UNIVERSITY OF SOUTH FLORIDA

POLICY

Number: 0-502
Title: Appropriate Use of Information Technology Resources
Responsible Office: Information Technology

Date of Origin: 2-23-95 **Date Last Amended:** 3-21-2023 **Date Last Reviewed**: 3-21-2023

I. PURPOSE & INTENT

The increasing reliance on information technology resources by the University of South Florida (USF) requires an environment in which these resources are used in a responsible and effective manner by everyone in the USF community. Such an environment will permit the most efficient and productive use of these resources.

The purpose of this policy is to establish guidelines for the appropriate and responsible use of information technology resources.

II. DEFINITION OF TERM

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

III. STATEMENT OF POLICY

The information technology resources of USF are a vital component of the teaching, research, and business environment of USF. It is the responsibility of all in the USF community to use these resources in a responsible, ethical, and lawful manner.

Any member of the USF 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 violations of state law.

Users are required to comply with state and federal laws, USF rules, regulations, policies and

terms of software license agreements.

All members of the USF community are responsible for all actions taken using any computer login ID assigned to them. These IDs and associated passwords are considered sensitive and confidential. Passwords issued to an individual to gain access to IT resources must be appropriately complex and must never be disclosed.

Authorized personnel connecting their personal computer to the USF network must abide by USF standards for information security, properly patched and with updated antivirus software. Registrants are responsible for ensuring that the personal computer is properly protected, and that the use of the computer does not infringe USF policies or standards of proper use, state, or federal law.

Copyrighted material 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 material is a violation of state law, and USF-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.
- Transmitting unsolicited material such as repetitive advertising, chain messages, or unofficial mass mailings, phone text messages (SMS), or instant messages (IM) in such a large volume that it tends to disrupt the proper functioning of university information technology resources or individuals' ability to use these resources.
- Transmission of emails or publishing of material that violates Federal or State Law or USF rules, regulations and policies including the Student Code of Conduct (examples include material that is illegal, threatening, harassing, or defamatory).
- Release of confidential, proprietary, or protected information, unless otherwise required by state or federal law.
- Attempts to masquerade as another user, hide your identity, or attempts to monitor

network traffic.

- Conducting oneself in a manner that results in academic restriction or expulsion from the University.

- Using autonomous computer technology to circumvent established university processes or manipulate the university's ability to fairly and equitably deliver IT services or assign IT resources.

The purpose of all IT resources owned by USF and made available to the USF community is to fulfill an academic or business need. Incidental personal use of IT resources including, but not limited to, copy machines, fax machines, telephones, computers, computer accounts, and email accounts, is only allowed when all the following conditions are met:

- The IT resource must be available for its designated USF business or academic use and the incidental use of the asset shall not impede USF business.

- The employee is required to meet his or her obligations in a timely and effective manner and the personal use of resources must not affect that obligation. Time spent by the employee on personal business shall not be considered to be USF work time.

- The use neither expresses nor implies sponsorship or endorsement by USF.

- The use must be consistent with state and federal laws, and USF policies and standards.

- Users must be aware that internal or external audit or other needs may require examination of uses of USF resources or services and should not expect such uses to be free from inspection.

Users should be aware that their use of USF computing resources is not completely private. Authorized USF officials do not routinely monitor individual usage of its computing resources; however, the normal operation and maintenance of USF's computing resources requires the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. USF may also specifically monitor the activity and accounts of individual users of USF computing resources, including individual login sessions and the content of individual communications, without notice, when:

- The user has voluntarily made them accessible to the public.

- It appears reasonable and necessary to do so to protect the integrity, security, or functionality of USF or other computing resources or to protect USF from liability.

- There is reasonable cause to believe that the user has violated or is violating this policy.

- An account appears to be engaged in unusual or unusually excessive activity; or
- It is otherwise required or permitted by law.

Any such monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to disruptions of network operations, must be authorized in advance by the appropriate Vice President or designee in consultation with the Office of the General Counsel.

IV. PROCESS STEPS

USF departments, units, and divisions 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 USF 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.

V. VIOLATIONS

Violations of this policy may lead to suspension of the user's computer account ID and/or disciplinary action (up to termination or expulsion) to be handled by Student Affairs, deans, or directors as appropriate. In addition, Chapter 815, Florida Statutes, the "Florida Computer Crimes Act," describes offenses which are crimes 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.

Date Approved: Jan. 23, 1995

Substantively Amended: (none)

Technically Amended: Mar. 21, 2023, Sept. 7, 2022, Jun. 11, 2021, Apr. 7, 2017, July 29, 2009, Oct. 8, 2008, Jun. 29, 2006

Biennial Review: Jan. 30, 2023

Other: Jul. 1, 2020 (Consolidation)