MSU Credit Card Processing

Purpose
The purpose of this policy is to define the guidelines for accepting and processing credit cards

Policy
All credit card transactions processed by MSU employees must meet the standards outlined in the policy:

a. Credit card information should be accepted online, by telephone, mail, or in person. This information should not be accepted via e-mail and departments should not e-mail credit card information.
b. Cardholder data must be locked in a secure area. Access should be limited to individuals that require the use of the data. Access should also be restricted on a 'need to know' basis.
c. Only essential information should be stored. Do not store the Card Validation Code (also known as the Security Digits, V Code, or CID). Do not store users PIN's or the full data from a cards magnetic stripe.
d. Credit card information should only be retained for the time needed to process, or if retained for reconciliation, for as long as one-year maximum.
e. Credit card information, if it does not need to be retained, should be destroyed. Information should be destroyed by shredding (cross-cut) immediately after processing, or immediately after they no longer need to be retained.
f. Credit card receipts may only show no more than the last four digits of the credit card number. If receipts show more than the last four digits, the receipts must be shredded or retained in a secure area.

Exceptions to the policy may be granted by the Vice President for Business Affairs

Adopted: May 4, 2009

Sponsor: Vice President for Business Affairs