CompTIA A+

1. **Mobile Devices**
    a. Given a scenario, install and configure laptop hardware and components
        1. Hardware/device replacement
    b. Given a scenario, install components within the display of a laptop
        1. Types
        2. WiFi antenna connector/placement
        3. Webcam
        4. Microphone
        5. Inverter
        6. Digitizer/touchscreen
    c. Given a scenario, use appropriate laptop features
        1. Special function keys
        2. Docking station
        3. Port replicator
        4. Physical laptop lock and cable lock
        5. Rotating/removable screens
    d. Compare and contrast characteristics of various types of other mobile devices
        1. Tablets
        2. Smartphones
        3. Smartphones
        4. Wearable technology devices
        5. E-readers
        6. GPS
    e. Given a scenario, connect and configure accessories and ports of other mobile devices
        1. Connection types
        2. Accessories
    f. Given a scenario, configure basic mobile device network connectivity and application support
        1. Wireless/cellular data network (enable/disable)
        2. Bluetooth
        3. Corporate and ISP email configuration
        4. Integrated commercial provider email configuration
        5. PRI updates/PRL updates/ baseband updates
        6. Radio firmware
        7. IMEI vs. IMSI
        8. VPN
    g. Given a scenario, use methods to perform mobile device synchronization
        1. Synchronization methods

2. Types of data to synchronize
3. Mutual authentication for multiple services (SSO)
4. Software requirements to install the application on the PC
5. Connection types to enable synchronization

2. Networking

. Compare and contrast TCP and UDP ports, protocols, and their purposes

1. Ports and protocols
2. TCP vs. UDP

a. Compare and contrast common networking hardware devices

1. Routers
2. Switches
3. Access points
4. Cloud-based network controller
5. Firewall
6. Network interface card
7. Repeater
8. Hub
9. Cable/DSL modem
10. Bridge
11. Patch panel
12. Power over Ethernet (PoE)
13. Ethernet over Power

b. Given a scenario, install and configure a basic wired/wireless SOHO network

1. Router/switch functionality
2. Access point settings
3. IP addressing
4. NIC configuration
5. End-user device configuration
6. IoT device configuration
7. Cable/DSL modem configuration
8. Firewall settings
9. QoS
10. Wireless settings

c. Compare and contrast wireless networking protocols

1. 802.11a
2. 802.11b
3. 802.11g
4. 802.11n
5. 802.11ac

6. Frequencies
7. Channels
8. Bluetooth
9. NFC
10. RFID
11. Zigbee
12. Z-Wave
13. 3G
14. 4G
15. 5G
16. LTE

d. Summarize the properties and purposes of services provided by networked hosts
   1. Server roles
   2. Internet appliance
   3. Legacy/embedded systems

e. Explain common network configuration concepts
   1. IP addressing
   2. DNS
   3. DHCP
   4. IPv4 vs. IPv6
   5. Subnet mask
   6. Gateway
   7. VPN
   8. VLAN
   9. NAT

f. Compare and contrast Internet connection types, network types, and their features
   1. Internet connection types
   2. Network types

g. Given a scenario, use appropriate networking tools
   1. Crimper
   2. Cable stripper
   3. Multimeter
   4. Tone generator and probe
   5. Cable tester
   6. Loopback plug
   7. Punchdown tool
   8. WiFi analyser

3. Hardware

. Explain basic cable types, features, and their purposes

1. Network cables
2. Video cables
3. Multipurpose cables
4. Peripheral cables
5. Hard drive cables
6. Adapters

a. Identify common connector types

1. RJ-11
2. RJ-45
3. RS-232
4. BNC
5. RG-59
6. RG-6
7. USB
8. Micro-USB
9. Mini-USB
10. USB-C
11. DB-9
12. Lightning
13. SCSI
14. eSATA
15. Molex

b. Given a scenario, install RAM types

1. RAM types
2. Single channel
3. Dual channel
4. Triple channel
5. Error correcting
6. Parity vs. non-parity

c. Given a scenario, select, install and configure storage devices

1. Optical drives
2. Solid-state drives
3. Magnetic hard drives
4. Hybrid drives
5. Flash
6. Configurations

d. Given a scenario, install and configure motherboards, CPUs, and add-on cards

1. Motherboard form factor
2. Motherboard connectors types
3. BIOS/UEFI settings
4. CMOS battery
5. CPU features
6. Compatibility
7. Cooling mechanism
8. Expansion cards

e. Explain the purposes and uses of various peripheral types
   1. Printer
   2. ADF/flatbed scanner
   3. Barcode scanner/QR scanner
   4. Monitors
   5. VR headset
   6. Optical
   7. DVD drive
   8. Mouse
   9. Keyboard
   10. Touchpad
   11. Signature pad
   12. Game controllers
   13. Camera/webcam
   14. Microphone
   15. Speakers
   16. Headset
   17. Projector
   18. External storage drives
   19. KVM
   20. Magnetic reader/chip reader
   21. NFC/tap pay device
   22. Smart card reader

f. Summarize power supply types and features
   1. Input 115V vs. 220V
   2. Output 5.5V vs. 12V
   3. 24-pin motherboard adapter
   4. Wattage rating
   5. Number of devices/types of devices to be powered

g. Given a scenario, select and configure appropriate components for a custom PC configuration to meet customer specifications or needs

1. Graphic/CAD/CAM design workstation
2. Audio/video editing workstation
3. Virtualization workstation
4. Gaming PC
5. Standard thick client
6. Thin client
7. Network attached storage device

h. Given a scenario, install and configure common devices
   1. Desktop
   2. Laptop/common mobile devices

i. Given a scenario, configure SOHO multifunction devices/printers and settings
   1. Use appropriate drivers for a given operating system
   2. Device sharing
   3. Public/shared devices

j. Given a scenario, install and maintain various print technologies
   1. Laser
   2. Inkjet
   3. Thermal
   4. Impact
   5. Virtual
   6. 3D printers

4. Virtualization and Cloud Computing

. Compare and contrast cloud computing concepts
   1. Common cloud models
   2. Shared resources
   3. Rapid elasticity
   4. On-demand
   5. Resource pooling
   6. Measured service
   7. Metered
   8. Off-site email applications
   9. Cloud file storage services
   10. Virtual application streaming/ cloud-based applications
   11. Virtual desktop

a. Given a scenario, set up and configure client-side virtualization
   1. Purpose of virtual machines
   2. Resource requirements
   3. Emulator requirements
   4. Security requirements

5. Network requirements
6. Hypervisor

5. Hardware and Network Troubleshooting

. Given a scenario, use the best practice methodology to resolve problems
   1. Always consider corporate policies, procedures, and impacts before implementing changes

a. Given a scenario, troubleshoot problems related to motherboards, RAM, CPUs, and power
   1. Common symptoms

b. Given a scenario, troubleshoot hard drives and RAID arrays
   1. Common symptoms

c. Given a scenario, troubleshoot video, projector, and display issues
   1. Common symptoms

d. Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures
   1. Common symptoms
   2. Disassembling processes for proper reassembly

e. Given a scenario, troubleshoot printers
   1. Common symptoms

f. Given a scenario, troubleshoot common wired and wireless network problem
   1. Common symptoms

6. Operating Systems

. Compare and contrast common operating system types and their purposes
   1. 32-bit vs. 64-bit
   2. Workstation operating systems
   3. Cell phone/tablet operating systems
   4. Vendor-specific limitations
   5. Compatibility concerns between operating systems

a. Compare and contrast features of Microsoft Windows versions
   1. Windows 7
   2. Windows 8
   3. Windows 8.1
   4. Windows 10
   5. Corporate vs. personal needs
   6. Desktop styles/user interface

b. Summarize general OS installation considerations and upgrade methods.
   1. Boot methods
   2. Type of installations
   3. Partitioning - Dynamic
   4. File system types/formatting

5. Load alternate third-party drivers when necessary
6. Workgroup vs. Domain setup
7. Time/date/region/language settings
8. Driver installation, software, and Windows updates
9. Factory recovery partition
10. Properly formatted boot drive with the correct partitions/format
11. Prerequisites/hardware compatibility
12. Application compatibility
13. OS compatibility/upgrade path

c. Given a scenario, use appropriate Microsoft command line tools

1. Navigation
2. ipconfig
3. ping
4. tracert
5. netstat
6. nslookup
7. shutdown
8. dism
9. sfc
10. chkdsk
11. diskpart
12. taskkill
13. gpupdate
14. gpresult
15. format
16. copy
17. xcopy
18. robocopy
19. net use
20. net user
21. [command name] /?
22. Commands available with standard privileges vs. administrative privileges

d. Given a scenario, use Microsoft operating system features and tools

1. Administrative
2. MSConfig
3. Task Manager
4. Disk Management
5. System utilities

e. Given a scenario, use Microsoft Windows Control Panel utilities
    1. Internet Options
    2. Display/Display Settings
    3. User Accounts
    4. Folder Options
    5. System
    6. Windows Firewall
    7. Power Options
    8. Credential Manager
    9. Programs and features
    10. HomeGroup
    11. Devices and Printers
    12. Sound
    13. Troubleshooting
    14. Network and Sharing Center
    15. Device Manager
    16. Bitlocker
    17. Sync Center
f. Summarize application installation and configuration concepts
    1. System requirements
    2. OS requirements
    3. Methods of installation and deployment
    4. Local user permissions
    5. Security considerations
g. Given a scenario, configure Microsoft Windows networking on a client/desktop
    1. HomeGroup vs. Workgroup
    2. Domain setup
    3. Network shares/administrative shares/mapping drives
    4. Printer sharing vs. network printer mapping
    5. Establish networking connections
    6. Proxy settings
    7. Remote Desktop Connection
    8. Remote Assistance
    9. Home vs. Work vs. Public network settings
    10. Firewall settings
    11. Configuring an alternative IP address in Windows
    12. Network card properties
h. Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems

1. Best practices
2. Tools
3. Features
4. Basic Linux commands

7. Security

. Summarize the importance of physical security measures

1. Mantrap
2. Badge reader
3. Smart card
4. Security guard
5. Door lock
6. Biometric locks
7. Hardware tokens
8. Cable locks
9. Server locks
10. USB locks
11. Privacy screen
12. Key fobs
13. Entry control roster

a. Explain logical security concepts

1. Active Directory
2. Software tokens
3. MDM policies
4. Port security
5. MAC address filtering
6. Certificates
7. Antivirus/Anti-malware
8. Firewalls
9. User authentication/strong passwords
10. Multifactor authentication
11. Directory permissions
12. VPN
13. DLP
14. Access control lists
15. Smart card
16. Email filtering
17. Trusted/untrusted software sources
18. Principle of least privilege

b. Compare and contrast wireless security protocols and authentication methods

1. Protocols and encryption
2. Authentication

c. Given a scenario, detect, remove, and prevent malware using appropriate tools and methods
   1. Malware
   2. Tools and methods

d. Compare and contrast social engineering, threats, and vulnerabilities
   1. Social engineering
   2. DDoS
   3. DoS
   4. Zero-day
   5. Man-in-the-middle
   6. Brute force
   7. Dictionary
   8. Rainbow table
   9. Spoofing
   10. Non-compliant systems
   11. Zombie

e. Compare and contrast the differences of basic Microsoft Windows OS security settings
   1. User and groups
   2. NTFS vs. share permissions
   3. Shared files and folders
   4. System files and folders
   5. User authentication
   6. Run as administrator vs. standard user
   7. BitLocker
   8. BitLocker To Go
   9. EFS

f. Given a scenario, implement security best practices to secure a workstation
   1. Password best practices
   2. Account management
   3. Disable autorun
   4. Data encryption
   5. Patch/update management

g. Given a scenario, implement methods for securing mobile devices
   1. Screen locks
   2. Remote wipes
   3. Locator applications
   4. Remote backup applications
   5. Failed login attempts restrictions

6. Antivirus/Anti-malware
7. Patching/OS updates
8. Biometric authentication
9. Full device encryption
10. Multifactor authentication
11. Authenticator applications
12. Trusted sources vs. untrusted sources
13. Firewalls
14. Policies and procedures

h. Given a scenario, implement appropriate data destruction and disposal methods
   1. Physical destruction
   2. Recycling or repurposing best practices

i. Given a scenario, configure security on SOHO wireless and wired networks
   1. Wireless
   2. Change default usernames and passwords
   3. Enable MAC filtering
   4. Assign static IP addresses
   5. Firewall settings
   6. Port forwarding/mapping
   7. Disabling ports
   8. Content filtering/parental controls
   9. Update firmware
   10. Physical security

8. Software Troubleshooting

. Given a scenario, troubleshoot Microsoft Windows OS problems
   1. Common symptoms
   2. Common solutions

a. Given a scenario, troubleshoot and resolve PC security issues
   1. Common symptoms

b. Given a scenario, use best practice procedures for malware removal
   1. Identify and research malware symptoms.
   2. Quarantine the infected systems.
   3. Disable System Restore (in Windows).
   4. Remediate the infected systems.
   5. Schedule scans and run updates.
   6. Enable System Restore and create a restore point (in Windows).
   7. Educate the end user

c. Given a scenario, troubleshoot mobile OS and application issues
   1. Common symptoms

d. Given a scenario, troubleshoot mobile OS and application security issues
    1. Common symptoms

9. Operational Procedures

. Compare and contrast best practices associated with types of documentation
    1. Network topology diagrams
    2. Knowledge base/articles
    3. Incident documentation
    4. Regulatory and compliance policy
    5. Acceptable use policy
    6. Password policy
    7. Inventory management

a. Given a scenario, implement basic change management best practices
    1. Documented business processes
    2. Purpose of the change
    3. Scope the change
    4. Risk analysis
    5. Plan for change
    6. End-user acceptance
    7. Change board
    8. Backout plan
    9. Document changes

b. Given a scenario, implement basic disaster prevention and recovery methods
    1. Backup and recovery
    2. Backup testing
    3. UPS
    4. Surge protector
    5. Cloud storage vs. local storage backups
    6. Account recovery options

c. Explain common safety procedures
    1. Equipment grounding
    2. Proper component handling and storage
    3. Toxic waste handling
    4. Personal safety
    5. Compliance with government regulations

d. Explain environmental impacts and appropriate controls
    1. MSDS documentation for handling and disposal
    2. Temperature, humidity level awareness, and proper ventilation
    3. Power surges, brownouts, and blackouts
    4. Protection from airborne particles

5. Dust and debris
6. Compliance to government regulations

e. Explain the processes for addressing prohibited content/ activity, and privacy, licensing, and policy concepts
   1. Incident response
   2. Licensing/DRM/EULA
   3. Regulated data
   4. Follow all policies and security best practices

f. Given a scenario, use proper communication techniques and professionalism
   1. Use proper language and avoid jargon, acronyms, and slang, when applicable
   2. Maintain a positive attitude/ project confidence
   3. Actively listen (taking notes) and avoid interrupting the customer
   4. Be culturally sensitive - Use appropriate professional titles, when applicable
   5. Be on time (if late, contact the customer)
   6. Avoid distractions
   7. Dealing with difficult customers or situations
   8. Set and meet expectations/timeline and communicate status with the customer
   9. Deal appropriately with customer's confidential and private materials

g. Identify the basics of scripting
   1. Script file types
   2. Environment variables
   3. Comment syntax
   4. Basic script constructs
   5. Basic data types

h. Given a scenario, use remote access technologies
   1. RDP
   2. Telnet
   3. SSH
   4. Third-party tools
   5. Security considerations of each access method