

## How to Encrypt Documents on Your Windows Computer

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 personal private information (PPI)—the information that is most in demand by identity thieves. Examples of PPI include: name, address, birth date, gender, Social Security number, Visa status, driver's license number, credit card number, student number, bank account number, ethnicity, disability information, marital status and criminal record.

You need to protect PPI, because in the wrong hands it could be used to commit identity fraud. At a minimum, you should always secure your data by locking your laptop out of sight when it's not in use. But if your laptop falls outside of your physical control due to loss or theft, you can protect the data inside your computer by making it electronically inaccessible.

Encryption is the standard technology used to protect sensitive data such as PPI from unauthorized disclosure. Microsoft Windows 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:

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.

Keep in mind that 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. Also, EFS does not protect your data when you log in and visit a malicious Web site or open a malicious e-mail.

If your laptop is managed by an IT department, contact them before proceeding.

### WHAT'S IN THIS DOCUMENT

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

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

*Step 1: Create a Folder to Store Encrypted Documents...2*

*Step 2: Store and Access Encrypted Documents...4*

*Step 3: Password Protect Your Decryption Key...5*

*Step 4: Back-Up Your Decryption Key...7*

## 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.

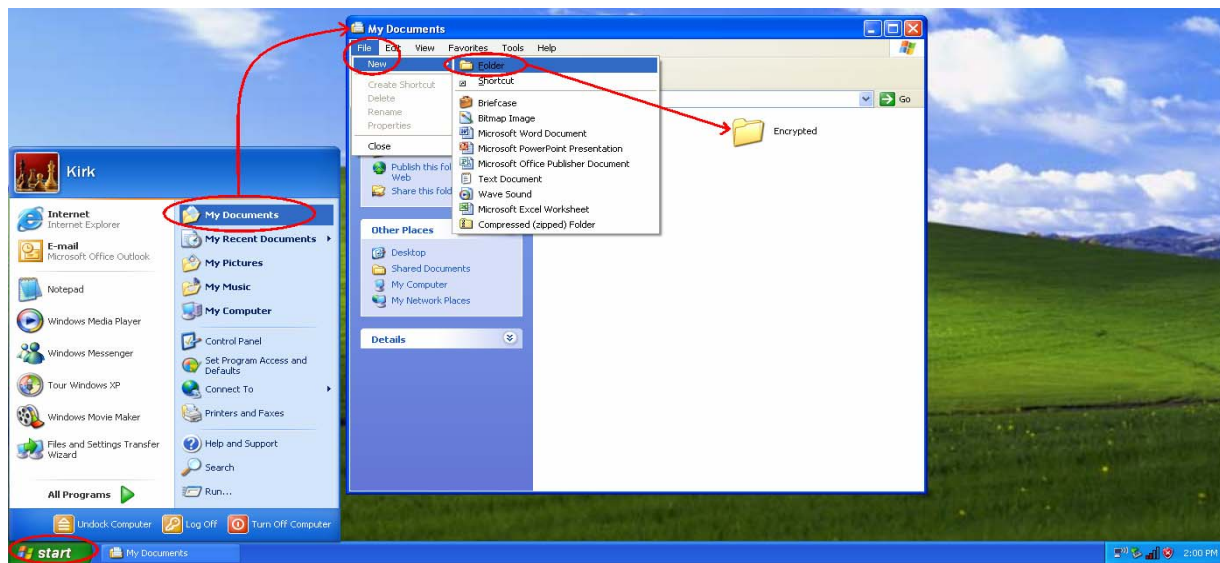
**Note:** *You must have administrative rights to your computer to complete this step.*

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 a password**.
4. Create a strong password or "pass-phrase" by choosing a long but easily remembered phrase such as "Rudolph is my favorite reindeer."

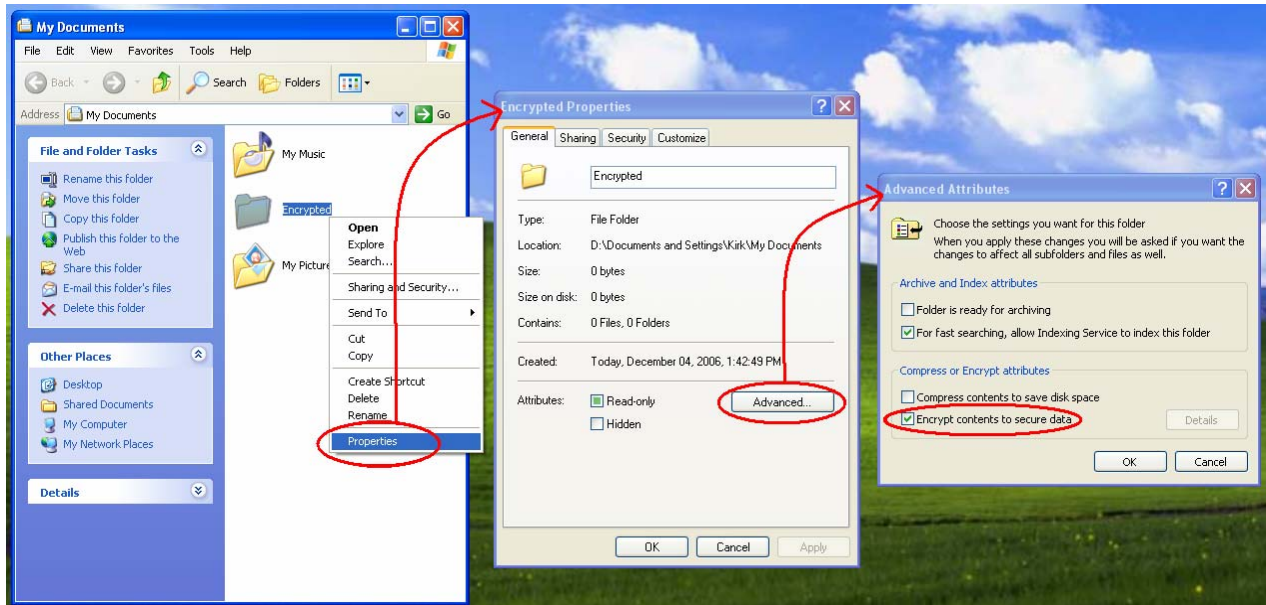
## Step 1: Create a Folder to Store Encrypted Documents

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.

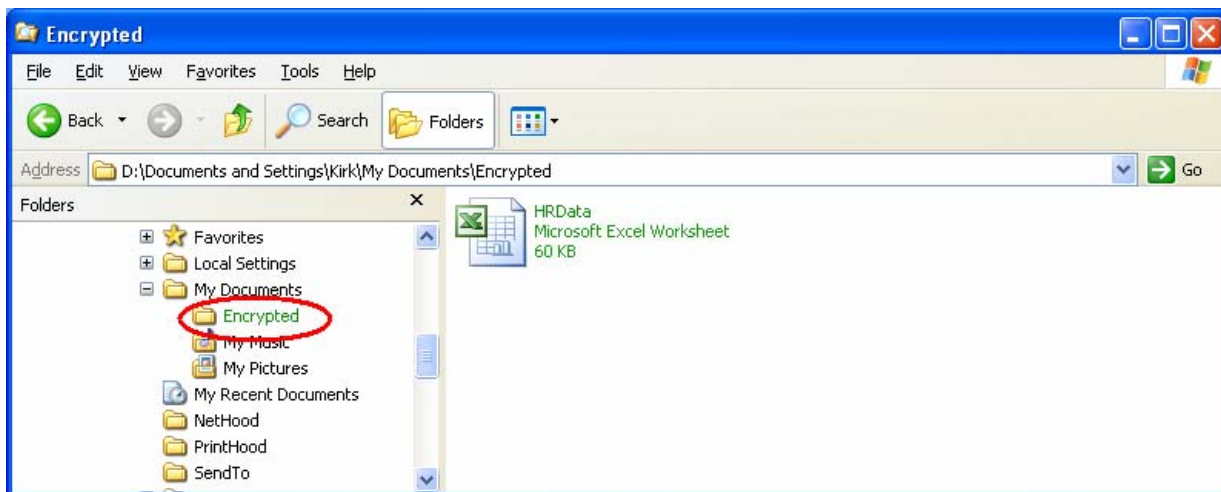
## Step 2: Store and Access Encrypted Documents

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 3-4 above). Turn off the **Encrypt contents to secure data** button and click **OK**.



## Step 3: Password Protect Your Decryption Key

The EFS uses a key to encrypt and decrypt your documents. This is like putting the key to your house under your doormat—convenient, but easily discovered by someone who knows where to look. Similarly, a thief with physical access to your laptop can find your keys and decrypt your documents.

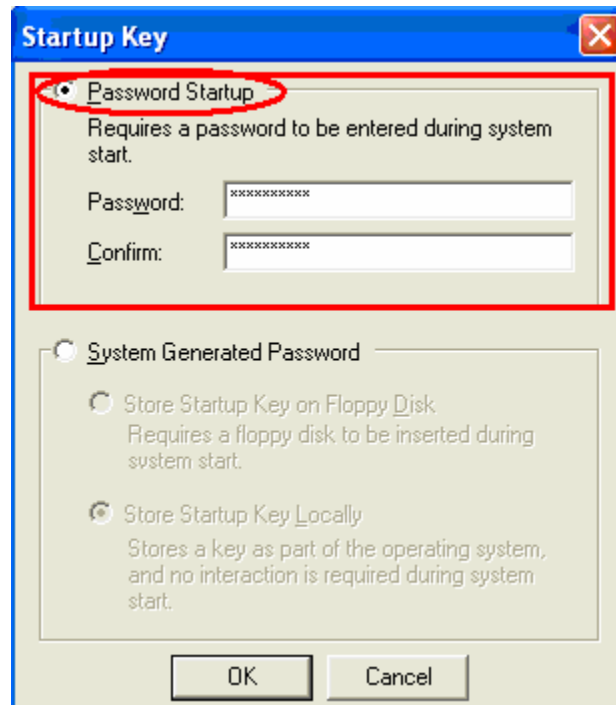
As one final security measure, protect this decryption key by using a password that is *not* stored on the laptop.

**Note:** *You must have administrative rights to your computer to complete this step.*

1. Click **Start** and select **Run**. Type **SysKey** in the **Open** text box.
2. Turn on the **Encryption Enabled** button and click **Update**.



3. Turn on the **Password Startup** button and type a password or pass-phrase. Click **OK**.



You now have a SysKey password. This extra layer of security figuratively moved your house key from under the doormat into a vault to which only you know the password. Whenever your system is powered on, you'll be prompted for this password:



**Warning:** *If you forget this password, you will not be able to boot your system. Thus, it is imperative that you write your SysKey password down and store it in a safe place away from your computer.*

## Step 4: Back-Up Your Decryption Key

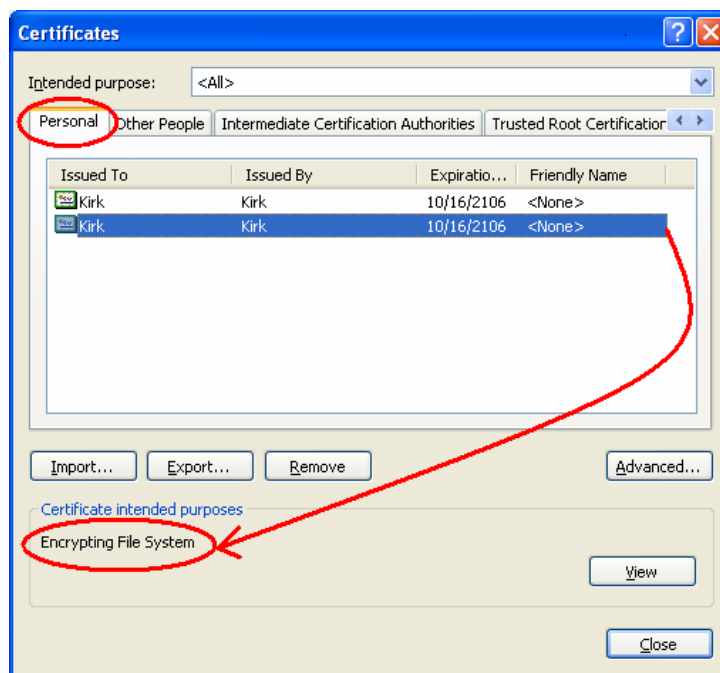
Encryption does a very good job at protecting your data—so good, in fact, that if you forget your password or if the decryption key that is stored on the system becomes corrupted, you won't be able to recover your files.

To prevent this, back up your decryption key to a USB drive and store it away from your computer.

**Note:** *You must have administrative rights to your computer to complete this step.*

**Warning:** *Don't skip this step!*

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. Keep it with your written down SysKey password so you have everything in one place.

If you need to access this key, give your thumb drive to a trusted expert who will use it to decrypt your information.

**Warning:** *If your trusted expert has to reset your user account password for you, remember to repeat Step 4 to back up your new decryption key after you get up and running again.*