2024-2025
Technical Skills Assessment
Cybersecurity

IDAHO Division of Career Technical Education

Results by Standard

Legend (%)		
0-50%	51-75%	76-100%

Assessment: Cybersecurity	% Correct 24-25
Number tested: 55	
CONTENT STANDARD 1.0: Demonstrate Cybersecurity Career Basics	84.72%
Performance Standard 1.2: Identify the Role of Cybersecurity and Professional Mindsets	84.72%
1.2.1 Describe the objective of cybersecurity in businesses and organizations.	78.33%
1.2.2 Identify the mindsets and traits (e.g., continuous learning, passion, integrity, curiosity) of the cybersecurity professional.	97.50%
CONTENT STANDARD 2.0: Demonstrate Cybersecurity Fundamentals	78.44%
Performance Standard 2.1: Identify Cybersecurity Concepts	77.97%
2.1.1 Describe data and data types.	77.78%
2.1.2 Explain the CIA model (confidentiality, integrity, availability).	82.08%
2.1.3 Explain the concepts of authentication, authorization and auditing (AAA).	72.22%
2.1.5 Identify the concepts of access control principles.	65.56%
2.1.7 Explain the principle of least privilege.	83.33%
2.1.9 Identify techniques to protect data in all three states (i.e., "data in use", "data at rest" and "data in motion").	74.44%
2.1.10 Explain types of vulnerabilities, exploits, and cyber threats.	93.75%
2.1.11 Identify the common types of cyber threat actors.	73.33%
2.1.13 Describe vulnerability management.	78.33%
2.1.14 Explain the importance of asset inventory.	86.67%
2.1.15 Define risk and risk management.	53.89%
2.1.16 Describe the value of risk assessment.	71.67%
2.1.17 Describe the importance of cybersecurity policies and procedures.	85.83%
Performance Standard 2.2: Explain Law and Ethics Related to Cybersecurity	81.67%
2.2.1 Explain ethical and legal issues related to cybersecurity.	87.78%

Assessment: Cybersecurity	% Correct 24-25
Number tested: 55	
2.2.2 Describe ethical hacking and non-ethical hacking.	75.56%
CONTENT STANDARD 3.0: Demonstrate Cybersecurity Skills on Systems and Networks	75.37%
Performance Standard 3.1: Work with Systems	88.89%
3.1.6 Describe password policies.	88.89%
Performance Standard 3.2: Work with Networks and the Internet	68.61%
3.2.2 Describe various network communication technologies (e.g., Wi-Fi, mobile data, Ethernet).	55.00%
3.2.15 Define Cloud Computing.	82.22%
CONTENT STANDARD 4.0: Demonstrate Cybersecurity Operations	70.00%
Performance Standard 4.1: Manage Systems, Servers, and Network Operations	66.11%
4.1.9 Describe the value of logging and monitoring.	66.11%
Performance Standard 4.2: Demonstrate Troubleshooting Techniques	71.94%
4.2.2 Describe troubleshooting techniques used with hardware and software to identify and fix errors.	84.44%
4.2.3 Implement systematic troubleshooting strategies used with hardware and software to identify and fix errors.	59.44%
CONTENT STANDARD 5.0: Mitigate Risk and Vulnerability	82.65%
Performance Standard 5.1: Manage Risk	76.00%
5.1.2 Identify types of tools that can be used to monitor, collect, and analyze information across platforms.	44.17%
5.1.3 Describe how a security framework is used to assess the security posture of an enterprise environment.	70.83%
5.1.4 Define defense in depth.	92.50%
5.1.5 Describe social engineering.	86.25%
Performance Standard 5.3: Explore Physical Security	92.14%
5.3.1 Describe the different types of attacks that affect physical security.	92.78%
5.3.2 Describe physical access controls.	91.67%
CONTENT STANDARD 6.0: Explore Incident Response	80.00%
Performance Standard 6.1: Explore Incident Response, Digital Forensics, and Recovery	80.00%
6.1.1 Define incident response.	85.56%
6.1.2 Describe the steps of incident response.	77.78%
6.1.3 Explain basic forensic concepts and practices including eDiscovery, documentation, chain of custody, and data transport.	75.00%
6.1.4 Describe the importance of policies and procedures in incident response.	79.44%
6.1.5 Define recovery.	78.33%