Appendix A

CYBER SECURITY SPECIALIST

WORK PROCESS SCHEDULE AND

RELATED INSTRUCTION OUTLINE

Appendix A

WORK PROCESS SCHEDULE
CYBER SECURITY SPECIALIST

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.

1. APPRENTICESHIP APPROACH

☐ Time-based ☒ Competency-based ☐ Hybrid

2. TERM OF APPRENTICESHIP

The term of **Cybersecurity Specialist** is **Competency Based** supplemented by the minimum required 144 hours of related instruction per year.

3. RATIO OF APPRENTICES TO JOURNEYWORKERS

The apprentice to journeyworker ratio is: **1** Apprentice(s) to **1** Journeyworker(s).

4. 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: $**35.00**/per hour.

Period	Wage (Hourly)	Description
1	16.00	6 months + hours
2	16.50	6 months + hours
3	17.00	6 months + hours
4	17.50	6 months + hours

5. PROBATIONARY PERIOD

Applicants selected for apprenticeship will serve a probationary period of **1000** Hours.

6. SELECTION PROCEDURES

Applicants will be selected by individual participating employer sponsors using selection method #4_, as outlined in the California Code of Regulations, Title 8, Chapter 2, Part 1, Section 215, Chapter 6, from a pool of eligible created during the established recruiting process in accordance with the State and Federal Equal Opportunity regulations.

1. Minimum age of all applicants shall be 16 years. There is no maximum age;
2. Educational prerequisite for entry: High school diploma or GED/equivalent;
3. Physical prerequisites: Applicant must have the ability to safely perform the work of the trade/occupation. Physical examination required for entry is at no cost to the applicant and the physical exam will be defined by the individual employersponsor.
4. Written Test: Administered by Faculty and/or Program Coordinator
5. Oral Interview: None Required
6. All applicants will be notified in writing of Acceptance or Rejection.
7. If rejected, reasons for rejections will be stated.
8. A pool of applicants will be established and maintained for two years as follows:
   a. Interested applicants will have an opportunity to attend a publicorientation and enroll in the program’s employment preparation course. Completers of the course will be guided through the development of a resume and job application, which will be published to participating employer partners.
9. And applicants will be employed as follows:
   a. Applicants will follow directives of individual employer partners throughjob application, interview and pre-screening.
   b. Applicant's prior work experience and training will be evaluated by the committee at the time of registration, and appropriate credit will be given toward a higher apprenticeship and/or wage bracket. Apprentice applicant must verify, in writing, all past experience/education for consideration of credit.
   c. Each participating employer sponsor, upon determination of the need to employ and train an apprentice, will register an apprentice after upholding a fair and consistent sourcing, recruiting, and evaluation process;
   d. Participating employer sponsors will report recruitment and selection data annually to the Program Name Apprenticeship Training Program coordinator/director;
   e. Minimum age of all applicants shall be 16 years. There is no maximum age;
   f. Educational prerequisite for entry: High school diploma or GED/equivalent;
   g. Physical prerequisites: Applicant must have the ability to safely performthe work of the trade/occupation. Physical examination required for entry is at no cost to the applicant and the physical exam will be defined by the individual employer sponsor.
   h. Drug screening prior to employment, as well as random drug screening throughout the apprenticeship program may be required for selection and/or continued participation/employment;
   i. General aptitude or other skills test shall be defined by the individual employer sponsor and administered by the employer sponsor or its delegated agent;
   j. Oral interview is per employer sponsor’s individual selection procedures with selection documentation to be on file with the Program Name program director/coordinator.

WORK PROCESS SCHEDULE
CYBER SECURITY SPECIALIST

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

On-the-Job Learning Outline

Provides technical support to users or customers. Installs, configures, tests, operates, maintains and manages networks and their firewalls including hardware and software that permit sharing and transmission of information.		
Competencies	Date Completed	Initial
A. Manages inventory of IT resources		
B. Diagnoses and resolves customer-reported system incidents		
C. Installs and configures hardware, software, and peripheral equipment for system users		
D. Monitors client-level computer system performance		
E. Tests computer system performance		
F. Troubleshoots system hardware and software		
G. Administers accounts, network rights, and access to systems and equipment		
H. Implements security measures for uses in system and ensures that system designs incorporate security configuration guidelines		
I. Collaborates with system developers and users to assist in the selection of appropriate design solutions to ensure the compatibility of system components		
J. Installs, replaces, configures, and optimizes network hubs, routers and switches		
K. Assists in network backup and recovery procedures		
L. Diagnoses network connectivity problems		
M. Modifies network infrastructure to serve new purposes or improve workflow		
N. Integrates new systems into existing network architecture		
O. Patches network vulnerabilities to ensure information is safeguarded against outside parties		
P. Repairs network connectivity problems		
Q. Tests and maintains network infrastructure including software and hardware devices		
R. Establishes adequate access controls based on principles of least privilege and need-to-know		
S. Implements security measures for users in system and ensures that system designs incorporate security configuration guidelines		

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. Configures tools and technologies to detect, mitigate and prevent potential threats.		
Competencies	Date Completed	Initial
A. Collaborates with system developers and users to assist in the selection of appropriate design solutions to ensure the compatibility of system components		
B. Installs, replaces, configures, and optimizes network hubs, routers, and switches		
C. Assists in network backup and recovery procedures		
D. Diagnoses network connectivity problems		
E. Modifies network infrastructure to serve new purposes or improve workflow		
F. Integrates new systems into existing network architecture		
G. Patches network vulnerabilities to ensure information is safeguarded against outside parties		
H. Repairs network connectivity problems		

I. Tests and maintains network infrastructure including software and hardware devices		
J. Establishes adequate access controls based on principles of least privilege and need-to-know		
K. Implements security measures for users in system and ensures that system designs incorporate security configuration guidelines		
L. Installs and maintains cyber security detection, monitoring and threat management software		
M. Coordinates with network administrators to administer the updating of rules and signatures for intrusion/detection protection systems, anti-virus, and network black- and whitelist		
N. Manages IP addresses based on current threat environment		
O. Ensures application of security patches for commercial products integrated into system design		
P. Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity		

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. Responds to cyber intrusions and attacks and provides defensive strategies.		
Competencies	Date Completed	Initial
A. Checks system hardware availability, functionality, integrity, and efficiency		
B. Conducts functional and connectivity testing to ensure continuing operability		
C. Conducts periodic server maintenance including cleaning (physically and electronically), disk checks, system configuration and monitoring, data downloads, backups, and testing		
D. Assists in the development of group policies and access control lists to ensure compatibility with organizational standards, business rules and needs		
E. Documents compliance with or changes to system administration standard operating procedures		
F. Installs server fixes, updates, and enhancements		
G. Maintains baseline system security according to organizational policies		
H. Manages accounts, network rights and access to systems and equipment		
I. Monitors and maintains server configuration		
J. Supports network components		
K. Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs		
L. Verifies data redundancy and system recovery procedures		
M. Assists in the coordination or installation of new or modified hardware, operating systems, and another baseline software		
N. Provides ongoing optimization and problem- solving support		
O. Resolves hardware/software interface and interoperability problems		
P. Establishes adequate access controls based on principles of least privilege, role-based access controls (RBAC) and need-to-know		

Responds to cyber intrusions and attacks and provides defensive strategies. Reviews network utilization data to identify unusual patterns, suspicious activity or signs of potential threats		
Competencies	**Date Completed**	**Initial**
A. Assists in the development of appropriate courses of action in response to identified anomalous network activity		
B. Triages systems operations impact: malware, worms, man-in-the-middle attack, denial of service, rootkits, keystroke loggers, SQL injection and cross-site scripting		
C. Reconstructs a malicious attack or activity based on network traffic		
D. Correlates incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation		
E. 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		
F. Performs analysis of log files from a variety of sources to identify threats to network security; performs file signature analysis		
G. 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		
H. Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts		
I. Tracks and documents computer network defense incidents from initial detection through final resolution		
J. Collects intrusion artifacts and uses discovered data to enable mitigation of potential computer network defense (CND) incidents		
K. Performs virus scanning on digital media		
L. Characterizes and analyzes network traffic to identify anomalous activity and potential threats; performs computer network defense trend analysis and reporting		
M. Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts		
N. Runs tests to detect real or potential threats, viruses, malware, etc.		
O. Helps perform damage assessments in the event of an attack		
P. Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities		
Q. Provides timely detection, identification and alerts of possible attacks and intrusions, anomalous activities, and distinguish these incidents and events from normal baseline activities		
R. Uses network monitoring tools to capture and analyze network traffic associated with malicious activity		
S. Performs intrusion analysis		
T. Sets containment blockers to align with company policy regarding computer use and web access		

RELATED INSTRUCTION OUTLINE

CYBER SECURITY SPECIALIST

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

Through consultation with the Apprenticeship Committee and the indenturing employer, apprentices will select an applicable program of study/course track and complete a minimum of 144 hours of related instruction per year of apprenticeship. Courses will be approved by the Apprenticeship Committee and made available to applicable apprentices by approved education providers/institutions. Apprentices will enroll in, and complete, the required coursework that satisfies the minimum requirements of the program. Prior applicable education and training will be credited towards completion of related education requirements and apprentices will be offered tracks advancing their technical aptitude in the profession.

Source: Moreno Valley College

The following related training outline identifies the courses that are currently identified as suggested course work for this occupation:

Advanced Security Concepts and Practices – 72 hours
Computer Forensics Fundamentals – 72 hours
Fundamentals: Information Systems Security Auditing – 54 hours
Healthcare Information Security & Privacy for Practitioner – 80 hours
Information and Communication Technology Essentials – 54 hours
Information and Network Security – 54 hours
Introduction to Cybersecurity: Ethical Hacking – 72 hours
Introduction to Computer Information Systems – 72 hours
Introduction to Python Programming – 75 hours
Principles of Cybersecurity Analysis – 80 hours
Systems and Network – 48 hours
Administration – 80 hours

Optional Supplemental Instruction

Calculus I – 90 hours
Cisco Networking Academy 1A – 72 hours
Computer Networking Fundamentals – 80 hours
Introduction to Programming Concepts and Methodology I: C++ – 72 hours

This workforce product was funded by a $4,697,637 grant awarded to Riverside Community College District by the U.S. Department of Labor (DOL) – Apprenticeship Building America (ABA) Grant. The total cost of the product is financed with 100% Federal funds. The product was created by the recipient and does not necessarily reflect the official position of DOL-ETA. DOL-ETA makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability, or ownership. This product is copyrighted by the institution that created it.