Information Technology/Networking CTAG Alignments

This document contains information about 4 Career-Technical Articulation Numbers (CTANs) for Information Technology Career-Technical Assurance Guide (CTAG). The CTANs are:

1. **CTIT002 - Networking/CompTIA Network+**
2. **CTIT016 – Linux**
3. **CTIT013 – Microsoft Server Administration**
4. **CTIT005 – Desktop Operating Systems**

1. **CTIT002 - Networking/CompTIA Network+**

CTAN alignment with the Tech Prep Network Systems Pathway in the Career Field Technical Content Standards of the Ohio Department of Education

Course Description:

This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a network. Data communications, network components, the OSI reference model and popular industry communication protocols are explored. Major types of network topologies and infrastructures are discussed. This course will help prepare students for the CompTIA Network+ certification exam.

Advising Notes:

- Career-technical (adult or secondary) program must be an approved Networking or Information Support and Services Information Technology program.
- Students must the CETE End of Course Assessment to be eligible for college credit.
  - Or, hold current CompTIA Network+ certificate
  - Or, hold current Cisco certification
- Students must hold Cisco Certified Network Associate (CCNA) certificate
  - Or hold Cisco Certified Entry Networking Technician (CCENT) certificate
  - Or pass Cisco I and II semester tests (proctored and closed book test environment.)
- Students must access credit within 3 years of program completion or within currency of certificate.

Semester Credit Hours: 3

Alignment:

Learning Outcomes The student will be able to:	Alignment to the 2013 Competencies from the Ohio Department of Education Career Field Technical Content Standards
1. Describe Network Concepts*	**2.2 Apply networking fundamentals to infrastructure systems** **2.2.5 Identify and apply Transmission Control Protocol and Internet Protocol (TCP/IP; Internet Protocol Version 4 [IPv4], Internet Protocol Version 6 [IPv6]) applications and services (e.g., rlogin, Simple Mail Transfer Protocol [SMTP], Telecommunications Network [Telnet], File Transfer Protocol [FTP], Domain Name System [DNS], Network File System [NFS], Voice over Internet Protocol [VoIP], Internet Control Message Protocol [ICMP]).** **2.2.8. Describe the characteristics and uses of networks, network devices, and components (e.g., hubs, switches, routers, firewalls).** **4.2 Describe the Open Systems Interconnection (OSI) standard (International Organization for Standardization [ISO] Standard 7498)** **4.2.1 Identify the benefits of using a layered network model).** **4.2.2 Compare OSI stack positions and their relationships to one another** **4.2.3 Compare the seven layers of the OSI stack to the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack.** **4.2.4 Compare the basics of TCP/IP layers, components, and functions.** **4.2.5 Describe actions to be performed at each of the OSI physical layers.** **4.2.6 Explain how the OSI layers relate to the elements of network communication** **4.7 Describe IP addressing schemes and create subnet masks** **4.7.1 Explain Fully Qualified Domain Names (FQDNs) and how they are used** **4.7.2 Explain the IP addressing scheme and how it is used** **4.7.3 Identify Class A, B, and C reserved (i.e., private) address ranges and why they are used** **4.7.4 Identify the class of network to which a given address belongs.** **4.7.5 Differentiate between default subnet masks and custom subnet masks** **4.7.6 Explain the relationship between an IP address and its associated subnet mask** **4.7.7 Identify the differences between classful and classless addressing schemes** **4.7.8 Identify multicasting addresses and explain why they are used.** **4.7.9 Create custom subnet masks to meet network design requirements** **4.7.10 Compare and contrast Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6)** **4.10 Administer network operating systems and services** **4.10.10. Troubleshoot network performance connectivity (e.g. performance monitor, command line utilities)** **4.11 Implement a hypervisor.** **4.11.2. Provision cloud services (e.g., Software as a Service [SaaS], Platform as a Service [PaaS], Infrastructure as a Service [IaaS], Security as a Service)**

	4.12 Design a wide area network (WAN). **4.12.9 Evaluate and select routing protocols (e.g., Border Gateway Routing Protocol (BGRP), Open Shortest Path First (OSPF), Routing Information Protocol Version 2 (RIPv2])**
2. Perform Network Installation and Configuration*	**4.1 Build a multinode network.** **4.1.6. Configure and build a network** **4.4 Explain wireless communications.** **4.4.1 Compare and contrast wireless standards in common use (e.g. Institute of Electrical and Electronics Engineers [IEEE] 802.11, Bluetooth, Worldwide Interoperability for Microwave Access [WiMAX], Radio Frequency Identification [RFID], Near Field Communication [NFC])** **4.4.2 Compare and contrast characteristics of wireless signals (e.g. reflection, diffraction, scattering, fading)** **4.4.3 Differentiate media access methods used by wireless** **4.4.4 Describe appropriate applications of wireless technologies to specific communication scenarios.** **4.5 Design and implement wireless network solutions.** **4.5.1 Compare and contrast secure wireless solutions operating in ad-hoc mode and infrastructure mode** **4.5.2 Describe the frequency ranges and associated rules in the wireless spectrum as managed by the Federal Communication Commission (FCC)** **4.5.3 Describe the Service Set Identifier (SSID) as used in wireless communications** **4.5.4 Select and install access points, wireless Network Interface Cards (NICs), antennas, and other hardware and software components to provide a wireless networking solution as determined by a site and customer survey** **4.5.5 Troubleshoot Wireless Local Area Networks (WLANs) using system logs, vendor-provided utilities, and diagnostic tools** **4.6 Compare and contrast network protocols.** **4.6.2. Identify the advantages and disadvantages of well-known protocols (e.g., Domain Name System [DNS], File Transfer Protocol [FTP], Secure Hypertext Transfer Protocol [HTTPS], Telecommunications Network [Telnet], Dynamic Host Configuration Protocol [DHCP], Remote Desktop Protocol [RDP]) and associated port numbers** **4.10 Administer network operating systems and services.** **4.10.10. Troubleshoot network performance connectivity (e.g. performance monitor, command line utilities)** **4.10.11. Explain the fundamentals of Quality of Service (QoS)** **4.12 Design a wide area network (WAN).** **4.12.1. Select WAN connections (e.g., satellite, Synchronous Optical Network (SONET), T1, T3, E1, E3, Digital Subscriber Line [DSL], cable, Worldwide Interoperability for Microwave Access [WiMAX], Multiprotocol Label Switching [MPLS], frame relay)** **4.12.3. Evaluate and select basic telecommunications services (e.g., satellite, circuit switching, wireless, packet switching) and carriers for WAN requirements** **4.12.9 Evaluate and select routing protocols (e.g., Border Gateway Routing Protocol (BGRP), Open Shortest Path First (OSPF), Routing Information Protocol Version 2 (RIPv2])**
3. Explain Network Media and Topologies*	**2.2 Apply networking fundamentals to infrastructure systems** **2.2.2. Select the basic point-to- point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, network, mesh, irregular) and broadband and baseband transmission methods**

	2.2.6 Differentiate between cable types (e.g., fiber optic, twisted pair, coaxial) and interfaces **4.3 Select, assemble, terminate, and test media** **4.3.1 Identify the criteria used in selecting media (e.g., physical properties, transmission technologies, transmission span, bandwidth, topology, security, noise immunity, installation considerations, cost)** **4.3.2 Differentiate between media types (e.g., coaxial, twisted pair, fiber optic) and interfaces** **4.3.3 Compare and contrast media categories (e.g., single mode, multimode, CAT5, CAT5E, CAT6+)** **4.3.4 Describe types of media connectors (e.g., Bayonet Neill-Concelman [BNC], Registered Jack [RJ]-45, LC, ST) and grounding techniques** **4.3.5 Identify media standards (e.g., American National Standards Institute [ANSI], Electronic Industries Alliance /Telecommunications Industry Association [EIA/TIA]-568, EIA/TIA-568A and 568B)** **4.3.6 Identify the advantages and disadvantages of cabling systems** **4.3.7 Describe typical problems associated with cable installation.** **4.3.8 Assemble and test Ethernet cable (e.g., straight-through, crossover, loopback)** **4.4 Explain wireless communications.** **4.4.2 Compare and contrast characteristics of wireless signals (e.g., reflection, diffraction, scattering, fading)** **4.4.3 Differentiate media access methods used by wireless** **4.4.4 Describe appropriate applications of wireless technologies to specific communication scenarios** **4.8 Describe network architecture** **4.8.1 Describe media-access protocols (e.g., Carrier Sense Multiple Access with Collision Detection [CSMA/CD], Carrier Sense Multiple Access with Collision Avoidance [CSMA/CA])** **4.8.2 Identify the components of and relationships within the Institute of Electrical and Electronics Engineers (IEEE) 802 standards** **4.8.3 Identify Local Area Network (LAN) performance factors (e.g. signal attenuation, signal propagation delay)** **4.10 Administer network operating systems and services.** **4.10.1. Select physical and logical topology** **4.12 Design a wide area network (WAN).** **4.12.1. Select WAN connections (e.g., satellite, Synchronous Optical Network (SONET), T1, T3, E1, E3, Digital Subscriber Line [DSL], cable, Worldwide Interoperability for Microwave Access [WiMAX], Multiprotocol Label Switching [MPLS], frame relay)** **4.12.2. Describe point-to-point (PTP) and point-to-multipoint (PTMP) interconnection** **4.12.8. Evaluate and select transmission options**
4. Demonstrate Network Management*	**2.11 Select and apply troubleshooting methodologies for problem solving.** **2.11.1. Identify the problem** **2.11.3. Investigate symptoms based on the selected methodology** **2.11.4. Gather and analyze data about the problem** **2.12 Develop performance tests and acceptance plans.** **2.12.2. Develop a test system that accurately mimics external interfaces** **2.12.3. Develop test cases that are realistic, that compare with expected performance, and that include targeted platforms and device types**

	3.4 Explain information technology mechanisms as they apply to a multilayer defense structure. **3.4.3 Compare and contrast network analysis software (e.g., network analyzer) and hardware tools to identify security risks and vulnerabilities** **4.3 Select, assemble, terminate, and test media.** **4.3.7 Describe typical problems associated with cable installation** **4.6 Compare and contrast network protocols.** **4.6.8 Capture and analyze data packets** **4.8 Describe network architecture.** **4.8.3 Identify Local Area Network (LAN) performance factors (e.g. signal attenuation, signal propagation delay)** **4.10 Administer network operating systems and services.** **4.10.10. Troubleshoot network performance connectivity (e.g. performance monitor, command line utilities)** **4.10.11. Explain the fundamentals of Quality of Service (QoS)**
5. Describe Network Security*	**2.1 Describe the need for security and explain security risks and security safeguards** 2.1.12. Practice information security per job requirements **3.1 Components of Information Security: Describe the components associated with information security systems** 3.1.1 Differentiate between authentication and authorization 3.1.2 Compare and contrast authentication techniques (e.g. Single factor, multifactor, passwords, biometrics, certificates, Radio Frequency Identification [RFID] cards) 3.1.3 Compare and contrast methods of achieving information assurance and integrity and confidentiality (e.g. digital signatures, digital certifications, hashing algorithms, encryption) 3.1.4 Describe Virtual Private Networks (VPNs) using tunneling protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Secure Socket Tunneling Protocol [SSTP], Point-to-Point Tunneling Protocol [PPTP]) and encrypting techniques) 3.1.5 Discuss the role of certificate authorities (CAs) and Public Key Infrastructure (PKI) **3.3 Implement and maintain network security** 3.3.1. Describe network security policies (e.g., acceptable use policy) 3.3.2. Identify security appliances and describe the role of each in a networked environment 3.3.3. Devise account administration functions to support network security 3.3.4. Describe Access Control Lists (ACLs) and explain why they are used. 3.3.6. Describe patch management and its purposes. **3.4 Explain information technology mechanisms as they apply to a multilayer defense structure.** 3.4.1. Describe available systems for intrusion prevention, detection, and mitigation 3.4.2. Review system log files to identify security risks 3.4.3. Compare and contrast network analysis software (e.g., network analyzer) and hardware tools to identify security risks and vulnerabilities **3.5 Implement secure wireless networks.** 3.5.1. Describe wireless security risks (e.g., unauthorized access) and how to mitigate them. 3.5.2. Compare and contrast methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wired Equivalent Privacy [WEP], Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication

	Dial In User Service [RADIUS]) 3.5.4. Describe practices and policies for preventing and detecting installation of rogue networks 3.5.5. Describe security practices and policies for personal devices 3.5.6 Implement and test the security of a wireless network **4.6 Compare and contrast network protocols.** 4.6.7. Describe a Virtual Private Network (VPN) and identify associated protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Point-to-Point Tunneling Protocol [PPTP]) **5.1 Learners apply principles of computer programming and software development to develop code; build, test, and debug programs; create finished products; and plan, analyze, design, develop, implement, and support software applications.** 5.1.1. Describe authentication, authorization, and auditing. 5.1.2. Describe multilevel security 5.1.3. Identify security risks and describe associated safeguards and methodologies (e.g., auditing) 5.1.4. Describe major threats to computer systems (e.g., internal threats, viruses, worms, spyware, malware, ransomware, spoofing, hacking) 5.1.5. Describe the components of the physical environment (e.g., wiring closets, server rooms) and physical security systems 5.1.6. Describe the need for security in networking
6. Describe emerging networking technology*	*This is included in the first learning objective Networking Concepts.*

2. Linux: Alignment with the Tech Prep Network Systems Pathway in the Career Field Technical Content Standards of the Ohio Department of Education

Course Description:

This course is designed to teach critical knowledge of installation, operation, administration and troubleshooting services common to all distributions of the Linux operating system. Topics include managing user accounts, command line utilities, file system creation, file system maintenance, access permissions, system backup, and operation system installation. This course will help prepare students for an industry standard certification exam.

Advising Notes:

- Career-technical (adult or secondary) program must be an approved Networking or Information Support and Services Information Technology program.
- Students must pass the CETE End of Course Assessment to be eligible for college credit.
    - Or, hold one the following current certifications: CompTIA Linux+, Linux Professional Institute Junior Exam, Red Hat Certified System Administrator, Novell Certified Linux Administrator
- Students must access credit within 3 years of program completion or within currency of certificate.

Semester Credit Hours: 3

Alignment:

Learning Outcomes **The student will be able to:**	**Alignment to the 2013 Competencies from the Ohio Department of Education Career Field Technical Content Standards**
1. Explain system hardware architecture such as major system devices, peripheral devices, and network connectivity devices*	**2.2 Apply networking fundamentals to infrastructure systems.** 2.2.3. Select network storage techniques (e.g., fiber channel, Internet Small Computer System Interface [iSCSI], Internet Protocol [IP],Fiber Channel over Ethernet [FCoE], Serial Attached SCSI [SAS], Network File Systems [NFS], Network Attached Storage/Server Message Blocks [NAS/SMB], Redundant Array of Inexpensive Disks [RAID]) 2.2.8. Describe the characteristics and uses of networks, network devices, and components (e.g., hubs, switches, routers, firewalls) **2.10 Select, operate, and maintain equipment.** 2.10.1. Identify hardware platforms, configurations, and support models 2.10.2. Identify processor, memory, and storage requirements 2.10.3. Identify architecture requirements
2. Perform Operating System and Application Software Installation*	**2.12 Develop performance tests and acceptance plans.** 2.12.4 Develop, perform, and document usability and testing integration **4.9 Describe and install network operating systems (OSs).** 4.9.1 Explain how the components of a network OS (i.e., server platform, network services software, network redirection software, communications software) all support network operations 4.9.2 Identify licensing requirements. 4.9.3. Describe the characteristics of the tiered model (e.g., peer-to-peer, thin client, thick client, cloud). 4.9.4. Analyze the advantages and disadvantages of the client/server model. 4.9.5. Select network and desktop OSs (e.g., Windows, Linux, MacOS, iOS, Android).

	4.9.6. Install, test, and patch network OSs manually and using automation. 4.9.7 Log in to a network device (e.g., router, Secure File Transfer Protocol [SFTP] server, directory server). 4.9.8 Evaluate the performance of the network OS
3. Use common command line and scripting utilities*	**2.5 Maintain operating systems (OSs).** 2.5.5 Use system utilities to maintain an OS **4.9 Describe and install network operating systems (OSs).** 4.9.1 Explain how the components of a network OS (i.e., server platform, network services software, network redirection software, communications software) all support network operations 4.9.2 Identify licensing requirements 4.9.3. Describe the characteristics of the tiered model (e.g., peer-to-peer, thin client, thick client, cloud) 4.9.4. Analyze the advantages and disadvantages of the client/server model 4.9.5 Select network and desktop OSs (e.g., Windows, Linux, MacOS, iOS, Android). 4.9.6 Install, test, and patch network OSs manually and using automation 4.9.7 Log in to a network device (e.g., router, Secure File Transfer Protocol [SFTP] server, directory server) 4.9.8 Evaluate the performance of the network OS **4.10 Administer network operating systems and services.** 4.10.10. Troubleshoot network performance connectivity (e.g., performance monitor, command line utilities)
4. Manage the Filesystem*	**2.10 Select, operate, and maintain equipment.** 2.10.7 Backup, archive, and manage data **4.10 Administer network operating systems and services.** 4.10.6. Establish shared network resources 4.10.7. Define and set access controls on files, folders, shares, and directories
5. Perform Common Administrative Tasks*	**4.9 Describe and install network operating systems (Oss).** 4.9.7 Log in to a network device (e.g., router, Secure File Transfer Protocol [SFTP] server, directory server) 4.9.8 Evaluate the performance of the network OS **4.10 Administer network operating systems and services.** 4.10.5. Create user accounts, groups, and login scripts 4.10.7. Define and set access controls on files, folders, shares, and directories. 4.10.10. Troubleshoot network performance connectivity (e.g. performance monitor, command line utilities) **4.13 Recommend disaster recovery and business continuity plans.** 4.13.4. Establish process for archiving files
6. Explain and Apply Fundamental Networking concepts and protocols.*	**2.2 Apply networking fundamentals to infrastructure systems.** 2.2.5 Identify and apply Transmission Control Protocol and Internet Protocol (TCP/IP; Internet Protocol Version 4 [IPv4], Internet Protocol Version 6 [IPv6]) applications and services (e.g., rlogin, Simple Mail Transfer Protocol [SMTP], Telecommunications Network [Telnet], File Transfer Protocol [FTP], Domain Name System [DNS], Network File System [NFS], Voice over Internet Protocol [VoIP], Internet Control Message Protocol [ICMP]) 2.2.8. Describe the characteristics and uses of networks, network devices, and components (e.g., hubs, switches, routers, firewalls)

	4.7 Describe IP addressing schemes and create subnet masks 4.7.1. Explain Fully Qualified Domain Names (FQDNs) and how they are used 4.7.2. Explain the IP addressing scheme and how it is used 4.7.3. Identify Class A, B, and C reserved (i.e., private) address ranges and why they are used 4.7.4. Identify the class of network to which a given address belongs 4.7.5. Differentiate between default subnet masks and custom subnet masks 4.7.6. Explain the relationship between an IP address and its associated subnet mask 4.7.7. Identify the differences between classful and classless addressing schemes 4.7.8. Identify multicasting addresses and explain why they are used 4.7.9. Create custom subnet masks to meet network design requirements 4.7.10. Compare and contrast Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) **4.10 Administer network operating systems and services.** 4.10.10 Troubleshoot network performance connectivity (e.g. performance monitor, command line utilities).

3. CTIT013 - Microsoft Server Administration: CTAN alignment with the Tech Prep Network Systems Pathway in the Career Field Technical Content Standards of the Ohio Department of Education

Course Description:

This course trains students in the operations and day to day management of Windows Server. They will examine the server operating system, file services, directory services, software distribution, fault tolerance, remote access as well as system monitoring and troubleshooting. This course will help prepare student to sit for the current Microsoft Server Administrator exam.

Advising Notes:

- Career-technical (adult or secondary) program must be an approved Networking or Information Support and Services Information Technology program.
- Students must pass the CETE End of Course Assessment to be eligible for college credit.
    - Or, student must hold current Microsoft Server Certification. For example, Windows Server 2008, Server Administrator Exam (MS Examination 70-646) or current equivalent exam
- Student must access credit within 3 years of program completion or certification.

Semester Credit Hours: 3

Alignment:

Learning Outcomes The student will be able to:	Alignment to the 2013 Competencies from the Ohio Department of Education Career Field Technical Content Standards
1. Explain and Implement Server Deployment Concepts*	**2.4 Identify trending technologies, their fundamental architecture, and their value in the marketplace.** 2.4.2. Describe the differences, advantages, and limitations of cloud computing (e.g., public cloud, private cloud, hybrid cloud) and on-premises computing 2.4.3. Utilize cloud computing applications (e.g. services, applications, virtual environments) **2.10 Select, operate, and maintain equipment.** 2.10.1. Identify hardware platforms, configurations, and support models 2.10.2. Identify processor, memory, and storage requirements 2.10.3. Identify architecture requirements 2.10.4. Identify software application requirements 2.10.5. Prepare and operate equipment per project design specifications 2.10.6. Monitor equipment operation and troubleshoot issues and problems 2.10.7. Backup, archive, and manage data 2.10.8. Prepare equipment for storage or decommissioning 2.10.9. Perform routine maintenance per manufacturer specifications **2.13 Plan rollout and facilitate handoff to customer.** 2.13.1. Include overall project goals and timelines in the rollout plan 2.13.2. Communicate rollout plans to key stakeholders in a timely manner 2.13.3. Conduct final review and approvals according to company standards 2.13.4. Identify support staff, training needs, and contingency plans in the rollout plan 2.13.5. Test delivered application to assure that it is fully functional for the customer or user and meets all requirements 2.13.6. Deliver support and training materials **4.9 Describe and install network operating systems (OSs).** 4.9.1. Explain how the components of a network OS (i.e., server platform, network services software, network redirection software, communications software) all support network operations) 4.9.2. Identify licensing requirements 4.9.3. Describe the characteristics of the tiered model (e.g., peer-to-peer, thin client, thick client, cloud) 4.9.4. Analyze the advantages and disadvantages of the client/server model 4.9.6. Install, test, and patch network OSs manually and using automation 4.9.7. Log in to a network device (e.g., router, Secure File Transfer Protocol [SFTP] server, directory server) **4.10 Administer network operating systems and services.** 4.10.6. Establish shared network resources
2. Perform Server Management*	**4.9 Describe and install network operating systems (OSs).** 4.9.6. Install, test, and patch network OSs manually and using automation

	4.9.8. Evaluate the performance of the network OS **4.10 Administer network operating systems and services.** 4.10.9. Create roaming user profiles and use Group Policy Objects to manage the user environment 4.10.12 Securely delegate standard management tasks
3. Monitor and Maintain Servers*	**2.1 Describe the need for security and explain security risks and security safeguards.** 2.1.2 Describe authentication, authorization, and auditing 2.1.3 Describe multilevel security 2.1.4 Identify security risks and describe associated safeguards and methodologies (e.g., auditing) 2.1.7. Describe the need for security in networking **2.10 Select, operate, and maintain equipment.** 2.10.1. Identify hardware platforms, configurations, and support models 2.10.2. Identify processor, memory, and storage requirements 2.10.3. Identify architecture requirements 2.10.4. Identify software application requirements 2.10.5. Prepare and operate equipment per project design specifications 2.10.6. Monitor equipment operation and troubleshoot issues and problems 2.10.7. Backup, archive, and manage data 2.10.8. Prepare equipment for storage or decommissioning 2.10.9. Perform routine maintenance per manufacturer specifications **2.12 Develop performance tests and acceptance plans** 2.12.2. Develop a test system that accurately mimics external interfaces 2.12.3. Develop test cases that are realistic, that compare with expected performance, and that include targeted platforms and device types 2.12.4. Develop, perform, and document usability and testing integration 2.13.5. Test delivered application to assure that it is fully functional for the customer or user and meets all requirements **3.3 Implement and maintain network security.** 3.3.1. Describe network security policies (e.g., acceptable use policy) 3.3.2. Identify security appliances and describe the role of each in a networked environment 3.3.4. Describe Access Control Lists (ACLs) and explain why they are used **4.9 Describe and install network operating systems (OSs).** 4.9.6. Install, test, and patch network OSs manually and using automation. **4.10 Administer network operating systems and services.** 4.10.10.Troubleshoot network performance connectivity (e.g., performance monitor, command line utilities)
4. Define Application and Data Provisioning*	**2.4 Identify trending technologies, their fundamental architecture, and their value in the marketplace.** 2.4.3 Utilize cloud computing applications (e.g. services, applications, virtual environments) 2.4.2. Describe the differences, advantages, and limitations of cloud computing (e.g., public cloud, private cloud, hybrid cloud) and on-premises computing 2.6.4. Install and test new software and software upgrades on stand-alone, mobile, and networked systems.

	4.10 Administer network operating systems and services. 4.10.6. Establish shared network resources
5. Plan for Business Continuity and High Availability*	**2.2 Apply networking fundamentals to infrastructure systems.** 2.2.3. Select network storage techniques (e.g., fiber channel, Internet Small Computer System Interface [iSCSI], Internet Protocol [IP], Fiber Channel over Ethernet [FCoE], Serial Attached SCSI [SAS], Network File Systems [NFS], Network Attached Storage/Server Message Blocks [NAS/SMB], Redundant Array of Inexpensive Disks [RAID]) **3.2 Implement and maintain general security compliance.** 3.2.1. Implement backup and verification procedures (e.g., tape, disk, cloud) 3.2.8 Identify the need for disaster recovery policies and procedures **4.13 Recommend disaster recovery and business continuity plans.** 4.13.1. Differentiate between disaster recovery and business continuity 4.13.4. Establish process for archiving files 4.13.5. Develop a disaster recovery plan

4. CTIT005 - Introduction to Desktop Operating Systems: CTAN alignment with the Tech Prep Network Systems Pathway in the Career Field Technical Content Standards of the Ohio Department of Education

Course Description:

This course is a broad overview of computer operating systems. Core operating system concepts are covered. Computer memory utilization is explored, basic security compliance is examined and common system operation procedures are applied. The student will learn to respond to system needs and perform basic backup tasks.

Advising Notes:

- Career-technical (adult or secondary) program must be an approved Networking or Information Support and Services Information Technology program.
- Students must pass the CETE End of Course Assessment to be eligible for college credit.
- Students must access credit within 3 years of program completion or within currency of certificate.

Semester Credit Hours: 3

Alignment:

Learning Outcomes The student will be able to:	Alignment to the 2013 Competencies from the Ohio Department of Education Career Field Technical Content Standards
1. **Explain operating systems***	**2.5 Maintain operating systems (OSs).** 2.5.1 Compare and contrast OSs for computer hardware (e.g. personal computers, servers, mainframes, and mobile devices) 2.5.2 Describe virtual machines and why they are used 2.5.3 Identify the properties of open and proprietary systems 2.5.6. Describe OS interfaces (e.g., command line, Graphic User Interface [GUI]) **2.6 Install and configure hardware and software.** 2.6.1. Comply with license agreements for software and hardware and describe the consequences of noncompliance
3 Implement and maintain security compliance*	**2.1 Describe the need for security and explain security risks and security safeguards.** 2.1.1 Explain the need for confidentiality, integrity, and availability (CIA) of information 2.1.2 Describe authentication, authorization, and auditing 2.1.3 Describe multilevel security 2.1.4 Identify security risks and describe associated safeguards and methodologies (e.g., auditing) 2.1.5 Describe major threats to computer systems (e.g., internal threats, viruses, worms, spyware, malware, ransomware, spoofing, hacking) 2.1.6 Describe the components of the physical environment (e.g., wiring closets, server rooms) and physical security systems 2.1.7 Describe the need for security in networking 2.1.10. Describe computer forensics, its importance in information security and cybersecurity, and its relevance to law enforcement 2.1.11. Identify the need for personal security in digital information and describe how personal information can be safeguarded 2.1.12. Practice information security per job requirements. 2.1.13. Describe privacy security compliance on systems (e.g., Health Insurance Portability and Accountability Act [HIPAA], Payment Card Industry [PCI], Sarbanes-Oxley Act [SOX], Americans with Disabilities Act [ADA]) **3.2 Implement and maintain general security compliance** 3.2.1. Identify and implement data and application security 3.2.2. Implement backup and verification procedures (e.g., tape, disk, cloud) 3.2.3. Describe and assign permissions (e.g., read-only, read-write) 3.2.4. Provide user authentication (e.g., assign and reset user accounts and passwords). 3.2.5. Install, test, implement, and update virus and malware detection and protection software 3.2.6. Identify sources of virus and malware infection and remove viruses and malware 3.2.7. Provide documentation, training, and support to users on established security procedures 3.2.8. Identify the need for disaster recovery policies and procedures

4. **Apply systems operations procedures***	*Combined with maintain and respond to system needs.*
5. **Maintain and respond to system needs***	**1.2 Process, maintain, evaluate, and disseminate information in a business. Develop leadership and team building to promote collaboration.** 1.2.11 Write professional correspondence, documents, job applications, and résumés **1.4 Demonstrate current and emerging strategies and technologies used to collect, analyze, record, and share information in business operations.** 1.4.6. Use electronic database to access and create business and technical information **2.5 Maintain operating systems (OSs).** 2.5.2 Maintain file structures in an OS 2.5.3 Identify the properties of open and proprietary systems 2.5.5 Use system utilities to maintain an OS 2.5.7 Install and test updates and patches to Oss **2.6 Install and configure hardware and software.** 2.6.8 Document the installation and configuration of hardware and Software
6. Perform standard computer backup procedures*	**4.13 Recommend disaster recovery and business continuity plans** 4.13.1 Differentiate between disaster recovery and business continuity 4.13.2 Identify common backup devices 4.13.3 Identify the criteria for selecting a backup system 4.13.4 Establish process for archiving files 4.13.5 Develop a disaster recovery plan

Information Technology/ISS CTAG Alignments

This document contains information about 5 Career-Technical Articulation Numbers (CTANs) for the Information Technology Career-Technical Assurance Guide (CTAG). The CTANs are:

1. CTIT015: CompTia Security+
2. CTIT003: PC Hardware Operation and Maintenance/A+ Essentials*
2. CTIT004: PC Hardware Operation and Maintenance/A+ Practical Application*
***CTIT014: BOTH 003 AND 004 ARE NOW COMBINED INTO ONE CTAN. THE FOLLOWING ALIGNMENT IS FOR THE COMBINED CTAN ***
3. CTIT006: Introduction to User Support
4. CTIT011: Microsoft Windows Desktop Operating System

1. **CTIT015: CompTIA Security+** CTAN alignment with the Tech Prep Pathway in the Career Field Technical Content Standards of the Ohio Department of Education

Semester Credit Hours: 3

Course Description: CompTIA Security+ A current overview of both network and Internet based security practices and conventions; including planning, implementing, and managing network security. Through an exploration of security technologies, a vulnerability assessment and attack method, this course offers methods to minimize potential security risks by means of organizational policy, education and technology. This course helps students prepare for the CompTIA Security+ certification exam.

Advising Notes:

- Career-technical (adult or secondary) program must be an approved Networking or Information Support and Services Information Technology program.
- Students must pass the CETE End of Course Assessment to be eligible for college credit.
    - Or, holds current CompTIA Security+ certification (current exam #SY0-301 or current equivalent exam).
- Student must access credit within 3 years of program completion or within currency of certificate.
- Strongly recommended prerequisite courses: CTIT002 – Networking/CompTIA Network+ **or** CTIT007 Cisco I **and** CTIT005 Introduction to Desktop Operating Systems **or** CTIT011 Microsoft Windows Desktop Operating System
- All learning outcomes marked with an asterisk are considered essential.

Alignment:

Learning Outcomes The student will be able to:	Outcomes and competencies from the REVISED Career Field Technical Content Standards
1. Implement practices to properly harden operating systems and application software on a continuing basis.*	**2.5 Maintain operating systems (OSs).** 2.5.3 Use system utilities to maintain an OS 2.5.7. Install and test updates and patches to OSs **2.12 Develop performance tests and acceptance plans.** 2.12.5. Create a written procedure agreed by the stakeholders and project team for determining the acceptability of the project deliverables 2.12.6. Develop a test system that accurately mimics external interfaces 2.12.7. Develop test cases that are realistic, that compare with expected performance, and that include targeted platforms and device types 2.12.8. Develop, perform, and document usability and testing integration. 2.12.9. Make corrections indicated by test results 2.12.10. Seek stakeholder acceptance upon successful completion of the test plan
2. Identify commonly used ports and protocols, in both wired and wireless communications, their vulnerabilities and methods to mitigate those vulnerabilities.*	**3.5 Implement secure wireless networks.** 3.5.3. Describe wireless security risks (e.g., unauthorized access) and how to mitigate them 3.5.4. Compare and contrast methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wired Equivalent Privacy [WEP], Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dial In User Service [RADIUS]) 3.5.5. Identify security enhancements provided by Institute of Electrical and Electronics Engineers (IEEE) 802.11(x) 3.5.6. Describe practices and policies for preventing and detecting installation of rogue networks 3.5.7. Describe security practices and policies for personal devices. 3.5.8. Implement and test the security of a wireless network **4.6 Compare and contrast network protocols.** 4.6.1 Explain network protocols (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP], User Datagram Protocol (UDP), Internet Protocol Version 4 [IPv4], Internet Protocol Version 6 [IPv6]) 4.6.2 Identify the advantages and disadvantages of well-known protocols (e.g., Domain Name System [DNS], File Transfer Protocol [FTP], Secure Hypertext Transfer Protocol [HTTPS], Telecommunications Network [Telnet], Dynamic Host Configuration Protocol [DHCP], Remote Desktop Protocol [RDP]) and associated port numbers 4.6.5. Identify TCP and UDP conventional ports (e.g., Simple Mail Transfer Protocol [SMTP], Telnet, Hypertext Transfer Protocol [HTTP], FTP) 4.6.6. Explain TCP/IP protocol details (e.g., Internet addresses, Address Resolution Protocol [ARP], Reverse Address Resolution Protocol [RARP], IP datagram format, routing IP datagrams, TCP segment format, IPv4, IPv6)

3. Identify and implement software and hardware tools (IP scanning, packet sniffing, and others) to increase network security.*	**3.4 Explain information technology mechanisms as they apply to a multilayer defense structure.** 3.4.1 Describe available systems for intrusion prevention, detection, and mitigation 3.4.3. Compare and contrast network analysis software (e.g., network analyzer) and hardware tools to identify security risks and vulnerabilities **4.6 Compare and contrast network protocols.** 4.6.8. Capture and analyze data packets
4. Conduct risk and vulnerability assessments and implement appropriate plans to mitigate common risks and vulnerabilities.*	**2.1 Describe the need for security and explain security risks and security safeguards.** 2.1.4 Identify security risks and describe associated safeguards and methodologies (e.g., auditing) 2.1.5 Describe major threats to computer systems (e.g., internal threats, viruses, worms, spyware, malware, ransomware, spoofing, hacking) **3.3 Implement and maintain network security.** 3.3.5 Assess risks based on vulnerability of the organization, likelihood of risk, and impact on the organization **3.4 Explain information technology mechanisms as they apply to a multilayer defense structure.** 3.4.4 Identify the components of human security (e.g., social engineering) and techniques to mitigate human security threats (e.g., policies, procedures, training
5. Implement procedures to properly log system events, review those logs and audit security settings on a regular basis.*	**2.5 Maintain operating systems (OSs).** 2.5.5 Use system utilities to maintain an OS **2.10 Select, operate, and maintain equipment.** 2.10.6 Monitor equipment operation and troubleshoot issues and problems **3.4 Explain information technology mechanisms as they apply to a multilayer defense structure.** 3.4.2 Review system log files to identify security risks
6. Explain and implement redundancy planning, disaster recovery and incident response as means to provide business continuity.*	**3.2 Implement and maintain general security compliance.** 3.2.2 Implement backup and verification procedures (e.g., tape, disk, cloud) 3.2.8 Identify the need for disaster recovery policies and procedures **4.13 Recommend disaster recovery and business continuity plans** 4.13.5. Differentiate between disaster recovery and business continuity 4.13.6. Identify common backup devices 4.13.7. Identify the criteria for selecting a backup system 4.13.8. Establish process for archiving files 4.13.9. Develop a disaster recovery plan
7. Explain the impact of organizational policy, state and federal legislation, and environmental controls on security planning.*	**2.1 Describe the need for security and explain security risks and security safeguards.** 2.1.12 Practice information security per job requirements 2.1.13 Describe privacy security compliance on systems (e.g., Health Insurance Portability and Accountability Act [HIPAA], Payment Card Industry [PCI], Sarbanes-Oxley Act [SOX], Americans with Disabilities Act [ADA]) **3.3 Implement and maintain network security.** 3.3.1 Describe network security policies (e.g., acceptable use policy)

8. Compare and contrast access control methods including role based, discretionary, mandatory and rule based and implement appropriately to secure network resources.*	**3.2 Implement and maintain general security compliance.** 3.2.3 Describe and assign permissions (e.g., read-only, read-write) 3.2.4 Provide user authentication (e.g., assign and reset user accounts and passwords). **3.3 Implement and maintain network security.** 3.3.3 Devise account administration functions to support network security 3.3.4 Describe Access Control Lists (ACLs) and explain why they are used **4.10 Administer network operating systems and services.** 4.10.6 Establish shared network resources 4.10.7 Define and set access controls on files, folders, shares, and directories
9. Summarize and deploy various authentication methods including password based, biometric and certificate based models.*	**2.1 Describe the need for security and explain security risks and security safeguards.** 2.1.2 Describe authentication, authorization, and auditing **3.1 Describe the components associated with information security systems.** 3.1.1 Differentiate between authentication and authorization 3.1.2 Compare and contrast authentication techniques (e.g. single factor, multifactor, passwords, biometrics, certificates, Radio Frequency Identification [RFID] cards) **3.2 Implement and maintain general security compliance.** 3.2.4 Provide user authentication (e.g., assign and reset user accounts and passwords).
10. Explain general cryptographic concepts including hashing, symmetric and asymmetric encryption, digital certificates and public key infrastructure (PKI)*	**3.1 Describe the components associated with information security systems.** 3.1.3 Compare and contrast methods of achieving information assurance and integrity and confidentiality (e.g. digital signatures, digital certifications, hashing algorithms, encryption) 3.1.5 Discuss the role of certificate authorities (CAs) and Public Key Infrastructure (PKI)
11. Explain secure protocols including Secure Socket Layer (SSL) and IPSec to provide encrypted communication*	**3.1 Describe the components associated with information security systems.** 3.1.4 Describe Virtual Private Networks (VPNs) using tunneling protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Secure Socket Tunneling Protocol [SSTP], Point-to-Point Tunneling Protocol [PPTP]) and encrypting techniques) **4.6 Compare and contrast network protocols.** 4.6.2. Identify the advantages and disadvantages of well-known protocols (e.g., Domain Name System [DNS], File Transfer Protocol [FTP], Secure Hypertext Transfer Protocol [HTTPS], Telecommunications Network [Telnet], Dynamic Host Configuration Protocol [DHCP], Remote Desktop Protocol [RDP]) and associated port numbers 4.6.7 Describe a Virtual Private Network (VPN) and identify associated protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Point-to-Point Tunneling Protocol [PPTP])

2. **CTIT014: PC Operating System and Hardware Operation and Maintenance/A+**
CTAN alignment with the Tech Prep Pathway in the Career Field Technical Content Standards of the Ohio Department of Education

Semester Credit Hours: 3

Course Description CTIT014: PC Operating System and Hardware Operation and Maintenance/A+:
This course provides basic knowledge for properly installing, configuring, upgrading, maintaining and troubleshooting modern computer hardware including CPUs, storage devices, adapters, video displays, printers and communication devices. Coverage includes desktop and server systems, basic networking and security; it includes functions and characteristics of operating systems in common use. Emphasis will be given to the current Windows operating system, small office/home office (SOHO) networks and security practices for both. This course will ***help*** students prepare for the CompTIA A+ certification exam. It should be noted, however, that additional test preparation work is recommended before attempting the actual certification exam.

Advising Notes:
Career-technical (adult or secondary) program must be an approved Networking or Information Support and Services Information Technology program.

- Students must pass the CETE End of Course Assessment to be eligible for college credit.
  - Or, hold current CompTIA A+ certificate (current exams #220-801 and 220-802 or current equivalent exam)
- All learning outcomes marked with an asterisk are considered essential.
- Must access credit within 3 years of program completion or within currency of certificate.

Alignment:

Learning Outcomes The student will be able to:	**Outcomes and/or Competencies in ODE's REVISED Career Field Technical Content Standards**
1. Explain, compare and contrast common hardware components of a modern personal computer including storage devices, motherboards, power supplies, processors, memory, display, printers and other peripherals.*	**2.6 Install and configure hardware and software.** 2.6.6 Determine compatibility of software and hardware and resolve any conflicts. 2.6.7 Install and test hardware peripherals 2.6.8 Document the installation and configuration of hardware and software. **2.10 Select, operate, and maintain equipment.** 2.10.1 Identify hardware platforms, configurations, and support models. 2.10.2 Identify processor, memory, and storage requirements. 2.10.3 Identify architecture requirements. 2.10.4 Identify software application requirements. 2.10.5 Prepare and operate equipment per project design specifications. 2.10.6 Monitor equipment operation and troubleshoot issues and problems. 2.10.7 Backup, archive, and manage data.

	2.10.8 Prepare equipment for storage or decommissioning. 2.10.9 Perform routine maintenance per manufacturer specifications.
2. Install and configure hardware and software components including printers, multimedia devices, scanners, video devices, etc.*	**2.6 Install and configure hardware and software.** 2.6.6 Determine compatibility of software and hardware and resolve any conflicts. 2.6.7 Install and test hardware peripherals 2.6.8 Document the installation and configuration of hardware and software.
3. Interpret common hardware and software symptoms and apply appropriate troubleshooting methods to resolve the identified problems.*	**2.11 Select and apply troubleshooting methodologies for problem solving.** 2.11.1. Identify the problem. 2.11.2. Select troubleshooting methodology (e.g. top down, bottom up, follow the path, and spot the differences). 2.11.3. Investigate symptoms based on the selected methodology. 2.11.4. Gather and analyze data about the problem. 2.11.5. Design a solution. 2.11.6. Test a solution. 2.11.7. Implement a solution. 2.11.8. Document the problem and the verified solution.
4. Compare and contrast common versions of the Windows operating system, their features, installation methods and utilities.*	**2.5 Maintain operating systems (OSs).** 2.5.1. Compare and contrast OSs for computer hardware (e.g. personal computers, servers, mainframes, and mobile devices). 2.5.2. Describe virtual machines and why they are used 2.5.3. Identify the properties of open and proprietary systems. 2.5.4. Maintain file structures in an OS. 2.5.5. Use system utilities to maintain an OS. 2.5.6. Describe OS interfaces (e.g., command line, Graphic User Interface [GUI]). 2.5.7. Install and test updates and patches to OSs.
5. Summarize basic networking fundamentals including devices (hubs, switches, routers, etc.), protocols (TCP/IP, HTTP, FTP, SMTP, etc.), media (UTP, STP, fiber or coaxial) and types (wireless, Bluetooth, cellular and others).*	**2.2 Apply networking fundamentals to infrastructure systems.** 2.2.1 Differentiate between Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), and Near Field Communication (NFC). 2.2.2 Select the basic point-to-point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, network, mesh, irregular) and broadband and baseband transmission methods. 2.2.3 Select network storage techniques (e.g., fiber channel, Internet Small Computer System Interface [iSCSI], Internet Protocol [IP], Fiber Channel over Ethernet [FCoE], Serial Attached SCSI [SAS], Network File Systems [NFS], Network Attached Storage/Server Message Blocks [NAS/SMB], and Redundant Array of Inexpensive Disks [RAID]). 2.2.4 Differentiate between the Internet, intranets, and extranets. 2.2.5 Identify and apply Transmission Control Protocol and Internet Protocol (TCP/IP), Internet Protocol Version 4 (IPv4), Internet Protocol Version 6 (IPv6) applications and services (e.g. rlogin, Simple Mail Transfer Protocol [SMTP], Telecommunications Network [Telnet], File Transfer Protocol [FTP], Domain Name System [DNS], Network File System [NFS], Voice over Internet Protocol [VoIP], Internet Control Message Protocol [ICMP]).

	2.2.6 Differentiate between cable types (e.g., fiber optic, twisted pair, coaxial) and interfaces. 2.2.7 Identify the top-level domains (e.g., .gov, .com, .edu). 2.2.8 Describe the characteristics and uses of networks, network devices, and components (e.g. hubs, switches, routers, firewalls). **4.3 Select, assemble, terminate, and test media.** 4.3.1 Identify the criteria used in selecting media (e.g., physical properties, transmission technologies, transmission span, bandwidth, topology, security, noise immunity, installation considerations, and cost). 4.3.3 Compare and contrast media categories (e.g., single mode, multimode, CAT5, CAT5e, CAT6+)
6. Explain basic principles and concepts of securing networks and devices including encryption, firewalls, authentication, authorization, malicious software, etc.*	**3.1 Describe the components associated with information security systems.** 3.1.1 Differentiate between authentication and authorization. 3.1.2 Compare and contrast authentication techniques (e.g. single factor, multifactor, passwords, biometrics, certificates, Radio Frequency Identification [RFID] cards). 3.1.3 Compare and contrast methods of achieving information assurance and integrity and confidentiality (e.g. digital signatures, digital certifications, hashing algorithms, encryption). 3.1.4 Describe Virtual Private Networks (VPNs) using tunneling protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Secure Socket Tunneling Protocol [SSTP], Point-to-Point Tunneling Protocol [PPTP]) and encrypting techniques). 3.1.5 Discuss the role of certificate authorities (CAs) and Public Key Infrastructure (PKI). **3.2 Implement and maintain general security compliance.** 3.2.2. Identify and implement data and application security. 3.2.3. Implement backup and verification procedures (e.g., tape, disk, cloud). 3.2.4. Describe and assign permissions (e.g., read-only, read-write). 3.2.5. Provide user authentication (e.g., assign and reset user accounts and passwords). 3.2.6. Install, test, implement, and update virus and malware detection and protection software. 3.2.7. Identify sources of virus and malware infection and remove viruses and malware. 3.2.8. Provide documentation, training, and support to users on established security procedures. 3.2.9. Identify the need for disaster recovery policies and procedures. **3.4 Explain information technology mechanisms as they apply to a multilayer defense structure.** 3.4.1. Describe available systems for intrusion prevention, detection, and mitigation. 3.4.2. Review system log files to identify security risks. 3.4.3. Compare and contrast network analysis software (e.g., network analyzer) and hardware tools to identify security risks and vulnerabilities. 3.4.4. Identify the components of human security (e.g., social engineering) and techniques to mitigate human security threats (e.g., policies, procedures, training). **3.5: Wireless Security: Implement secure wireless network.** 3.5.1. Describe wireless security risks (e.g., unauthorized access) and how to mitigate them. 3.5.2. Compare and contrast methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wired Equivalent Privacy [WEP], Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dialup User Service [RADIUS]). 3.5.3. Identify security enhancements provided by Institute of Electrical and Electronics Engineers (IEEE) 802.11(x).

	3.5.4. Describe practices and policies for preventing and detecting installation of rogue networks. 3.5.5. Describe security practices and policies for personal devices. 3.5.6. Implement and test the security of a wireless network.
7. Outline appropriate operational procedures to address safety and environmental issues and their impact on customers.*	**2.12: Performance Tests and Acceptance Plans: Develop performance tests and acceptance plans.** 2.12.1. Create a written procedure agreed by the stakeholders and project team for determining the acceptability of the project deliverables. 2.12.2. Develop a test system that accurately mimics external interfaces. 2.12.3. Develop test cases that are realistic, that compare with expected performance, and that include targeted platforms and device types. 2.12.4. Develop, perform, and document usability and testing integration. 2.12.5. Make corrections indicated by test results. 2.12.6 Seek stakeholder acceptance upon successful completion of the test plan. **2.13 Plan rollout and facilitate handoff to customer.** 2.13.1. Include overall project goals and timelines in the rollout plan. 2.13.2. Communicate rollout plans to key stakeholders in a timely manner. 2.13.3. Conduct final review and approvals according to company standards. 2.13.4. Identify support staff, training needs, and contingency plans in the rollout plan. 2.13.5. Test delivered application to assure that it is fully functional for the customer or user and meets all requirements. 2.13.6. Deliver support and training materials.
8. Install, configure, maintain, troubleshoot and repair components of a modern personal computer, both desktop and laptop, including storage devices, motherboards, processors, memory, adapters and printers using appropriate tools.*	**2.6 Install and configure hardware and software.** 2.6.6 Determine compatibility of software and hardware and resolve any conflicts. 2.6.7 Install and test hardware peripherals 2.6.8 Document the installation and configuration of hardware and software. **2.10 Select, operate, and maintain equipment.** 2.10.1 Identify hardware platforms, configurations, and support models. 2.10.2 Identify processor, memory, and storage requirements. 2.10.3 Identify architecture requirements. 2.10.4 Identify software application requirements. 2.10.5 Prepare and operate equipment per project design specifications. 2.10.6 Monitor equipment operation and troubleshoot issues and problems. 2.10.7 Backup, archive, and manage data. 2.10.8 Prepare equipment for storage or decommissioning. 2.10.9 Perform routine maintenance per manufacturer specifications.
9. Differentiate between recent versions of Windows Client Operating Systems in their directory structure including user	**2.5 Maintain operating systems (OSs).** 2.5.1. Compare and contrast OSs for computer hardware (e.g. personal computers, servers, mainframes, and mobile devices). 2.5.2. Describe virtual machines and why they are used 2.5.3. Identify the properties of open and proprietary systems. 2.5.4. Maintain file structures in an OS.

folder locations, program files, temporary files and offline files and folders.*	2.5.5. Use system utilities to maintain an OS. 2.5.6. Describe OS interfaces (e.g., command line, Graphic User Interface [GUI]). 2.5.7. Install and test updates and patches to OSs.
10. For recent versions of Windows Client Operating Systems, use system utilities (device manager, disk management, administrative tools, task manager, etc.) and command line tools (msconfig, chkdsk, copy, format, ipconfig, pint, etc.) to troubleshoot and resolve issues.*	**2.5 Maintain operating systems (OSs).** 2.5.1. Compare and contrast OSs for computer hardware (e.g. personal computers, servers, mainframes, and mobile devices). 2.5.2. Describe virtual machines and why they are used. 2.5.3. Identify the properties of open and proprietary systems. 2.5.4. Maintain file structures in an OS. 2.5.5. Use system utilities to maintain an OS. 2.5.6. Describe OS interfaces (e.g., command line, Graphic User Interface [GUI]). 2.5.7. Install and test updates and patches to OSs.
11. Troubleshoot and resolve client-networking problems using protocol (TCP/IP, FTP, SMTP, etc.) settings, firewall configuration settings and system tools (ping, tracert, nslookup, ipconfig, etc.).*	**2.2 Apply networking fundamentals to infrastructure systems.** 2.2.5 Identify and apply Transmission Control Protocol and Internet Protocol (TCP/IP; Internet Protocol Version 4 [IPv4], Internet Protocol Version 6 [IPv6]) applications and services (e.g., rlogin, Simple Mail Transfer Protocol [SMTP], Telecommunications Network [Telnet], File Transfer Protocol [FTP], Domain Name System [DNS], Network File System [NFS], Voice over Internet Protocol [VoIP], Internet Control Message Protocol [ICMP]). 2.2.6 Differentiate between cable types (e.g., fiber optic, twisted pair, coaxial) and interfaces. **2.11 Select and apply troubleshooting methodologies for problem solving.** 2.11.1. Identify the problem. 2.11.2. Select troubleshooting methodology (e.g. top down, bottom up, follow the path, spot the differences). 2.11.3 Investigate symptoms based on the selected methodology. 2.11.4 Gather and analyze data about the problem. 2.11.5 Design a solution. 2.11.6 Test a solution. 2.11.7 Implement a solution. 2.11.8 Document the problem and the verified solution. **3.5 Implement secure wireless networks.** 3.5.1 Describe wireless security risks (e.g., unauthorized access) and how to mitigate them 3.5.2 Compare and contrast methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wired Equivalent Privacy [WEP], Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dialup User Service [RADIUS]). 3.5.3 Identify security enhancements provided by Institute of Electrical and Electronics Engineers (IEEE) 802.11(x). 3.5.4 Describe practices and policies for preventing and detecting installation of rogue networks. 3.5.5 Describe security practices and policies for personal devices.

	3.5.6 Implement and test the security of a wireless network. **4.1 Build a multinode network.** 4.1.3 Compare the characteristics of connection-oriented and connectionless protocols and select protocols based on given criteria. **4.3 Select, assemble, terminate, and test media.** 4.3.3. Compare and contrast media categories (e.g., single mode, multimode, CAT5, CAT5E, CAT6+ 4.3.1. Identify the criteria used in selecting media (e.g., physical properties, transmission technologies, transmission span, bandwidth, topology, security, noise immunity, installation considerations, and cost).
12. Install and configure a fully featured small office or home office (SOHO) network including a shared broadband connection (DSL, cable, ISDN or satellite), wireless devices using encrypted communication methods, routers/access points, bluetooth and firewall devices.*	**3.5 Implement secure wireless networks.** 3.5.1 Describe wireless security risks (e.g., unauthorized access) and how to mitigate them 3.5.2 Compare and contrast methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wired Equivalent Privacy [WEP], Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dial In User Service [RADIUS]). 3.5.3 Identify security enhancements provided by Institute of Electrical and Electronics Engineers (IEEE) 802.11(x). 3.5.4 Describe practices and policies for preventing and detecting installation of rogue networks. 3.5.5 Describe security practices and policies for personal devices. 3.5.6 Implement and test the security of a wireless network. **4.3 Select, assemble, terminate, and test media.** 4.3.1 Identify the criteria used in selecting media (e.g., physical properties, transmission technologies, transmission span, bandwidth, topology, security, noise immunity, installation considerations, cost). 4.3.2 Differentiate between media types (e.g., coaxial, twisted pair, fiber optic) and interfaces. 4.3.3 Compare and contrast media categories (e.g., single mode, multimode, CAT5, CAT5E, CAT6+) 4.3.4 Describe types of media connectors (e.g., Bayonet Neill-Concelman [BNC], Registered Jack [RJ]-45, LC, ST) and grounding techniques. 4.3.5 Identify media standards (e.g., American National Standards Institute [ANSI], Electronic Industries Alliance/Telecommunications Industry Association [EIA/TIA]-568, EIA/TIA-568A and 568B). 4.3.6 Identify the advantages and disadvantages of cabling systems. 4.3.7 Describe typical problems associated with cable installation. 4.3.8 Assemble and test Ethernet cable (e.g., straight-through, crossover, loopback).
13. Install and configure system software to reduce the risk of malware infection via scheduled system scans and signature updates and identify, quarantine and repair infected systems.*	2.1.4 Identify security risks and describe associated safeguards and methodologies (e.g., auditing). 2.1.5 Describe major threats to computer systems (e.g., internal threats, viruses, worms, spyware, malware, ransomware, spoofing, hacking). **3.2 Implement and maintain general security compliance.** 3.2.5. Install, test, implement, and update virus and malware detection and protection software. 3.2.6. Identify sources of virus and malware infection and remove viruses and malware

14. Increase operating system security by managing local users and groups, file and folder permissions, share permissions, encryption and BIOS security*	**3.2 Implement and maintain general security compliance.** 3.2.3 Describe and assign permissions (e.g., read-only, read-write). 3.2.4 Provide user authentication (e.g., assign and reset user accounts and passwords).

3. CTIT006: Introduction to User Support

This CTAN corresponds to the Microsoft Certification Exam #70-685 Enterprise Desktop Support Technician for Windows 7; or successor exams and operating systems as released by Microsoft. CTAN alignment with the Tech Prep Pathway in the Career Field Technical Content Standards of the Ohio Department of Education

Course Description: CTIT006

Introduction to the skills and abilities required to provide technical support and assistance to computer users with an emphasis on current Microsoft Client operating systems. Additional emphasis is on customer service, problem solving and communication skills (needs analysis, troubleshooting and interaction with users). Topics include service concepts, technical skill sets, career paths, strategies to provide technical support and operations of the help desk and user support industry.

Advising Notes:

- Career-technical (adult or secondary) program must be an approved Information Support and Services Information Technology program.
- Students must pass the CETE End of Course Assessment to be eligible for college credit.
  - Or, hold current Microsoft Enterprise Desktop Support Technician (current Exam #70-685 or current equivalent exam)
- Student must access credit within 3 years of program completion or within currency of certificate.
- All learning outcomes marked with an asterisk are considered essential.

Semester Credit Hours: 3

Alignment:

Learning Outcomes The student will be able to:	**Outcomes and/or Competencies in ODE's Revised Career Field Technical Content Standards**
1. Identify causes of and resolution for desktop application issues including installation related issues and general software failures.*	**2.6 Install and configure hardware and software.** 2.6.3 Verify software compatibility and troubleshoot any software incompatibility 2.6.4 Install and test new software and software upgrades on stand-alone, mobile, and networked systems 2.6.6 Determine compatibility of software and hardware and resolve any conflicts **2.10 Select, operate, and maintain equipment.** 2.10.4 Identify software application requirements **2.11 Select and apply troubleshooting methodologies for problem solving**

	2.11.1. Identify the problem 2.11.2. Select troubleshooting methodology (e.g. top down, bottom up, follow the path, spot the differences) 2.11.3. Investigate symptoms based on the selected methodology. 2.11.4. Gather and analyze data about the problem 2.11.5. Design a solution 2.11.6. Test a solution 2.11.7. Implement a solution 2.11.8. Document the problem and the verified solution
2. Identify causes of and resolution for networking issues including connectivity, name resolution, logon and printing issues.*	**2.2 Apply networking fundamentals to infrastructure systems** 2.2.1. Differentiate between Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), and Near Field Communication (NFC) 2.2.2. Select the basic point-to-point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, network, mesh, irregular) and broadband and baseband transmission methods 2.2.3. Select network storage techniques (e.g., fiber channel, Internet Small Computer System Interface [iSCSI], Internet Protocol [IP], Fiber Channel over Ethernet [FCoE], Serial Attached SCSI [SAS], Network File Systems [NFS], Network Attached Storage /Server Message Blocks [NAS/SMB], Redundant Array of Inexpensive Disks [RAID]) 2.2.4. Differentiate between the Internet, intranets, and extranets. 2.2.5. Identify and apply Transmission Control Protocol and Internet Protocol (TCP/IP; Internet Protocol Version 4 [IPv4], Internet Protocol Version 6 [IPv6]) applications and services (e.g., rlogin, Simple Mail Transfer Protocol [SMTP], Telecommunications Network [Telnet], File Transfer Protocol [FTP], Domain Name System [DNS], Network File System [NFS], Voice over Internet Protocol [VoIP], Internet Control Message Protocol [ICMP]) 2.2.6. Differentiate between cable types (e.g., fiber optic, twisted pair, coaxial) and interfaces 2.2.7. Identify the top-level domains (e.g., .gov, .com, .edu) 2.2.8. Describe the characteristics and uses of networks, network devices, and components (e.g., hubs, switches, routers, firewalls) **2.11 Select and apply troubleshooting methodologies for problem solving** 2.11.1 Identify the problem 2.11.2 Select troubleshooting methodology (e.g. top down, bottom up, follow the path, spot the differences) 2.11.3 Investigate symptoms based on the selected methodology 2.11.4 Gather and analyze data about the problem 2.11.5 Design a solution 2.11.6 Test a solution 2.11.7 Implement a solution 2.11.8 Document the problem and the verified solution **4.5 Design and implement wireless network solutions.** 4.5.5 Troubleshoot Wireless Local Area Networks (WLANs) using system logs, vendor-provided utilities, and diagnostic tools **4.10 Administer network operating systems and services.**

	4.10.6 Establish shared network resources 4.10.10 Troubleshoot network performance connectivity (e.g., performance monitor, command line utilities)
3. Manage and maintain systems that run the current Microsoft client operating system including performance issues and common hardware failures.*	**2.5 Maintain operating systems (OSs).** 2.5.1. Compare and contrast OSs for computer hardware (e.g. personal computers, servers, mainframes, and mobile devices) 2.5.2. Describe virtual machines and why they are used 2.5.3. Identify the properties of open and proprietary systems 2.5.4. Maintain file structures in an OS 2.5.5. Use system utilities to maintain an OS 2.5.6. Describe OS interfaces (e.g., command line, Graphic User Interface [GUI]) 2.5.7. Install and test updates and patches to OSs. **4.9 Describe and install network operating systems (OSs).** 4.9.5. Select network and desktop OSs (e.g., Windows, Linux, MacOS, iOS, Android) 4.9.6. Install, test, and patch network OSs manually and using automation **4.10 Administer network operating systems and services** 4.10.1. Select physical and logical topology 4.10.2. Connect devices to network systems. 4.10.3. Create domain trusts 4.10.4. Maintain domain controllers 4.10.5. Create user accounts, groups, and login scripts 4.10.6. Establish shared network resources. 4.10.7. Define and set access controls on files, folders, shares, and directories 4.10.8. Configure network domain accounts and profiles 4.10.9. Create roaming user profiles and use Group Policy Objects to manage the user environment 4.10.10. Troubleshoot network performance connectivity (e.g., performance monitor, command line utilities) 4.10.11. Explain the fundamentals of Quality of Service (QoS) 4.10.12. Securely delegate standard management tasks
4. Support mobile users and issues they report including wireless connectivity and remote access issues.*	**3.1 Describe the components associated with information security systems.** 3.1.4 Describe Virtual Private Networks (VPNs) using tunneling protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Secure Socket Tunneling Protocol [SSTP], Point-to-Point Tunneling Protocol [PPTP]) and encrypting techniques) **3.5 Implement secure wireless networks** 3.5.1. Describe wireless security risks (e.g., unauthorized access) and how to mitigate them 3.5.2. Compare and contrast methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wired Equivalent Privacy [WEP], Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dial In User Service [RADIUS]) 3.5.3. Identify security enhancements provided by Institute of Electrical and Electronics Engineers (IEEE) 802.11(x) 3.5.4. Describe practices and policies for preventing and detecting installation of rogue networks 3.5.5. Describe security practices and policies for personal devices

	3.5.6. Implement and test the security of a wireless network **4.4 Explain wireless communications.** 4.4.1. Compare and contrast wireless standards in common use (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.11, Bluetooth, Worldwide Interoperability for Microwave Access [WiMAX], Radio Frequency Identification [RFID], Near Field Communication [NFC]) 4.4.2. Compare and contrast characteristics of wireless signals (e.g., reflection, diffraction, scattering, fading) 4.4.3. Differentiate media access methods used by wireless 4.4.4. Describe appropriate applications of wireless technologies to specific communication scenarios **4.5 Design and implement wireless network solutions** 4.5.1 Compare and contrast secure wireless solutions operating in ad-hoc mode and infrastructure mode 4.5.2 Describe the frequency ranges and associated rules in the wireless spectrum as managed by the Federal Communication Commission (FCC) 4.5.3 Describe the Service Set Identifier (SSID) as used in wireless communications. 4.5.4 Select and install access points, wireless Network Interface Cards (NICs), antennas, and other hardware and software components to provide a wireless networking solution as determined by a site and customer survey 4.5.5 Troubleshoot Wireless Local Area Networks (WLANs) using system logs, vendor-provided utilities, and diagnostic tools 4.5.6 Secure the wireless network **4.6 Compare and contrast network protocols.** 4.6.7 Describe a Virtual Private Network (VPN) and identify associated protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Point-to-Point Tunneling Protocol [PPTP])
5. Identify causes of and resolution of security issues including resolving incidents related to malicious software, web browsers and cryptographic key management.*	**2.1 Describe the need for security and explain security risks and security safeguards** 2.1.1 Explain the need for confidentiality, integrity, and availability (CIA) of information 2.1.2 Describe authentication, authorization, and auditing 2.1.3 Describe multilevel security 2.1.4 Identify security risks and describe associated safeguards and methodologies (e.g., auditing) 2.1.5 Describe major threats to computer systems (e.g., internal threats, viruses, worms, spyware, malware, ransomware, spoofing, hacking) 2.1.6 Describe the components of the physical environment (e.g., wiring closets, server rooms) and physical security systems 2.1.7 Describe the need for security in networking 2.1.8 Describe the need for security in application development 2.1.9 Track and catalogue physical assets 2.1.10 Describe computer forensics, its importance in information security and cybersecurity, and its relevance to law enforcement 2.1.11 Identify the need for personal security in digital information and describe how personal information can be safeguarded 2.1.12 Practice information security per job requirements 2.1.13 Describe privacy security compliance on systems (e.g., Health Insurance Portability and Accountability Act [HIPAA], Payment Card Industry [PCI], Sarbanes-Oxley Act [SOX], Americans with Disabilities Act [ADA])

	2.5 Maintain operating systems (OSs). 2.5.5 Use system utilities to maintain an OS 2.5.6 Describe OS interfaces (e.g., command line, Graphic User Interface [GUI]) 2.5.7 Install and test updates and patches to Oss **2.8 Describe the fundamentals of databases.** 2.8.8 Explain the importance of data integrity and security **3.2 Implement and maintain general security compliance.** 3.2.5 Install, test, implement, and update virus and malware detection and protection software 3.2.6 Identify sources of virus and malware infection and remove viruses and malware **3.4 Explain information technology mechanisms as they apply to a multilayer defense structure** 3.4.1. Describe available systems for intrusion prevention, detection, and mitigation 3.4.2. Review system log files to identify security risks 3.4.3. Compare and contrast network analysis software (e.g., network analyzer) and hardware tools to identify security risks and vulnerabilities 3.4.4. Identify the components of human security (e.g., social engineering) and techniques to mitigate human security threats (e.g., policies, procedures, training) **3.5 Implement secure wireless networks** 3.5.1. Describe wireless security risks (e.g., unauthorized access) and how to mitigate them 3.5.2. Compare and contrast methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wired Equivalent Privacy [WEP], Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dial In User Service [RADIUS]) 3.5.3. Identify security enhancements provided by Institute of Electrical and Electronics Engineers (IEEE) 802.11(x) 3.5.4. Describe practices and policies for preventing and detecting installation of rogue networks 3.5.5. Describe security practices and policies for personal devices 3.5.6. Implement and test the security of a wireless network **4.7 Describe IP addressing schemes and create subnet masks.** 4.7.11. Describe methods of securely transmitting dat. 4.7.12. Describe ways to present data (e.g., mobile applications, desktop applications, web applications) 4.7.13. Differentiate between a client and a server. 4.7.14. Identify how the use of different browsers and devices affects the look of a webpage 4.7.15. Explain the relationship between data transmission volumes, bandwidth, and latency 4.7.16. Describe the characteristics and use of browser plug-ins. 4.7.17. Compare the advantages and disadvantages of running an in-house server or using a service provider 4.7.18. Describe the difference between static and dynamic sites and the reasons for using each

4. CTIT011: Microsoft Windows Desktop Operating System This CTAN corresponds to the Microsoft Certification Exam: #70-680, #70-682 or #70-685 for Windows 7, or #70-687 or #70-688 for Windows 8.1; or successor exams and operating systems as released by Microsoft. CTAN alignment with the Tech Prep Pathway in the Career Field Technical Content Standards of the Ohio Department of Education

Semester Credit Hours: 3

Course Description: CTIT011 Windows Desktop OS:
Perform clean installations of or upgrades to the current Windows client operating system from previous versions of Windows including the migration of user profiles. Create and manage system images as a method of deployment. Configure aspects of a Windows client including hardware devices and application software; network connectivity including IPv4 and IPv6, firewall settings and remote management; and mobile computing features of Windows including BitLocker, DirectAccess and remote connectivity. Manage access to resources via authentication, authorization and user account control. Manage and monitor systems including system performance, backup and recovery. This course helps prepare students for a current Microsoft desktop based certification exam.

Advising Notes:

- Career-technical (adult or secondary) program must be an approved Networking or Information Support and Services Information Technology program.
- Student must pass the CETE End of Course Assessment to be eligible for college credit.
    - Or, hold current Microsoft Client Operating System certification (current exams #70-620 or 70-680 or current equivalent exam).
- Student must access credit within 3 years of program completion or within currency of certificate.
- All learning outcomes marked with an asterisk are considered essential.

Alignment:

Learning Outcomes The student will be able to:	**Outcomes and/or Competencies in ODE's REVISED Career Field Technical Content Standards**
1. Manage the installation of the current Microsoft desktop operating system as a clean install or an upgrade from a previous version including the migration of user data.*	**2.5: Operating Systems: Maintain operating systems (OSs).** 2.5.1. Compare and contrast OSs for computer hardware (e.g. personal computers, servers, mainframes, and mobile devices) 2.5.2. Describe virtual machines and why they are used 2.5.3. Identify the properties of open and proprietary systems 2.5.4. Maintain file structures in an OS 2.5.5. Use system utilities to maintain an OS 2.5.6. Describe OS interfaces (e.g., command line, Graphic User Interface [GUI]) 2.5.7. Install and test updates and patches to Oss **4.9 Describe and install network operating systems (OSs).** 4.9.5. Select network and desktop OSs (e.g., Windows, Linux, MacOS, iOS, Android) 4.9.6. Install, test, and patch network OSs manually and using automation

2. Create, modify and deploy system images as a method of installation.*	**4.9 Describe and install network operating systems (OSs).** 4.9.6 Install, test, and patch network OSs manually and using automation
3. Configure hardware devices and their associated drivers*	**2.5 Maintain operating systems (OSs).** 2.5.1 Compare and contrast OSs for computer hardware (e.g. personal computers, servers, mainframes, and mobile devices) **2.6 Install and configure hardware and software.** 2.6.6 Determine compatibility of software and hardware and resolve any conflicts **2.10 Select, operate, and maintain equipment.** 2.10.1 Identify hardware platforms, configurations, and support models 2.10.5 Prepare and operate equipment per project design specifications **4.5 Design and implement wireless network solutions** 4.5.4 Select and install access points, wireless Network Interface Cards (NICs), antennas, and other hardware and software components to provide a wireless networking solution as determined by a site and customer survey
4. Configure software applications and their related settings and restrictions via local policies or group policies*	**2.6 Install and configure hardware and software.** 2.6.2 Identify hardware requirements for software applications 2.6.3 Verify software compatibility and troubleshoot any software incompatibility 2.6.6 Determine compatibility of software and hardware and resolve any conflicts 2.6.8 Document the installation and configuration of hardware and software **2.10 Select, operate, and maintain equipment.** 2.10.4 Identify software application requirements **3.2 Implement and maintain general security compliance.** 3.2.1 Identify and implement data and application security
5. Manage and configure network protocols, e.g., IPv4 and IPv6, and related settings such as Windows Firewall and remote management.*	**2.2 Apply networking fundamentals to infrastructure systems.** 2.2.5 Identify and apply Transmission Control Protocol and Internet Protocol (TCP/IP; Internet Protocol Version 4 [IPv4], Internet Protocol Version 6 [IPv6]) applications and services (e.g., rlogin, Simple Mail Transfer Protocol [SMTP], Telecommunications Network [Telnet], File Transfer Protocol [FTP], Domain Name System [DNS], Network File System [NFS], Voice over Internet Protocol [VoIP], Internet Control Message Protocol [ICMP]) **4.6 Compare and contrast network protocols** 4.6.1. Explain network protocols (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP], User Datagram Protocol (UDP), Internet Protocol Version 4 [IPv4], Internet Protocol Version 6 [IPv6]) 4.6.2. Identify the advantages and disadvantages of well-known protocols (e.g., Domain Name System [DNS], File Transfer Protocol [FTP], Secure Hypertext Transfer Protocol [HTTPS], Telecommunications Network [Telnet], Dynamic Host Configuration Protocol [DHCP], Remote Desktop Protocol [RDP]) and associated port numbers 4.6.3. Explain the purposes of encapsulation and decapsulation and their relationship to the Open Systems Interconnection (OSI) model. 4.6.4. Explain the difference between User Datagram Protocol (UDP) and TCP 4.6.5. Identify TCP and UDP conventional ports (e.g., Simple Mail Transfer Protocol [SMTP], Telnet, Hypertext Transfer Protocol [HTTP], FTP)

	4.6.6. Explain TCP/IP protocol details (e.g., Internet addresses, Address Resolution Protocol [ARP], Reverse Address Resolution Protocol [RARP], IP datagram format, routing IP datagrams, TCP segment format, IPv4, IPv6) 4.6.7. Describe a Virtual Private Network (VPN) and identify associated protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Point-to-Point Tunneling Protocol [PPTP]) 4.6.8. Capture and analyze data packets **4.7 Describe IP addressing schemes and create subnet masks** 4.7.1. Explain Fully Qualified Domain Names (FQDNs) and how they are used 4.7.2. Explain the IP addressing scheme and how it is used 4.7.3. Identify Class A, B, and C reserved (i.e., private) address ranges and why they are used 4.7.4. Identify the class of network to which a given address belongs 4.7.5. Differentiate between default subnet masks and custom subnet masks 4.7.6. Explain the relationship between an IP address and its associated subnet mask 4.7.7. Identify the differences between classful and classless addressing schemes 4.7.8. Identify multicasting addresses and explain why they are used. 4.7.9. Create custom subnet masks to meet network design requirements 4.7.10. Compare and contrast Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6)
6. Manage resource access issues including sharing, file and folder permissions via NTFS, user account control and Encrypting File System (EFS).*	**2.1 Describe the need for security and explain security risks and security safeguards.** 2.1.2 Describe authentication, authorization, and auditing **3.1 Describe the components associated with information security systems.** 3.1.1 Differentiate between authentication and authorization 3.1.2 Compare and contrast authentication techniques (e.g. single factor, multifactor, passwords, biometrics, certificates, Radio Frequency Identification [RFID] cards) **3.2 Implement and maintain general security compliance.** 3.2.1 Identify and implement data and application security. 3.2.3 Describe and assign permissions (e.g., read-only, read-write) 3.2.4 Provide user authentication (e.g., assign and reset user accounts and passwords) **3.3 Implement and maintain network security.** 3.3.3 Describe Access Control Lists (ACLs) and explain why they are used. **4.10 Administer network operating systems and services.** 4.10.6 Establish shared network resources 4.10.7 Define and set access controls on files, folders, shares, and directories
7. Configure features related to mobile computing including BitLocker, Trusted Platform Module (TPM), Direct Access and mobility options.*	**2.4 Identify trending technologies, their fundamental architecture, and their value in the marketplace.** 2.4.1 Investigate the scope and the impact of mobile computing environments on society

8. Monitor and maintain systems via software updates, disk management and performance settings.*	**2.5 Maintain operating systems (OSs).** 2.5.5. Use system utilities to maintain an OS 2.5.7. Install and test updates and patches to Oss **2.6 Install and configure hardware and software.** 2.6.4. Install and test new software and software upgrades on stand-alone, mobile, and networked systems **2.10 Select, operate, and maintain equipment.** 2.10.5 Prepare and operate equipment per project design specifications 2.10.6 Monitor equipment operation and troubleshoot issues and problems **3.2 Implement and maintain general security compliance.** 3.2.5 Install, test, implement, and update virus and malware detection and protection software **4.9 Describe and install network operating systems (OSs).** 4.9.6 Install, test, and patch network OSs 4.9.8 Evaluate the performance of the network OS. **4.10 Administer network operating systems and services.** 4.10.10 Troubleshoot network performance connectivity (e.g., performance monitor, command line utilities)
9. Perform activities in support of a sound strategy for backup and recovery options and business continuity*	**2.10 Select, operate, and maintain equipment.** 2.10.7 Backup, archive, and manage data. 2.10.9 Perform routine maintenance per manufacturer specifications. **3.2 Implement and maintain general security compliance.** 3.2.8 Identify the need for disaster recovery policies and procedures **4.13 Recommend disaster recovery and business continuity plans.** 4.13.1. Differentiate between disaster recovery and business continuity. 4.13.2. Identify common backup devices 4.13.3. Identify the criteria for selecting a backup system 4.13.4. Establish process for archiving files 4.13.5. Develop a disaster recovery plan