

Macintosh File Encryption

MacOS X FileVault

MacOS X 10.4 provides a system-level option for encrypting files on your hard drive. FileVault secures files in your home folder by encrypting and decrypting these files while you are using them. Files are encrypted with the login password for the individual user. If there are multiple user accounts on the local Macintosh system, each will need to be set up with FileVault separately. To be effective, auto-login of the user on the Macintosh should be turned off, requiring the user to type in their password each time the Mac is turned on or restarted.

FileVault settings are managed under System Preferences. A Master Password can also be set, allowing you to unlock any FileVault account on the computer. If either password is lost, there is no way to reset them and data can be permanently lost. As with any password, they should be selected for their security. If a Macintosh hard drive protected with FileVault becomes damaged or corrupt, file recovery will be far less likely, so proper backups are all the more important.

Disk Utility

Disk Utility (Applications -> Utilities -> Disk Utility) can encrypt data on a more limited basis. It provides the ability to encrypt a disk image of a folder on the local hard disk, which could then be stored according to university security policy. Again, as with FileVault, if the password is lost any data within the disk image cannot be recovered.

The Security Control Panel

This System Preference Panel provides access to several security features. These options include FileVault for encrypting home directories, Secure Swap Space which eliminates the chance of someone being able to sift through the swap space trolling for passwords. It also provides configuration options as to when passwords are needed to gain system access.

MacOS X Screen Saver

The user password can be required to wake the system from sleep or screen saver mode by going to the Security option under System Preferences. Make sure that the box is checked next to "Require password to wake this computer from sleep or screensaver". This will help prevent people walking by accessing the workstation.

MacOS X Auto Login

Macintosh systems can be set to auto-login as a certain user. Turning this feature off will enhance the security of the system. To check this setting, go to System Preferences, Accounts and click on Login Options. (You may be required to unlock the Accounts screen by providing the password for the admin account to gain access to Login Options.) On the Login Options screen, make sure that "Automatically log in" is not checked. With this feature turned off, each time the Mac is turned on or restarted, you will be challenged for a user name and password.

Keychain

Mac OS X includes an application called Keychain. It is used to store and access usernames and passwords, such those used by web sites that require logins. The default Keychain is called "login" and uses the login password. For further security, you can change the Keychain password so that it must be authenticated to separately. This way if someone gained access to your account, they would not have instant access to your Keychain also. Keychain can also be configured to lock after a set period of inactivity. This option can be found under Edit -> Change settings for Keychain Login in the Keychain Access application.

Apple iPod

PodSmith 2.0 can encrypt the sync data in your iPod and keep your privacy even if stolen.

[Get PodSmith 2.0 \(free trial\)](#)

Screen Lock

You can lock and unlock the screen by un-mounting and mounting your iPod. Of course you can unlock the computer by typing your password without your iPod.

File/Folder Lock

Specified folders or files can be locked by un-mounting your iPod.

Application Lock

Disable all applications except those you specify.

Mount Lock

Disable and mount the removable devices such as USB memory, iPod, CD-R/RW, and external hard disks.

This function protects you from unexpected data theft or leak.

Monitoring

PodSmith allows you to monitor the mounted drives, application usage, and contents of the drives.