Cardholder Information Security Policy

**PURPOSE:**

The University is required to conform to standards set forth by the Payment Card Industry Data Security Standard. Failure to comply with this standard may jeopardize the University's ability to accept credit cards for payment.

The cardholder information security policy establishes responsibility and authority for securing credit card account information at the University of Miami. The policy requires internal controls, testing, and training for compliance.

**SCOPE:**

This policy applies to all University employees, faculty, students, contractors, guests, consultants, temporary employees, and any other users, including all personnel affiliated with third parties who engage in the processing, transmission and storing of credit card information.

**DEFINITIONS:**

**Payment Card Industry Data Security Standard (PCI DSS):** Guidance developed by the major credit card companies to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing card payments must be PCI compliant or risk losing the ability to process credit card payments.

**Cardholder Information:** Cardholder information as defined by PCI DSS includes Personal Account Number (or credit card number), name on the card, expiration date, and security code.

**System Administrator:** 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 may function as system administrators.

**Data Custodian:** The person responsible for, or the person with administrative control over, granting access to an organization's documents or electronic files while protecting the data as defined by the organization's security policy or its standard IT practices.

**University:** “University” refers to the University of Miami as a whole and includes all units.
**Personally Identifiable Information (PII):** Any piece of information which must be maintained in confidence by law or which the affected individual has information the university must be maintained as confidential. Examples of PII include Protected Health Information, Credit Card Numbers, and Social Security Numbers.

**POLICY:**

**Confidentiality and security of account information:**
- University of Miami employees are governed by various policies that include the Code of Conduct, Acceptable Use, and Information Security policies. These policies include the responsibility to protect the confidentiality of personally identifiable information (PII) and other information that should not be publically disclosed.
- The University of Miami will comply with PCI DSS requirements and is subject to examination of system security and configuration to ensure cardholder information is maintained in a secure manner.

**Data access and Configuration:**
- Encryption must be used at all times whenever credit card account numbers are transmitted electronically (e.g. email).
- The practice of “least privilege” will be utilized to restrict access to sensitive data.
- Credit card account numbers shall be masked to protect account information for all users except those who have a legitimate business/academic need. The first six or last four digits are the maximum number of digits that may be displayed. Any changes to systems housing account information must be performed only when:
  - Thorough testing has taken place to ensure adequacies of controls;
  - Code reviews have taken place;
  - Functionality testing with clients has taken place;
  - Any needed training for clients has taken place;
  - The change control process has been followed as defined by the change and incident management policy.
- Access to the cardholder database will require the use of multi-factor authentication.
- Automatic disconnect of idle sessions for remote access is required.

**Data storage and destruction:**
- Hardcopy containing cardholder data will be destroyed immediately after processing when possible. Any hardcopy data must be stored in a secured area with limited access. Access to such areas shall be provided to those who have a legitimate business/academic need and should be documented via a hardcopy access log. Logs should be maintained for a period of 1 year.
- All electronic media containing cardholder information must be encrypted, labeled and/or documented and identified as confidential by the system administrator and/or data custodian.
- An inventory of media containing cardholder information must be performed regularly.
- Audit logs for systems housing cardholder data will be available for a period of 1 year and will be reviewed daily.
- Electronic backup media containing cardholder data will be available for a period of 1 year and then properly erased or decommissioned and destroyed.
- All new critical security patches must be installed within one month of publication.

**Additional Requirements:**
- On a yearly basis, quarterly external penetration scans must be completed by an approved scanning vendor (ASV).
• Internal penetration testing must be completed at least quarterly or when major changes occur.
• A list of all PCI related devices and personnel with access must be created.
• All PCI related devices must be labeled as follows:
  o Device owner,
  o Contact information; and
  o Purpose.
• Training requirements:
  o The security awareness program requires employees subject to the scope of this policy to acknowledge the University's information security policies at least annually and provide multiple methods of communicating awareness and educating employees (i.e., posters, letters, memos, web based training, meetings, and promotions).
  o Such employees must participate in awareness training upon hire and at least annually.
  o Staff with security breach responsibilities must be trained in this area at least annually.

Release of Information:
It is the policy of the University to protect personal cardholder information to the maximum extent possible. Court orders, subpoenas, or governmental requests seeking cardholder information must be referred to the Office of the General Counsel. Information essential to the processing of card transactions may be provided through normal credit processing channels to the issuing institution. The provision of cardholder information for any other purpose (e.g. to student loan service providers) is permitted under this policy only if:

• expressly authorized by the cardholder, or
• allowed under a separate university policy which, consistent with federal and state law, authorizes the disclosure.

Any other requests for release of credit card information must be submitted to Treasury Operations for approval.

Third Parties:

All third parties storing, transmitting, and/or processing credit card information are required to hold a valid PCI certificate throughout any partnership/collaboration with the University of Miami.

Compensating Controls:

For any system or application unable to meet the requirements of this policy and which facilitates a critical business/academic process, appropriate compensating controls must be implemented. Any instance of non-compliance will be evaluated on a case by case basis to ensure appropriate controls are in place to mitigate risk. Ultimate approval will be made by the University office of the CSO responsible for PCI compliance.

EXCEPTIONS:
Any requests for exceptions to this policy must be submitted in writing and will be reviewed on a case by case basis. Exceptions shall be permitted only after written approval from Treasury Operations. The list of exceptions shall be reviewed annually and cancelled as required.
IMPLEMENTATION:

System Administrators:
- Responsible for granting permissions to sensitive areas based on the principle of “least privilege.”
- Responsible for configuring masking of account numbers based on a user’s access.

Chief Information Security Office:
- Responsible for regular review of this Policy. The review will occur annually or when significant changes occur.

Network Officer:
- Responsible for approving installation, modifications, and removal of all network hardware devices throughout the University of Miami.

Responsible Vice President or CIO:
- Responsible for reviewing and approving or denying exception requests.
- Responsible for reviewing exceptions yearly.
- Responsible for monitoring the enforcement of the policy.

SANCTIONS:

Accounts and network access may be administratively suspended with or without notice by the University when, in the University's judgment, continued use of the University's resources may interfere with the work of others, places the University or others at risk, or violates University policy.

Violations of the policy will be addressed by disciplinary policies and procedures applicable to the individual.

All known and/or suspected violations must be reported to the applicable Systems Administrator, who will report, as appropriate, to Information Technology's Security and Control Department. All such allegations of misuse will be investigated by the appropriate University administrative office with the assistance of the Department of Information Technology and the Department of Human Resources.

Penalties may include:
- Suspension or termination of access to computer and/or network resources;
- Suspension or termination of employment, to the extent authorized by other university published policies and procedures;
- Suspension or termination of contract computer and/or network services; or
- Criminal and/or civil prosecution.

OTHER APPLICABLE POLICIES:
- E071: Credit Card Processing & Security Policy
- BSJ-028: Contracting Requirements
- A050: System Administrator Policy
- Change and Incident Management Policy