UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Security and Control	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A020-019-01
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 is steadily becoming more dependent on computerized information systems. Implementation of more sophisticated technologies implies better service-levels and increasing automation of operational and managerial procedures. Consequently, the University becomes more vulnerable to interruption and corruption of computing resources.

Protection of these resources from deliberate and/or accidental unauthorized access, use or modification is a major concern. Security of resources depends on some combination of access control measures, for which certain users possess keys. No combination provides absolute security. Ultimately, the level of security provided at any particular installation must result from a conscious decision weighing the trade-offs between the perceived risk, the cost of reducing that risk and the associated benefit from the risk reduction. The policy identifies the responsibilities of University organizational units with respect to these issues.

II. SCOPE:

This policy applies to all University employees, faculty, contractors, guests, consultants, temporary employees and any other users, including all personnel affiliated with third parties who are responsible for the security and protection of University information technology resources.

III. POLICY:

The Vice President for Information Technology is responsible for providing the means for accomplishing physical and logical security for the hardware, software and data under the direct control of his/her department.

Users are responsible for providing physical and logical security for University resources under their direct control. In this context, each University organizational unit (including Information Technology) as well as sub units, is considered a user.

Physical security includes but is not limited to:

- Controlling access to computer hardware.
- Preventing service interruptions (power, hardware failure).
- Planning for disaster and other contingencies.

Logical security includes but is not limited to:

- Controlling access to and use of software and data.
- Recovering data, transmissions and software.
- Archiving data, software and documentation.

IV. DEFINITIONS:

University: "University" refers to the University of Miami as a whole and includes all units.

V. PROCEDURE:

A. Chief Information Security Officer:

- Coordinates ongoing efforts to identify security issues, develop and distribute standards and procedures.
- Implements both immediate and long range security and control means and strategies.
- Provides consultation, upon request, to the user for areas under his/her direct control.
- Ensures physical and logical security status are monitored, and violations are reported to the appropriate level of authority.

B. 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

C. Other Applicable Policies:

N/A

D. Enforcement

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