NETWORK SECURITY 11.1999.00
TECHNICAL STANDARDS

An Industry Technical Standards Validation Committee developed and validated these standards on December 7 and January 24, 2024. The Arizona Career and Technical Education Quality Commission, the validating authority for the Arizona Skills Standards Assessment System, endorsed these standards on May 14, 2024.

Note: Arizona's Professional Skills are taught as an integral part of the **Network Security** program.

The Technical Skills Assessment for Network Security is available SY2024-2025.

Note: In this document i.e. explains or clarifies the content and e.g. provides examples of the content that must be taught.

STANDARD 1.0 INVESTIGATE NETWORK SECURITY AS A CAREER

1.1 Explain network security (e.g., the protection of data that is stored on the network or which is in transit across, into, and out of the network)

1.2 Describe the responsibilities of a network security technician (i.e., ensure the network works securely, test and configure software, provide IT support, troubleshoot the network or server, resolve infrastructure issues, etc.)

1.3 Identify skills and ethical characteristics needed to be a successful network security technician (i.e., critical thinking, problem solving, prioritizing, reading, and interpreting network diagrams and technical schematics, preparing and presenting technical information verbally and in writing to different audiences, keeping up to date on network security, etc.)

1.4 Describe education and training opportunities including industry certifications and licensures (i.e., CompTIA, CISCO, CISSP, CEH, etc.)

1.5 Identify career opportunities in network security

STANDARD 2.0 MAINTAIN A SAFE, ENVIRONMENTALLY CONSCIOUS NETWORKING ENVIRONMENT

2.1 Identify hazards and unsafe practices that can lead to serious accidents or injuries (i.e., electrostatic discharge hazards, poor ergonomic practices, etc.)

2.2 Describe OSHA and other state and national regulations designed to reduce safety risks and workplace injuries

2.3 Explain environmental considerations when disposing of computer/network components (i.e., disposing of batteries, devices with lithium batteries, etc.)

2.4 Use techniques to manage power consumption in the networked environment (i.e., test wattage usage, power control, explore green methods such as climate batteries and energy efficiency methods, cloud-based software, etc.)

2.5 Identify energy efficiencies and suggest ways to improve consumption (i.e., office environment AC units, thermostats, computer power settings, etc.)

2.6 Use, maintain, and store tools and equipment according to manufacturer's standards

STANDARD 3.0 DEMONSTRATE BASIC MATHEMATICS FOR NETWORK SECURITY

3.1 Define the number base systems in mathematics related to network technology

3.2 Perform decimal to binary and binary to decimal conversions (e.g., dotted decimal IPv4)

3.3 Perform decimal to hexadecimal and hexadecimal to decimal conversions

3.4 Perform hexadecimal to binary and binary to hexadecimal conversions

3.5 Determine the appropriate method to perform conversions (e.g., paper-pencil and electronic resources)

3.6 Use basic Boolean logic for actions such as Google searches and scripting (e.g., and, not, and or)

STANDARD 4.0 DESCRIBE THE DEVELOPMENT AND EVOLUTION OF COMPUTERS AND NETWORKING

4.1 Define a computer and describe its components and their basic functions (i.e., OSI Model and TCP/IP Model; Input Unit, Output Unit, and Central Processing Unit; displaying data, coding, transferring and processing data; programming programs; etc.)

4.2 Discuss the evolution of computers and future trends in computer networking [i.e., Advanced Research Projects Agency Network (ARPANET), Internet of Things (IoT), privacy, etc.] and societal impacts

4.3 Discuss issues and controversies pertaining to the evolution of mobile computing and the dissemination and centralization of data and its societal impacts (i.e., IoT, Microsoft, Google, anticompetitive practices, privacy, etc.)

4.4 Explain an information system's structure and components [e.g., applications; media (copper cables, fiber, and wireless); network devices (i.e., router, switches, etc.); operating systems; and servers]

4.5 Discuss recent advancements in cybersecurity technologies, threats, and the basics of artificial intelligence (AI) concerning network security

4.6 Discuss emerging problem-solving methodologies such as Zero Trust principles and AI-driven threat detection

STANDARD 5.0 UTILIZE BEST PRACTICES FOR COMPUTER AND NETWORK RISKS AND THREATS

5.1 Explain the risk management process (i.e., define risk, determine risk level, identify methods to address risk, identify inventory assets that may be compromised, identify functionalities, etc.)

5.2 Define network threats to data availability, confidentiality, and integrity

5.3 Discuss and give examples of the severity of data loss to an individual and to an organization

5.4 Identify security threats related to computer data, hardware, and software (i.e., denial of service, eavesdropping, intrusion, unauthorized access, unauthorized use, spoofing, tampering, repudiation, information disclosure, elevation of privilege, etc.)

5.5 Explain the importance of physical security of computer and network hardware following best practices (e.g., cameras, locks, USB port blocking, encryption, bit-locker for Windows, and LBM for Linux)

5.6 Describe network threats (i.e., denial of service, email spoofing, hacking/cracking, intrusion, malware, phishing, social engineering, spamming, system vulnerabilities, website defacement, tampering, repudiation, information disclosure, elevation of privilege, etc.)

5.7 Describe best practices to protect against network threats of data at rest, data in transit, and data during processing (i.e., access control, antivirus software, awareness and training, encryption, firewalls, incident detection systems/tools, intrusion detection prevention, network segmentation, port/service blocking, software updates/patches, etc.)

5.8 Describe password best practices [i.e., authentication, authorization, and accountability (AAA), passphrases, physical keys, password managers, age, complexity, history, length, lockout, etc.]

5.9 Analyze authentication methods used to secure access to the network [i.e., biometrics, key cards, multi-factor authentication (MFA), passwords, single sign-on (SSO), two-factor authentication (2FA), etc.]

5.10 Identify best practices for access control (i.e., changing default passwords, disabling unused accounts, least privileges, privileged account management, role-based access control, etc.) and legal liability of collecting biometric data (e.g., identification of medical information, inadvertently collecting privacy information, and compromising a situation)

STANDARD 6.0 ANALYZE NETWORK MEDIA AND NETWORK TECHNOLOGIES

6.1 Explain the purpose of and types of network media (i.e., fiber optic cable, coaxial cable, ethernet, etc.)

6.2 Explain the purpose and types of topologies (i.e., bus, ring, tree, star, mesh, etc.)

6.3 Compare proper physical network topology

6.4 Identify appropriate connectors, media types, and uses for various networks

6.5 Compare physical and virtual networks [i.e., Software-Defined Wide-Area Network (SD-WAN), Virtual Local Area Network (VLAN), etc.]

6.6 Specify the characteristics of physical network technologies including cable types, length, speed, and topology

6.7 Specify the characteristics of wireless network technologies including frequency, speed, topology, and transmission [i.e., local area, metropolitan area, wide area networks, 5G cellular, Bluetooth, IoT, satellite, Citizens Broadband Radio Service (CBRS), Unlicensed spectrum, etc.]

6.8 Describe the structure of the internet (network of networks)

6.9 Identify the features, functions, and purpose of commonly used network components [i.e., routers, modems, switches, bridges, network interface card (NIC), etc.]

STANDARD 7.0 ANALYZE NETWORK PROTOCOLS AND STANDARDS

7.1 Define a network protocol and explain how it works (e.g., internal and external routing protocol)

7.2 Describe the characteristics, name, and use of the four-layer model of the Transmission Control Protocol/Internet Protocol (TCP/IP) [e.g., Media Access Control (MAC)]

7.3 Describe the characteristics, name, and use of the seven layers of the Open Systems Interconnect (OSI) model

7.4 Explain the concept of ports and identify the port ranges used in networking services and protocols [i.e., dynamic/private (49152-65535); system (0-1023); user (1024-49151); Internet Control Message Protocol (ICMP); Address Resolution Protocol (ARP); etc.]

7.5 Explain the purpose of dynamic and static routing protocols

7.6 Describe standard network ports and protocols [i.e., Domain Name System (DNS); Dynamic Host Configuration Protocol (DHCP); File Transfer Protocol (FTP); Hypertext Transfer Protocol (HTTP); Post Office Protocol (POP); Simple Mail Transfer Protocol (SMTP); Hypertext Transfer Protocol Secure (HTTPS); Secure File Transfer Protocol (SFTP); Virtual Private Network (VPN); Secure Shell (SSH); ICMP/ARP; etc.]

Note: In this document i.e. explains or clarifies the content and e.g. provides examples of the content that must be taught.

7.7 Describe the applications and characteristics of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

7.8 Differentiate IPv4/IPv6 addresses and their corresponding subnet masks [i.e., classful networks, Classless Interdomain Routing (CIDR), private vs. public IP, etc.]

7.9 Summarize the basic characteristics and protocols of Metropolitan Area Network (MAN), Software-Defined Wide Area Network (SD-WAN), and Wide Area Network (WAN) technologies (i.e., frame relay, etc.)

7.10 Describe remote access protocols and services [i.e., remote desktop protocols (RDP), terminal emulator, etc.]

7.11 Describe the function and purpose of security protocols [i.e., Hypertext Transfer Protocol Secure (HTTPS); Secure File Transfer Protocol (SFTP); Virtual Private Network (VPN); Point-to-Point Tunneling Protocol (PPTP); etc.]

7.12 Explain the importance of proper documentation according to industry standards

7.13 Discuss where RFCs (standards) are developed (i.e., IETF, IEEE, 3GPP, etc.)

7.14 Describe methods to determine priorities in establishing and maintaining a computer network

STANDARD 8.0 CONFIGURE A BASIC NETWORK

8.1 Design a network map with virtual and physical segments, (e.g., logical network map)

8.2 Construct dynamic and static routes

8.3 Explain labeling according to industry standards (i.e., cable, device, rack, wall plates, etc.)

8.4 Describe the components needed and purpose to build fault tolerance into a network

8.5 Describe the purpose of a disaster recovery plan for a network

8.6 Install and configure a physical and/or virtual networking system [e.g., Linux/UNIX (3-layer model: kernel, shell, utilities), pipes, and Windows]

8.7 Configure network cards, network settings, and an operating system that provides common services for computer programs

8.8 Configure and connect devices to the network (i.e., computers, printers, routers, switches, etc.)

8.9 Identify and use tools for diagnostic tasks or network repair (i.e., execute Traceroute, ipconfig, Ping, etc.)

STANDARD 9.0 HARDEN A NETWORK

9.1 Explain how to harden the network against unauthorized access and abuse

9.2 Explain the difference among hardening, patching, and types of vulnerabilities (i.e., social, cognitive, environmental, emotional, military, etc.)

9.3 Identify common network threats (i.e., denial of service, eavesdropping, intrusion, probing, unauthorized access, 2.4v5G, Wi-Fi attack vectors, etc.)

9.4 Identify physical network threats [i.e., disrupting media (cutting fiber), environmental/power disruption, unauthorized access to devices, Farraday Cage, etc.]

9.5 Describe the benefits and purpose of segmenting networks (i.e., VLAN, DMZ, etc.)

9.6 Describe the benefits of enabling and disabling ports and network services

9.7 Describe the techniques to secure a Wi-Fi network [i.e., Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 3 (WPA3), IoT device security, etc.]

9.8 Explain the principles of firewall rules and their importance in network hardening (i.e., application, packet filtering, stateful, etc.)

9.9 Describe the benefits, disadvantages, and purposes of using a proxy service

9.10 Describe the benefits, disadvantages, and purposes of using network intrusion detection/prevention systems [i.e., Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Security information and event management (SIEM), etc.]

STANDARD 10.0 PERFORM NETWORK MAINTENANCE AND RESOLVE ISSUES

10.1 Explain the troubleshooting process (e.g., define problem, identify probable cause, test hypothesis, create action, implement action plan, verify solution, and document)

10.2 Prepare a work/maintenance plan and prioritize and schedule network security tasks (i.e., Cron Jobs)

10.3 Describe the purpose and benefits of network utilities [i.e., Network Statistics (netstat), Name Server Lookup (nslookup), Ping, Traceroute, etc.]

10.4 Demonstrate the use of visual indicators and diagnostic utilities (i.e., Wireshark, etc.) to interpret problems

10.5 Identify connectivity issues in various node environments (i.e., smartphones, switches, tablets, Linux/UNIX, Windows, etc.)

10.6 Identify and resolve network issues (i.e., cable failure, connection failure, environmental, misconfigurations, power failure, user error, etc.)

10.7 Identify common tools and methods for monitoring a network (i.e., automation, scripting, AI tools, etc.)

10.8 Describe AI and Machine Learning-based tools for network maintenance and issue resolution [e.g., large language models (LLMs)]

Note: In this document i.e. explains or clarifies the content and e.g. provides examples of the content that must be taught.

STANDARD 11.0 INVESTIGATE LEGAL AND ETHICAL ISSUES RELATED TO NETWORK SECURITY

11.1 Research issues regarding intellectual property rights including software licensing and software duplication [e.g., Business Software Alliance, Creative Commons, Digital Right Management (DRM), Electronic Freedom Foundation (EFF), and Intellectual Property Watch]

11.2 Differentiate among freeware, open source, proprietary, and shareware software relative to legal and ethical issues

11.3 Identify issues, laws, and trends affecting data and privacy [e.g., Certified Network Professional (CNP); General Data Protection Regulation (GDPR); Health Insurance Portability and Accountability Act (HIPAA); Payment Card Industry Data Security Standard (PCI-DSS); Sarbanes-Oxley Act (SOX); Federal Communications System (FCC); and Family Education Rights and Privacy Act (FERPA)]

11.4 Describe acceptable use of industry-related data, private and public networks, and social networking

11.5 Research how data privacy laws and regulations influence network security business practices

11.6 Discuss the responsibilities of network security professionals (i.e., protecting organizational assets, and maintaining consistent and equitable cyber practices, etc.), and explore consequences of unethical behavior to include personal legal liability (i.e., Cyberwire.com/caveat, etc.)