I. **INTRODUCTION** (Purpose and Intent)

It is the policy of the University of South Florida System (University/USF) that all information utilized in the course of business, research, and education is considered an asset, and as such, administration, faculty, staff, and students are responsible and accountable for its viability and protection. Under various federal and state laws, it is the University’s responsibility to maintain security and integrity of confidential information that is transmitted, stored or maintained using information technology resources through the appropriate legal, auditable controls that will protect the information from unauthorized access, intentional or accidental disclosure, modification, destruction, denial of service, or misappropriation of data or hardware.

The purpose of this policy is to define the overall information security structure which will insure the confidentiality, availability, and integrity of all critical University data and information systems. Components of that structure may be found by reference to individual University organizational units. Due to the continued proliferation and distribution of computing and information systems across the entire University, an effective structure must be distributed and a consistent program for addressing security is required.

This policy establishes the organizational structure and processes applicable to the University of South Florida System to ensure compliance with applicable federal and state laws regarding the security and confidentiality of information that is transmitted, stored, maintained; or otherwise utilized information technology resources.
II. SCOPE
This policy will apply at all University of South Florida System locations and to information and systems when used remotely from University locations.

III. STATEMENT OF POLICY

A. Information Security Manager (ISM)
The Information Security Manager is responsible for University-wide efforts related to data and information system security, such as development of USF data security policies, negotiation and evaluation of site licenses for security-related software, training, coordination of efforts to improve data security controls, and dissemination of security-related information and incidents, which could affect the availability, and integrity of computing resources on campus.

When security issues with a particular University computing resource arise in such manner that threaten the integrity and availability of the University computing infrastructure, the ISM, under advice of the other members of the Incident Response Team, has the authority and responsibility to isolate the offending computing resource until the issue has been resolved.

The ISM will maintain communications with the Information Security Officers and Administrators, regularly educating and updating them on information security issues that may need to be addressed.

B. Information Security Workgroup (ISW)
The Information Security Workgroup is the steering committee responsible for recommending policies and assisting in the overall coordination of the University information security program. It will advise the Information Security Manager on the development and maintenance of standards and guidelines that will direct the Information Security Officers in their role. The Information Security Workgroup will also assist the Information Security Manager on evaluating risk analysis surveys completed by individual University units.

The ISW is responsible for incorporating methods for a systematic, University-wide, risk assessment framework through which appropriate changes in policy, standards, and guidelines will be implemented and enforced. This framework will be continuously re-evaluated to respond to developing information security issues. The results of this risk assessment will be submitted to the Information Technology Management Council (ITMC) with enough supporting information to allow the ITMC to make a decision on the acceptable level of risk for the University.
The Information Security Workgroup will be chaired by the Information Security Manager. Its membership will be reviewed and updated as appropriate and published in the USF Security Website, [http://www.usf.edu/it/services/data-security.aspx](http://www.usf.edu/it/services/data-security.aspx).

C. Incident Response Team (IRT)

The primary goal of the Incident Response Team is to protect the overall computing infrastructure of the University. The team is responsible for quickly identifying threats to the campus data infrastructure, assess the level of risk, and immediately take steps to mitigate the risks considered critical and harmful to the integrity of University information system resources. IRT members will notify local Information Security Officers and Administrators of any incident involving their resources.

Members of the Incident Response Team should be notified as soon as an incident is detected within the University. After control is restored, a report must be presented to all members of the IRT and local administration, clearly outlining the extent of the breach, and the steps taken to avoid future incidents. These incidents will be reviewed by the ISM as part of the continuous risk assessment program.

Members of the IRT will perform localized vulnerability assessment as needed and report their findings to the appropriate local Information Security Officer and Information Security Administrator. IRT members will also conduct University-wide vulnerability assessments during emergency situations, in order to protect the integrity and availability of the University infrastructure, and take actions as deemed appropriate.

The Incident Response Team (IRT) will be composed of the Information Security Manager and key members of the campus network administration and security staff.

D. Information Security Officer (ISO)

It is the responsibility of the head of each department, unit, and division of the University to appoint an Information Security Officer (ISO). Each ISO will have oversight responsibly in their respective area for insuring that information security practices are followed. Current personnel may be designated as an ISO, with the duties and responsibilities becoming an additional part of that person’s job.
The ISO must understand the importance of security, be capable of learning security basics, and most notably, have the authority to carry out the responsibilities assigned. Additional responsibilities include:

1. Adherence to University policies and standards.
2. Ensuring that information security requirements are met for their organizational area including the performance of continuous risk analysis and business resumption planning in the event of technology failure.
3. Help to promote security awareness in their organizational area.
4. Advising administration of security shortfalls.

E. Information Security Administrator (ISA)

Technical members of the local computer and network support personnel who also have security-related duties are designated Information Security Administrators (ISA). The ISO may also hold the designation of ISA. The ISAs are responsible for the establishment and maintenance of security for computing systems and networks. The ISO should identify the local Information Security Administrators and coordinate their roles and responsibilities with respect to information security. The Information Security Workgroup will provide assistance in educating the ISOs and ISAs with the standards and guidelines of the University.

In accordance with University Policy 0-501 (Using and Protecting Information Technology Resources) separate personnel may be responsible for the administration of systems. Under this policy those persons shall be designated as System Administrators. System Administrators will follow the University’s standards and guidelines for system administration and will be monitored by the Information Security Administrators to insure compliance with security procedures.

*Current Responsible Office: Information Technology*

*Refer to the appropriate Responsible Office website for a current name of the Vice President or other Responsible Officer.*