INFO6001 – 23W	EXERCISE 4	Encrypting File System

Use the Snipping Tool to capture the 9 steps below and insert into a .ppt file as a study aid for Test 1. ~~Add acover sheet with the Course, Exercise and Student information - submit to drobox.~~ This is not a marked Lab Assignment.

Part 1: Using EFS

Open the Win7 VMware image
Login to the Account **User** with password **Windows1**
Create a new folder on drive C with ***yourFOLusername*** as the folder name
Highlight the ***yourFOLusername*** folder right click and select **Properties**
In the **Folder Properties** window select the **Advanced** button
In the bottom panel click on the box **Encrypt contents to secure data OK - Apply - OK**
All files placed in the directory by the owner will be encrypted using Microsoft EFS
Notice the folder name is presented in a different color.
When a file is saved to the folder it will be automatically encrypted.
Open notepad and enter your full name and student number as the file content.
Save the file in the ***yourFOLusername*** folder. Use your ***first name*** as the filename.
Create a new admin user named **student1**. Insure that the **User** account also has administrator privileges.
Logoff the account **User** and logon as the new user **student1**
Open notepad and select File – Open
Navigate to Computer – Local Disk (C:) – ***yourFOLusername*** folder
Select the file with your first name and select **Open**
Were you able to access the file?
Multiple users can share the PC and still maintain confidentiality of their personal or work-related files.

1. ***Take a screen capture of the error box that states you don't have permission to open this file***

As the new user **student1**, create an *encrypted* folder **info6001 off drive C**
Open notepad and create a text document. Enter your full name and date and save as ***yourFOLname1*.txt**. in the info6001 folder
Logoff as user **student1** and logon as the account **User**
Open notepad and select **File – Open** Navigate to **Computer – Local Disk (C:)** – ***info6001*** folder
Select the file with your ***yourFOLname1*.txt**.and select **Open**

Can the **User** account read the file? _____.

2. ***Take a screen capture of the error box that reads you don't have permission to open this file***

View the properties of the encrypted file
Right click on the file ***yourFOLname1*.txt** select **Properties - advanced - details**
Note the Recovery Certificate panel is blank

3. ***Take a screen capture of the Recovery Certificate***

Part 2: Cipher

Open a command prompt and enter the following command
C:\> cipher *yourFOLusername* *
A list of the encrypted files will be displayed. Files with the **E** attribute are encrypted files

Create a new folder on root of drive C named ***yourinitials*** with a sub folder named **private.** Open notepad and enter your full name as the text content. Save a file with name **mydata.txt,** in the **private** folder. Use the **cipher** command to encrypt the **private** subfolder which includes the text file named **mydata.txt C:\> cipher /e /s:c:*yourinitials***

4. ***Take a screen capture of the command prompt showing output of cipher command***

Use explorer to navigate back to the **private** folder

Note: The file has the color green for encryption.

5. ***Take a screen capture of the files in the private folder***

Part 3: EFS Certificates

Choose Start – All Programs - Accessories - Run and type **mmc (Microsoft Management Console).**
Next, you'll add your own plugins to this blank MMC: Select
File → Add/Remove Snap-in. .
Select **Certificates** and click **Add**
In the Certificates snap-in windows – Select **My user account** (default)
Click → **Finish**
In the Add/remove Snap-in window **Certificates-Current User** will be displayed
Click → **OK**
Note: The plug-in is now be listed in the Left Panel of Console Root window

On the left panel Expand **Certificates - Current User**
Expand **Personal** → Select **Certificates**
In the right panel the **User** certificates are displayed Expand
window to full screen to view the details

Note the intended purpose column has EFS listed
Note the expiry date is 100 years

Exit the Console1 and **do not** save
File - Exit

Part 4: Recovery Agent.

The recovery agent is used as a backup and to store the private keys in a location off the local computer. The recovery agent is also able to retrieve the files encrypted by a user if the user forgets their password or leaves the company.

From the **User** account use the cipher utility to designate the file name where the recovery agent certificates are to be stored.
Open a command prompt
C:\User\User> cipher /r:recoverAg
When prompted enter a password to protect the two recovery (.PFX) files.
Use **info6001** as the password
The **.cer** file is the certificate and the **.pfx** file is the private key for the recovery agent. These files have been saved in the **current** directory.

View the directory contents to verify
C:\User\User> dir

6. ***Take a screen capture showing the files***

Exit the command prompt

Create the Recovery Agent
Choose Start – Accessories – Run and type **mmc.**
Next, you'll add your own plugins to this blank MMC: Select
File → Add/Remove Snap-in.
Select **Certificates → Add**
In the Certificates snap-in windows – Select **My user account** (default)
Select → **Finish**
In the Add/remove Snap-in window **Certificates-Current User** will be displayed
Select → OK
On the left panel Expand **Certificates - Current User**
Expand **Personal** → Select **Certificates**

Highlight the **Certificate** folder and from the **Action** menu item select **All Tasks → Import**
When the Certificate Import Wizard opens Select → **Next**
In the Certificate Import Wizard window select **Browse**
In the **Open** window change the file type to **.pfx**
Select the file **recoverAg.pfx** Select
Open → Next

Enter the password **info6001** used to create the recovery files

Check the box **Mark this key as exportable** → Next
On the **Certificate Store** window select **Automatically select the certificate store based on the type of certificate → Next→ Finish**

Import was successful

7. ***Take a screen capture of the message "Import was successful"***

Now specify the Recovery Agent to recover the file encryption keys

Go to **Control Panel → System & Security → Administrative Tools**
Open **Local Security Policies**
Expand the **Public Key Policy** folder
Right click **Encrypting File Systems** folder and select **Add Data Recovery Agent→ Next**

In the **Add Recovery Agent Wizard → Next**
Click the **Browse Folders** button and click the **recoverAg.cer** file and click **Open** Click **Yes** to install the certificate
In the Select Recovery Agents window the new recovery agent is displayed as

Users - **USER_UNKNOWN** Certificates – **User → Next → Finish**

The **User** account is now the designated recovery agent for the files on the local computer.

As the **User** try, to access the current encrypted file in the **info6001** folder.

Were you able to access the file?_____.

Log off as **User** and log on as **Student1**

Place a second text file in the info6001 folder with name ***newfile.***

Log off as **student1** and log on as **User** Can the **User** account access the second text file? .

For the info6001 folder view the properties of each file→ Advanced → Details

Note the Recovery Agent specified in the bottom panel in each file

8. ***Take a screen capture showing the details of the recovery agent for both files in the info6001 folder.***

The attributes marking the recovery agent are only added to files created or opened and saved **after** the Recovery Agent is created.

The first step in managing the computer for using EFS would be to create the Recovery Agent before the other user accounts are created.

Part 5: Exporting Certificates

For security the Recovery Agent private key and certificate should be exported and saved in a location remote to the local computer.

From the command line open the MMC to the Certificate manger Snap-in
Run → **certmgr.msc**
When the Certificate Manger Window opens expand the **Personal** Folder and select the **Certificate** sub folder.
In the right panel note the certificates available (view full screen)
Locate the administrator (**User**) certificate for File Recovery (Intended Purpose)
Right click on the certificate and select **All Task → Export** In
the Certificate Export Wizard select → **Next**
Click **Yes, export the private key** → next
Click **Personal Information Exchange – PKCS #12 (.pfx) → next**

> If the *Delete the private key if the export is successful is checked the private key is deleted and the Recovery Agent cannot access the files, until the certificates are restored*

In the **Password** dialog box enter a new password for the private key → **next**
Give the key file a name **Xport1** (this is the name to be used on the new file created) → **next**
Select **Finish**
The Export Certificate Wizard box should state export successful → OK

9. Take a screen capture showing the export was successful

Navigate to the **C:\ User\User** folder

The certificate **Xport1** should be copied from the stored directory to a removable media for storage.

You can now copy the certificate from the stored directory to a removable media for storage (USB key).
Now delete the recovery agent certificate (To do this follow steps below)
Open the MMC to the Certificate manager Snap-in (Run → **certmgr.msc**)
When the Certificate Manager Window opens expand the Personal Folder and select the Certificate sub folder.
Select the first (top) certificate in the right hand panel and delete it
Select **Action → Delete**
Now as administrator view the contents of the file(s) in the info6080 folder (student1.txt)

Can the file contents be viewed?_____ Explain:_____

10. Take a screen capture showing the contents of the file – include the answers to the question above.

To restore the recovery key: Move to the directory where the key has been stored (USB key) Double click on the key and restore the key.