Credit Card Acceptance and Security Policy

All University personnel accepting credit cards for payment of services or goods must protect and secure all credit card data collected, regardless of how it is stored (physically or electronically, including but not limited to account information, card imprints, correspondence and Terminal Identification Numbers).

All department heads and personnel should strictly observe and enforce this policy to ensure that TWU customer information and privacy is protected and to assure compliance with the Payment Card Industry Data Security Standard (PCI DSS).

The compromise of any cardholder information should be reported immediately by submitting an email containing a complete overview of the incident to payments@twu.edu. TWU's Controller and Information Security Office will be advised as deemed appropriate.

Data is considered to be secured only if the following criteria are met:

- Only approved processing software programs and hardware with secure communication protocols and/or encrypted connections are used for the processing of electronic transactions. .
    - Departments requesting merchant capabilities are required to complete and submit an application to the Bursar.
- Access for credit card and/or electronic payment data and processing should be limited to essential personnel who have completed cash handling training or are authorized on a 'need to know' basis.
- Email is **not used** to transmit credit card payment information.
    - If the use of email is necessary, only the last four digits of the credit card number are displayed.
- Fax transmissions, (both sending and receiving) of credit card and electronic payment information is strongly discouraged. If necessary, transmissions are strictly limited to those fax machines whose access is secured and restricted to authorized individuals only.
- **All transactions must be processed immediately and documents containing cardholder and card information must be shredded.**
    - **The card-validation code of a credit card is never stored in any form.**
    - **No more than six digits of any credit card account number can be stored.**
    - **All credit card and electronic payment data that is no longer deemed necessary or appropriate to store is destroyed or rendered unreadable.**
    - **The processing and storage of personally identifiable credit card or electronic payment information on University computers and servers is prohibited.**
    - **Credit card or electronic payment information is never downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants.**
- No credit card receipt, document, or correspondence of any kind, referencing the transaction shall include more than the last four digits of the account number or the month and year of the expiration date.
- No University employee, contractor or agent who obtains access to credit card or other personal payment information may sell, purchase, provide, or exchange said information in any form to any third party other than to the University's acquiring bank, depository bank, Visa, MasterCard or other credit card company, or pursuant to a government request.
- All requests to provide information to any outside party must be reviewed and approved in advance by the Bursar, Controller or their designee.