UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Use of University Computing Facilities	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A046-022-01
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.

I. PURPOSE:

It is the purpose of this policy to inform users of expected standards of conduct related to the use of University computing facilities and the disciplinary measures for failing to adhere to them.

II. SCOPE:

This policy applies to all University employees, scientific and technical staff, administrative staff, students, faculty, guest investigators, visiting professors, as well as to all other users of the University Computing Facilities or those who have contracted for access to such facilities. Users of University computing facilities are not only subject to University policies, but to applicable local, state, and federal laws.

III. POLICY:

Open access to University computing facilities is a privilege granted by the University to authorized users and may be administratively suspended with or without notice when, in the University's judgment, continued use of University resources may interfere with the work of others, places the University or others at risk, or violates University policy. Proper use of University computing facilities involves only those activities performed in support of University contractual and/or operational requirements. Determining authorized use is the responsibility of senior management within the individual administrative units.

Unauthorized or Illegal Use of University Computing Facilities:

Unauthorized or illegal use of University computing facilities is prohibited:

- applying for a fraudulent user ID;
- use in violation of the terms included in federal, state and private grants and contracts awarded to the University community;
- use for commercial applications unrelated to the University's assigned functions and authorized activities;
- use of computer accounts and/or electronic identification addresses without authorization;

- obtaining passwords without the consent of owners or divulging any confidential information (including user ID) or passwords to any third parties (persons who divulge such information to third parties are solely responsible for the actions of such third parties);
- gaining access to any University computer and/or any remote computer or network, or to information contained therein, without authorized permission;
- intentional or reckless disruption of system or user passwords is prohibited;
- intentionally performing acts which interfere with the normal operations of computers, terminals, peripherals, or networks;
- attempts to secure a higher level of access or privilege without appropriate authorization;
- knowingly installing and being on any computer system or network or giving to another user a program designed to damage or render unusable a computer system or network (e.g. viruses);
- unauthorized circumvention of system security schemes;
- violating terms of software licensing agreements or copyright laws;
- monitoring or tampering with others' communications;
- reading, copying, changing, or deleting software without explicit consent of the owners, without the authorization of the appropriate system administrator;
- transmitting information which is obscene or otherwise prohibited by law;
- taking or disclosing, without authorization, data which is confidential as provided by law;
- modifying or destroying data without authorization;
- conducting any activities with are illegal under Federal or State Law, or which violate any other University policy.

Implementation and Authority of Systems Administrators:

- Access to the University Computing Facilities increases the vulnerability of equipment and software connected to it. The University promotes the use of security measures on all of its computer communication facilities.
- Security measures must be supported by all users. Theft, loss, or damage to data, computer/network and software applications, as well as unauthorized access to information, may occur from inadequate system security protection mechanisms, despite efforts to maintain those systems and network security facilities.
- The University makes no warranty, either expressed or implied, with respect to security measures implemented on University computing facilities. System administrators are responsible for implementing measures to protect hardware, software, data and/or security on their individual systems.
- Where access to the contents of any individual's communications or other information stored in the system is required pursuant to a valid subpoena, search warrant or other compulsory process, the University will provide notice to such individuals as provided by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2710, et. seq. and other applicable laws.
- It is neither University policy nor practice to routinely examine transmissions or files maintained on the University computing facilities. In certain limited circumstances, however, appropriate user files are subject to monitoring or examination for legitimate business purposes at any time by authorized University officials in the ordinary course of their employment, when necessary to protect the integrity of University computing facilities, the rights or property of the University or third parties, or to insure compliance with University policy and applicable law.

- Legitimate business purposes shall be determined by the University under the circumstances of each case. In such cases, the individual whose file or communications contents are reviewed shall be notified after such review has taken place. In addition, Systems Administrators or employee supervisors may also conduct any monitoring of technical data and network traffic as needed to insure reasonable maintenance and use of system hardware, software, and data.
- Any examination of user files, or monitoring of technical data or network traffic, shall be subject to the guidelines of the Systems Administrator Policy. All University personnel, staff, students, researchers, faculty, guest investigators and visiting professors must cooperate fully with any search conducted by the University for any lawful purpose, including internal audits.

IV. DEFINITIONS:

Administrative Unit: The department, school/college, office, administrative or scientific unit with financial responsibility for the acquisition, operation and/or maintenance of a computing or network resource.

University Computing Facilities: The University of Miami network and any other computing and data resources, including hardware and software, owned by the University whether or not such computing resources are connected to the University network.

V. PROCEDURE:

Chief Information Security Office:

- Responsible for regular review of this Policy. The review will occur on a biennial cycle or when significant changes occur.

Responsible Vice President or CIO:

- Responsible for reviewing and approving or denying exception requests.
- Responsible for reviewing exceptions annually.
- Responsible for monitoring the enforcement of the policy.

System Administrators:

- Responsible for following policy requirements as required by role.

Users:

- Responsible for following policy requirements

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 System 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.

Enforcement:

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

Other Applicable Policies

- System Administrator Policy
- Malicious Software Prevention Policy