must meet the requirements of Sections D.4.h-i below.

vii. Merchant departments must ensure that the storage of printed cardholder data (such as merchant copies of receipts or daily batch reports), are secured in a location with access limited to those with a legitimate business need.

viii. Before engaging with third party service providers who support the transaction process (through software, equipment, hosting, personnel, etc.), merchant departments must ensure the vendor can prove PCI compliance, can take contractual responsibility for cardholder security to the extent of their control, and can commit to ongoing PCI security compliance.

ix. The UTRGV CISO Office will perform periodic reviews of computer or computer networks to ensure that security features are in place and are adequate to protect credit card data. Treasury will periodically perform reviews of business procedures to help merchants identify ways to better protect cardholder information. Reviews are also available upon request.

e. Cash Over/Short Differences (Unreconciled Cash)

i. Cash over/short amounts, often referred to as unreconciled cash amounts, must be reported and accounted for within 24 hours. Cash shortages in excess of $25.00 must be reported to the UTRGV Police Department, and an incident report must be completed and communicated to the appropriate stakeholders, including staff within Treasury, the Financial Services organization, and up to the divisional head.

ii. Cash overages in excess of $25.00 must be reported to the immediate supervisor, the department administrator, Treasury, and Bursar’s Office. All overages will be deposited immediately to the institutional over/short account.

f. Change Funds Restrictions

Absolutely no borrowing, lending, or check cashing from any UTRGV cash operation is permitted. Private or personal funds may not be combined with change funds.

g. Closing Cash Funds

When the need for cash funds ceases to exist, department heads or delegated custodians are responsible for ensuring that all cash be deposited at the Bursar’s Office(s) and notify Treasury to properly close out the cash fund. Any change in custody must be documented and made in the presence of the current custodian and either the new custodian or the department head/administrator. The Bursar’s Office and Treasury must be notified by the department head/administrator within three (3) business days if the custodian of a change fund transfers to a different department or terminates employment from UTRGV.

h. Employee Clearance (Background Checks)

All prospective employees with job responsibilities involving the handling of cash in any capacity or access to cardholder data must successfully complete required background checks under ADM 04-202 Employee Criminal Background Check before assuming their duties. For security reasons or as otherwise necessary to meet the institution's fiduciary responsibilities, post-hiring background checks may be conducted on current employees as needed to verify the employees' continued eligibility for employment.

i. Employee Training

i. Each employee that is identified to be handling cash must complete the Cash Handling training. Each department is responsible for identifying those employees to be trained; for submitting a form to the Bursar's Office to request that the employee(s) attend Cash Handling training prior to the employee(s) assuming cash handling tasks; and for employees completing a renewal class every two years. The required training includes employees that handle cash and their supervisors.

ii. Merchant staff who answer questions on the annual PCI questionnaire or who have access to cardholder data, including IT staff who support payment systems, are required to complete an online PCI Security training course. Annual refresher courses are also required. The merchant department is responsible for providing sufficient training to volunteers based on the types of transactions volunteers may process. For more information on available training, please contact at Treasury@utrgv.edu .

j. Endorsements

i. Checks

i.i All checks should be made payable to "The University of Texas Rio Grande Valley." A restrictive endorsement in the name of UTRGV must be placed on each check at the time of receipt. The restrictive endorsement must say the following:

1. For Deposit Only
2. UTRGV
3. (Your Department Name)

i.ii Each check received by a UTRGV employee must be stamped with an endorsement stamp. All checks returned to UTRGV as insufficient funds (NSF) will be aggressively pursued for payment. To the extent allowed by law, a return fee of at least $25.00 shall be applied to any check returned for insufficient funds. Failure to comply with these endorsement guidelines may result in rejections from the bank or delays in deposits into their respective cost centers/projects.

ii. Cashiers

Prior to finalizing a transaction, cashiers must write the customer's driver's license number or other government-issued identification on the back of the check, along with a UTRGV Student ID Number or UTRGV Employee ID if applicable.

iii. Deposits

iii.i In general, all UTRGV departments (including the School of Medicine clinics) should make deposits on a daily basis unless other accommodations have been made with Financial Services/Comptroller.

iii.ii All departments transmitting deposits must secure funds by utilizing a tamper proof locked bag or equivalent (i.e., money bag with lock and key). Any transfer of assets shall be documented and signed by both sending and receiving parties, and a log of these transfers maintained to document the transfers.

iii.iii Deposits consisting of $5,000 or more per day must be transmitted to the Bursar's Office on each of the campuses with police escort or through armored car services. Departments are responsible for contacting UTRGV's Police Department or contracting armored car services to transport such deposits.

k. Online Methods and UTRGV Cashiering System

i. UTRGV Student Pay and UTRGV Non-Student Pay gives campus units the ability to create a fully customized user experience while still providing secure payments. All UTRGV units conducting online payments are required to use one of these methods unless an exception is granted under Section D.4.k.iv.

ii. Accepting online payments comes with a cost for doing business. Merchant departments are responsible for paying credit-card fees charged by the credit card brands, as well as a small per-transaction fee for the use of UTRGV's payment gateway. Treasury can provide estimates upon request.

iii. Payment information must be closely guarded and compliant with the appropriate web security standards approved by the Chief Information Security Officer.

iv. To enroll in either of the two systems, contact Treasury.

v. Any requests for exceptions to this requirement must be submitted in writing and approved by Financial Services organization. The written request for the exception must include a summary of the reasons why these systems will not fit departmental needs; a description of the alternate processes proposed for online payment; a risk assessment and cost-benefit analysis; and a description of the security measures in place ensuring PCI-DSS (in the form of a PCI self-assessment questionnaire) or PA-DSS compliance (in the form of a complete Attestation of Validation).

5. *Disposal of Surplus or Nonfunctional Equipment*

   When a department no longer needs a particular device to swipe or read credit cards, that card-reader must be returned to Treasury for disposal.

6. Internal Audit

   All procedures are subject to a periodic compliance review or audit by the Office of Audits and Consulting Services. An annual confirmation of all change funds and petty cash funds is to be conducted by the Bursar's Office and should include verification of fund amount and identification of the custodian.

7. Unrelated Business Income Taxes (UBIT)

   Subsequent to accepting cash in the name of UTRGV for sales or services rendered, the Tax Compliance Office must make a determination regarding whether the payment received will be considered unrelated business income for the purpose of calculating UBIT. If the payment activities are considered to be UBIT eligible, additional requirements may be imposed on the requesting department(s).

E. Definitions

1. *Automated Clearing House (ACH)* - transactions governed by the National Automated Clearing House Association (NACHA) and controlled through UTS banking services agreement.

2. *Cash* - under this policy, cash refers to currency, checks, credit cards, web payment, and electronic payments (i.e., ACH and wire transfers).

3. *Change Fund* - funds maintained by individual departments authorized to handle cash to be utilized for the sole purpose of carrying on their cashiering operation and **not** for the purpose of obtaining miscellaneous items, paying for minor unanticipated operating expenses, cashing employee checks, or making loans for any reason.

4. *Deposits* - to include all payments of coin, currency, checks, electronic media and all negotiable instruments.

5. *Merchant* - a unit, department or college which processes credit card transactions as a method of payment.

6. *Merchant Accounts* - a unique identification number issued by a merchant processing bank (also called a credit card processor) that allow a business to accept credit, debit, gift, and other payment cards.

7. *Merchant Fees* - monthly fees assessed based on the merchant's total monthly net credit card sales and fixed rate for certain debit transactions.

8. *Merchant Level* - this classification is based on transaction volume. Merchants are ranked as level 1 through 4, with highest-volume merchants as Level 1. Security audit requirements become correspondingly higher with merchant level ranking. Most merchants at UTRGV are the lowest rank, Level 4.

9. *Merchant Processing Bank* - a bank or financial institution that processes credit and/or debit card payments on behalf of the university. Compliance to the PCI DSS is validated directly to this entity.

10. *Online Payment Processor* - all credit card transactions are done through UTRGV's online third-party payment processor. Any exception to this must be reviewed by the UTRGV IT CISO Office as applicable. Approval for the exception will be granted by Treasury.

    a. UTRGV Student Pay is a system of conducting transactions in which the university is responsible for

    b. maintaining the charges displayed to the students online via the third-party application. Students can sign into the third-party application to select charges to be paid and are redirected to the authorized payment gateway for collecting payment.

    c. UTRGV Non-Student Pay is a ready-built shopping cart system hosted entirely by a third party. There are no technical infrastructure requirements for a department to use this system.

11. *Payment Card* - support for cashless payment for goods and services. Examples include, but are not limited to, credit cards, debit cards, and reloadable prepaid cards.

12. *Payment Card Industry Data Security Standards (PCI DSS)* - a set of comprehensive requirements for enhancing payment account data security, developed by the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis. The precise security measures required by a department will vary depending on how credit cards are accepted—in person, over the phone, or on the internet—but all are covered in the PCI DSS.

13. *PCI Security* - refers to a specific set of security requirements put forth by the Payment Card Industry Security Council. Every merchant and service provider in the transaction process is required to maintain compliance with PCI security standards.

14. *Self–Assessment Questionnaire (SAQ)* - a validation tool intended to assist a merchant and third-party service provider(s) in self-evaluating their compliance with PCI DSS.

15. *Third Party Service Provider* - a business entity which is directly involved in the processing, storage, or transmission of cardholder data on behalf of another business. This also includes companies that provide services that control or could impact the security of cardholder data.

F. Related Statutes or Regulations, Rules, Policies, or Standards

The University of Texas System UTS166, Cash Management and Cash Handling Policy

Payment Card Industry Data Security Standards (PCI DSS)

G. Dates Reviewed or Amended

Reviewed and amended – March 18, 2019.

Reviewed and amended – December 22, 2021.