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, 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.

This policy establishes a framework for establishing access control and user account management as well as adhering to regulatory and compliance requirements.

SCOPE:

This policy applies to all University employees, faculty, students, contractors, guests, consultants, temporary employees, and any other users who may have access to University resources containing protected data.

DEFINITIONS:

- **Access Control**: To permit or deny access to a particular resource.
- **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 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.
- **User Account Management**: Identity life cycle ranging from creating, maintaining, and ultimately decommissioning/deleting user accounts.
- **Legacy System:** An older computer system or application program that has not been replaced by newer technology.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.

- **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.

- **Privileged Accounts:** An account with the ability to establish or modify application system policies, perform administrative tasks and make global changes which can impact entire systems or processes.

POLICY:

Access control:

All individuals who require access to University information resources containing Protected Data must be appropriately authorized prior to such access being granted. The authorization will be approved on a need-to-know basis by the relevant manager. Access to information systems must be restricted to authorized personnel in order to prevent and detect unauthorized access or abuse. To maintain effective security it is vital for the University to ensure that data can only be accessed and processed by authorized personnel.

System Administrators and Data Custodians must strictly control access to information resources under their direction or ownership. When approving access rights, the respective manager must ensure the following requirements are considered and evaluated prior to approving such access and before forwarding the request to the system administrator or data custodian:

- User's need for access;
- Potential conflict with segregation of duties;
- Any regulatory requirements;
- Level of access required (read, update, delete); and,
- Access duration.

User Account Management:

The following requirements regarding User account Management must be implemented:

- All users must be assigned their own unique user account with only the privileges needed to perform their job.
- There must be a formal registration and de-registration procedure for providing an employee with a University account requiring authorization from appropriate management, or an authorized delegate.
- Identifiers and authentication for accounts must be independent of the employees' internal unique identifiers.
- Account creation, updates, disabling, suspending, resetting, and re-enabling must be a defined process. All such account activity should be logged in a secure audit trail.
- The number of users/administrators with privileged accounts on servers must be restricted. Appropriate managers must specifically authorize privileged accounts.
- Administrators must use unique administrator account allocated per administrator.
- Every unique user ID must correspond to an individual unless there is an operational need to allocate a generic user ID, in which case the appropriate justification must be presented in writing to the IT Security staff at the appropriate campus to determine if adequate compensating controls may be implemented to track and monitor use of the account.
- The use of any anonymous accounts (such as the UNIX root or NT Administrator account) or guest accounts must be limited to emergency access or if they are specifically required and must be authorized by appropriate managers.
- Where accounts for employees, faculty and staff must be automatically disabled upon separation from the university.
- All other accounts must be automatically disabled after 180 days of inactivity. Inactive faculty accounts will be checked to determine if the faculty member is on sabbatical, visiting away, or away for extended research.
- Disabled accounts must be deleted after 180 days of being disabled.

Note: Documentation for legacy systems that cannot meet these standards must be maintained and alternative controls implemented dependent on the levels of data held on such systems. The capability of meeting information security and compliance requirements should be an important consideration when acquiring new information resources.

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:

Users:

- Responsible for maintaining the confidentiality of their account(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.
- Responsible for the provisioning and deprovisioning of accounts within their respective systems.

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 CIO:

- 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, violates University policy, or interferes with disaster recovery efforts.

Violations of the policy will be addressed by disciplinary policies and procedures applicable to the individual.

All known and/or suspected violations, or knowing interference with disaster recovery efforts must be reported to the applicable Systems Administrator, who will report, as appropriate, to the applicable Technology 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:

- POL-UMIT-A180-015-00 Mobile Computing Policy
- POL-UMIT-A131-005-00 Password Policy
- POL-UMIT-A155-010-00 Information Security Policy
- POL-UMIT-A190-016-00 Remote Access Policy
- POL-UMIT-A140-007-00 Cardholder Information Security Policy

ENFORCEMENT:

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