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, the following framework has been identified to promote the best balance possible between information security and academic freedom.

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.

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.

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.

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.

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:

University members/Affiliates:

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

Chief Information Security Office:

- Responsible for regular review of the Information Technology Security Incident Notification Policy. The review will occur annually or when significant changes occur.

Responsible Vice President or Information Technology designee:

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

SANCTIONS:

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.

Knowing 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 the applicable Systems Administrator, who will report, as appropriate, to the applicable department. All such allegations of misuse will be investigated by the appropriate University administrative office with the assistance of the Department of Information Technology and the Department of Human Resources, and where appropriate, by the Faculty Affairs Office and/or the Office of the General Counsel.

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:

- POL-UMIT-A165-012-00 Information Technology Security Incident Response Procedures Policy
- POL-UMIT-A155-010-00 Information Security Policy
- POL-UMIT-A140-007-00 Cardholder Information Security Policy
- POL-UMIT-A140-007-00 Change and Incident Management Policy
- POL-UMIT-A180-015-00 Mobile Computing Policy

ENFORCEMENT:

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