# Section 3: Work Process Schedule

|  |  |  |
| --- | --- | --- |
| WORK PROCESS SCHEDULE  Cyber Security Support Technician | | ONET Code: 15.1122  RAPIDS Code: |
| NOTE: This occupational framework has been mapped to the NICE Framework to ensure consistency with the lexicon developed by the NICE working group. (https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework) | | |
| JOB TITLE: | | |
| LEVEL: | SPECIALIZATION: | |
| STACKABLE PROGRAM \_\_\_Yes \_\_\_\_\_\_no  BASE OCCUPATION NAME: IT Generalist | | |
| Company Contact: Name | | |
| Address: | Phone | Email |
| Apprenticeship Type:  \_\_\_\_\_\_\_Competency-Based  \_\_\_\_\_\_\_Time-Based \_\_\_\_\_\_\_Hybrid |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| JOB FUNCTION 1: Assists in developing security policies and protocols; assists in enforcing company compliance with network security policies and protocols | Core or Optional | | Level |
| Competencies | Level | NICE Framework Category | NICE Framework Specialty Area |
| 1. Locates (in Intranet, employee handbook or security protocols) organizational policies intended to maintain security and minimize risk and explains their use | Basic | Oversee and Govern | Education and Training |
| 1. 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 | Advanced | Securely Provision | Information Assurance Compliance |
| 1. Ensures that password characteristics are explained and enforced and that updates are required and enforced based on appropriate time intervals | Basic | Securely Provision | Information Assurance Compliance |
| 1. 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 | Intermediate | Oversee and Govern | Education and Training |
| 1. 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 | Advanced | Securely Provision | Information Assurance Compliance |
| 1. Assists employees in the use of technologies that restrict or allow for remote access to the organization's information technology network | Intermediate | Oversee and Develop | Education and Training |
| 1. Develops security compliance policies and protocols for external services (i.e. Cloud service providers, software services, external data centers) | Advanced | Securely Provision | Information Assurance Compliance |
| 1. Complies with incident response and handling methodologies | Advanced | Protect and Defend | Computer Network Defense Analysis |
| 1. Articulates the business need or mission of the organization as it pertains to the use of IT systems and the storage of sensitive data | Intermediate | Securely Provision | System Security Architecture |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| JOB FUNCTION 2: Provides technical support to users or customers | Core or Optional | | | | Level | | |
| Competencies | Level | NICE Framework Category | | | NICE Framework Specialty Area | | |
| 1. Manages inventory of IT resources | Basic | Operate/  Maintain | | | Customer Service and Technical Support | | |
| 1. Diagnoses and resolves customer-reported system incidents | Intermediate | Investigate | | | Digital forensics | | |
| 1. Installs and configures hardware, software and peripheral equipment for system users | Basic | Operate/  Maintain | | | Customer Service and Technical Support | | |
| 1. Monitors client-level computer system performance | Basic | Operate/  Maintain | | | Customer Service and Technical Support | | |
| 1. Tests computer system performance | Basic | Operate/  Maintain | | | Customer Service and Technical Support | | |
| 1. Troubleshoots system hardware and software | Basic | Operate/  Maintain | | | Customer Service and Technical Support | | |
| 1. Administers accounts, network rights, and access to systems and equipment | Intermediate | Operate/  Maintain | | | Customer Service and Technical Support | | |
| 1. Implements security measures for uses in system and ensures that system designs incorporate security configuration guidelines | Advanced | Operate/  Maintain | | | Systems Security Analysis | | |
|  |  | | | |  | | |
| 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 | Core or Optional | | | | Level | | |
| Competencies | Level | | NICE Framework Category | | NICE Framework Specialty Area | | |
| 1. Collaborates with system developers and users to assist in the selection of appropriate design solutions to ensure the compatibility of system components | Intermediate | | Securely Provision | | Systems Security Architecture | | |
| 1. Installs, replaces, configures and optimizes network hubs, routers and switches | Advanced | | Operate and Maintain | | Network Services | | |
| 1. Assists in network backup and recovery procedures | Intermediate | | Operate and Maintain | | Network Services | | |
| 1. Diagnoses network connectivity problems | Basic | | Operate and Maintain | | Network Services | | |
| 1. Modifies network infrastructure to serve new purposes or improve workflow | Advanced | | Operate and Maintain | | Network Services | | |
| 1. Integrates new systems into existing network architecture | Intermediate | | Operate and Maintain | | Network Services | | |
| 1. Patches network vulnerabilities to ensure information is safeguarded against outside parties | Intermediate | | Operate and Maintain | | Network Services | | |
| 1. Repairs network connectivity problems | Basic | | Operate and Maintain | | Network Services | | |
| 1. Tests and maintains network infrastructure including software and hardware devices | Basic | | Operate and Maintain | | Network Services | | |
| 1. Establishes adequate access controls based on principles of least privilege and need-to-know | Intermediate | | Operate and Maintain | | Network Services | | |
| 1. Implements security measures for users in system and ensures that system designs incorporate security configuration guidelines | Basic | | Operate and Maintain | | Systems Security Analysis | | |
|  |  | | | |  | |
| **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** | Core or Optional | | | | Level | |
| Competencies | Level | | NICE Framework Category | | NICE Framework Specialty Area | |
| 1. Checks system hardware availability, functionality, integrity and efficiency | Intermediate | | Operate and Maintain | | System Admin | |
| 1. Conducts functional and connectivity testing to ensure continuing operability | Basic | | Operate and Maintain | | System Admin | |
| 1. Conducts periodic server maintenance including cleaning (physically and electronically), disk checks, system configuration and monitoring, data downloads, backups and testing | Basic | | Operate and Maintain | | System Admin | |
| 1. Assists in the development of group policies and access control lists to ensure compatibility with organizational standards, business rules and needs | Advanced | | Operate and Maintain | | System Admin | |
| 1. Documents compliance with or changes to system administration standard operating procedures | Intermediate | | Operate and Maintain | | System Admin | |
| 1. Installs server fixes, updates and enhancements | Intermediate | | Operate and Maintain | | System Admin | |
| 1. Maintains baseline system security according to organizational policies | Intermediate | | Operate and Maintain | | System Admin | |
| 1. Manages accounts, network rights and access to systems and equipment | Basic | | Operate and Maintain | | System Admin | |
| 1. Monitors and maintains server configuration | Intermediate | | Operate and Maintain | | System Admin | |
| 1. Supports network components | Basic | | Operate and Maintain | | System Admin | |
| 1. Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs | Basic | | Operate and Maintain | | System Admin | |
| 1. Verifies data redundancy and system recovery procedures | Intermediate | | Operate and Maintain | | System Admin | |
| 1. Assists in the coordination or installation of new or modified hardware, operating systems and other baseline software | Intermediate | | Operate and Maintain | | System Admin | |
| 1. Provides ongoing optimization and problem-solving support | Intermediate | | Operate and Maintain | | System Admin | |
| 1. Resolves hardware/software interface and interoperability problems | Basic | | Operate and Maintain | | System Admin | |
| 1. Establishes adequate access controls based on principles of least privilege, role based access controls (RBAC) and need-to-know | Advanced | | Operate and Maintain | | System Admin | |
|  |  | | | | |  | | |
| JOB FUNCTION 5: Configures tools and technologies to detect, mitigate and prevent potential threats | Core or Optional | | | | | Level | | |
| Competencies | Level | | | NICE Framework Category | | NICE Framework Specialty Area | |
| 1. Installs and maintains cyber security detection, monitoring and threat management software | Intermediate | | |  | |  | |
| 1. 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 | Intermediate | | |  | |  | |
| 1. Manages IP addresses based on current threat environment | Intermediate | | |  | |  | |
| 1. Ensures application of security patches for commercial products integrated into system design | Basic | | |  | |  | |
| 1. Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity | Advanced | | |  | |  | |
|  |  | | | | |  | | |
| JOB FUNCTION 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities | Core or Optional | | | | | Level | | |
| Competencies | Level | | | NICE Framework Category | | NICE Framework Specialty Area | |
| 1. Applies security policies to meet security objectives of the system | Intermediate | | | Operate and Maintain | | Systems Security Analysis | |
| 1. Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices | Intermediate | | | Operate and Maintain | | Systems Security Analysis | |
| 1. Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs | Basic | | | Operate and Maintain | | Systems Security Analysis | |
| 1. Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization | Advanced | | | Operate and Maintain | | Systems Security Analysis | |
| 1. Installs, manages and updates intrusion detection system | Advanced | | | Operate and Maintain | | Systems Security Analysis | |
| 1. Performs technical and non-technical risk and vulnerability assessments of relevant technology focus areas | Advanced | | | Protect and Defend | | Vulnerability Assessment & Management | |
| 1. Conducts authorized penetration testing (Wi-Fi, network perimeter, application security, cloud, mobile devices) and assesses results | Intermediate | | | Protect and Defend | | Vulnerability Assessment & Management | |
| 1. Documents systems security operations and maintenance activities | Intermediate | | | Operate and Maintain | | Systems Security Analysis | |
| 1. Communicates potential risks or vulnerabilities to manager. Collaborates with others to recommend vulnerability corrections | Advanced | | | Protect and Defend | | Computer Network Defense and Analysis | |
| 1. Identifies information technology security program implications of new technologies or technology upgrades | Advanced | | | Protect and Defend | | Computer Network Defense and Analysis | |
|  |  | | | | |  | | |
| **JOB FUNCTION 7: Reviews network utilization data to identify unusual patterns, suspicious activity or signs of potential threats** | Core or Optional | | | | | Level | | |
| Competencies | Level | | | NICE Framework Category | | NICE Framework Specialty Area | |
| 1. Identifies organizational trends with regard to the security posture of systems; identifies unusual patterns or activities | Basic | | | Operate and Maintain | | Systems Security Analysis | |
| 1. Characterizes and analyzes network traffic to identify anomalous activity and potential threats; performs computer network defense trend analysis and reporting | Advanced | | | Protect and Defend | | Computer network Defense and Analysis | |
| 1. Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | Advanced | | | Protect and Defend | | Computer network Defense and Analysis | |
| 1. Runs tests to detect real or potential threats, viruses, malware, etc. | Advanced | | |  | |  | |
| 1. Assists in researching cost-effective security controls to mitigate risks | Intermediate | | | Protect and Defend | | Vulnerability Assessment and Management | |
| 1. Helps perform damage assessments in the event of an attack | Advanced | | |  | |  | |
| 1. Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities | Advanced | | | Operate and Maintain | | Systems Security Analysis | |
| 1. Documents and escalates incidents that may cause immediate or long-term impact to the environment | Intermediate | | | Protect and Defend | | Computer network Defense Analysis | |
| 1. Provides timely detection, identification and alerts of possible attacks and intrusions, anomalous activities, and distinguish these incidents and events from normal baseline activities | Advanced | | | Protect and Defend | | Computer network Defense Analysis | |
| 1. Uses network monitoring tools to capture and analyze network traffic associated with malicious activity | Advanced | | | Investigate | | Digital Forensics | |
| 1. Performs intrusion analysis | Advanced | | | Investigate | | Digital Forensics | |
| 1. Sets containment blockers to align with company policy regarding computer use and web access | Intermediate | | | Protect and Defend | | Computer network Defense Analysis | |
|  |  | | | | |  | | |
| JOB FUNCTION 8: Responds to cyber intrusions and **attacks and provides defensive strategies** | Core or Optional | | | | | Level | | |
| Competencies | Level | | | NICE Framework Category | | NICE Framework Specialty Area | |
| 1. Assists in the development of appropriate courses of action in response to identified anomalous network activity | Advanced | | | Protect and Defend | | Computer network Defense Analysis | |
| 1. Triages systems operations impact: malware, worms, man-in-the-middle attack, denial of service, rootkits, keystroke loggers, SQL injection and cross-site scripting | Advanced | | | Protect and Defend | | Computer network Defense Analysis | |
| 1. Reconstructs a malicious attack or activity based on network traffic | Advanced | | | Protect and Defend | | Computer network Defense Analysis | |
| 1. Correlates incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation | Advanced | | | Protect and Defend | | Incident Response | |
| 1. 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 | Advanced | | | Protect and Defend | | Incident Response | |
| 1. Performs analysis of log files from a variety of sources to identify threats to network security; performs file signature analysis | Advanced | | | Protect and Defend | | Incident Response | |
| 1. 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 | Advanced | | | Protect and Defend | | Incident Response | |
| 1. Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | Advanced | | | Protect and Defend | | Incident Response | |
| 1. Tracks and documents computer network defense incidents from initial detection through final resolution | Intermediate | | | Protect and Defend | | Incident Response | |
| 1. Collects intrusion artifacts and uses discovered data to enable mitigation of potential computer network defense (CND) incidents | Advanced | | | Protect and Defend | | Incident Response | |
| 1. Competency 8k: Performs virus scanning on digital media | Basic | | | Investigate | | Digital forensics | |

## Related Technical Instruction Plan

|  |  |
| --- | --- |
| COURSE NAME | Course Number |
| Hours |
| LEARNING OBJECTIVES | |
|  | |
| COURSE NAME | Course Number |
| Hours |
| LEARNING OBJECTIVES | |
|  | |
| COURSE NAME | Course Number |
| Hours |
| LEARNING OBJECTIVES | |
|  | |
| COURSE NAME | Course Number |
| Hours |
| LEARNING OBJECTIVES | |
|  | |
| COURSE NAME | Course Number |
| Hours |
| LEARNING OBJECTIVES | |
|  | |