E071 CREDIT CARD PROCESSING & SECURITY POLICY

PURPOSE
The purpose of this policy is to establish guidelines for processing charges/credits on Credit Cards to protect against exposure and possible theft of account and personal cardholder information that has been provided to the University of Miami; and to comply with the Payment Card Industry's Data Security Standards (PCI) requirements for transferring, handling and storage of credit card information.

DEFINITIONS
Cardholder Information Security Program (CISP): Visa's Cardholder Information Security Program (CISP) is designed to ensure that all merchants that store, process, or transmit Visa cardholder data, protect it properly. To achieve CISP compliance, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard.

PCI: The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

Cardholder Data: Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, Card Validation Code CVC 2 (MasterCard), Card Verification Value CVV2 (VISA), Cardmember ID (Discover) or CID - Card Identification Number (American Express) (e.g., three- or four-digit value printed on the front or back of a payment card.

System Administrator / Data Custodian: An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and permanent part-time employees of the University and/or third party vendors approved by IT and/or Treasury Operations may function as system/network administrators and/or data custodians.

SCOPE
This policy applies to all University of Miami employees, contractors, consultants, temporaries, and other workers. This policy is applicable to any unit that processes, transmits, or handles cardholder information in a physical or electronic format. Affiliated corporations are encouraged to comply.
POLICY
All transactions (including electronic based) that involve the transfer of credit card information must be performed on systems approved by the University's Office of the Treasurer, after a prior compliance and security review from Information Technology. All specialized servers approved for this activity must be housed within the Department of Information Technology and administered in accordance with the requirements of all University of Miami policies and the Cardholder Information Security Program (CISP). University of Miami is involved in PCI DSS compliance and is subject to examination of system security and configuration to ensure cardholder information is securely maintained. The Treasury Operations Office will be responsible for verifying compliance with industry best practices for conducting electronic payment transactions through Data Capture / Point of Sale machines (Credit Card Terminals), while Web Based procurement of credit cards will be monitored by the Business analyst of Information Technology. In addition:

A. No electronic credit card numbers should be transmitted or stored in any other system, personal computer, or e-mail account.
B. Physical cardholder data must be locked in a secure area, and limited to only those individuals that require access to that data. In addition, restrict access to data on a "need to know" basis.
C. Store only essential information. Do not store the Card Validation Code, or the PIN Number. Do not store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.)
D. Stored credit card information will be retained for a maximum of 60 days. All media used for credit cards must be destroyed when retired from use. All hardcopy must be shredded prior to disposal.
E. Departments must comply with the PCI Data Security Standard Payment Card Industry Data Security Standard
F. Exceptions to this policy may be granted only after a written request from the unit has been reviewed and approved by the University Office of the Treasurer.

PROCEDURE
Confidentiality and Security of Account Information

University of Miami employees are governed by various policies that include the Code of Conduct, Acceptable Use, Information Security policies, the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach Bliley Act (GLBA), and the Red Flag Policy. These policies include the responsibility to protect the confidentiality of individual's personal information.

All credit card & debit card transactions, including web based procurement of the same, must be initiated and controlled through the Office of the Treasurer. Because the sale of goods and services to entities outside the university community may raise special considerations (e.g. unrelated business tax,
accounting, legal, etc) questionable sales should be reviewed by the Controller's Office, and or General Counsel.

Departments, who need to accept credit/debit cards and obtain a physical terminal to either swipe or key transactions through that Data Capture machine, need to contact the Executive Director of Treasury Operations to execute the required paperwork, obtain a Merchant Number, receive training, and be given direction as how to journalize those transactions on the books of the University.

Departments wishing to engage in electronic commerce are required to use University of Miami's E-Pay, a web based solution through NelNet. After contacting the Executive Director of Treasury Operations, a specialized Merchant Number will be established, and the department will be directed to the Business Analyst of Information Technology who will provide technical instructions and documentation. Requesting departments must also inform Financial Reporting's Senior Bookkeeper in the Controllers Department of newly requested and processed accounts for credit card devices. Departments will be responsible for creating their own web site "storefront" with assistance from Information Technology's Business Analyst for integration with NelNet. Once the storefront program passes required payment parameters to U.M., secure payment, E-Pay, will be executed. Approval codes and other related elements will be returned to the originating web site. In addition, the accounting of journal entries will be automatically processed.

The practice of least privilege will be utilized to restrict access to sensitive data. This practice involves assigning individual access on a "need-to-know" basis. Positions requiring specific levels of data access will be provided with approval by the department head and IT. For employees without a "need to know", credit card account numbers will be masked to protect account information. The first six and last four digits are the maximum number of digits to be displayed.

Under no circumstances will it be permissible to obtain credit card information or transmit credit card information by e-mail.

Under no circumstances will any other payment mechanism other than NelNet be permissible for electronic commerce on the web. Exceptions to this procedure must be submitted in writing to the University's Office of the Treasurer.

Any changes to systems housing account information must only be performed when:

- Thorough testing has taken place to ensure adequacies of controls;
- Functionality testing with clients has taken place;
- Required client training is completed;
- Change control processes have been followed.

Enforcement by Information Technology

Chief Security Office (CSO):
• Responsible for approving installation, modifications, and removal of all network hardware devices throughout the University of Miami
• Responsible for monitoring the enforcement of this policy

System Administrators:

• Responsible for granting permission to sensitive areas based on the principle of least privilege.
• Responsible for configuring the masking of account numbers based on a user's access.

Data Storage and Destruction

The following processes must be followed for all data storage and destruction:

• Hardcopy containing cardholder data will be destroyed immediately after processing.
• All electronic media containing cardholder information should be labeled and identified as confidential.
• An inventory of media containing cardholder information should be performed monthly.
• Audit logs for system housing cardholder data will be available for a period of four (4) years.
• Electronic backup media containing cardholder data will be available for a period of four (4) years and then properly erased or decommissioned and destroyed on a monthly basis.

SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of physical and or electronic payment capability for affected units. Additionally, fines may be imposed by the affected credit card company, beginning at $50,000 for the first violation.

Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, suspension, termination of employment and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

Violations of the policy will be addressed by the individual's respective disciplinary policies and procedures. All known and/or suspected violations must be reported to the applicable Network/System Administrator who will report, as appropriate, to the Information Technology Security Department (security@miami.edu).
The appropriate University administrative office will investigate all such allegations of misuse with the assistance of the Department of Information Technology, Treasury Operations, General Counsel, and the Department of Human Resources.

Updated 02/2010
Reviewed 12/2011