STRANDS AND STANDARDS
COMPUTER SYSTEMS 2

Course Description
Students will learn necessary competencies for an entry-level IT professional including troubleshooting, optimizing, diagnosing, and performing preventive maintenance of basic personal computer hardware and operating systems.

Relationship to the CompTIA Certification
To receive CompTIA A+ certification a candidate must pass two exams. The first exam is the CompTIA A+ Certification Exam: Core 1 (220-1001) as of 09/2020. The Strands & Standards for Computer Systems 1 match to this certification. The candidate must also pass the CompTIA A+ Certification Exam: Core 2 (220-1002) as of 09/2020. This is the second exam required for CompTIA A+ certification candidates to complete their certification. The Strand & Standards for Computer Systems 2 match to this certification.

Intended Grade Level	10-12
Units of Credit	0.5
Core Code	35.01.00.00.041
Concurrent Enrollment Core Code	35.01.00.13.041
Prerequisite	Computer Systems 1
Skill Certification Test Number	885 CompTIA IT Fundamentals (FCO-U61), CompTIA A+ Core 1 (220-1001), CompTIA A+ Core 2 (220-1002), TestOut PC Pro
Skill Certification Cut Score	**885 - 73%** CompTIA IT Fundamentals (FCO-U61), CompTIA A+ Core 1 (220-1001), CompTIA A+ Core 2 (220-1002), TestOut PC Pro (no cut score)
Test Weight	0.5
License Area of Concentration	CTE and/or Secondary Education 6-12
Required Endorsement(s)	
Endorsement 1 or	Cybersecurity
Endorsement 2	Information Technology System

CompTIA A+ Certification Exam: Core 2 Objectives

The table below lists the domains measured by the CompTIA A+ Core 2 exam and the extent to which they are represented. The CompTIA A+ Core 2 exam is based on these objectives.

Domain A+ (220-1001)	Percentage of Exam
1.0 Operating Systems	27%
2.0 Security	24%
3.0 Software Troubleshooting	26%
4.0 Operational Procedures	23%
Total	**100**%

These strand and standards align with the CompTIA A+ Certification Exam: Core 2. These strands and standards also align with the TestOut PC Pro (Chapters 8 – 14).

STRAND 1

Operating Systems

Standard 1

Understand common operating systems and their purposes.

- Software compatibility
- Workstation operating systems
  - Microsoft Windows
  - Apple Macintosh OS
  - Linux Distributions
- Cell Phone/tablet operating systems
  - Microsoft Windows
  - Android
  - iOS
  - Chrome OS
- Vendor specific limitations

Standard 2

Understand general OS installation considerations and upgrade methods.

- Boot Methods
  - Optical disc (CD-ROM, DVD, Blu-ray)
  - External drive/flash drive (USB/eSATA)
  - Network boot (PXE)
  - Internal fixed disk (HDD/SSD)
  - Internal hard drive (partition)
- Type of installations
  - Unattended installation
  - In-place upgrade
  - Clean install
  - Repair installation
  - Multiboot
  - Remote network installation
  - Image deployment
  - Recovery partition
  - Refresh/restore
- Partitioning
  - Dynamic
  - Basic
  - Primary
  - Extended
  - Logical
  - GPT

- File system types/formatting
  - ExFAT
  - FAT32
  - NTFS
  - CDFS
  - NFS
  - XFS
  - ext3, ext4, ext4 journaling
  - HFS
  - Swap partition
  - Quick format vs. full format
- 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

Standard 3

Demonstrate the use of Microsoft command line tools.

- Navigation
  - dir
  - cd
  - ..
- 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

Standard 4

Demonstrate the use of Microsoft operating system features and tools.

- Administrative
  - Computer Management
  - Device Manager
  - Local Users and Groups
  - Local Security Policy
  - Performance Monitor
  - Services
  - System Configuration
  - Task Scheduler
  - Component Services
  - Data Sources
  - Print Management
  - Windows Memory Diagnostics
  - Windows Firewall
  - Advanced Security
  - Event Viewer
  - User Account Management
- MSConfig
  - General
  - Boot
  - Services
  - Startup
  - Tools
- Task Manager
  - Applications
  - Processes
  - Performance
  - Networking
  - Users
- Disk Management
  - Drive status
  - Mounting
  - Initializing
  - Extending partitions
  - Splitting partitions
  - Shrink partitions
  - Assigning/changing drive letters
  - Adding drives
  - Adding arrays
  - Storage spaces

- System Utilities
  - Regedit
  - Command
  - Services.msc
  - MMC
  - MSTSC
  - Notepad
  - Explorer
  - Msinfo32
  - DxDiag
  - Disk Defragmenter
  - System Restore
  - Windows Update

Standard 5

Demonstrate the use of Microsoft Windows Control Panel utilities.

- Internet Options
  - Connections
  - Security
  - General
  - Privacy
  - Programs
  - Advanced
- Display/Display Settings
  - Resolution
  - Color depth
  - Refresh rate
- User Accounts
- Folder Options
  - View hidden files
  - Hide extensions
  - General options
  - View options
- System
  - Performance (virtual memory)
  - Remote settings
  - System protection
- Windows Firewall
- Power Options
  - Hibernate
  - Power plans
  - Sleep/suspend
  - Standby

- Credential Manager
- Programs and features
- HomeGroup
- Devices and Printers
- Sound
- Troubleshooting
- Network and Sharing Center
- Device Manager
- BitLocker
- Sync Center

Standard 6

Demonstrate Microsoft Windows networking installation on a client/desktop.

- HomeGroup vs. Workgroup
- Domain setup
- Network shares/administrative shares/mapping drives
- Printer sharing vs. network printer mapping
- Establish networking connections
  - VPN
  - Dial-ups
  - Wireless
  - Wired
  - WWAN (Cellular)
- Proxy settings
- Remote Desktop Connection
- Remote Assistance
- Home vs. Work vs. Public network settings
- Firewall settings
  - Exceptions
  - Configuration
  - Enabling/disabling Windows Firewall
- Configuring an alternative
- IP address in Windows
  - IP addressing
  - Subnet mask
  - DNS
  - DHCP
  - Gateway
- Network card properties
  - Half duplex/full duplex/auto
  - Speed
  - Wake-on-LAN
  - QoS
  - BIOS (on-board NIC)

Standard 7

Demonstrate the use of features and tools of Mac OS and Linux based systems.

- Best practices
  - Scheduled backups
  - Scheduled disk maintenance
  - System updates/App Store
  - Patch management
  - Driver/firmware updates
  - Antivirus/Anti-malware updates
- Tools
  - Backup/Time Machine
  - Restore/Snapshot
  - Image recovery
  - Disk maintenance utilities
  - Shell/Terminal
  - Screen sharing
  - Force Quit
- Features
  - Multiple desktops/Mission Control
  - Key Chain
  - Spot Light
  - iCloud
  - Gestures
  - Finder
  - Remote Disc
  - Dock
  - Boot Camp
- Basic Linux commands
  - ls
  - grep
  - cd
  - shutdown
  - pwd vs. passwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - iwconfig/ifconfig
  - ps
  - su/sudo
  - apt-get
  - vi
  - dd
  - kill

STRAND 2

Security

Standard 1

Understand 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

Standard 2

Understand logical security concepts.

- Active Directory
  - Login script
  - Domain
  - Group Policy/Updates
  - Organizational Units
  - Home Folder
  - Folder redirection
- 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

Standard 3

Understand wireless security protocols and authentication methods.

- Protocols and encryption
  - WEP
  - WPA
  - WPA2
  - TKIP
  - AES
- Authentication
  - Single-factor
  - Multifactor
  - RADIUS
  - TACACS

Standard 4

Demonstrate detection, removal, and prevention of malware using appropriate tools and methods.

- Malware
  - Ransomware
  - Trojan
  - Keylogger
  - Rootkit
  - Virus
  - Botnet
  - Worm
  - Spyware
  - Adware
  - Rootkits
  - Rogue Security Software
- Tools and methods
  - Antivirus
  - Anti-malware
  - Recovery console
  - Backup/restore
  - End user education
  - Software firewalls
  - DNS configuration

Standard 5

Understand social engineering, threats, and vulnerabilities.

- Social engineering
  - Phishing
  - Pharming
  - Spear phishing
  - Impersonation
  - Shoulder surfing
  - Tailgating
  - Dumpster diving
- DDoS
- DoS
- Zero-day
- Man-in-the-middle
- Brute force
- Dictionary
- Rainbow table
- Spoofing
- Non-compliant systems
- Zombie

Standard 6

Understand the basic Microsoft Windows OS security settings.

- User and groups
  - Administrator
  - Power user
  - Guest
  - Standard user
- NTFS vs. share permissions
  - Allow vs. deny
  - Moving vs. copying folders and files
  - File attributes
- Shared files and folders
  - Administrative shares vs. local shares
  - Permission propagation
  - Inheritance
- System files and folders
- User authentication
  - Single sign-on (SSO)
- Run as administrator vs. standard user
- BitLocker
- BitLocker To Go
- EFS

Standard 7

Demonstrate best practices in securing devices.

- Password best practices
  - Password Entropy and Complexity
  - Password expiration
  - Screensaver required password
  - BIOS/UEFI passwords
  - Requiring passwords
- Account management
  - Restricting user permissions
  - Logon time restrictions
  - Disabling guest account
  - Failed attempts lockout
  - Timeout/screen lock
  - Change default admin user account/password
  - Basic Active Directory functions
    - Account creation
    - Account deletion
    - Password reset / unlock account
    - Disable account
- Disable autorun
- Data encryption
- Patch/update management
- Screen locks
  - Fingerprint lock
  - Face lock
  - Swipe lock
  - Passcode lock
- 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
  - BYOD vs. corporate-owned
  - Profile security requirements

Standard 8

Understand appropriate data destruction and disposal methods.

- Physical destruction
  - Shredder
  - Drill/hammer
  - Electromagnetic (Degaussing)
  - Incineration
  - Certificate of destruction
- Recycling or repurposing best practices
  - Low-level format vs. standard format
  - Overwrite
  - Drive wipe

Standard 9

Understand security configuration protocols on networks.

- Wireless-specific
  - Changing default SSID
  - Setting encryption
  - Disabling SSID broadcast
  - Antenna and access point placement
  - Radio power levels (waves)
  - WPS
- 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

STRAND 3

Software Troubleshooting

Standard 1

Demonstrate the ability to troubleshoot Microsoft Windows OS problems.

- Common symptoms
  - Slow performance
  - Limited connectivity
  - Failure to boot
  - No OS found
  - Application crashes
  - Blue screens
  - Black screens
  - Printing issues
  - Services fail to start
  - Slow bootup
  - Slow profile load
- Common solutions
  - Defragment the hard drive
  - Reboot
  - Kill tasks
  - Restart services
  - Update network settings
  - Reimage/reload OS
  - Roll back updates
  - Roll back device drivers
  - Apply updates
  - Repair application
  - Update boot order
  - Disable Windows services/applications
  - Disable application startup
  - Safe boot
  - Rebuild Windows profiles

Standard 2

Understand problems that stem from PC security issues.

- Common symptoms
  - Pop-ups
  - Browser redirection
  - Security alerts
  - Slow performance
  - Internet connectivity issues
  - PC/OS lockup
  - Application crash
  - OS updates failures
  - Rogue antivirus
  - Spam
  - Renamed system files
  - Disappearing files
  - File permission changes
  - Hijacked email
    - Responses from users regarding email
    - Automated replies from unknown sent email
  - Access denied
  - Invalid certificate (trusted root CA)
  - System/application log errors

Standard 3

Understand tools and best practices for malware removal.

- Identify and research malware symptoms.
- Quarantine the infected systems.
- Disable System Restore (in Windows).
- Remediate the infected systems.
  - Update the anti-malware software.
  - Scan and use removal techniques (safe mode, pre-installation environment).
- Schedule scans and run updates.
- Enable System Restore and create a restore point (in Windows).
- Educate the end user.

STRAND 4

Operational Procedures

Standard 1

Understand best practices of documenting asset management and enterprise policies.

- Network topology diagrams
- Knowledge base/articles
- Incident documentation
- Regulatory and compliance policy
- Acceptable use policy
- Password policy
- Inventory management
  - Asset tags
  - Barcodes
- Documented business processes
- Purpose of the change
- Scope the change
- Risk analysis
- Plan for change
- End-user acceptance
- Change board
  - Approvals
- Backout plan
- Document changes
- Incident response
  - First response
    - Identify
    - Report through proper channels
    - Data/device preservation
  - Use of documentation/ documentation changes
  - Chain of custody
    - Tracking of evidence/documenting process
- Licensing/DRM/EULA
  - Open-source vs. commercial license
  - Personal license vs. enterprise licenses
  - Public domain
  - Permissive
  - LGPL
  - Copyleft
  - Proprietary
- Regulated data
  - PII
  - PCI
  - GDPR
  - PHI
- Follow all policies and security best practices

Standard 2

Understand safety procedures and environmental concerns.

- Backup and recovery
  - Image level
  - File level
  - Critical applications
- Backup testing
- UPS
- Surge protector
- Cloud storage vs. local storage backups
- Account recovery options
- Equipment grounding
- Proper component handling and storage
  - Antistatic bags
  - ESD straps
  - ESD mats
  - Self-grounding
- Toxic waste handling
  - Batteries
  - Toner
  - CRT
  - Cell phones
  - Tablets
- Personal safety
  - Disconnect power before repairing PC
  - Remove jewelry
  - Lifting techniques
  - Weight limitations
  - Electrical fire safety
  - Cable management
  - Safety goggles
  - Air filter mask
- MSDS documentation for handling and disposal
- Temperature, humidity level awareness, and proper ventilation
- Power surges, brownouts, and blackouts
  - Battery backup
  - Surge suppressor
- Protection from airborne particles
  - Enclosures
  - Air filters/mask
- Dust and debris
  - Compressed air
  - Vacuums
- Compliance with all government regulations

Standard 3

Understand 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
  - Use appropriate professional titles, when applicable
- Be on time (if late, contact the customer)
- Avoid distractions
  - Personal calls
  - Texting/social media sites
  - Talking to coworkers while interacting with customers
  - Personal interruptions
- Dealing with difficult customers or situations
  - Do not argue with customers and/or be defensive
  - Avoid dismissing customer problems
  - Avoid being judgmental
  - Clarify customer statements (ask open-ended questions to narrow the
  - scope of the problem, restate the issue, or question to verify understanding)
  - Do not disclose experiences via social media outlets
- Set and meet expectations/timeline and communicate status with the customer
  - Offer different repair/ replacement options, if applicable
  - Provide proper documentation on the services provided
  - Follow up with customer/user at a later date to verify satisfaction
- Deal appropriately with customers' confidential and private materials
  - Located on a computer, desktop, printer, etc.

Performance Skills

- Remote support from an external location.
- Assisting with software, hardware, and operating systems installations, including troubleshooting.
- Ask client/customer various questions about the installed computer systems, run diagnostic, handle software security.
- Highlight customer service and listening skills to understand a customer's problem so that student can help them, even when they are frustrated.
- Problem-solving skills are paramount so that you can figure out exactly what is causing the tricky hardware and software issues.

Workplace Skills

The following workplace skills should be discussed, taught, and re-enforced in the course:

- Communication
- Problem Solving
- Teamwork,
- Critical Thinking
- Dependability
- Accountability
- Legal requirements/expectations

Skill Certification Test Points by Strand

Test Name	Test #	Number of Test Points by Strand										Total Points	Total Questions
		1	2	3	4	5	6	7	8	9	10		
Computer Systems 2	885	21	6	11	6							44	44