



Computer Networking Technology and Cybersecurity

Program / Hours: CIP 11.0901 – 2 Year Half Day Program

Course Description

This program focuses on the design, implementation, management, optimization, security, and troubleshooting of computers, networks, peripherals, linked computer systems, and associated software. Students develop the technical knowledge and hands-on skills needed to support operating systems, applications, network systems, devices, and users, while preparing for entry-level roles as network specialists, computer support technicians, and related information technology professionals.

Learning Activities / Modes of Assessment

Small Group
Large Group
Independent Work
One-on-One
Classwork Activities
Presentations
Research Projects
Research Reports
Technology Use
Tests and Quizzes

Individual Resources

Textbooks
Workbooks
Online Resources
PowerPoint Presentations
Computer Applications
Networking Equipment and Tools
Lab Simulations

Year 1, MP 1

Task #	K - Know	U - Understand	D - Do
101	List common causes of accidents and injuries in a computer facility.	Common workplace hazards can be anticipated and prevented through safe routines.	Identify accident risks in a computer lab and describe prevention steps.
102	Wear personal protective equipment.	PPE protects people and equipment when conditions require added safety controls.	Select and properly use required PPE during lab or shop activities.
103	List and identify safety hazard symbols.	Hazard symbols communicate risk quickly and guide safe handling decisions.	Match safety symbols to hazards and respond using appropriate precautions.
104	Review Safety Data Sheets (SDS) and explain their requirements in handling hazardous materials.	SDS information explains chemical risks, handling, storage, and emergency response.	Use an SDS to determine safe handling and disposal procedures.
105	Describe types of fire extinguishers and explain which types to use for extinguishing various fires.	Different fire classes require the correct extinguisher type and response.	Choose the proper extinguisher type for common classroom or equipment fires.
106	Use safe procedures when lifting and carrying heavy objects.	Proper lifting prevents injury and protects equipment from damage.	Demonstrate safe lifting, carrying, and team-lift procedures.
107	Describe the importance of safety as it relates to environmental issues.	Technology work affects the environment through waste, energy use, and recycling.	Explain environmentally responsible handling of equipment, waste, and supplies.
108	Identify potential hazards with power supplies.	Power supplies contain electrical hazards even when systems appear inactive.	Identify PSU hazards and follow safe inspection or replacement procedures.
109	Identify disposal procedures for batteries, display devices, and electronic equipment.	Electronic waste requires responsible disposal to protect people and the environment.	Sort batteries, displays, and electronics for approved disposal or recycling.

Task #	K - Know	U - Understand	D - Do
110	Identify disposal procedures for chemical solvents and pressurized cans.	Solvents and pressurized cans require controlled storage, use, and disposal.	Identify safe disposal steps for solvents and pressurized containers.
111	Prevent electrostatic discharge conditions.	Static electricity can silently damage sensitive electronic components.	Apply ESD controls using straps, mats, bags, and safe handling.
113	Configure a computer's power management settings.	Power settings affect performance, energy use, and device availability.	Configure workstation power plans and explain operational tradeoffs.
114	Maintain safe work area to avoid common accidents and injuries.	An organized workspace reduces accidents and supports professional productivity.	Maintain a clean, safe, and ready computer work area.
115	Demonstrate safe procedures when using ladders.	Ladder safety depends on setup, inspection, positioning, and controlled movement.	Demonstrate safe ladder selection, placement, climbing, and use.

Year 1, MP 2

201	Categorize storage devices, backup media, and RAID.	Storage choices affect performance, capacity, redundancy, and recovery.	Compare drives, backup media, and RAID options for given scenarios.
202	Categorize the different types of computer cases.	Case form factors affect compatibility, airflow, expansion, and serviceability.	Identify case types and select one for a workstation need.
203	Explain motherboard components, types, and features.	Motherboards connect and control system components through standards and features.	Identify motherboard parts, form factors, sockets, slots, and connectors.
204	Categorize power supply types and characteristics.	Power supply specifications must match system load and component requirements.	Select and evaluate a PSU by wattage, connectors, and form factor.

205	Explain the purpose and characteristics of CPUs and their features.	CPU features affect performance, compatibility, virtualization, and workload suitability.	Identify CPU characteristics and match processors to system requirements.
206	Explain cooling methods and devices.	Cooling protects components by controlling heat under normal and heavy loads.	Identify, install, inspect, and explain common cooling solutions.
207	Compare and contrast memory types, characteristics, and their purpose.	Memory type, speed, capacity, and channels affect compatibility and performance.	Identify RAM types and install compatible memory correctly.
208	Distinguish among different display devices and their characteristics.	Display technologies vary by connection, resolution, refresh, and use case.	Compare display devices and configure basic display settings.
209	Summarize the function and types of adapter cards.	Adapter cards expand system capability through specialized interfaces and functions.	Identify, install, and explain common expansion cards.
210	Install and configure peripherals and input devices.	Peripherals require correct connection, drivers, configuration, and user support.	Install, configure, and test common input/output devices.
211	Configure and optimize portable devices.	Portable devices require settings that balance usability, security, and battery life.	Configure mobile or portable device settings for an assigned scenario.
212	Install and configure printers.	Printer installation requires drivers, connections, consumables, and maintenance awareness.	Install, configure, share, maintain, or troubleshoot a printer.
213	Install, configure and maintain personal computer components.	PC maintenance combines correct assembly, configuration, testing, and documentation.	Install, configure, maintain, and document internal PC components.
214	Replace desktop and laptop computer components.	Desktop and laptop repairs require compatibility checks and careful disassembly.	Replace assigned desktop or laptop components using safe procedures.

Year 1, MP 3

301	Apply industry standard troubleshooting methods.	Structured troubleshooting prevents guessing and supports repeatable problem solving.	Apply a documented troubleshooting process to diagnose a technical issue.
302	Troubleshoot common hardware and operating system symptoms and their causes.	Symptoms point to likely hardware, software, configuration, or OS causes.	Diagnose and resolve common PC hardware or OS problems.
304	Identify common laptop issues and determine the appropriate basic troubleshooting method.	Laptop issues often involve integrated parts, power, display, and portability.	Identify laptop symptoms and choose an appropriate basic repair path.
305	Integrate common preventative maintenance techniques.	Preventive maintenance reduces downtime and extends equipment life.	Perform cleaning, updates, inspections, and basic maintenance documentation.
307	Diagnose and repair common printer issues.	Printer faults require attention to paper path, consumables, drivers, and connectivity.	Diagnose and repair common printer problems using safe procedures.

Year 1, MP 4

401	Identify different operating systems by their features.	Operating systems differ by interface, file system, licensing, and use case.	Compare OS features and identify appropriate operating systems for scenarios.
402	Use various user interfaces.	Technicians must navigate graphical and command-line interfaces efficiently.	Use Windows, Linux, and web-based interfaces to complete tasks.
403	Install and configure a workstation operating system.	A workstation OS must be installed, updated, secured, and configured.	Install and configure a workstation operating system for classroom use.
404	Explain boot sequences, methods, and startup utilities for various operating systems.	Boot processes determine how systems start, recover, and load operating systems.	Use BIOS/UEFI, boot media, and startup tools to resolve issues.

406	Differentiate between various operating system directory structures.	Directory structures organize files, permissions, profiles, and system resources.	Navigate and compare Windows and Linux directory structures.
407	Use system utilities/tools and evaluate the results.	System utilities reveal configuration, performance, storage, and service status.	Run utilities and interpret results to support decisions.
408	Troubleshoot common OS and software issues.	OS and software issues can stem from settings, updates, files, or malware.	Troubleshoot common OS and application problems using evidence.
409	Manage local users, groups, and security policies.	Local accounts and policies control access, permissions, and workstation security.	Create users/groups and configure basic local security settings.
410	Install and configure a network operating system.	Network operating systems provide shared services, authentication, and administration.	Install or configure server/network OS roles in a lab environment.
501	Explain the function of the TCP/IP protocol suite.	TCP/IP enables communication through layered protocols and addressing.	Explain protocol roles and trace data flow through TCP/IP.
502	Identify commonly used TCP and UDP default ports.	Default ports identify common services and support troubleshooting/security decisions.	Match services to TCP/UDP ports and explain their use.
503	Identify address formats including IPv4, IPv6, and MAC.	IPv4, IPv6, and MAC addresses identify devices at different layers.	Read, compare, and apply common network address formats.

Task #	K - Know	U - Understand	D - Do
504	Evaluate the proper use of addressing technologies and addressing schemes.	Addressing schemes must support growth, segmentation, management, and routing.	Design or evaluate IP addressing for a small network.
505	Identify common IPv4 and IPv6 routing protocols.	Routing protocols exchange path information in different ways and contexts.	Identify routing protocols and describe basic use cases.

Year 2, MP 1

506	Explain the purpose and properties of routing.	Routing moves traffic between networks using paths, gateways, and metrics.	Configure or interpret basic routes and verify connectivity.
507	Identify the characteristics of wireless communication.	Wireless communication is affected by standards, frequency, distance, and interference.	Identify wireless characteristics and plan basic wireless coverage.
508	Identify the basic elements of unified communication technology.	Unified communications integrate voice, video, messaging, and collaboration services.	Identify UC components and explain their network requirements.
509	Categorize technologies that support cloud computing.	Cloud computing delivers shared compute, storage, applications, and services.	Categorize cloud service and deployment models for scenarios.
510	Implement virtualization technologies.	Virtualization separates workloads from physical hardware for flexibility and labs.	Create, configure, and manage virtual machines or containers.
601	Categorize standard cable types and their properties.	Cable type determines speed, distance, shielding, and installation suitability.	Identify cable categories/media and select cable for requirements.

602	Identify common connector types.	Connector types must match media, tools, equipment, and standards.	Identify connectors and match them to cables and devices.
603	Identify common physical network topologies.	Physical topology affects installation layout, reliability, and troubleshooting.	Identify or sketch common physical network layouts.
604	Fabricate cables according to TIA/EIA standards.	TIA/EIA standards ensure reliable and consistent copper cable termination.	Terminate, test, and document cables to T568A/B standards.
605	Categorize common WAN technology types and properties.	WAN technologies connect sites using provider-based services and tradeoffs.	Compare WAN options by speed, cost, reliability, and use case.
606	Categorize common LAN technology types and ethernet properties.	LAN and Ethernet technologies define local connectivity and performance.	Identify Ethernet standards and explain LAN characteristics.
607	Explain common logical network topologies and their characteristics.	Logical topology describes traffic flow beyond physical cable layout.	Explain logical bus, star, mesh, VLAN, and client/server relationships.
608	Install components of wiring distribution and verify installation.	Distribution systems organize cabling for reliability, labeling, and serviceability.	Install, label, test, and verify basic wiring-distribution components.

Year 2, MP 2

701	Install, configure, and differentiate between common network connectivity devices.	Connectivity devices operate at different layers and serve different roles.	Install/configure switches, routers, APs, and related devices.
702	Identify the functions of specialized network devices.	Specialized devices provide targeted security, storage, voice, or monitoring functions.	Identify specialized network devices and explain their purpose.

703	Explain the advanced features of a switch.	Switch features improve segmentation, redundancy, security, and performance.	Configure or explain VLANs, trunks, STP, LACP, and management features.
704	Install a basic wireless network.	Wireless networks require planning for SSID, placement, addressing, and access.	Install and test a basic wireless network.
705	Configure appropriate encryption and verify wireless installation.	Wireless encryption protects access and must be verified after setup.	Configure wireless security and confirm clients connect securely.
801	Explain, compare, and contrast the layers of the TCP/IP and OSI models.	OSI and TCP/IP models organize how networks communicate and troubleshoot.	Map protocols/devices to layers and use models to diagnose issues.
802	Prepare physical and logical network diagrams and documentation.	Accurate diagrams and documentation support installation, troubleshooting, and continuity.	Create physical/logical diagrams, labels, and network documentation.
803	Evaluate the network based on configuration management documentation.	Configuration documentation helps compare intended design to actual network state.	Review configs and identify discrepancies, risks, or needed updates.
804	Conduct network monitoring to identify performance and connectivity issues.	Monitoring reveals availability, performance trends, and connectivity problems.	Use monitoring tools to identify and report network issues.
806	Implement remote management technologies.	Remote management enables efficient support but requires secure access controls.	Configure or use SSH, RDP, web, VPN, or management consoles.

Year 2, MP 3

901	Utilize command line/graphical tools and interpret the output.	Command output provides evidence for configuration, connectivity, and faults.	Run CLI/GUI tools and interpret results accurately.
-----	--	---	---

902	Use network scanners.	Network scanners discover hosts, services, and possible security concerns.	Use scanning tools responsibly and report findings.
903	Utilize appropriate hardware tools for cable fabrication and troubleshooting.	Cable tools verify termination quality and locate physical-layer faults.	Use crimpers, testers, toners, and related tools correctly.
904	Implement network troubleshooting methodologies.	Network troubleshooting requires a structured method and documented evidence.	Apply methodology to isolate, test, fix, and document network faults.
906	Troubleshoot common wired and wireless connectivity issues.	Connectivity failures may involve cabling, addressing, wireless, switching, or routing.	Troubleshoot wired/wireless issues and verify restored connectivity.
907	Troubleshoot and resolve common WAN issues.	WAN issues often involve provider links, routes, DNS, latency, or outages.	Diagnose common WAN symptoms and document escalation evidence.

Year 2, MP 4

1001	Configure hardware and software security devices.	Security devices enforce controls between users, systems, and networks.	Configure or evaluate basic security hardware/software settings.
1002	Implement features of a network firewall.	Firewalls control traffic using rules, zones, ports, and policies.	Create, test, and explain basic firewall rules.
1003	Configure network access security.	Network access security limits who can connect and what they can reach.	Apply access controls such as passwords, VLANs, or authentication settings.
1004	Differentiate the principles of user authentication.	Authentication verifies identity using factors, credentials, and trust relationships.	Compare authentication methods and select appropriate controls.

1005	Evaluate issues that affect device security.	Device security depends on updates, configuration, access, and physical controls.	Evaluate devices for common security weaknesses.
1006	Identify and mitigate common security threats.	Threats can be reduced through awareness, controls, updates, and response.	Identify threats and recommend practical mitigation steps.
1007	Implement security features.	Security features must be enabled, tested, documented, and maintained.	Implement security settings and verify their effect.
1008	Demonstrate basic forensic concepts.	Forensics preserves evidence while investigating incidents responsibly.	Demonstrate basic evidence identification, preservation, and documentation.
1009	Explain disaster recovery best practices.	Recovery planning reduces downtime after loss, failure, or compromise.	Create or evaluate backup, restore, and disaster recovery procedures.
1101	Use effective soft skills such as proper etiquette and active listening.	Professional communication builds trust with users, peers, and employers.	Use active listening, etiquette, and clear communication in scenarios.
1102	Solve customer problems.	Customer service combines problem solving, empathy, documentation, and follow-up.	Resolve a user issue and document the support interaction.
1103	Implement and adhere to acceptable use policies.	Acceptable use policies define responsible technology behavior and consequences.	Interpret and follow AUP requirements in classroom/workplace scenarios.
1104	Maintain confidentiality.	Confidentiality protects private information and professional trust.	Handle user, system, and school data using appropriate privacy practices.
1105	Maintain asset inventory.	Accurate inventory supports accountability, maintenance, budgeting, and security.	Record, update, and verify hardware/software asset information.
1106	Evaluate the impact of new and emerging technologies.	Emerging technologies create new opportunities, risks, and skill requirements.	Research and evaluate new technology for program or workplace impact.