UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE: Mobile Computing
CATEGORY: Information Technology
APPROVER: David Ertel
Interim Senior Vice President
Business and Finance

REFERENCE: Reformat
PAGE: 1
SUPERSEDES: POL-UMIT-A180-015-01
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 following framework has been identified to promote the best balance possible between information security and academic freedom.

I. PURPOSE:

To maintain the confidentiality, integrity and availability of data and network resources at the University of Miami, the Mobile Computing Policy establishes requirements for safeguarding portable electronic devices that can contain Protected Data.

II. SCOPE:

This policy applies to all electronic devices, both University owned and purchased by individuals, that can contain Protected Data. It applies to employees, faculty, students, contractors, guests, consultants, temporary employees, and any other users, including all personnel affiliated with third parties University resources.

III. POLICY:

It is the University of Miami's policy to protect mobile computing devices and the information contained on such devices. University Members must ensure that they protect the hardware provided from theft and unnecessary damage. To protect such devices and the information users therefore should:

- Keep electronic devices within view or securely stored at ALL times.
- When possible avoid packing electronic devices in luggage that will be checked at airports and outside of the individual's custody.
- Ensure that the electronic device is shut down or secured when not in use (e.g., password protect devices offering such capabilities).

- Ensure that University-approved anti-malicious software applications and signatures are up-to-date and a personal firewall is installed and configured when available on all devices.
- Avoid unsecured or untrusted networks.
- Use a University-approved backup process when available for Protected Data.
- Use encryption to safeguard all storage media, (e.g., hard drives, USBs).
- Promptly notify IT Security and Physical Security if any electronic device has been lost or stolen.

Note: Mobile computing devices or information contained on them may be subject to Export Control laws. Prior to traveling to counties listed in 15 C.F.R. 742.1 (As of May 2009: Iran, North Korea, Syria, Cuba or Sudan) the individual must contact the Office of Research Compliance for an Export Control review and determination. Individuals should not assume they, their electronic device, or information are exempt when traveling overseas and are encouraged to visit the Export Control webpage at: www.miami.edu/exportcompliance for further information. Questions may be directed to the Director of Research Compliance at researchcompliance@miami.edu or 305-243-4538.

Additional requirements for securing protected data:

Where there are large amounts of Protected Data, supplemental measures need to be taken to further minimize the risk of loss. The amount of data that would constitute a large amount for these purposes will vary, depending on:

- the quantity and extent of the data records;
- how readily the data can be used to identify individuals;
- how serious the consequences would be for the University if the data were successfully stolen or publically released; and
- the legal duties, if any, to protect the information.

Each academic or administrative unit possessing large amounts of Protected Data must publish policies explaining the data to be protected and what is meant by a large amount in that unit's context. (For additional guidance, see NIST-SP-800-122.)

The unit's policy statement will also set forth the supplemental measures that will be taken to protect such data. These may include the use of dedicated non-networked computers, physical access limitations, multiple layers of passwords and/or pass phrases; biometric access control; and/or more frequent security audits and reviews.

Mobile Devices are particularly vulnerable and should not be used for the storage of or access to large amounts of Protected Data. Where there is nevertheless a compelling academic or business reason to allow the use of a Mobile Device for that purpose, the Dean or Vice President in charge of the unit and the CIO will

jointly determine what supplemental security measures are prudent given the quantity and sensitivity of the data. These measures will include, at a minimum, either (1) de-identification of the data to prevent information being tied to particular individuals or (2) at least two layers of access control, plus inspection of the device to verify that appropriate encryption software has been installed and activated.

IV. DEFINITIONS:

- **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.
    - **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.
    - **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.
    - **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.
- **University Member/Affiliate**: Anyone associated with the University of Miami including employees, students, contractors, guests, consultants, temporary employees, and any other users who may have access to University resources.
- **University**: "University" refers to the University of Miami as a whole and includes all units.
- **Portable devices**: devices that contain or intended to contain protected data, i.e. laptops, mobile phones, USB devices, etc. used by University members who work outside of the office or who travel and need to maintain connectivity to University of Miami information and resources.

V. PROCEDURE:

System Administrator:

- Responsible for configuring electronic devices and client workstations for their supported areas to adhere to this policy.

University Members/Affiliates:

- Responsible for adhering to requirements outlined in this policy.

Chief Information Security Office:

- Responsible for regular review of the Mobile Computing 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.

Violations:

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