ComputerMinds.com

WORK PROCESS SCHEDULE

AND

RELATED INSTRUCTION OUTLINE

Cost breakdown for Related Instruction

Registration	$100.00
Tuition	$8895.00
Books & Supplies	$1500.00
Other – Certification exams	$1500.00
Total	$11995.00

Appendix A

WORK PROCESS SCHEDULE
OCCUPATIONAL TITLE: COMPUTER SUPPORT SPECIALIST
O*NET-SOC CODE: 15-1151.00   RAPIDS CODE: 1131HY

This schedule is attached to and a part of these Standards for the above identified occupation.

1.	**TYPE OF OCCUPATION**

☐ Time-based   ☐ Competency-based   ☒ Hybrid

2.	**TERM OF APPRENTICESHIP**

The term of the occupation is hybrid-based training. There are <u>2200 – 2660</u> hours of OJL supplemented by and 360 hours of related instruction.

3.	**RATIO OF APPRENTICES TO JOURNEYWORKERS**

The apprentice to Mentor ratio is: 3 Apprentices to 1 Mentor.

4.	**APPRENTICE WAGE SCHEDULE**

Apprentices shall be paid a progressively increasing schedule of wages based on a dollar amount of the Mentor wage rate, which is <u>$25.00</u> per hour.

Term:

Unpaid related instruction training (front- loaded)
1st $8.34 to $15.00 (6 months)
2nd $15.00 to $18.00 (6 months)

5.	**WORK PROCESS SCHEDULE** (See attached Work Process Schedule)

6.	**RELATED INSTRUCTION OUTLINE** (See attached Related Instruction Outline)

Appendix A

WORK PROCESS SCHEDULE
OCCUPATIONAL TITLE: COMPUTER SUPPORT SPECIALIST
O*NET-SOC CODE: 15-1151.00   RAPIDS CODE: 1131HY

JOB FUNCTION 1: Sets up and removes employee or client workstations or devices, including setting up access controls			
Competencies	Core or Optional	RI	OJL
Sets up desktop, laptop and other devices for employees	Core	4.0	40-50
Installs software on network or individual users' computers, laptops or devices and sets appropriate access controls or authorities	Core	5.0	50-60
Sets up user identifications and passwords and implements policies regarding passwords and user/administrator permissions	Core	5.0	50-60
Establishes secure external connections to network or desktops using secure remote access technology	Core	4.0	40-50
Installs printers on networks or individual devices	Core	4.0	40-50
Sets up network map, employee folders and centralized data repositories	Core	4.0	40-50
Sets up email account for users and establishes storage limits and backup parameters	Core	4.0	40-50
Maintains and manages software licenses	Core	4.0	40-50
Removes users from network, archives data and files, removes workstations and disables devices for users exiting the organization or prohibited from using IT resources	Core	6.0	60-70
		40.0	340-430
JOB FUNCTION 2: Installs, provides user support for, or troubleshoots hardware and commercial software			
Competencies	Core or Optional	RI	OJL
Uses FAQ's or other job aids to troubleshoot hardware or software faults	Core	6.0	60-70
Uses logic to discover source of faults and recommends appropriate solutions	Core	6.0	60-70
Demonstrates ability to use basic software, including set-up of preferred default settings, instructs other users on the basic features of standard software packages, and identifies and	Core	8.0	80-90

remedies typical faults in relevant software packages			
Identifies situations in which the fault must be escalated to a higher-level technology support individual, including an outside vendor	Core	8.0	80-90
Contacts outside vendors or vendor-supported help desk to solve difficult problems or procure software patches	Core	6.0	60-70
Prioritizes "tickets" or requests for help based on business need, staff hierarchy or urgency of problems	Core	6.0	60-70
		40.0	400-460

JOB FUNCTION 3: Supports internal or external clients in the use of audio/visual technology and conference technology

Competencies	Core or Optional	RI	OJL
Sets up and links audiovisual equipment, including projectors, screens, laptops, cameras and related device	Optional	7.0	70-80
Installs, launches, operates and troubleshoots software designed to facilitate presentations, web-based conferencing and audioconferencing	Optional	7.0	70-80
Tests equipment and software prior to use to ensure sound and video quality is acceptable	Optional	7.0	70-80
Sets up, schedules and manages web-based or video conferences	Optional	7.0	70-80
Provides support to users during meetings, conferences or webinars	Optional	6.0	70-80
Sets up user accounts on voice technologies or systems, including voicemail	Optional	6.0	70-80
		40	420-480

JOB FUNCTION 4: Installs, maintains and troubleshoots networks

Competencies	Core	RI	OJL
Installs and maintains wired and wireless networks	Core	10.0	50-60
Connects devices to networks physically and using remote access technologies	Core	10.0	50-60
Installs network security software and devices and monitors system for signs of hacking, intrusion or viruses	Core	10.0	50-60

Tests resiliency of security devices or software and monitors bandwidth utilization	Core	8.0	40-50
Establishes and sets access levels and permissions based on employees' job roles and company policies	Core	10.0	50-60
Assists in setting up, configuring and managing servers including data storage	Core	12.0	60-70
Sets up user identification parameters on servers	Core	8.0	40-50
Assists in monitoring server use, efficacy of data back-up and storage systems and integrity of redundant systems or technologies	Core	12.0	60-70
		80	400-480

JOB FUNCTION 5: Makes minor software modifications to improve performance or customize to user needs			
Competencies	Core	RI	OJL
Surveys user needs to understand what modifications are needed	Optional	5.0	50-60
Modifies a program within a software package, including securing permission from vendors to do so	Optional	5.0	50-60
Inserts or loads organizational templates or standards into software, such as presentation templates in PowerPoint or equivalent software	Optional	4.0	40-50
Monitors computer performance and recommends/makes upgrades or modifications as necessary to improve speed or other performance parameters	Optional	5.0	50-60
Uses software to set up needed business functions, such as workflows, tracking, archiving or other functions	Optional	5.0	50-60
		24.0	240-290

JOB FUNCTION 6: Assists in maintaining or updating web content and manages user access profiles and authorities			
Competencies	Core	RI	OJL
Sets user/author access permissions based on organization's policies	Optional	4.0	40-50
Uploads new content to organization's website or removes old content as instructed	Optional	4.0	40-50
Tests functionality of links embedded in the website	Optional	4.0	40-50
Notifies appropriate person if incorrect, outdated or otherwise problematic content is identified	Optional	4.0	40-50

Notifies appropriate person if website is not functioning properly	Optional	4.0	40-50
		20.0	200-250

JOB FUNCTION 7: Monitors and helps maintain network security by adhering to security policies			
Competencies	Core	OJL	RI
Monitors adherence to password policies, including enforcement of password update intervals	Core	3.0	30-40
Sets user access levels and permissions based on organizational policies	Core	3.0	30-40
Monitors antiviral software to understand potential threats and updates as needed	Core	3.0	30-40
Reads, attends conferences or interacts with other IT professionals to know and understand current threat levels and mechanisms	Core	3.0	30-40
Ensures that encryption technology and access controls are utilized to protect sensitive data	Core	4.0	40-50
Ensures that off-site staff are using secure connections to access network	Core	2.0	20-30
Assists in or monitors use of back-up technologies and network redundancies to minimize risk	Core	2.0	20-30
		20.0	200-270
Total		304	2200-2660

Appendix A

RELATED INSTRUCTION OUTLINE
OCCUPATIONAL TITLE: COMPUTER SUPPORT SPECIALIST
O*NET-SOC CODE: 15-1151.00   RAPIDS CODE: 1131HY

PC Hardware – Given a scenario, configure settings and use BIOS/UEFI tools on a PC. Explain the importance of motherboard components, their purpose, and properties, Compare and contrast various RAM types and their features, Install and configure PC expansion cards, Install and configure storage devices and use appropriate media,	
Networking – Identify the various types of network cables and connectors, Compare and contrast the characteristics of connectors and cabling. Explain the properties and characteristics of TCP/IP. Explain common TCP and UDP ports, protocols, and their purpose	
Mobile Devices- Install and configure laptop hardware and components., Explain the function of components within the display of a laptop	
Hardware & Network Troubleshooting- Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU and power with appropriate tools.	
Windows Operating Systems- Compare and contrast various features and requirements of Microsoft Operating Systems (Windows 7, Windows 8, Windows 8.1, Windows 10), Given a scenario, install and configure Windows networking on a client/desktop.	
Other Operating Systems & Technologies – Identify common features and functionality of the Mac OS and Linux operating systems, Summarize methods and data related to mobile device synchronization, Install and configure basic mobile device network connectivity and email	
Security – Identify common security threats and vulnerabilities, Given a scenario, deploy and enforce security best practices to secure a workstation Compare and contrast differences of basic Windows OS security settings.	
Software Troubleshooting – Given a scenario, troubleshoot PC operating system problems with appropriate tools. Given a scenario, troubleshoot common PC security issues with appropriate tools and best practices. Given a scenario, troubleshoot common mobile OS and application issues with appropriate tools	
Operational Procedures – Given a scenario, use appropriate safety procedures. Demonstrate proper communication techniques and professionalism, Summarize the process of addressing prohibited content/activity, and explain privacy, licensing, and policy concepts,	

Exit – CompTIA A+ certification and or Microsoft Windows MTA certification	**80**

Main topics or lessons	
1.0 Network architecture -Explain the functions and applications of various network devices. Compare and contrast the use of networking services and applications, Install and configure the following networking services/applications, Explain the characteristics and benefits of various WAN technologies, Install and properly terminate various cable types and connectors using appropriate tools, Differentiate between common network topologies., Differentiate between network infrastructure implementations	
2.0 Network Operations – Given a scenario, use appropriate monitoring tools. Given a scenario, analyze metrics and reports from monitoring and tracking performance tools. Given a scenario, use appropriate resources to support configuration management, Explain the importance of implementing network segmentation.	
3.0 Network security – Compare and contrast risk related concepts, Compare and contrast common network vulnerabilities and threats, Given a scenario, implement network hardening techniques, Compare and contrast physical security controls, Given a scenario, install and configure a basic firewall.. Explain the purpose of various network access control models	
4.0 Troubleshooting – Given a scenario, implement the following network troubleshooting methodology. Given a scenario, analyze and interpret the output of troubleshooting tools. Given a scenario, troubleshoot and resolve common wireless issues, Given a scenario, troubleshoot and resolve common copper cable issues. Given a scenario, troubleshoot and resolve common fiber cable issues. Given a scenario, troubleshoot and resolve common network issue, Given a scenario, troubleshoot and resolve common security issues, Given a scenario, troubleshoot and resolve common WAN issues.	
5.0 Industry standards, practices, and network theory – Analyze a scenario and determine the corresponding OSI layer, Explain the basics of network theory and concepts, Given a scenario, deploy the appropriate wireless standard, Given a scenario, deploy the appropriate wired connectivity standard	
Exit – CompTIA Network+ certification and or Microsoft Networking MTA certification	
Main topics or lessons	**80**

Network Fundamentals - Compare and contrast OSI and TCP/IP models Compare and contrast TCP and UDP protocols, Describe the effects of cloud resources on enterprise network architecture, Compare and contrast collapsed core and three-tier architectures, Compare and contrast network topologies, Compare and contrast IPv4 address types, Describe the need for private IPv4 addressing, Configure, verify, and troubleshoot IPv6 addressing, Configure and verify IPv6 Stateless Address Auto Configuration, Compare and contrast IPv6 address types	
Routing Fundamentals- Describe the routing concepts, Interpret the components of a routing table, Describe how a routing table is populated by different routing information sources,	
Infrastructure Maintenance - Configure and verify device-monitoring protocols, Troubleshoot network connectivity issues using ICMP echo-based IP SLA, Configure and verify device management, Configure and verify initial device configuration, Perform device maintenance	
LAN Switching Technologies - Describe and verify switching concepts, Interpret Ethernet frame format, Troubleshoot interface and cable issues (collisions, errors, duplex, speed), Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches	
WAN Technologies- Configure and verify PPP and MLPPP on WAN interfaces using local authentication, Configure, verify, and troubleshoot PPPoE client-side interfaces using local authentication, Configure, verify, and troubleshoot GRE tunnel connectivity, Describe WAN topology options	
Infrastructure Services - Describe DNS lookup operation, Troubleshoot client connectivity issues involving DNS, Configure and verify DHCP on a router (excluding static reservations), Troubleshoot client- and router-based DHCP connectivity issues, Configure, verify, and troubleshoot basic HSRP	
Infrastructure Maintenance - Configure and verify device-monitoring protocols, Troubleshoot network connectivity issues using ICMP echo-based IP SLA, Configure and verify device management, Configure and verify initial device configuration, Perform device maintenance	
Exit – Cisco Certified Technician and or Cisco CCENT/ CCNA certification	**80**

Main topics or lessons	
Service Management as a Practice; Best-Practice Approaches and ITIL; Why is ITIL So Successful; Services, Customers, and Stakeholders; Understanding the Concepts of Service Management and IT; Understanding Processes and Functions; Introducing the Service Lifecycle	
Understanding Service Strategy; Understanding the Service Strategy Stage; Understanding Key Concepts of Service Strategy	
Service Strategy Processes; Understanding Service Portfolio Management; Understanding the Financial Management Process; Understanding the Business Relationship Management	
Understanding Service Design; Understanding the Purpose, Objective, and Scope for Service Design; Describing the Service; Four Key Elements of Service Design; Building the Service; Five Major Aspects of Service Design	
Service Level Management: Aligning IT with Business Requirements; The Purpose, Objectives, and Scope of Service Level Management; Capturing Service Level Requirements; Understanding the Service Level Agreement; Monitoring and Improving Service Delivery; Interfacing with Other Service Management Processes	
Service Design Roles; Roles and Responsibilities in Service Management; Designing Roles Using the RACI Model; Competence and Training	
Understanding Service Transition and the Change Management Processes; Understanding Service Transition; Introduction to the Change Management Process	
Service Transition Processes; Transition Planning and Support; Service Asset and Configuration Management; Knowledge Management; Release and Deployment Management	
Delivering the Service; The Service Operation Lifecycle Stage; Understanding the Purpose, Objectives, and Scope of Service Operation; Organizing for Service Operations	
Exit – ITIL Foundation certification exam	24

Main topics or lessons	
1.0 Network Security - Implement security configuration parameters on network devices and other Technologies, Given a scenario, use secure network administration principles, Explain network design elements and components. , Given a scenario, implement common protocols and services, Given a scenario, troubleshoot security issues related to wireless networking.	
2.0 Compliance and Operational Security - Explain the importance of risk related concepts, Summarize the security implications of integrating systems and data with third parties, Given a scenario, implement appropriate risk mitigation strategies, Given a scenario, implement basic forensic procedures. Summarize common incident response procedures, Explain the importance of security related awareness and training., Compare and contrast physical security and environmental controls, Summarize risk management best practices. Given a scenario, select the appropriate control to meet the goals of security.	
3.0 Threats and Vulnerabilities - Explain types of malware. Summarize various types of attacks, Summarize social engineering attacks and the associated effectiveness with each attack, Explain types of wireless attacks, Explain types of application attacks, Analyze a scenario and select the appropriate type of mitigation and deterrent techniques, Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities, Explain the proper use of penetration testing versus vulnerability scanning.	
4.0 Application, Data and Host Security - Explain the importance of application security controls and techniques, Summarize mobile security concepts and technologies, Given a scenario, select the appropriate solution to establish host security, Implement the appropriate controls to ensure data security, Compare and contrast alternative methods to mitigate security risks in static Environments.	
5.0 Access Control and Identity Management - Compare and contrast the function and purpose of authentication services, Given a scenario, select the appropriate authentication, authorization or access control, Install and configure security controls when performing account management,	
6.0 Cryptography Given a scenario, utilize general cryptography concepts. Given a scenario, use appropriate cryptographic methods, Given a scenario, use appropriate PKI, certificate management and associated Components,	
Exit – CompTIA Security + certification and or Microsoft Security MTA certification	**40**