REVISION HISTORY

Revision No.	Revision Date	Author	Description of Changes
2.0	09 February 2016	Krista Theodore	Update to Reflect Changes in the PCI DSS

APPROVED BY

This Policy is established for Policies pertaining to the University by the approval signatures below.

Name	Title	Signature	Date
Hiram Sem	Executive Director, Treasury Operations	*Signature on File*	09 May 2016
Charmel Maynard	Assistant Vice President & Assistant Treasurer	*Signature on File*	09 May 2016
Tim Ramsay	Associate Vice President, Chief Information Security Officer	*Signature on File*	09 May 2016
Geoffrey Kirles	Vice President, Finance & Treasurer	*Signature on File*	09 May 2016
Steve Cawley	Vice President, Information Technology and CIO	*Signature on File*	09 May 2016

Information Security exists to further the mission of the University. The University is comprised of large and diverse populations with evolving needs related to information technology resources and data. University management is committed to safeguarding those resources while protecting and promoting academic freedom. The requirements that follow have been identified to promote the best balance possible between information security and academic freedom.

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 payment cards.

The payment card processing and security policy establishes responsibility and authority for securing payment 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 payment card information. Any individual involved in payment card processing at or on behalf of the University of Miami must screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)

DEFINITIONS:

- **Payment Card Industry Data Security Standard (PCI DSS):** Guidance developed by the major payment card companies to help organizations that process card payments, prevent payment card fraud, hacking and various other security issues. A company processing card payments must be PCI compliant or risk losing the ability to process payment cards.
- **Cardholder Information:** Cardholder information as defined by PCI DSS includes Personal Account Number (or payment 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.
- **University:** "University" refers to the University of Miami as a whole and includes all units.

POLICY:

All transactions (including electronic based) that involve the transfer of payment 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 Office will be responsible for verifying compliance with industry best practices for conducting transactions.

All payment card transactions 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. Under no circumstances will any other payment mechanisms, other than those approved by Treasury and Information Security Office, be implemented, configured, or established without written approval.

Requirement 1: Build and Maintain a Secure Network

Firewall Configuration
Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. Access to the internet must be through a firewall, as must any direct connection to a vendor, processor, or service provider.(PCI Requirement 1.2)
Inbound and outbound traffic must be restricted by the firewalls to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied. (PCI Requirement 1.2.1)
Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)
Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment. (PCI Requirement 1.3.3)

- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized by management and controlled by the firewall. (PCI Requirement 1.3.5)
- Firewalls used to protect the cardholder data environment must implement stateful inspection, also known as dynamic packet filtering. (PCI Requirement 1.3.6)

Any mobile and/or employee-owned computers with direct connectivity the Internet (for example, laptops used by employees), which also have the ability to access the organization's cardholder data environment must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or employee-owned computer users. (PCI Requirement 1.4)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Vendor Defaults
Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)
Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to: (PCI Requirement 2.1.1)

- Default encryption keys
- Passwords
- SNMP community strings
- Default passwords/passphrases on access points
- Other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption (such as WPA or WPA2) for authentication and transmission of data over wireless networks.

Configuration Standards for Systems
Configuration standards for all system components must be developed and enforced. University of Miami must insure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. (PCI Requirement 2.2)
Configuration standards must be updated as new vulnerability issues are identified, and they must be enforced on any new systems before they are added to the cardholder data environment. The standards must cover the following:

- Changing of all vendor-supplied defaults and elimination of unnecessary default accounts.
- Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (PCI Requirement 2.2.1)
- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system. (PCI Requirement 2.2.2)

- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure. (PCI Requirement 2.2.3)
- Configuring system security parameters to prevent misuse
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (PCI Requirement 2.2.5)

System administrators and any other personnel that configure system components must be knowledgeable about common security parameter settings for those system components. They must also be responsible to insure that security parameter settings set appropriately on all system components before they enter production. (PCI Requirement 2.2.4)

System administrators are responsible to insure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (PCI Requirement 2.5)

Non-Console Administrative Access
Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. Encryption technologies must include the following: (PCI Requirement 2.3)

- Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested.
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.
- Must include administrator access to web-based management interfaces.
- Use vendor documentation and knowledge of personnel to verify that strong cryptography is in use for all non-console access and that for the technology in use it is implemented according to industry best practices and vendor recommendations.

Requirement 3: Protect Stored Cardholder Data
Prohibited Data
Processes must be in place to securely delete sensitive authentication data (defined below) post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)
Payment systems must not store of sensitive authentication data in any form after authorization (even if encrypted). Sensitive authentication data is defined as the following:

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block is not stored under any circumstance. (PCI Requirement 3.2.3)

Displaying PAN

University of Miami will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show at most only the first six and the last four digits of the PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data for example, legal or payment card brand requirements for point-of-sale (POS) receipts. Policies and procedures for masking the display of PANs must mandate the following: (PCI requirement 3.3)

- A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access.
- PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN.
- All other roles not specifically authorized to see the full PAN must only see masked PANs.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

In order to safeguard sensitive cardholder data during transmission over open, public networks, University of Miami will use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.). These controls will be implemented as follows: (PCI Requirement 4.1)

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use.

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. Weak encryption (for example, WEP, SSL version 2.0 or older) is not to be used as a security control for authentication or transmission. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Requirement 5: Use and Regularly Update Anti-Virus Software or Programs

Anti-Virus Protection

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software. (PCI Requirement 5.1, 5.1.1)

For systems considered to be not commonly affected by malicious software, University of Miami will perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. (PCI Requirement 5.1.2)

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and be capable of as well as configured to generate audit logs. Anti-virus logs must also be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2)

Steps must be taken to insure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. (PCI Requirement 5.3)

Requirement 6: Develop and Maintain Secure Systems and Applications

Risk and Vulnerability
University of Miami will establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.

Risk rankings are to be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. (PCI Requirement 6.1)

All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. All applicable non-critical vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). (PCI Requirement 6.2)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data
Access to University of Miami's cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

- Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.2)
- Privileges must be assigned to individuals based on job classification and function (also called "role-based access control). (PCI Requirement 7.1.3)

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Remote Access
Two-factor authentication must be incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (PCI Requirement 8.3)

Vendor Accounts
All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. (PCI Requirement 8.1.5)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically Secure All Areas and Media Containing Cardholder Data

All publicly accessible network jacks must have physical and/or logical controls to restrict access to the secure network by unauthorized personnel. (PCI requirement 9.1.2)
Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:
All media must be physically secured. (PCI requirement 9.5)
Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include: (PCI Requirement 9.6)

- Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.6.1)
- Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.6.2)
- Management approval must be obtained prior to moving the media from the secured area. (PCI Requirement 9.6.3)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.7)

Destruction of Data
All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.8)
Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI requirement 9.8.1.a)
Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. (PCI requirement 9.8.1.b)

Protection of Payment Devices

Devices that capture payment card data via direct physical interaction with the card (such as swipe readers and any other payment terminals) must be protected. This protection must include preventing the devices from being tampered with or substituted. (PCI requirement 9.9)

University of Miami must maintain an up-to-date list of devices and personnel with access to cardholder data. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following: (PCI requirement 9.9.1)

- Merchant ID associated with the device
- List of employees with access to each device with contact information (C#, Employee ID, Department, Email, Phone, Address
- Make and model of all devices.
- Location of each device (for example, the address of the site or facility where the device is located and where in the area it is located, such as front desk).
- Serial Number
- IP Address, if applicable
- MAC Address, if applicable
- Firmware, if applicable
- Payment Applications, if applicable
- All other connected systems and devices

The payment devices must be periodically inspected. Check surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). (PCI requirement 9.9.2)

Employees and contractors who interact with the payment devices must be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI requirement 9.9.3)

- Employees must verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices.
- Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added.
- Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).

Requirement 10: Regularly Monitor and Test Networks

Audit Log Collection

University of Miami will implement technical controls that create audit trails in order to link all access to system components to an individual user. The automated audit trails created will capture sufficient detail to reconstruct the following events:

- All actions taken by any individual with root or administrative privileges. (PCI Requirement 10.2.2)
- All invalid logical access attempts (failed logins). (PCI Requirement 10.2.4)
- Any use of and changes to identification and authentication mechanisms including but not limited to creation of new accounts and elevation of privileges and all changes, additions, or deletions to accounts with root or administrative privileges. (PCI Requirement 10.2.5)

University of Miami's log generating and collecting solution will capture the following data elements for the above events:

- User identification. (PCI Requirement 10.3.1)
- Type of event. (PCI Requirement 10.3.2)
- Date and time. (PCI Requirement 10.3.3)
- Success or failure indication. (PCI Requirement 10.3.4)
- Origination of event. (PCI Requirement 10.3.5)
- Identity or name of affected data, system component, or resource. (PCI Requirement 10.3.6)

Audit Log Review

University of Miami's systems administrators will perform daily review of the audit logs. This review may be manual or automated but must monitor for and evaluate: (PCI Requirement 10.6.1)

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

The audit review must also check the logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. (PCI Requirement 10.6.2)

Subsequent to log review, systems administrators or other responsible personnel will follow up exceptions and anomalies identified during the review process. (PCI Requirement 10.6.3)

University of Miami must retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). (PCI Requirement 10.7)

Requirement 11: Regularly Test Security Systems and Processes

Testing for Unauthorized Wireless Access Points
At least quarterly, University of Miami will perform testing to ensure there are no unauthorized wireless access points (802.11) present in the cardholder environment. (PCI Requirement 11.1)

The methodology must be adequate to detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components.
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.).
- Wireless devices attached to a network port or network device.

To facilitate the detection process, University of Miami will maintain an inventory of authorized wireless access points including a documented business justification. (PCI Requirement 11.1.1)

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), the configuration must be capable of generating alerts to notify personnel. Detection of unauthorized wireless devices must be included in the Incident Response Plan (see PCI Requirement 12.10). (PCI Requirement 11.1.2)

Vulnerability Scanning
At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), University of Miami will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Internal vulnerability scans must be performed at a minimum quarterly and repeated until passing results are obtained, or until all "high" vulnerabilities as defined in PCI Requirement 6.1 are resolved. Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.1)
Quarterly external vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures). External vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.2)

For both internal and external vulnerability scans, University of Miami shall perform rescans as needed to validate remediation of failures detected during previous scans, as well as after any significant change to the network. Scans must be performed and reviewed by qualified personnel. (PCI Requirement 11.2.3)

If segmentation is used to isolate the CDE from other networks, perform tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. These tests need to be done from multiple locations on the internal network, checking both for improper accessibility from the out-of-scope zones to the in-scope zone as well as the reverse. (PCI Requirement 11.3.4)

For all in-scope systems for which it is technically possible, University of Miami must deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. The change detection software must be integrated with the logging solution described above, and it must be capable of raising alerts to responsible personnel. (PCI Requirement 11.5.1)

For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider). (PCI Requirement 11.5)

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

Security Policy
University of Miami shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data. (PCI Requirement 12.1)
This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.1)

Critical Technologies
University of Miami shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)
These policies must include the following:

- Explicit approval by authorized parties to use the technologies. (PCI Requirement 12.3.1)
- Authentication for use of the technology. (PCI Requirement 12.3.2)
- A list of all such devices and personnel with access. (PCI Requirement 12.3.3)
- Acceptable uses of the technologies. (PCI Requirement 12.3.5)
- Acceptable network locations for the technologies. (PCI Requirement 12.3.6)
- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. (PCI Requirement 12.3.8)
- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. (PCI Requirement 12.3.9)

Security Responsibilities
University of Miami's policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

Incident Response Policy
University of Miami shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification
Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud Inaccurate information within databases, logs, files or paper records.

Security Awareness
University of Miami shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

Service Providers
University of Miami shall implement and maintain policies and procedures to manage service providers. (PCI requirement 12.8)

This process must include the following:

- Maintain a list of service providers. (PCI requirement 12.8.1)
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess. (PCI requirement 12.8.2)
- Implement a process to perform proper due diligence prior to engaging a service provider. (PCI requirement 12.8.3)
- Monitor service providers' PCI DSS compliance status. (PCI requirement 12.8.4)
- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. (PCI requirement 12.8.5)

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 payment 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 payment card information must be submitted to Treasury for approval.

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.

RESPONSIBILITIES:

Please refer to Appendix I: RACI Matrix. (*Additional PCI Requirements listed in RACI*)

Available for Download at https://umshare.miami.edu/web/wda/itcisosec/PCI RACI Matrix.xlsx.

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 and the Information Security Office. The list of exceptions shall be reviewed annually and cancelled as required.

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 payment 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.

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 Treasury. All such allegations of misuse will be investigated by the appropriate University administrative office with the assistance of the Department of Information Technology, Treasury, General Counsel, 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:

- BSJ-028: Contracting Requirements
- A050: System Administrator Policy
- POL-UMIT-A145-008-00 Change and Incident Management Policy
- POL-UMIT-A155-010-01 - Information Security Policy
- POL-UMIT-A160-011-01 - Security Incident Response Notification Policy
- POL-UMIT-A165-012-01 - Security Incident Response Procedures Policy
- POL-UMIT-A175-014-01 - Electronic Data Protection and Encryption Policy
- POL-UMIT-A130-004-01 - Access Control User Account Management
- POL-UMIT-A131-005-03 - Password Security Policy
- SOP-UMIT-MSWP-137-01 - Patching Managed Microsoft Windows Workstations
- SOP-UMIT-UNXP-138-01 - Patching Unix Server Operating Systems

ENFORCEMENT:

Chief Information Security Officer of designee (CISO) is Responsible for monitoring the enforcement of the policy