

Requirements for Securing a Windows XP Workstation that Processes Sensitive Information

Policy | Standard | **Procedure** | Informative

Version: 10.

Last Update/Review: 30Nov09

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

Minimum requirements to ensure that your **Windows XP** workstation is compliant with [Information System Use Policies](#).

1. Install antivirus software.

McAfee VirusScan Enterprise software can be obtained from the university's download site (<http://av.gsu.edu>). To determine if McAfee VirusScan is already installed on your machine, look in the system tray (bottom right corner of your screen). A red 'M' shield icon indicates that VirusScan is installed. When you run your mouse over the 'M,' you should see "McAfee status: OK."

If you are installing McAfee VirusScan on a non-university owned system, you should use the unmanaged software client.

Alternatively, if you are installing McAfee VirusScan on a university-owned computer, you should install a 'managed' client. A managed client installs an ePO agent, which allows IS&T and/or your departmental technology staffs, to transparently install additional security software to protect your computer, update protection policies and initiate on demand scans.

2. Install firewall software.

*Internet Security Systems firewall software can be obtained from your college/department technology representative (student version can be downloaded from <http://desktopprotector.gsu.edu>). To determine if the firewall software is already installed on your machine, look in the system tray (bottom right corner of your screen) for either the **ISS Desktop Protector** icon (a **black crown with a blue dot**) or the **ISS Proventia Desktop** icon (a **half moon within a blue circle**).*

3. Choose a secure password.

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@\$\$w0r\$**

4. Secure Novell password.

- a) Confirm that the **GSU** with the tree to the left is highlighted.
- b) Press **Control/Alt/Delete**.
- c) Enter your **old password**, your **new password**, and then your **new password** a second time.
- d) Click **OK**.

5. Secure Administrator password.

- a) Open User Accounts in Control Panel.
- b) Under or pick an account to change, click the administrator account.
- c) Click Change my password.
- d) Type your current password in Type your current password.
- e) Type your new password in Type a new password and Type the new password again to confirm.
- f) You can type a word or phrase to use as a memory aid for the new password in Type a word or phrase to use as a password hint.

- g) Click Change Password.
6. Critical software updates will be installed in a timely manner for software installed on the workstation.
- a) Go to your Desktop.
 - b) Click **Start**.
 - c) Click **Settings**.
 - d) Click **Control Panel**.
 - e) Click **System**.
 - f) Click **Automatic Updates**.
 - g) Select **Download Automatically**, and Notify Me Before Installing. Click OK.

7. 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.)

8. Turn on auditing.

- a) Click **Start**, Click **Settings**, click **Control Panel** and then click **Administrative Tools**.
- b) Double-click **Local Security Policy**.
- c) In the left pane, double-click **Local Policies** to expand it.
- d) In the left pane, click **Audit Policy** to display the individual policy settings in the right pane.
- e) Double-click Audit objects listed below and change access accordingly:

Event	Level of Auditing
Account logon events	Success, failure
Account management	Success, failure
Logon events	Success, failure
Policy change	Success, failure
Privilege use	Success, failure
System events	Success, failure

9. Check the credentials of anyone asking for information about your computer.

10. With the exception of non university Instant Messaging (IM), peer to peer (P2P), and Internet Relay Chat (IRC) software, users can install software/applications that have been approved by the organization's technology representative and/or information technology manager.

- a) Click **Start**, click **Control Panel**, double-click on **Add or Remove Programs**.
- b) Select the IM, IRC, or P2P software to be removed and click **Change/Remove**.
- c) Select yes in the warning popup.

11. 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).

12. 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.