Section 06.05.05.01
CREDIT CARD GUIDELINES FOR INTERNET E-COMMERCE

Guidelines/Best Practices for E-Commerce/Internet Interfacing with TouchNet

- Install and maintain a working network firewall
- Keep security patches current
- Do not store sensitive cardholder data
- Encrypt data sent via open networks
- Always use updated anti-virus software
- Restrict access to data to a 'need to know" basis
- Assign a unique ID to each user
- Track access to the data by that unique ID
- Never use vendor-supplied defaults as passwords or other security features
- Test the security system and processes regularly
- Require employees that have access to TouchNet to complete HR Connect's Payment Card Industry Data Security Standard Training
- Your website must contain, in a clear manner, departmental contact information, including e-mail address and phone number, refund/return policy and privacy policy
- Transaction Receipt
    - University name and department name and address
    - Description of merchandise/services
    - Transaction amount
    - Transaction Date
    - Transaction Type
    - Purchases Name
    - Authorization code (provide by TouchNet)
    - Unique transaction identification number (provided by TouchNet)