**Module 2**

**{Installation and Maintenance of**

**Hardware and Its components}**

**User Management**

1. What is user management?

🡪 User management is the process of controlling access to resources within a system or application by creating, modifying, and deleting user accounts, assigning permissions, roles, and privileges, and ensuring security and compliance.

2. Why is user management needed?

🡪 User management is needed to control access to resources, ensure security, comply with regulations, streamline operations, facilitate collaboration, and maintain accountability.

3. Where can we access the user management?

🡪 User management functionalities are typically accessible through administrative interfaces within computer systems, applications, or platforms. This can include user management consoles, control panels, or settings sections within the software or platform itself.

4. What are the features of user management?Top of Form

🡪 User management features include account creation, modification, and deletion, assigning roles and permissions, enforcing password policies, enabling multi-factor authentication, auditing user activities, and facilitating user provisioning and deprovisioning.

**File and Folder Permission**

1. What is file folder permission?

🡪File folder permissions control who can access, modify, or delete files and folders on a computer system or network. They specify the level of access granted to users or groups, such as read, write, execute, or delete permissions.

2. What is the use of file and folder permission?

🡪 File and folder permissions control access to files and directories, ensuring that only authorized users or groups can view, modify, or delete them. They help maintain security, privacy, and data integrity within computer systems and networks.

3. wirte down the steps to give a folder read only permission.

🡪1. Right-click on the folder

2. Select "Propertie"

3. Go to the "Security" tab

4. Click "Edit"

5. Choose the user or group

6. Check "Read & execute"

7. Click "Apply" and then "OK"

4. Write a step to give a file only admin permission.

🡪 To give a file only admin permission on a Windows operating system:

1. Right-click on the file to modify

2. Select Properties

3. In the Properties window, go to the Security

4. Click on the Edit button

5. Select the user or group you want to restrict access to

6. Under the Allow column, check the box next to "Full control" to grant administrative permissions

7. Click "Apply" and then "OK" to save the changes

**Install OS**

1. What is OS?

🡪"OS" stands for "Operating System." It is a software program that manages computer hardware and provides common services for computer programs. The operating system acts as an intermediary between users and the computer hardware, enabling users to interact with the computer without needing to understand its internal workings. Examples of operating systems include Windows, macOS, Linux, and Unix.

2. What are the types of OS?

🡪1. Single-User, Single-Tasking

2. Single-User, Multi-Tasking

3. Multi-User

4. Real-Time

5. Distributed

6. Embedded

**Clean Install**

1. What is clean install?

🡪 Installing an operating system or software on a computer or device "cleanly" means that no prior data or settings are kept. In order to ensure a fresh start free of traces from earlier installations, it entails wiping the current data on the storage device and installing the operating system or software from scratch.

2. What is the process for clean install?

🡪Backing up data, formatting the disk, installing the operating system or software, adjusting settings, installing drivers and updates, restoring data, and confirming the installation are all steps in the process of a clean install.

3. what are the benefits of clean install?

🡪 The benefits of a clean install include improved system performance, stability and the removal of unnecessary clutter and old configurations.

**Upgrade installation**

1.What is upgrade installation?

🡪Installing an operating system or software update over an existing version while keeping user data, preferences, and programs intact is known as an upgrade installation.

2.What is the benefit of upgrade installation?

🡪 The benefit of upgrade installation is the retention of user data, settings, and applications while transitioning to a newer version of the operating system or software.

3.Write down the steps of upgrade installation.

🡪1. Launching the installation process.

2. Selecting the upgrade option.

3. Following prompts to complete the installation.

4. Allowing the installer to update the existing system files.

5. Verifying successful installation and retaining user data, settings, and applications.

**Partition & Formatting**

1. What is partitioning?

🡪Partitioning is the process of dividing a physical storage device, such as a hard drive or SSD, into multiple logical sections called partitions. Each partition functions as a separate unit, enabling users to organize and manage their data more effectively.

2. What is partition?

🡪 A partition is a logical division of a storage device, such as a hard drive or SSD, into separate sections. Each partition functions as an independent unit with its own file system, allowing users organize or store data separately from other partitions or same device.

3. What is format?

🡪Formatting is the process of preparing a storage device, hard rive, SSD, or USB flash drive, for data storage by creating a file system on it. Formatting erases any existing data on the device and sets up the necessary structures for organizing and storing files.

**Transferring Files**

1. What is transferring Files?

🡪 Transferring files involves moving data from one location to another, whether between devices, computers, or networks.

2. What are the ways of transferring files?

🡪 File transfers can be done via Bluetooth, NFC, USB, network, email attachments, cloud storage, FTP, Bluetooth, QR codes, P2P sharing, and file-sharing applications.

3. How do we transfer files from one system to another?

🡪 Files can be transferred from one system to another through various methods such as USB transfer, network sharing, cloud storage, email attachments, Bluetooth, NFC, QR codes, or file-sharing apps.

4. Types of file transferring media.🡪 Types of file transferring media include physical media, network, internet, wireless, and cloud storage services.

**Administrative tools**

1. What are administrative tools?

🡪 Software programs or utilities known as administrative tools are made to help with the management, configuration, and upkeep of servers, networks, and computer systems. They simplify processes including troubleshooting, system monitoring, user management, performance optimization, and performance optimization, enabling effective IT infrastructure management and operation.

2. What is the use of administrative tools?

🡪Administrative tools are used to manage and configure various aspects of a computer system, including system settings, user accounts, hardware devices, and network configurations.

3. List out the administrative tools.

🡪1. Control Panel

2. Disk Management

3. Task Manager

4. Device Manager

5. Computer Management

6. System Preferences

7. Terminal

8. Network Utility

9. Activity Monitor

10. Users & Groups

4. What is disk management tools.🡪 Disk Management tools are software applications or utilities used to manage and manipulate storage devices connected to a computer. They enable users to perform tasks partitioning, formatting, resizing, and assigning drive letters to storage devices hard drives, SSD, and USB drives.

**Windows Feature.**

1. What is windows features?

🡪Windows features are extra features or parts that can be added to an existing Windows operating system to increase its functionality. These features consist of programs, services, and tools that the user can add as needed; they might not be installed by default.

2. List out the windows features.

🡪1. Internet Information Services

2. Telnet Client

3. Hyper-V

4. .NET Framework

5. Windows Subsystem for Linux

6. Remote Server Administration Tools

7. Windows PowerShell

8. Windows Media Player

9. Windows Defender Antivirus

10. BitLocker Drive Encryption

3. What is the use of IIS?🡪 IIS is a web server software developed by Microsoft. It is used to host and manage websites and web applications on Windows servers.

**Backup & Restore**

1. What is backup?

🡪Backup is the process of creating copies of important data to protect against data loss. To ensure that data can be restored in the event of an accident, hardware failure, or other unanticipated circumstance, these copies can be kept in a different place or on alternative storage media.

2. What is Restore?

🡪Restore refers to the process of retrieving and returning backed-up data to its original location or to a different location after it has been lost, corrupted, or accidentally deleted.

3. What is the need of backup

🡪 The need for backup arises from the importance of data protection. Backup ensures that critical data is preserved and can be recovered in case of accidental deletion, hardware failure, data corruption, cyber attacks, or natural disasters. It helps to preserve personal data integrity and business continuity while acting as a safety net against loss.

4. What are the tools of backup?

🡪 Backup tools include Windows Backup and Restore, Time Machine, Acronis True Image, EaseUS Todo Backup, Carbonite, Backblaze, Veeam Backup & Replication, Veritas NetBackup, Duplicati, and Rsync.

5. How do we restore?

🡪 To restore, use a backup tool or service to retrieve backed-up data and return it to its original location or to a specified location.

6. How to create a restore point?

🡪 1. Open the Start menu.

2. Type "Create a restore point" and press Enter.

3. In the System Properties window, click the "System Protection" tab.

4. Click the "Create" button.

5. Enter a description for the restore point and click "Create."

**Disk Management**

1. What is Disk Management?

🡪 Disk Management is a built-in utility in Windows operating systems that allows users to manage their hard drives and storage devices. It enables users to view, create, delete, format, and manage disk partitions.

2. What is the use of Disk Management?

🡪The primary use of Disk Management is to manage disk partitions on a computer's hard drive or storage device. It allows users to allocate and reallocate disk space, format disks, create new partitions, extend or shrink existing partitions, change drive letters, and set partition attributes.

3. What are the merits of Disk Management tool?

🡪 Some merits of the Disk Management tool include:

- User-friendly interface: It provides a simple and intuitive interface for managing disk partitions.

- Built-in utility: As a built-in tool in Windows, it eliminates the need for third-party partition management software.

- Comprehensive features: Disk Management offers a wide range of features for managing disk partitions, making it suitable for most disk management tasks.

- Compatibility: It works with various disk formats, including NTFS, FAT32, and exFAT, ensuring compatibility with different storage devices

1. Where can we find the Disk Management tool?

🡪 The Disk Management tool can be found in the Windows Administrative Tools. To access it:

- Open the Control Panel.

- Navigate to Administrative Tools.

- Click on Computer Management.

- In Computer Management, select Disk Management under the Storage section.

2. List out the operations we can do with the Disk Management tool

🡪 Operations that can be performed with the Disk Management tool include:

- Creating new partitions

- Deleting existing partitions

- Formatting partitions

- Changing drive letters

- Extending partitions

- Shrinking partitions

- Assigning or changing partition attribut

1. Practical to create a new partition with Disk Management tool:

🡪 To create a new partition with Disk Management:

- Open Disk Management as described in the Intermediate level.

- Right-click on the unallocated space on the disk where you want to create the new partition.

- Select "New Simple Volume" from the context menu.

- Follow the wizard to specify the partition size, assign a drive letter, choose a file system, and format the partition.

2. Practical to convert from MBR to GPT using Disk Management tool:

🡪 Converting from MBR to GPT involves data loss, so ensure you have backups. To do this:

- Open Disk Management.

- Right-click on the disk you want to convert.

- Select "Convert to GPT Disk."

3. Practical to create a new partition from an existing partition:

🡪 To create a new partition from an existing partition:

- Open Disk Management.

- Right-click on the existing partition you want to shrink to create space for the new partition.

- Select "Shrink Volume" and follow the wizard to specify the amount of space to shrink.

- Once the shrink process is complete, right-click on the unallocated space and select "New Simple Volume" to create a new partition.

**Device Management**

1. What is Device Management?

🡪 Device Management refers to the process of managing and controlling hardware devices connected to a computer system or network. It involves tasks such as installing, configuring, monitoring, updating, and troubleshooting devices to ensure their proper functioning.

2. What is the need for Device Management?

🡪 The need for Device Management arises from the increasing complexity and diversity of hardware devices used in computer systems. It ensures that devices are correctly installed, configured, and maintained to optimize performance, reliability, and security. Without proper device management, systems may experience compatibility issues, performance degradation, security vulnerabilities, and difficulties in troubleshooting hardware-related problems.

3. What are the benefits of Device Management?

🡪Some benefits of Device Management include:

- Improved system performance and reliability: Properly managed devices contribute to the overall stability and efficiency of computer systems.

- Enhanced security: Device Management helps ensure that devices are configured securely, reducing the risk of security breaches and unauthorized access.

- Simplified administration: Centralized management of devices streamlines administrative tasks such as device installation, configuration, and updates.

- Better resource utilization: Effective Device Management helps optimize resource allocation, ensuring that hardware devices are used efficiently.

- Reduced downtime: Proactive monitoring and maintenance of devices minimize the likelihood of hardware failures and downtime.

1. Where can we access Device Management?

🡪 Device Management can be accessed through the Device Manager utility in the Windows operating system. To access Device Manager:

- Right-click on the Start button.

- Select "Device Manager" from the context menu.

2. List out the devices connected to Device Management.

🡪 The devices connected to Device Management typically include:

- Display adapters

- Network adapters

- Sound, video, and game controllers

- Printers and scanners

- Disk drives

- Universal Serial Bus controllers

- Human Interface Devices

- Imaging devices

- Ports

1. Practical to add a device with Device Management tool:

🡪 To add a device using Device Manager:

- Open Device Manager.

- Right-click on the category under which the new device should be added.

- Select "Scan for hardware changes" from the context menu. Windows will search for new devices and automatically install them if drivers are available.

2. Practical to delete a driver from the Device Management tool:

🡪 To delete a driver using Device Manager:

- Open Device Manager.

- Locate the device whose driver you want to delete.

- Right-click on the device and select "Uninstall device" from the context menu.

- Follow the on-screen prompts to uninstall the driver. Physical security

**Physical security**

1. Why is physical security needed?

🡪 Physical security is essential to protect physical assets, including people, hardware, software, networks, and data, from physical threats such as theft, vandalism, natural disasters, and unauthorized access. It ensures the safety and integrity of resources and prevents potential damage or loss.

2. What is physical security?

🡪Physical security refers to the measures and mechanisms implemented to safeguard physical assets, facilities, and resources from unauthorized access, damage, or theft. It encompasses various strategies, policies, and technologies designed to protect physical infrastructure, personnel, and information assets.

1. List out the ways of physical security:

🡪 Physical security methods include:

- Perimeter security: Fencing, gates, walls, and barriers to control access to facilities.

- Access control: Locks, keys, access cards, biometric authentication, and security guards to regulate entry to buildings and restricted areas.

- Surveillance: Video cameras, motion sensors, and alarms to monitor and detect unauthorized activities.

- Lighting: Adequate lighting to deter intruders and enhance visibility.

- Security patrols: Regular patrols by security personnel to monitor premises and respond to incidents.

- Intrusion detection systems (IDS): Sensors and alarms to detect unauthorized entry or breaches.

- Environmental controls: Fire suppression systems, temperature control, and humidity control to protect against environmental hazards.

- Backup power: Uninterruptible Power Supply (UPS) systems and generators to maintain power during outages.

- Secure storage: Safes, vaults, and secure cabinets to store valuable assets and sensitive information.

- Security policies: Establishing policies and procedures for access control, visitor management, and incident response.

2. How to protect the system from malfunctioning due to electrical fluctuation?

🡪 To protect systems from malfunctioning due to electrical fluctuation, you can implement the following measures:

- Use surge protectors: Install surge protectors or uninterruptible power supply (UPS) systems to regulate voltage and protect equipment from power surges and spikes.

- Voltage regulators: Use voltage regulators to stabilize voltage levels and prevent damage caused by fluctuations.

- Grounding: Ensure proper grounding of electrical systems to minimize the risk of electrical shocks and equipment damage.

- Isolation transformers: Install isolation transformers to protect equipment from electrical noise and interference.

- Backup power: Implement backup power solutions such as generators or battery backups to maintain power during outages and prevent data loss or system downtime.

- Regular maintenance: Conduct regular inspections and maintenance of electrical systems to identify and address potential issues before they cause damage.

- Training and awareness: Educate users about the risks of electrical fluctuations and the importance of following best practices to protect equipment and data.

**Firewall setting**

1. What is a firewall?

🡪A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and protect against cyber threats.

2. Why is a firewall needed?

🡪Firewalls are needed to enhance the security of computer networks by:

- Filtering incoming and outgoing traffic to prevent unauthorized access and protect against cyber attacks such as malware, viruses, and hacking attempts.

- Enforcing security policies to control network communication and ensure compliance with organizational guidelines.

- Monitoring network traffic for suspicious activities and alerting administrators to potential security breaches.

- Safeguarding sensitive data and resources from unauthorized access or disclosure. - Providing a layer of defense against various network threats and vulnerabilities, thereby improving overall network security

1. What are the features of a firewall?

🡪The features of a firewall typically include: - Packet filtering: Examining network packets and allowing or blocking them based on predefined rules. - Stateful inspection: Tracking the state of active connections and allowing only legitimate traffic

- Application layer filtering: Analyzing network traffic at the application layer to detect and block specific types of traffic or applications.

- VPN support: Facilitating secure remote access through Virtual Private Networks (VPNs) by encrypting data and authenticating users. - Intrusion detection and prevention: Identifying and blocking suspicious or malicious network activity to prevent security breaches.

- Logging and reporting: Recording firewall activities and generating reports for analysis and aiding purposes.- High availability and scalability: Ensuring uninterrupted network connectivity and supporting the expansion of network infrastructure as needed.

2. Describe types of firewall:

🡪 Types of firewalls include:

- Packet-filtering firewall: Examines packets based on predefined rules, such as source/destination IP addresses, ports, and protocols, and allows or blocks them accordingly.

- Stateful inspection firewall: Tracks the state of active connections and makes decisions based on the context of the traffic, offering better security than packet-filtering firewalls.

- Proxy firewall: Acts as an intermediary between internal and external networks, forwarding requests on behalf of clients and filtering traffic at the application layer.

- Next-generation firewall (NGFW): Combines traditional firewall functionality with Advanced features such as intrusion prevention, application awareness, and deep packet inspection to provide comprehensive security.

- Unified Threat Management (UTM) firewall: Integrates multiple security features, including firewall, antivirus, intrusion detection/prevention, content filtering, and VPN, into a single appliance or software solution.

1. Practical to allow AnyDesk through firewall:

🡪Open Windows Firewall settings.

- Click on "Allow an app or feature through Windows Firewall."

- Click on "Change settings" and then "Allow another app."

- Browse and select the AnyDesk executable file (usually located in Program Files).

- Click "Add," then ensure both public and private checkboxes are checked for AnyDesk.

- Click "OK" to save the changes.

2. Practical to turn off the services of the firewall:

🡪 Open Windows Firewall settings.

- Click on "Turn Windows Defender Firewall on or off" in the left panel.

- Select "Turn off Windows Defender Firewall" for both private and public network settings.

- Click "OK" to apply the changes.

3. Practical to block IP Messenger from accessing the network

🡪 Open Windows Firewall settings.

- Click on "Advanced settings" in the left panel.

- In the inbound or outbound rules section, create a new rule to block a program.

- Browse and select the IP Messenger executable file.

- Choose to block the connection and apply the rule to both public and private networks.

- Save the rule and exit the firewall settings.