UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Access Control User Account Management	REFERENCE:	Reformat
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A130-004-01
APPROVER:	David Ertel Interim Senior Vice President Business and Finance	VERSION: EFFECTIVE:	2 May 16, 2017

I. 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.

II. 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.

III. POLICY:

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 Windows 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.

IV. 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.

V. PROCEDURE:

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 de-provisioning 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

Violations:

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

Other Applicable Policies:

- Mobile Computing Policy
- Password Policy
- Information Security Policy
- Remote Access Policy
- Cardholder Information Security Policy