UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE: Electronic Data Protection and Encryption
REFERENCE: Reformat
CATEGORY: Information Technology
PAGE: 1
SUPERSEDES: POL-UMIT-A175-014-01
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:

This policy establishes a framework that outlines when encryption must be used to secure the University's data from risks including but not limited to, access, use, disclosure, and removal as well as to adhere to regulatory and compliance requirements.

II. SCOPE:

This policy applies to all electronic data stored on any media or system(s) throughout the University of Miami and applies to all individuals storing, accessing, or working with the data, in any way, including all University employees, students, contractors, guests, consultants, temporary employees, and any other users who may have access to University resources.

III. POLICY:

The University of Miami requires that Protected Data be secured at all times. Therefore, University Protected Data must never be moved or copied outside of standard approved operating procedures.

Data encryption:

The University requires data be encrypted under the following circumstances:

1. Physically moving data:

1.1. University Protected Data must be encrypted when residing on any media. This includes but is not limited to:

- Laptops
- Desktops
- Backup media

- DVDs
- External hard drives, thumb drives, etc.

Note: The list above applies to all devices, regardless of ownership, whenever they contain Protected Data.

2. Electronically transmitting data:

   2.1. Protected Data must be encrypted when transmitted over an electronic communication network (internally and externally).

   2.2. Email containing Protected Data destined for external email recipients must be encrypted and contain the following confidentiality statement:

   "The information contained in this transmission may contain privileged and confidential information, including information protected by federal and state privacy laws. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message."

   2.3. Protected Data shall not be sent through insecure public instant messaging networks. Examples of insecure instant messaging networks include, but are not restricted to, AOL Instant Messenger, Yahoo Messenger, MSN Messenger, and Google Talk.

3. System Administrators shall implement formal, documented processes for utilizing encryption and integrity controls on University Protected Data being transmitted over electronic communications networks. At a minimum, such processes shall include:

   3.1. A procedure enabling Protected Data recipients to report instances of attempted or successful unauthorized access to University Protected Data that is transmitted over an electronic communications network.

   3.2. A procedure for responding to instances of attempted or successful unauthorized access to University Protected Data that is transmitted over an electronic communications network.

Encryption standards:

The University requires all of the following minimum encryption criteria:

1. Standard encryption algorithms must be used. Some examples include: 3DES, Blowfish, RSA, RC5 and IDEA.
2. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Information Technology Security Department.
3. A one-way hash to encrypt data irreversibly must be used for:

   - Private keys must be kept confidential,
   - Key management must be fully automated,
   - Short life keys are to be used, ensured by having activation and deactivation dates,
   - Long-life keys are to be used sparingly,
   - Keys in storage and transit must be encrypted,

- Keys must be chosen randomly from entire key space,
- Keys for encrypting keys must be used separately from keys used for decrypting data. They are not interchangeable.

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:

- **Data:** Information stored on any electronic media throughout the University of Miami.
- **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.

- **Cryptography:** The science of radically changing information in order to conceal the content from a third party.
- **Encryption Algorithm:** A mathematical formula used to encrypt and decrypt data.
- **External Email Recipients:** Email recipients who are not part of a University maintained email system.
- **Proprietary Algorithm:** An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
- **One-way Hash Function:** An algorithm that does not require a key and produces an irreversibly encrypted cipher-text. Other names for this are message digest, fingerprint, digital signature, and compression function.
- **Personally Identifiable Information (PII):** Any piece of information contained in Protected Data which can potentially be used to uniquely identify, contact, or locate a single person. Examples of PII include Protected Health Information, Credit Card Numbers, Social Security Numbers, etc.
- **System Administrator:** An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and permanent part-time employees of the University and/or third party vendors approved by IT may function as system/network administrators.
- **Data Custodian:** The person responsible for, or the person with administrative control over, granting access to an organization's documents or electronic files while protecting the data as defined by the organization's security policy or its standard IT practices.
- **University:** "University" refers to the University of Miami as a whole and includes all units.

V. PROCEDURE:

System Administrator/ Data Custodian:

- Responsible for following the policy by encrypting data whenever required.
- Responsible for communicating any exception requests to the Vice President or Information Technology designee of the respective campus.

Chief Information Security Officer

- Responsible for regular review of the Encryption Policy. The review will occur annually or when significant changes occur.

Responsible Vice President of 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.