UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	System Administrator	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A050-023-01
APPROVER:	David Ertel Interim Senior Vice President Business and Finance	VERSION: EFFECTIVE:	2 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. 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:

The purpose of this document is to establish guidelines for individuals who perform system administration duties on University of Miami (UM) information technology resources.

II. SCOPE:

This document applies to all University Member/Affiliates who are granted System Administrator access or an elevated privileged account to any UM managed service, application or server. For purposes of this document, System Administrator, Network/Systems Administrator, Security Administrator, Email Administrator and any individual with elevated privileged access to a University information technology resource, are collectively referred to as “System Administrator”.

III. POLICY:

It is the responsibility of the System Administrator to follow the guidelines of their administrative unit as well as all pertinent University of Miami policies, licensing agreements with software manufacturers, and local, state and federal regulations. Individuals with privileged access rights to UM information resources are entrusted to use such access in an accountable, professional and secure manner which is consistent with designated job responsibilities.

IV. DEFINITIONS:

Administrative Unit: Any school, department, division, office, or person that provides or facilitates computing, telecommunications or network services to the members of the University of Miami community.

Network/Systems Administrator: A person who configures network and server hardware and the operating systems running on them in order to ensure that the information accessible through UM managed information technology systems will be available when needed.

Security Administrator: A person who manages user access, request process and ensures that privileges are provided to those individuals who have been authorized access to a UM information technology resource.

System Administrator: A person who manages the technical aspects of an information system and provides effective information system utilization, adequate security parameters and sound implementation. A system administrator includes any University Member/Affiliate with privileged account access that is above a normal user.

University Member/Affiliate: Employees, faculty, students, volunteers, trainees, contractors and other entities or persons who perform work for or on behalf of UM.

Privileged Accounts: A system user granted elevated privileged access with the ability to establish or modify application system policies, perform system administrative tasks and make global changes which can impact entire systems or processes.

V. PROCEDURE:

A. Responsibilities

As part of normal business practices, System Administrators are held to the highest standard of behavior and ethics as they have the responsibility and trustworthiness to maintain system integrity, reliability and availability. The responsibilities for individuals who configure and manage services and systems are:

1. Documentation

System documentation, inventory and operational procedures will be developed and maintained current. Applicable change control procedures will be followed.

2. Security

a) Technical security controls will be implemented in order to mitigate risk, maintain stable operations, and comply with applicable regulations. Technical security controls will include but are not limited to:

b) Applying operating system, service and application patches, hot fixes, updates and new releases as necessary

c) Maintaining systems and servers with the minimum services, applications and open TCP/UDP ports required in order to mitigate exploitation of the system.

d) Implementing encryption requirements for data classified as sensitive or protected.

e) Notifying UMIT Security Team of suspected incidents and assist in the investigation and remediation of incidents as needed.

f) The use of a privileged access account is for system administration functions only. A privileged access account or system administrator account may not be used when performing normal user activities.

g) Changing default passwords of root and admin accounts.

h) Enabling operating system, service and application logging.

i) Taking precautions against theft or damage to the system components.

3. User Accounts

The creation of user accounts will be approved by the business owner, documented, controlled on the basis of “least privilege” and need to know. . Ongoing user administration will be managed effectively and efficiently. User accounts will be disabled after a designated number of consecutive days of inactivity. The disabling of inactive user accounts will be determined by the administrative unit and will be based on business needs and applicable regulatory compliance requirements. A decision not to disable accounts for unlimited days of inactivity must be documented.

4. Professionalism

Services and systems will be configured to fulfill the needs of the University. Working with users, vendors, consultants, upper management and other system administrators requires patience and care to maintain a level of respect. At times, this will include cooperating with fellow colleagues with the implementation or upgrade of services or applying corrective and protective actions.

5. Privacy and Ethics

Individuals with privileged access will take necessary precautions to protect the confidentiality of information encountered in the performance of their duties. Good faith efforts will be taken to obtain account owner consent before accessing files or interfering with their processes. If during the performance of duties, information indicating inappropriate use is discovered, UMIT security will be consulted.

B. Sanctions:

Accounts and network access may be administratively suspended with or without notice by the University as per existing University regulations, Faculty manual where applicable, and due process when in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University policy.

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

C. Other Applicable Policies:

- Data Classification Policy
- Malicious Software Prevention Policy
- Access Control and User Account Management Policy
- Electronic Data Protection and Encryption Policy
- Password Security Policy

D. Enforcement

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