Policy Number: 246.0
Policy: Safeguarding Customer Information
Effective Date: 3/2013
Revision Date: 3/2013
Approved by: Business Services Director

PROCEDURE:

I. **Safeguarding Customer Information Procedures:**

A. Approvals

1. Obtain approvals from Information Technology, Internal Audit, and/or Business Service's Office by completing the required forms.

B. Program Requirements

1. Information Technology is responsible for these procedures to establish a secure computing environment.

a. Install and maintain an effective network firewall to protect data accessible via the Internet.
b. Keep operating system and application software security patches up-to-date.
c. Encrypt stored data.
d. Encrypt data sent across open networks.
e. Use and regularly update anti-virus software

C. Development

1. Develop adequate office procedures for staff or contract service providers to maintain secure information.

a. Restrict access to data by business "need-to-know".
b. Assign a unique ID to each person with computer access to data.
c. Do not use vendor-supplied defaults for system passwords and others security parameters.
d. Track access to data by unique ID.
e. Regularly test security systems and processes.
f. Maintain a policy that addresses information security for employees and contractors.
g. Restrict physical access to cardholder information. Records need to be in locked file cabinets at all times. Rooms need to be locked when not occupied.

II. **Internal Controls**

A. Segregation of duties is important to protect against fraud and maintain confidentiality.

1. Individuals who collect monies and/or write receipts may not be the same individuals who account for deposits.

2. Different Individuals are to perform the following functions:
a. Collecting monies and preparing receipts
b. Depositing receipts

c. Accounting for receipts

3. Limit access to information such as ID and credit card numbers only to those individuals who need to know.

4. All documents kept in the campus departments must mask the credit card information.

5. Protect and shred confidential information.

6. Small departments that do not have sufficient staff to meet ideal segregation of duties requirements must ensure that detailed supervisory review compensates for this weakness