REVISION HISTORY

Revision No.	Revision Date	Authors	Description of Changes
1.0	11/04/2013	CISO	Populate Into Standard Template

APPROVED BY

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

Name	Title	Signature	Date
Connie Barrera	Executive Director, Information Security and Compliance	*Signature on file*	*12/04/2013*
Tim Ramsay	Chief Information Security Officer	*Signature on file*	*12/04/2013*

PURPOSE:

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. Although intrinsic tension exists between the free exchange of ideas and information security, and can manifest itself in some circumstances, the requirements that follow have been identified to promote the best balance possible between information security and academic freedom.

The Information Technology Security Audit Policy establishes a framework for conducting audit-related reviews of information resources at the University of Miami.

SCOPE:

This policy applies to all University employees, faculty, contractors, and any other users who may conduct and/or participate with IT Audits in any capacity.

DEFINITIONS:

- **Security Audit:** Involves formally testing and evaluating vulnerabilities and controls within the Information Technology environment, performed by an independent third party, requiring the assessor to obtain independent corroboration (sampling in nature) to substantiate information provided by personnel.

- **Security Review:** Involves similar evaluation performed in a security audit but typically omits obtaining independent corroboration (non-sampling in nature) and testing to substantiate information provided by personnel. Security reviews may be performed in-house or outsourced to a third party.

- **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/network administrators and/or data custodians.

- **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.

- **Resource**: One element of hardware, software, or data that is part of a larger system.

POLICY:

It is the University of Miami's policy to conduct annual information technology security audits and reviews. The University of Miami Information Technology Department in concert with Medical Information Technology and the Privacy Office will conduct security audit and/or security reviews of identified University systems and resources at least on a yearly basis as required by compliance regulations (i.e. PCI), and in support of assessing the security posture of the organization's critical academic and business systems. Each of these offices must develop and maintain a review methodology to include the following:

- Audit/Review approval procedures
- Preliminary risk analysis
- Planning phase
- Testing phase
- Communicating results
- Remediation validation
- Final reporting

Every audit and/or review must be approved in writing in advance by appropriate designated security officer to Information Technology, Medical Information Technology and Privacy Office as well as appropriate Vice-President, Dean, and/or designee. In addition, detailed documentation of all audits must be produced and securely archived by the above offices in compliance with University data retention policies. Work may be performed completely in-house or by outside firms. In addition, IT will collect and monitor applicable log data to identify intrusion attempts and potential attacks. University entities and personnel will provide the appropriate department with timely and complete responses to all audit activities and related inquiries.

Note: *This policy does not replace the auditing and monitoring responsibilities of individual system administrators and data custodians.*

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 the responsible Vice President or Information Technology designee of the respective campus. The list of exceptions shall be reviewed annually and cancelled as required.

IMPLEMENTATION:

System Administrators/Data Custodians:

- Work with appropriate administrative and academic units during all phases of the audit, providing information whenever appropriate.
- Work with appropriate units to implement recommendations and/or execute remediation for vulnerabilities identified and confirmed.

Chief Information Security Office:

- Responsible for regular review of the IT Security Audit Policy. The review will occur annually or when significant changes occur.

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:

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

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:

- A050: System Administrator Policy
- B008: External Audits
- B009: External Auditor- Partner rotation and hiring of external auditor's personnel

ENFORCEMENT:

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