**Name of Policy:** Credit Cards  
**Policy Number:** 3364-40-24  
**Approving Officer:** President  
**Responsible Agent:** Treasurer  
**Original effective date:** February 11, 2015

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>New policy proposal</td>
</tr>
<tr>
<td>□</td>
<td>Minor/technical revision of existing policy</td>
</tr>
<tr>
<td>□</td>
<td>Major revision of existing policy</td>
</tr>
<tr>
<td>□</td>
<td>Reaffirmation of existing policy</td>
</tr>
</tbody>
</table>

(A) **Policy statement**

To define the policy and procedures for the acceptance of credit cards by Merchants affiliated with The University. 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 SAQ A), “standalone and dial-out terminals – no electronic cardholder data storage” (aka SAQ B), and “hardware payment terminals in a validated Point-To-Point Encryption” (aka SAQ P2PE-HW).

Note: **SAQ -- Self-Assessment Questionnaire**

(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 are not permitted to transmit, process, or store credit card information on University computer systems or the Internet unless specifically approved. Storage of credit card information on University computer systems is prohibited.

(c) When cardholders visit University online sites they must be redirected 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) Periodic reviews of Merchants will be coordinated by the Office of the Treasurer and the Office of the Chief Information Officer (Information Security). 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

As stated previously, 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. Each department that processes credit card transactions (under the oversight of the Business Manager) is charged with supporting 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/NS/Security/index.html)

(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) Procedure

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. It is recommended that both documents be reviewed in conjunction with each other. 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. Any transactions that are not reconciled via the First Data report are recorded in miscellaneous revenue and cash by Treasury (monthly). The department’s appropriate GL accounts will be recorded and miscellaneous revenue relieved once Treasury receives a reconciled FD report 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, departments will be notified via email regarding any disputed charge card sale. It is a department's responsibility to research and respond within the designated time period, 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, which is discussed in 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 cards shall be accepted 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.

(ii.) The expiration date on the credit card must be verified.

(iv) In the case of face-to-face credit card transactions, the customer receives the copy of the sales draft that has only four (4) 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 16-digit credit card number printed on it. Drafts should be safeguarded in an appropriate locking file cabinet or safe.
(v.) Full credit card numbers are not to be sent via e-mail or fax. Partial credit card numbers may be sent via email or fax (first four digits and last four digits).

(f) Access to physical or electronic cardholder data must be restricted to individuals whose job requires access. (Reference: 3364-65-02 Access control policy (http://www.utoledo.edu/policies/administration/info_tech/pdfs/3364-65-02_Access_control_policy.pdf)).

(g) A unique ID must be assigned to each person with computer access to credit card information. User names and passwords may not be shared. (Reference: 3364-65-02 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 can be found on the front of the card.

(i) Full or partial credit card numbers in combination with the three or four digit validation codes (usually on the back of credit cards) may not be faxed e-mailed, or stored. Departments will reconcile their weekly credit card transactions against reports run by Treasury that are emailed to each department representative. Only partial credit card numbers will be provided (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 12 of the 16 digits of the credit card number, usually the first 6 digits and the last 4 digits of the credit card number.
(m) Imprint machines are not permitted to process credit card payments as they display the full 16-digit credit card number on the customer copy.

(n) If an employee suspects that credit card information has been exposed, stolen, or misused this incident must be reported 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 fees charged by the credit card companies are 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) Please contact Treasury for current fees to process credit card transactions.

(5) Rocket Cards (IDs)

(a) Rocket Cards should be considered separate from credit cards since they do not currently fall under PCI requirements. Rocket Cards may not be processed on the same equipment as credit cards.