

Requirements for Securing a Macintosh Computer that Processes Confidential Information

Policy | Standard | **Procedure** | Informative

Version: 30.

Last Update/Review: 30Nov09

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

Information Security Coordination

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

- 1. Centrally managed encryption software will be used to protect confidential data on desktops, laptops, and removable drives.**
- 2. Workstations that store, process, and submit confidential data are subject to random Information Assurance Vulnerability Assessment (IAVA) scans.**
- 3. Install anti-virus software.**

McAfee VirusScan software for the Macintosh can be obtained from the [university's download site](#).

- 4. Use a firewall.**

Configuring the Mac OS X firewall (ipfw). Turn on all of the advanced firewall settings (Block UDP Traffic, Enable Firewall Logging, and Enable Stealth Mode) by clicking on the Advanced tab and checking the boxes.

- 5. Choose a secure password.**

Passwords should:

- be at least ten 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\$**

- 6. Install critical software and operating system updates in a timely manner.**

Mac OS X can download software updates directly from Apple automatically.

- 7. Use an Operating System Screen Saver Password on the computer.**

Use the Mac OS X screen saver (Screen Effects). Turn on the screen saver from within System Preferences (it has its own panel) via the Activation tab — configure it to ask for your password before releasing the machine.

- 8. Check the credentials of anyone asking for information about your computer.**

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

information technology manager.

10. Set a Firmware password by downloading and running the Open Firmware Password application in accordance with Apple's instructions.

- [Instructions for installing/configuring the firmware password protection](#) for the Open Firmware Password application
- [Version 1.0.2 of the Open Firmware Password application](#) is only for Mac OS X 10.1 through 10.3.9
- For Mac OS X 10.4 or later, use the updated version of the Open Firmware Password application that can be copied from the software installation disc (located at /Applications/Utilities/ on the disc).

11. In accordance with the principle of least privilege, you can only use minimal user profile privileges on computers that are based on your job necessities (the 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.