Ohio CTE

Information Technology Career Field: Network Security

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. 2

Outcome 2.1 **Security, Risks, and Safeguards: 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. 2.1.1.

2 Describe authentication, authorization, and auditing. 2.1.2.

3 Describe multilevel security. 2.1.3.

4 Identify security risks and describe associated safeguards and methodologies (e.g., auditing). 2.1.4.

5 Describe major threats to computer systems (e.g., insider threats, viruses, worms, spyware, ransomware, spoofing, hacking, social engineering, phishing). 2.1.5.

6 Describe the components of the physical environment (e.g., wiring closets, server rooms) and physical security systems. 2.1.6.

7 Describe the need for security in networking (e.g., firewall, access controls, encryption, demilitarized zone). 2.1.7.

8 Describe the need for security in application development. 2.1.8.

9 Track and catalogue physical assets. 2.1.9.

10 Describe computer forensics, its importance in information security and cybersecurity, and its relevance to law enforcement. 2.1.10.

11 Identify the need for personal security in digital information and describe how personal information can be safeguarded. 2.1.11.

12 Practice information security per job requirements. 2.1.12.

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], General Data Protection Regulation [GDPR], European Union Data Protection Regulation [EUDPR]). 2.1.13.

Outcome 2.3 **Alphanumeric Encoding: Explain and describe data encoding basics.** 2.3.

1. Identify and explain coding information and representation of characters (e.g., American Standard Code for Information Interchange [ASCII], Extended Binary Coded Decimal Interchange Code [EBCDIC], Unicode). 2.3.1.
2. Convert between numbering systems (e.g., binary, hexadecimal, decimal). 2.3.2.

Outcome 2.4 **Emerging Technologies: 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. 2.4.1.
2. Describe the differences, advantages, and limitations of cloud computing (e.g., public cloud, private cloud, hybrid cloud) and on premises computing. 2.4.2.
3. Utilize cloud computing applications (e.g., services, applications, virtual environments). 2.4.3.
4. Describe emerging technologies (e.g., Bring your Own Device [BYOD], Services Virtualization, Augmented Reality [AR], SMART Devices, Additive Manufacturing [3D Printing]). 2.4.4.

Outcome 2.7 **Web Architecture: Explain the fundamentals of delivering information and applications using web architecture.** 2.7.

1. Describe methods of securely transmitting data. 2.7.1.
2. Describe ways to present data (e.g., responsive web design, mobile applications, desktop applications, web applications). 2.7.2.
3. Differentiate between a client and a server. 2.7.3.
4. Identify how the use of different browsers and devices effects the look of a webpage (e.g., Americans with Disabilities Act [ADA]). 2.7.4.
5. Explain the relationship between data transmission volumes, bandwidth, and latency. 2.7.5.
6. Describe the characteristics and use of browser plug-ins. 2.7.6.
7. Compare the advantages and disadvantages of running an in-house server or using a service provider. 2.7.7.
8. Describe the difference between static and dynamic sites and the reasons for using each. 2.7.8.

Outcome 2.9 **Project Concept Proposal: Develop a project concept proposal.** 2.9.

2 Determine the scope and purpose of the project. 2.9.2.

3 Determine the target audience, client needs, expected outcomes, objectives, and budget. 2.9.3.

4 Develop a conceptual model and design brief for the project. 2.9.4.

5 Develop a timeline, a communication plan, a task breakdown, costs (e.g., equipment, labor), deliverables, and responsibilities for completion. 2.9.5.

6 Develop and present a comprehensive proposal to stakeholders. 2.9.6.

Outcome 2.10 **Equipment: Select, operate, and maintain equipment.** 2.10.

1 Identify hardware platforms, configurations, and support models. 2.10.1.

2 Identify processor, memory, storage, power and environmental requirements. 2.10.2.

3 Identify architecture requirements. 2.10.3.

4 Identify software application requirements. 2.10.4.

5 Prepare and operate equipment per project design specifications. 2.10.5.

6 Monitor equipment operation and troubleshoot issues and problems. 2.10.6.

7 Backup, restore, test, archive, and manage data. 2.10.7.

8 Prepare equipment for storage or decommissioning. 2.10.8.

9 Perform routine maintenance per manufacturer specifications. 2.10.9.

Outcome 2.11 **Troubleshooting: Select and apply troubleshooting methodologies for problem solving.** 2.11.

1 Identify the problem. 2.11.1.

2 Select troubleshooting methodology (e.g., top down, bottom up, follow the path, spot the differences). 2.11.2.

3 Investigate symptoms based on the selected methodology. 2.11.3.

4 Gather and analyze data about the problem. 2.11.4.

5 Design a solution. 2.11.5.

6 Test a solution. 2.11.6.

7 Implement a solution. 2.11.7.

8 Document the problem and the verified solution. 2.11.8.

Outcome 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. 2.12.1.
2. Develop a test system that accurately mimics external interfaces. 2.12.2.
3. Develop test cases that are realistic, compare with expected performance, and include targeted platforms and device types. 2.12.3.
4. Develop, perform, and document usability and testing integration. 2.12.4.
5. Make corrections indicated by test results. 2.12.5.
6. Seek stakeholder acceptance upon successful completion of the test plan. 2.12.6.

Outcome 2.13 **Rollout and Handoff: Plan rollout and facilitate handoff to customer.** 2.13.

1. Include overall project goals and timelines in the rollout plan. 2.13.1.
2. Communicate rollout plans to key stakeholders in a timely manner. 2.13.2.
3. Conduct final review and approvals according to company standards. 2.12.3.
4. Identify support staff, training needs, and contingency plans in the rollout plan. 2.13.4.
5. Test delivered application to assure that it is fully functional for the customer or user and meets all requirements. 2.13.5.
6. Deliver support and training materials. 2.13.6.

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. 3

Outcome 3.1 **Components of Information Security: Describe the components associated with information security systems.** 3.1.

1 Differentiate between authentication and authorization. 3.1.1.

2 Compare authentication techniques (e.g. single factor, multifactor, passwords, biometrics, certificates, Radio Frequency Identification [RFID] cards). 3.1.2.

3 Compare methods of achieving information assurance and integrity and confidentiality (e.g. digital signatures, digital certifications, hashing algorithms, encryption). 3.1.3.

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). 3.1.4.

5 Discuss the role of certificate authorities (CAs) and Public Key Infrastructure (PKI). 3.1.5.

Outcome 3.2 **General Security Compliance: Implement and maintain general security compliance.** 3.2.

1 Identify and implement data and application security. 3.2.1.

2 Implement backup, restore, and verification procedures (e.g., tape, disk, cloud). 3.2.2.

3 Describe and assign permissions (e.g., read-only, read-write). 3.2.3.

4 Provide user authentication (e.g., assign and reset user accounts and passwords). 3.2.4.

5 Install, test, implement, and update virus and malware detection and protection software. 3.2.5.

6 Identify sources of virus and malware infection and remove viruses and malware. 3.2.6.

7 Provide documentation, training, and support to users on established security procedures. 3.2.7.

8 Identify the need for disaster recovery policies and procedures. 3.2.8.

Outcome 3.3 **Network Security: Implement and maintain network security.** 3.3.

1. Describe network security policies (e.g., acceptable use policy). 3.3.1.
2. Identify security appliances and describe the role of each in a networked environment. 3.3.2.
3. Devise account administration functions to support network security. 3.3.3.
4. Describe Access Control Lists (ACLs) and explain why they are used. 3.3.4.
5. Assess risks based on vulnerability of the organization, likelihood of risk, and impact on the organization. 3.3.5.
6. Describe the functions and uses of patch management. 3.3.6.
7. Train users in network security procedures. 3.3.7.

Outcome 3.4 **Multilayer Defense Structure: Explain information technology mechanisms as they apply to a multilayer defense structure.** 3.4.

1. Describe available systems for intrusion prevention, detection, and mitigation. 3.4.1.
2. Analyze system log files to identify security risks. 3.4.2.
3. Compare network analysis software (e.g., network analyzer) and hardware tools to identify security risks and vulnerabilities. 3.4.3.
4. Identify the components of human security (e.g., social engineering) and techniques to mitigate human security threats (e.g., policies, procedures, training). 3.4.4

Outcome 3.5 **Wireless Security: Implement secure wireless networks.** 3.5.

1. Describe wireless security risks (e.g., unauthorized access) and how to mitigate them. 3.5.1.
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]). 3.5.2.
3. Identify security enhancements provided by Institute of Electrical and Electronics Engineers (IEEE). 3.5.3.
4. Describe practices and policies for preventing and detecting installation of rogue networks. 3.5.4.
5. Describe security practices and policies for personal devices. 3.5.5.
6. Implement and test the security of a wireless network. 3.5.6.

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. 4

Outcome 4.2 **Open Systems Interconnection: 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. 4.2.1.
2. Compare Open Systems Interconnection stack positions and their relationships to one another. 4.2.2.
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. 4.2.3.
4. Compare the basics of Transmission Control Protocol/Internet layers, components, and functions. 4.2.4.
5. Describe actions to be performed at each of the Open Systems Interconnection physical layers. 4.2.5.
6. Explain how the Open Systems Interconnection layers relate to the elements of network communication. 4.2.6.

Outcome 4.4 **Wireless Communications: Explain wireless communications.** 4.4.

1. Compare wireless standards in common use (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.11, Cellular, Bluetooth, Worldwide Interoperability for Microwave Access [WiMAX], Radio Frequency Identification [RFID], Near Field Communication [NFC]). 4.4.1.
2. Compare characteristics of wireless signals (e.g., reflection, diffraction, scattering, fading). 4.4.2.
3. Differentiate media access methods used by wireless. 4.4.3.
4. Describe appropriate applications of wireless technologies to specific communication scenarios. 4.4.4.
5. Compare Radio Frequency functions and principles. 4.4.5.

Outcome 4.5 **Wireless Network Solutions: Design and implement wireless network solutions.** 4.5.

1. Compare secure wireless solutions operating in ad-hoc mode and infrastructure mode 4.5.1.
2. Describe the frequency ranges and associated rules in the wireless spectrum as managed by the Federal Communication Commission (FCC). 4.5.2.
3. Describe the Service Set Identifier (SSID) as used in wireless communications. 4.5.3.
. 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. 4.5.4.
. Troubleshoot Wireless Local Area Networks (WLANs) using system logs, vendor-provided utilities, and diagnostic tools. 4.5.5.
6. Secure the wireless network. 4.5.6.

Outcome 4.6 **Network Protocols: Compare 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]). 4.6.1.
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. 4.6.2.
3. Explain the purposes of encapsulation and decapsulation and their relationship to the Open Systems Interconnection (OSI) model. 4.6.3.
4. Explain the difference between User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). 4.6.4.
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]). 4.6.5.
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). 4.6.6.
7. Describe a Virtual Private Network (VPN) and identify associated protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Point-to-Point Tunneling Protocol [PPTP]). 4.6.7.
8. Capture and analyze data packets. 4.6.8.

Outcome 4.7 **Transmission Control Protocol/Internet Protocol (TCP/IP): Describe IP addressing schemes and create subnet masks.** 4.7.

1. Explain Fully Qualified Domain Names (FQDNs) and how they are used. 4.7.1.
2. Explain the IP addressing scheme and how it is used. 4.7.2.
3. Identify Class A, B, and C reserved (i.e., private) address ranges and why they are used. 4.7.3.
4. Identify the class of network to which a given address belongs. 4.7.4.
5. Differentiate between default subnet masks and custom subnet masks. 4.7.5.
6. Explain the relationship between an IP address and its associated subnet mask. 4.7.6.
7. Identify the differences between classful and classless addressing schemes. 4.7.7.
8. Identify multicasting addresses and explain why they are used. 4.7.8.
9. Create custom subnet masks to meet network design requirements. 4.7.9.
10. Compare Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6). 4.7.10

Outcome 4.8 **Network Architecture: 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]). 4.8.1.
2. Identify the components and relationships within the Institute of Electrical and Electronics Engineers (IEEE) 802 standards. 4.8.2.
3. Identify Local Area Network (LAN) performance factors (e.g., signal attenuation, signal propagation delay). 4.8.3.
4. Explain the role of the Internet Engineering Task Force (IETF) in facilitating protocol development. 4.8.4.

Outcome 4.9 **Network Operating Systems: Describe and install network operating systems (OSs).** 4.9.

1 Explain how the components of a network operating system (i.e., server platform, network services software, network redirection software, communications software) support network operations. 4.9.1.

2 Identify licensing requirements. 4.9.2.

3 Describe the characteristics of the tiered model (e.g., peer-to-peer, thin client, thick client, cloud). 4.9.3.

4 Analyze the advantages and disadvantages of the client/server model. 4.9.4.

5 Select network, desktop, and mobile Operating Systems. 4.9.5.

6 Install, test, and patch network Operating Systems manually and using automation. 4.9.6.

7 Log in to a network device (e.g., router, Secure File Transfer Protocol [SFTP] server, directory server). 4.9.7.

8 Evaluate the performance of the network Operating System. 4.9.8.

Outcome 4.10 **Network Administration: Administer network operating systems and services.** 4.10.

1 Select physical and logical topology. 4.10.1.

2 Connect devices to network systems. 4.10.2.

3 Create domain trusts. 4.10.3.

4 Maintain domain controllers. 4.10.4.

5 Create user accounts, groups, and login scripts. 4.10.5.

6 Establish shared network resources. 4.10.6.

7 Define and set access controls on files, folders, shares, and directories. 4.10.7.

8 Configure network domain accounts and profiles. 4.10.8.

9 Create roaming user profiles and use Group Policy Objects (GPO) to manage the user environment. 4.10.9.

10 Troubleshoot network performance connectivity (e.g., performance monitor, command line utilities). 4.10.10.

11 Explain the fundamentals of Quality of Service (QoS). 4.10.11.

12 Securely delegate standard management tasks. 4.10.12.

Outcome 4.12 **Wide Area Network: Design a wide area network (WAN).** 4.12.

1. Select Wide Area Network connections (WAN), (e.g., satellite, broadband, lease line, cellular, Multiprotocol Label Switching [MPLS], SD-WAN, Asynchronous Transfer Mode [ATM]). 4.12.1.
2. Describe point-to-point (PTP) and point-to-multipoint (PTMP) interconnection. 4.12.2.
3. Evaluate and select basic telecommunications services (e.g., satellite, circuit switching, wireless, packet switching) and carriers for WAN requirements. 4.12.3.
4. Identify advantages to a software defined WAN (SD-WAN). 4.12.4.
5. Determine availability from Local Area Network (LAN) to meet WAN requirements. 4.12.5.
6. Determine the speed needed between sites to access applications. 4.12.6.
7. Determine the subnets needed on the WAN (e.g., Variable Length Subnet Masking [VLSM]). 4.12.7.
8. Evaluate and select transmission options. 4.12.8.
9. Evaluate and select routing protocols (e.g., Border Gateway Routing Protocol [BGRP], Open Shortest Path First [OSPF], Routing Information Protocol Version 2 [RIPv2]). 4.12.9.

Outcome 4.13 **Disaster Recovery: Recommend disaster recovery and business continuity plans.** 4.13.

1. Differentiate between disaster recovery and business continuity. 4.13.1.
2. Identify common backup devices. 4.13.2.
3. Identify the criteria for selecting a backup system. 4.13.3.
4. Establish a process for archiving files. 4.13.4.
5. Develop a disaster recovery plan. 4.13.5.