


UNIVERSITY OF SOUTH FLORIDA

Policies and Procedures Manual

| | | | |
|--|--|-----------------|---------------|
|  | Subject of Policy Statement | Effective Date | Policy Number |
| | Appropriate Use of Information Technology Resources | 02/23/95 | 0-502 |

I. INTRODUCTION (Purpose and Intent)

The increasing reliance on information technology resources by the University requires an environment in which these resources are used in a responsible and effective manner by everyone in the University community. Such an environment will permit the most efficient and productive use of these resources. The purpose of this policy, therefore, is to establish guidelines for the appropriate and responsible use of information technology resources by University students, faculty and staff.

Information technology resources shall be interpreted to include all University computing and telecommunications facilities, equipment, hardware, software, systems, networks and services which are used for the support of the teaching, research and administrative activities of the University.

II. STATEMENT OF POLICY

The information technology resources of the University of South Florida are a vital component of the academic and administrative environment of the University. It is the responsibility of all University students, faculty and staff to use these resources in a responsible, ethical and lawful manner. Any member of the University community who abuses these resources has engaged in unacceptable conduct. Activities which intentionally damage or interfere with the work of other users are especially inappropriate and may constitute felonies under Florida state law.

Students, faculty and staff are responsible for all actions taken using any computer logon ID assigned to them. Appropriate use of a logon ID includes proper password protection for the logon ID, not allowing anyone else to use the logon ID, not using someone else's logon ID and not abusing the privileges granted to the logon ID.

University Policy 0-501 assigns responsibility for protecting University information to all faculty, staff and students. Each college, division or unit is required to administer appropriate controls to protect the confidentiality, integrity and availability of University information.

Copyrighted software must only be used in accordance with its license or purchase agreement and must not be copied or altered except as permitted by law or by the software licensing agreement. Unauthorized copying, distribution or use of such software is a crime and the University as well as individuals may be held legally liable for these actions.

Other examples of inappropriate actions under this policy include, but are not limited to, the following:

- Unauthorized access, alteration or destruction of another user's data, programs, electronic mail or voice mail.
- Attempts to obtain unauthorized access to either local or remote computer systems or networks.
- Attempts to circumvent established security procedures or to obtain access privileges to which the user is not entitled.
- Attempts to modify computer systems or software in any unauthorized manner.
- Unauthorized use of computing resources for private purposes.
- Transmitting unsolicited material such as repetitive mass mailings, advertising or chain messages.

III. PROCEDURES

Individual colleges and departmental units shall advise users in their areas of these policies and may also issue additional "conditions of use" for facilities under their control. Such conditions must be consistent with this University policy but may provide additional detail, guidelines, restrictions and/or enforcement mechanisms appropriate to their area. Units may require signatures of individuals acknowledging an understanding of these policies and conditions before providing access.

Violations of this policy may lead to suspension of the user's computer logon ID and/or disciplinary action to be handled by Student Affairs, deans or directors as appropriate. In any investigation of misuse of information technology resources, the system administrator may inspect, without notice, the contents of computer files, system output, electronic mail and other related materials.

Chapter 815, Florida Statutes, the "Florida Computer Crimes Act," describes offenses which are felonies under Florida law. These offenses include unauthorized modification of programs or data, unauthorized disclosure or use of confidential data, unauthorized access to computer systems or networks and denial of computer system services to an authorized user. Offenses under the Florida Computer Crimes Act shall be investigated by the appropriate law enforcement agencies. Some offenses may require investigation by federal law enforcement agencies.

Claire S. Robinson
Associate Vice President
Resource Management and
Information Technology

Betty Castor
President

[USF World Wide Web Guidelines](#)

Copyright, University of South Florida, 1998

[SEARCHUSF](#)

[DIRECTORY](#)

[STATISTICS](#)

