Revised 4/17/2012

BAYLOR UNIVERSITY
Payment Card Procedural Requirements: General

1. All payment card processing is subject to review by the Payment Card Oversight (PCO) Committee to help ensure Baylor University's compliance with Payment Card Industry (PCI) standards.
2. No cardholder information is to be stored electronically on any device. Delete any pre-existing cardholder information from electronic databases, including computer hard drives, CDs, disks, and other external storage media, using PGP shredder or other mechanism approved by Baylor Information Technology Services (ITS).
3. For any cardholder information to be stored, it must be documented by the department and approved by a designee of the PCO Committee.
4. Sensitive authentication data (e.g., CVC2, CVV2, CID, PIN) must not be stored.
5. Paper documents containing cardholder information must be treated as confidential and secured properly at all times. When not in use, documents containing cardholder information must be stored in a locked location. Documents containing cardholder information must be destroyed using a cross-cut shredder after transaction authorization has been received and the cardholder information is no longer needed.
6. Inventories of paper documents containing cardholder information must be conducted on at least a quarterly basis to ensure secure destruction of stored data that exceeds defined retention requirements.
7. Access to cardholder information must be limited to those individuals whose job requires access.
8. At least annually, employees handling cardholder information must receive training and acknowledge their understanding of their responsibility for compliance with University policies and procedures.
9. Background checks must be performed on employees who will be handling cardholder information.
10. Suspected security incidents must be reported immediately.
11. Payment card transactions must represent bona fide purchases of goods or services (or, if applicable, bona fide charitable contributions) between Baylor and the cardholder.
12. Cardholder information may not be sent or accepted via unencrypted electronic communication (e.g., email, instant messaging, chat, text messaging).
13. An authorization approval code, a 6-digit code that shows the transaction was approved, must be obtained for all transactions processed.
14. A single purchase may not be divided into more than one transaction to the same card.
15. Refunds of credit card payments should not be given in the form of cash, check, or in-store credit. Refunds should be processed to the card used in the original transaction.
16. Refunds may not be issued for more than the amount of the original payment card transaction.