**Appendix A**

**Cybersecurity Support Technician**

**O\*NET-SOC CODE: 15-1212.00 RAPIDS CODE: 2050CB**

**WORK PROCESS SCHEDULE**

**AND**

**RELATED INSTRUCTION OUTLINE**

**Appendix A**

**WORK PROCESS SCHEDULE**

**Cybersecurity Support Technician**

**O\*NET-SOC CODE: 15-1212.00 RAPIDS CODE: 2050CB**

This schedule is attached to and a part of these Standards for the above identified occupation.

# APPRENTICESHIP APPROACH

[ ]  Time-based [x]  Competency-based [ ]  Hybrid

# TERM OF APPRENTICESHIP

The term of the apprenticeship is 1 years with an OJL attainment of 86 competencies, supplemented by the minimum required 753 hours of related instruction.

# RATIO OF APPRENTICES TO JOURNEYWORKERS

The apprentice to journeyworker ratio is: 1 Apprentice to1 Journeyworker at worksite.

# APPRENTICE WAGE SCHEDULE

Apprentices shall be paid a progressively increasing schedule of wages based on either a percentage or a dollar amount of the current hourly journeyworker wage rate, which is:
*$*31/hr.

1-Year Term:

Wage upon entering apprenticeship program= $24/hr

Wage upon completion of 43 competencies = $27.50/hr

Final wage upon completion of all competencies = $31/hr.

# PROBATIONARY PERIOD

Every applicant selected for apprenticeship will serve a probationary period of *12 weeks*.

# SELECTION PROCEDURES

Please see page A- 8 .

**Appendix A**

**ON-THE-JOB LEARNING OUTLINE**

**Cybersecurity Support Technician**

**O\*NET-SOC CODE: 15-1212.00 RAPIDS CODE: 2050CB**

Tech Support Specialists are responsible for analyzing, troubleshooting, and rectifying day-to-day technology problems and challenges. This role may support internal clients (employees within the company) or external customers either in-person, on the phone, or via webchat. The specialist may focus on helping individuals and businesses better use or troubleshoot the company’s own technical products, or the specialist may offer support to those using third-party hardware and software applications to do business. In the latter role, the Tech Support Specialist is the person one might call to troubleshoot one’s Wi-Fi router when the internet is down, obtain online permissions to access accounts or files, or to set up a new employee’s email and workstation. In short, Tech Support Specialists are the steady and calm go- to people for those of us who pull our hair out when something goes wrong with our computers.

The following is the rating systems that will be used to determine competency:

|  |  |  |
| --- | --- | --- |
| **Rating System** | **Description** | **Points** |
| Exceeds All Expectations | Consistently exceeds performance standard established for the time in position.  Achieves results above and beyond what is required.  Extends themselves in their roles to exceed personally and as a team to achieve exceptional results. | 5 |
| Meets & Exceeds Some Expectations | Apprentice not only meets all expectations in a fully satisfactory way, but exceeds some of the objectives. | 4 |
| Meets Expectations | Consistently meets the performance standards established for time in position.  Handles routine tasks & some unexpected situation with the usual amount of supervision.  Can continue to develop with coaching, advanced training or more experience | 3 |
| Meets Some Expectations | Apprentice occasionally meets some of the objectives related to this goal, but does not meet others in a fully satisfactory way.  This performance level generally indicates the need for additional coaching, training or other plan for performance improvements. | 2 |
| Does Not Meet / Meets Some Expectations | Does not consistently meet performance standards established for time in position.  Requires basic training, coaching or experience to improve performance and become consistent.  Additional follow-up will be necessary. | 1 |
| Does Not Meet Expectations | Clearly and repeatedly does not meet the performance standards established for time in position.  Additional follow-up and specific suggestions for improvement mandatory. | 0 |

**Apprenticeship Competencies – Technical**

| **Work Processes** | **Validated By** | **Rating** | **Date** | **COMPTIA Assessment** |
| --- | --- | --- | --- | --- |
| **Part 1 Basic Hardware** |  |
| 1. Demonstrate knowledge of various mobile device types, their features, and purpose.  |  |  |  | **Completion of COMPTIA A+ 1101 Coursework** |
| 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). |  |  |  | **Completion of COMPTIA A+ 1101 Coursework** |
| 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 |  |  |  | **Completion of COMPTIA A+ 1101 Coursework** |
| 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. |  |  |  | **Completion of COMPTIA A+ 1101 Coursework** |
| 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. |  |  |  | **Completion of COMPTIA A+ 1101 Coursework** |
| 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. |  |  |  | **Completion of COMPTIA A+ 1101 Coursework** |
| 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. |  |  |  | **Completion of COMPTIA A+ 1101 Coursework** |
| 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. |  |  |  | **Completion of CompTIA Network+ Coursework** |
| 25. Demonstrate knowledge of network topologies and network types. |  |  |  |
| 26. Demonstrate knowledge of cables, types of connectors, and the purpose for each.  |  |  |  | **Completion of CompTIA Network+ Coursework** |
| 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.  |  |  |  | **Completion of CompTIA Network+ Coursework** |
| 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. |  |  |  | **Completion of CompTIA Network+ Coursework** |
| 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.  |  |  |  | **Completion of CompTIA Network+ Coursework** |
| 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. |  |  |  | **Completion of CompTIA Network+ Coursework** |
| 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.  |  |  |  | **Completion of CompTIA Security+ Coursework** |
| 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.  |  |  |  |
| 49. Demonstrate knowledge of threat actors, vectors, and intelligence sources.  |  |  |  |
| 50. Demonstrate knowledge of security concerns related to several types of vulnerabilities. |  |  |  |
| 51. Demonstrate knowledge of methods used to assess organizational security, including compliance and security assessments and penetration tests. |  |  |  |  |
| **Part 13 Architecture and Design** |  |  |  |  |
| 52. Demonstrate knowledge of foundational security concepts.  |  |  |  | **Completion of CompTIA Security+ Coursework** |
| 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.  |  |  |  | **Evaluated by Participating Employer Partner** |
| 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.  |  |  |  | **Evaluated by Participating Employer Partner** |
| 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.  |  |  |  | **Evaluated by Participating Employer Partner** |
| 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.  |  |  |  | **Completion of CompTIA Security+ Coursework** |
| 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. |  |  |  | **Evaluated by participating employer partner** |
| 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). |  |  |  | **Completion of ITIL 4 Foundation Coursework** |
| 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. |  |  |  |

**Appendix A**

**RELATED INSTRUCTION OUTLINE**

**Cybersecurity Support Technician**

**O\*NET-SOC CODE: 15-1212.00 RAPIDS CODE: 2050CB**

Related instruction to be provided by ACI Learning

8663 Baypine Road, Building 4, Suite 104

Jacksonville, FL 32256

**Related Instruction Descriptions: Approximate 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 • 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, CompTIA 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 – edXCybersecurity Risk Management Certificate** | **96** |
| • 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 |  |
| **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**

**SELECTION PROCEDURES**

* 1. Each applicant will complete an open position application and submit all required documentation.
	2. Receipt of the properly completed application form along with required supporting documents (driver’s license, birth certificate, or other acceptable proof of age; copy of high school diploma, GED certificate, or other acceptable documentation of education) will constitute receipt of a completed application.
	3. Once a list of qualified applicants is received, the employer partner and their designated officials will interview each candidate and forward its recommendations to the Human Resources Manager.

* 1. Each applicant will be required to review the Apprenticeship Program Standards and will be provided information about the program.
	2. The Human Resources Manager and Department Manager will make the final selection based upon occupational requirements and needs of the company.
	3. Selected applicants must respond to the notice of selection within 48 hours of notice. If an applicant cannot be reached by telephone or e-mail, their name will be passed and notification of missed opportunity will be sent. If no response is received within 15 days, applicant will be dropped from ranking list.
	4. Upon selection to the registered apprenticeship program, selected applicants will be registered into the RAPIDS 2.0 system.