

## How to Encrypt Documents on Your Windows XP Computer

ESTIMATED TIME TO COMPLETE: 15 MINS

What do you carry around on your laptop? Does it include things like your resume, transcripts, school or internship applications or financial records? If you are using a laptop for your job, maybe you have files like human resources records, student applications, transcripts, human subject research data or payroll information.

These documents likely include some form of SENSITIVE DATA, which is data whose unauthorized disclosure may have serious adverse effect on the University's reputation, resources, services, or individuals. If your laptop falls outside of your physical control due to loss or theft, the data inside your computer should already be made electronically inaccessible.

Encryption is the standard technology used to protect sensitive data from unauthorized disclosure. Microsoft Windows XP makes encryption easy by providing a built-in tool called the **Encrypting File System** (EFS); The following steps detail how to put these security measures in place for a Windows-based computer.

### BEFORE YOU PROCEED:

**These Security Shorts are intended for non-technical users who manage their own computers. If your laptop is managed by an IT department, do not proceed. Contact your IT administrator for further assistance.**

Make sure you have Microsoft Windows XP Service Pack 2 (SP2) installed. Running SP2 is one of the most important security measures you can take. Furthermore, these instructions may not work unless you are running SP2.

If you are using Microsoft Vista, please refer to the security short: How to Encrypt Documents on Your Vista Computer.

Keep in mind:

- Disk encryption technologies such as EFS can protect your data from unauthorized access, but it does nothing to protect data that is transmitted over the network or via e-mail.
- EFS does not protect your data when you log in and visit a malicious Web site or open a malicious e-mail.
- Remember to back up your data and encryption keys, or you risk losing your data irretrievably.

### WHAT'S IN THIS DOCUMENT

***How to Encrypt Documents on Your Windows XP Computer..1***

***Step 0: Password Protect Your Account..2***

***Step 1: Create a Folder to Store Encrypted Document..3***

***Step 2: Store and Access Encrypted Documents..5***

***Step 3: Back-Up Your Decryption Key..6***

***Step 4: Backing Up your EFS Encrypted Documents..8***

***To unencrypt an individual file..9***

***To unencrypt a folder and all files in it..9***

***If you lost your thumbdrive or your password had to be reset..9***

***To Recover an Encrypted File or Folder..10***

## Step 0: Password Protect Your Account

If you haven't already, you need to build the first level of defense for your data, which is password protection. Consider using a pass-phrase, which is a more complex combination of letters than a typical password.

1. Click **Start** and select **Settings > Control Panel**.
2. Click **User Accounts in the Control Panel window**.
3. Select your user account, and then select **Create (or Change) a password**.
4. Create a strong password or pass-phrase by choosing a long but easily remembered phrase.

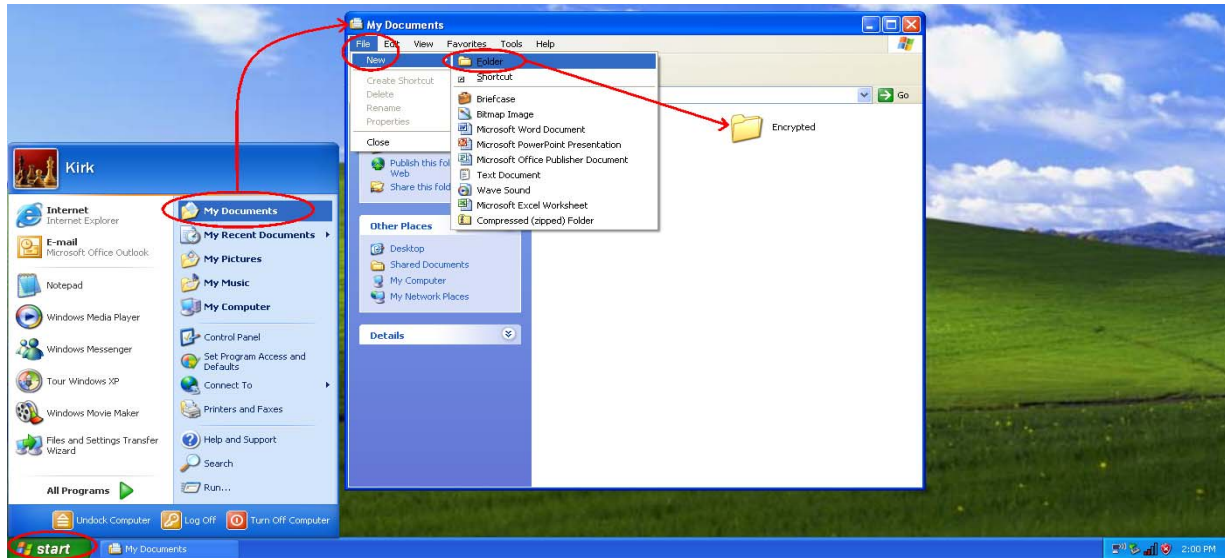
Here are some things to keep in mind when you create your new password:

- Select a unique password — not one you are using or have used elsewhere. Do not use a PIN number or a password used for other computing accounts like AOL or hotmail.
- Use at least nine characters containing a mix of upper- (capital) and lower-case letters, numbers, and common punctuation. However, do not use a forward slash (/) or a space bar.
- The best passwords are made up. (Of course, don't use any examples shown here.)
  - Use the first letter of words in a phrase and include numbers and punctuation; for example, "Do you know the way to San Jose on US-12?" becomes "DyktwtSJoUS-12?"
  - Use an entire phrase, like Rudolph Is My Favorite Reindeer.

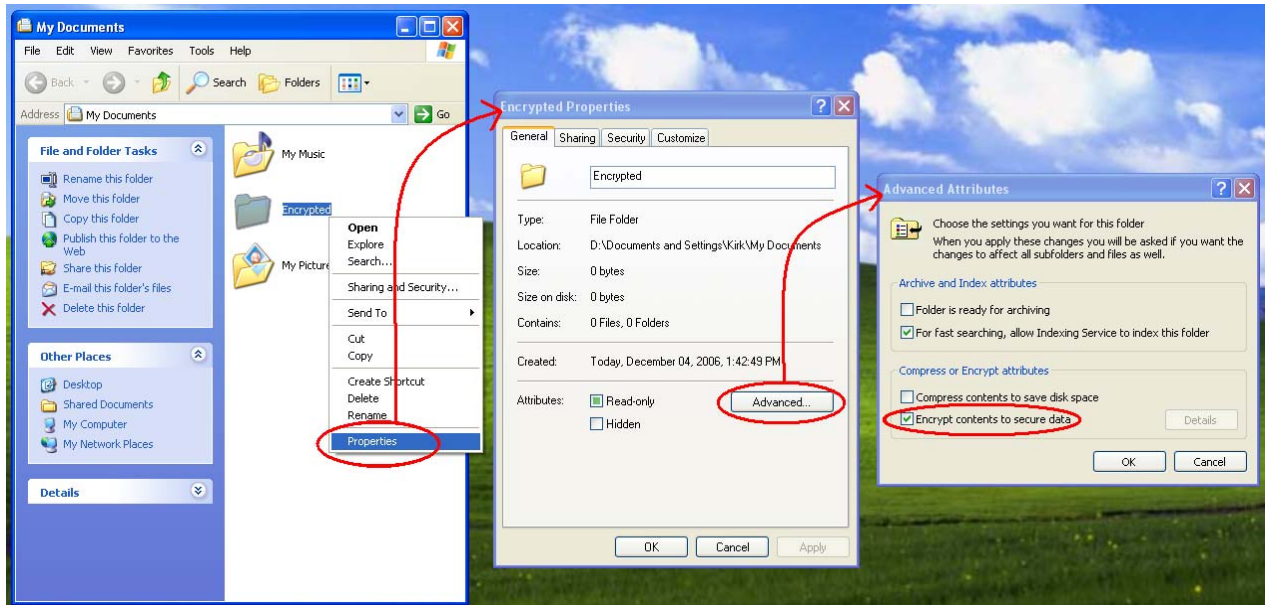
## Step I: Create a Folder to Store Encrypted Documents

To create a folder to store encrypted documents:

1. Open **My Documents** window on your Windows-based computer.
2. From the File menu, select **New > Folder**. Change the folder name from New Folder to a name of your choice. In this example, the folder is named “Encrypted.”



3. Right-click on the new folder and select **Properties** from the pop-up menu.
4. Click **Advanced**. The **Advanced Attributes** window displays.
5. Turn on the **Encrypt contents to secure data** checkbox, and click **OK**.
6. Click **OK** again. The name on the folder that you encrypt will turn green.



**Note:** If the option to encrypt cannot be selected, contact the systems administrator or IT specialist in your department and ask them for the recommended way to encrypt your sensitive documents.

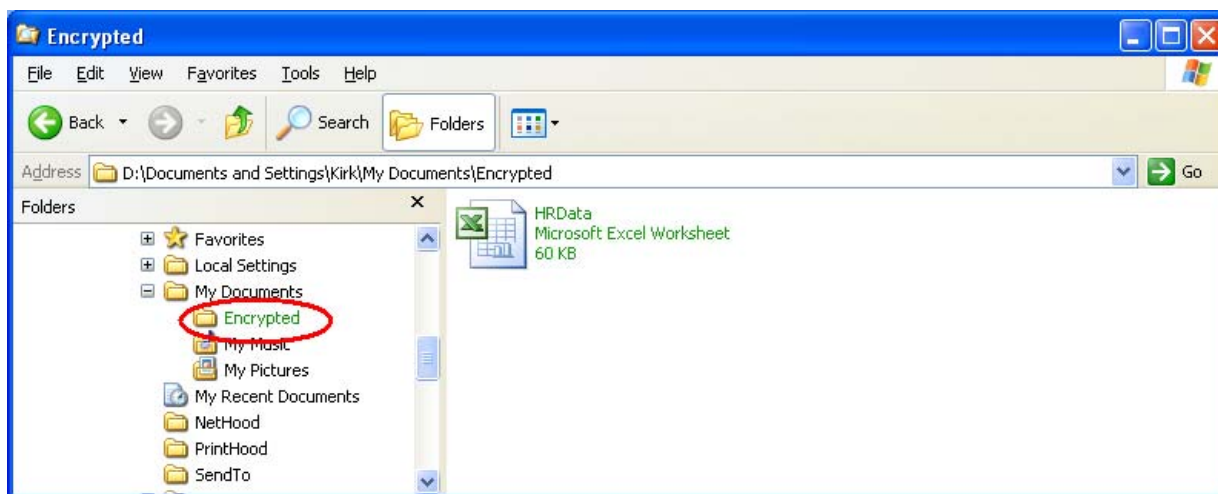
## Step 2: Store and Access Encrypted Documents

Store any file that needs to be protected in your new folder. These files will automatically be encrypted and the filenames will also turn green (*Example: HRData*).

When you move a file out of an encrypted folder, the filename may turn black, indicating that it is no longer encrypted.

Getting access to your encrypted documents is the same as getting access to everything else.

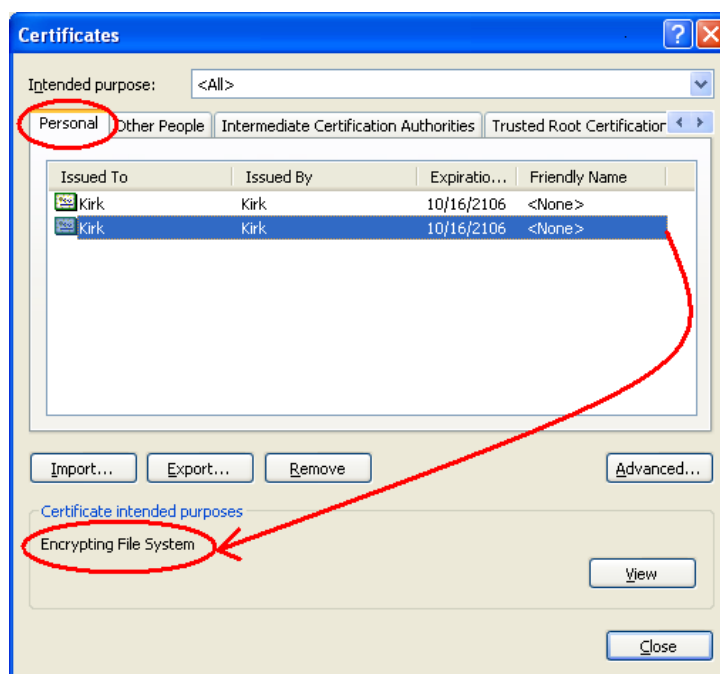
To unencrypt the folder, return to the Advanced Properties window (see steps 1.3-1.4 above). Turn off the **Encrypt contents to secure data** button and click **OK**.



## Step 3: Back-Up Your Decryption Key

Encryption does a very good job at protecting your data—so good, in fact, that if you forget your password or if the decryption key that is stored on the system becomes corrupted, you won't be able to recover your files. To prevent this, back up your decryption key to a USB drive and store it away from your computer.

1. Open Microsoft Internet Explorer.
2. From the **Tools** menu, select **Internet Options**.
3. Click the **Content** tab.
4. Click **Certificates** in the middle of the dialog.
5. Click the **Personal** tab. Note that you may have several certificates for different purposes:



6. Select one certificate at a time until the **Certificate intended purposes** field indicates that the selected certificate is for the **Encrypting File System**. This condition is highlighted in red above.
7. Click **Export** to launch the Certificate Export Wizard.
8. Click **Next** to skip the Welcome page.
9. Click **Yes** to export the private key, and click **Next**.
10. Choose **Personal Information Exchange - PKCS#12 (.PFX)** format and check the box to **Enable strong protection**. Then click **Next**.
11. Skip creating a password for your exported certificate by clicking **Next** (chances are the reason you'll need your back-up is because you have already forgotten one password).
12. Browse to the location where you will save the certificate and decryption key, like a USB thumb drive or CD. Name the file and click **Next**.
13. Click **Finish > Close > OK**.

14. Store the thumb drive in a safe place away from your computer.

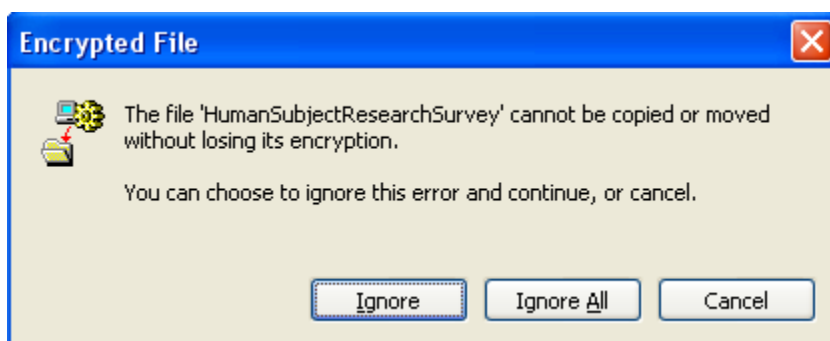
If you need to access this key, give your thumb drive to a trusted expert who will use it to decrypt your information using the "Recovery Steps" on page 10

**Warning:** *If your trusted expert has to reset your user account password for you, remember to repeat Step 3 to back up your new decryption key after you get up and running again.*

## Step 4: Backing Up your EFS Encrypted Documents

This security short is primarily about encrypting data on laptop computers to prevent unauthorized access to sensitive data when the laptop is lost, stolen, confiscated, or otherwise physically compromised. With that in mind, we support creating clear-text backups of sensitive data as long as those clear-text backups are physically secured away from the mobile laptop in a safe, vault, locked cabinet, server room etc. Creating clear-text backups has the added advantage of providing access to your data in the event that the key recovery process (also described in this document) fails for some reason (such as losing your thumb drive).

To back up your EFS encrypted documents in clear-text, simply copy them from your encrypted folder to a network server, external hard drive, CD ROM, USB Flash Drive etc. When you perform that copy operation, Windows will likely inform you that your backup copy will be unencrypted:



If you currently use a backup program (rather than manually copying your files) there are three ways that backup product will interact with EFS encrypted documents. Specifically, your current backup solution will either:

- a. Fail completely when it attempts to back up your EFS encrypted documents
- b. Backup your EFS Encrypted Documents in clear-text format
- c. Backup your EFS Encrypted Documents and keep them encrypted

You should test your backup solution and verify that it minimally will make a clear-text backup of your EFS encrypted documents. If it fails to backup your EFS encrypted documents entirely, you should contact the vendor to identify their EFS support plans. In the meantime, you can manually backup the encrypted files as described above by copying them yourself.

Note: NTBackup.exe, which is the backup program this is built into Windows XP will back up EFS encrypted files while preserving the encryption (i.e. option C above).

## To unencrypt an individual file:

1. In Windows Explorer, **Right-click the file** you want to decrypt, and then click **Properties**
2. Click the **Advanced** button in the General tab on the Properties sheet
3. **Clear the Encrypt contents to secure data check box**, and then click **OK**
4. **Click OK again** on the Properties sheet

## To unencrypt a folder and all files in it:

1. In Windows Explorer, **Right-click the folder** you want to decrypt, and then click **Properties**
2. Click the **Advanced** button in the General tab on the Properties sheet
3. **Clear the Encrypt contents to secure data check box**, and then click **OK**
4. **Click OK again** on the Properties sheet
5. On the Confirm Attribute Changes dialog, select the option to **Apply changes to this folder, subfolders, and files**, then click **OK**

## If you lost your thumbdrive or your password had to be reset:

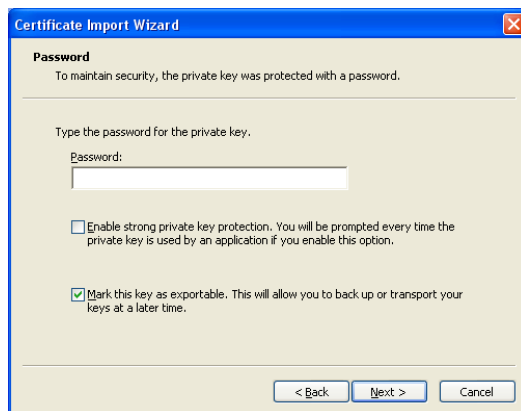
Back up all your EFS encryption keys using Step 3

## To Recover an Encrypted File or Folder

If you can see the file or folder, but are unable to decrypt it for some reason, follow these steps:

**Note:** *This information will not help recover a file from your backup tape if your hard disk has crashed.*

1. Insert the USB Flash Drive that contains your backed-up EFS certificate
  - You backed up your EFS certificate and stored it in a safe place in Step 3 above
2. From the AutoPlay Dialog, **Open folder to view files**
  - If AutoPlay is disabled and no dialog pops up when you insert your flash drive, then navigate to the flash drive using Windows Explorer
3. Double click the (.pfx) file that contains your backed-up certificate.
  - You entered the filename in Step 3.12 above
  - This opens the Certificate Import wizard
4. On the Welcome page, click **Next**.
5. On the File to Import page, click **Next**
  - The filename should already be entered since you launched the Import wizard by clicking on the filename
6. On the password page select the option to mark this key as exportable. Click **Next**.



On the Certificate Store page,

- a. Select the option to **Place all certificates in the following store**
  - b. Click the **Browse** button and select the **Personal** store then click OK.
  - c. Click **Next**
7. On the Completion page, click **Finish**.

After the certificate is imported, you should have access to the encrypted files.