UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Password Security	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A131-005-04
APPROVER:	David Ertel Interim Senior Vice President Business and Finance	VERSION: EFFECTIVE:	4 March 1, 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.

I. PURPOSE:

This policy establishes a framework for establishing password security as well as adhering to regulatory and compliance requirements.

II. SCOPE:

This policy applies to all electronic hardware and protected data stored on any media or system(s) throughout the University of Miami and applies to all University employees, faculty, students, contractors, guests, consultants, temporary employees, and any other users who may have access to University resources.

III. POLICY:

It is the University of Miami's policy to secure access to University information resources by implementing a strong password management program.

Passwords used to access the University information resources must be hardened through implementation of the following criteria:

- Passwords must be at least 7 characters and consist of the following four character types:
  - Uppercase alphabet characters (A through Z)
  - Lowercase alphabet characters (a through z)
  - Arabic numeric characters (0-9)
  - Non alphanumeric characters (for example, !, $, #, %)
- Beginning in June 2015, all passwords must be changed every 180 days. Users who have access to data that a Regulatory Agency requires have more frequent password changes, or who have access to large quantities of any protected data will be required to have more frequent password changes. PCI/DSS requires that all related users and systems passwords must be changed every 90 days.

- The account must be locked after 10 failed password attempts, until manually reset by an administrator or a 30-minute timeout period has elapsed.
- The password history must be such that it is unique over the last 10 passwords;
- A password change must require the user to enter the previous password or other information known only to the user such as a response to a security question.
- For devices used in patient care, monitoring experiments or otherwise cannot be locked out, supplemental security measures will be required. All other devices must be locked out for inactivity. The required setting for inactivity is 15 minutes for HIPAA data or large quantities of any other protected data. For all other computers the recommended setting is 30 minutes. Nothing in this policy precludes users from establishing even shorter lockout periods.

  Note: For legacy, proprietary, and/or third party systems that cannot meet these standards, the most restrictive password policy appropriate for the environment and other compensating controls should be implemented and documented as an exception. In addition, the capability to meet password security requirements should be an important consideration when acquiring new information resources.

To preserve password security, the following practices must be adopted:

- During new user orientation, employees must be advised as to how to choose a good password (e.g., must not be a word found in any dictionary, must not be the same as the account name, no blanks, must not be a spouse, child, or pet name, etc.).
- Passwords must not be written down.
- Clear text passwords must not be entered into script files, macro functions or function keys.
- Passwords must not be communicated to or shared with others.
- Passwords must be changed immediately upon:
  - Learning a password has been compromised;
  - A security breach is suspected;
  - Learning a password has been shared with another individual;
  - Changes of personnel or personnel leaving University (i.e. departmental inbox); or,
  - User no longer requires access to the system.

  Note: Process/activities that require the use of service accounts are acceptable as long as the account password is protected.

When emergency copies of passwords are kept by system administrators, security procedures (approved by the appropriate designated security officer at Information Technology, Medical Information Technology or Privacy Office) must be put in place to ensure that they are retained under the control of authorized personnel (for example, securely kept in sealed envelopes or encrypted data files in a secure environment).

IV. DEFINITIONS:

Password Security: A set of rules designed to enhance computer security by requiring users to establish secure passwords.

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 and/or data custodians.

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.

Proprietary Software: Proprietary software is one designed and owned by a company who has not divulged specifications that would allow other companies to duplicate the product.

Third Party Software: An auxiliary product not supplied by the primary manufacturer to the end user.

Legacy System: An older computer system or application program that has not been replaced by newer technology.

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.
- **FDA:** US Food and Drug Administration with the purpose of protecting research data used in regulatory submissions.
- **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.

V. PROCEDURE:

Users:

- Responsible for maintaining the confidentiality of their password(s).

System Administrator/Data Custodian:

- Responsible for following the policy of granting access to University resources to necessary individuals on a need-to-know basis.
- Responsible for communicating any exception requests to the Vice President or Information Technology designee of the respective campus.

Chief Information Security Office:

- Responsible for regular review of this 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.

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:

- Mobile Computing Policy
- Access Control and User Account Management Policy
- Information Security Policy
- Cardholder Information Security Policy

Enforcement:

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