**Appendix A3**

**WORK PROCESS SCHEDULE**

**AND**

**RELATED INSTRUCTION OUTLINE**

**DEVELOPED BY**

**United States Help Desk Academy**

**FOR THE OCCUPATION OF**

**Cybersecurity Support Technician**

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

**Appendix A3**

**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 ☒ Competency-based ☐ Hybrid

# TERM OF APPRENTICESHIP

The term of the apprenticeship is reasonably expected to be completed within one year with an on-the-job learning (OJL) attainment of all competencies of the position, supplemented by the minimum recommended 140 hours of related instruction.

# RATIO OF APPRENTICES TO JOURNEYWORKERS

The apprentice to journeyworker ratio is: 1 Apprentice to 1 Journeyworker.

# 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: $30.00.

|  |  |  |
| --- | --- | --- |
| **Period** | **Percent of Journeyworker Wage** | **Wage (Hourly)** |
| 1st | 83% | $25.00 |
| 2nd | 92% | $27.50 |

# PROBATIONARY PERIOD

Every applicant selected for apprenticeship will serve a probationary period of 25% of the OJL hours which equals 500 hours.

# SELECTION PROCEDURES

Applicants will be accepted throughout the year or as specified by the employer. Every person requesting an application will have one made available upon signing the applicant log.

All applications will be identical in form and requirements. The application form will be numbered in sequence corresponding with the number appearing on the applicant log so that all applications can be accounted for. Columns will be provided on the applicant log to show race, ethnicity, and sex and the progress by dates and final disposition of each application.

Before completing the application, each applicant will be required to review the Apprenticeship Standards and will be provided information about the program. If the applicant has any additional questions on the qualifications or needs additional information to complete the application, it will be provided by the sponsor.

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 the completed application.

Completed applications will be checked for minimum qualifications. Applicants deficient in one or more qualifications or requirements or making false statements on their applications will be notified in writing of their disqualification and of the appeal rights available to them. No further processing of such applications will be taken.

Applicants meeting the minimum qualifications and submitting the required documents will be notified where and when to appear for an interview (if applicable).

The sponsor may select apprentices from a pool of eligible applicants on the basis of the rank order of their scores on one or more qualification standards where there is a significant statistical relationship between rank order of scores and performance in the apprenticeship program. The selection of any qualification standards beyond minimum legal working age, the use of oral interviews, the notification of applicants, and the establishment of goals for the admission of minorities and women (minority and nonminority) into the pool of eligibles must proceed in accordance with the requirements of 29 CFR § 30.S(b)(l) and NAC 610.845. The method of rating is listed by each employer.

An individual who has completed a structure pre-apprenticeship training program that meets the requirements outlined in Training and Employment Notice 13-12, Defining a Quality Pre-Apprenticeship Program and Related Tools and Resources, in any occupational area covered in these standards of apprenticeship and who meets the minimum qualifications of the apprenticeship program may be admitted directly into the program. The candidate shall provide official documentation confirming that he or she fulfilled the specific requirements of the pre-apprenticeship program, such as completion/graduation certificates, transcripts, notarized letters of confirmation, and sworn statements.

The sponsor will evaluate the training received to grant appropriate credit on the term of apprenticeship. Entry of pre-apprenticeship candidates shall be done without regard to race, color, religion, national origin, or sex. (Note: This is a method of direct entry into the apprenticeship program.)

**WORK PROCESS SCHEDULE**

**Cybersecurity Support Technician**

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

**Description:**  A Cybersecurity Support Specialist plans, implements, upgrades, or monitors security measures for the protection of computer networks and information. Assesses system vulnerabilities for security risks and proposes and implements risk mitigation strategies. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses.

The term of the apprenticeship shall be defined by the attainment of competencies, both technical and behavioral, of the apprenticeship as listed in the tables reasonably within one year of OJL.

Competency in the work processes outlined herein can be demonstrated through a variety of venues including: observation, proficiency demonstration/aptitude exam, questions and answers, learner’s products, simulations, project work, and/or mentor testimony or evidence as demonstrated on the job.

United States Help Desk Academy will assess each apprentice’s prior experience to determine what credit for advanced standing will be awarded for work processes schedule (WPS) and Related Instruction (RI). Prior experience will be assessed through resumes, interviews, previous job assignments and/or demonstration of competencies. Assigned mentors will assess apprentices for credit for prior experience at any time during the probationary period.

**Apprenticeship Competencies – Technical**

**Evaluation Matrix**

**Work Processes Assessment**

The following is a sample recommended rating system to determine competency. Mentors may utilize an equivalent tool, such as a learning plan, for documenting competency. Assessments will occur not less frequently than the wage schedule periods indicated.

|  |  |  |
| --- | --- | --- |
| **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 | Employee 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 | Employee 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 |

**WORK PROCESS SCHEDULE**

The following are the core Cybersecurity Support Technician related work processes for the apprenticeship.

|  |  |  |  |
| --- | --- | --- | --- |
| **Job Function 1: Assists in developing security policies and protocols; assists in enforcing company compliance with network security policies and protocols** | **Rating** | **Validated by**  **Initials** | **Date** |
| Locates (in Intranet, employee handbook or security protocols) organizational policies intended to maintain security and minimize risk and explains their use |  |  |  |
| Provides guidance to employees on how to access networks, set passwords, reduce security threats and provide defensive measures associated with searches, software downloads, email, Internet, add-ons, software coding and transferred files |  |  |  |
| Ensures that password characteristics are explained and enforced and that updates are required and enforced based on appropriate time intervals |  |  |  |
| Explains company or organization’s policies regarding the storage, use and transfer of sensitive data, including intellectual property and personally identifiable information. Identifies data life cycle, data storage facilities, technologies and describes business continuity risks |  |  |  |
| Assigns individuals to the appropriate permission or access level to control access to certain web IP addresses, information and the ability to download programs and transfer data to various locations |  |  |  |
| Assists employees in the use of technologies that restrict or allow for remote access to the organization's information technology network |  |  |  |
| Develops security compliance policies and protocols for external services (i.e. Cloud service providers, software services, external data centers) |  |  |  |
| Complies with incident response and handling methodologies |  |  |  |
| Articulates the business need or mission of the organization as it pertains to the use of IT systems and the storage of sensitive data |  |  |  |
| **Job Function 2: Provides technical support to users or customers** | **Rating** | **Validated by**  **Initials** | **Date** |
| Manages inventory of IT resources |  |  |  |
| Diagnoses and resolves customer-reported system incidents |  |  |  |
| Installs and configures hardware, software and peripheral equipment for system users |  |  |  |
| Monitors client-level computer system performance |  |  |  |
| Tests computer system performance |  |  |  |
| Troubleshoots system hardware and software |  |  |  |
| Administers accounts, network rights, and access to systems and equipment |  |  |  |
| Implements security measures for uses in system and ensures that system designs incorporate security configuration guidelines |  |  |  |
| **Job Function 3:**  **Installs, configures, tests, operates, maintains and manages networks and their firewalls including hardware and software that permit sharing and transmission of information** | **Rating** | **Validated by**  **Initials** | **Date** |
| Collaborates with system developers and users to assist in the selection of appropriate design solutions to ensure the compatibility of system components |  |  |  |
| Installs, replaces, configures and optimizes network hubs, routers and switches |  |  |  |
| Assists in network backup and recovery procedures |  |  |  |
| Diagnoses network connectivity problems |  |  |  |
| Modifies network infrastructure to serve new purposes or improve workflow |  |  |  |
| Integrates new systems into existing network architecture |  |  |  |
| Patches network vulnerabilities to ensure information is safeguarded against outside parties |  |  |  |
| Repairs network connectivity problems |  |  |  |
| Tests and maintains network infrastructure including software and hardware devices |  |  |  |
| Establishes adequate access controls based on principles of least privilege and need-to-know |  |  |  |
| Implements security measures for users in system and ensures that system designs incorporate security configuration guidelines |  |  |  |
| **Job Function 4:**  **Installs, configures, troubleshoots and maintains server configurations to ensure their confidentiality, integrity and availability; also manages accounts, firewalls, configuration, patch and vulnerability management. Is responsible for access control, security configuration and administration** | **Rating** | **Validated by**  **Initials** | **Date** |
| Checks system hardware availability, functionality, integrity and efficiency |  |  |  |
| Conducts functional and connectivity testing to ensure continuing operability |  |  |  |
| Conducts periodic server maintenance including cleaning (physically and electronically), disk checks, system configuration and monitoring, data downloads, backups and testing |  |  |  |
| Assists in the development of group policies and access control lists to ensure compatibility with organizational standards, business rules and needs |  |  |  |
| Documents compliance with or changes to system administration standard operating procedures |  |  |  |
| Installs server fixes, updates and enhancements |  |  |  |
| Maintains baseline system security according to organizational policies |  |  |  |
| Manages accounts, network rights and access to systems and equipment |  |  |  |
| Monitors and maintains server configuration |  |  |  |
| Supports network components |  |  |  |
| Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs |  |  |  |
| Verifies data redundancy and system recovery procedures |  |  |  |
| Assists in the coordination or installation of new or modified hardware, operating systems and other baseline software |  |  |  |
| Provides ongoing optimization and problem-solving support |  |  |  |
| Resolves hardware/software interface and interoperability problems |  |  |  |
| Establishes adequate access controls based on principles of least privilege, role based access controls (RBAC) and need-to- know |  |  |  |
| **Job Function 5:**  **Configures tools and technologies to detect, mitigate and prevent potential threats** | **Rating** | **Validated by**  **Initials** | **Date** |
| Installs and maintains cyber security detection, monitoring and threat management software |  |  |  |
| Coordinates with network administrators to administer the updating of rules and signatures for intrusion/detection protection systems, anti-virus and network black and white list |  |  |  |
| Manages IP addresses based on current threat environment |  |  |  |
| Ensures application of security patches for commercial products integrated into system design |  |  |  |
| Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity |  |  |  |
| **Job Function 6:**  **Assesses and mitigates system network, business continuity and related security risks and vulnerabilities** | **Rating** | **Validated by**  **Initials** | **Date** |
| Applies security policies to meet security objectives of the system |  |  |  |
| Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices |  |  |  |
| Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs |  |  |  |
| Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization |  |  |  |
| Installs, manages and updates intrusion detection system |  |  |  |
| Performs technical and non- technical risk and vulnerability assessments of relevant technology focus areas |  |  |  |
| Conducts authorized penetration testing (Wi-Fi, network perimeter, application security, cloud, mobile devices) and assesses results |  |  |  |
| Documents systems security operations and maintenance activities |  |  |  |
| Communicates potential risks or vulnerabilities to manager. Collaborates with others to recommend vulnerability corrections |  |  |  |
| Identifies information technology security program implications of new technologies or technology upgrades |  |  |  |
| **Job Function 7:**  **Reviews network utilization data to identify unusual patterns, suspicious activity or signs of potential threats** | **Rating** | **Validated by**  **Initials** | **Date** |
| Identifies organizational trends with regard to the security posture of systems; identifies |  |  |  |
| Characterizes and analyzes network traffic to identify anomalous activity and potential threats; performs computer network defense trend analysis and reporting |  |  |  |
| Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts |  |  |  |
| Runs tests to detect real or potential threats, viruses, malware, etc. |  |  |  |
| Assists in researching cost-effective security controls to mitigate risks |  |  |  |
| Helps perform damage assessments in the event of an attack |  |  |  |
| Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities |  |  |  |
| Documents and escalates incidents that may cause immediate or long-term impact to the environment |  |  |  |
| Provides timely documentation, identification and alerts of possible attacks and intrusions, anomalous activities, and distinguish these incidents and events from normal baseline activities |  |  |  |
| Uses network monitoring tools to capture and analyze network traffic associated with malicious activity |  |  |  |
| Performs intrusion analysis |  |  |  |
| Sets containment blockers to align with company policy regarding computer use and web access |  |  |  |
| **Job Function 8:**  **Responds to cyber intrusions and attacks and provides defensive strategies** | **Rating** | **Validated by**  **Initials** | **Date** |
| Assists in the development of appropriate courses of action in response to identified anomalous network activity |  |  |  |
| Triages systems operations impact: malware, worms, man-in-the-middle attack, denial of service, rootkits, keystroke loggers, SQL injection and cross- site scripting |  |  |  |
| Reconstructs a malicious attack or activity based on network traffic |  |  |  |
| Correlates incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation |  |  |  |
| Monitors external data sources to maintain currency of Computer Network Defense threat condition and determines which security issues may have an impact on the enterprise. Performs file signature analysis |  |  |  |
| Performs analysis of log files from a variety of sources to identify threats to network security; performs file signature analysis |  |  |  |
| Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation |  |  |  |
| Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts |  |  |  |
| Tracks and documents computer network defense incidents from initial detection through final resolution |  |  |  |
| Collects intrusion artifacts and uses discovered data to enable mitigation of potential computer network defense (CND) incidents |  |  |  |
| Performs virus scanning on digital media |  |  |  |

A combination of the above work processes will be reasonably completed within one year of OJL in the apprenticeship. Based on the apprentice’s work assignment, the time spent in each of the work processes will vary.

The above on-the-job-training (OJT) work process schedule is intended as a guide. The WPS need not be followed in any sequence, and it is understood that some adjustments may be necessary in the percentage of time spent in each of the work processes to allow for different work experiences. In all cases, the apprentice is to receive sufficient work experiences to make them fully competent and use good workmanship in all work processes, which are a part of the industry. In addition, the apprentice shall be fully instructed in safety and OSHA requirements.

**Apprenticeship Competencies – Behavioral**

In addition to mastering all of the essential technical competencies, an apprentice must consistently demonstrate at an acceptable level the following behavioral competencies in order to complete the apprenticeship.

|  |  |
| --- | --- |
| **Item #** | **Behavioral Competencies** |
| **1.** | Participate and focus in team discussions/meetings |
| **2.** | Able to work independently |
| **3.** | Openness to new ideas and change |
| **4.** | Ability to deal with ambiguity by exploring, asking questions, etc. |
| **5.** | Knows when to ask for help |
| **6.** | Able to demonstrate effective presentation skills |
| **7.** | Able to demonstrate effective communication skills individually and in group settings |
| **8.** | Maintains an acceptable attendance record |
| **9.** | Reports to work on time |
| **10.** | Completes assigned tasks on time |
| **11.** | Uses appropriate language |
| **12.** | Demonstrates respect for students, co-workers and supervisors |
| **13.** | Demonstrates trust, honesty and integrity |
| **14.** | Requests and performs work assignments without prompting |
| **15.** | Appropriately cares for personal dress, grooming and hygiene |
| **16.** | Maintains a positive attitude |
| **17.** | Collaborate with and assists co-workers |
| **18.** | Follows instructions/directions |
| **19.** | Able to work under supervision |
| **20.** | Able to self-reflect and accept constructive feedback and criticism |
| **21.** | Able to follow safety rules |
| **22.** | Able to take care of equipment and work place |
| **23.** | Able to keep work area neat and clean |
| **24.** | Able to meet supervisor's work standards |
| **25.** | Able to not let personal life interfere with work |
| **26.** | Adheres to work policies/rules/regulations |

**RELATED INSTRUCTION OUTLINE**

**Cybersecurity Support Technician**

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

The related instruction has been developed by the employer as part of the Computer User Support Specialist apprenticeship. This instruction shall include a minimum recommended 140 hours of related instruction (RI) throughout the apprenticeship. The curriculum is defined as a variety of courses, including self-directed web-based courses with oversight by a trainer, around which the projects and assessments are based. By defining the RI this way, all competencies required of the apprentices are met, through project work.

United States Help Desk Academy will assess each apprentice’s prior learning to determine what credit will be awarded for the RI, as well as for meeting the prerequisite and completion requirements of the apprenticeship. Prior learning will be assessed through transcripts, certifications, course credits, and/or demonstrated skills. Assigned mentors will assess apprentices for credit for prior learning at any time during the probationary period.

The following core and as-assigned course topics outlined below may be delivered by various educational institutions and training providers, as determined and approved by sponsor and employer.

**COURSE TOPICS**

The following are the core technical course topics for the apprenticeship.

|  |  |
| --- | --- |
| **CORE COURSE TOPICS** | **HOURS** |
| Cybersecurity Threat Landscape | 4 |
| Security concepts of Information assurance | 2 |
| Risk Management Process | 7.25 |
| Security Controls | 3 |
| Governance, Elements and Processes | 4 |
| Attacks, Threats and Vulnerabilities | 5 |
| Access Control Concepts | 4.75 |
| Physical Access Controls | 2.5 |
| Physical Security Introduction | 3 |
| Intro to Cyber Threat Intelligence | 4.5 |
| Identify Attack Types/Surfaces | 4.75 |
| Computer Networking | 5 |
| Network Threats and Attacks | 4 |
| Network Security Infrastructure | 5.25 |
| Remote Access | 9.5 |
| Network Authentication | 4 |
| Cryptography Implementations | 5 |
| Hashing | 2 |
| Using File Encryption to Secure Information | 3.5 |
| Incident Response | 3 |
| Business Continuity | 4 |
| Disaster Recovery | 7 |
| Data Security | 8 |
| Data System Hardening | 3 |
| Best Practice Security Policies | 5 |
| Windows Fundamentals | 12 |
| Linux Fundamentals | 15 |
|  |  |
| **Total Core Hours** | **140** |

The following are as-assigned course topics for the apprenticeship. An employer or program may require these additional course topics as part of a program-specific assignment. These as-assigned course topics may differ for the occupational variation in focus of the apprenticeship. The number of hours shows a range, adjustable based on the employer’s needs and areas of emphasis.

|  |  |
| --- | --- |
| **AS-ASSIGNED COURSE TOPICS** | **Hours** |
| Teamwork and Collaboration | 8 |
| Communication | 10 |
| Problem Solving | 5 |
| Critical Thinking | 3 |
| Conflict Management | 3 |
| Time Management | 5 |
| Customer Service | 3 |
| **Total Recommended Hours** | **37** |

The above related instruction (RI) outline is intended as a guide. The course topics need not be followed in any sequence, and it is understood that some adjustments in course topics/subtopics may be necessary to allow for different learning experiences. In all cases, the apprentice is to receive sufficient RI to allow them to obtain the knowledge necessary to perform the relevant competencies using good workmanship in all work processes which are a part of the industry. In addition, the apprentice shall be fully instructed in safety and OSHA requirements.