UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	IT Security Audit	REFERENCE:	Reformat
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A125-003-01
APPROVER:	David Ertel Interim Senior Vice President Business and Finance	VERSION: EFFECTIVE:	2 May 16, 2017

I. 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.

II. 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.

III. 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.

IV. 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.

V. PROCEDURE:

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.

Violations:

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

Other Applicable Policies:

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