

Securing a Windows Server (Server 2003) that is used to Process Sensitive Information

Policy | Standard | **Procedure** | Informative

Version: 6

Last Updated: **30Nov09**

Approved By: **Ms. Tammy Clark, Chief Information Security Officer**

Information Security Coordination

Ensure that your **Server 2003** installation/operation is compliant with [Information System Use Policies](#).

Checklist:

1. Install antivirus software.

(McAfee VirusScan for servers can be obtained from IS&T upon request.)

2. Install centrally managed firewall software. Server firewalls be configured with a minimalist approach to filtration. In particular, all traffic that originates from external hosts is to be blocked unless the communication is required for business purposes.

3. Mandate the use of secure passwords.

Passwords should:

- be at least eight characters long
- consist of mixed case (at least one each of upper and lower case)
- contain at least one non-alpha character (such as a number or symbol)
- be significantly different from prior passwords
- be changed at least every 120 days

Hint: A strong password might look something like: **P@\$\$w0rd0!**

- a) Click **Start**, click **Run**, type gpedit.msc, and then press ENTER.
- b) In the Group Policy Object Editor MMC, double-click Computer Configuration, double-click Windows Settings, double-click Security Settings, double-click Account Policies.

4. Rename the Administrator account.

- a) Right-click **My Computer** and select **Manage**
- b) Expand (+) Local Users and Groups
- c) Select **Users**
- d) Right-click Administrator
- e) Select Rename

5. Operate an Operating System Screen Saver Password on the computer.

- a) Click **Start**.
- b) Click **Settings**.
- c) Click **Control Panel**.
- d) Click **Display**.
- e) Click the **Screen Saver** tab.
- f) Click the **drop-down box arrow**, and then choose a **Screen Saver**.
- g) Click the **Settings** tab.
- h) Check the **Password Protector** box.
- i) Fill in **Wait X minutes** (This is the number of minutes you want the

computer to wait before displaying the screen saver.)

6. Ensure that remote management software (such as pcAnywhere or Terminal Services) is configured to use encryption (at least 128 bit key strength).
7. Where appropriate, users can install software/applications that have been approved by the organization's technology representative and/or information technology manager. However, where practicable, unneeded services and features will be turned off.
8. In accordance with the principle of least privilege, users will only use minimal user profile privileges on computers that are based on users' job necessities (default is to deny access).
9. Unless there is a conflict, technical problem, or scheduled delay critical security patches will be installed for the operating system applications. All updates are to be applied in a timely manner (within 30 days). This includes items such as Windows updates, virus definition updates, firewall software patches...
10. File an Incident Report to report any suspicious activity on your machine by sending an email that contains the following information to help.gsu.edu.
 - a) Type "Security Incident - High Priority" in the subject line of the email.
 - b) Give the date the incident occurred.
 - c) Describe the incident.
 - d) Optional: If you know your IP address, or the IP address of your attacker, please include.
 - e) Provide contact information such as your name, phone number, and department.

Help: If you have questions, or need assistance, please contact Information Security (security@gsu.edu) or the IS&T Help Center at 404-413-HELP (4357), help@gsu.edu.