GEORGIA SOUTHERN UNIVERSITY

OFFICE OF THE VICE PRESIDENT FOR INFORMATION TECHNOLOGY
POST OFFICE BOX 8122
STATESBORO, GEORGIA 30460-8122
TELEPHONE (912) 478-1294
FAX (912) 478-7720

WORKSTATION MANAGEMENT STANDARD PROCEDURES

I. Authorization

These standards and procedures are developed in accordance with the Workstation Management Policy. Authority of enforcement of these standards and procedures is delegated by the Chief Information Officer to the Chief Security Officer (CSO) and the ITS Director of Technical Services.

II. Authorized Equipment

It is important to know and control what equipment is attached to the University network. Some equipment can be harmful to the operation of this resource causing potential disruptions to critical services, instruction or research.

a. Only equipment and systems that are approved by the CIO or his/her designee will be allowed to connect to the University network.

III. Authentication

Ensuring the authentic use of computing resources is an essential element of the University's security plan and is necessary for compliance with University System of Georgia Computer Use Policy.

a. All workstations must employ, according to the University IT Security Standard, a mechanism to authenticate the person who is using the computer.

b. User credentials shall be authenticated against authorized sources and mechanisms.

IV. Communication

Good communication is the foundation of excellent service. Notifying people about planned events or recent service calls is essential professional courtesy and an operational requirement.

a. Users of laboratory, classroom and community-use workstations affected by workstation management tasks should be appropriately notified at least one business day prior to the planned service activities. Ideally, planned changes should be communicated 10 business days in advance of the activity.

b. When accessing a computer workstation assigned to the personal use of an individual:
   i. Notification must be provided in advance of any service to the individual user.

   ii. Where individual machines are involved, reboots must be negotiated with the user.

c. If any service is in response to an urgent order by the CIO or his/her designee, or is in response to an eminent security threat, the service may be performed without notification. However, the affected person(s) must be notified about the service as

soon as possible thereafter.

V. Performing Technical Services

The maintenance of the University's computer resources often requires the services of authorized technicians.

a. **Personal Equipment**

Under no circumstances will the University be held liable for damage to hardware or software, or loss of data on privately owned equipment. The owners of such equipment shall sign an acknowledgment and hold harmless agreement on a form approved by the Office of Legal Affairs prior to any such assistance being provided. Reference the "Registration of Privately Owned Equipment Standard" for more information.

b. Automatic Updates

It is important that computer workstations have the latest approved security patches and bug fixes applied in a timely manner. Automatic updates provide an efficient and non-invasive means of ensuring that computers have these necessary updates.

i. All computer workstations will employ an approved mechanism to acquire and automatically install updates. This includes the Operating System updates and Antivirus updates.

c. **Remote Access and Assistance**

The ability to provide remote assistance to persons is efficient and effective. Technology allows a person to share a view of their desktop and transfer control to a remote technician to resolve problems, provide training, and install software and numerous other tasks that would otherwise be performed in person.

i. Only technicians authorized by the CSO or his designee(s) will be allowed to provide remote access and assistance.

ii. Only applications approved by the CSO are to be used for remotely accessing or assisting users.

iii. Remote access and assistance can only be conducted with the <u>explicit</u> permission of the user to which the computer workstation is assigned.

iv. There is to be no monitoring or collection of data concerning computer use, data files, cookies or other personal data without <u>explicit</u> permission of the workstation computer owner or unless otherwise directed by the CSO.

d. **Wake on LAN Capability**

The ability to start a computer remotely allows for effective and efficient management of computer resources.

i. Authorized technicians may utilize wake on LAN capability to provide services as long as the policy guidelines for communication are followed and authorized mechanisms are used.

VI. **Workstation naming**

A consistently applied naming convention is essential to asset management.

a. Computers will follow the institutional computer naming convention as established by the CIO or his/her designee. Reference the IT Security Standards for more information.

VII. Security

Secured workstations help maintain an environment that protects users and data that is used in the work environment.

a. Computers must be configured according to the Workstations – Non-Lab Environments, Personal and Transient Workstations section in the University's IT Security Standards.

b. Computers must be configured according to the university Workstation policy settings template, at a minimum. For more information see the University's IT Security Standards.

VIII. Workstation Management Software

Workstation management software can greatly improve the efficiency, effectiveness and timeliness of technical services. It can significantly decrease the response time to counter-act malware or virus attacks and preserve the availability of computing resources.

a. Every University owned computer workstation shall utilize workstation management software.

b. Only approved workstation management software is to be used to manage workstations.

c. Reference the IT Security Standards for authorized software

IX. Campus Standard Configurations

Providing consistent configurations for all computers on campus ensures the portability of knowledge, policy and technical resources throughout the institution. It also serves to extend the essential and required elements to every computer owned by the institution.

a. ITS will maintain a list of standard software.

b. ITS will provide base-line configurations of standard software for installation on faculty, staff and student use computers.

c. Additional software packages may be installed on computers provided the software is properly licensed.

d. Departments will maintain documentation on any additions or modifications deployed to workstations and the licenses to use such software.

X. Asset Management/Inventory

Knowing the presence of both hardware and software assets is essential for the university to maintain compliance with USG policies and State regulations.

a. The University will utilize information about installed applications inventoried from computers to manage software and hardware assets.

b. Each workstation will be configured and enabled with the ability for hardware and installed software inventory on each system.

c. Annually, an inventory of all computer devices on the network and the applications installed on them will be provided to the Chief Security Officer, the University Auditor and Property Control. Reports derived from the approved workstation management software will suffice as a physical inventory audit if the workstation information has been updated in the past 90 days.

d. Technicians that use manual and/or automated processes for asset management and inventory must respect the privacy of data, files, cookies and any information in addition to system configuration hardware and software installed.

XI. Workstation Backup

It is essential that every user have the means to backup and restore university owned data files and information stored on a computer workstation assigned to their use. There are several means and techniques available depending on the nature and volume of this data. Examples of appropriate backup methods include, but are not limited to:

a. Campus Network Storage
b. DVD/CD
c. Encrypted USB flash drives

Every computer workstation will have a means of copying and restoring data in the event of accidental or catastrophic loss.

XII. Related Documents

University IT policies are available at:
http://www.georgiasouthern.edu/policies/
USG Security Policies are available at:
http://www.usg.edu/infosec/policy_management/policies/

XIII. Definitions

Workstations include: laptops, desktops, PDAs and other computers and devices accessing the Georgia Southern University network.

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of Georgia Southern University.

CIO is the Chief Information Officer. This person is responsible for the information technology and computer systems that support the University.

CSO is the Chief Security Officer. This person is responsible for oversight of all the security constructs and computer use policies of the University.

LAN is the campus local area network. It includes any device that has or uses a Georgia Southern IP address.

XIV. Revision History

Original: October 15, 2009

Revisied: March 8, 2011. Updated Section X.c. and delegate to Technical Services Director.

XV. Approval

President's Cabinet on October 15, 2009