I. INTRODUCTION  (Purpose and Intent)

Advances in technology have enabled the implementation of a substantial number of computer-based application systems by the University of South Florida System (USF System) campuses, colleges, departments and entities. In some cases, these applications have become critical to the operation of the organization and the USF System. It is essential, therefore, that adequate measures be used to protect the integrity and reliability of those computing systems and the USF System data they process.

The purpose of this policy is to help USF System units maintain the confidentiality, integrity, and availability of their information technology resources by establishing a basic set of minimum standards for management, use, and protection.

II. DEFINITIONS

Information technology (IT) resources shall be interpreted to include all USF System 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 the USF System.

A USF System Unit consists of any College, Department, Research Center, Institute, Direct Support Organization, or other administrative subdivisions that are connected to the University of South Florida System network.
III. SCOPE

This policy applies to all IT resources, persons and entities connected to the USF System network and include the hardware, software, and USF System data used in these environments, except for specific entities who operate under additional federal regulations that would not normally be applicable to an educational environment. These areas may include clinical healthcare or clinical research, where federal regulation mandates an even more stringent and different security structure. Even in these cases, reasonable efforts should be made to follow the spirit of USF System policy.

IV. STATEMENT OF POLICY

• INITIATIVE

All USF System information security policies, standards, guidelines and practices shall be coordinated through the Office of Information Security and shall be consistent with a USF System-wide approach in developing, implementing and managing data, system, and network security.

The protection of the USF System's ability to conduct its business extends beyond basic procedures for handling, storing and disposing of information. Each USF System unit must ensure a level of protection not only appropriate for the computers and networks in its own environment but also with regard to the level of protection used for the larger campus networks of which they are a part.
The University of South Florida is a System of higher education composed of multiple campuses and separately accredited institutions located in Tampa, St. Petersburg and Sarasota-Manatee. Regional campuses and separately accredited institutions may have unique characteristics. Students, faculty and staff must check with their individual campuses and apply System-wide policies in conjunction and consistent with the specific characteristics and guidelines applicable to those campuses. Notwithstanding, this policy is intended to set minimum guidelines for the entire USF System. Regional campuses, separately accredited institutions and administrative offices may not adopt less restrictive standards than the ones outlined in this policy. The CTO or equivalent head of IT department in each campus shall be responsible for initiating the implementation of the provisions of this Policy in his or her respective area.

In accordance with USF System Policy 0-508 (University Information Security Structure), the head of each USF System unit shall be responsible for initiating the implementation of the provisions of this policy in his or her respective areas. These procedures shall include the following areas:

A. Management and Access Controls

Each IT resource shall have a designee who is responsible for its security and management. The designee will be responsible for following and implementing standards and guidelines for system management as established and maintained by the Information Security Workgroup (ISW), as defined in USF System Policy 0-508, and published on the USF System Security Website, http://www.usf.edu/it/about-us/policies-and-standards.aspx
According to USF System Policy 0-515, Protection of Electronic Personal Information, access to Personal Identifiable Information (PII) shall be granted only when required by official USF System business. When granted, access shall be closely monitored by the data owners, data custodians and the Office of Information Security, following the standards established by USF Policy 0-515 and supplemental standards and guidelines posted on the USF System Security website. Access reviews should be done at least annually to verify that owners/supervisors validate the user level of access and the changes effected.

Each authorized user of a system shall have a unique login ID. Any ID which is used to access a system, and which does not provide a unique user identification, shall have access only to specific restricted system resources.

Access to services and/or resources will be suspended, and the appropriate account deleted when there is no longer a business or academic need for access. Employees are required to remove any personal data from USF computer systems prior to their last day at USF. The deprovisioning of the account will be performed in a manner proportionate to the level of risk posed by such access, including immediate suspension of access and privileges and deletion of the account if necessary.

It is the responsibility of each user to understand the retention requirements put
upon the data they store on IT systems by State and Federal Law. In case of employee termination, that responsibility falls upon the department and the user's supervisor. Information Technology will, upon an employee’s termination and departmental request, duplicate files stored in network drives on to another network share and make these files available to the new departmental data owner. By default, IT will keep email, calendar, and network share files for a period of one (1) year, at the end of which the files will be purged from the system.

Access control procedures shall be used to authenticate all users who access each system. Such controls shall include, at a minimum, a login ID and a response mechanism (such as a password) for each user. All user accounts shall be required to change passwords periodically. The frequency should be determined by the enforced length and complexity of the password combined with the sensitivity of the information data protected, in accordance with industry standards and guidelines published in the security website.

Login IDs which have with 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 routine system access.

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.

Information Security Administrators (ISAs), as defined by USF System Policy 0-508, shall ensure that other administrators are sufficiently trained and that the nature of their appointment (student, OPS, etc.) does not present an unacceptable risk to the USF System.

B. Software Management

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

Where justifiable and when it benefits the University, procedures shall be established and maintained to allow for the installation of employee legally-owned software. Employee-owned software must be removed from USF System equipment when the equipment is no longer being used by that employee, or upon that employee's termination of employment with the unit or the USF System. Procedures shall be established to ensure that any employee-owned software installed on USF System equipment has been legally obtained by the employee.
At the time of termination of employment from a unit or from the USF System, the employee being terminated shall certify as part of the unit's termination processing that all USF System software has been removed from the employee's personally-owned home equipment and that all original software media or copies have been returned to the USF System.

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 USF licensed software shall be removed from any non-USF System equipment at the conclusion of the telecommuting arrangement or at the termination of employment with a unit or with the USF System.

C. Data Backup

System Administrators shall carry out the procedures for backup of systems data and software. Effective backup procedures shall be maintained for the data and software residing on systems according to the ISW standards. Procedures shall also address periodic testing to ensure the ability to successfully restore data from these backups. Backup systems shall not be used as archiving for record retention purposes. The goal of these systems is to protect USF System data, allowing recovery in the case of a disaster.

Backups shall be stored in a secured area that would not be subject to the same disruption of services as the location where the system is located. Backups of
data considered mission-critical to the operation of the unit shall also be maintained in an alternate location. USF System units using backup services must ensure that appropriate measures are taken to preserve the confidentiality of the data as specified by industry standards and the standards published on the Security Website, http://it.usf.edu/standards/security.

Users are not authorized to back up USF Institutional Data to cloud services other than the ones specifically approved by the ITMC. Data stored on not-approved cloud services are outside the control of Information Technology and may provide the means for the leakage of restricted USF Institutional Data. Nevertheless, all restricted information stored on an approved cloud service must be encrypted prior to storage.

D. 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 computer and system 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 unit. These plans shall address areas such as a replacement of hardware and software, restoration of data, relocation of personnel and so on, as appropriate to the needs of the unit.
E. Awareness and Training

A robust and enterprise wide awareness and training program is paramount to understanding IT security responsibilities, organizational policies, and how to properly use and protect the entrusted IT resources in a proper manner. The program shall ensure that all individuals are appropriately trained in how to fulfill their security responsibilities. Such training shall provide employees with the rules of the system and apprise them of available assistance, security products, and techniques. Behavior consistent with the rules of the system and periodic re-training shall be required for continued access to the University systems.

F. Physical Security

Procedures shall be developed and maintained for protecting computer equipment and components from theft and physical damage. Equipment shall be located only in areas that have sufficient physical access controls and are already properly conditioned; critical servers, in particular, shall be in a secure area designated by IT as a Data Center, with access permitted only by authorized persons. Due to the duties they perform it may be necessary to house servers related to network operations outside the Data Center. The Infrastructure group will take steps to protect these servers from physical threats as much as possible. Protective measures shall include power surge protection, fire or smoke detection, alarm systems, air conditioning, humidity control, and other devices as appropriate.
G. Network Connection

Connection to the USF System network is a privilege and all persons and USF System Units connecting to it must comply with USF System standards, published on the Security Website http://it.usf.edu/standards/security http://security.usf.edu, and USF System Policies and Regulations. Failure to comply can result in disconnection from the network or removal of services at the direction of the Information Security Manager (ISM) or Information Security Officer (ISO), as outlined in USF System Policy 0-508.

H. Media Disposal

Procedures shall be established for the management of data residing on storage media that are transferred, surplused, or disposed of otherwise. If equipment is transferred to another USF System unit, then all USF System data shall be removed from the storage media prior to the transfer. Special care shall be taken to remove all confidential data from storage media that are being surplused, donated, or disposed of otherwise. Further guidance can be found in the USF System Security Website.

I. Risk Assessment

Risk assessments shall be conducted on a basis consistent with system criticality. A risk assessment will be performed by local systems administrators on a not less
than yearly basis. The ISW will be responsible for conducting a continuous, USF System-wide risk assessment program as outlined in Policy 0-508.

V. ENFORCEMENT OF POLICY

All USF System students, staff and faculty and employees shall comply with this policy, including all future information security policies and standards.

Compliance with the USF System’s information security policy and procedures shall be monitored regularly. USF’s Incident Response Team (IRT) is responsible for the initial evaluation of security threats found in the USF System and are authorized to take appropriate action, up to and including removal of the network access for that threat system. Members of the IRT, as outlined on USF System Policy 0-508, shall use Office of Information Security (OIS) approved guidelines approved by the Office of Information Security (OIS) to help determine the threat level and the appropriate action.

Individual user violations of any policy or standard published by the OIS may be subject to disciplinary or corrective actions based upon the policies, rules, regulations and procedures of the University of South Florida System. These actions may include sanctions including, but not limited to, revocation of the employee or student privileges up to and including termination of employment or expulsion. Certain violations, misuse, or disclosures of confidential information may include civil and/or criminal penalties.

Authorized and signed by:
Michael Pearce, Vice President, Information Technology
Judy Genshaft, President