UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE: Information Technology Security Incident Response Procedure	REFERENCE: Reformat
CATEGORY: Information Technology	PAGE: 1
	SUPERSEDES: POL-UMIT-A165-012-01
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 Response Procedures Policy requires that appropriate procedures and protocols be developed to identify and report information security incidents at the University and that the procedures and protocols be implemented by appropriate personnel.

II. SCOPE:

This policy applies to all Information Technology Units and any University employees, faculty, students, contractors, guests, consultants, and temporary employees, who are independently responsible for the technical administration of information technology resources.

III. POLICY:

Security incidents may occur that require full participation of Information Technology technical personnel as well as University leadership to manage the outcome properly. The process developed by each IT Unit or independent administrator must enable efficient notification of events, allow timely and efficient recovery from events, prevent or minimize disruption of critical computer services, and minimize loss or theft of protected data. To this end, each Information Technology Unit or independent administrator will establish incident response procedures that adhere to the following minimum guidelines:

- Establish a framework to allow University members/affiliates to efficiently report suspected and/or confirmed security incidents to the Central IT CIO or designee
- Formulate and activate an Incident Response Team

- Assess the seriousness of an incident
- Assess the extent of damage
- Identify the vulnerability created
- Estimate what additional resources are required to mitigate the incident, and
- Ensure that proper follow-up reporting occurs and that procedures are adjusted so that responses to future security incidents are improved

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.
- **Incident Response Team:** Multi-disciplinary team assembled and activated to address security incidents.
- **Information Technology Unit:** The collective description of a group of Information Technology professionals who are not part of the centralized IT department yet provide Information Technology services to a particular population of constituents throughout the University.
- **Independent Administrator:** Any individual, who is not a member of a group of Information Technology professionals, yet provides IT administration of one or more systems throughout the University.
- **Protected Data:** Any data governed under Federal or State regulatory or compliance requirements such as HIPAA, FERPA, GLBA, PCI/DSS, Red Flag, and FISMA as well as data deemed critical to business and academic processes which, if compromised, may cause substantial harm and/or financial loss.
    - **HIPAA:** The Health Insurance Portability and Accountability Act of 1996 with the purpose of ensuring the privacy of a patient's medical records.
    - **FERPA:** The Family Educational Right and Privacy act of 1974 with the purpose of protecting the privacy of student education records.
    - **GLBA:** The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, contains privacy provisions requiring the protection of a consumer's financial information.
    - **FISMA:** The Federal Information Security Management act of 2002 recognizes the importance of information security to the economic and national security interests of the United States and as a result sets forth information security requirements that federal agencies and any other parties collaborating with such agencies must follow in an effort to effectively safeguard IT systems and the data they contain.
    - **PCI/DSS**: Payment and Credit Card Industry Data Security Standards is guidance developed by the major credit card companies to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing card payments must be PCI compliant or risk losing the ability to process credit card payments.
    - **Red Flag:** A mandate developed by the Federal Trade Commission (FTC) requiring institutions to develop identity theft prevention programs.

V. PROCEDURE:

Central IT CIO or designee:

- Responsible for reviewing and approving individual IT Unit Incident Response Procedures.

IT Units and independent Administrators

- Responsible for developing and maintaining Incident Response Procedures in support of their respective Information Technology environment.

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 reviewing exceptions yearly.
- Responsible for monitoring the enforcement of the policy.

Violations:

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