CompTIA A+ Prep Course prepares you for the A+ certification exams based on the 2019 objectives exams Core 1 220-1001 & Core 2 220-1002.

Each participant in an authorized training CompTIA A+ Prep Course held in Compendium CE will be able to:

- Assemble components based on customer requirements
- Install, configure and maintain devices, PCs and software for end users
- Understand the basics of networking and security, including forensics
- Apply troubleshooting skills to diagnose, resolve and document common hardware and software issues
- Provide appropriate customer support
- Understand the basics of virtualization, desktop imaging and deployment
receive a free 220-1001 & 220-1002 CompTIA A+ Certification Exam vouchers.

Who Should Attend:

- Service Desk Analyst
- Help Desk Tech
- Technical Support Specialist
- Field Service Technician
- Associate Network Engineer
- Data Support Technician
- Desktop Support Administrator
- End User Computing Technician
- Help Desk Technician
- System Support Specialist

Plan szkolenia:

- Mobile Devices
  - Given a scenario, install and configure laptop hardware and components.
    - Hardware/device replacement
    - Keyboard
    - Hard drive
    - Memory
    - Smart card reader
    - Optical drive
    - Wireless card/Bluetooth module
    - Cellular card
    - Video card
    - Mini PCIe
    - Screen
    - DC jack
    - Battery
    - Touchpad
    - Plastics/frames
    - Speaker
    - System board
    - CPU
  - Given a scenario, install components within the display of a laptop.
- WiFi antenna connector/placement
- Webcam
- Microphone
- Inverter
- Digitizer/touchscreen

- Given a scenario, use appropriate laptop features.
  - Special function keys
  - Docking station
  - Port replicator
  - Physical laptop lock and cable lock
  - Rotating/removable screens

- Compare and contrast characteristics of various types of other mobile devices.
  - Tablets
  - Smartphones
  - Wearable technology devices
  - E-readers
  - GPS

- Given a scenario, connect and configure accessories and ports of other mobile devices.
  - Connection types
  - Wireless
  - Accessories

- Given a scenario, configure basic mobile device network connectivity and application support.
  - Wireless/cellular data network (enable/disable)
  - Bluetooth
  - Corporate and ISP email configuration
  - Integrated commercial provider email configuration
  - PRI updates/PRL updates/baseband updates
  - Radio firmware
  - IMEI vs. IMSI
  - VPN

- Given a scenario, use methods to perform mobile device synchronization.
  - Synchronization methods
  - Types of data to synchronize
  - Mutual authentication for multiple services (SSO)
  - Software requirements to install the application on the PC
- Connection types to enable synchronization

- Networking
  - Compare and contrast TCP and UDP ports, protocols, and their purposes.
    - Ports and protocols
    - TCP vs. UDP
  - Compare and contrast common networking hardware devices.
    - Routers
    - Switches
    - Access points
    - Cloud-based network controller
    - Firewall
    - Network interface card
    - Repeater
    - Hub
    - Cable/DSL modem
    - Bridge
    - Patch panel
    - Power over Ethernet (PoE)
    - Ethernet over Power
  - Given a scenario, install and configure a basic wired/wireless SOHO network.
    - Router/switch functionality
    - Access point settings
    - IP addressing
    - NIC configuration
    - End-user device configuration
    - IoT device configuration
    - Cable/DSL modem configuration
    - Firewall settings
    - QoS
    - Wireless settings
  - Compare and contrast wireless networking protocols.
    - 802.11a
    - 802.11b
    - 802.11g
    - 802.11n
    - 802.11ac
○ Frequencies
○ Channels
○ Bluetooth
○ NFC
○ RFID
○ Zigbee
○ Z-Wave
○ 3G
○ 4G
○ 5G
○ LTE

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

○ Explain common network configuration concepts.
  ○ IP addressing
  ○ DNS
  ○ DHCP
  ○ IPv4 vs. IPv6
  ○ Subnet mask
  ○ Gateway
  ○ VPN
  ○ VLAN
  ○ NAT

○ Compare and contrast Internet connection types, network types, and their features.
  ○ Internet connection types
  ○ Network types

○ Given a scenario, use appropriate networking tools.
  ○ Crimper
  ○ Cable stripper
  ○ Multimeter
  ○ Tone generator and probe
  ○ Cable tester
  ○ Loopback plug
  ○ Punchdown tool
WiFi analyzer

Hardware
- Explain basic cable types, features, and their purposes.
  - Network cables
  - Video cables
  - Multipurpose cables
  - Peripheral cables
  - Hard drive cables
  - Adapters
- Identify common connector types.
  - RJ-11
  - RJ-45
  - RS-232
  - BNC
  - RG-59
  - RG-6
  - USB
  - Micro-USB
  - Mini-USB
  - USB-C
  - DB-9
  - Lightning
  - SCSI
  - eSATA
  - Molex
- Given a scenario, install RAM types.
  - RAM types
  - Single channel
  - Dual channel
  - Triple channel
  - Error correcting
  - Parity vs. non-parity
- Given a scenario, select, install and configure storage devices.
  - Optical drives
  - Solid-state drives
  - Magnetic hard drives
Hybrid drives
Flash
Configurations

Given a scenario, install and configure motherboards, CPUs, and add-on cards.
- Motherboard form factor
- Motherboard connectors types
- BIOS/UEFI settings
- CMOS battery
- CPU features
- Compatibility
- Cooling mechanism
- Expansion cards

Explain the purposes and uses of various peripheral types.
- Printer
- ADF/flatbed scanner
- Barcode scanner/QR scanner
- Monitors
- VR headset
- Optical drive types
- Mouse
- Keyboard
- Touchpad
- Signature pad
- Game controllers
- Camera/webcam
- Microphone
- Speakers
- Headset
- Projector
- External storage drives
- KVM
- Magnetic reader/chip reader
- NFC/tap pay device
- Smart card reader

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

- Given a scenario, select and configure appropriate components for a custom PC configuration to meet customer specifications or needs.
  - Graphic/CAD/CAM design workstation
  - Audio/video editing workstation
  - Virtualization workstation
  - Gaming PC
  - Network attached storage device
  - Standard thick client
  - Thin client

- Given a scenario, install and configure common devices.
  - Desktop
  - Laptop/common mobile devices

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

- Given a scenario, install and maintain various print technologies.
  - Laser
  - Inkjet
  - Thermal
  - Impact
  - Virtual
  - 3D printers

- Virtualization and Cloud Computing
  - Compare and contrast cloud computing concepts.
    - Common cloud models
    - Shared resources
    - Rapid elasticity
    - On-demand
    - Resource pooling
    - Measured service
    - Metered
○ Off-site email applications
○ Cloud file storage services
○ Virtual application streaming/cloud-based applications
○ Virtual desktop

○ Given a scenario, set up and configure client-side virtualization.
  ○ Purpose of virtual machines
  ○ Resource requirements
  ○ Emulator requirements
  ○ Security requirements
  ○ Network requirements
  ○ Hypervisor

○ Hardware and Network Troubleshooting
  ○ Given a scenario, use the best practice methodology to resolve problems.
    ○ Always consider corporate policies, procedures, and impacts before implementing changes
  ○ Given a scenario, troubleshoot problems related to motherboards, RAM, CPUs, and power.
  ○ Given a scenario, troubleshoot hard drives and RAID arrays.
  ○ Given a scenario, troubleshoot video, projector, and display issues.
  ○ Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures.
  ○ Given a scenario, troubleshoot printers.
  ○ Given a scenario, troubleshoot common wired and wireless network problems.

○ Operating Systems
  ○ Compare and contrast common operating system types and their purposes.
    ○ 32-bit vs. 64-bit
    ○ Workstation operating systems
    ○ Cell phone/tablet operating systems
    ○ Vendor-specific limitations
    ○ Compatibility concerns between operating systems
  ○ Compare and contrast features of Microsoft Windows versions.
    ○ Windows 7
    ○ Windows 8
    ○ Windows 8.1
    ○ Windows 10
    ○ Corporate vs. personal needs
    ○ Desktop styles/user interface
  ○ Summarize general OS installation considerations and upgrade methods.
○ Boot methods
○ Type of installations
○ Partitioning
○ File system types/formatting
○ Load alternate third-party drivers when necessary
○ Workgroup vs. Domain setup
○ Time/date/region/language settings
○ Driver installation, software, and Windows updates
○ Factory recovery partition
○ Properly formatted boot drive with the correct partitions/format
○ Prerequisites/hardware compatibility
○ Application compatibility
○ OS compatibility/upgrade path

○ Given a scenario, use appropriate Microsoft command line tools.
  ○ Navigation
  ○ ipconfig
  ○ ping
  ○ tracert
  ○ netstat
  ○ nslookup
  ○ shutdown
  ○ dism
  ○ sfc
  ○ chkdsk
  ○ diskpart
  ○ taskkill
  ○ gpupdate
  ○ gpresult
  ○ format
  ○ copy
  ○ xcopy
  ○ robocopy
  ○ net use
  ○ net user
  ○ [command name] /?
○ Commands available with standard privileges vs. administrative privileges
- Given a scenario, use Microsoft operating system features and tools.
  - Administrative
  - MSConfig
  - Task Manager
  - Disk Management
  - System utilities

- Given a scenario, use Microsoft Windows Control Panel utilities.
  - Internet Options
  - Display/Display Settings
  - User Accounts
  - Folder Options
  - System
  - Windows Firewall
  - Power Options
  - Credential Manager
  - Programs and features
  - HomeGroup
  - Devices and Printers
  - Sound
  - Troubleshooting
  - Network and Sharing Center
  - Device Manager
  - BitLocker
  - Sync Center

- Summarize application installation and configuration concepts.
  - System requirements
  - OS requirements
  - Methods of installation and deployment
  - Local user permissions
  - Security considerations

- Given a scenario, configure Microsoft Windows networking on a client/desktop.
  - HomeGroup vs. Workgroup
  - Domain setup
  - Network shares/administrative shares/mapping drives
  - Printer sharing vs. network printer mapping
  - Establish networking connections
- Proxy settings
- Remote Desktop Connection
- Remote Assistance
- Home vs. Work vs. Public network settings
- Firewall settings
- Configuring an alternative IP address in Windows
- Network card properties
- Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems.
  - Best practices
  - Tools
  - Features
  - Basic Linux commands

- Security
  - Summarize the importance of physical security measures.
    - Mantrap
    - Badge reader
    - Smart card
    - Security guard
    - Door lock
    - Biometric locks
    - Hardware tokens
    - Cable locks
    - Server locks
    - USB locks
    - Privacy screen
    - Key fobs
    - Entry control roster
  - Explain logical security concepts.
    - Active Directory
    - Software tokens
    - MDM policies
    - Port security
    - MAC address filtering
    - Certificates
    - Antivirus/Anti-malware
○ Firewalls
  ○ User authentication/strong passwords
  ○ Multifactor authentication
  ○ Directory permissions
  ○ VPN
  ○ DLP
  ○ Access control lists
  ○ Smart card
  ○ Email filtering
  ○ Trusted/untrusted software sources
  ○ Principle of least privilege

○ Compare and contrast wireless security protocols and authentication methods.
  ○ Protocols and encryption
  ○ Authentication

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

○ Compare and contrast social engineering, threats, and vulnerabilities.
  ○ Social engineering
  ○ DDoS
  ○ DoS
  ○ Zero-day
  ○ Man-in-the-middle
  ○ Brute force
  ○ Dictionary
  ○ Rainbow table
  ○ Spoofing
  ○ Non-compliant systems
  ○ Zombie

○ Compare and contrast the differences of basic Microsoft Windows OS security settings.
  ○ User and groups
  ○ NTFS vs. share permissions
  ○ Shared files and folders
  ○ System files and folders
  ○ User authentication
- Run as administrator vs. standard user
- BitLocker
- BitLocker To Go
- EFS

- Given a scenario, implement security best practices to secure a workstation.
  - Password best practices
  - Account management
  - Disable autorun
  - Data encryption
  - Patch/update management

- Given a scenario, implement methods for securing mobile devices.
  - Screen locks
  - Remote wipes
  - Locator applications
  - Remote backup applications
  - Failed login attempts restrictions
  - Antivirus/Anti-malware
  - Patching/OS updates
  - Biometric authentication
  - Full device encryption
  - Multifactor authentication
  - Authenticator applications
  - Trusted sources vs. untrusted sources
  - Firewalls
  - Policies and procedures

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

- Given a scenario, configure security on SOHO wireless and wired networks.
  - Wireless-specific
  - Change default usernames and passwords
  - Enable MAC filtering
  - Assign static IP addresses
  - Firewall settings
  - Port forwarding/mapping
  - Disabling ports
- Content filtering/parental controls
- Update firmware
- Physical security

Software Troubleshooting
- Given a scenario, troubleshoot Microsoft Windows OS problems.
- Given a scenario, troubleshoot and resolve PC security issues.
- Given a scenario, use best practice procedures for malware removal.
  - Identify and research malware symptoms.
  - Quarantine the infected systems.
  - Disable System Restore (in Windows).
  - Remediate the infected systems.
  - Schedule scans and run updates.
  - Enable System Restore and create a restore point (in Windows).
  - Educate the end user.
- Given a scenario, troubleshoot mobile OS and application issues.
- Given a scenario, troubleshoot mobile OS and application security issues.

Operational Procedures
- Compare and contrast best practices associated with types of documentation.
  - Network topology diagrams
  - Knowledge base/articles
  - Incident documentation
  - Regulatory and compliance policy
  - Acceptable use policy
  - Password policy
  - Inventory management
- Given a scenario, implement basic change management best practices.
  - Documented business processes
  - Purpose of the change
  - Scope the change
  - Risk analysis
  - Plan for change
  - End-user acceptance
  - Change board
  - Backout plan
  - Document changes
- Given a scenario, implement basic disaster prevention and recovery methods.
○ Backup and recovery
○ Backup testing
○ UPS
○ Surge protector
○ Cloud storage vs. local storage backups
○ Account recovery options
○ Explain common safety procedures.
  ○ Equipment grounding
  ○ Proper component handling and storage
  ○ Toxic waste handling
  ○ Personal safety
  ○ Compliance with government regulations
○ Explain environmental impacts and appropriate controls.
  ○ MSDS documentation for handling and disposal
  ○ Temperature, humidity level awareness, and proper ventilation
  ○ Power surges, brownouts, and blackouts
  ○ Protection from airborne particles
  ○ Dust and debris
  ○ Compliance to government regulations
○ Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts.
  ○ Incident response
  ○ Licensing/DRM/EULA
  ○ Regulated data
  ○ Follow all policies and security best practices
○ Given a scenario, use proper communication techniques and professionalism.
  ○ Use proper language and avoid jargon, acronyms, and slang, when applicable
  ○ Maintain a positive attitude/project confidence
  ○ Actively listen (taking notes) and avoid interrupting the customer
  ○ Be culturally sensitive
  ○ Be on time (if late, contact the customer)
  ○ Avoid distractions
  ○ Dealing with difficult customers or situations
  ○ Set and meet expectations/timeline and communicate status with the customer
  ○ Deal appropriately with customers’ confidential and private materials
○ Identify the basics of scripting.
- Script file types
- Environment variables
- Comment syntax
- Basic script constructs
- Basic data types

- Given a scenario, use remote access technologies.
  - RDP
  - Telnet
  - SSH
  - Third-party tools
  - Security considerations of each access method

Wymagania:

- Basic knowledge of computing concepts
- End user skills with Windows operation system

Poziom trudności

Certyfikaty:

The participants will obtain certificates signed by CompTIA (course completion). This course will help prepare you for the **CompTIA A+ certification exams**, which is available through the Pearson VUE test centers.

Each participant in an authorized training CompTIA A+ Prep Course held in Compendium CE will receive a free **Core 1 220-1001 & Core 2 220-1002** CompTIA A+ Certification Exam vouchers.

Prowadzący:

Autoryzowany trener CompTIA.

Informacje dodatkowe:

CompTIA A+ is accredited by ANSI as meeting the ISO/IEC 17024 standard and is approved by U.S. Department of Defense (DoD) to fulfill Directive 8570.01-M requirements.