


UNIVERSITY OF SOUTH FLORIDA

Policies and Procedures Manual

	Subject of Policy Statement	Effective Date	Policy Number
	Using and Protecting Microcomputing Resources	05/15/98	0-501

I. INTRODUCTION (Purpose and Intent)

The purpose of this policy is to define the basic set of procedures that colleges and departments shall establish and maintain for the management, use, and protection of their microcomputing resources. This policy applies to all Wide Area Networks (WANs), college and department Local Area Networks (LANs), college and department microcomputers and includes the hardware, software, and University data used in these environments. Microcomputers and LANs which are not connected to any larger network may differ somewhat in their protection requirements from those that are so connected.

In accordance with University Policy 0-508 (information and communication security program), each department, unit or division of the University is responsible for implementing procedures and controls for protecting University information. But the protection of the University's ability to conduct its business extends beyond basic procedures for handling, storing and disposing of information.

Advances in technology have enabled the implementation of a substantial number of microcomputer-based application systems by University colleges and departments. In some cases, these applications have become critical to the operation of the department and the University. It is essential, therefore, that adequate measures be used to protect the integrity and reliability of those microcomputing systems and the University data they process. Each college or department must ensure a level of protection not only appropriate for the microcomputers and LANs in its own environment but also with regard to the level of protection used for the larger campus networks of which they may be a part.

II. STATEMENT OF POLICY

Each college, department, unit or division of the University shall establish and maintain procedures which are adequate to protect the microcomputing resources under its management. These procedures shall include the following areas:

LAN Administration

Each LAN shall have a designated LAN administrator who is responsible for the operation, security, management, and user support functions for the LAN.

The LAN administrator shall ensure that all software residing on the LAN server has been properly purchased and licensed.

The LAN administrator shall be responsible for implementing procedures to protect the LAN from virus attacks and for removing a virus if one is found.

The scope of the privileges granted to the LAN administrator and the resulting high level of access to data may present serious exposures. Consequently, only regular position staff should be assigned duties as a LAN administrator.

LAN administrators shall carry out the college or department procedures for backup of its LAN data and software.

System and Data Access Controls

Each fully-authorized user of a LAN shall have a unique logon ID. Users who no longer have access shall have their logon IDs suspended or deleted in a timely manner. (See University Policy 0-511 for existing host procedures for removing access from transferring or terminating employees.) Any ID which is used to access a LAN, and which does not provide a unique user identification, shall have access only to specific restricted LAN resources.

Access control procedures shall be used to authenticate all users who access each LAN. Such controls shall include, at a minimum, a logon ID and a response mechanism (such as a password) for each user. The network operating system shall be configured to encourage a periodic expiration of all passwords as well as to establish a suitable minimum length for passwords.

Logon IDs which have supervisor or root privileges shall be highly secured. Such IDs shall be reserved for system management tasks and shall not be used as the IDs for normal day-to-day work by the users having these privileges.

Access rights and privileges for all authorized users shall be maintained and managed so as to secure access to data in a manner appropriate to the needs of the user and the value of the data.

Confidential data shall be protected against unauthorized access regardless of form, computing environment or location. Serious access control problems can be created when confidential University data is downloaded or otherwise transferred from a secure environment to a less secure environment.

Procedures shall be established for the management of data residing on the hard drives of any equipment

that is transferred or surplused. If equipment is transferred to another University department, then all University and department data shall be removed from the equipment hard drive prior to the transfer. Special care shall be taken to remove all data from the hard drive of equipment that is being surplused or donated.

At the time of termination of employment from a department or from the University, an employee shall certify as part of the department's termination processing that all University or department data has been removed from the employee's personally-owned home equipment.

Software Integrity

Appropriate procedures shall be established and documented for the management of microcomputer and LAN software. These procedures shall address the processes by which such software is acquired, installed, tested, documented, changed, and maintained.

All proprietary software installed on University equipment shall be administered in accordance with each individual software license agreement. Software that is surplused or donated must be removed from the equipment to which it is currently licensed. USF Policy 5-014, "Disposal of Surplus Property", provides further information regarding forms to be used for this purpose.

Procedures shall be established for the management of employee-owned software which is installed on University equipment. Employee-owned software must be removed from University equipment when the equipment is no longer being used by that employee, or upon that employee's termination of employment with the department or the University. Procedures shall be established to ensure that any employee-owned software installed on University equipment has been legally obtained by the employee. Departments and colleges shall retain the right to prohibit the installation of any employee-owned software on University equipment.

At the time of termination of employment from a department or from the University, an employee shall certify as part of the department's termination processing that all University or department software has been removed from the employee's personally-owned home equipment and that all original software diskettes or copies have been returned to the University.

Procedures shall be established for the management of proprietary software purchased for an employee's use in a telecommuting arrangement. The procedures shall ensure that the software is removed from any non-University equipment at the conclusion of the telecommuting arrangement or at the termination of the employee's employment with a department or with the University.

Software and File Backup

Effective backup procedures shall be maintained for the data and software residing on LAN servers. Full-volume backups, incremental backups and application-based backups shall be utilized on a regular basis

as appropriate to the college or department needs and to the value of the data. Procedures shall also address periodic testing to ensure the ability to successfully restore data from these backups.

Backups shall be stored on-site in a secured area which would not be subject to the same disruption of services as the LAN server area. All data considered mission-critical to the operation of the department shall also be maintained in an alternate backup location.

Business Resumption Planning

Recovery plans shall be developed and maintained for the restoration and continuation of critical services in the event of a significant disruption of normal microcomputer and LAN operations. These shall include plans for interim manual processing, as well as plans for resuming operations in an alternate location should that be necessary to maintain the mission-critical functions of the college or department. These plans shall address areas such as replacement of hardware and software, restoration of data, relocation of personnel and so on, as appropriate to the needs of the college or department.

Training

Programs shall be developed and maintained for training employees in the proper use and protection of microcomputing resources. Appropriate training areas should include logon ID and password management, detection and prevention of viruses, backup procedures for client data, proper uses of proprietary software, LAN administrator training and general security awareness. Programs shall also include the provision and availability of appropriate hardware and software reference materials for employees.

Equipment Protection

Procedures shall be developed and maintained for protecting microcomputer equipment and components from theft and physical damage. Equipment shall be located only in areas that have sufficient physical access controls; file servers, in particular, shall be in a secure area with access permitted only by authorized persons. Protective measures shall include power surge protection, fire or smoke detection, alarm systems and other devices as appropriate.

III. PROCEDURES

Deans, Directors and Department Chairpersons shall be responsible for implementing the provisions of this policy in their respective areas.

Laurey T. Stryker
Vice President

**Budgets, Human Resources, and
Information Technology**

**Betty Castor
President**

[USF World Wide Web Guidelines](#)

Copyright, University of South Florida, 1998

[SEARCHUSF](#)

[DIRECTORY](#)

[STATISTICS](#)

