CompTIA Apprenticeships for Tech

CONNECTING DIVERSE TECH TALENT FOR EVERY INDUSTRY

National Guideline Standards for Cybersecurity Support Technician

AIR®
Advancing Evidence.
Improving Lives.

This document summarizes CompTIA's National Guideline Standards (NGS) for apprenticeship programs for Cybersecurity Support Technician

The NGS define:

- The competencies the apprentices will be trained on at the workplace (referred to as the work process schedule)
- The supplemental coursework the apprentice will complete (referred to as the related instruction outline)
- Some elements of the structure of an apprenticeship program

By using the NGS as a starting point, businesses and partners can accelerate program development and more quickly launch Registered Apprenticeship Programs for Cybersecurity Support Technician. The NGS are:

- Designed to be **customizable** to meet the needs of each employer;
- **Competency-based** which provide more program flexibility;
- Complete with recommended minimum **coursework**; and
- **Complementary** and stackable.

OCCUPATION DESCRIPTION

Cybersecurity support technicians detect cyber threats and implement changes to protect an organization. A Security Operations Center (SOC) team typically has several tiers of cybersecurity professionals who are responsible for monitoring, directing, containing, and remediating IT threats. Cybersecurity professionals may be tasked with anything from installing, administering, and troubleshooting security solutions to creating security policies and training documents for colleagues. While other IT job roles are responsible for specific parts of the overall system, cybersecurity professionals must be able to take a step back in order to see the big picture and keep every aspect of the system secure from threats. They may progress in their knowledge and training to become security analysts, cloud security engineers, threat hunters, penetration testers, and compliance managers.

For more information on CompTIA Apprenticeships for Tech or to request the full NGS documents approved by the U.S. Department of Labor, contact us at **ApprenticeshipsForTech@air.org**

Program Structure Elements

The NGS outline many important elements of a quality apprenticeship program, such as:

- Safety of apprentices
- Apprenticeship completion
- Mentoring
- Credit for previous experience
- Equal opportunity pledge

Technical aspects of the NGS are detailed below.

Model: Competency-based apprenticeship

Duration: 2,753 hours – not less than 2,000 hours of on-the-job learning, supplemented by the recommended minimum 753 hours of related instruction.

Minimum Qualifications: 10th grade math and English (apprenticeship program sponsors can identify additional minimum qualifications).

Recommended Wage Schedule: Apprentices shall be paid a progressively increasing schedule of wages based on the current industry average hourly mentor wage rate of $48.00.

- First third of apprenticeship: industry average $25.00
- Second third of apprenticeship: industry average $30.00
- Last third of apprenticeship: industry average $35.00

Recruitment: Apprenticeship program sponsors recruit and select applicants either through an internal process for incumbent workers and/or make the apprenticeship opportunity available to the public and external organizations through outreach efforts, job fairs, collaborative partnerships, and web-based activities. Program sponsors can work with community-based organizations; educational institutions, such as community colleges, technical schools, and high schools; workforce organizations; or other partners to create appropriate outreach and positive recruitment efforts that would reasonably be expected to increase underrepresented population participation in the apprenticeship.

U.S. Department of Labor Codes:

- O*NET-SOC code: ***15-1212.00 Information Security Analysts***
- Registered Apprentice Occupation Code (RAPIDS code): 2050CB

Competencies

The competency sets include both technical and employability skills that the apprenticeship will learn at the workplace. The technical competencies align with designated CompTIA certifications and can be readily aligned with courses designed to prepare students for certification.

PART 1 – BASIC HARDWARE

1. Demonstrate knowledge of various mobile device types, their features, and purpose.
2. Demonstrate skills required to manage and troubleshoot computer hardware and peripheral devices.
3. Demonstrate knowledge of common computer hardware and interfaces.
4. Demonstrate skills required to troubleshoot general computer hardware issues and printer problems.
5. Demonstrate skills required to configure peripherals, printers, and related applications to support external hardware.

PART 2 – BASIC NETWORKING

6. Demonstrate knowledge of basic networking concepts (wired and wireless).
7. Demonstrate skills required to configure and troubleshoot device connectivity (LAN and Internet Access).

PART 3 – CLOUD AND VIRTUALIZATION TECHNOLOGIES

8. Demonstrate knowledge of cloud computing concepts, including cloud storage and security configurations.
9. Demonstrate skills required to configure client-side virtualization, cloud storage applications, and file synchronization features.

PART 4 – OPERATING SYSTEM BASICS

10. Demonstrate knowledge of important Microsoft Windows 10 operating system features and their purpose.
11. Demonstrate skills required to install, configure, and secure Microsoft Windows 10 operating system versions.
12. Demonstrate skills required to troubleshoot Microsoft Windows operating system problems.
13. Demonstrate knowledge of important Mac OS and Linux OS desktop operating system features and their purpose.
14. Demonstrate skills required to configure, secure, and troubleshoot various operating systems Mac OS and Linux OS.
15. Demonstrate skills required to troubleshoot mobile operating systems.

PART 5 – IT SECURITY BASICS

16. Demonstrate knowledge of basic enterprise security concepts and wireless security protocols.
17. Demonstrate skills required to perform account management, configure wireless security, and detect and remove malware on workstations and mobile devices.
18. Demonstrate skills to troubleshoot common computer security issues.
19. Demonstrate skills required to troubleshoot application security issues.

PART 6 – GENERAL IT OPERATIONS

20. Demonstrate knowledge of ticketing systems and documentation procedures.
21. Demonstrate knowledge of disaster recovery concepts and backup procedures.
22. Demonstrate knowledge of licensing and privacy and policy concepts, including how to address prohibited content.
23. Demonstrate knowledge of scripting languages, basic functions, and logic structures.

PART 7 – NETWORK FUNDAMENTALS

24. Demonstrate knowledge of the OSI model and relevant encapsulation concepts.
25. Demonstrate knowledge of network topologies and network types.
26. Demonstrate knowledge of cables, types of connectors, and the purpose for each.
27. Demonstrate skills required to configure a subnet and use appropriate IP addressing schemes.
28. Demonstrate knowledge of ports, protocols, and services, as well as their purpose.
29. Demonstrate knowledge of basic architecture concepts related to corporate and datacenter network environments.
30. Demonstrate knowledge of cloud concepts and connectivity alternatives.

PART 8 – NETWORK IMPLEMENTATIONS

31. Demonstrate knowledge of network devices, their features, and placement within a network.
32. Demonstrate knowledge of routing technologies and concepts for bandwidth management.
33. Demonstrate skills required to configure and deploy Ethernet switching solutions, including VLANs.
34. Demonstrate skills required to deploy wireless standards configurations and technologies.

PART 9 – NETWORK OPERATIONS

35. Demonstrate skills required to leverage statistics and sensors in support of network availability.
36. Demonstrate knowledge of organizational documents and policies.
37. Demonstrate knowledge of high availability and disaster recovery concepts.

PART 10 – NETWORK SECURITY

38. Demonstrate knowledge of network security concepts.
39. Demonstrate knowledge of types of network attacks.
40. Demonstrate skills required to implement network hardening techniques.
41. Demonstrate knowledge of remote access techniques and related security risks.

PART 11 – NETWORK TROUBLESHOOTING

42. Demonstrate skills and best practices required to troubleshoot networking issues.
43. Demonstrate skills required to troubleshoot cable connectivity issues.
44. Demonstrate skills required to use network software tools and commands.
45. Demonstrate skills required to troubleshoot wireless connectivity issues.

PART 12 – THREATS, ATTACKS, AND VULNERABILITIES

46. Demonstrate knowledge of types of social engineering methods.
47. Demonstrate skills required to analyze potential signs to determine the type of attack.
48. Demonstrate skills required to analyze potential signs related to application attacks, including network-based attacks.

PART 13 – ARCHITECTURE AND DESIGN

52. Demonstrate knowledge of foundational security concepts.
53. Demonstrate knowledge of virtualization and cloud computing concepts.
54. Demonstrate knowledge of secure application development, deployment, and automation concepts.
55. Demonstrate knowledge of concepts related to authentication and authorization design.
56. Demonstrate skills required to deploy cybersecurity resilience.
57. Demonstrate knowledge of security risks related to embedded and specialized systems.
58. Demonstrate knowledge of physical security methods.
59. Demonstrate knowledge of cryptographic concepts.

PART 14 – IMPLEMENTATION

60. Demonstrate skills required to deploy host and application security solutions.
61. Demonstrate skills required to deploy secure network designs.
62. Demonstrate skills required to apply configurations for wireless security.
63. Demonstrate skills required to deploy secure mobile phones/devices.
64. Demonstrate skills required to deploy cybersecurity solutions in a cloud environment.
65. Demonstrate skills required to implement identity and account management controls, including public key infrastructure.

PART 15 – OPERATIONS AND INCIDENT RESPONSE

66. Demonstrate knowledge of incident response policies, processes, and procedures.
67. Demonstrate skills required to leverage data sources in support of an investigation.
68. Demonstrate skills required to implement mitigation techniques or controls to secure an environment.
69. Demonstrate knowledge of important aspects related to digital forensics.

PART 16 – GOVERNANCE, RISK AND COMPLIANCE

70. Demonstrate knowledge of relevant regulations, standards, or frameworks that impact the security posture of an organization.
71. Demonstrate knowledge of risk management processes and concepts.
72. Demonstrate knowledge of privacy and sensitive data concepts as they relate to security.

PART 17 – BUSINESS ACUMEN

73. Demonstrate a basic understanding of the employer's corporate structure and business model, including its product and services portfolio, its primary customers, and its top competitors.
74. Demonstrate a basic knowledge of the employer's brand messaging, its value proposition in the marketplace, and key success metrics.

PART 18 – EMPLOYABILITY SKILLS

75. Demonstrate skills to provide competent customer service using active listening and empathy during various interactions (e.g., in-person, over telephone, email, and chat).
76. Demonstrate ability to manage stress and other emotions in the workplace to reduce conflict, foster collaboration, and promote wellness.
77. Demonstrate skills required to take and give productive critical feedback.
78. Demonstrate skills required to problem-solve using critical thinking, clarifying questions, and knowing when to escalate a situation to a superior.
79. Demonstrate skills to explain complex issues to non-technical customers without jargon or blaming.
80. Demonstrate ability to conduct oneself with integrity, professionalism, and in accordance with organization policy and procedure.
81. Demonstrate skills to communicate with colleagues, managers, and end users effectively and clearly, in a timely manner.
82. Demonstrate ability to use language, tone of voice, and non-verbal communication to neutralize conflict in the workplace.
83. Demonstrate skills required to collaborate effectively with team members from across the organization.
84. Demonstrate ability to use respectful cross-cultural communication to work successfully across the organization and with diverse coworkers.
85. Demonstrate knowledge required to manage time effectively, minimizing distractions to maintain productivity, prioritize work appropriately, and meet deadlines with situational awareness.
86. Demonstrate ability to adapt to changing organizational landscape.

Coursework (Related Instruction Outline)

Related instruction can be delivered to apprentices through in-house training, in a classroom, and/or online. The instruction can be provided by any combination of a community college, private industry training provider, sponsoring employer, or computer-based training. The NGS provide approximate number of hours for the related instruction. Course titles and classes may differ slightly from the descriptions below depending upon the related instruction provider.

RELATED INSTRUCTION DESCRIPTIONS	HOURS
New Employee Skills	**15**
• Safety training • Company orientation including privacy and confidentiality • Tools (internal messaging apps, office applications) • Sexual harassment prevention	
Business Acumen	**3**
• Company vision, mission, and key success metrics • The company's products and services and value proposition in the market	
Employability Skills	**60**
• Managing conflict • Being an effective team member • Business communication etiquette • Interpersonal communication • Intercultural communication • Critical thinking • Time management • Workplace wellness and managing stress • Handling workplace change • Leading across generations and personalities • Understanding diversity, equity, and inclusion fundamentals	
Technical and Professional Skills - CompTIA A+ Coursework and Certification	**220**
• Hardware – Identify, use, and connect hardware components and devices • Windows Operating System – Install and support Windows OS including command line and client support • Mobile Devices – Install and configure laptops and other mobile devices • Software Troubleshooting – Troubleshoot computer and mobile device issues including application security support • Networking – Explain types of networks and connections including TCP/IP, WIFI and SOHO • Other OS & technologies – Understand Mac OS, Linux and mobile OS • Hardware and Network Troubleshooting – Troubleshoot device and network issues • Security – Identify and protect against security vulnerabilities for devices and their network connections	

RELATED INSTRUCTION DESCRIPTIONS	HOURS
• Operational Procedures – Follow best practices for safety, environmental impacts, and communication and professionalism • CompTIA A+ CertMaster Learn, CompTIA Labs and CertMaster Practice (or similar courseware) • Pass CompTIA A+ exam	
Technical and Professional Skills - CompTIA Network+ Coursework and Certification	**158**
• Network Fundamentals – OSI model layers and encapsulation concepts. Configuring a subnet and using appropriate IP addressing schemes. • Network implementation – Network devices, their features, and appropriate placement on the network. Configuring and deploying Ethernet switching features, including VLANs. • Network Operations – Using statistics and sensors to ensure network availability. High availability and disaster recovery concepts and solutions. • Network Security – Understand types of network attacks, remote access methods, and related security implications. • Network Troubleshooting – Use appropriate network software tools and commands. Configure and troubleshoot physical and wireless networks. • CompTIA Network+ CertMaster Learn, CertMaster Labs and CertMaster Practice (or similar courseware) • Pass CompTIA Network+ exam	
Technical and Professional Skills - CompTIA Security+ Coursework and Certification	**176**
• Threats, Attacks, and Vulnerabilities • Architecture and Design • Implementation of Cybersecurity • Operations and Incident Response • Governance, Risk, and Compliance • CompTIA Security+ CertMaster Learn, CertMaster Labs (integrated) and CertMaster Practice (or similar courseware) • Pass Security+ exam	
Cybersecurity Risk Management - edX Cybersecurity Risk Management Certificate	**96**
(or similar risk management training) • Information security risk management framework and methodologies • Identifying and modeling information security risks • Qualitative and quantitative risk assessment methods	
Customer Engagement Skills – IBM Professional Certificate	**25**
(or similar customer service training) • Communication skills focused on clear concise communication and listening • Appropriate empathetic behavior such as such as patience, curiosity, and willingness to help • Problem solving to research an issue and help determine an appropriate resolution • Process adherence to ensure the proper flow and Service Level Agreements are met	
TOTAL MINIMUM HOURS:	**753**

"This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under Contract number, 1605C2-20-C-0009, the contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor docs mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government."

CompTIA