Foundations of Cybersecurity (Proc 24)

PRE-TEST/POST-TEST TEKS BLUEPRINT

Pre-Test/Post-Test Development Overview

TEKS Addressed Selection Process

The Texas Essential Knowledge & Skills (TEKS) included in the course pre-test and post-test were selected for their direct relevance to the course content. This selection process was guided by the goal of assessing learners' understanding of specific topics and skills that are integral to the course. As a result, TEKS related to general employability skills or broader topics were often excluded. This focus ensures that the assessments accurately measure students' mastery of the subject matter, allowing educators to gain a clear insight into areas where students excel or may need additional support. By concentrating on content-specific TEKS, the tests provide a more precise evaluation of the students' knowledge and understanding of the core material.

Test Question Development Process

The questions created for the pre-test and post-test were designed using psychometric principles to ensure they are of high quality and fairness. This approach helps to accurately assess student understanding. These principles guide the development of questions to be reliable, valid, and free from bias, ensuring that they effectively measure the knowledge and skills the students are expected to acquire in the course.

Foundations of Cybersecurity (Proc 24) Pre-Test/Post-Test TEKS Blueprint

Knowledge & Skills Statement	Student Expectation	iCEV Lesson Title
(2) Professional awareness. The student identifies various employment opportunities and requirements in the cybersecurity field. The student is expected to:	(D) explain the different types of services and roles found within a cybersecurity functional area such as a security operations center (SOC).	Basic Cybersecurity Concepts: Security and Incident Response
(3) Ethics and laws. The student understands ethical and current legal standards, rights and restrictions governing technology, technology systems, digital media, and the use of social media. The student is expected to:	(B) investigate and analyze local, state, national, and international cybersecurity laws such as the USA PATRIOT Act of 2001, General Data Protection Regulation, Digital Millennium Copyright Act, Computer Fraud and Abuse Act, and Health Insurance Portability and Accountability Act of 1996 (HIPAA);	Cybersecurity Ethics and Laws
(3) Ethics and laws. The student understands ethical and current legal standards, rights and restrictions governing technology, technology systems, digital media, and the use of social media. The student is expected to:	(D) communicate an understanding of ethical and legal behavior when presented with various scenarios related to cybersecurity activities;	Cybersecurity Ethics and Laws
(4) Ethics and laws. The student differentiates between ethical and malicious hacking. The student is expected to:	(A) identify motivations and perspectives for hacking;	Introduction to Cybersecurity
(4) Ethics and laws. The student differentiates between ethical and malicious hacking. The student is expected to:	(D) differentiate between industry terminology for types of hackers such as black hats, white hats, and gray hats; and	Introduction to Cybersecurity - Cybercrimes and Threats
(4) Ethics and laws. The student differentiates between ethical and malicious hacking. The student is expected to:	(E) determine and describe possible outcomes and legal ramifications of ethical versus malicious hacking practices.	Introduction to Cybersecurity - Cybercrimes and Threats Hackers
(5) Ethics and laws. The student identifies and defines cyberterrorism and counterterrorism. The student is expected to:	(B) compare and contrast physical terrorism and cyberterrorism, including domestic and foreign actors;	Cyberterrorism and Counterterrorism
(5) Ethics and laws. The student identifies and defines cyberterrorism and counterterrorism. The student is expected to:	(D) explain the role of cyber defense in protecting national interests and corporations;	Cyberterrorism and Counterterrorism
(5) Ethics and laws. The student identifies and defines cyberterrorism and counterterrorism. The student is expected to:	(F) explain the importance of protecting public infrastructures such as electrical power grids, water systems, pipelines, transportation, and power generation facilities from cyberterrorism.	Cyberterrorism and Counterterrorism
(6) Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding significant issues related to digital technology, digital hygiene, and cyberbullying. The student is expected to:	(B) analyze the positive and negative implications of a digital footprint and the maintenance and monitoring of an online presence;	Digital Citizenship
(7) Digital citizenship. The student understands the implications of sharing information and access with others. The student is expected to:	(A) define personally identifiable information (PII);	Risks of Sharing Information - What is Personally Identifiable Information?
(7) Digital citizenship. The student understands the implications of sharing information and access with others. The student is expected to:	(D) describe the risks of granting third parties access to personal and proprietary data on social media and systems; and	Risks of Sharing Information - What is Personally Identifiable Information?
(7) Digital citizenship. The student understands the implications of sharing information and access with others. The student is expected to:	(E) describe the risks involved with accepting Terms of Service (ToS) or End User License Agreements (EULA) without a basic understanding of the terms or agreements.	Risks of Sharing Information - Risks of Terms of Service (ToS) and User Agreements
(8) Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:	(A) define cybersecurity and inform	Basic Cybersecurity Concepts: Risk Management
(8) Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:	(B) identify basic risk management and risk assessment principles related to cybersecurity threats and vulnerabilities, including the Zero Trust model;	Basic Cybersecurity Concepts: Risk Management
(8) Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:	(E) identify and analyze cybersecurity breaches and incident responses	Basic Cybersecurity Concepts: Security and Incident Response
(8) Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:	(I) explore and discuss the vulnerabilities of network connected devices such as Internet of Things (IoT);	Basic Cybersecurity Concepts: Security and Incident Response
(8) Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:	(L) explore and identify common industry frameworks such as MITRE ATTandCKTM , MITRE Engage TM , and Cyber Kill Chain, and the Diamond Model.	Basic Cybersecurity Concepts: Security and Incident Response

Foundations of Cybersecurity (Proc 24) Pre-Test/Post-Test TEKS Blueprint

Knowledge & Skills Statement	Student Expectation	iCEV Lesson Title
(9) Cybersecurity skills. The student understands and explains various types of malicious software (malware). The student is expected to:	(A) define malware, including spyware, ransomware, viruses, and rootkits;	Malware - What is Malware?
(9) Cybersecurity skills. The student understands and explains various types of malicious software (malware). The student is expected to:	(B) identify the transmission and function of malware such as trojan horses, worms, and viruses;	Malware - What is Malware?
(9) Cybersecurity skills. The student understands and explains various types of malicious software (malware). The student is expected to:	(D) explain the role of reverse engineering for the detection of malware and viruses; and	Malware - Detection of Malware
(9) Cybersecurity skills. The student understands and explains various types of malicious software (malware). The student is expected to:	(E) describe free and commercial antivirus and anti-malware software also known as Endpoint Detection and Response software.	Malware - Protection Against Malware
(10) Cybersecurity skills. The student understands and demonstrates knowledge of techniques and strategies to prevent a system from being compromised. The student is expected to:	(A) define system hardening;	Preventing System Compromise: System Protection and Awareness
(10) Cybersecurity skills. The student understands and demonstrates knowledge of techniques and strategies to prevent a system from being compromised. The student is expected to:	(C) explain the importance of patching operating systems;	Preventing System Compromise: System Administration and Services
(10) Cybersecurity skills. The student understands and demonstrates knowledge of techniques and strategies to prevent a system from being compromised. The student is expected to:	(D) explain the importance of software updates;	Preventing System Compromise: System Administration and Services
(10) Cybersecurity skills. The student understands and demonstrates knowledge of techniques and strategies to prevent a system from being compromised. The student is expected to:	(G) research and explain standard practices for securing computers, networks, and operating systems, including the concept of least privilege; and	Preventing System Compromise: System Protection and Awareness
(11) Cybersecurity skills. The student understands basic network operations. The student is expected to:	(B) define network addressing;	Principles of Network Operations: Network Addressing and Devices
(11) Cybersecurity skills. The student understands basic network operations. The student is expected to:	(C) analyze incoming and outgoing rules for traffic passing through a firewall;	Principles of Network Operations: Ports, Protocols and Monitoring
(11) Cybersecurity skills. The student understands basic network operations. The student is expected to:	(D) identify well known ports by number and service provided, including port 22 (Secure Shell Protocol/ssh), port 80 (Hypertext Transfer Protocol/http), and port 443 (Hypertext Transfer Protocol Secure/https);	Principles of Network Operations: Ports, Protocols and Monitoring
(12) Cybersecurity skills. The student identifies standard practices of system administration. The student is expected to:	(A) define what constitutes a secure password;	System Administration Practices
(12) Cybersecurity skills. The student identifies standard practices of system administration. The student is expected to:	(B) create a secure password policy, including length, complexity, account lockout, and rotation;	System Administration Practices
(12) Cybersecurity skills. The student identifies standard practices of system administration. The student is expected to:	(C) identify methods of password cracking such as brute force and dictionary attacks; and	System Administration Practices
(13) Cybersecurity skills. The student demonstrates necessary steps to maintain user access on the system. The student is expected to:	(D) define and explain the purpose and benefits of an air gapped computer; and	System Administration Practices
(13) Cybersecurity skills. The student demonstrates necessary steps to maintain user access on the system. The student is expected to:	(E) explain how hashes and checksums may be used to validate the integrity of transferred data.	System Administration Practices
(14) Cybersecurity skills. The student explores the field of digital forensics. The student is expected to:	(B) identify the role of chain of custody in digital forensics;	Digital Forensics Basics - Chain of Custody Process
(14) Cybersecurity skills. The student explores the field of digital forensics. The student is expected to:	(E) identify information that can be recovered from digital forensics investigations such as metadata and event logs; and	Digital Forensics Basics - Digital Forensics Investigations
(14) Cybersecurity skills. The student explores the field of digital forensics. The student is expected to:	(F) analyze the purpose of event logs and identify suspicious activity.	Digital Forensics Basics - Digital Forensics Investigations

Foundations of Cybersecurity (Proc 24) Pre-Test/Post-Test TEKS Blueprint

Knowledge & Skills Statement	Student Expectation	iCEV Lesson Title
(15) Cybersecurity skills. The student explores the operations of cryptography. The student is expected to:	(A) explain the purpose of cryptography and encrypting data;	Cryptography Basics - Purpose of Cryptography
(15) Cybersecurity skills. The student explores the operations of cryptography. The student is expected to:	(C) review and explain simple cryptography methods such as shift cipher and substitution cipher	Cryptography Basics - Cryptography Methods
(15) Cybersecurity skills. The student explores the operations of cryptography. The student is expected to:	(E) compare and contrast symmetric and asymmetric encryption.	Cryptography Basics - Cryptography Methods
(16) Vulnerabilities, threats, and attacks. The student understands vulnerabilities, threats, and attacks. The student is expected to:	(A) explain how computer vulnerabilities leave systems open to cyberattacks;	Cyber Vulnerabilities, Threats and Attacks
(16) Vulnerabilities, threats, and attacks. The student understands vulnerabilities, threats, and attacks. The student is expected to:	(B) explain how users are the most common vehicle for compromising a system at the application level;	Cyber Vulnerabilities, Threats and Attacks
(16) Vulnerabilities, threats, and attacks. The student understands vulnerabilities, threats, and attacks. The student is expected to:	(E) define and describe cyberattacks, including man-in-the middle, distributed denial of service, spoofing, and back door attacks;	Cyber Vulnerabilities, Threats and Attacks
(17) Vulnerabilities, threats, and attacks. The student evaluates the vulnerabilities of networks. The student is expected to:	(A) compare vulnerabilities associated with connecting devices to public and private networks;	Network Vulnerabilities
(17) Vulnerabilities, threats, and attacks. The student evaluates the vulnerabilities of networks. The student is expected to:	(C) compare and contrast protocols such as HTTP versus HTTPS;	Network Vulnerabilities
(17) Vulnerabilities, threats, and attacks. The student evaluates the vulnerabilities of networks. The student is expected to:	(D) debate the broadcasting or hiding of a wireless service set identifier (SSID); and	Network Vulnerabilities
(17) Vulnerabilities, threats, and attacks. The student evaluates the vulnerabilities of networks. The student is expected to:	(E) research and discuss threats such as mandatory access control (MAC) spoofing and packet sniffing.	Network Vulnerabilities
(18) Vulnerabilities, threats, and attacks. The student analyzes threats to computer applications. The student is expected to:	(C) explain the purpose and function of vulnerability scanners;	Threats to Computer Applications
(19) Risk assessment. The student understands risk and how risk assessment and risk management defend against attacks. The student is expected to:	(A) define commonly used risk assessment terms, including risk, asset, and inventory;	Assessing Cybersecurity Risk - Assessing Cybersecurity Risk
(19) Risk assessment. The student understands risk and how risk assessment and risk management defend against attacks. The student is expected to:	(C) compare and contrast risks based on an industry accepted rubric or metric such as Risk Assessment Matrix.	Assessing Cybersecurity Risk - Assessing Cybersecurity Risk