UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Software Copyright	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A040-020-01
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:

University members should be aware of the provisions of the United States Copyright Law and the application of these provisions to the use of software purchased or licensed from outside vendors. This policy has been developed in an effort to increase awareness of and encourage compliance with these provisions.

II. SCOPE:

This policy applies to all University employees, faculty, students, contractors, guests, consultants, temporary employees and any other users, who are responsible for or have access to University information technology resources.

III. POLICY:

Students in all courses making extensive use of copyrighted programs are to be made aware of the ethical and practical problems caused by software piracy.

The copyright law of the United States, Title 17 of the United States Code, governs copying and use of computer programs which are copyrighted. However, the particular license agreement applicable to the software may be more restrictive than the copyright laws. In that event, the program user must adhere to the provisions of the applicable license agreement as well as the provisions of U.S. law.

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

IV. DEFINITIONS:

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

PROCEDURE:

A. U.S. Copyright Law Requirements

1. U.S. copyright law provides that it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaption of that program provided:
    a. That such a new copy or adaption is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, *or*
    b. That such a new copy and adaption is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.
2. If the compliance with the above provisions is not acceptable, *i.e.* if the user wishes to make additional copies, the user should obtain the prior written permission of the company holding the copyright to the software to use or copy the programs in a manner other than as provided by law or the terms of the license agreement.

B. Software Licensing

1. The Vice President for Business Services, or his designee, is the only individual who may sign license agreements for software for the University.
2. Each college, school, and division in the University is responsible for establishing practices which will enforce this policy. The following is appropriate for posting near computers and/or computer terminals:
    i. Computer programs may be protected by federal copyright law or license agreements.
    ii. Copying such programs without appropriate written permission is prohibited.

C. Sanctions

1. Knowing violations of the policy will be addressed by disciplinary policies and procedures applicable to the individual.
2. 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.
3. Penalties may include:
    i. Suspension or termination of access to computer and/or network resources;
    ii. Suspension or termination of employment, to the extent authorized by other university published policies and procedures;
    iii. Suspension or termination of contract computer and/or network services; *or*
    iv. Criminal and/or civil prosecution.

D. Enforcement

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