Appendix A -1

WORK PROCESS SCHEDULES

AND

RELATED INSTRUCTION OUTLINE

Nevada Help Desk

CyberSecurity Support Technician

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

APPROVED BY
THE NEVADA LABOR COMMISSIONER AND THE NEVADA STATE APPRENTICESHIP COUNCIL

Richard J. Williams, Nevada State Apprenticeship Director

REGISTRATION DATE: Pending

RAPIDS PROGRAM ID NUMBER: Pending

DEVELOPED IN COOPERATION WITH THE
THE NEVADA LABOR COMMISSIONER, THE NEVADA STATE APPRENTICESHIP COUNCIL AND THE U.S. DEPARTMENT OF LABOR

Appendix A-1

WORK PROCESS SCHEDULE

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

1. TYPE OF OCCUPATION

☒Competency-based

2. TERM OF APPRENTICESHIP

The term of the occupation shall be defined by the attainment of all competencies of the position, which would be expected to occur within approximately 2,000 hours (must be at least 2,000 hours) of OJL, supplemented by the minimum of 190 hours and 38 minutes of related instruction per year of the apprenticeship.

3. RATIO OF APPRENTICES TO JOURNEYWORKERS

The apprentice to journey worker/fully trained worker ratio is: 1 apprentice to 1 journey worker/fully trained worker.

4. APPRENTICE WAGE SCHEDULE

An apprentice minimum starting wage will be at least $25.00 per hour. Apprentices shall be paid a progressively increasing schedule of wages based on either a percentage or a dollar amount of the current hourly journey worker/fully trained worker wage.

1-Year Term Example:

1st 6 months = $25.00 2nd 6 months = $27.50

A journey worker/fully trained worker minimum wage will be at least $30.00

Periodic review and evaluation of the apprentice's on-the-job learning and related technical instruction will be conducted in alignment with the wage schedule established.

5. WORK PROCESS SCHEDULE (See attached Work Process Schedule)

The sponsor may modify the work processes to meet local needs prior to submitting these Standards to the appropriate Registration Agency for approval.

6. RELATED INSTRUCTION OUTLINE (See attached Related Instruction Outline)

The sponsor may modify the related instruction to meet local needs prior to submitting these Standards to the appropriate Registration Agency for approval.

Appendix A-1

Apprenticeship Competencies – Technical

The following is the rating system 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

On-the-Job Learning Outline

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
A. 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
B. 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
C. 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
D. 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
E. **Assigns individuals to the appropriate permission or access level to control access to certain web IP addresses, information and the ability to**	Advanced	Securely Provision	Information Assurance Compliance

download programs and transfer data to various locations			
F. **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
G. **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
H. **Complies with incident response and handling methodologies**	Advanced	Protect and Defend	Computer Network Defense Analysis
I. **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
A. Manages inventory of IT resources	Basic	Operate/ Maintain	Customer Service and Technical Support
B. Diagnoses and resolves customer-reported system incidents	Intermediate	Investigate	Digital forensics
C. Installs and configures hardware, software and peripheral equipment for system users	Basic	Operate/ Maintain	Customer Service and Technical Support
D. Monitors client-level computer system performance	Basic	Operate/ Maintain	Customer Service and Technical Support
E. Tests computer system performance	Basic	Operate/ Maintain	Customer Service and Technical Support

F. Troubleshoots system hardware and software	Basic	Operate/ Maintain	Customer Service and Technical Support
G. Administers accounts, network rights, and access to systems and equipment	Intermediate	Operate/ Maintain	Customer Service and Technical Support
H. 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
A. 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
B. Installs, replaces, configures and optimizes network hubs, routers and switches	Advanced	Operate and Maintain	Network Services
C. Assists in network backup and recovery procedures	Intermediate	Operate and Maintain	Network Services
D. Diagnoses network connectivity problems	Basic	Operate and Maintain	Network Services
E. Modifies network infrastructure to serve new purposes or improve workflow	Advanced	Operate and Maintain	Network Services
F. Integrates new systems into existing network architecture	Intermediate	Operate and Maintain	Network Services

G. Patches network vulnerabilities to ensure information is safeguarded against outside parties	Intermediate	Operate and Maintain	Network Services
H. Repairs network connectivity problems	Basic	Operate and Maintain	Network Services
I. Tests and maintains network infrastructure including software and hardware devices	Basic	Operate and Maintain	Network Services
J. Establishes adequate access controls based on principles of least privilege and need-to-know	Intermediate	Operate and Maintain	Network Services
K. 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
A. Checks system hardware availability, functionality, integrity and efficiency	Intermediate	Operate and Maintain	System Admin
B. Conducts functional and connectivity testing to ensure continuing operability	Basic	Operate and Maintain	System Admin
C. Conducts periodic server maintenance including cleaning (physically and electronically), disk checks, system configuration	Basic	Operate and Maintain	System Admin

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	Advanced	Operate and Maintain	System Admin
E. **Documents compliance with or changes to system administration standard operating procedures**	Intermediate	Operate and Maintain	System Admin
F. **Installs server fixes, updates and enhancements**	Intermediate	Operate and Maintain	System Admin
G. **Maintains baseline system security according to organizational policies**	Intermediate	Operate and Maintain	System Admin
H. **Manages accounts, network rights and access to systems and equipment**	Basic	Operate and Maintain	System Admin
I. **Monitors and maintains server configuration**	Intermediate	Operate and Maintain	System Admin
J. **Supports network components**	Basic	Operate and Maintain	System Admin
K. **Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs**	Basic	Operate and Maintain	System Admin
L. **Verifies data redundancy and system recovery procedures**	Intermediate	Operate and Maintain	System Admin
M. **Assists in the coordination or installation of new or modified hardware, operating systems and other baseline software**	Intermediate	Operate and Maintain	System Admin
N. **Provides ongoing optimization and problem-solving support**	Intermediate	Operate and Maintain	System Admin

O. **Resolves hardware/software interface and interoperability problems**	Basic	Operate and Maintain	System Admin
P. **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
A. Installs and maintains cyber security detection, monitoring and threat management software	Intermediate		
B. 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		
C. Manages IP addresses based on current threat environment	Intermediate		
D. Ensures application of security patches for commercial products integrated into system design	Basic		
E. 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	Core or Optional	Level

vulnerabilities			
Competencies	Level	NICE Framework Category	NICE Framework Specialty Area
A. Applies security policies to meet security objectives of the system	Intermediate	Operate and Maintain	Systems Security Analysis
B. Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices	Intermediate	Operate and Maintain	Systems Security Analysis
C. 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
D. Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization	Advanced	Operate and Maintain	Systems Security Analysis
E. Installs, manages and updates intrusion detection system	Advanced	Operate and Maintain	Systems Security Analysis
F. Performs technical and non-technical risk and vulnerability assessments of relevant technology focus areas	Advanced	Protect and Defend	Vulnerability Assessment & Management
G. Conducts authorized penetration testing (Wi-Fi, network perimeter, application security, cloud, mobile devices) and assesses results	Intermediate	Protect and Defend	Vulnerability Assessment & Management
H. Documents systems security operations and maintenance activities	Intermediate	Operate and Maintain	Systems Security Analysis
I. Communicates potential risks or vulnerabilities to manager. Collaborates with others to	Advanced	Protect and Defend	Computer Network Defense and Analysis

recommend vulnerability corrections			
J. 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
A. Identifies organizational trends with regard to the security posture of systems; identifies unusual patterns or activities	Basic	Operate and Maintain	Systems Security Analysis
B. 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
C. 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
D. Runs tests to detect real or potential threats, viruses, malware, etc.	Advanced		
E. Assists in researching cost-effective security controls to mitigate risks	Intermediate	Protect and Defend	Vulnerability Assessment and Management
F. Helps perform damage assessments in the event of an attack	Advanced		

G. Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities	Advanced	Operate and Maintain	Systems Security Analysis
H. Documents and escalates incidents that may cause immediate or long-term impact to the environment	Intermediate	Protect and Defend	Computer network Defense Analysis
I. 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
J. Uses network monitoring tools to capture and analyze network traffic associated with malicious activity	Advanced	Investigate	Digital Forensics
K. Performs intrusion analysis	Advanced	Investigate	Digital Forensics
L. 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
A. Assists in the development of appropriate courses of action in response to identified anomalous network activity	Advanced	Protect and Defend	Computer network Defense Analysis
B. Triages systems operations impact: malware, worms, man-in-	Advanced	Protect and Defend	Computer network Defense

the-middle attack, denial of service, rootkits, keystroke loggers, SQL injection and cross-site scripting			Analysis
C. Reconstructs a malicious attack or activity based on network traffic	Advanced	Protect and Defend	Computer network Defense Analysis
D. Correlates incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation	Advanced	Protect and Defend	Incident Response
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	Advanced	Protect and Defend	Incident Response
F. 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
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	Advanced	Protect and Defend	Incident Response
H. Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts	Advanced	Protect and Defend	Incident Response
I. Tracks and documents computer network defense incidents from initial detection through final resolution	Intermediate	Protect and Defend	Incident Response

J. Collects intrusion artifacts and uses discovered data to enable mitigation of potential computer network defense (CND) incidents	Advanced	Protect and Defend	Incident Response
K. Performs virus scanning on digital media	Basic	Investigate	Digital forensics

RELATED INSTRUCTION OUTLINE
IT GENERALIST
O*NET-SOC CODE: 15-1232.00 RAPIDS CODE: 2018CB

This RI gives guidance, knowledge, and proficiency in the core skills necessary for a career as a IT Generalist. The related instruction has been developed in cooperation with employer-partners as part of the apprenticeship. Method of Delivery: in-house training, classroom, and/or online. Source of Instruction: any combination of community college, private industry training provider, sponsoring employer, or computer-based training. Note: These are National Guideline Standards. Course titles and classes may differ slightly depending upon the RTI provider. The following is a set of courses to be delivered by subject matter experts. Related Technical Instruction (RTI) - This instruction shall include, but not be limited to, at least 180 hours per year for each year of the apprenticeship. The related theoretical education listed below is tightly integrated with real work experiences. The curriculum is defined as a variety of classes, around which the exams and projects are based. By defining the RTI this way, all competencies required of the students are met, through project work.

Core Courses, Virtual Labs, Practice Tests, Course Name, Approximate Hours RELATED

1.Fundamentals of Cybersecurity Architecture(C) (CMMC assessment)	3 hours 11 minutes
2.CIS Top 20 Critical Security Controls(C) (NIST800-171/DFAR)	9 hours 54 minutes
3.Malware Threats(C)	4 hours 17 minutes
4.Fundamentals of Risk Policies and Security Controls(C)	44 minutes
5.Fundamentals of Vulnerability Management(C))(Kali Linux scans)	10 hours 55 minutes
6.Perform a Network Vulnerability Assessment Using Nmap(L))(scans)	1 hour
7.Identify Non-secure Network Traffic(L) (Wireshark)	45 minutes
8.Application of the MITRE ATT&CK Framework(C)	8 hours 28 minutes
9.Security Engineering(C) (CMMC assessment)	3 hours
10.Using Encryption to Secure Information(L) (CMMC assessment)	45 minutes
11.Intro to Cyber Threat Intelligence(C)	4 hours 30 minutes
12.Identify Attack Types/Surfaces(L) (CMMC assessment)	45 minutes
13.Threat Designation(L)	1 hour
14.Incident Response Planning(C) (CMMC assessment)	55 minutes
15.Incident Response Lifecycle(C) (CMMC assessment)	5 hours 19 minutes
16.Intro to Malware Analysis and Reverse Engineering(C)	9 hours 30 minutes
17.Everyday Digital Forensics(C) (Kali Linux OpenVas)	4 hours
18.Creating a Baseline Using the Windows Forensic Toolchest(L)	45 minutes
19.Computer Hacking and Forensics(C)	17 hours 45 minutes
20.Memory Extraction and Analysis(L)	3 hours 40 minutes
21. Scoping requirements (L) (CMMC assessment)	1 hour
22.Evidence Handling: Do it the Right Way(C) (CMMC assessment)	45 minutes
23.Intro to Cloud Based Sec	7 hours 30 minutes
24.Certificate of Cloud Security Knowledge (CCSK)(C)	10 hours
25 Plans Policy development (CMMC assessment)	40 hours
26. Preassessment Readiness Review procedures training	40 hours
Total RI Hours:	**190 hours 38 minutes**

In addition, and to meet the recommended minimum 190 hours and 38 minutes per year,

Employers may select from the following modules as needed:

1. Teamwork and Collaboration 8
2. Communication 10
3. Problem Solving 5
4. Critical Thinking 3
5. Conflict Management 3
6. Time Management 5
7. Customer Service 3

TOTAL: 37

Course Descriptions

Certified Ethical Hacker (CEH)
A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.
The purpose of the CEH credential is to:

- Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.
- Inform the public that credentialed individuals meet or exceed the minimum standards.
- Reinforce ethical hacking as a unique and self-regulating profession.

Global Information Assurance Certification (GIAC) Certified Incident Handler (GCIH)
The GIAC Incident Handler certification validates a practitioner's ability to detect, respond, and resolve computer security incidents using a wide range of essential security skills. GCIH certification holders have the knowledge needed to manage security incidents by understanding common attack techniques, vectors and tools, as well as defend against and respond to such attacks when they occur.
Areas Covered

- Incident Handling and Computer Crime Investigation
- Computer and Network Hacker Exploits
- Hacker Tools (Nmap, Nessus, Metasploit and Netcat)
- Exam Certification Objectives & Outcome Statements

The topic areas for each exam part follow:

Covering Tracks on Hosts

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against methods attackers use to remove evidence of compromise on hosts.

Covering Tracks on the Network

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against methods attackers use to remove evidence of compromise on the network.

Domain Attacks

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against Domain attacks in Windows environments.

Drive-By Attacks

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against drive-by attacks in modern environments.

Endpoint Attacks and Pivoting

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against attacks against endpoints and attack pivoting.

Incident Handling and Digital Investigations

- The candidate will demonstrate an understanding of what Incident Handling is, why it is important, an understanding of the PICERL incident handling process, and industry best practices in Incident Handling and Digital Investigations.

Memory and Malware Investigations

- The candidate will demonstrate an understanding of the steps necessary to perform basic memory forensics, including collection and analysis of processes and network connections and basic malware analysis.

Metasploit

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against the use of Metasploit.

Netcat

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against the use of covert tools such as netcat.

Network Investigations

- The candidate will demonstrate an understanding of the steps necessary to perform effective digital investigations of network data.

Password Attacks

- The candidate will demonstrate a detailed understanding of the three methods of password cracking.

Physical Access Attacks

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against physical access attacks.

Reconnaissance and Open-Source Intelligence

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate public and open source reconnaissance techniques.

Scanning and Mapping

- The candidate will demonstrate an understanding the fundamentals of how to identify, defend against, and mitigate against scanning; to discover and map networks and hosts, and reveal services and vulnerabilities.

SMB Scanning

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate reconnaissance and scanning of SMB services.

Web App Attacks

- The candidate will demonstrate an understanding of how to identify, defend against, and mitigate against Web Application Attacks.

CompTIA Cybersecurity Analyst (CySA)

CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity threats through continuous security monitoring.

It will validate an IT professional's ability to proactively defend and continuously improve the security of an organization. CySA+ will verify the successful candidate has the knowledge and skills required to:

- Leverage intelligence and threat detection techniques
- Analyze and interpret data
- Identify and address vulnerabilities
- Suggest preventative measures
- Effectively respond to and recover from incidents

CompTIA CySA+ meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA).

SELECTION PROCEDURES

The sponsor has adopted the following selection procedures, consistent with the requirements set forth in 29 CFR § 30.10(b):

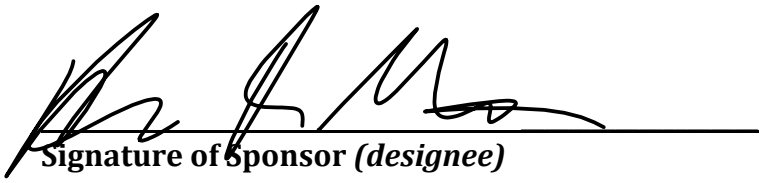
The sponsor will recruit from (but not limited to) the following sources:

Incumbent workers
Colleges, Universities, Community Colleges, and Career and Technical Education Centers
One-Stop Centers, as established under the Workforce Investment Act, and reauthorized in the Workforce Innovation and Opportunities Act of 2014.

OFFICIAL ADOPTION OF APPRENTICESHIP STANDARDS

Nevada Help Desk hereby adopts these standards of apprenticeship.

Sponsor(s) designate the appropriate person(s) to sign the standards on their behalf.



Signature of Sponsor *(designee)* **Date:** 8/26/21

Duana Malone, Executive Director
Type Name & Title