3364-40-24 Credit cards.

(A) Policy statement

To define the policy for the acceptance of credit cards by merchants affiliated with the university of Toledo ("the university" or "UT"). For the purpose of this policy, a merchant is defined as a department or entity affiliated with the university. The university will comply with payment card industry ("PCI") data security standards ("DSS") pertaining to: "card-not-present with all cardholder data functions outsourced" (also known as self-assessment questionnaire,"saq" "a"), "standalone and dial-out terminals – no electronic cardholder data storage" (also known as self-assessment questionnaire "saq" "b"), and "hardware payment terminals in a validated point-to-point encryption" ("saq p2pe-hw").

(B) Purpose of policy

(1) Acceptance of credit cards

(a) The university accepts credit card payments as a convenient service for customers. Departments may accept visa, mastercard, discover, American express, and debit cards with a visa or mastercard logo.

(b) Each department that accepts credit cards for payment must be approved by the office of the treasurer and where applicable approved by the office of the chief information officer before entering into any contract, purchase, acquisition, or replacement of equipment, software, internet provider, or wireless device related to credit cards.

(2) Data security standards

(a) Credit card merchants at the university are required to follow strict procedures to protect customers' credit card data. The credit card companies (including visa, mastercard, discover, and American express) have developed standards which credit card merchants must follow called PCI DSS. All Merchants must comply with the PCI standards (https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php).

(b) While departments may facilitate credit cards on UT computing equipment, they may not transmit, process, or store credit card information on university computer systems or the internet unless specifically approved. Card information may not be stored on university computer systems.

(c) University online sites that cardholders visit must redirect to a PCI approved third party site to transmit, process, or store the credit card information. This should happen automatically upon the processing of the payment. Contact the office of the treasurer for information.

(d) The office of the treasurer and the office of the chief information officer (information security) will coordinate periodic reviews of merchants. Credit card handling procedures are subject to audit by internal audit and compliance or an external audit organization. Departments not complying with approved safeguarding and processing procedures may lose the privilege to serve as a credit card merchant.

(C) Scope

For the purpose of this policy, a merchant is defined as a department or entity affiliated with the university.

All credit card merchants and application systems that process credit card data **that wish to do business with the university of Toledo** must comply with the appropriate PCI standard by June 30, 2015. These merchants must work with the office of the treasurer to ensure the proper level of compliance. The office of the treasurer will engage all necessary university resources to make its determination.

The office of the treasurer is ultimately accountable for the university's state of PCI compliance and for completing the university's annual assessment. Departments that process credit card transactions (under the oversight of the b business manager) will support the office of the treasurer in these efforts. This includes, but is not limited to, the successful completion of all relevant self-assessment questionnaires and an attestation of compliance. The office of the

treasurer will gather, assimilate, and review all departmental data prior to completing the annual assessment.

(D) Key contacts/resources

(1) Office of the cio information security group (http://www.utoledo.edu/it/security/)

(2) Office of the treasurer website (http://www.utoledo.edu/offices/treasurer/index.html)

(3) Office of internal audit and compliance (http://www.utoledo.edu/offices/internalaudit/index.html)

(E) Roles and responsibilities

Note: Responsibilities and procedures for establishing and managing credit cards are complex. This policy provides basic information. Detailed and technical information including systems specifications, contract and liability information is provided in the office of the treasurer credit card merchant/credit card handling responsibilities and procedures. The office of the treasurer is available to provide assistance and address questions as needed.

(1) Setting up a credit card account

(a) To set up a credit card terminal account, please refer to the office of the treasurer website.

(b) To use third-party web providers, software, or a wireless terminal, complete a credit card merchant agreement and request form, accessible through the office of the treasurer website.

(2) Accounting for transactions

(a) The office of the treasurer sends first data ("FD") reports to the department. Treasury will then make transaction entries within the current month to the general ledger based on the department's chart of accounts, and based on

reconciling items identified by both the department and treasury.

(b) A monthly reconciliation to cash process takes place, which includes the following: Treasury (monthly) records any transactions that are not reconciled via the FD report in miscellaneous revenue and cash. Treasury will record the department's appropriate general ledger ("GL") accounts and relieve miscellaneous revenue relieved once a reconciled FD report is received from the department.

(c) It is the department's responsibility to reconcile the settlement amount in the general ledger to the credit card receipts and to the statements issued by the credit card processor on a regular basis, but no less than monthly.

(d) When customers dispute a charge, treasury will notify departments via email regarding any disputed charge card sale. It is a department's responsibility to research and respond within the designated time, including correcting the chargeback if needed.

(3) Credit card data security

(a) Business managers must maintain a department PCI security policy. In addition to complying with established UT policies, supervisors must establish policies and procedures for safeguarding cardholder information and satisfy PCI requirements.

(b) The department is responsible for: (i) establishing procedures to prevent access to cardholder data in physical form, and (ii) prohibiting storing cardholder data electronically. Hard copy media containing credit card information must be stored in a locked drawer or office, with visitor sign-in logs, escorts and other means used to restrict access to documents.

(c) The information technology department has established password protection on computers, per the IT workstation policy, access control policy, and password policy.

(d) Supervisors including deans and business managers must communicate the office of the treasurer credit card merchant/credit card handling responsibilities and procedures to their staff, and maintain responsibilities of credit card handlers and processors documents for all personnel involved in credit card transactions.

(e) All personnel involved in credit card transactions shall do the following:

(i) Charge credit cards for no more than the amount of purchase unless the office of the treasurer has approved the surcharge.

(ii) The signature on the charge card, if available, must agree to the draft.

(iii.) Verify the expiration date on the credit card.

(iv.) In the case of face-to-face credit card transactions, the customer receives the copy of the sales draft that has only four digits of the credit card number. The department retains the other copy and must securely protect these drafts, especially if the drafts have the full sixteen-digit credit card number printed on it. Safeguard drafts in an appropriate locking file cabinet or safe.

(v.) Do not send full credit card numbers via e-mail or fax. Partial credit card numbers sent via email or fax (first four digits and last four digits) is permissible.

(vi.) The cardholder should retain possession of his/her credit card throughout the entire transaction (i.e., a university of Toledo employee should not touch the card).

(f) Access to physical or electronic cardholder data must be restricted to individuals whose job requires access as

approved specifically by the university treasurer. (Reference: 3364-65-02 of the Administrative Code (access control policy) (http://www.utoledo.edu/policies/administration/info_tech/pdfs/3364-65-02_Access control policy.pdf)).

(g) Each person with computer access to credit card information receives a unique identification, with private user names and passwords (Reference: 3364-65-02 of the Administrative Code (access control policy) (http://www.utoledo.edu/policies/administration/info_tech/pdfs/3364-65-02_Access control policy.pdf)).

(h) Storing (electronically or physically) a card verification value code ("cvv" or "cvv2"), or personal identification number ("PIN") number is prohibited. This is a three or four digit number found on the back of most credit cards, except for American express cards where it is on the front of the card.

(i) Do not fax, e-mail, or store full or partial credit card numbers in combination with the three or four digit validation codes (usually on the back of credit cards). Departments will reconcile their weekly credit card transactions against reports run by treasury and emailed to each department representative (partial credit card numbers only -- first five digits and last four digits).

(j) There must be appropriate segregation of duties between personnel handling credit card processing, the processing of refunds, and the reconciliation function.

(k) Departments must perform applicable background checks on potential employees who have access to systems, networks, or cardholder data within the limits of UT human resource policy and local law. This includes established UT employees that may transition to new job roles within the university. If employees have access to only one card number at a time to facilitate a transaction, such as store cashiers in a supervised setting, background checks are not required.

(l) Terminals and computers must mask twelve of the sixteen digits of the credit card number, usually the first six digits and the last four digits of the credit card number.

(m) Imprint machines may not process credit card payments as they display the full sixteen-digit credit card number on the customer copy.

(n) If an employee suspects that credit card information is exposed, stolen, or misused, report this incident immediately to the office of the treasurer and the office of the chief information officer (information security). This report must not disclose by fax or e-mail credit card numbers, three or four digit validation codes, or PINs.

(4) Merchant fees

(a) The credit card companies charge fees based on a variety of factors including the type of card the customer presents. To obtain the lowest rate for credit card terminal transactions the merchant should refer to the office of the treasurer website.

(b) Contact treasury for current fees to process credit card transactions.

(5) Rocket cards (identifications or “IDs”)

(a) Do not process rocket cards on the same equipment as credit cards.

Effective: 10/22/2018

CERTIFIED ELECTRONICALLY

Certification

10/12/2018

Date

Promulgated Under: 111.15
Statutory Authority: 3364
Rule Amplifies: 3364