


UNIVERSITY OF SOUTH FLORIDA

Policies and Procedures Manual

	Subject of Policy Statement	Effective Date	Policy Number
	Information and Communication Security Program	Rev. 06/02/95	0-508

I. INTRODUCTION (Purpose and Intent)

Florida Statutes, Section 282.318 - 1984 "Security of Data and Information Technology Resources Act" requires each head of a department to be responsible for assuring an adequate level of security for all data information technology resources.

The State University System has issued a Standard Practice entitled "Security" in response to the security legislation. The Standard requires each University to establish an Information Security Manager (ISM). The ISM is required to perform a risk analysis and to certify compliance annually. Further activities include administering the security program, developing policies and procedures, implementing cost effective safeguards, ensuring periodic internal audits, including written security specifications in the solicitation of information and communication technology resources, and including a description of the existing security program and further plans for assuring the security of data and information technology resources as a part of the Information Resource Commission's planning process.

An information and communication security program is not just a mainframe computer issue. While mainframe computing will be a part of the program other items such as personnel, environment, utilities, purchasing practices, and public safety will also play a part. This program will apply at all University of South Florida locations and to information and systems when used remotely from the University of South Florida location.

The Security and Retention Subcommittee of the Committee on Administrative Computing Systems (CACS) will continue to be the group advising the University Information Security Officer. This group will follow up on the results of the Risk Analysis Survey and make recommendations. They will review the State University System's security Standard Practice and make recommendations for areas of action. Also, this group will work with other security interests on campus to recommend policies, procedures, and standards in this area.

To establish the basis for an information and communication security program, the Academic

Computing Committee (ACC) and the Committee for Administrative Computing Systems (CACS) recommended the following policy.

II. STATEMENT OF POLICY

It is the policy of the University of South Florida that all information utilized in the course of business and education is considered an asset, and as such, administration, faculty, staff, and students are responsible and accountable for its viability and protection. It is a management responsibility to maintain information security and integrity through administration of appropriate legal, auditable controls to protect University information from unauthorized, intentional or accidental disclosure, modification, destruction, denial, or misappropriation.

Information and communication security shall be the operational responsibility of the assigned representative within each college, division, or unit. The responsibility for developing and coordinating the security program shall ultimately rest with the University Information Security Manager.

Security standards shall be recommended by the Committee on Administrative Computing Systems (CACS) and the Academic Computing Committee (ACC) for the following categories: physical environment, data and software, physical access, logical access, personnel issues (as related to security), records management, and communication. These standards and the application thereof shall be in compliance with the laws of the State of Florida and subject to periodic audit by the established authority.

Laurey Stryker
Executive Director
Planning, Budget and Information Technology

Betty Castor
President

[USF World Wide Web Guidelines](#)

Copyright, University of South Florida, 1998

[SEARCHUSF](#)

[DIRECTORY](#)

[STATISTICS](#)

