CompTIA Strata – Fundamentals of PC Functionality

1.0 Technology

1.1 Identify basic IT vocabulary.

- Processor speed/cores
  - Single/Dual/Quad core
  - Intel based/AMD based / Cell based
  - GHz vs. MHz
  - Processor cache size
  - Bus speed (as they relate to motherboards, memory, etc)
- RAM
  - Single data rate, dual data rate, triple data rate
  - DIMMS vs. SODIMMS
- Hard drives
  - RPMs
  - Cache size
  - Flash based vs. traditional hard drives
  - SATA, SCSI, IDE
  - Internal vs. external
  - Local vs. network shares
- Networking
  - Wireless networking terms
    - 802.11a/b/g/n
    - Bluetooth
    - RF (Radio Frequency)
    - Interference
    - WAP (Wireless Access Point)
    - SSID
    - Wireless router
  - Ethernet technologies
    - CAT5, CAT5e connections and cables
    - Home plug (Ethernet over Power)
    - Broadband router
    - DSL and cable modems
    - Standard vs. crossover cables
    - Auto-negotiating (speed and duplex)
  - Internet
    - Protocols
      - HTTP vs. HTTPS
      - FTP
      - SSL
      - POP3
      - SMTP
      - IMAP
      - DNS

        - DHCP
        - TCP/IP (IPv4 address, IPv6 address)
    - Browser features
        - Plug-ins
        - Customization (text sizes, text styles, etc)
        - Anti-phishing features
        - ActiveX and Java
        - Cookies
        - Internet Cache

1.2 Identify the risks associated with upgrading the following technologies and equipment.

- Operating systems (open source and commercial)
    - Compatibility issues
    - Upgrade issues
    - Data loss
- PC Speed/storage capability
    - Compatibility issues
    - Upgrade issues
    - Bus differences
    - Hardware failure
- Application
    - Minimum requirements
    - Compatibility issues
- Bandwidth and contention
    - VoIP
    - Streaming
    - Web delivered services
- Automatic application and operating system updates
    - Risks of automatic updates
    - Risks of not using automatic updates
    - Risks of not using manufacturer websites

1.3 Demonstrate the ability to set up a basic PC workstation

- Identify differences between connector types
    - DVI, VGA, HDMI
    - USB, PS/2
    - FireWire
    - Bluetooth and Wireless
    - Serial
    - Network connectors
    - PCMCIA
    - ExpressCard
    - 3.5mm audio jack
    - Power connectors
- Monitor types
- Computer (desktop, tower, laptop, custom cases)
- Keyboard (keyboard layout: regionalization)
- Mouse (touchpad, optical, trackball)
- Printer (USB, wireless, networked)

- Voltage and power requirements
- Turn on and use the PC and peripherals

2.0 Software Installation and Functions

2.1 Conduct basic software installation, removal and/or upgrading.

- Follow basic installation/upgrade procedures
    - Check PC meets minimum requirements
    - Administrative Rights
    - Firewall access (unblocking ports for proper functionality)
- Configure the OS
    - Adjust basic settings (e.g. volume, date, time, time zone)
    - User accounts
    - Power settings (power save, sleep mode, etc)
    - Screen resolutions
- Documentation
    - Licensing (Commercial, Freeware, Shareware)
    - Software registration
- Digital Rights Management
- Software removal (clean un-installation)
- Re-installation (clean installation)

2.2 Identify issues related to folder and file management

- Create, delete, rename and move folders
    - Assign folder structure during installation
- Create, delete, rename, move and print files
- Importance of following back-up guidelines and procedures

2.3 Explain the function and purpose of software tools

- Performance and error correction tools
- Activity or event logging
- Back-up tools
- Disk clean-up tools
- File compression tools

3.0 Security

3.1 Recognize basic security risks and procedures to prevent them.

- Identify Risks
    - Social Engineering
    - Viruses
    - Worms
    - Trojan Horses
    - Unauthorized Access
        - Hackers
        - Phishing
        - Spyware
        - Adware

        - Malware
        - Identity Fraud
    - File and folder sharing
    - Web browser risks
    - Operating System vulnerability
        - Service packs
        - Security updates
    - Theft
    - Open or free networks
- Identify prevention methods
    - User awareness/education
    - Anti-virus software
    - Ensure proper security certificate is used (SSL)
    - Wireless encryption (WPA/WEP)
    - Anti-spyware
    - File encryption
    - Firewalls
    - Anti-spam software
    - Password best practice
        - Complexity (password construction)
        - Password confidentiality
        - Change frequency
        - Re-use
        - Utilization
- Identify access control methods
    - Passwords and User ID
    - Screensavers
    - Physical security of hardware
    - Locks
    - Parental controls
    - Smart card
    - Fingerprint reader
    - One time password
- Identify security threats related to the following:
    - Media used for backup (theft or loss)
    - Screen visibility (shoulder surfing)
    - Cookies (can be stolen, stores passwords, browser tracking)
    - Pop-ups (automatic installations, click on links to malware)
    - Accidental mis-configuration

3.2 Recognize security breaches and ways to resolve them.

- Recognize the proper diagnostic procedures when infected with a virus
    - Run anti-virus scan
    - Quarantine virus when possible
    - Escalate to IT professional when needed
- Recognize the proper procedures to maintain a secure environment
    - Regular antivirus and malware scans
    - Application / operating system updates

3.3 Recognize IT related laws and guidelines

- Data Protection Act
- Copyright Act
- Computer Misuse Act
- Freedom of Information Act