UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Vulnerability Management	REFERENCE:	New
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	New
APPROVER:	David Ertel Interim Senior Vice President Business and Finance	VERSION: EFFECTIVE:	1 May 16, 2017

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.

I. PURPOSE:

The purpose of this policy is to authorize an information security vulnerability assessment process to determine areas of vulnerability in network assets and services and the remediation of findings.

II. SCOPE:

Vulnerability scans will be conducted on information systems, network hosts, devices and software applications owned, operated, maintained and controlled by the University, and other information systems, both internally and externally, that interact with these systems. This document also applies to University employees, faculty, students, contractors, guests, consultants, temporary employees and any other users who are responsible for the maintenance of a University information system, application, host or network device.

III. POLICY:

The University is required to comply with applicable laws, regulations, contractual obligations and institutional policies that ensure the confidentiality, integrity and availability (CIA) of institutional information assets. Vulnerabilities identified on University information systems, applications, network hosts and devices must be remediated. Inadequate system security controls do not meet compliance criteria and are a risk to information assets due to threats and other types of external and internal attacks. Vulnerability management is an essential component to information security and will be followed as listed below:

- The development, implementation and execution of the vulnerability management program is the responsibility of the Chief Information Security Office.
- A centrally managed vulnerability assessment system will be deployed. Use of any other network based tools to scan or verify vulnerabilities must be approved, in writing, by the Chief Information Security Office.
- Continuous monitoring scans will be conducted on applications, network hosts and devices residing on the University internal and external IP address space.

Frequency of a scan will be determined by application type and compliance requirements.

- An ad-hoc scan may be performed upon request by the system administrator.
- Vulnerability assessment is the joint responsibility of the Chief Information Security Office and the system administrator responsible for the asset, product or service assessed.
- The business owner and system administrator(s) will cooperate with any vulnerability assessment conducted on systems which they are held accountable.
- The business owner and system administrator will cooperate with the UMIT Security team in the implementation of remediation expectations.
- Follow up scans will be conducted upon expiration of the remediation deadline.
- As a baseline security control, security patch management, software updates and security configurations will be maintained to mitigate future threats and potential incidents.
- Third-party external vulnerability scans and penetration tests will be conducted as required by applicable governing regulations.
- Exceptions for specific systems and network areas require business justification and approval.

IV. DEFINITIONS:

Remediation: The act of correcting a vulnerability or eliminating a threat. Four possible types of remediation are installing vendor provided security patches, updating a software version, adjusting configuration settings or uninstalling a software application.

University: "University" refers to the University of Miami as a whole and includes all units.

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.

V. PROCEDURE:

Chief Information Security Office:

- Responsible for regular review of this Policy. The review will occur on a biennial cycle or when significant changes occur.
- Responsible for monitoring the enforcement of the policy.

Responsible Vice President or CIO:

- Responsible for reviewing and approving or denying exception requests.
- Responsible for reviewing exceptions annually.
- Responsible for monitoring the enforcement of the policy.

System Administrator:

- Responsible for following policy requirements as required by their role.

Business Owner:

- Responsible for following policy requirements as required by their role.

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

Other Applicable Policies:

- System Administrator Policy
- Malicious Software Prevention Policy