

2022 Cybersecurity

Program Standards

CONTENT STANDARD 1.0: Demonstrate Cybersecurity Career Basics

Performance Standard 1.1: Identify Cybersecurity Career Pathways

- 1.1.1 Identify career pathways in cybersecurity.
- 1.1.2 Identify industry certification options for career pathways.
- 1.1.3 Identify postsecondary options that will advance career pathway goals.

Performance Standard 1.2: Identify the Role of Cybersecurity and Professional Mindsets

- 1.2.1 Describe the objective of cybersecurity in businesses and organizations.
- 1.2.2 Identify the mindsets and traits (e.g., continuous learning, passion, integrity, curiosity) of the cybersecurity professional.

CONTENT STANDARD 2.0: Demonstrate Cybersecurity Fundamentals

Performance Standard 2.1: Identify Cybersecurity Concepts

- 2.1.1 Describe data and data types.
- 2.1.2 Explain the CIA model (confidentiality, integrity, availability).
- 2.1.3 Explain the concepts of authentication, authorization and auditing (AAA).
- 2.1.4 Identify basic cryptography concepts, methods, and uses.
- 2.1.5 Identify the concepts of access control principles.
- 2.1.6 Identify access control models.
- 2.1.7 Explain the principle of least privilege.
- 2.1.8 Describe Zero Trust architecture.
- 2.1.9 Identify techniques to protect data in all three states (i.e., "data in use", "data at rest" and "data in motion").
- 2.1.10 Explain types of vulnerabilities, exploits, and cyber threats.
- 2.1.11 Identify the common types of cyber threat actors.
- 2.1.12 Describe the phases of Cyber Kill Chain framework
- 2.1.13 Describe vulnerability management.
- 2.1.14 Explain the importance of asset inventory.
- 2.1.15 Define *risk* and *risk management*.
- 2.1.16 Describe the value of risk assessment.
- 2.1.17 Describe the importance of cybersecurity policies and procedures.

Performance Standard 2.2: Explain Law and Ethics Related to Cybersecurity

- 2.2.1 Explain ethical and legal issues related to cybersecurity.
- 2.2.2 Describe ethical hacking and non-ethical hacking.
- 2.2.3 Identify cyber laws and regulations for individuals and businesses.
- 2.2.4 Explain the importance of protecting intellectual property.

CONTENT STANDARD 3.0: Demonstrate Cybersecurity Skills on Systems and Networks

Performance Standard 3.1: Work with Systems

- 3.1.1 Compare storage media.
- 3.1.2 Describe the architecture of a computer.
- 3.1.3 Compare read-only memory (ROM) and random-access memory (RAM).
- 3.1.4 Describe basic boot methods and boot order.
- 3.1.5 Compare the file structures of Windows and Linux.
- 3.1.6 Describe password policies.
- 3.1.7 Identify programming languages used in cybersecurity.
- 3.1.8 Program with a text-based language (e.g., Python), using version control, unit testing and recommended styles and idioms.



3.1.9 Describe the role of Bash and PowerShell, used by cybersecurity analysts.

Performance Standard 3.2: Work with Networks and the Internet

- 3.2.1 Describe types of area networks (e.g., LAN, WAN, MAN).
- 3.2.2 Describe various network communication technologies (e.g., Wi-Fi, mobile data, Ethernet).
- 3.2.3 Identify networkable devices (i.e., Internet of Things [IoT]), their categories, benefits and security risks.
- 3.2.4 Compare the Open Systems Interconnection (OSI) model and the TCP/IP model.
- 3.2.5 Describe tools and techniques available to identify networking interfaces and their settings.
- 3.2.6 Describe the following network services: Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS).
- 3.2.7 Describe subnetting of Layer 3 addresses.
- 3.2.8 Identify the common TCP and UDP ports used in networking.
- 3.2.9 Compare the two transport methods used in Layer 4 of the OSI model within the TCP/IP stack.
- 3.2.10 Describe the use of an access control list on an interface.
- 3.2.11 Describe the use of IP tables for access control.
- 3.2.12 Describe the use of Windows firewall for access control.
- 3.2.13 Compare communication types: unicast, broadcast, multicast, and anycast.
- 3.2.14 Describe the purposes and types of virtual access.
- 3.2.15 Define Cloud Computing.

CONTENT STANDARD 4.0: Demonstrate Cybersecurity Operations

Performance Standard 4.1: Manage Systems, Servers, and Network Operations

- 4.1.1 Install and configure Windows desktop operating system.
- 4.1.2 Install and configure Linux desktop operating system.
- 4.1.3 Install and configure server operating system.
- 4.1.4 Manage a desktop operating system through its lifecycle.
- 4.1.5 Manage a server operating system through its lifecycle.
- 4.1.6 Recover a desktop operating system
- 4.1.7 Recover a server operating system.
- 4.1.8 Explain reasons and options for segmentation.
- 4.1.9 Describe the value of logging and monitoring.
- 4.1.10 Obtain information and navigate an operating system, using command line.
- 4.1.11 Perform basic configurations for routers and switches.
- 4.1.12 Implement IP addressing schemes, given an address space.
- 4.1.13 Map different network layer identifiers for a process.
- 4.1.14 Describe network device port security and hardening.
- 4.1.15 Describe operating system hardening.
- 4.1.16 Apply encryption methods and tools to decipher encrypted data.
- 4.1.17 Identify different options for redundancy.
- 4.1.18 Implement redundancy.
- 4.1.19 Identify important data or systems that need redundancy.
- 4.1.20 Define high availability (HA).

Performance Standard 4.2: Demonstrate Troubleshooting Techniques

- 4.2.1 Describe basic hardware and software problems, using industry terminology.
- 4.2.2 Describe troubleshooting techniques used with hardware and software to identify and fix errors.
- 4.2.3 Implement systematic troubleshooting strategies used with hardware and software to identify and fix errors.

CONTENT STANDARD 5.0: Mitigate Risk and Vulnerability



Performance Standard 5.1: Manage Risk

- 5.1.1 Perform device discovery.
- 5.1.2 Identify types of tools that can be used to monitor, collect, and analyze information across platforms
- 5.1.3 Describe how a security framework is used to assess the security posture of an enterprise environment.
- 5.1.4 Define defense in depth.
- 5.1.5 Describe social engineering.

Performance Standard 5.2: Explore Penetration Testing

- 5.2.1 Explain the proper use of penetration testing versus vulnerability scanning.
- 5.2.2 Describe the steps of a penetration test and its role in securing a business.
- 5.2.3 Identify the Open Web Application Security Project (OWASP) Top 10.
- 5.2.4 Identify Common Vulnerability and Exposure (CVE), a list of specific vulnerabilities for specific products.

Performance Standard 5.3: Explore Physical Security

- 5.3.1 Describe the different types of attacks that affect physical security.
- 5.3.2 Describe physical access controls.

CONTENT STANDARD 6.0: Explore Incident Response

Performance Standard 6.1: Explore Incident Response, Digital Forensics, and Recovery

- 6.1.1 Define incident response.
- 6.1.2 Describe the steps of incident response.
- 6.1.3 Explain basic forensic concepts and practices including eDiscovery, documentation, chain of custody, and data transport.
- 6.1.4 Describe the importance of policies and procedures in incident response.
- 6.1.5 Define recovery.