Cybersecurity
Program of Study with
Complementary Course Standards

This document was prepared by:

Office of Career Readiness, Adult Learning, and Education Options
Nevada Department of Education
755 N. Roop Street, Suite 201
Carson City, NV 89701

www.doe.nv.gov

Draft for Review by the Nevada State Board of Education on
November 6, 2024

This page will be removed for posting

Nevada State Board of Education

Dr. René Cantú
Maggie Carlton
Dr. Katherine Dockweiler, Vice President
Tate Else
Stephanie Goodman
Tamara Hudson
Tim Hughes
Michael Keyes
Angela Orr
Felicia Ortiz, President
Mike Walker

Nevada Department of Education

Jhone M. Ebert
Superintendent of Public Instruction

Christy McGill
Deputy Superintendent for Educator Effectiveness and Family Engagement

Craig Statucki
Director for the Office of Career Readiness, Adult Learning, and Education Options

Anna Reynolds
Education Programs Supervisor, Office of Career Readiness, Adult Learning, and Education Options

Vision

All Nevada students are equipped and feel empowered to attain their vision of success

Mission

To improve student achievement and educator effectiveness by ensuring opportunities, facilitating learning, and promoting excellence

This page will be removed for posting

Table of Contents

This page will be removed for posting

Acknowledgements

The development of Nevada career and technical education (CTE) standards and assessments is a collaborative effort sponsored by the Nevada Department of Education (NDE) Office of Career Readiness, Adult Learning, and Education Options. The Nevada Department of Education relies on educators and industry representatives who have the technical expertise and teaching experience to develop standards and performance indicators that truly measure student skill attainment. More importantly, the NDE would like to recognize the time and commitment by the writing team members in developing the career and technical standards for Cybersecurity.

Standards Development Members

Name	Occupation/Title	Stakeholder Affiliation	School/Organization
Fran Bromley-Norwood	Administrator	District Administrator	Clark County School District
Frankie Clark	Instructor	Secondary Educator	North Valleys High School, Washoe County School District
Dustin Daniels	Instructor	Secondary Educator	Pinecrest Academy of Nevada, Cadence, State Public Charter School Authority
Lloyd Mann	Instructor	Secondary Educator	Shadow Ridge High School, Clark County School District
Daryl Pfeif	Founder and CEO	Business and Industry Representative	Digital Forensics Solutions, LLC, New Orleans, LA
Arthur Salmon	Instructor	Postsecondary Educator	College of Southern Nevada, Las Vegas
Margaret Taylor	Instructor	Postsecondary Educator	College of Southern Nevada, Las Vegas

Business and Industry Validation

All CTE standards developed through the Nevada Department of Education are validated by business and industry through one or more of the following processes: (1) the standards are developed by a team consisting of business and industry representatives, or (2) a separate review panel is coordinated with industry experts to ensure the standards include the proper content, or (3) nationally recognized standards currently endorsed by business and industry.

The Cybersecurity standards were validated through active participation of business and industry representatives on the development team.

This page will be removed for posting

Introduction

The standards in this document are designed to clearly state what the student should know and be able to do upon completion of a high school Cybersecurity program of study. These standards are designed for a two-credit course sequence that prepares the student for a technical assessment directly aligned to the standards.

These exit-level standards are designed for the student to complete all standards through their completion of a program of study. These standards are intended to guide curriculum objectives for a program of study.

The standards are organized as follows:

- **Content Standards** are general statements that identify major areas of knowledge, understanding, and the skills students are expected to learn in key subject and career areas by the end of the program.
- **Performance Standards** follow each content standard. Performance standards identify the more specific components of each content standard and define the expected abilities of students within each content standard.
- **Performance Indicators** are very specific criteria statements for determining whether a student meets the performance standard. Performance indicators may also be used as learning outcomes, which teachers can identify as they plan their program learning objectives. The indicators are followed by designations that reflect the course sequence (e.g., L1 for the first-year course of a two-year program and L2 for the second-year course, C is to designate the indicators to be taught in the complementary courses) as referenced in the Core Course Sequence table.

The crosswalks and alignments are located in the Program Supplemental Program Resources document. These will show where the performance indicators support the Nevada Academic Content Standards. For individual course descriptions, please reference the Supplemental Program Resource or the Nevada CTE Catalog.

All students are encouraged to participate in the career and technical student organization (CTSO) that relates to the Cybersecurity program. CTSOs are co-curricular national organizations that directly reinforce learning in the CTE classroom through curriculum resources, competitive events, and leadership development. CTSOs provide students the ability to apply academic and technical knowledge, develop communication and teamwork skills, and cultivate leadership skills to ensure college and career readiness.

The Employability Skills for Career Readiness identify the skills needed to be successful in all careers and must be taught as an integrated component of all CTE course sequences. These standards are available in a separate document.

The **Standards Reference Code** is only used to identify or align performance indicators listed in the standards to daily lesson plans, curriculum documents, or national standards. The Standards Reference Code is an abbreviated name for the program, and the content standard, performance standard and performance indicator are referenced in the program standards. This abbreviated code for identifying standards uses each of these items. For example, CYBR is the Standards Reference Code for Cybersecurity. For Content Standard 2, Performance Standard 3 and Performance Indicator 4 the Standards Reference Code would be CYBR.2.3.4.

Cybersecurity

Program Information

Program of Study: **Cybersecurity**
Standards Reference Code: **CYBR**
Career Cluster: **Information Technology**
Career Pathway(s): **Network Systems**
Program Length: **2-year, completed sequentially**
CTSO: **FBLA/SkillsUSA**

Program Structure Required Program of Study Courses

The core course sequencing is provided in the following table. Complementary Courses are available and provided later in this document. The following courses provide a completed program of study. The Lab is a complementary course available concurrently with the Cybersecurity II course.

Core Course Sequence (R) with Lab Course(s) (C)

Required/ Complementary	Course Title	Abbreviated Name
R	Cybersecurity I	CYBRSECU I
R	Cybersecurity II	CYBRSECU II
C	Cybersecurity II LAB	CYBRSECU II L

CONTENT STANDARD 1.0: INTEGRATE CAREER AND TECHNICAL STUDENT ORGANIZATIONS (CTSOs)

Performance Standard 1.1: Explore the History and Organization of CTSOs

1.1.1 Discuss the requirements of CTSO participation/involvement as described in Carl D. Perkins Law (Level 1 (L1), Level 2 (L2), Complementary (C))

1.1.2 Research nationally recognized CTSOs (L1, L2, C)

1.1.3 Investigate the impact of federal and state government regarding the progression and operation of CTSOs (e.g., Federal Statutes and Regulations, Nevada Administrative Code [NAC], Nevada Revised Statutes [NRS]) (L1, L2, C)

Performance Standard 1.2: Develop Leadership Skills

1.2.1 Discuss the purpose of parliamentary procedure (L1, L2, C)

1.2.2 Demonstrate the proper use of parliamentary procedure (L1, L2, C)

1.2.3 Differentiate between an office and a committee (L1, L2, C)

1.2.4 Discuss the importance of participation in local, regional, state, and national conferences, events, and competitions (L1, L2, C)

1.2.5 Participate in local, regional, state, or national conferences, events, or competitions (L1, L2, C)

1.2.6 Describe the importance of a constitution and bylaws to the operation of a CTSO chapter (L1, L2, C)

Performance Standard 1.3: Participate in Community Service

1.3.1 Explore opportunities in community service-related work-based learning (WBL) (L1, L2, C)

1.3.2 Participate in a service learning (program related) and/or community service project or activity (L1, L2, C)

1.3.3 Engage with business and industry partners for community service (L1, L2, C)

Performance Standard 1.4: Develop Professional and Career Skills

1.4.1 Demonstrate college and career readiness (e.g., applications, resumes, interview skills, presentation skills) (L1, L2, C)

1.4.2 Describe the appropriate professional/workplace attire and its importance (L1, L2, C)

1.4.3 Investigate industry-standard credentials/certifications available within this Career Cluster™ (L1, L2, C)

1.4.4 Participate in authentic contextualized instructional activities (L1, L2, C)

1.4.5 Demonstrate technical skills in various student organization activities/events (L1, L2, C)

Performance Standard 1.5: Understand the Relevance of Career and Technical Education (CTE)

1.5.1 Make a connection between program standards to career pathway(s) (L1, L2, C)

1.5.2 Explain the importance of participation and completion of a program of study (L1, L2, C)

1.5.3 Promote community awareness of local student organizations associated with CTE programs (L1, L2, C)

CONTENT STANDARD 2.0: SAFETY PROCEDURES AND PROPER USE OF TOOLS

Performance Standard 2.1: Demonstrate Proper Safety Procedures

2.1.1 Demonstrate the proper use of safety devices based on industry regulations (L1)

2.1.2 Research the environmental impact of production based on industry standards (L1)

2.1.3 Research local, state, federal, and international regulations related to material handling (L1)

2.1.4 Demonstrate secure disposal of technology materials and data (L1)

2.1.5 Introduce Material Safety Data Sheets (MSDS) (L1)

2.1.6 Explain the relationship between organization and safety (L1)

2.1.7 Demonstrate an organized work environment (L1)

2.1.8 Demonstrate electrical safety (e.g., grounding, ESD [static]) (L1)

2.1.9 Apply installation safety (e.g., lifting, overhead movements) (L1)

2.1.10 Analyze emergency procedures (building layout, fire escape plan, safety/emergency exits, fail open/close, alert systems, natural disasters) (L1)

Performance Standard 2.2: Identify, Categorize, and Employ Industry Standard Tools

2.2.1 Explain common tools used in computer repair (L1)

2.2.2 Demonstrate the use of common networking and repair tools (L1)

2.2.3 Select the proper tool for diagnostic and troubleshooting procedures (L1)

2.2.4 Discuss fire suppression systems, the purpose of Heating, Ventilation, and Air Conditioning (HVAC) systems, and industry standards when dealing with the loss of power (L1)

CONTENT STANDARD 3.0: UNDERSTAND TECHNICAL, LEGAL, AND ETHICAL ISSUES

Performance Standard 3.1: Analyze Legal and Ethical Issues Related to Technology

- 3.1.1 Analyze legal issues in technology (L1)
- 3.1.2 Evaluate intellectual property laws (L1)
- 3.1.3 Explain differences between licensing, copyright, and infringement (L1)
- 3.1.4 Explain the differences between restricted content, prohibited or illegal content (L1)
- 3.1.5 Examine state, federal, and international regulations related to technology (e.g., legal holds, disposal methods, data retention, discoverability, data protection) (L1)

Performance Standard 3.2: Evaluate Privacy Issues Related to Technology

- 3.2.1 Analyze acceptable use policies (L1)
- 3.2.2 Explain the difference between technology policies, privacy standards, and best practices (L1)
- 3.2.3 Explain data and privacy encryption issues related to using technology (L1)
- 3.2.4 Evaluate appropriate consent policies to monitoring various stakeholders (L1)
- 3.2.5 Explain appropriate data classification (L1)

Performance Standard 3.3: Describe the Importance of Customer Relations

- 3.3.1 Communicate with customers to ensure understanding of customer requirements, scope, and concerns (L1)
- 3.3.2 Utilize appropriate documentation systems (L1)
- 3.3.3 Explain the purpose of business agreements (e.g., memos of understanding, service level agreement, statement of work, master services agreement) (L1)

CONTENT STANDARD 4.0: UNDERSTAND HARDWARE COMPONENTS

Performance Standard 4.1: Identify Basic Hardware Components

4.1.1 Categorize system unit components (e.g., power supply connectors, motherboard characteristics, form factors, Central Processing Unit (CPU) features, memory module attributes, and expansion business types) (L1)

4.1.2 Use industry standard vocabulary to identify components (L1)

Performance Standard 4.2: Install and Configure Motherboard

4.2.1 Select and install appropriate system unit components to meet customer specifications (L1)

4.2.2 Interpret BIOS/UEFI settings for basic hardware components (L1)

4.2.3 Configure the settings of basic hardware components (L1)

4.2.4 Troubleshoot basic hardware components and resolve issues (L1)

Performance Standard 4.3: Install and Configure Audio and Video Components

4.3.1 Categorize audio and video device components, connectors, and cables (L1)

4.3.2 Install appropriate sound and video cards to match specifications and end-user requirements (L1)

4.3.3 Configure display and video settings (L1)

4.3.4 Manage sound card and audio device settings (L1)

Performance Standard 4.4: Install and Configure Storage and Other External Devices

4.4.1 Identify external device components, connectors, and cables (L1)

4.4.2 Connect external devices using the appropriate connectors and cables (L1)

4.4.3 Manage device driver updates and roll back drivers (L1)

4.4.4 Enable or disable devices (L1)

4.4.5 Install drivers for external devices (L1)

4.4.6 Prepare devices for safe removal (L1)

4.4.7 Manipulate system utilities to configure storage and external devices (L1)

Performance Standard 4.5: Install and Maintain Printers

4.5.1 Install small office/home office network (SOHO) multifunction device/printers and configure appropriate settings (L1)

4.5.2 Compare and contrast differences between the various print technologies and the associated imaging process (L1)

4.5.3 Perform appropriate printer maintenance (L1)

CONTENT STANDARD 5.0: UNDERSTAND OPERATING SYSTEMS

Performance Standard 5.1: Evaluate, Install, and Secure Operating Systems

- 5.1.1 Use industry standard vocabulary in relation to operating systems (OS) (L1, L2)
- 5.1.2 Compare and contrast (L1, L2)
- 5.1.3 Install and secure operating systems (L1, L2)
- 5.1.4 Install and configure Windows networking (L1, L2)

Performance Standard 5.2: Employ and Configure Windows Tools

- 5.2.1 Explain various features and tools of operating systems (L1, L2)
- 5.2.2 Apply appropriate command line tools (L1, L2)
- 5.2.3 Select appropriate operating system features and tools based on customer requirements (L1, L2)
- 5.2.4 Configure Windows Update settings (L1, L2)
- 5.2.5 Configure local users and groups for a Windows networking system (L1, L2)
- 5.2.6 Configure User Access Control (UAC) (L1, L2)
- 5.2.7 Use Windows Control Panel utilities (L1, L2)
- 5.2.8 Perform common preventive maintenance procedures using the appropriate Windows OS tools (L1, L2)
- 5.2.9 Troubleshoot common PC security issues using best practices (L1, L2)

Performance Standard 5.3: Troubleshoot Common Windows Operating Systems and Software

- 5.3.1 Explain key terms and acronyms used in diagnostic testing and troubleshooting (L1, L2)
- 5.3.2 Identify common symptoms for a given discrepancy (L1, L2)
- 5.3.3 Develop a solution for a given discrepancy (L1, L2)
- 5.3.4 Document the solution (L1, L2)

Performance Standard 5.4: Analyze Other Operating Systems, Mobile, and IoT Devices

- 5.4.1 Identify common features and functionality of Mac OS, Chrome, and other Linux operating systems (L1, L2)
- 5.4.2 Set up and use client-side virtualization and introduce server virtualization topics (L1, L2)
- 5.4.3 Identify basic features of mobile operating systems (L1, L2)
- 5.4.4 Install and configure basic mobile device network connectivity and email (L1, L2)
- 5.4.5 Summarize methods and data related to mobile device synchronization (L1, L2)
- 5.4.6 Compare and contrast methods to secure mobile devices (L1, L2)
- 5.4.7 Explain the characteristics of various types of other mobile devices (L1)
- 5.4.8 Compare and contrast accessories, features, and ports of mobile and IoT devices (L1, L2)
- 5.4.9 Troubleshoot common mobile OS and tablet software/hardware issues (L1, L2)

Performance Standard 5.5: Compare Features of Laptops and Tablets

5.5.1 Compare and contrast laptops, tablets, and computer form factors (L1)

5.5.2 Explain current trends in laptops and tablet applications (L1)

5.5.3 Compare laptop and tablet operating systems (L1)

5.5.4 Explain the function of components within the display of a laptop and tablet (L1)

5.5.5 Compare and contrast accessories, features, and ports of laptops and tablets (L1)

Performance Standard 5.6: Understand Cloud Computing

5.6.1 Identify basic cloud concepts (L1)

5.6.2 Summarize the properties and purpose of services provided by networked hosts (L2)

CONTENT STANDARD 6.0: UNDERSTAND INDUSTRY STANDARDS, PRACTICES, AND NETWORK THEORY

Performance Standard 6.1: Determine ISO Layers

6.1.1 Describe the OSI model and relate to hardware in a network (L1, L2)

6.1.2 Implement the appropriate industry policy and procedures (L1, L2)

6.1.3 Compare and contrast the ports and protocols (HTTP – Hypertext Transfer Protocol, NetBIOS – Network Basic Input/Output System, SMTP – Simple Mail Transfer Protocol, TCP – Transmission Control Protocol, UDP – User Datagram Protocol, etc.) (L1, L2)

6.1.4 Configure and apply appropriate ports and protocols (FTP, SSH, Telnet, DHCP, TFTP, etc.) (L2)

6.1.5 Utilize appropriate wired connections (L2)

6.1.6 Utilize appropriate wireless connections (L2)

Performance Standard 6.2: Demonstrate the Basics of Network Theory and Concepts

6.2.1 Describe encapsulation/de-encapsulation (L1)

6.2.2 Explain modulation techniques (L1)

6.2.3 Apply numbering systems (e.g., binary, octal, hexadecimal) (L1)

6.2.4 Demonstrate addressing and subnetting techniques (L1)

6.2.5 Compare broadband/baseband (L1)

6.2.6 Compare and contrast bit rates versus baud rates (L1)

6.2.7 Describe code-division multiple access (CDMA) (L1)

6.2.8 Explain the difference between carrier sense multiple access with collision detection (CSMA/CD) and collision avoidance (CSMA/CA) (L1)

6.2.9 Describe wavelength (L1)

6.2.10 Apply transmission control protocol/internet protocol (TCP/IP) suite (TCP, UDP, ICMP – internet control message protocol) (L1)

Performance Standard 6.3: Configure Equipment Location Using Best Practices

6.3.1 Compare main distribution frame (MDF) and intermediate distribution frame (IDF) (L1, L2)

6.3.2 Implement a cable management solution (L1, L2)

6.3.3 Analyze and create a power management plan (i.e., power converters, circuits, UPS – uninterruptible power supply [power redundancy], inverters, load capacity) (L1, L2)

6.3.4 Determine proper airflow for optimal performance (L1, L2)

6.3.5 Utilize correct rack systems for location and operation (L1)

6.3.6 Employ consistent labeling methodologies (port, system, circuit, patch panel) (L1)

6.3.7 Develop a plan to monitor rack security and environmental conditions (L1)

CONTENT STANDARD 7.0: UNDERSTAND NETWORKING

Performance Standard 7.1: Install Networks

7.1.1 Categorize Ethernet wired network adapter components, features, and connectors (L2)
7.1.2 Categorize Ethernet wireless access point components, features, connectors, and cables (L2)
7.1.3 Describe common network connectivity devices and their roles (L2)
7.1.4 Distinguish between the various network types (L2)
7.1.5 Apply appropriate networking utilities to view, test, and troubleshoot basic network configuration, topology, communicant, and connectivity problems (L2)

Performance Standard 7.2: Utilize and Implement Network Security Practices and Techniques

7.2.1 Deploy best practices to secure any device accessing a network (L2)
7.2.2 Compare and contrast physical security controls (L2)
7.2.3 Compare and contrast risk-related concepts (L2)
7.2.4 Implement network hardening techniques (L2)
7.2.5 Configure a basic firewall (L2)
7.2.6 Explain the purpose of various network access control models (L2)
7.2.7 Secure SOHO wired and wireless networks (L2)
7.2.8 Identify common network vulnerabilities, threats, and risks (L2)
7.2.9 Analyze and implement security settings on figure BIOS/UEFI security settings (L2)

Performance Standard 7.3: Practice Network Troubleshooting

7.3.1 Implement various networking troubleshooting methodologies (L2)
7.3.2 Analyze and interpret the output of troubleshooting tools (L2)
7.3.3 Troubleshoot and resolve common wireless issues (L2)
7.3.4 Troubleshoot and resolve common copper and fiber cable issues (L2)
7.3.5 Troubleshoot and resolve common network issues (L2)
7.3.6 Troubleshoot and resolve common security issues (L2)
7.3.7 Troubleshoot and resolve common wide area network (WAN) issues (L2)

Performance Standard 7.4: Describe Network Architecture

7.4.1 Explain the functions and application of various network devices (L2)
7.4.2 Compare the use of networking services and applications (L2)
7.4.3 Install and configure networking services and applications (L2)
7.4.4 Explain the characteristics and benefits of various WAN technologies (L2)
7.4.5 Install and terminate various cable types and connectors using appropriate tools (L2)
7.4.6 Differentiate between network infrastructure implementations (L2)
7.4.7 Implement and configure the appropriate addressing schema (L2)
7.4.8 Explain the basics of routing (L2)
7.4.9 Describe the elements of unified communications technologies (L2)

CONTENT STANDARD 8.0: UNDERSTAND NETWORK OPERATIONS

Performance Standard 8.1: Use Appropriate Monitoring Tools

8.1.1 Describe the use of packet tracing tools and network analyzing tools (L2)
8.1.2 Demonstrate the use of network monitoring tools (L2)
8.1.3 Demonstrate the use of port and vulnerability scanning tools (L2)
8.1.4 Describe the use of SMTP monitoring software (L2)
8.1.5 Demonstrate an understanding of security information and event management (SIEM) tools (L2)
8.1.6 Demonstrate the use of environmental monitoring tools (L2)
8.1.7 Operate power monitoring tools (L2)
8.1.8 Demonstrate the use of wireless survey tools (L2)

Performance Standard 8.2: Metrics and Reports from Monitoring and Tracking Performance Tools

8.2.1 Analyze SYSLOG data (L2)
8.2.2 Demonstrate the use of log management (L2)
8.2.3 Apply interface monitoring tools (L2)
8.2.4 Evaluate system performance metrics against baseline data (L2)
8.2.5 Evaluate system metrics and logs for resource depletion (L2)
8.2.6 Evaluate system metrics and logs for network connectivity (L2)

Performance Standard 8.3: Use Appropriate Resources to Support Configuration Management

8.3.1 Prepare archives/backups (L2)
8.3.2 Build a system baseline based on normal operations (L2)
8.3.3 Describe provisioning and de-provisioning of mobile devices (enterprise, BYOD – bring your own device) (L2)
8.3.4 Illustrate network access control (NAC) (L2)
8.3.5 Document a configuration management strategy (L2)

Performance Standard 8.4: Explain the Importance of Implementing Network Segmentation

8.4.1 Compare and contrast protecting supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS) (L2)
8.4.2 Determine a plan to protect legacy systems (L2)
8.4.3 Explain how to separate private/public networks (L2)
8.4.4 Describe theft detection technologies (honeypot/honeynet) (L2)
8.4.5 Research the need for a testing lab (development ops/DevOps) (L2)
8.4.6 Determine a plan for load balancing the network (L2)
8.4.7 Create a plan for performance optimization (tuning) (L2)

Performance Standard 8.5: Apply System Patches and Updates

8.5.1 Install software and hardware patches and updates (OS, critical, non-critical, etc.) (L1)

8.5.2 Compare and contrast firmware and driver updates (L1)

8.5.3 Recognize the difference between feature releases/security updates (L1)

8.5.4 Develop rollout/rollback procedures (L1)

Performance Standard 8.6: Configure a Switch Using Proper Setup and Features

8.6.1 Set up, configure, and secure a virtual local area network (VLAN), physically or virtually (L2)

8.6.2 Configure a Spanning Tree Protocol (STP), ensuring you do not create any loops (L2)

8.6.3 Set up an Ethernet Interface via the interface configuration file, including demonstrating how to give your network card an IP address (DHCP – dynamic host configuration protocol); set up routing information; configure IP masquerading; and set default routes (L2)

8.6.4 Set up and configure a default gateway, defining where to send packets for IP addresses for which they can determine no specific route (L2)

8.6.5 Describe and demonstrate several common techniques for transmitting power over Ethernet cabling (L2)

8.6.6 Compare and contrast managed versus unmanaged switches (L2)

CONTENT STANDARD 9.0: UNDERSTAND THE CYBERSECURITY LIFECYCLE

Performance Standard 9.1: Explain the Cybersecurity Lifecycle

9.1.1 Describe the steps of the cybersecurity lifecycle (e.g., people, process, and tools) (L1)

9.1.2 Write a set of principles, rules, and practices to provide guidance and direction (L1)

9.1.3 Follow appropriate decision-making models to determine correct response procedures (L1)

Performance Standard 9.2: Develop an Incident Response Plan

9.2.1 Plan, prepare, and develop scope for a Cyber Incident Response Plan (L1)

9.2.2 Determine correct detection, mitigation, and reporting processes (L1)

9.2.3 Evaluate assessment and decision-making steps when handling an incident or event (L1)

9.2.4 Determine correct investigative procedures (L1)

9.2.5 Gather intelligence from a variety of sources, including open source and others (L1)

9.2.6 Document intelligence-gathering efforts, including who, what, when, where, why, and how (L1)

9.2.7 Determine the extent of event or incident scope, including severity (L1)

9.2.8 Determine the correct containment steps based on the type of incident or event encountered (L2)

9.2.9 Implement the correct eradication response and processes (L2)

9.2.10 Determine the next steps post investigation (post breach) from legal, HR, news media response (L2)

Performance Standard 9.3: Design Specific Plans for the Protection of Property, Systems, and Data

9.3.1 Determine the appropriate security control, technique, or process based on the property, system, or data you are protecting (L2)

9.3.2 Explain the importance of security controls, techniques, and threat risk assessments (L2)

9.3.3 Select the appropriate solution to eliminate vulnerabilities and establish a security baseline (L2)

9.3.4 Develop plans to protect a variety of property, systems, or data (L2)

9.3.5 Implement the appropriate controls to ensure security of property, systems, or data (L2)

9.3.6 Compare and contrast alternative methods to mitigate security risks for data in transit and data at rest (L2)

Performance Standard 9.4: Explain Incident and Event Handling Functions in a System

- 9.4.1 Describe the digital chain of custody process for tracking data and equipment (legal evidence) (L2)
- 9.4.2 Describe all steps to capture and maintain evidence (L2)
- 9.4.3 Follow chain of custody procedures (L2)
- 9.4.4 Maintain detailed records (e.g., chain of custody forms, evidence collection forms) (L2)
- 9.4.5 Track digital evidence (e.g., how it has been gathered, tracked, and protected) (L2)
- 9.4.6 Describe a chain of custody (L2)
- 9.4.7 Develop a plan for data transport, encryption to avoid alteration of data, and legal holds (L2)
- 9.4.8 Develop a plan for recovery, disposal of evidence, and follow-up (L2)
- 9.4.9 Write a forensics summary report (L2)

CONTENT STANDARD 10.0: UNDERSTAND COMPUTER FORENSICS CONCEPTS

Performance Standard 10.1: Determine Investigative Objectives

10.1.1 Summarize basic forensic concepts and practices, including eDiscovery, documentation, chain of custody, and data transport (L2)

10.1.2 Determine a first responder's logical approach during an investigation with objective, evidence-based research (L2)

10.1.3 Review the First Responder steps and processes for proper documentation (L2)

10.1.4 Explain what eDiscovery is, including the contextual process for electronic evidence collection (Electronically Stored Information [ESI]) (L2)

10.1.5 Observe and discuss legal restrictions, stipulations, regulatory compliance, and confidentiality when gathering evidence (L2)

10.1.6 Summarize chain of custody processes during investigations (L2)

Performance Standard 10.2: Examine Exploits, Threats, Attacks, and Targets

10.2.1 Explain the proper use of penetration testing versus vulnerability scanning (L1)

10.2.2 Explain the many types of vulnerabilities, exploits, and cyber threats a First Responder encounters (L1)

10.2.3 Discover the common types of cyber threat actors, including Cybercriminals, Attention-Seekers, Script Kiddies, Hacktivists, and Nation States (L1)

10.2.4 Explain and summarize the common cybersecurity attacks, including the preferred tactics, techniques, and procedures (TTPS) of threat actors (L1)

10.2.5 Examine and summarize the targets of cyber threat actors, including governments, military agencies, non-profits, and businesses across sectors including retail, legal, energy, healthcare, technology, entertainment, and telecommunications (L1)

10.2.6 Review and examine geopolitical flashpoints (L1)

Performance Standard 10.3: Digital Forensics and Forensic Response Tools and Methods

10.3.1 Describe and demonstrate various methods and tools for threat detection and eDiscovery (L2)

10.3.2 Describe and demonstrate vulnerability management methods, practices, and scanning tools (L2)

10.3.3 Describe and demonstrate various practices, methods, and tools for penetration testing (L2)

10.3.4 Identify encryption methods and demonstrate tools to decipher encrypted data (L1)

10.3.5 Review basic cryptography concepts, methods, and their relationship to forensics (L2)

10.3.6 Identify Web application exploits and vulnerabilities (L1)

10.3.7 Describe and demonstrate Web Application Security and Scanning methods and tools (L1)

10.3.8 Identify methods or tools to eliminate cloud exploits and vulnerabilities (L2)

10.3.9 Describe and demonstrate a working knowledge of phishing attacks and mitigation steps (L1)

Performance Standard 10.4: Perform Forensic Analysis and Analyze Malware

10.4.1 Explain what malware is, including its history (L2)

10.4.2 Review and define the most common malware terminologies (L2)

10.4.3 Describe the ways and methods malware is spread (L2)

10.4.4 Review current types of malware (e.g., viruses, worms, trojan horses, rootkits, ransomware, keyloggers, and grayware attacks) (L2)

10.4.5 Select the appropriate types of mitigation and deterrent techniques for malware scenarios (L2)

10.4.6 Use appropriate tools and techniques to eliminate malware from spreading (L2)

CONTENT STANDARD 11.0: UNDERSTAND EMERGING TECHNOLOGIES

Performance Standard 11.1: Explain Workforce and Society Needs Related to New and Emerging Technologies

11.1.1 Describe job skills needed for potential careers in new and emerging technologies (L1)

11.1.2 Explore potential uses for and industries that may use emerging technologies (L1)

11.1.3 Explain the role of ethics as it relates to security and emerging technologies (L1)

This Page was Intentionally Left Blank.

Complementary Courses

State Complementary Skill Standards

State complementary skill standards are designed to clearly state what the student should know and be able to do upon completion of a **one-year** complementary course related to their career and technical education (CTE) program of study. **Completion of the qualifying Program of Study is required prior to enrollment in a complementary course.**

Employability Skills for Career Readiness Standards

Students have completed all program content standards and will pursue advanced study through investigation and in-depth research.

Complementary Course Standards Contributing Members

Course Contribution(s)	Name	Occupation/Title	Stakeholder Affiliation	School/Organization
Cryptography	Fran Bromley-Norwood	Instructor	Secondary Educator	Clark High School, Clark County School District
Cryptography	Frankie Clark	Instructor	Secondary Educator	North Valleys High School, Washoe County School District
Cryptography	Robbie Pearce	Instructor	Secondary Educator	Cheyenne High School, Clark County School District
Cryptography	Sharona Thompson	Instructor	Secondary Educator	Valley High School, Clark County School District
Ethical Hacking	Reuben Bellotte	Instructor	Secondary Educator	Advanced Technologies Academy, Clark County School District
Ethical Hacking	Frankie Clark	Instructor	Secondary Educator	North Valleys High School, Washoe County School District
Ethical Hacking	Ben Crenshaw	Head of Cyber Education	Business and Industry Representative	Work ED
Ethical Hacking	Jackie Fernandes	Security& Data Privacy Compliance Consultant	Business and Industry Representative	Transparency Inc.
Ethical Hacking	Chris Forte	President	Business and Industry Representative	C2Society
Ethical Hacking	Jefferson Grace	Chief Information Security Officer	Business and Industry Representative	Nevada Department of Transportation
Ethical Hacking	Christina Mendenhall	Instructor	Secondary Educator	Spanish Springs High School, Washoe County School District
Ethical Hacking	Greg Moody	Instructor	Postsecondary Educator	University of Nevada, Las Vegas
Ethical Hacking	Shawn Riley	Senior Principal Cyber Scientist and Director of Cybersecurity Science	Business and Industry Representative	Telos Corp.
Ethical Hacking	Kevin Rutherford	President and Founder	Business and Industry Representative	Null404: Cyber Security Research
Ethical Hacking	Arthur Salmon	Instructor	Post Secondary Educator	College of Southern Nevada, Las Vegas
Ethical Hacking	Robert Speciale	Instructor	Secondary Educator	West Career and Technical Academy, Clark County School District

Business and Industry Validation

All CTE standards developed through the Nevada Department of Education are validated by business and industry through one or more of the following processes: (1) the standards are developed by a team consisting of business and industry representatives, or (2) a separate review panel is coordinated with industry experts to ensure the standards include the proper content, or (3) nationally recognized standards currently endorsed by business and industry.

The Cryptography and Ethical Hacking complementary standards for Cybersecurity program of study were validated through active participation of business and industry representatives through the criticality survey.

Complementary Course Information for Cybersecurity

Program Information

Qualifying Program of Study: **Cybersecurity**
Career Cluster: **Information Technology**
Career Pathway(s): **Network Systems**
CTSO: **FBLA/SkillsUSA**
Grade Level: **11-12**

Program Structure for Complementary Courses

The complementary courses are provided in the following table. **The qualifying program of study must be completed prior to enrolling in the complementary courses** (except labs that are done concurrently with the second-year course). A program does not have to utilize the complementary courses for students to complete their program of study.

Complementary Courses

Required/ Complementary	Course Title	Abbreviated Name
C	Cryptography	CRYPTO
C	Ethical Hacking	ETHICAL HACK
C	Cybersecurity Advanced Studies	CYBRSECU AS
C	Industry-Recognized Credential – Cybersecurity	IRC CYBRSECU
C	CTE Work Experience – Information Technology	WORK EXPER IT

Complementary Course Standards
Cryptography

CONTENT STANDARD 1.0: OVERVIEW OF CRYPTOGRAPHY

Performance Standard 1.1: Describe the Nature of Cryptography

1.1.1 Research various types of cryptography
1.1.2 Describe occupations that use cryptography
1.1.3 Explain how people encounter cryptography in day-to-day life
1.1.4 Explain the connection between math, algorithms, and ciphers
1.1.5 Explain the difference between blockchain and block cipher
1.1.6 Define cryptanalysis as it relates to cryptography

Performance Standard 1.2: Explain the History of Ciphers

1.2.1 Explain the history of cryptography
1.2.2 Describe the importance of the Enigma and Turing (The Bombe) machines
1.2.3 Explain the need for ciphering with the birth of the digital age
1.2.4 Describe the use of RSA (Rivest–Shamir–Adleman) in today's online environment

CONTENT STANDARD 2.0: ANALOG CIPHERING METHODS

Performance Standard 2.1: Identify the Origins of Various Cyphers

2.1.1 Explain substitution ciphers (e.g., Masonic, polyalphabetic, etc.)
2.1.2 Describe Caesar ciphers
2.1.3 Explain transposition ciphers
2.1.4 Compare steganography and cryptography as used in ciphers

Performance Standard 2.2: Create Analog Ciphers

2.2.1 Apply a cipher technique to keep information secret
2.2.2 Develop a key to decipher the message
2.2.3 Decipher a cipher

CONTENT STANDARD 3.0: DIGITAL CIPHERING METHODS

Performance Standard 3.1: Identify Digital Cryptography Techniques

3.1.1 Compare block and stream ciphers (i.e., of Advanced Secret Writing Standard (AES) and Data Secret Writing Standard (DES))
3.1.2 Research the role of block ciphers in data integrity
3.1.3 Relate key stream synchronicity to stream ciphers
3.1.4 Explain the use of hash functions
3.1.5 Discuss the difference between steganography and cryptography
3.1.6 Identify challenges when managing encryption on a large scale
3.1.7 Apply tools and protocols to real world practice

Performance Standard 3.2: Build a Block Cipher

- 3.2.1 Build a block cipher with a data integrity component
- 3.2.2 Create a crypto key
- 3.2.3 Write an algorithm for a cipher
- 3.2.4 Describe how keys are generated

Performance Standard 3.3 Explain Public Keys

- 3.3.1 Define the purpose of public vs. private keys
- 3.3.2 Compare symmetric and asymmetric keys
- 3.3.3 Explain various security mechanisms
- 3.3.4 Describe the strengths and weakness of the Diffie-Hellman protocol
- 3.3.5 Explain the importance of authentication
- 3.3.6 Describe the strengths and weakness of the RSA protocol

CONTENT STANDARD 4.0: CRYPTOGRAPHIC ATTACKS AND DEFENSES

Performance Standard 4.1 Explore Cryptographic Vulnerabilities

- 4.1.1 Describe different types of attacks on cryptographic systems
- 4.1.2 Research different types of defenses against cryptographic attacks
- 4.1.3 Differentiate between passive and active attacks
- 4.1.4 Apply various techniques to encrypt a message
- 4.1.5 Analyze a passive attack using network traffic data and analysis

CONTENT STANDARD 5.0: CRYPTOGRAPHY IN TODAY'S WORLD

Performance Standard 5.1 Explore Ethical and Legal Issues Related to Cryptography

- 5.1.1 Research the ethics of cryptography
- 5.1.2 Discuss the balance between privacy and security
- 5.1.3 Research regulations and laws of cryptography and encryption

Performance Standard 5.2 Explore Future Trends in Cryptography

- 5.2.1 Describe the role of computational mathematics in the development of future cryptographic systems
- 5.2.2 Research how future technology may threaten cryptography
- 5.2.3 Discuss the role cryptography plays in the development of digital currencies
- 5.2.4 Examine ways in which encryption using cryptography can be applied in the future

Complementary Course Standards
Ethical Hacking

CONTENT STANDARD 1.0: OVERVIEW OF ETHICAL HACKING

Performance Standard 1.1: Introduction to Ethical Hacking

1.1.1 Define Ethical Hacking
1.1.2 Identify the skills and qualifications to be an ethical hacker
1.1.3 Explore careers in cybersecurity
1.1.4 Discuss the importance of networking with other professionals
1.1.5 Analyze how different nations handle cybersecurity
1.1.6 Discuss the magnitude and impact of the global cyber war
1.1.7 Discuss emerging and disruptive trends in cybersecurity
1.1.8 Describe the phases of an attack
1.1.9 Review attack vectors and threats
1.1.10 Compare the types of penetration tests
1.1.11 Compare Cyber Attack Frameworks (Ex. NIST, OWASP, ATT&CK, CAPEC, Cyber Kill Chain, Cobit etc)
1.1.12 Review and analyze types of hackers
1.1.13 Describe ethics in cybersecurity
1.1.14 Discuss cybersecurity laws and the consequences for breaking those laws
1.1.15 Identify why we need ethical hackers

CONTENT STANDARD 2.0: SHELL SCRIPTING

Performance Standard 2.1: Overview of Linux for ethical hackers

2.1.1 Identify and use file descriptors
2.1.2 Identify and use escape spaces
2.1.3 Use the find command
2.1.4 Use the strings command
2.1.5 Use the file command
2.1.6 Create and modify users and groups
2.1.7 Use stdin, stdout, stderr streams
2.1.8 Use the uniq, less, and sort commands
2.1.9 Invert a match using the grep command
2.1.10 Decode base64 in the terminal
2.1.11 Use strings command to read binary data
2.1.12 Explore the reasons for using file compression
2.1.13 Send files with netcat
2.1.14 Work with hex dump
2.1.15 Use the wheel group

2.1.16 Use the visudo command
2.1.17 Use a for loop to brute-force a pin
2.1.18 Complete command injection by stalling a zoom buffer
2.1.19 Use Vim to execute commands
2.1.20 Use cron jobs
2.1.21 Execute OS commands using ssh
2.1.22 Use openssh to connect to host machines
2.1.23 Compare two files in the terminal and see the difference using the diff command

CONTENT STANDARD 3.0: PROGRAMMING

Performance Standard 3.1: Python and PHP Scripting for Ethical Hackers

3.1.1 Use appropriate syntax in Python
3.1.2 Use variables for storing data of various types in Python
3.1.3 Convert strings into integers
3.1.4 Use conditional statements and loops in Python
3.1.5 Use functions in Python
3.1.6 Use try and except blocks for exception handling
3.1.7 Create a user-friendly script that allows custom input
3.1.8 Run scripts from other scripts
3.1.9 Use Python modules for networking
3.1.10 Open, read, and compare two files
3.1.11 Handle socket errors
3.1.12 Import IP from the IPy Python library and use it for network coding
3.1.13 Explain the purpose of Python docstrings
3.1.14 Run Python scripts in a Windows environment
3.1.15 Automate scripts in a Windows environment
3.1.16 Use .bat files
3.1.17 Create a counter that fires a function
3.1.18 Interact with APIs using Python
3.1.19 Modify scripts so they work on a Windows system
3.1.20 Work with proxy settings that prevent Python scripts from running
3.1.21 Use a text editor with Python code to test and parse website data
3.1.22 Use Python Requests and Regular Expression modules
3.1.23 Examine web pages for vulnerabilities using Python code
3.1.24 Manipulate HTTP headers using Python code

CONTENT STANDARD 4.0: THE SECURITY ASSESSMENT

Performance Standard 4.1 Reconnaissance

4.1.1 Perform passive footprinting using search engines and web services
4.1.2 Perform competitive intelligence
4.1.3 Perform a Whois lookup

Performance Standard 4.2 Scanning and Enumeration

4.2.1 Review legal issues when scanning
4.2.2 Review the OSI Model, TCP/IP Model and the Protocols
4.2.3 Review Nmap scanning procedures
4.2.4 Utilize Metasploit
4.2.5 Define Target identification with Metasploit and Nmap
4.2.6 Perform advanced scanning with Metasploit and Nmap
4.2.7 Perform Banner Grabbing
4.2.8 Explore other scanning and enumeration tools
4.2.9 Discuss vulnerability assessment concepts
4.2.10 Use vulnerability analysis tools

Performance Standard 4.3 Sniffing, IDS, and Firewall Evasion

4.3.1 Define sniffing
4.3.2 Compare passive and active sniffing
4.3.3 Analyze and use sniffing tools
4.3.4 Recognize a secure domain
4.3.5 Sniff credentials from an insecure web app
4.3.6 Analyze a domain for security
4.3.7 Explain the applied application for different sniffing tools
4.3.8 Filter packets with sniffing tools
4.3.9 Detect malicious attacks with sniffing tools
4.3.10 Distinguish between types of IDS/Firewall alerts
4.3.11 Review detection evasion types and techniques
4.3.12 Perform detection evasion techniques
4.3.13 Define IP and MAC address spoofing
4.3.14 Summarize packet creation
4.3.15 Review network connections using various tools
4.3.16 Create a custom packet and observe it on the wire
4.3.17 Create a shell

Performance Standard 4.4 Attacks and Exploits

4.4.1 Describe the post exploitation process
4.4.2 Define cryptography
4.4.3 Examine cryptographic hash types

4.4.4 Review tools and methods used to crack authentications
4.4.5 Describe the importance of password strength
4.4.6 Discuss how backdoors are wrapped in applications
4.4.7 Give examples of how social engineering relates to backdoor wrapping
4.4.8 Learn the countermeasures to prevent users from installing backdoors
4.4.9 Identify types of Denial of Service (DoS) attacks
4.4.10 Identify DoS countermeasures
4.4.11 Review how to modify the bash terminal

Performance Standard 4.5 Web Apps and Data Servers

4.5.1 Discuss the importance of thorough reconnaissance
4.5.2 Give examples of the types of attack vectors in Web Applications
4.5.3 Review Bug Bounty programs
4.5.4 Discover subdomains
4.5.5 Discover web application directories
4.5.6 Describe how a proxy works
4.5.7 Setup a proxy for web application testing
4.5.8 Explore web traffic analysis
4.5.9 Perform a manual vulnerability test
4.5.10 Review the Open Web Application Security Project (OWASP) top 10
4.5.11 Describe the process of spidering
4.5.12 Review Cross Site Scripting vulnerabilities
4.5.13 Review basics of SQL databases
4.5.14 Examine and Utilize MySQL Database commands
4.5.15 List types of SQL injection vulnerabilities
4.5.16 Examine the impact of SQL injection
4.5.17 Examine web application code for security flaws
4.5.18 Review web application vulnerability scanning techniques
4.5.19 Research scanning tools
4.5.20 Review the web app vulnerability stack
4.5.21 Identify different types of web application shells
4.5.22 Test for and discover file upload vulnerabilities

Performance Standard 4.6 Basics of Server Side Web Security

4.6.1 Identify Python methods hackers use to discretely retrieve data from compromised systems
4.6.2 Exploit a directory traversal vulnerability using Python
4.6.3 Exploit a Local File Inclusion vulnerability using Python
4.6.4 Analyze cryptographic encryption and reverse it for decryption
4.6.5 Exploit with Python a command injection vulnerability against a web application
4.6.6 Bypass filters that prevent access to sensitive content
4.6.7 Exploit a command substitution vulnerability

4.6.8 Exploit a time-based SQL injection
4.6.9 Exploit a session vulnerability

Performance Standard 4.7 Advanced Social Engineering

4.7.1 Define and understand pretexting
4.7.2 Define and understand spoofing
4.7.3 Create a spoofed email
4.7.4 Identify SMTP vulnerabilities
4.7.5 Review the Social Engineering Attack Cycle
4.7.6 Describe types of social engineering attacks designed to harvest credentials
4.7.7 Explore Social Engineering tools and frameworks
4.7.8 Examine human hacking techniques and how to detect them
4.7.9 Examine engagements in Social Engineering
4.7.10 Describe difference between common phishing and spear phishing
4.7.11 Identify common manipulation tactics
4.7.12 Create a Spear Phishing email

Performance Standard 4.8 Security Training on a Virtual Machine

4.8.1 Examine processes for locating system vulnerabilities
4.8.2 Examine web applications for vulnerabilities
4.8.3 Examine data collection techniques and their controversies
4.8.4 Use encoding and decoding methods

Performance Standard 4.9 Privilege Escalation and Post Exploitation

4.9.1 Complete post exploitation of a Windows System
4.9.2 Identify the types of information to collect once exploitation has occurred
4.9.3 Use pivoting in a penetration test engagement
4.9.4 Use port forwarding in a penetration test engagement
4.9.5 Describe how to use winPEAS
4.9.6 Complete enumeration of a Windows system with winPEAS
4.9.7 Enumerate a Linux device for credentials and vulnerabilities
4.9.8 Use SSH for remote access
4.9.9 Locate and modify SSH configuration files
4.9.10 Obtain SSH private keys

Performance Standard 4.10 Penetration Testing

4.10.1 Complete post exploitation of a Windows System
4.10.2 Identify the types of information to collect once exploitation has occurred
4.10.3 Use pivoting in a penetration test engagement
4.10.4 Use port forwarding in a penetration test engagement
4.10.5 Describe how to use winPEAS
4.10.6 Complete enumeration of a Windows system with winPEAS

Performance Standard 4.11 Reporting for Penetration Testers

4.11.1 Discuss report writing and its importance

4.11.2 Identify the elements that should be included in a report

4.11.3 Identify common mistakes when writing a report

4.11.4 Generate a template for report formatting and setup

4.11.5 Write a report from a penetration test