

Desktop Support Engineer / System Support Engineer Module Objective

S.No.	Days	Content	Explanation	Time Duration	Remark
1	Day 1	IT Support	Introduction of IT support and related keywords like System, OS, BIOS, Boot	60 min	
2	Day 2	Boot & BIOS	Process of Booting, types, POST, Boot Menu, Boot BIOS/UEFI, Devices.	60 min	
3	Day 3	Hardware Component	Motherboard, Processor, RAM, ROM, Hard Disk, SSD,	60 min	
4	Day 4	Hardware Component	Motherboard, Processor, RAM, ROM, Hard Disk, SSD,	60 min	
5	Day 5	Power Supply	SMPS, PG	60 Min	
6	Day 6	Number System	Binary, Hexadecimal	60 Min	
7	Day 7	Number System	Binary, Hexadecimal	60 Min	
8	Day 8	Processor	Clock Speed, FSB, Case Memory,	60 min	
9	Day 9	RAM	Frequency, Type	60 min	
10	Day 10	Hard Disk, SSD, RAID, SCSI	Storage, Permanent Memory	60 min	
11	Day 11	File System	FAT, NTFS	60 min	
12	Day 12	Disk Management	Diskpart, MBR, GPT	60 min	
13	Day 13	Operating System	Windows, Linux, MAC	60 min	
14	Day 14	Operating System	Windows, Linux, MAC	60 min	
15	Day 15	Operating System	Windows, Linux, MAC	60 min	
16	Day 16	Operating System	Windows, Linux, MAC	60 min	

17	Day 17	Device Driver	Audio, Video, Network installation, update, uninstallation	60 min	
18	Day 18	Device Driver	Audio, Video, Network installation, update, uninstallation	60 min	
19	Day 19	Application	Installation, Uninstallation, Update, location	60 min	MS Office, PDF, Photo
20	Day 20	Application	Installation, Uninstallation, Update, location	60 min	Brouser, ZIP,
21	Day 21	Application	Installation, Uninstallation, Update, location	60 min	Remote Application
22	Day 22	Application	Installation, Uninstallation, Update, location	60 min	Meeting Application
23	Day 23	Application	Installation, Uninstallation, Update, location	60 min	SQL, Oracal, Python, JAVA
24	Day 24	Application	Installation, Uninstallation, Update, location	60 min	Linux Software
25	Day 25	Controle panel	Time, Date, Language, Power Setting	60 min	
26	Day 26	Controle panel	Time, Date, Language, Power, Display Setting	60 min	
27	Day 27	Task manager	Process, Utilization	60 min	
28	Day 28	Command	Run, cmd, Dir, Attributes	60 min	
29	Day 29	Registry	regedit	60 min	
30	Day 30	Local Policy	user & permission	60 min	
31	Day 31	Services	start & stop	60 min	
32	Day 32	Disk cleanup	temp delete	60 min	
33	Day 33	System Properties	Computer name, workgroup & Domain	60 min	
34	Day 34	Internet	IP configuration	60 min	
35	Day 35	Wi-Fi	SSID	60 min	
36	Day 36	Outlook		60 min	
37	Day 37	One Drive		60 min	
38	Day 38	Active Directory		60 min	
39	Day 39	Domain		60 min	
40	Day 40	Printer	Laser, DMO, Inkjet	60 min	
41	Day 41	Printer	Driver, Installation	60 min	
42	Day 42	Printer	Issue	60 min	
43	Day 43	Scanner		60 min	
44	Day 44	Audio		60 min	
45	Day 45	System performance		60 min	
46	Day 46	Network	LAN, WAN, MAN	60 min	
47	Day 47	Networking	Workgroup, Domain	60 min	
48	Day 48	Media	UTP, Fiber	60 min	

49	Day 49	Cabling		60 min	
50	Day 50	IEEE	802.3, 802.111	60 min	
51	Day 51	Topology	Campus, Data Center	60 min	
52	Day 52	Protocol	TPC/IP	60 min	
53	Day 53	IP Address	Ipv4, 32 bit	60 min	
54	Day 54	MAC	Physical address	60 min	
55	Day 55	Troubleshoot	Display, Power, RAM	60 min	
56	Day 56	Troubleshoot	Disk, Partition	60 min	
57	Day 57	Troubleshoot	Operating System	60 min	
58	Day 58	Troubleshoot	Software, Application	60 min	

Module 1 – Course Overview

Welcome to the first module of the **Desktop Support Engineer Training Program**. This introductory module sets the foundation for your learning journey by outlining the course goals, defining the role of a Desktop Support Engineer, identifying the key skills you'll need, and walking you through the basic tools and environment setup.

Course Objectives

By the end of this course, you will:

- Understand the core responsibilities of a Desktop Support Engineer.
- Gain practical knowledge of troubleshooting hardware and software issues.
- Learn how to support end-users in a corporate or organizational environment.
- Become familiar with the tools and technologies used in desktop support.
- Be equipped to manage and maintain user workstations, operating systems, and basic networking issues.
- Prepare for industry-recognized certifications or entry-level roles in IT support.

Role of a Desktop Support Engineer

A **Desktop Support Engineer** is the first line of defense in an organization's IT infrastructure. This role is crucial for maintaining smooth daily operations by ensuring that all end-user systems are functional and efficient.

Key responsibilities include:

- Installing, configuring, and maintaining desktop hardware and software.
- Responding to user queries and resolving technical issues in-person or remotely.
- Managing operating systems, applications, and peripheral devices.
- Setting up new systems for users and ensuring compliance with company standards.
- Documenting issues and solutions for future reference.
- Collaborating with other IT teams to escalate or resolve more complex issues.

This role requires both technical proficiency and excellent communication skills, as you'll be interfacing directly with users.

Skills Required

To become a successful Desktop Support Engineer, you'll need a combination of technical and soft skills. Here are the key areas to focus on:

Technical Skills:

- Knowledge of **operating systems** (Windows, macOS, Linux).
- Understanding of **hardware components** and troubleshooting.
- Familiarity with **network basics** (IP, DNS, DHCP, LAN/WAN).
- Experience with **software installation and configuration**.
- Use of **remote support tools** (e.g., TeamViewer, AnyDesk, RDP).
- Working with **Active Directory** and user account management.
- Basic scripting or command line (PowerShell, CMD, Bash – optional but helpful).

Soft Skills:

- **Problem-solving ability** – thinking logically and troubleshooting effectively.
- **Customer service orientation** – helping users in a patient and friendly manner.
- **Communication skills** – clearly explaining technical solutions to non-technical users.
- **Time management** – handling multiple support tickets or tasks efficiently.

Tools & Environment Setup

Before diving into hands-on tasks, it's important to set up your working environment. Here's what you need to get started:

Hardware Requirements:

- A reliable PC or laptop with at least:
 - 8 GB RAM
 - 100 GB free disk space
 - Intel i5 processor (or equivalent)
- Internet connection for remote support tools and updates

Software Requirements:

- **Virtualization software** (e.g., VirtualBox or VMware Workstation)
- Installation ISOs for:
 - Windows 10/11
 - Linux (Ubuntu or any preferred distro)
- **Remote access tools** (TeamViewer, AnyDesk, etc.)
- **IT support ticketing system** (e.g., Freshdesk, Spiceworks – optional for demo)
- **Productivity tools** (Microsoft Office, Google Workspace)

Recommended Accounts & Resources:

- Microsoft account for Windows OS downloads and tools
- Google account for collaborative tools

- GitHub account (optional – for storing documentation or scripts)
- Access to forums and knowledge bases (e.g., Spiceworks Community, Reddit IT subs, TechNet)

This module gives you a roadmap of what to expect in the course and ensures you're fully prepared for the hands-on modules ahead. As we move forward, you'll begin developing the real-world skills and confidence needed to thrive as a Desktop Support Engineer.

Module 2 – System Installation & Setup

In this module, we dive into the core task of every Desktop Support Engineer: installing and configuring an operating system. You'll learn how to install **Windows 10/11**, set up the system BIOS/UEFI, partition disks, and install essential drivers and updates. This module combines theory with hands-on practice to ensure you are confident performing installations on physical or virtual machines.

1. Windows 10/11 Installation

Installing Windows is a fundamental skill. This process includes preparing installation media, booting the system, and following the installation wizard.

Steps Overview:

1. **Create Installation Media:**
 - Use the **Windows Media Creation Tool** to create a bootable USB drive or ISO image.
2. **Boot from Installation Media:**
 - Insert USB and boot from it via BIOS/UEFI.
 - Choose your language, keyboard layout, and version of Windows.
3. **Follow the Installation Wizard:**
 - Select the installation type: **Upgrade** or **Custom** (for clean installs).
 - Choose the target disk and partition (see next section).
 - Allow the OS to install and restart as needed.
4. **Initial Setup:**
 - Create a local or Microsoft user account.
 - Set up privacy preferences and network settings.

Tip: Always verify system requirements and ensure system compatibility before installation.

2. BIOS/UEFI Configuration

Before installing the OS, you may need to adjust settings in the **BIOS/UEFI**. This firmware interface controls low-level system settings.

Accessing BIOS/UEFI:

- Press **DEL**, **F2**, or another key during startup (varies by manufacturer).

Key Settings to Configure:

- **Boot Order:**
 - Ensure the USB/DVD is set as the first boot device for installation.
- **Secure Boot:**
 - May need to be disabled for custom installations or older OS versions.
- **UEFI vs Legacy Mode:**
 - Modern systems use **UEFI**. Ensure your bootable media supports the mode you're using.

Note: Incorrect BIOS/UEFI settings can prevent booting. Always document changes.

3. Disk Partitioning

Disk partitioning organizes the hard drive into usable sections for the OS and data.

During Installation:

You'll be prompted to select where to install Windows.

- **Delete existing partitions** if doing a clean install.
- **Create new partitions:**
 - **System Reserved** (automatically created)
 - **Primary partition** for Windows
 - Optional: additional partitions for data

Types of Partition Schemes:

Scheme	Description
MBR (Master Boot Record)	Older format; supports up to 2 TB
GPT (GUID Partition Table)	Modern format; required for UEFI; supports large drives

Best Practice: Use GPT with UEFI for Windows 10/11 installs.

4. Drivers & Updates

After installing Windows, it's essential to install the correct **drivers** and apply system **updates** to ensure full hardware functionality.

Drivers to Install:

- **Chipset drivers**
- **Display adapter (GPU)**
- **Network drivers (Wi-Fi/Ethernet)**
- **Audio drivers**
- **Touchpad or peripheral drivers**

Where to Find Drivers:

- **Manufacturer's website** (Dell, HP, Lenovo, etc.)
- **Windows Update** (Settings > Windows Update)

Steps to Update Windows:

1. Go to **Settings > Update & Security > Windows Update**
2. Click **Check for updates**
3. Install **all pending updates**, including optional ones if hardware-related

Important: Restart after installing drivers and updates to ensure proper installation.



Lab: Install Windows OS and Configure User Account

In this hands-on lab, you will:

1. Boot into a virtual machine (VM) using a Windows 10 or 11 ISO.
2. Perform a clean installation of the operating system.
3. Configure BIOS/UEFI settings if necessary.
4. Partition the disk during installation.
5. Create a local user account.
6. Install critical drivers and check for Windows updates.

Checklist:

- ☒ Boot VM and access installation media
- ☒ Perform installation using correct partition scheme
- ☒ Set up user account and password
- ☒ Install at least one essential driver
- ☒ Run Windows Update



Instructor Note:

- **Always demonstrate using a virtual machine** (e.g., VirtualBox, VMware) to keep the learning environment safe and isolated.
- Emphasize **UEFI vs Legacy boot**, partitioning choices, and handling driver installations.
- Allow learners to repeat the installation multiple times for confidence.

Module 3 – User & System Management

This module focuses on the daily tasks that Desktop Support Engineers perform to ensure user access, system stability, and optimal performance. You'll learn how to manage user accounts and permissions, utilize key system tools like **Device Manager**, and optimize system performance through various settings.

1. User Accounts, Groups & Permissions

Properly managing user accounts is vital for maintaining security and ensuring users have the right level of access to perform their work.

User Account Types:

- **Local Accounts:**
 - Created and stored on the individual machine.
 - Used in small environments or standalone systems.
- **Domain Accounts:**
 - Managed through **Active Directory (AD)** in enterprise environments.
 - Centralized authentication across multiple systems.

**Note:**

Local users are limited to one machine. Domain users can log into any system on the domain, making them ideal for corporate environments.

User Groups:

Groups simplify permission management by applying access rules to multiple users at once.

- **Common Built-in Groups:**

- **Administrators:** Full system control.
- **Standard Users:** Limited access.
- **Guests:** Temporary access (disabled by default).
- **Remote Desktop Users:** For users who need remote access.

Managing Accounts (GUI):

- **Settings > Accounts > Family & Other Users**
- **Control Panel > User Accounts**

Managing Accounts (Command Line):

```
net user username password /add
```

```
net localgroup administrators username /add
```

Permissions:

Manage **file and folder access** using NTFS permissions:

Permission	Description
Full Control	Read/write/edit/delete everything
Modify	Read/write/edit
Read/Execute	Open files, run programs
Read	View files only
Write	Add/edit content

2. Device Manager

Device Manager is a key tool for managing hardware components.

Key Functions:

- View all connected hardware
- Check driver status
- Update or roll back drivers
- Disable or uninstall malfunctioning devices

Common Use Cases:

- Fixing driver issues (e.g., network, display, audio)
- Diagnosing hardware failures
- Checking hardware status after OS installation



Access:

Right-click **Start > Device Manager**

3. Control Panel & Settings

Windows offers two main interfaces for system management:

Control Panel (Legacy):

Still useful for:

- User accounts
- Administrative tools
- Device & printer settings

- Programs and features (uninstall software)

Settings App (Modern):

Useful for:

- System preferences (display, sound, power)
- Accounts
- Privacy & security
- Updates

📌 Both interfaces are still in use — familiarize yourself with both for complete support coverage.

4. System Performance Optimization

Slow systems are a common user complaint. As a Desktop Support Engineer, you'll need to identify and resolve performance issues.

Steps to Optimize System Performance:

1. **Disable Unnecessary Startup Programs:**
 - Task Manager > Startup tab
2. **Check for Background Processes:**
 - Task Manager > Processes tab
3. **Adjust Visual Effects:**
 - System Properties > Advanced > Performance Settings
4. **Clean Up Temporary Files:**
 - Use **Disk Cleanup** or **Storage Sense**
5. **Update Drivers and Windows:**
 - Keep systems patched and secure
6. **Check for Malware or Bloatware:**
 - Use Windows Defender or trusted third-party tools

Lab: Create Users and Apply Permissions

In this lab, you will:

1. Create two local user accounts: one admin, one standard.
2. Add one user to a group and assign permissions to a folder.
3. Log in as the standard user and verify access.
4. Restrict access to specific system tools using group settings.
5. Check Device Manager for missing drivers and update them.

✅ Deliverables:

- Screenshots of created accounts and group assignments
- Folder with customized permissions
- Notes on any driver issues resolved via Device Manager

Instructor Note:

- Discuss and demonstrate the **difference between local and domain users**:
 - Set up a simulated domain environment (optional) or explain AD conceptually.
- Use real-world examples:
 - “Finance” user group with limited access to sensitive files.
- Encourage students to explore **Device Manager** to identify common driver-related issues (e.g., yellow warning icons).

Module 4 – Networking Fundamentals

Networking is the backbone of IT operations. As a Desktop Support Engineer, you must understand how computers connect, communicate, and resolve network issues. In this module, we'll explore core networking concepts, configurations, and troubleshooting methods you'll use daily.

1. IP Addressing & Subnetting

What is an IP Address?

An **IP address** (Internet Protocol address) is a unique identifier assigned to each device on a network.

- **IPv4 Example:** 192.168.1.10
- **IPv6 Example:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Types of IP Addresses:

Type	Description
------	-------------

Static IP	Manually assigned to a device. Does not change.
------------------	---

Dynamic IP	Automatically assigned by DHCP. Can change over time.
-------------------	---

Private vs Public IPs:

- **Private IPs (used in LANs):**
192.168.x.x, 10.x.x.x, 172.16.x.x – 172.31.x.x
- **Public IPs (used on the internet):** Assigned by ISPs

Subnetting (Basic Overview):

Subnetting divides large networks into smaller, manageable sub-networks.

- **Subnet Mask defines the range:**
 - Example: 255.255.255.0 = 256 total IPs in subnet

2. DNS, DHCP, Gateway

DNS (Domain Name System):

- Translates domain names (e.g., www.google.com) into IP addresses.
- If DNS fails, you can't access websites by name.

DHCP (Dynamic Host Configuration Protocol):

- Automatically assigns IP addresses, subnet masks, gateway, and DNS to devices.
- Reduces manual network configuration.

Default Gateway:

- The gateway is the router or firewall that connects your local network to other networks, such as the internet.
- Usually ends in .1 (e.g., 192.168.1.1)

3. LAN / WAN Configuration

LAN (Local Area Network):

- Covers small geographical area (e.g., office, building).
- Devices communicate directly.
- Uses private IP addresses.

WAN (Wide Area Network):

- Covers large areas (cities, countries).
- Connects multiple LANs.
- Uses public IPs and leased lines.

Basic Configuration Steps:

- Assign IP (static or via DHCP)
- Set subnet mask, gateway, and DNS
- Test connectivity with tools like ping or ipconfig

4. Network Troubleshooting

Common Issues:

- No internet or limited connectivity
- IP conflict
- DNS resolution failure
- Slow or unstable network

Tools to Use:

Tool	Command	Purpose
ipconfig	ipconfig /all	View IP, gateway, DNS settings
	ipconfig /release / renew	Refresh IP address
ping	ping 8.8.8.8	Test internet reachability
nslookup	nslookup google.com	Check DNS resolution
tracert	tracert google.com	Trace path to destination
netstat	netstat -an	Show active network connections

 **Tip:** If ping works with IP but not domain, it's likely a DNS issue.

Lab: Assign Static IP, Join Domain, Ping Test

Objective:

Practice basic network setup and testing connectivity.

Tasks:

1. Assign a Static IP:
 - Go to Control Panel > Network & Sharing Center > Adapter Settings
 - Right-click Ethernet/Wi-Fi > Properties > IPv4
 - Set:
 - IP Address: 192.168.1.100
 - Subnet Mask: 255.255.255.0
 - Gateway: 192.168.1.1
 - DNS: 8.8.8.8
2. Join a Domain (if available):
 - Right-click This PC > Properties > Change Settings
 - Under "Computer Name", click Change
 - Enter domain name (e.g., corp.local)
 - Provide domain credentials to join
3. Ping Test:
 - Open Command Prompt
 - Run:

ping 8.8.8.8 # Test internet

ping domain.com # Test DNS resolution

ping 192.168.1.1 # Test gateway

Instructor Note:

- Explain why static IPs are useful (e.g., printers, servers).
- If no domain environment is available, simulate with hostnames and explain how domains function in enterprise networks.
- Discuss real-world scenarios: user unable to access the internet, IP conflict, etc.
- Demonstrate use of tools like ipconfig and ping live.

Module 5 – Troubleshooting & Maintenance

Overview

In this module, you'll learn how to identify, troubleshoot, and resolve common hardware and software issues that affect system performance. You'll also get hands-on experience using key diagnostic tools like Command Prompt (CMD) and Event Viewer to diagnose and analyze system problems.

1. Common Hardware & Software Issues

Understanding the typical problems users encounter is the first step to effective troubleshooting. These issues generally fall into two categories:

Hardware Issues

- **Faulty RAM:** Causes random reboots or application crashes.
- **Overheating:** Often due to dust buildup or failing fans.
- **Hard Drive Failures:** Result in data loss or system boot failures.
- **Peripheral Malfunctions:** Mouse, keyboard, or printer not responding due to driver or connection issues.

Software Issues

- **Corrupted System Files:** Can cause unexpected errors or crashes.
- **Driver Conflicts:** Often occur after hardware changes or updates.
- **Malware Infections:** Lead to poor performance, pop-ups, or security breaches.
- **Failed Updates:** OS or application updates that do not install correctly can cause instability.

2. Specific Problems: Causes & Solutions

🔵 Blue Screen of Death (BSOD)

- **Cause:** Critical system errors such as hardware failure or incompatible drivers.
- **Solution:** Use Event Viewer to analyze crash logs; update or roll back drivers; run memory diagnostics.

🕒 Slow Boot Times

- **Cause:** Too many startup programs, fragmented hard drive, or outdated firmware.
- **Solution:** Disable unnecessary startup apps, defragment hard drive (HDDs), update BIOS/UEFI.

🌐 Connectivity Issues

- **Cause:** Incorrect IP settings, driver issues, router configuration errors.
- **Solution:** Use ipconfig, ping, or tracert in CMD to diagnose; reinstall network adapter driver; reset router settings.

3. Diagnostic Tools



Command Prompt (CMD)

Useful commands for troubleshooting:

- ipconfig /all – Displays network settings.
- ping [address] – Tests connectivity.
- sfc /scannow – Scans and repairs corrupted system files.
- chkdsk – Checks for hard drive errors.
- tasklist & taskkill – Manage running processes.



Event Viewer

Event Viewer provides detailed logs of system, application, and security events.

- **Accessing:** Press Win + R, type eventvwr, press Enter.
- **Logs to Check:**
 - **System:** Hardware-related errors and boot issues.
 - **Application:** Crashes or issues with installed apps.
 - **Security:** Login attempts and permissions issues.
- **Filters:** Use custom views to isolate critical or error-level events.



Lab: Troubleshoot Sample Error Using Event Viewer

Objective:

Identify the root cause of a system crash using Event Viewer and suggest a resolution.

Scenario:

A user reports frequent system crashes with a blue screen. Your task is to:

1. Open **Event Viewer**.
2. Navigate to **Windows Logs > System**.
3. Look for **critical or error events** around the time of the last crash.
4. Note the **Event ID, Source, and Description**.
5. Research the Event ID online or in Microsoft documentation.
6. Determine the probable cause (e.g., driver, memory, hardware).
7. Suggest corrective action (e.g., update driver, run memory diagnostics).

Expected Outcome:

- Accurate identification of the error cause.
- A documented troubleshooting process.
- A recommended fix implemented or prepared for escalation.

Summary

Troubleshooting requires both technical knowledge and logical thinking. By recognizing common problems, using built-in tools like CMD and Event Viewer, and practicing hands-on diagnostics, you'll build the skills needed to keep systems running smoothly and efficiently.

Module 6 – Security & Backup

Overview

In this module, we explore how to secure a Windows system using built-in tools and policies. You'll learn how to manage antivirus protection, enforce security settings

through Group Policy, back up critical data, and ensure systems stay protected with regular updates. This module also includes a practical lab on applying local security policies.

1. Antivirus & Windows Defender

Windows Security (Defender)

Windows Defender is Microsoft's built-in antivirus and antimalware solution. It offers real-time protection against:

- Viruses
- Spyware
- Ransomware
- Other malicious software

Features

- **Real-Time Protection:** Monitors and blocks threats as they appear.
- **Firewall & Network Protection:** Controls inbound/outbound traffic.
- **Controlled Folder Access:** Protects important folders from ransomware.
- **Virus & Threat History:** View quarantined files and actions taken.

Best Practices

- Ensure Defender is up to date.
- Regularly scan the system.
- Schedule full scans during off-hours.
- Avoid disabling protection unless troubleshooting.

2. Group Policy Management

Group Policy is a powerful feature used to manage security and configuration settings across a system or network.

What is Group Policy?

Group Policy allows administrators to define rules and restrictions for users and computers.

Local Group Policy Editor

- Open via gpedit.msc
- Allows configuration of settings like:
 - Password policies
 - Software restrictions
 - USB/device control
 - Desktop environment control

Key Paths

- **Computer Configuration:** Applies settings at the system level.
- **User Configuration:** Applies settings to user profiles.

Note: Group Policy is available in Professional and Enterprise editions of Windows.

3. Data Backup & Restore

Why Back Up?

Regular backups protect data against:

- Hardware failure
- Ransomware attacks
- Accidental deletion

Backup Tools in Windows

- **File History:** Automatically backs up user folders (Documents, Pictures, etc.)
- **Windows Backup:** Full system image backup
- **OneDrive Integration:** Cloud-based backup for important files

Restore Options

- Restore from File History
- System Restore (for system settings and registry)
- Recovery Drive (bootable USB for recovery)

4. Security Updates



Importance of Updates

Security updates patch vulnerabilities that could be exploited by malware or attackers.

Managing Updates

- **Windows Update Settings:** Configure active hours and restart behavior.
- **Update History:** Track installed patches and identify failed updates.
- **Optional Updates:** Include feature updates and hardware drivers.

Best Practices

- Enable automatic updates.
- Monitor update success.
- Delay non-critical updates in enterprise settings to test compatibility.



Lab: Create and Apply Local Policy

Objective

Learn how to apply a basic local security policy using the Group Policy Editor.

Scenario

You are tasked with improving local system security by enforcing a password complexity policy and disabling access to the Control Panel.

Steps

1. Press Win + R, type gpedit.msc, and press **Enter**.
2. Navigate to:
 - **Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy**
 - Enable **Password must meet complexity requirements**
3. Navigate to:
 - **User Configuration > Administrative Templates > Control Panel**
 - Set **Prohibit access to Control Panel and PC settings** to **Enabled**
4. Close the Group Policy Editor.
5. Reboot or run gpupdate /force in CMD to apply changes.

Expected Outcome

- Users must create stronger passwords.
- Control Panel access is restricted.
- System security posture is improved.

Summary

This module has equipped you with essential tools and practices to secure a Windows system. From antivirus protection to group policies and backups, maintaining a proactive security and recovery strategy is key to system integrity and data protection.

Module 7 – Helpdesk & Communication

Overview

This module focuses on the essential skills and tools used in IT support environments. From managing tickets in professional systems like **JIRA** and **ServiceNow** to writing clear reports and communicating with users, this module builds your effectiveness as a support technician.



Instructor Tip:

Throughout this module, emphasize that technical knowledge is only half the job—clear, professional communication and accurate documentation are what turn a good technician into a great one.

1. IT Ticketing Systems

IT ticketing systems are essential tools used by helpdesk teams to manage, track, and resolve user issues.



Common Platforms

- **JIRA Service Management**
 - Used widely for IT and software support.
 - Tracks incidents, changes, and service requests.
 - Integrates well with development and Agile tools.
- **ServiceNow**
 - Enterprise-grade ITSM (IT Service Management) platform.
 - Offers modules for incident, problem, and change management.
 - Automates workflows and reporting.

Key Ticket Elements

- **Ticket ID:** Unique reference number
- **Issue Summary:** Short description of the problem
- **Category/Priority:** Helps with triaging and routing
- **Status:** Open, In Progress, Resolved, Closed
- **Resolution Notes:** Details of what was done to fix the issue
- **Time Logs:** Records of time spent on each ticket

2. Reporting & Documentation

Proper documentation is crucial for team collaboration, auditing, and future troubleshooting.



Types of Documentation

- **Incident Reports:** Detail user problems and their resolutions.
- **Knowledge Base Articles:** Step-by-step guides for recurring issues.
- **Daily Logs:** Summary of support activity per technician or shift.
- **Asset Documentation:** Inventory of hardware/software used.



Tips for Effective Documentation

- Be **clear** and **concise**: Avoid jargon unless necessary.
- Use **bullet points** or numbered lists when documenting steps.
- Always include **what was done**, **why**, and **the outcome**.
- Use **timestamps** and your **name/ID** when applicable.

3. Customer Communication

Support technicians often act as the bridge between users and IT solutions. Strong interpersonal skills can make or break a support experience.



Best Practices for Communication

- **Be empathetic:** Understand the user's frustration or urgency.
- **Listen actively:** Repeat back key points to confirm understanding.
- **Avoid blaming:** Focus on solutions, not who's at fault.
- **Use plain language:** Explain technical issues in non-technical terms.
- **Keep users updated:** Let them know you're working on it, especially for longer fixes.

Communication Channels

- Email: For formal updates or follow-ups.
- Phone: For urgent or complex issues.
- Chat/Instant Messaging: For real-time support.
- In-person: Use respectful body language and tone.



Instructor Tip: Develop Soft Skills Alongside Technical Skills

Many IT issues are repeatable—but users are not. Teach students to:

- Tailor their communication to the user's technical level.
- Remain patient, even when under pressure.
- Document clearly so another technician can pick up where they left off.

Summary

In the world of IT support, your ability to solve problems is only as good as your ability to explain, document, and communicate your solutions. Ticketing systems, accurate documentation, and effective user communication are core skills every technician must master to succeed in a professional helpdesk environment.

Module 8 – Student Workbook & Assessment

1. Short Answer Questions

These questions encourage students to explain concepts in their own words, demonstrating comprehension.

Example Questions:

- What is the main purpose of Group Policy in Windows?
- Explain how Windows Defender protects a system.
- Describe the steps you would take to troubleshoot a slow boot issue.
- What information can you find in the Event Viewer?
- Why is regular data backup important?

2. Practical Exercises

Hands-on tasks to apply theoretical knowledge in real or simulated environments.

Examples:

- Use the Command Prompt to run ipconfig and interpret the output.
- Create a local Group Policy to enforce password complexity.
- Set up a scheduled Windows Defender scan.
- Back up a folder using File History and restore a file.

- Use Event Viewer to identify and document a system error.

3. Troubleshooting Scenarios

Scenario-based questions challenge students to diagnose and resolve problems.

Example Scenario:

A user reports that their computer displays a blue screen with an error code. Walk through the steps you would take to diagnose and resolve the issue.

Expected student response:

- Check Event Viewer for error logs.
- Identify recent hardware or software changes.
- Run memory and disk diagnostics.
- Update or roll back drivers.
- Document findings and resolution steps.

4. Multiple Choice Questions

Quick knowledge checks for key concepts.

Sample Questions:

1. Which tool in Windows is used to view system and application logs?
 - a) Task Manager
 - b) Event Viewer
 - c) Device Manager
 - d) Disk Management
2. What does sfc /scannow do?
 - a) Checks network status
 - b) Scans and repairs system files
 - c) Displays IP configuration
 - d) Manages user accounts
3. Which Group Policy setting enforces strong passwords?
 - a) Account Lockout Policy
 - b) Password Policy
 - c) Security Options
 - d) Audit Policy

5. Instructor Evaluation Sheet

A simple rubric for instructors to assess student performance based on key criteria.

Criteria	Excellent (4)	Good (3)	Needs Improvement (2)	Unsatisfactory (1)
Understanding of Concepts	Demonstrates thorough understanding of all topics.	Understands most concepts with minor errors.	Partial understanding, some misconceptions.	Lacks understanding of key concepts.
Practical Skills	Completes all exercises accurately and efficiently.	Completes exercises with minor errors.	Struggles with some exercises.	Unable to complete practical tasks.
Troubleshooting Ability	Effectively diagnoses and	Resolves most scenarios with guidance.	Attempts troubleshooting	Unable to diagnose or

	resolves scenarios.		but misses key steps.	resolve problems.
Communication & Documentation	Clear, concise, and complete documentation and communication.	Generally clear documentation with minor omissions.	Documentation lacks clarity or detail.	Documentation incomplete or unclear.
Participation & Attitude	Actively participates and shows positive attitude.	Participates but occasionally disengaged.	Limited participation and inconsistent attitude.	Disengaged or disruptive behavior.