TMEP Project – Graphic Design Company

Assignment Overview

This project will test your ability to install, configure and administrate a Windows 11 system. You will need to demonstrate a variety of skills that you have acquired throughout the course. You will be using many of the procedures that you have learned to implement a solution in a typical business setting.

Materials Required

- VMware (Download virtual machine and you can add the hardware required in the project virtually on VMWare machine).
  - https://cutt.ly/Uwz59tHj (Download VMware Workstation Pro)
- Windows 11 Media Creation Tool and ISO Download
  - https://go.microsoft.com/fwlink/?linkid=2156295
- TeamViewer
  - https://download.teamviewer.com/download/TeamViewer_Setup_x64.exe

- Using the virtual environment in VMWare, add the following hardware:
  - A PC with a DVD drive that meets or exceeds the minimum hardware requirements of Windows 11 (VMware 17 PRO)
  - 1 SSD 500 GB minimum 3 HDD 2TB minimum
  - 3 HDD 2TB minimum

Submission Guidelines

- The project will be graded remotely on your computer using **TeamViewer**. When your project is complete, send your instructors your **partner ID** and **password**.
- Projects that are more than three days late will earn a maximum score of 60%
- For all projects submitted more than 5 days late, a grade of zero (0) will be applied.

Marking Scheme

You will be graded on:

Project component	Points
Installing Windows 11 PRO	25%
Setting up multiple partitions	15%
Creating and configuring user and group accounts	15%
Setting up local security policies	15%
Setting up a printing environment	15%
Implementing system fault-tolerance measures	15%
The total number of possible points is:	100%

Instructions:

You have been assigned to implement a Windows 11 system in a Graphic Design Manufacturing plant, where workers from several different departments will periodically require access to their respective data.

To separate the information stored for each department, a decision has been made to divide the system hard drive into four separate partitions. For additional security, different user and group accounts will be created and a local security policy will be configured. The system will also be used for printing documents, with various levels of access for groups of workers. Finally, to secure the system against hardware failures and software corruption, some fault-tolerance measures will need to be undertaken.

The instructions given below will guide you through the steps required to successfully implement the necessary solution.

1. **Step 1: Installing Windows 11**

   You have been given a PC with 4 empty hard drives. You will be installing Windows 11 using the Windows 11 Installation DVD and the local DVD drive.

   Start your installation by booting the system with the first setup disk. As you proceed, follow the steps listed below:

   - On the first hard drive, create a 400 GB main partition to host Windows 11 operating system files. Leave the remaining space on the hard drive unpartitioned for now.
   - In the networking portion of the installation, assume the computer is not connected to a network unless advised otherwise by your instructor.

2. **Step 2: Setting Up Multiple Partitions**

   - Use the second and third hard drives to create Mirrored Volumes of equal size. Name them: Design, Production and Supervisors.
   - Format them so that you can implement file system security on all three. Create simple text files in those folders and save them.
   - Set up the three partitions as mounted volumes connecting to three folders on the main 400GB partition. Name the three folders: Design, Production and Supervisors.

- Create a new partition on first drive. Name it: Drivers.
    - **Hint**: Use unpartitioned space on SSD Drive.
- Format the fourth hard drive labeled Backup.

3. Step 3: Creating and Configuring User and Group Accounts

- Create the users: Dora, Penelope and Sadie. These users should be able to use the system and save files, but they should not be able to install software or make changes to the system files and settings.
- Create the users: Derek, Phil and Scott. These users should be able to install software and make file and setting changes to the system, but they should not be able to read files belonging to other users.
- Create the users Adam and Ashley. They should have full administrative access to the system.
    - **Hint**: use an existing built-in group.
- Create four groups called: Design, Production, Supervisors and Administration. Place the users in the appropriate groups as outlined in table below:

Groups	Users
Design	Derek, Dora
Production	Phil, Penelope
Supervisors	Scott, Sadie
Administration	Adam, Ashley

- Set up folder permissions to grant members of the Design, Production, and Supervisors groups full access, except for full control, to their designated folders from step 2. A group should not have access to folders assigned to the other two groups (i.e.: A member from Production cannot have access to folders assigned to Design or Supervisors).
- Members of the Administration group should have full access, except for full control, to all three folders.

- Ensure that the same security is in place when accessing the contents of the folders directly through the corresponding partition drive letters, and also through the mounted volumes.

- **Note**: Access through the system group Users must not be available to these folders for this security scheme to be implemented correctly.

- Make Backup drive available only for members of the Administration group.

4. **Step 4: Setting Up Local Security Policies**

Implement the following policies on the system:

- Passwords must be changed every 30 days.

- Every user must employ a minimum of eight distinct passwords before reusing a previously used password.

- Any user logging into the system should be greeted with the following warning:

  "Warning: This computer system is the property of Graphic Design Company and for authorized use only."

- The login screen should not display the username of the most recent user who logged onto the system.

- Activate the Administrator Account and set the password as: Pa$$word.

5. **Step 5: Setting Up a Printing Environment**

- Create a local Lexmark XM1100 Series printer on USB1 and share it with the name: Main - Lexmark. Make it available between the hours of 7:00 a.m. and 8:30 p.m.

- Use the pscript.sep file to ensure that the printer inserts separator pages between print jobs. Prevent the printer from printing documents if the page setup and printer setup are incompatible.

- Configure printing permissions for all members belonging to the three designated groups—Design, Production, and Supervisors—to have access to print on this printer. Restrict printing access to only authorized individuals.
    - **Hint**: remove one of the default printing permissions
- Ensure that the two members of the Administration group have full control over the print jobs and the printer.

6. Implementing System Fault-Tolerance Measures

- Set up a Data Collector Sets alert whenever the %Processor Time counter goes above 60%.
- Ensure that an entry is recorded in the application event log when the alert is triggered.
- Create a backup schedule to full back up all components of the Mirrored Volumes at 11:00 p.m. every Saturday.
- Set backup destination file to: X:\ System Image (Where X:\ is the drive letter of backup hard drive).