Payment Card Processing Procedures

The main contact and employees that will have access to sensitive payment card information are responsible for completing the following applicable forms in order to establish a merchant account and meet Payment Card Industry Data Security Standards (PCI DSS) requirements:

I. Merchant Application
II. Background Check Request
III. Employee Statement of Understanding

Departments are responsible for ensuring that employees who will be involved in payment card processing or have access to such sensitive data have completed the following:

- Reviewed the University's Payment Card Processing Policy and become familiar with the Payment Card Industry Data Security Standards (PCI DSS)
- Department supervisor should complete the “Background Check Request Form” for each designated employee handling payment cards and submit the completed form(s) to Human Resources- PC 234. An e-mail notification by Human Resources indicating clearance of their background check and fingerprinting should be confirmed before access to cardholder information is granted.
- Attend "Red Flags Training" and retain certificate for your records.
- Obtain journal access and receive training on credit card journal entries by requesting such via e-mail at merchant@fiu.edu.
- Completed payment card processing training according to the selected approved method below.

The approved methods are as follows:

1. Point of Sale Terminal: Once the equipment is received, the training will be conducted over the phone. Contact 1-800-430-7161 option 4 for further instructions.
2. Mobile Readers: Once the equipment is received, contact Apriva customer support at 1-866-277-4820 for guidance on programming the device.
3. Internet (Online) Application- Cybersource Business Edition: Online training is available via tutorials, setting-up a test account, and access to supporting documentation. Existing merchants may contact CyberSource customer support at 1-866-501-7958.
4. Third-party vendor: Merchant will also be responsible for coordinating training with the third party vendor.

Additional requirements for departments to follow include:

- Constantly maintain your operation compliant with Payment Card Industry Data Security Standards.
- Mask the primary account number (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed).
- Never store the 3 digit authorization code (primarily found on the back of the card).
- Do not share payment card information via e-mail, voice message, or instant message. If information is received by fax, the transaction must be processed and the cardholder's sensitive information must be shredded immediately.
- If requesting an online merchant location, an approved privacy and refund policy must be approved by the Office of Integrity and Compliance (e-mail hyperlink) and listed on you FIU webpage.
- Complete and submit the Change of Merchant Employee form if an employee’s duties change or is no longer working for the department.
- Complete and submit the Cancellation of Merchant Services form in the event that your department will no longer process payment card transactions.

CONTACTS:

INITIAL SET-UP, FORMS AND GENERAL INFORMATION

Merchant Services
Office of the Controller, CSC 325
(305) 348-3888
(305) 348-1909 (fax)

JOURNAL TRAINING

Merchant Services
Office of the Controller, CSC 325
(305) 348-3888
(305) 348-1909 (fax)

OTHER PERTINENT CONTACTS

- AMEX Customer Support: 1-866-220-4272
- Bank of America Merchant Services (BAMS) Support: 1-800-430-7161
- Clientline Customer Support: 1-800-285-3978 and Reporting tool demo