

Career & Technical Education | Information Technology

Network Security

Subject Code: 145050

Outcome & Competency Descriptions

Course Description:

Students will securely install, configure, and troubleshoot network hardware and peripherals. Students will learn networking by exploring the OSI model, network topologies, and cabling. Students will design simple networks, know how to select physical devices, and be able to configure the equipment to optimize security. Knowledge and skills relating to the operation and usage of network protocols will be developed.

Strand 1. Business Operations / 21st Century Skills

Learners apply principles of economics, business management, marketing and employability in an entrepreneur, manager, and employee role to the leadership, planning, developing, and analyzing of business enterprises related to the career field.

Outcome: 1.3. Business Ethics and Law

Analyze how professional, ethical, and legal behavior contributes to continuous improvement in organizational performance and regulatory compliance.

Competencies

- 1.3.1. Analyze how regulatory compliance affects business operations and organizational performance.
- 1.3.2. Follow protocols and practices necessary to maintain a clean, safe, and healthy work environment.
- 1.3.3. Use ethical character traits consistent with workplace standards (e.g., honesty, personal integrity, compassion, justice).
- 1.3.4. Identify how federal and state consumer protection laws affect products and services.
- 1.3.5. Access and implement safety compliance measures (e.g., quality assurance information, safety data sheets [SDSs], product safety data sheets [PSDSs], United States Environmental Protection Agency [EPA], United States Occupational Safety and Health Administration [OSHA]) that contribute to the continuous improvement of the organization.
- 1.3.6. Identify deceptive practices (e.g., bait and switch, identity theft, unlawful door-to-door sales, deceptive service estimates, fraudulent misrepresentations) and their overall impact on organizational performance.
- 1.3.7. Identify the labor laws that affect employment and the consequences of noncompliance for both employee and employer (e.g., harassment, labor, employment, employment interview, testing, minor labor laws, Americans with

Disabilities Act, Fair Labor Standards Acts, Equal Employment Opportunity Commission [EEOC]).

1.3.8. Verify compliance with computer and intellectual property laws and regulations.

1.3.9. Identify potential conflicts of interest (e.g., personal gain, project bidding) between personal, organizational and professional ethical standards.

Outcome: 1.4. Knowledge Management and Information Technology

Demonstrate current and emerging strategies and technologies used to collect, analyze, record, and share information in business operations.

Competencies

1.4.3. Verify compliance with security rules, regulations and codes (e.g., property, privacy, access, accuracy issues, client and patient record confidentiality) pertaining to technology specific to the industry pathway.

Outcome: 1.5. Global Environment

Evaluate how beliefs, values, attitudes and behaviors influence organizational strategies and goals.

Competencies

1.5.2. Describe how cultural intelligence skills influence the overall success and survival of an organization.

1.5.3. Use cultural intelligence to interact with individuals from diverse cultural settings.

1.5.5. Recognize the ways in which bias and discrimination may influence productivity and profitability.

1.5.8. Identify how multicultural teaming and globalization can foster development of new and improved products and services and recognition of new opportunities.

Strand 2. IT Fundamentals

Learners apply fundamental principles of IT, including the history of IT and its impact on society, common industry terms, systems theory, information storage and retrieval, database management, and computer hardware, software, and peripheral device configuration and installation. This base of knowledge and skills may be applied across the career field.

Outcome: 2.1. Security, Risks, and Safeguards

Describe the need for security and explain security risks and security safeguards.

Competencies

- 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, malware, ransomware, spoofing, hacking, social engineering, phishing, Denial of Service, web application attacks, network-based attacks).
- 2.1.11. Identify the need for information security and implement best practices for maintaining cyber hygiene (e.g. personal identifiable information, private financial documents, corporate records).
- 2.1.12. 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], General Data Protection Regulation [GDPR], European Union Data Protection Regulation [EUDPR]).

Outcome 2.5. Operating Systems

Install and maintain operating systems (OSs).

Competencies

- 2.5.3. Identify the properties of open and proprietary systems.
- 2.5.5. Use system utilities to maintain an Operating System.
- 2.5.7. Install and test updates and patches to Operating Systems.

Outcome: 2.12. Performance Tests and Acceptance

Develop performance tests and acceptance plans.

Competencies

- 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, compare with expected performance, and 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.

Outcome: 2.14. Artificial Intelligence

Understand and apply prescribed methods of using Artificial Intelligence.

Competencies

- 2.14.2. Analyze how artificial intelligence technology impacts society and the ethical implications of its usage.

Strand 3. Information Security

Learners apply principles of information security to implement and maintain security compliance and network security. Learners select components and mechanisms required for a multilayer defense structure and evaluate and minimize security risks to wired and wireless networks and devices.

Outcome: 3.1. Components of Information Security

Describe the components associated with information security systems.

Competencies

- 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).

Outcome: 3.2. General Security Compliance

Implement and maintain general security compliance.

Competencies

- 3.2.1. Identify and implement data and application security.
- 3.2.2. Perform backup, restore, and verification procedures.
- 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 (e.g., business continuity plans, scenario testing).

Outcome: 3.3. Network Security

Implement and maintain network security.

Competencies

- 3.3.1. Describe network security policies (e.g., acceptable use policy, VLAN management, firewall rules).
- 3.3.2. Identify security appliances and tools (e.g., virtual private network gateways, IPS, firewalls, unified threat management, network access controls) 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.
- 3.3.5. Assess risk levels based on vulnerability of the organization, likelihood of risk, and impact on the organization.
- 3.3.6. Describe the relationships among change, vulnerability, configuration, and patch management to protect systems and applications.
- 3.3.7. Train users in network security procedures.

Outcome: 3.4. Multilayer Defense Structure

Explain information technology mechanisms as they apply to a multilayer defense structure.

Competencies

- 3.4.1. Describe available systems for intrusion prevention, detection, and mitigation.
- 3.4.2. Analyze system log files to identify security events.
- 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).

Outcome: 3.5. Wireless Security

Implement secure wireless networks.

Competencies

- 3.5.1. Describe wireless security risks (e.g., unauthorized access) and how to mitigate them.
- 3.5.2. Compare methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dial In User Service [RADIUS]).
- 3.5.3. Research security standards provided by Institute of Electrical and Electronics Engineers (IEEE).
- 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.

Strand 4. Infrastructure Systems

Learners apply principles of networking and infrastructure related to the installation, administration, and maintenance of computer networks and components. Knowledge and skills may be applied to network connectivity, cabling, protocols, architecture, classification, topologies, operating systems, Open Systems Interconnection (OSI) standards, data encoding, Quality of Service (QoS), Internet Protocol (IP) addressing, and wide area network (WAN) design.

Outcome: 4.1. Network Infrastructure Build a multinode network.

Competencies

- 4.1.1. Determine the basic point-to-point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, mesh, hybrid) and identify broadband and baseband (e.g., Ethernet) transmission methods and standards.
- 4.1.2. Explain packet-switching techniques.
- 4.1.3. Compare the characteristics of connection-oriented and connectionless protocols and select protocols based on given criteria.
- 4.1.4. Identify standard and emerging network technologies (e.g., broadband, satellite, optic, cellular, Local-Area Network (LAN) and WiFi).
- 4.1.5. Describe how Unified Communication (UC) integrates voice, data, and video communications.
- 4.1.6. Configure and build a network.

Outcome: 4.2. Open Systems Interconnection Describe the Open Systems Interconnection (OSI) standard (International Organization for Standardization [ISO] Standard 7498).

Competencies

- 4.2.1. Identify the benefits of using a layered network model.
- 4.2.2. Compare Open Systems Interconnection layer positions and their relationships to one another.
- 4.2.3. Compare the seven layers of the Open Systems Interconnection stack to the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack.
- 4.2.4. Compare the basics of Transmission Control Protocol/Internet layers, components, and functions.
- 4.2.5. Describe actions to be performed at each of the Open Systems Interconnection physical layers.
- 4.2.6. Explain how the Open Systems Interconnection layers relate to the elements of network communication.

Outcome: 4.5. Wireless Network Solutions

Design and implement wireless network solutions.

Competencies

- 4.5.1. Compare secure wireless solutions operating in ad-hoc, infrastructure, or mesh modes.
- 4.5.6. Secure the wireless network.
- 4.5.7. Configure a wireless mesh network with non-overlapping channels.

Outcome: 4.6. Network Protocols

Compare network protocols.

Competencies

- 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 of protocols (e.g., Domain Name System [DNS], File Transfer Protocol [FTP], Hypertext Transfer Protocol [HTTP], Telecommunications Network [Telnet], Remote Desktop Protocol [RDP], Secure Shell [SSH]) and associated port numbers.
- 4.6.3. Explain the purposes of encapsulation and decapsulation (or de-encapsulation) and their relationship to the Open Systems Interconnection (OSI) model.
- 4.6.4. Explain the difference between User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).
- 4.6.5. Identify Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) conventional ports (e.g., Simple Mail Transfer Protocol [SMTP], Telnet, Hypertext Transfer Protocol [HTTP], File Transfer Protocol [FTP]).
- 4.6.6. Explain Transmission Control Protocol/Internet Protocol (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 compare wired and wireless packets.

Outcome: 4.9. Network Administration

Administer network operating systems and services.

Competencies

- 4.9.6. Establish shared network resources.
- 4.9.7. Define and set access controls on files, folders, shares, and directories.
- 4.9.12. Securely delegate standard management tasks.
- 4.9.13. Establish a secure remote connection to manage network resources.

Outcome: 4.12. Disaster Recovery

Recommend disaster recovery and business continuity plans.

Competencies

- 4.12.1. Differentiate between disaster recovery and business continuity.
- 4.12.2. Identify common local and cloud-based backup options.
- 4.12.3. Identify the criteria for selecting a backup system.
- 4.12.4. Establish a process for archiving files.
- 4.12.5. Develop and simulate a disaster recovery plan.

Outcome: 4.13. Internet of Things

Install, configure, and operate IoT devices.

Competencies

- 4.13.1. Compare IoT wireless standards (e.g. Z-Wave, Zigbee).
- 4.13.2. Compare smart home ecosystems (e.g. Apple Homekit, Google Home, Amazon Alexa, Matter).
- 4.13.3. Configure, secure and connect IoT devices to the network.
- 4.13.4. Create IoT automations.
- 4.13.5. Explain fog computing in the IoT environment.

Strand 9. Cybersecurity

Learners apply principles of Cybersecurity to secure and defend information technology systems, selection and implementation of methods and tools to secure physical and digital assets, manage threats, deploy countermeasures, and establish strategies to protect business information using risk and incident management.

Outcome: 9.2. Access Control and Asset Security

Apply identification (ID), authorization, and physical asset security.

Competencies

- 9.2.1. Perform authorization control (e.g., least privilege, separation of duties, mandatory access, discretionary access, rule-based access control, role-based access control, time of day restrictions, location distractions).
- 9.2.2. Implement authentication techniques (e.g., Tokens, Common access card, Smart card, Multifactor authentication, Single sign-on, Biometrics, Personal identification verification card, Username, Federation, Transitive trust/authentication).
- 9.2.3. Use authentication factors (e.g., something you are, something you have, something you know).