INTRODUCTION (Purpose and Intent)

The USF IT Network Security Plan establishes guidelines for IT practices used on a day to day basis to provide a secure and robust computing environment. These practices are used to protect the mission, operation, and reputation of the USF System and its information systems.

These guidelines supplement the Official USF System Security Policies, Standards, and Procedures that have been established for the USF System. They are intended to comply with the regulations and policies set down by the State of Florida, the University of South Florida, and the Federal Information Security Management Act (FISMA).
3 SCOPE

These standards and procedures apply to all information systems and resources under the control of USF, including all computers connecting to the USF network and all USF System employees, faculty, students, contractors, and any other individuals who use and administer those systems and computers, particularly those involved with information system management.

4 STANDARD PROVISIONS

USF IT manages risk by identifying, evaluating, controlling, and mitigating vulnerabilities that are a potential threat to the data and information systems under its control.

User accounts and passwords are implemented to maintain individual accountability for network resource usage. Any user who obtains an account and password for accessing a University provided resource is required to keep these credentials confidential. Users of these systems may only use the accounts and passwords for which they have been assigned and authorized to use, and are prohibited from using the network to access these systems through any other means. This plan also prohibits the sharing of personal user accounts or passwords for accessing University or Internet computing resources. In the interest of maintaining account security, passwords are changed on a regular schedule or anytime the integrity of the account is in question.

USF IT network or computing resources may not be used for commercial purposes, for personal profit or to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of University resources for any illegal activity may result in loss of network access privileges, official reprimand, suspension or dismissal. USF cooperates with any legitimate law enforcement agency or inquiry in the investigation and prosecution of any alleged wrongful activity.

The University’s network or Internet facilities may not be used to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

University owned networking and communications equipment, may only be moved by Network and Computing Support staff, or authorized agents.

Reconfiguration of network hardware or software, except by designated individuals within IT, is strictly prohibited.

Before connecting any server, network communication or monitoring device to the University Network, approval must be obtained from Data Center Communications.

Attachment of any the following devices to the campus network, other than those provided or approved by Network and Computing Support, is strictly prohibited:

a. DHCP servers.
b. DNS servers.
c. NAT routers.
d. Network Gateways.
e. Packet-capturing or network monitoring devices.
f. Any device that disrupts or negatively impacts network operations.

5 STATEMENT OF PROCEDURES

The procedures for conducting a risk assessment and for the control and mitigation of risks to the USF Health information systems include:

5.1 NETWORK CONTROL

USF IT has software and systems in place that have the ability to monitor and record network, Internet and computer system usage. These systems include monitoring and security systems that are capable of recording network traffic, including traffic to World Wide Web sites, chat rooms, newsgroups and e-mail messages, file servers, telnet sessions and file transfers into and out of our internal networks. This capability is necessary to maintain the health of USF network operations and diagnose network related problems. USF IT reserves the right to perform network monitoring at any time. The information collected may be used by technicians and management to assess network utilization and trends, and may also be provided to upper management or other authorities as evidence as part of any investigation of alleged policy violations.

USF IT reserves the right to perform periodic port scans, segment sweeps, and vulnerability scans on all network segments.

Network operations, functions, and resources, which are not required as part of the normal and approved job duties or projects at the University, may be bandwidth limited or blocked by network control devices to protect the integrity and availability of the overall system.

USF IT may suspend network access to any location or system that disrupts normal network operations or systems that violate university policy. In this event, an attempt is made to contact the responsible individual to resolve the problem.

5.2 DHCP SERVICES

USF IT provides centralized and redundant DHCP and DNS services for the University. Due to the nature of these services, and because of the potential disruption of service and possible security breaches resulting from the incorrect setup of additional systems, attachment of unauthorized DHCP or DNS servers is prohibited. The following guidelines must be followed when requesting or using any DHCP or DNS services:

- Systems requiring an IP address must support DHCP and be capable of obtaining DHCP address information from one of the centrally administered University DHCP servers.
- Using DHCP, devices requesting an IP address are assigned a dynamic pool address from the subnet to which the device is attached. Devices with dynamically assigned IP addresses may have their address change.
- Static IP addresses, needed for server-class computers or dedicated instruments, must be requested from the Data Center Communications Team the Help Desk ticket.

5.3 DNS SERVICES
User workstations, which have been assigned a dynamic pool IP address, have an associated DNS name allocated by the network.

Any DNS name or domain name that is to be associated with the USF Network must be requested from and registered with Web Services. DNS names ending in usf.edu are made available upon request for University approved services.

Requests for assignment of DNS names must be for valid University related purposes.

DNS names for domains other than usf.edu, and which are to be hosted on University systems, must be requested from Web Services. Any charges for initial or ongoing registration of the requested name are the responsibility of the requestor. DNS names, not in the usf.edu domain, are handled on a case by case basis.

USF IT works with any user requesting a domain name to identify an appropriate and available name. However, USF IT has final approval for all DNS name assignments.

5.4 Wireless Network Services
Because wireless networks can be used to provide access to the same resources and services as wired network systems, the same basic procedures that are used in a wired network environment can also be applied in a wireless network environment. However, due to the nature of wireless networks, additional security, and control mechanisms are needed to maintain the security, operation, and interoperability of both traditional and wireless systems.

Wireless routers are not allowed on the USF network unless they have been approved by USF IT.

Access to the USF Wireless network is limited to individuals who have a USF account except in locations where the guest network is available.

The USF Guest Network is segregated from the internal servers and resources used by authenticated users to keep the network secure. The USF Guest Network is only available in approved areas and require a request to be expanded into any other areas. Users of the USF Guest Network are required to provide a valid cell phone number to authenticate.

5.5 Destruction and Disposal of Information and Devices
Restricted information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons.

When donating, selling, transferring, surplus or disposing of computers or removable media (such as DVDs), the proper procedures to make data unreadable on those media are taken. Acceptable procedures are listed on ISSP-009, “Medial Disposal.”
5.6 NETWORK ACCESS
Anyone who uses the campus computing environment must have appropriate status (e.g. staff, faculty and current students) and must be properly authenticated when required.

Access is provided to vendors and or other university partners through the sponsored VIP account process, as described on http://www.usf.edu/it/services/vip.aspx.

VIP accounts are reviewed and renewed at six-month intervals to see if access is still needed.

When an employee leaves the organization accounts is disabled as soon as the GEMS status is updated, and individual departments must approve re-activation of account access.

5.7 USER COMPUTING DEVICES
Users are responsible for the security and integrity of University information stored on their workstation, which includes controlling physical and network access to the equipment.

Users may not run or otherwise configure software or hardware that may allow access by unauthorized users.

Anti-virus software must be installed on all workstations that connect to the USF Network.

University Computers may not be used to copy, distribute, share, download, or upload any copyrighted material without the permission of the copyright owner.

5.8 PHYSICAL ACCESS
Access to USF IT Data Center should be restricted to those responsible for operation and maintenance. Access by non-IT personnel is not permitted unless they are escorted by an authorized IT staff member.

Computer installations should provide reasonable security measures to protect the computer system against natural disasters, accidents, loss or fluctuation of electrical power, and sabotage.

Networking and computing hardware are placed in secure and appropriately cooled areas for data integrity and security.

5.9 ACCESS TO RESTRICTED RESEARCH DATA
Access to Restricted Research Data, such as data containing PHI or Export Controlled data, is directly linked to the user’s official participation in a Research project. The Primary Investigator must notify the USF Information Security Team in the event immediately as soon as a member of the research team is removed from the (voluntarily or through other action). The Office of Information Security ensures the appropriate removal of the former member’s access to the data.
5.10 NETWORK HARDWARE
Network hardware is housed behind a locked door to protect physical access to switches and other network hardware. Access is only allowed with the use of card access or with a checked out key.

All switches and network hardware are password protected at a minimum via a local account setup on the device itself; these passwords are changed according to the published password management standards and also as administrators leave the organization.

Subnets allowed to authenticate with switch management will be restricted, to create tighter control of backend administration.

Exec level access Timeouts implemented on Console and VTY lines so that any idle sessions are terminated automatically.

All switches are time synced using NTP so that incidents can be tracked and correlated to the proper timeframe.

5.11 SERVER ENVIRONMENTS
All servers are subject to a security audit and evaluation before they are placed into production.

Administrative access to servers must be password protected and use two-factor authentication whenever possible.

Servers should be physically located in an access-controlled environment.

All internal servers deployed at USF must be owned by an operational group that is responsible for system administration.

Servers must be registered with the IT department. At a minimum, the following information is required to identify the point of contact:

- a. Server owner contact(s) and location.
- b. Hardware and Operating System/Version
- c. Main functions and applications
- d. MAC address (If not a virtual server)

Services and applications that no longer in operation must be disabled where practical.

Access to services should be logged and protected through access control methods to the extent possible.

The most recent security patches must be installed on the system as soon as practical.

Do not use administrator or root access when a non-privileged account can be used.

Privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
6 EXCEPTIONS

All requests for exceptions to these standards and procedures are handled upon request, and follow these guidelines:

- Must be submitted in writing to and approved by the CIO or with the proper authority.
- Reviewed on a case by case basis.

7 RELATED INFORMATION

USF Security – Procedures & Standards – the standards and procedures that are to be used for all information systems and computers connecting to the usf.edu domain and by all personnel who use and administer those systems and computers.