Duane's Incredibly Brief Guide on Maintaing a Secure File System on a Mac
http://www.cs.williams.edu/~bailey/securefs.pdf

With the advent of portable computers, it is vitally important that we develop strategies for protecting private data. For most faculty and staff, I suspect there are two basic forms of private data:

1. Work-related data about ourselves, colleagues, and students that we carry in confidence.
2. Personal, non-work-related data that we wish to avoid exposing at work.

If you are reading this document, it is likely that both types of data are on your computer, and that anyone who might have access to your computer would have access to either type of data. If you should lose your computer, of course, you should assume that anyone finding your computer will have access to this data.

This document describes a simple technique for constructing a secure, virtual file system that you may only access with a password. This approach is different than securing an entire physical file system, as it is much less error prone, and allows your system to be backed up to insecure devices without compromising your data.

The Virtual File System
File systems are simply hierarchies of folders (or directories) that are stored on a device. When you acquire a new hard drive, burn a new CD, or attach a new USB key, for example, you *partition* and *format* the drive. Partitioning the device breaks the physical drive into several smaller virtual devices. Formating a drive causes the system to start a new hierarchy of folders on that device. The tool used for this task is called the "Disk Utility" and can be found by looking in "Applications" and then opening the "Utilities" folder.

Disk Utility also has the ability to construct a new "virtual" device stored as a file in another file system. This device can then be formatted and accessed as though it were an ordinary physical device. This device is referred to as a "sparse image": while you may configure it to store 100-megabytes, that much space is not actually used until it is needed. It may, in fact, never reach the size of 100-megabytes because the disk image can make use of compression techniques.

Ways to Secure File Systems on a Mac
Mac OS X directly supports several forms of data encryption:

1. Encryption of your Home Directory (called File Vault).
2. Encryption of a file system.

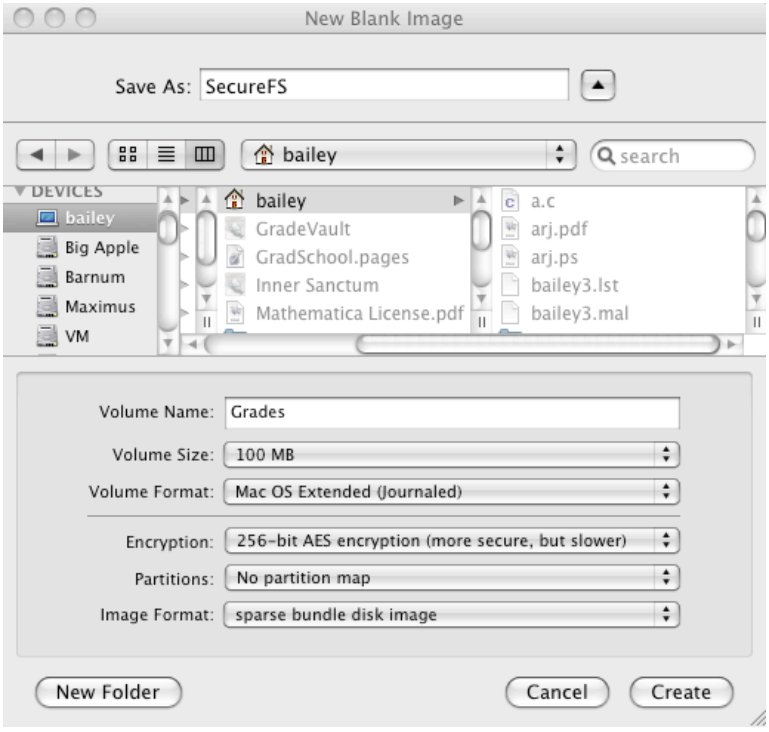
I would not suggest using File Vault to encrypt your home directory. First, while you're logged in, all of your data is generally accessible. If you never log out, your data is just as prone as if it were unencrypted. Second, your backup software must either back up your sensitive data encrypted or unencrypted. If it is backed up unencrypted, your sensitive data is now accessible to anyone who has access to the backup system. If it is encrypted, it can be difficult to restore from backup. In either case, if you forget your password, you will lose everything stored in your home directory—for most of us, an unimaginable disaster.

The second approach is to encrypt a physical or, more importantly, virtual file system. I advocate this approach for storing sensitive information. If you make use of a sparse disk image, then you control the information that is encrypted, and limit the damage of lost passwords.

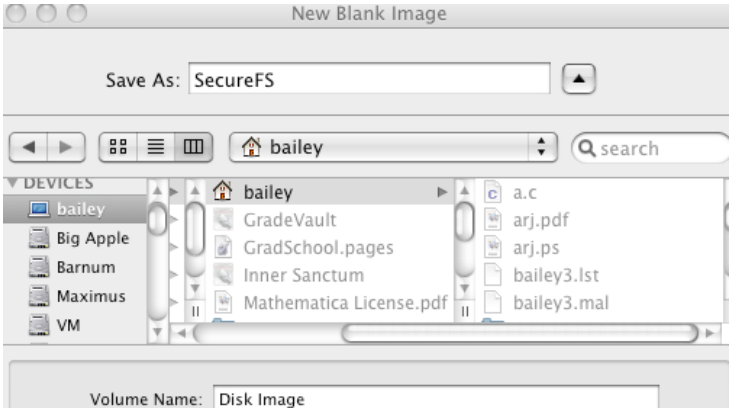
Constructing an Encrypted File System

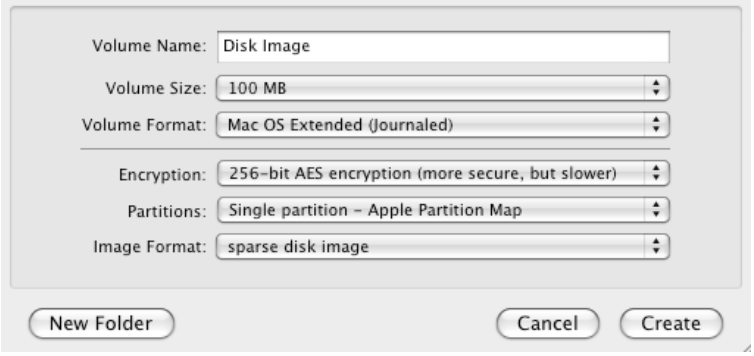
The process of constructing a encrypted file system is relatively straight forward. Before you begin, you need to estimate how much space you will need. You might, for example, find out how much space you are currently using, and then multiply that by a factor of two. If you outgrow that space, it is a simple matter to create a new file system and move your files over.

1. Start up "Disk Utility". Go to Applications, then Utilities, and double click on the Disk Utility application.



2. From the File menu, select, New..., and then "Blank Disk Image". Give a name for the file that holds the encrypted drive (e.g. SecureFS) and select a place to store the file system.





Fill in the form fields as follows:

- Volume Name: When you eventually open the file system, this is the name it will use. You probably want something descriptive, like Grades.
- Volume Size: This is how much space will be available on the virtual disk you create. You should be generous enough to allow yourself room to expand. Because we will compress this virtual device, it will likely take much less room to store this information on the physical device. This is another great advantage of virtual devices.
- Volume Format: This will default to Mac OS Extended (Journaled). Leave this selection to the default.
- Encryption: Select either 128-bit or 256-bit AES encryption. 128-bit will be faster, but less secure. 256-bit is more secure, but access will be slower. For most people, 128-bit security is sufficient.
- Partitions: Leave as "Single partition - Apple Partition Map". If you need more than one partition, I suggest you create several encrypted drives rather than several partitions.
- Image Format: Select either "sparse disk image" or (if you're using 10.5 or later) "sparse bundle disk image".

3. Press Create.
4. The next dialog box allows you to specify a password.

As you type in a password, the password strength meter increases. Including numeric digits and/or symbols will greatly improve your password security. Long phrases work well, if you can touch type. (If you're feeling unimaginative, pressing the key icon will generate suggested passwords. Make sure, however, you have a really memorable password. If you lose your password, your data cannot be recovered.) Type in the password, again, to verify it. **Unclick Remember password in my keychain.** Keeping

your password on the keychain increases your exposure, especially if you don't log out frequently. Press OK.

5. Select Quit from the File menu.

After the partition has been created, it will automatically be mounted on your desktop.

Before using it, I would eject the disk (either drag the disk icon (for me, called Grades) into the trash, or click once on the disk icon, and select "Eject" from the "File" menu).

Using Your Encrypted File System

You can now double-click on the encrypted partition (for me, SecureFS.sparsebundle). It will ask for your password; provide it. **Do not store this password on your keychain.** The disk will appear on your desktop. This encrypted virtual disk works like any other. Reading or writing to this device is (only slightly) slower than for unencrypted devices. Because you selected a "sparse" device, the amount of disk space actually used is often significantly less than it appears.

Tips on Encrypted File System Usage

You may find the following tips useful:

1. **DO NOT USE THIRD PARTY ENCRYPTION SOFTWARE.** The software available on Mac OS X is sufficient for most people's needs. It is very difficult to ensure that third party software is as secure as advertised.
2. Only mount your encrypted devices while you need them. Eject them when you're finished. It's hard to predict when you'll lose your laptop.
3. If possible, click "Require password to wake this computer...." in the General tab of the Security area of your System Settings. You should also Disable automatic login.
4. When you create an encrypted drive, copy your sensitive documents to the drive, and delete the originals. It doesn't help if you originals are left exposed.
5. Store different types of information in different encrypted drives. Do not mix sensitive personal and professional information on the same volume.
6. Use different passwords for different encrypted drives. Don't give passwords to others. It's not possible to change the password on a drive once it has been created. (If you need to change the password, create a new encrypted file system, and transfer the information from the old volume to the new. Then, unmount the old volume, and move its sparse image into the trash.
7. You can remove the ".sparseimage" or ".sparsebundle" suffix from the image file name. This makes your secure file systems less obvious.
8. For USB and other very portable devices (that can easily be lost), use a encrypted file system to maintain confidentiality. (These encryption mechanisms are not compatible with Windows; if you use a USB between Windows and Mac OS X, you should keep your USB clean.)
9. Encrypted sparse volumes may be moved or copied without fear. Their functionality has nothing to do with their location.