GEORGIA SOUTHERN UNIVERSITY

Workstation Security Standards

Area: Information Technology Services	Number:	
Subject: Workstation Management	Issued:	8/1/2012
Applies To: University	Revised:	
Sources:	Updated:	
	Reviewed:	
Responsible Party: Vice President for Information Technology	Page(s):	Page **1** of **5**

I. Purpose

Overview

Improperly configured computer systems can be compromised and have their data destroyed or stolen; used to store illegal data; relay spam e-mail; or attack other systems. Departments are responsible for maintaining secure workstations.

Scope

Included are all workstations that connect to the Georgia Southern University network (GSNet), wired or wireless, including but not limited to faculty, staff, students, vendors, contractors, and/or guests.

II. Policy Statement

Standard

This section lists items that are required and/or recommended for all workstations at Georgia Southern University.

1. **WORKSTATION CONFIGURATION**

   All workstations must, to the extent possible for the operating system (OS), application, and function, be configured in a way that reduces the risk to the system. Actual techniques vary according the hardware and operating system, but minimally include:

   a. Physically securing the workstation and console operations;
   b. Prompt patching and/or upgrading of vulnerable applications and services;
   c. Eliminating unnecessary services;
   d. Eliminating programs or services which cause unnecessary security risks or are not used;
   e. Managing file permissions;
   f. Establishing restrictions on user accounts and access;
   g. Password protecting the BIOS;
   h. Preventing autoboot from USB/CD/DVD;

i. Utilizing a host based firewall.

2. **ACCESS CONTROL**
   a. Local user account passwords must conform to the established university password standard, which includes password complexity and account lockout configurations.
   b. Workstations must be configured in a manner to require interactive user authentication instead of an automatic login where the password is stored on the workstation.
   c. Avoid storing passwords or shadow files on the workstation. If passwords are stored locally then they must be encrypted.
   d. Workstations must have password-protected screen savers, which automatically lock the workstation after a period of inactivity. An automatic screen saver workstation lock should be set to 15 minutes or less, exceptions must be approved by the CIO.
      i. An exception is hereby granted for workstations in smart classrooms or special use educational facilities where computer is used expressly for faculty presentation.
   e. Administrator accounts must be re-named.

3. **SHARED RESOURCES**
   a. Except for public Information Technology (IT) resources, all shared resources (e.g., mapped folders, drives, and devices) must have permissions set to allow only those individual accounts or groups that require access to that resource.
   b. Sharing resources from a workstation is strongly discouraged when other services are available for file sharing.

4. **PATCH MANAGEMENT**
   a. The university's centralized patch management system for Windows machines must be used.
   b. If centralized patch management service is not available, regularly scheduled manual or automated vendor updates must be implemented.
   c. The department is responsible for ensuring necessary patches are applied as soon as possible, as well as accelerated patch deployment if the Chief Information Security Officer (CISO) elevates the threat level.

5. **OS AND APPLICATION MAINTENANCE**
   a. Operating systems and applications must be maintained by the department at the most recent stable and institutionally-supported version that is compatible with the system's hardware and function, and critical security patches must be applied.
   b. Systems with operating systems or applications that cannot be upgraded due to hardware or functional restrictions must be removed from network access or replaced with newer systems. In cases where an older OS or application is required due to hardware or functional restrictions, measures must be taken to limit access to the system (via host- based firewall, router access control, internal limitation of

available services, or other measures) in order to reduce the exploitation risk of older vulnerabilities that cannot be mitigated.

6. **SYSTEM LOGGING**
    a. Operating system event logging must be enabled for security events such as failed and successful logins, and unauthorized connections for any commonly used service.
    b. Applications on workstations which manage confidential high-risk information must implement event logging to record unauthorized access attempts and, if possible, to track configuration changes.
    c. The log should be configured to retain those events for at least 30 days.

7. **SYSTEM MONITORING**
    a. Per HIPAA regulations, all departments who manage PHI (protected health information) are required to implement procedures to regularly review logs to ensure access is authorized and information integrity is protected.

8. **WORKSTATIONS WITH MULTIPLE USERS**
    a. All user accounts must be uniquely identified and must require authentication.
    b. Account creation and authorization processes must be based on the principle of least privilege, with access to systems granted only to those who require it on a need-to-know basis.
    c. A user’s access authorization shall be appropriately modified or removed when the user’s employment or job responsibility within the institution changes.
    d. Procedures must be in place for emergency termination of all domain, local, or other application user accounts.
    e. User accounts must be individually assigned and maintained except in cases where an application, hardware, or function requires that a single common account be used.
    f. Unused local accounts must be managed in a timely manner to prevent misuse of old accounts by intruders or users who no longer have the authority to access the system.
    g. If a user needs administrative access, they must be placed in an administrative group instead of logging in as administrator.

9. **DEFAULT ACCOUNT MANAGEMENT**
    a. Many operating systems and applications have default accounts and passwords built in or left over from the development or installation process. These accounts and passwords are a significant risk if they are left open and available for use; default accounts must be disabled, renamed, or their passwords changed.
    b. Use of university domain user accounts is required instead of local system and non-domain accounts

10. **PHYSICAL SECURITY:**
    a. Systems that contain sensitive information must be physically attached via a secure locking device to some relatively immobile object or housed in an area that uses access control systems (e.g., card-key, cryptolock), or otherwise provides strictly controlled access (e.g., in a room that is monitored for access).

b. Password-protected screensavers must be used for logged-in but unattended workstations.

11. **VIRUS AND MALWARE SCANNING**

a. All workstations, whether connected to GSNet or standalone, must use an approved antivirus product. Where possible in this scenario, at a minimum, a virus configuration should include:

i. Scheduled daily signature updates

ii. Scheduled weekly scans of all files and file types

iii. Real-time protection enabled for all devices including externally mounted devices (USB devices)

iv. The antivirus application must be initiated on system startup

v. If a virus is found, clean the threat first and quarantine the threat second

vi. Protected from unauthorized configuration change

12. **BACKUP**

a. If a workstation stores files locally that contain primary critical information or contain primary sensitive information, those files must be transferred to university network storage.

b. If the workstation is standalone and stores data, then local backup is required.

c. The backup process must be tested periodically for successful restorations.

d. Wherever possible, all workstations should have an established, documented, and consistently-used backup plan.

e. The frequency of the backup schedule will depend on the data classification of the data stored on the workstation.

13. **SEPARATION OF FUNCTION**

a. Workstations must be designed in a way that allows functions, applications, and data to be grouped or separated according to data classification and function. For example, public-use workstations must not be used to access or store sensitive information.

b. Servers, rather than workstations, must be used to house multiple user applications, databases, and/or shared resources.

14. **MISCELLANEOUS**

a. All Georgia Southern-owned workstations, whether on the university domain or not, must have a centrally-managed university administrative group required for the Information Security Function.

b. Georgia Southern owned computers must be joined to *the Georgia Southern domain*

c. Common access computers must require individual authentication

d. Workstations must use Georgia Southern DNS and DHCP settings

e. Configuring Georgia Southern owned portable devices in ad hoc mode or connecting to other non-university wireless access points is prohibited.

f. The use of insecure protocols (such as FTP and Telnet) to transmit confidential information is prohibited.

The use of secure protocols (such as SSH and SSL) is the required method of data transfer, both inside and outside the University

g. Use the Georgia Southern naming convention for the workstations

h. Use the Georgia Southern standard desktop image and baseline configurations.

i. Do not store confidential/sensitive information on mobile devices. If it is necessary to save confidential information on mobile devices then information must be in an encrypted format with an encryption scheme coordinated within the department and with the Information Security Office.

j. The use of host files (local files that override DNS settings) is prohibited except for development.

15. **Exceptions**

Any exceptions to this standard must be documented, reviewed and approved by the the CIO or his/her or delegated authority.

a. For the purpose of this policy, the Chief Information Security Officer is a named designee.

16. **Authorization**

The CIO is responsible for enforcement of this standard. Violations of this standard could result in serious security incidents involving sensitive university, state, federal and privacy data. Violations of this policy can lead to disciplinary action up to and including dismissal, and/or legal action. Any known violation of this policy is to be reported to the CIO or his/her designee.

17. **Related Documents**

a. Acceptable Use Policy

b. Data Stewardship and Classification Standards

c. Remote Access Policy

d. Remote Access Standards