UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Computer Access and Confidentiality	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A045-021-01
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 University has established an institution-wide system of computer data and information. University employees and faculty members are given certain types of access to certain databases consistent with their position and job responsibilities.

II. SCOPE:

This policy applies to all University employees, faculty, students, contractors, guests, consultants, temporary employees, and any other users, including all personnel affiliated with third parties who have access to University information technology resources.

III. POLICY:

Authorized system users and restricted access system users must keep information obtained from system access confidential except as otherwise necessary to perform the task assigned. In all instances, authorized system users and restricted access system users are responsible for having knowledge of and complying with all laws and University policies relative to confidentiality.

IV. DEFINITIONS:

Authorized system user: A person who has been given a sign-on access code by the appropriate data custodian. Such access may be restricted to certain limited information (see below).

Restricted access code system user: A person who has been given a sign-on access code, but who is restricted to limited information.

University – “University” refers to the University of Miami as a whole and include all units.

PROCEDURE:

A. Guidelines for Access to Data Bases:

1. Regular full-time and regular part-time employees should be provided access to information on the University's computer system only on a need-to-know basis.

2. Such limitations must be consistent with University policy and applicable law. For example, if student information is involved, such access must be consistent with the Family Educational Rights and Privacy Act (Buckley Amendment) (20 USC 1232g). If patient information or medical records are involved, such access must be consistent with applicable University policy and Florida and Federal Statutes (i.e., HIPPA). Access to personnel records is also limited by University policy and by applicable law. Except in limited circumstances, students, student assistants, and part-time (other than regular part-time) employees of the University shall not be permitted to have access to confidential information residing in the various applications.

3. Students and part-time (other than regular part-time) employees may be allowed to have only limited access sign-on codes into any of the applications systems. The determination of whether or not a student or part-time (other than regular part-time) employee should have such access will be as follows:

    i. The need to know or use the information to do a specific job for an authorized user.

    ii. The duties of the employee must be specifically assigned, and a determination made that the employee has a need to use certain confidential information.

    iii. There must be adequate supervision of the employee at all times while accessing the system. The preceding criteria should be documented by each department when requesting student assistants. The College Work-Study Department should include these criteria in the training session for departments and when assigning student assistants.

B. Confidentiality Obligations of All Employees:

1. All information obtained through the system must be kept confidential, and may not be modified, copied, disclosed or made available to others, except as permitted under Federal and Florida law and as required for the performance of the employee's job, without the prior permission or instruction of the supervisor.

2. Authorized system users and restricted access system users may not disclose their access code to anyone.

3. Authorized system users and restricted access system users must follow all applicable security guidelines relating to use of the system. System users are obligated to make every reasonable effort to prevent the viewing of information by unauthorized parties

4. Data custodians and supervisors are expected to inform each authorized system user and restricted access system user of this policy and any specific requirements relating to the user's specific circumstances.

5. Authorized system users and restricted access system users must be particularly aware of privacy issues when dealing with student and medical

patient information. Unauthorized disclosure of such information is strictly prohibited, and may violate federal and state laws.

6. Authorized system users and restricted access system users must sign a Computer Access Authorization Form (available from the appropriate data custodian) at the time of applying for an access code. Information on appropriate data custodians is available from Information Technology Security/Control Department.

C. Sanctions

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

D. Enforcement

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