This document is intended to help teachers evaluate the CyberStart America learning platform for classroom use in Foundations of Cybersecurity course. The matrices show connections between the *Texas Knowledge and Skills (TEKS)* and the CyberStart game's three "bases.

**Learn more about the CyberStart program at:**
**https://cyberstartamerica.org**

# CYBERSTART AMERICA IN TEXAS

## A Crosswalk between CyberStart America Challenges and the Texas Course: Foundations of Cybersecurity


This document was developed by WeTeach_Cyber, EPIC, at the Texas Advanced Computing Center at The University of Texas at Austin and the CyberStart America Texas Taskforce.

## §127.792 Foundations of Cybersecurity

| TEKS | HQ Base | Moon Base | Forensics Base |
|---|---|---|---|
| **1 Employability skills. The student demonstrates necessary skills for career development and successful completion of course outcomes. The student is expected to:** | | | |
| a. identify and demonstrate employable work behaviors such as regular attendance, punctuality, maintenance of a professional work environment, and effective written and verbal communication | | | |
| b. identify and demonstrate positive personal qualities such as authenticity, resilience, initiative, and a willingness to learn new knowledge and skills | X | X | X |
| c. solve problems and think critically | X | X | X |
| d. demonstrate leadership skills and function effectively as a team member | | | |
| e. demonstrate an understanding of ethical and legal responsibilities and ramifications in relation to the field of cybersecurity | | | |
| **2. Professional awareness. The student identifies various employment opportunities and requirements in the cybersecurity field. The student is expected to** | | | |
| a. identify job and internship opportunities and accompanying job duties and tasks | | | |
| b. research careers in cybersecurity and information security and develop professional profiles that match education and job skills required for obtaining a job in both the public and private sectors | X | X | X |
| c. identify and discuss certifications for cybersecurity-related careers | | | |
| d. explain the different types of services and roles found within a cybersecurity functional area such as a security operations center (SOC). | | | |
| **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:** | | | |
| a. demonstrate and advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers | X | X | X |
| 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) | | | |
| c. investigate and analyze noteworthy incidents or events regarding cybersecurity | X | X | X |
| d. communicate an understanding of ethical and legal behavior when presented with various scenarios related to cybersecurity activities | X | X | X |
| e. define and identify tactics used in an incident such as social engineering, malware, denial of service, spoofing, and data vandalism | X | X | X |

| TEKS | HQ Base | Moon Base | Forensics Base |
|---|---|---|---|
| f. identify and use appropriate methods for citing sources | | | |
| **4 Ethics and laws. The student differentiates between ethical and malicious hacking. The student is expected to:** | | | |
| a. identify motivations and perspectives for hacking | | | |
| b. distinguish between types of threat actors such as hacktivists, criminals, state-sponsored actors, and foreign governments | | | |
| c. identify and describe the impact of cyberattacks on the global community, society, and individuals | | | |
| d. differentiate between industry terminology for types of hackers such as black hats, white hats, and gray hat | | | |
| e. demonstrate an understanding of ethical and legal responsibilities and ramifications in relation to the field of cybersecurity | | | |
| **5. Ethics and laws. The student identifies and defines cyberterrorism and counterterrorism. The student is expected to:** | | | |
| a. define cyberterrorism, state-sponsored cyberterrorism, and hacktivism | | | |
| b. compare and contrast physical terrorism and cyberterrorism, including domestic and foreign actors | | | |
| c. define and explain intelligence gathering | | | |
| d. explain the role of cyber defense in protecting national interests and corporations | | | |
| e. explain the role of cyber defense in society and the global economy | | | |
| f. explain the importance of protecting public infrastructures such as electrical power grids, water systems, pipelines, transportation, and power generation facilities from cyberterrorism | | | |
| **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:** | | | |
| a. identify and understand the nature and value of privacy | | | |
| b. analyze the positive and negative implications of a digital footprint and the maintenance and monitoring of an online presence | | | |
| c. discuss the role and impact of technology on privacy | | | |
| d. identify the signs, emotional effects, and legal consequences of cyberbullying and cyberstalking | | | |
| e identify and discuss effective ways to deter and report cyberbullying | | | |

| TEKS | HQ Base | Moon Base | Forensics Base |
|---|---|---|---|
| **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) | | | |
| b. evaluate the risks and benefits of sharing PII | | | |
| c. describe the impact of granting applications unnecessary permissions such as mobile devices accessing camera and contacts | | | |
| d. describe the risks of granting third parties access to personal and proprietary data on social media and systems | | | |
| 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 | | | |
| **8. Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:** | | | |
| a. define cybersecurity and information security | X | X | X |
| b. identify basic risk management and risk assessment principles related to cybersecurity threats and vulnerabilities, including the Zero Trust model | | | |
| c. explain the fundamental concepts of confidentiality, integrity, and availability (CIA triad) | X | X | X |
| d. describe the trade-offs between convenience and security | | | |
| e. identify and analyze cybersecurity breaches and incident responses | | X | X |
| f. identify and analyze security challenges in domains such as physical, network, cloud, and web | X | | |
| g. define and discuss challenges faced by cybersecurity professionals such as internal and external threats: | X | X | X |
| h. identify indicators of compromise such as common risks, warning signs, and alerts of compromised systems | | | |
| i. explore and discuss the vulnerabilities of network-connected devices such as Internet of Things (IoT) | | | |
| j. use appropriate cybersecurity terminology | | | |
| k. explain the concept of penetration testing, including tools and techniques | | | |
| l. explore and identify common industry frameworks such as MITRE ATT&CK™, MITRE Engage ™, and Cyber Kill Chain, and the Diamond Model | | | |

| TEKS | HQ Base | Moon Base | Forensics Base |
|---|---|---|---|
| **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 | | X | X |
| b. identify the transmission and function of malware such as trojan horses, worms, and viruses | X | X | X |
| c. discuss the impact of malware and the model of "as a service" | | | |
| d. explain the role of reverse engineering for the detection of malware and viruses | | X | X |
| e. describe free and commercial antivirus and anti-malware software also known as Endpoint Detection and Response software | | | |
| **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 | | | |
| b. use basic system administration privileges | X | X | |
| c. explain the importance of patching operating systems | | | |
| d. explain the importance of software updates | | | |
| e. describe standard practices to configure system services | | X | X |
| f. explain the importance of backup files | | | X |
| g. research and explain standard practices for securing computers, networks, and operating systems, including the concept of least privilege | | X | |
| h. identify vulnerabilities caused by a lack of cybersecurity awareness and training such as weaknesses posed by individuals within an organization | X | X | X |
| **11. Cybersecurity skills. The student understands basic network operations. The student is expected to:** | | | |
| a. identify basic network devices, including routers and switches | | X | |
| b. define network addressing | | | |
| c. analyze incoming and outgoing rules for traffic passing through a firewall; | | X | |
| 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) | X | X | X |

| TEKS | HQ Base | Moon Base | Forensics Base |
|---|---|---|---|
| e. identify commonly exploited ports and services, including ports 20 and 21 (File Transfer Protocol/ftp), port 23 (telnet protocol), and port 3389 (Remote Desktop Protocol/rdp) | X | X | X |
| f. identify common tools for monitoring ports and network traffic | | X | X |
| **12. Cybersecurity skills. The student identifies standard practices of system administration. The student is expected to:** | | | |
| a. define what constitutes a secure password; | | | |
| b. create a secure password policy, including length, complexity, account lockout, and rotation | | | |
| c. identify methods of password cracking such as brute force and dictionary attacks | X | X | X |
| d. examine and configure security options to allow and restrict access based on user roles. | | | |
| **13. Cybersecurity skills. The student demonstrates necessary steps to maintain user access on the system. The student is expected to:** | | | |
| a. identify different types of user accounts and groups on an operating system; | | X | X |
| b. explain the fundamental concepts and standard practices related to access control, including authentication, authorization, and auditing | X | | X |
| c. compare methods for single- and multi-factor authentication such as passwords, biometrics, personal identification numbers (PINs), secure tokens, and other passwordless authentication methods | | | |
| d. define and explain the purpose and benefits of an air-gapped computer | | | |
| e. explain how hashes and checksums may be used to validate the integrity of transferred data | X | X | X |
| **14. Cybersecurity skills. The student explores the field of digital forensics. The student is expected to:** | | | |
| a. explain the importance of digital forensics to organizations, private citizens, and the public sector | | | |
| b. identify the role of chain of custody in digital forensics | | X | X |
| c. explain the four steps of the forensics process, including collection, examination, analysis, and reporting | | X | X |
| d. identify when a digital forensics investigation is necessary | | | |
| e. identify information that can be recovered from digital forensics investigations such as metadata and event logs | | | |
| f. analyze the purpose of event logs and identify suspicious activity | | | |

| TEKS | HQ Base | Moon Base | Forensics Base |
|---|---|---|---|
| **15 Cybersecurity skills. The student explores the operations of cryptography. The student is expected to:** | | | |
| a. explain the purpose of cryptography and encrypting data | X | X | X |
| b. research historical uses of cryptography | | | |
| c. review and explain simple cryptography methods such as shift cipher and substitution cipher | X | X | X |
| d. define and explain public key encryption | X | X | X |
| e. compare and contrast symmetric and asymmetric encryption | X | X | X |
| **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 | X | X | X |
| b. explain how users are the most common vehicle for compromising a system at the application level | | | |
| c. define and describe vulnerability, payload, exploit, port scanning, and packet sniffing | X | X | X |
| d. identify internal threats to systems such as logic bombs and insider threats | | | |
| e. define and describe cyberattacks, including man-in-the-middle, distributed denial of service, spoofing, and back-door attacks | | | X |
| f. differentiate types of social engineering techniques such as phishing; web links in email, instant messaging, social media, and other online communication with malicious links; shoulder surfing; and dumpster diving | X | | |
| g. identify various types of application-specific attacks such as cross-site scripting and injection attacks | X | X | X |
| **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 | | | |
| b. explain device vulnerabilities and security solutions on networks such as supply chain security and counterfeit products | | | |
| c. compare and contrast protocols such as HTTP versus HTTPS | | | |
| d. debate the broadcasting or hiding of a wireless service set identifier (SSID) | | | |
| e. research and discuss threats such as mandatory access control (MAC) spoofing and packet sniffing | | X | |

| TEKS | HQ Base | Moon Base | Forensics Base |
|---|---|---|---|
| **18. Vulnerabilities, threats, and attacks. The student analyzes threats to computer applications. The student is expected to:** | | | |
| a. define application security | | | X |
| b. identify methods of application security such as secure development policies and practices | | | |
| c. explain the purpose and function of vulnerability scanners | | | |
| d. explain how coding errors may create system vulnerabilities such as buffer overflows and lack of input validation | | X | X |
| e. analyze the risks of distributing insecure programs | | | |
| **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 | | | |
| b. identify risk management strategies, including acceptance, avoidance, transference, and mitigation | | | |
| c. compare and contrast risks based on an industry accepted rubric or metric such as Risk Assessment Matrix | | | |