

Georgia Southern University

Information Technology

Security Standards and Guidelines

Effective Date: 5/11/2006

Last Revised: 3/07/2006

Status: Approved

General Responsibilities

All authorized server administrators and users have an interest in the security and stability of the computer resources at Georgia Southern University, and share in the responsibility for protection of those resources, prevention of problems, and incident detection and response. Users must take responsibility for securing their own resources, engage in practices to maintain a secure and stable environment, and respond appropriately to threats against those resources as described in this and related documents.

Security Standards

Security standards are mandatory measures that shall be adhered to by authorized users of Georgia Southern University computer resources.

Prohibited Actions:

The following actions jeopardize a secure computing environment and are expressly prohibited.

1. No device shall be physically connected to the University network without prior approval of the Assistant Director, Network Services/Information Technology Services, or his designee.
 - a. Workstations: Approval for workstation connection must be obtained as part of the standard workstation installation process handled by Information Technology Services, or authorized departmental technical personnel.
 - b. Other devices (including, but not limited to, network components such as hubs, routers, switches, wireless access points, printers and other communication devices): Approval to connect devices other than

workstations must be expressly obtained from Information Technology Services/Network Services.

- c. Vendors/visitors can obtain a physical connection access to the University network through Information Technology Services on a per visit basis. This access will be granted for a specific period of time
2. Mail servers may not be run outside of Information Technology Services.

Required Actions:

Authorized users of Georgia Southern University computing resources shall perform the following actions to promote a safe and secure computing environment.

Servers

1. Servers that contain sensitive data* must meet the following requirements.
 - a. Server must be administered by dedicated technical support personnel.
 - b. Server must be housed in a secure facility.
 - c. If backups are necessary, backup media must be stored securely.
 - d. SSL must be used to transmit sensitive data.
 - e. Sensitive data covered by specific regulations (e.g. FERPA, HIPAA) must be secured in accordance with those regulations.

* Sensitive data includes but is not limited to: Social Security numbers; credit card information; health, counseling, human research subject, personnel, or non-directory student data. In short, sensitive data is non-directory information, the breach of which would compromise the privacy of individuals associated with the University.

2. All servers on campus, regardless of use or location, must be administered using the practices described below. The server administrator must record the execution of these items in the Server Administration Database on a monthly basis. The Server Administration Database may be accessed at: [LINK to database not active yet](#).
 - a. Server operating system must be vendor supported.
 - b. Operating system updates must be performed every 30 days. Critical security updates should be made immediately, and must be made within 3 business days of the date the necessary update is made available for that operating system.
 - c. Critical security updates to applications should be made immediately, and must be made within 3 business days of the date the necessary patch is made available for that application.
 - d. Standard anti-virus software (Symantec's Norton Anti-Virus) must be present and running, and virus definitions must be updated at least weekly.
 - e. A vulnerability scan must be run on the server at least every 90 days. Contact Information Technology Services for standard utilities.

- f. Open ports on the server must be identified and evaluated as valid at least every 90 days.
- g. Unused services running on the server must be identified and eliminated at least every 90 days.
- h. A password cracker utility must be run on the server at least every 90 days. Contact Information Technology Services for standard utilities.
- i. The server must be analyzed every 90 days for the presence of sensitive data.
- j. On Microsoft servers, the administrator account must be renamed.
- k. Account names and passwords must meet minimum standards (see below).
- l. File integrity checker such as Tripwire must be run daily.
- m. SSH (Protocol 2) must be used for server connections instead of Telnet and FTP.
- n. Service-providing programs must not be run as root/administrator.
- o. If backups are necessary, backup procedures must be documented.

Workstations – Non-Lab Environments, Personal and Transient Workstations

1. Passwords must meet minimum standards (see below).
2. Operating system software must be set up to automatically check for updates on a daily basis, and to download and apply those updates whenever they are available.
3. Anti-virus software must be installed and running, with virus definitions updated weekly at a minimum.
4. File and print sharing must be turned off when not used.
5. Unused software should be removed.
6. The Administrator named account should be renamed.
7. Unnecessary accounts must be eliminated, or renamed and disabled if they cannot be eliminated.
8. Unused operating system services must be disabled.
9. A screen saver with a lock feature must be active, and the lock feature must activate upon a maximum of 15 minutes of inactivity.
10. The BIOS must be password-protected.
11. All computers changing ownership shall have their hard drives formatted to remove any information from the previous owner.

Workstations – Student Lab Environments

1. Deep Freeze or some other management software must be enabled to control and restore machine configurations.
2. Operating system software must be set up to automatically check for updates on a daily basis, and to download and apply those updates whenever they are available.
3. Anti-virus software must be installed and running, with virus definitions updated weekly at a minimum.

Wireless Network Security

Wireless access must utilize strong encryption methods requiring authentication.

Physical Security

Only those individuals specifically authorized by the administrator of each of the listed resources shall have access to those resources:

1. backup tapes and other media;
2. servers;
3. wiring closets, communication access points and networking devices (restricted to personnel authorized for access by Information Technology Services); and
4. workstation data (individual authorized users of the workstation).

Password Security

Passwords are often the critical key to accessing data and computing resources. Where other attempts at security have failed, the password is often the last barrier to unauthorized access. As such, passwords shall be maintained by each user to be an effective prevention mechanism against unauthorized access. The following standards apply.

1. Passwords to any computing resource shall only be issued to authorized users. Password recipients are responsible for the integrity of their password and shall not distribute it to unauthorized users.
2. Every account must have a password.
3. Passwords must have a minimum of six (6) characters, and include three of four categories for complexity (combination of upper case, lower case, numbers, and special characters), to the extent allowed by the platform.
4. Passwords must be changed every 90 days.
5. Lockout features must be activated for servers.
6. Passwords may not be shared or given to others (exceptions listed in Accounts section).
7. Passwords must not be posted or displayed.
8. Applications and systems must be set up where possible so that passwords may not be changed more frequently than every seven days.
9. Passwords must be changed from their default values (especially networking devices and application servers).

Accounts (excluded from password sharing policy #6 above)

The following exceptions to the password standard allow password sharing among a very limited group of individuals in select circumstances.

1. Departmental or group accounts: requesting supervisor is responsible for actions taken with account.
2. Privileged accounts: the number of privileged accounts, as determined by the administrator of the machine in question, should be kept to a minimum; the password to a privileged account should only be provided to those personnel who require it.
3. Accounts for temporary or adjunct personnel, must be reviewed each semester for appropriate action (e.g. immediate termination of the account if the individual is no longer an authorized user as defined by the Computer Use Policies).
4. Accounts for student employees will be terminated each semester and must be reactivated by request of the department with which the student is employed.

Account Administration

1. Technical support personnel who administer passwords must have secure procedures to reset passwords or to identify personnel requesting a password or a password reset.
2. Procedures must be in place to eliminate and change access appropriately as personnel are terminated or reassigned.

Enforcement

Refer to Sanctions section of Computer Use policy.

Security Guidelines

Security guidelines are recommended "best" practices that should be adhered to by authorized users of Georgia Southern University computer resources.

Accounts

Definition and use of departmental accounts and shared accounts should be restricted as much as possible. Only those functions needed by the user should be made available through such accounts.

Servers

1. SSL should be implemented on Web servers if account log-in is required.
2. Server administrators should subscribe to and read general and platform-specific security lists such as SANS proc and Machine Makers Security First lists
3. Run intrusion detection system where appropriate
4. Install firewall system where appropriate
5. Application updates must be performed every 30 days.
6. Run file integrity checker such as Tripwire daily.

7. Periodically test backups for integrity.
8. Store backups offsite on a monthly basis.

Passwords

1. should not use any words found in dictionary of any language
2. should not use any combination of letters of a user's real name, username, initials or nickname
3. should not use any combination of a famous person's name
4. should not use any combination of a spouse's, girlfriend's, boyfriend's, or child's name
5. should not use any personalized numbers (SSN, driver's license, etc.)

Workstations

1. Turn off workstations overnight
2. Work-related files should be stored on the Novell cluster in the staff member's home directory or the department's work directory
3. Implement periodic backups (if not following Guideline 2)
4. Logging:
 - a. should be enabled to record:
 - i. successful and unsuccessful login attempts.
 - ii. system and application errors.

Revision History: 2/21/2006

3/07/2006