1.0 Windows Operating Systems

1.1 Compare and contrast various features and requirements of Microsoft Operating Systems (Windows Vista, Windows 7, Windows 8, Windows 8.1).

- Features:
  - 32-bit vs. 64-bit
  - Aero, gadgets, user account control, bit-locker, shadow copy, system restore, ready boost, sidebar, compatibility mode, virtual XP mode, easy transfer, administrative tools, defender, Windows firewall, security center, event viewer, file structure and paths, category view vs. classic view.
  - Side by side apps, Metro UI, Pinning, One Drive, Windows store, Multimonitor task bars, Charms, Start Screen, Power Shell, Live sign in, Action Center.
- Upgrade paths – differences between in place upgrades, compatibility tools, Windows upgrade OS advisor

1.2 Given a scenario, install Windows PC operating systems using appropriate methods.

- Boot methods
  - USB
  - CD-ROM
  - DVD
  - PXE
  - Solid state/flash drives
  - Netboot
  - External/hot swappable drive
  - Internal hard drive (partition)
- Type of installations
  - Unattended installation
  - 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
    - ext3, ext4
    - 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

1.3 Given a scenario, apply appropriate Microsoft command line tools.

- TASKKILL
- BOOTREC
- SHUTDOWN
- TASKLIST
- MD
- RD
- CD
- DEL
- FORMAT
- COPY
- XCOPY
- ROBOCOPY
- DISKPART
- SFC
- CHKDSK
- GPUPDATE
- GPRESULT
- DIR
- EXIT
- HELP
- EXPAND
- [command name] /?
- Commands available with standard privileges vs. administrative privileges.

1.4 Given a scenario, use appropriate 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
- 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
- Other
    - User State Migration tool (USMT)
    - Windows Easy Transfer
    - Windows Upgrade Advisor
- System utilities
    - REGEDIT
    - COMMAND
    - SERVICES.MSC
    - MMC
    - MSTSC
    - NOTEPAD
    - EXPLORER
    - MSINFO32
    - DXDIAG
    - DEFRAG
    - System restore
    - Windows Update

1.5 Given a scenario, use 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
- Programs and features
- HomeGroup
- Devices and Printers
- Sound
- Troubleshooting
- Network and Sharing Center
- Device Manager

1.6 Given a scenario, install and configure 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
    - VPN
    - Dialups
    - 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
    - Gateway
- Network card properties
    - Half duplex/full duplex/auto
    - Speed

- Wake-on-LAN
- QoS
- BIOS (on-board NIC)

1.7 Perform common preventive maintenance procedures using the appropriate Windows OS tools.

- Best practices
  - Scheduled backups
  - Scheduled disk maintenance
  - Windows updates
  - Patch management
  - Driver/firmware updates
  - Antivirus/ Antimalware updates
- Tools
  - Backup
  - System restore
  - Recovery image
  - Disk maintenance utilities

2.0 Other Operating Systems and Technologies

2.1 Identify common features and functionality of the Mac OS and Linux operating systems.

- Best practices
  - Scheduled backups
  - Scheduled disk maintenance
  - System updates/App store
  - Patch management
  - Driver/firmware updates
  - Antivirus/ Antimalware 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
- cd
- chown
- iwconfig/ifconfig
- ps
- q
- su/sudo
- apt-get
- vi
- dd

2.2 Given a scenario, setup and use client-side virtualization.

- Purpose of virtual machines
- Resource requirements
- Emulator requirements
- Security requirements
- Network requirements
- Hypervisor

2.3 Identify basic cloud concepts.

- SaaS
- IaaS
- Paas
- Public vs. Private vs. Hybrid vs. Community
- Rapid Elasticity
- On-demand
- Resource pooling
- Measured service

2.4 Summarize the properties and purpose of services provided by networked hosts.

- Server roles
  - Web server
  - File server
  - Print server
  - DHCP server
  - DNS server
  - Proxy server
  - Mail server
  - Authentication server
- Internet appliance
  - UTM
  - IDS
  - IPS
- Legacy / embedded systems

2.5 Identify basic features of mobile operating systems.

- Android vs. iOS vs. Windows

- Open source vs. closed source/vendor specific
- App source (play store, app store and store)
- Screen orientation (accelerometer/gyroscope)
- Screen calibration
- GPS and geotracking
- WiFi calling
- Launcher/GUI
- Virtual assistant
- SDK/APK
- Emergency notification
- Mobile payment service

2.6 Install and configure basic mobile device network connectivity and email.

- Wireless / cellular data network (enable/disable)
  - Hotspot
  - Tethering
  - Airplane mode
- Bluetooth
  - Enable Bluetooth
  - Enable pairing
  - Find device for pairing
  - Enter appropriate pin code
  - Test connectivity
- Corporate and ISP email configuration
  - POP3
  - IMAP
  - Port and SSL settings
  - Exchange, S/MIME
- Integrated commercial provider email configuration
  - Google/Inbox
  - Yahoo
  - Outlook.com
  - iCloud
- PRI updates/PRL updates/Baseband updates
- Radio firmware
- IMEI vs. IMSI
- VPN

2.7 Summarize methods and data related to mobile device synchronization.

- Types of data to synchronize
  - Contacts
  - Programs
  - Email
  - Pictures
  - Music
  - Videos
  - Calendar
  - Bookmarks
  - Documents
  - Location data
  - Social media data
  - eBooks

- Synchronization methods
    - Synchronize to the Cloud
    - Synchronize to the Desktop
- Mutual authentication for multiple services (SSO)
- Software requirements to install the application on the PC
- Connection types to enable synchronization

3.0 Security

3.1 Identify common security threats and vulnerabilities.

- Malware
    - Spyware
    - Viruses
    - Worms
    - Trojans
    - Rootkits
    - Ransomware
- Phishing
- Spear phishing
- Spoofing
- Social engineering
- Shoulder surfing
- Zero day attack
- Zombie/botnet
- Brute forcing
- Dictionary attacks
- Non-compliant systems
- Violations of security best practices
- Tailgating
- Man-in-the-middle

3.2 Compare and contrast common prevention methods.

- Physical security
    - Lock doors
    - Mantrap
    - Cable locks
    - Securing physical documents/passwords/shredding
    - Biometrics
    - ID badges
    - Key fobs
    - RFID badge
    - Smart card
    - Tokens
    - Privacy filters
    - Entry control roster
- Digital security
    - Antivirus/Antimalware
    - Firewalls
    - User authentication/strong passwords
    - Multifactor authentication

    - Directory permissions
    - VPN
    - DLP
    - Disabling ports
    - Access control lists
    - Smart card
    - Email filtering
    - Trusted/untrusted software sources
- User education/AUP
- Principle of least privilege

3.3 Compare and contrast differences of basic 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
- Run as administrator vs. standard user
- Bitlocker
- Bitlocker-To-Go
- EFS

3.4 Given a scenario, deploy and enforce security best practices to secure a workstation.

- Password best practices
    - Setting strong passwords
    - Password expiration
    - Changing default user names/passwords
    - Screensaver required password
    - BIOS/UEFI passwords
    - Requiring passwords
- Account management
    - Restricting user permissions
    - Login time restrictions
    - Disabling guest account
    - Failed attempts lockout
    - Timeout/screen lock
- Disable autorun
- Data encryption
- Patch/update management

3.5 Compare and contrast various methods for securing mobile devices.

- Screen locks
    - Fingerprint lock
    - Face lock
    - Swipe lock
    - Passcode lock
- Remote wipes
- Locator applications
- Remote backup applications
- Failed login attempts restrictions
- Antivirus/Antimalware
- 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

3.6 Given a scenario, use 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

3.7 Given a scenario, secure SOHO wireless and wired networks.

- Wireless specific
    - Changing default SSID
    - Setting encryption
    - Disabling SSID broadcast
    - Antenna and access point placement
    - Radio power levels
    - WPS
- Change default user-names and passwords
- Enable MAC filtering
- Assign static IP addresses
- Firewall settings
- Port forwarding/mapping
- Disabling ports
- Content filtering / parental controls
- Update firmware
- Physical security

4.0 Software Troubleshooting

4.1 Given a scenario, troubleshoot PC operating system problems with appropriate tools.

- Common symptoms
  - Proprietary crash screens (BSOD/pin wheel)
  - Failure to boot
  - Improper shutdown
  - Spontaneous shutdown/restart
  - Device fails to start/detected
  - Missing dll message
  - Services fails to start
  - Compatibility error
  - Slow system performance
  - Boots to safe mode
  - File fails to open
  - Missing NTLDR
  - Missing Boot Configuration Data
  - Missing operating system
  - Missing Graphical Interface
  - Missing GRUB/LILO
  - Kernel panic
  - Graphical Interface fails to load
  - Multiple monitor misalignment/orientation
- Tools
  - BIOS/UEFI
  - SFC
  - Logs
  - System Recovery Options
  - Repair disks
  - Pre-installation environments
  - MSCONFIG
  - DEFRAG
  - REGSRV32
  - REGEDIT
  - Event viewer
  - Safe mode
  - Command prompt
  - Uninstall/reinstall/repair

4.2 Given a scenario, troubleshoot common PC security issues with appropriate tools and best practices.

- Common symptoms
  - Pop-ups
  - Browser redirection
  - Security alerts
  - Slow performance
  - Internet connectivity issues
  - PC/OS lock up
  - Application crash
  - OS updates failures
  - Rogue antivirus
  - Spam

    - Renamed system files
    - Files disappearing
    - File permission changes
    - Hijacked email
        - Responses from users regarding email
        - Automated replies from unknown sent email
    - Access denied
    - Invalid certificate (trusted root CA)
- Tools
    - Antivirus software
    - Antimalware software
    - Recovery console
    - Terminal
    - System restore/Snapshot
    - Pre-installation environments
    - Event viewer
    - Refresh/restore
    - MSCONFIG/Safe boot
- Best practice procedure for malware removal
    1. Identify malware symptoms
    2. Quarantine infected system
    3. Disable system restore (in Windows)
    4. Remediate infected systems
        a. Update antimalware software
        b. Scan and removal techniques (safe mode, pre-installation environment)
    5. Schedule scans and run updates
    6. Enable system restore and create restore point (in Windows)
    7. Educate end user

4.3 Given a scenario, troubleshoot common mobile OS and application issues with appropriate tools.

- Common symptoms
    - Dim display
    - Intermittent wireless
    - No wireless connectivity
    - No bluetooth connectivity
    - Cannot broadcast to external monitor
    - Touchscreen non-responsive
    - Apps not loading
    - Slow performance
    - Unable to decrypt email
    - Extremely short battery life
    - Overheating
    - Frozen system
    - No sound from speakers
    - Inaccurate touch screen response
    - System lockout
- Tools
    - Hard reset
    - Soft reset
    - Close running applications
    - Reset to factory default
    - Adjust configurations/settings

- Uninstall/reinstall apps
- Force stop

4.4 Given a scenario, troubleshoot common mobile OS and application security issues with appropriate tools.

- Common symptoms
  - Signal drop/weak signal
  - Power drain
  - Slow data speeds
  - Unintended WiFi connection
  - Unintended Bluetooth pairing
  - Leaked personal files/data
  - Data transmission overlimit
  - Unauthorized account access
  - Unauthorized root access
  - Unauthorized location tracking
  - Unauthorized camera/microphone activation
  - High resource utilization
- Tools
  - Antimalware
  - App scanner
  - Factory reset/Clean install
  - Uninstall/reinstall apps
  - WiFi analyzer
  - Force stop
  - Cell tower analyzer
  - Backup/restore
    - iTunes/iCloud/Apple Configurator
    - Google sync
    - One Drive

5.0 Operational Procedures

5.1 Given a scenario, use appropriate safety procedures.

- Equipment grounding
- Proper component handling and storage
  - Antistatic bags
  - ESD straps
  - ESD mats
  - Self-grounding
- Toxic waste handling
  - Batteries
  - Toner
  - CRT
- Personal safety
  - Disconnect power before repairing PC
  - Remove jewelry
  - Lifting techniques
  - Weight limitations
  - Electrical fire safety
  - Cable management
  - Safety goggles

    - Air filter mask
- Compliance with local government regulations

5.2 Given a scenario with potential environmental impacts, apply the appropriate controls.

- MSDS documentation for handling and disposal
- Temperature, humidity level awareness and proper ventilation
- Power surges, brownouts, blackouts
    - Battery backup
    - Surge suppressor
- Protection from airborne particles
    - Enclosures
    - Air filters/Mask
- Dust and debris
    - Compressed air
    - Vacuums
- Compliance to local government regulations

5.3 Summarize the process of addressing prohibited content/activity, and explain privacy, licensing, and policy concepts.

- 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
- Personally Identifiable Information
- Follow corporate end-user policies and security best practices

5.4 Demonstrate proper communication techniques and professionalism.

- Use proper language – avoid jargon, acronyms, 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 co-workers while interacting with customers
    - Personal interruptions
- Dealing with difficult customer or situation
    - 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

5.5 Given a scenario, explain the troubleshooting theory.

- Always consider corporate policies, procedures and impacts before implementing changes.

1. Identify the problem
    - Question the user and identify user changes to computer and perform backups before making changes
2. Establish a theory of probable cause (question the obvious)
    - If necessary, conduct external or internal research based on symptoms
3. Test the theory to determine cause
    - Once theory is confirmed determine next steps to resolve problem
    - If theory is not confirmed re-establish new theory or escalate
4. Establish a plan of action to resolve the problem and implement the solution
5. Verify full system functionality and if applicable implement preventive measures
6. Document findings, actions and outcomes