

Credit Card Policies and Procedures

- 1) Secure all confidential cardholder numbers and information. Credit card receipts should typically be treated the same as you would treat cash. Departments will be responsible for any losses due to poor internal and inadequate controls.
 - Credit card numbers must never be transmitted by e-mail, unsecured fax, or through campus mail (sealed envelopes may be used).
 - All documentation containing credit card account numbers must be maintained in a “secure” location that is accessible to only accountable staff members. Secure locations include locked drawers and safes.
 - All documentation containing card account numbers must be destroyed in such a way that they will be deemed unreadable.
- 2) Restrict access to credit data and processing to appropriate and authorized personnel.
- 3) Establish segregation of duties between the credit card processing and reconciliation.
- 4) Perform an annual self-assessment to ensure compliance with this policy and associated procedures, and report the results of this assessment to Business Operations.
- 5) Credit card authorizations must be kept for 18 months for response to charge-backs and other disputes.
- 6) Business Operations will conduct periodic reviews of existing credit card accounts regarding safeguarding and storage of cardholder information as well as provide periodic training on credit card policies in conjunction with cash handling training.

1/15/09