

MAC Rebuild Guidelines

These are policies related to the use of computers owned by Penn State and computers connected to any Penn State network. Please read, understand, and adhere to these policies. Note: Anyone from outside the Penn State University network may not be able to view some of these files.

The documents on this web page contain only suggested guidelines for rebuilding and securing your machines. Because the process is different for every computer manufacturer, these guides are written at a high level. Any questions you have about this process should be directed to the [Help Desk](#), area [RESCOM](#), a faculty/staff IT contact or [Information Systems Consulting Services](#) for a specialized affordable alternative. Carefully consider which guidelines to implement, as every environment will have very differing needs and requirements. It is recommended that you implement one modification at a time to determine the impact of the change. Always be sure to document all modifications that are made and implement them in a test environment prior to deployment in a production environment.

1. Disconnect from the network

Unplug the PC's network cable and remove any wireless network adapters if you are near a wireless access point that allows automatic connections without any configuration by the user. If the wireless adapter is built-in, you are most likely using a laptop. Take the PC somewhere out of range of the wireless network.

2. Back up your files

Consider the files that you need to keep (word documents you have written, school projects, e-mail). Make copies of the files that are unique to you or irreplaceable. You can use an actual back up program, or you can manually copy the files. Either way, you will need to get the files to a location other than the drive where you plan to install the OS. Some examples, are; another hard drive installed in the PC or connected to it via USB or FireWire, one or more CDs or DVDs, another computer, via the network, zip disks, Jaz disks, or SuperDrive. Also MAC offers [instructions](#) on backing up the system.

3. Preparation Steps

Once you have reformatted the machine, you will need to install several files before placing it on the network for the first time to prevent it from becoming infected again. Service Packs, patches, and hotfixes are software update programs which eliminate specific vulnerabilities that have been discovered in a larger piece of software. You can find some of the updates via the links below. You will need to use either a writeable optical drive (CD/DVD-R), a mobile/external drive, a logical drive, or your [PASS](#) space (although PASS is limited in size) to download the updates and burn them to a CD **before** you do the reformat from another computer. Patches should be downloaded from a trusted machine rather than a compromised host.

The most highly recommended security updates and patches can be found below, however, this is not a comprehensive list of all the patches that exist. ALWAYS check the applicable operating system website to get the latest patches for your computer. Mac OS X users can install the patch through Apple's Software Update service, or through Apple's [support website](#). Many applications that are running on your system also have patches and hotfixes, and these updates will also need to be downloaded and applied prior to placing your computer on the Internet for the first time.

Internet Explorer 5.2.3 for Mac OS X	Microsoft Office v. X for Mac Security Update (10.1.6)
Security Update 2004-12-02 v.1.0 (Mac OS X 10.2.8 Client)	Security Update 2004-12-02 v.1.0 (Mac OS X 10.2.8 Server)
Security Update 2004-12-02 v.1.0 (Mac OS X 10.3.6 Server)	Mac OS X Update 10.3.6

4. Reformat & Reinstall

- 1) Put your Mac OS System CD into your CD-ROM drive.
- 2) Restart your Mac holding the "C" key down; the Mac will boot from the CD as a result.
- 3) When the Mac has finished booting from the CD, double click on "Mac OS Install".
- 4) Select your destination drive, if you have more than one; (almost anything from a Zip Disk to a 2nd hard drive can hold a bootable Mac OS System folder; the "Start-up Disk" Control Panel lets you select between multiple Drives containing valid System Folders).
- 5) To perform a clean installation click on the "Option" button and select "Perform Clean Installation".
- 6) The Mac will choose an easy install by default. If you want to customize the install, click on the "Customize" button and select only the items you want.
- 7) Wait five to nine minutes, then let the Mac restart to a completely fresh Mac OS!

Reformatting your machine removes all data from your computer. This is an irreversible process.

A clean installation will put a completely fresh System Folder with fresh contents on your hard drive, and rename your previous System Folder as "Previous System Folder", so that you can sort through any old preferences, or third party System Extensions, Control Panels or Startup Screens you might wish to keep and transfer at a later stage.

A word of caution here: Should you be experiencing problems with your Mac, it is highly recommended that you only implement old system items in a cautious and logical manner that allows you to find the damaged culprit.

A damaged preference file causes the majority of problems on Mac systems. Mac problems can also be caused by corrupt fonts, if you use volumes of dodgy third party fonts. Most issues can be avoided long before a clean install is ever required, in which case you simply delete the culprit preference file, and let the Mac build a new one.

To find a problematic preference file, temporarily move preference files starting with "A-M" from the "Preferences" folder in your "System Folder" to a spare folder on your desktop.

Restart and see if the problem goes away. If it works, split "A-M" into "A-G" and "H-M" etc. until you find it. You can use variously colored "Labels" - under the "File" menu "Label" to help differentiate among files.

If the culprit isn't in "A-M", repeat the exact same procedure with "N-Z". Don't forget to copy all of your good preferences back into your Preferences folder when you are finished, replacing the new ones that the Mac OS creates along the way.

5. Create Passwords

Intruders do attempt to gain access to shared computer systems through the accounts of others. Their motives vary from curiosity to criminal malice. It is part of your responsibility as a computer user to create a strong password for both your Penn State access account and all operating system accounts on your computer. It is your privacy, your reputation, your files, and your computing resources that are all at risk. Often times passwords/password files are commonly collected for future use when a system is compromised. All passwords should be changed and strengthened in the event of compromise. For detailed instructions on how to create a good password go to the [SOS passwords page](#).

6. Install Firewalls

Mac OS X has a built-in firewalls. For other operating systems, you should buy or download and install a personal firewall. It is important to ensure your firewall is enabled for complete protection. Instructions for configuring your firewall can be found at the Penn State ITS Helpdesk links below.

Mac OS X	http://helpdesk.psu.edu/mac/os10/osxfirewall.html
----------	---

7. Automate Live Antivirus Updates

New vulnerabilities are continuously discovered and attacks to exploit vulnerabilities are continuously written. Many of the more common viruses "morph" or change frequently to make them more difficult to detect. Viruses spread rapidly and by many different ways (for example, via e-mail attachments; infected document files; Web sites that contain hostile code that can infect your computer through vulnerable browsers; and unprotected file shares). Using Symantec Antivirus ([FREE for Penn State students, faculty, and staff](#)) and configuring it to update virus definitions automatically with the directions below will help keep your computer protected.

Live Update for Mac OS X	http://helpdesk.psu.edu/virus/liveupdmac.html
Live Update for Mac OS 9	http://helpdesk.psu.edu/virus/liveupdateos9x.html

8. External Security Guides and Documents

Securing Mac OS X	http://www.psiborg.net/transceiver/txt/osx.html
oMacOS X: User Friendlier Security for Unix	http://www.sans.org/rr/whitepapers/apple/1282.php
A Corsaire White Paper: Securing Mac OS X	http://www.net-security.org/dl/articles/Securing_Mac_OS_X.pdf