UNIVERSITY
OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE: Information Technology Security Incident Notification
REFERENCE: Reformat
CATEGORY: Information Technology
PAGE: 1
SUPERSEDES: POL-UMIT-A160-011-01
APPROVER: David Ertel
Interim Senior Vice President
Business and Finance
VERSION: 2
EFFECTIVE: 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. 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.

I. PURPOSE:

To ensure the confidentiality, integrity and availability of data and resources, the Information Technology Security Incident Notification Policy requires that appropriate procedures be followed to identify and report all information security events and incidents at the University.

II. 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 have access to University resources.

III. POLICY:

In the event of a confirmed or suspected security incident, University Members/affiliates must immediately notify central IT security and must not take any actions that interfere with the investigation.

IV. DEFINITIONS:

- **Security Incident:** An event involving any aspect of Information Technology, which is not part of standard operations and has the potential to cause harm to University data resources and reputation and/or financial loss.
- **University Member/Affiliate:** Anyone associated with the University of Miami including, but not limited to, employees, students, contractors, guests, consultants, temporary employees, and any other users who have access to University resource.

V. PROCEDURE:

Central IT CIO or designee:

- Responsible for reporting suspected and/or confirmed security incidents.

Chief Information Security Office:

- Responsible for regular review of the Information Technology Security Incident Response Procedures 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 monitoring the enforcement of the policy.

Violations:

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