eDynamic Learing Course Title: Cybersecurity 1a / 1b

State: TX
State Course Title: Principles of Cybersecurity
State Course Code: N/A
State Standards: Innovative Course
Date of Standards: N/A

TEKS	Course	Unit Name(s)	Lesson(s) Numbers
(1) The student demonstrates necessary skills for career development and successful completion of course outcomes.			
(A) identify and demonstrate positive work behaviors such as regular attendance, punctuality, maintenance of a clean work environment, and professional written and spoken communication;	Cybersecurity 1A and 1B	All units	All lessons
(B) identify and demonstrate positive personal qualities such as resilience, initiative, and a willingness to learn new knowledge and skills;	Cybersecurity 1A and 1B	All units	All lessons
(C) employ effective reading and writing skills;	Cybersecurity 1A and 1B	All units	All lessons
(D) solve problems and think critically;	Cybersecurity 1A and 1B	All units	All lessons
(E) demonstrate leadership skills and function effectively as a team member; and	Cybersecurity 1B	Unit 8: Cybersecurity Careers	Unit 8 Lab
(F) demonstrate an understanding of ethical and legal responsibilities in relation to the field of information technology.	Cybersecurity 1B	Unit 2: Laws, Ethics, and Digital Boundaries	Lessons 1 and 2
(2) The student identifies various employment opportunities and skill competitions in the cybersecurity field.			
(A) identify job opportunities and accompanying job duties and tasks;	Cybersecurity 1A	Unit 8: Trends and Challenges	Lesson 1
(B) research careers in cybersecurity along with the education and job skills required for obtaining a job in cybersecurity in both the public and private sector;	Cybersecurity 1A	Unit 8: Trends and Challenges	Lesson 1
(C) explain the functions of resumes and portfolios in the cybersecurity field;	Cybersecurity 1B	Unit 8: Cybersecurity Careers	Lesson 2
(D) identify cybersecurity mental sports such as CyberPatriot, CyberLympics and Panoply; and	Cybersecurity 1B	Unit 8: Cybersecurity Careers	Lesson 3

(E) identify and discuss cybersecurity certifications for cybersecurity related careers.	Cybersecurity 1A	Unit 8: Trends and Challenges	Lesson 1
(3) The student understands current ethical and legal standards, rights and restrictions governing technology, technology systems, digital media and information technology, and the use of social media in the context of today's society.			
(A) demonstrate and advocate for ethical and legal behaviors both online and offline among peers, family, and community;	Cybersecurity 1B	Unit 2: Laws, Ethics, and Digital Boundaries	Lessons 1 and 2
(B) identify and define unethical practices such as hacking, phishing, social engineering, online piracy, spoofing, and data vandalism;	Cybersecurity 1B	Unit 1: Cybersecurity Threats	Lesson 3
(C) demonstrate ethical and legal behavior when confronted with usage dilemmas while using technology, technology systems, digital media, and information technology	Cybersecurity 1B	Unit 2: Laws, Ethics, and Digital Boundaries	Lessons 1 and 2
(4) The student understands and demonstrates the social responsibility of end users regarding the significant issues relating to digital technology and privacy, safety, and cyberbullying as it relates to cybersecurity.			
(A) identify and understand the nature and value of privacy;	Cybersecurity 1B	Unit 2: Laws, Ethics, and Digital Boundaries	Lesson 3
(B) evaluate arguments related to the impact of emerging technologies on privacy;	Cybersecurity 1B	Unit 2: Laws, Ethics, and Digital Boundaries	Lesson 3
(C) discuss the role of privacy in the student's lives and the impact of technology on the student's privacy;	Cybersecurity 1B	Unit 2: Laws, Ethics, and Digital Boundaries	Lesson 3
(D) identify the importance of online identity management and monitoring;	Cybersecurity 1B	Unit 4: Cyber Safety	Lessons 2-4
(E) identify the signs, emotional effects, and the legal consequences of cyberbullying; and	Cybersecurity 1B	Unit 2: Laws, Ethics, and Digital Boundaries	Unit 2 Lab
(F) identify and discuss some effective ways to prevent, fight, and stop cyberbullying.	Cybersecurity 1B	Unit 4: Cyber Safety	Lesson 3
(5) The student identifies the consequences of practicing ethical hacking versus malicious hacking.			
(A) identify motivations for hacking;	Cybersecurity 1B	Unit 1: Cybersecurity Threats	Lesson 2
(B) identify and describe the impact of cyber-attacks on the global economy, society, and individuals;	Cybersecurity 1B	Unit 1: Cybersecurity Threats	Lesson 3
(C) distinguish between a cyber defender and a cyber attacker;	Cybersecurity 1B	Unit 1: Cybersecurity Threats	Lesson 2
(D) differentiate types of hackers based on behaviors such as black-hats, white-hats, and gray-hats hackers;	Cybersecurity 1B	Unit 1: Cybersecurity Threats	Lesson 2
(E) determine possible outcomes and legal ramifications of ethical versus malicious hacking practices; and	Cybersecurity 1B	Unit 1: Cybersecurity Threats	Lesson 2
(F) debate whether it is ever appropriate to engage in ethical or malicious hacking practice.	Cybersecurity 1B	Unit 1: Cybersecurity Threats	Lesson 2
(6) The student understands basic cybersecurity concepts and definitions.			
(A) define information security and cyber defense;	Cybersecurity 1A and 1B	All units	All lessons
(B) identify basic risk management and risk assessment principles relating to cybersecurity threats and vulnerabilities;	Cybersecurity 1B	Unit 5: Personal Cybersecurity Inventory	Lesson 3
(C) explain the fundamental concepts of Confidentiality, Integrity, and Availability also known as the CIA triad;	Cybersecurity 1A	Unit 1: Basics of Cybersecurity	Lesson 3

(D) identify and analyze current security concerns and recent cybersecurity breaches;	Cybersecurity 1B	Unit 5: Personal Cybersecurity Inventory	Lesson 3
(E) define and discuss challenges faced by information security professionals;	Cybersecurity 1A and 1B	All units	All lessons
(F) identify common risks, alerts, and warning signs of compromised computer and network systems;	Cybersecurity 1B	Unit 7: Incident Response, Investigations, and Digital Forensics	Lesson 1
G) understand and explore the Internet of Things (IoT) and the vulnerability of network connected devices; and	Cybersecurity 1A	Unit 2: Computers and Operating Systems	Lesson 1
(H) create an academic vocabulary using appropriate cybersecurity terminology.	Cybersecurity 1A and 1B	All units	All lessons
(7) The student understands and defines hacking.			
(A) establish the proper definition of a hacker	Cybersecurity 1B	Unit 1: Cybersecurity Threats	Lesson 2
(8) The student identifies and defines cyber terrorism and counterterrorism.			
(A) define and explain counterterrorism;	Cybersecurity 1A	Unit 8: Trends and Challenges	Lesson 1
(B) compare and contrast physical terrorism and cyber terrorism;	Cybersecurity 1A	Unit 8: Trends and Challenges	Lesson 1
(C) construct standardized definitions of terrorism and cyber terrorism by interacting with multiple sources that provide examples and working definitions, including private and government agencies;	Cybersecurity 1A	Unit 8: Trends and Challenges	Lesson 1
(D) identify the role of cyber defenders in protecting nations and corporations from physical and cyber terrorism, including hacktivism and state-sponsored terrorism;	Cybersecurity 1A	Unit 8: Trends and Challenges	Lesson 1
(E) identify the role of cyber defense in 21st century society and global economy; and	Cybersecurity 1A	Unit 8: Trends and Challenges	Lesson 1
(F) explain the importance of protecting important public infrastructures such as electrical power grids, public water, pipeline safety, railroads, sewer systems, and nuclear plants from cyber-attack.	Cybersecurity 1A	Unit 8: Trends and Challenges	Lesson 1
(9) The student understands and explains various types of malicious software. The student is expected to			
(A) define malicious software;	Cybersecurity 1A	Unit 2: Computers and Operating Systems	Lesson 4
(B) identify characteristics and traits of malicious software, including transmission and function;	Cybersecurity 1A	Unit 2: Computers and Operating Systems	Lesson 4
(C) describe various types of malicious software, including Trojans, worms, and viruses;	Cybersecurity 1A	Unit 2: Computers and Operating Systems	Lesson 4
(D) discuss how malicious software has shaped the global cybersecurity landscape and its future impact; and	Cybersecurity 1A	Unit 1: Basics of Cybersecurity	Lesson 2
(E) identify and critique delivery techniques for various types of malware such as spoofing, email attachment, and end user error.	Cybersecurity 1A	Unit 2: Computers and Operating Systems	Lesson 4

(10) The student identifies methods for countering malicious software and protecting computer systems.			
(A) identify methods for manually and automatically removing malicious software from compromised computer systems, such as a virus or a trojan using anti-virus software or anti-malware programs;	Cybersecurity 1A	Unit 2: Computers and Operating Systems	Lesson 4
(B) evaluate and compare free and commercial versions of the same antivirus software; and	Cybersecurity 1A	Unit 2: Computers and Operating Systems	Lesson 4
(C) evaluate anti-malware programs for efficacy.	Cybersecurity 1A	Unit 2: Computers and Operating Systems	Lesson 4
(11) The student understands information security vulnerabilities, threats, and computer attacks.			
(A) identify and define cyber-attacks and computer vulnerabilities;	Cybersecurity 1B	Unit 4: Cyber Safety	Lesson 1
(B) explore computer security vulnerabilities and different approaches to cybersecurity;	Cybersecurity 1A and 1B	All units	All lessons
(C) explain how computer vulnerabilities leave systems open to cyber-attacks;	Cybersecurity 1A	Unit 2: Computers and Operating Systems	Lesson 2
(D) identify emerging threats to computer systems due to programmer error as well as malicious hackers such as back door attacks;	Cybersecurity 1B	Unit 1: Cybersecurity Threats	Lesson 3
(E) identify and differentiate attacks using malware;	Cybersecurity 1A	Unit 2: Computers and Operating Systems	Lesson 4
(F) identify and differentiate different types of social engineering attacks such as shoulder surfing and dumpster diving;	Cybersecurity 1A	Unit 8: Trends and Challenges	Lesson 2
(G) identify and classify various types of attacks on wireless systems; and	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 3
(H) identify various types of application specific attacks.	Cybersecurity 1B	Unit 3: Black Hats	Lesson 4
(12) The student understands, identifies, and explains the strategies and techniques of both ethical and malicious hackers.			
(A) identify internal and external threats to computer systems;	Cybersecurity 1B	Unit 1: Cybersecurity Threats	Lesson 1
(B) identify and analyze different types of cyber-attack signatures;	Cybersecurity 1B	Unit 3: Black Hats	Lesson 4
(C) identify the capabilities of vulnerability assessment tools, including open source tools; and	Cybersecurity 1B	Unit 3: Black Hats	Lesson 2
(D) explain the concept of penetration testing, tools, and techniques.	Cybersecurity 1B	Unit 6: White Hat Hackers	Lesson 2
(13) The student understands and demonstrates knowledge of system hardening techniques and strategies to prevent a computer system from being compromised by known vulnerabilities.			
(A) explain the importance of patched operating systems as it relates to securing a computer system;	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 1
(B) demonstrate basic use of system administration in control panel;	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 1
(C) activate and explain the importance of automatic updates;	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 1
(D) analyze and configure active and inactive services;	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 1

(E) explain the importance of creating a restore point and backup files; and	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 1
(F) research and understand best practices for securing computers, networks, and operating systems.	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 1
(14) The student demonstrates how to properly configure a computer network firewall.			
(A) identify and explain the basic function and purpose of network devices and technologies, including firewall and switches;	Cybersecurity 1A	Unit 4: Network Security	Lesson 2
(B) analyze and establish incoming and outgoing rules for traffic passing through a computer network firewall;			
(C) identify necessary and commonly used default ports and protocols according to number and service provided, such as Port 22 (ssh), Port 80 (http), and Port 443 (https);	Cybersecurity 1A	Unit 3: Networking Fundamentals	Lab
(D) identify common tools for monitoring ports and network traffic.	Cybersecurity 1A	Unit 4: Network Security	Lesson 2
(15) The student identifies best practices for creating secure local security policy.			
(A) establish secure password policy based on industry defined best practices;	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 1
(B) define what constitutes a complex and secure password;	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 1
(C) identify methods of attacking passwords, such as brute force and dictionary attacks;	Cybersecurity 1B	Unit 3: Black Hats	Lesson 2
(D) identify available user tools for the creation of complex secure passwords;	Cybersecurity 1B	Unit 4: Cyber Safety	Unit 4 Lab
(E) analyze event logs for suspicious behavior; and	Cybersecurity 1A	Unit 5: Access Control	Unit 5 Activity
(F) examine and correctly configure the security options of a computer to ensure only authorized users have access.	Cybersecurity 1A	Unit 5: Access Control	Unit 5 Lab
(16) The student demonstrates necessary steps to maintain confidentiality and integrity of data on the computer system.			
(A) identify the different types of user accounts and groups on an operating system;	Cybersecurity 1A	Unit 5: Access Control	Lesson 2
(B) establish policy to determine which users should have administrative rights on a computer system with role-based access control;	Cybersecurity 1A	Unit 5: Access Control	Lesson 3
(C) explain the fundamental concepts and best practices related to authentication, authorization, and access control;	Cybersecurity 1A	Unit 5: Access Control	Lesson 3
(D) identify multiple methods for authentication such as passwords, biometric verification, and security tokens;	Cybersecurity 1A	Unit 5: Access Control	Lesson 3
(E) define and explain the purpose of an air -gapped computer;	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 1
(F) define and explain how checksums may be used to validate the integrity of transferred data;	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 4
(G) explain the importance of encrypting data to ensure integrity and to prevent unauthorized access	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 3

(17) The student evaluates the potential risks and benefits of unsecured wireless networks.			
(A) identify the common risks associated with connecting portable devices to a variety of wireless networks such as public and home Wi-Fi;	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 1
(B) determine and evaluate the potential negative consequences of connecting a portable device to an unsecured wireless network;	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 1
(C) explain portable device vulnerabilities and wireless security solutions;	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 1
(D) compare WEP and WPA 2 encryption;	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 1
(E) justify the purpose of broadcasting or hiding your wireless SSID; and	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 1
(F) research and discuss wireless attacks, including Bluetooth, MAC spoofing, war driving, eavesdropping, and man in the middle.	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 3
(18) The student analyzes common threats to computer applications.			
(A) define application security;	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 2
(B) identify methods of application security such as application development security, application hardening, and patch management;	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 2
(C) analyze web links in email, instant messaging, social media, and other online communication for spoofing or malicious links;	Cybersecurity 1B	Unit 4: Cyber Safety	Lesson 2
(D) explain how users are the most common vehicle for compromising a system at the application level;	Cybersecurity 1B	Unit 4: Cyber Safety	Lesson 1
(E) demonstrate how to properly configure applications for automatic updates;	Cybersecurity 1B	Unit 4: Cyber Safety	Lesson 1
(F) research and explain ways to improve application security;	Cybersecurity 1A	Unit 7: Protecting Data	Lesson 2
(G) identify web application vulnerability scanners and their function; and	Cybersecurity 1B	Unit 3: Black Hats	Lesson 2
(H) explain how coding errors can create vulnerabilities in the security of the application.	Cybersecurity 1B	Unit 3: Black Hats	Lesson 2
(19) The student explores possible exploits in mobile applications.			
(A) explain how changing the firmware to jail break a mobile devices can increase the potential for new exploits;	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 3
(B) describe how users often give mobile applications unnecessary permissions which facilitates fraudulent activities; and	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 3
(C) identify how client-side restrictions such as device security attributes, user location, and the security of the network connection can mitigate exploits on mobile devices.	Cybersecurity 1A	Unit 6: Mobile Devices and Cloud Computing	Lesson 3

(20) The student explores the field of computer forensics.			
(A) define computer forensics;	Cybersecurity 1B	Unit 7: Incident Response, Investigations, and Digital Forensics	Lesson 2
(B) explain the importance of computer forensics to law enforcement and corporations and its implications for individuals;	Cybersecurity 1B	Unit 7: Incident Response, Investigations, and Digital Forensics	Lesson 2
(C) identify and explain the four steps of the forensics process, including collection, examination, analysis, and reporting;	Cybersecurity 1B	Unit 7: Incident Response, Investigations, and Digital Forensics	Lesson 2
(D) identify under which circumstances a computer forensics investigation is necessary; and	Cybersecurity 1B	Unit 7: Incident Response, Investigations, and Digital Forensics	Lesson 1
(E) identify what types of information can be recovered in computer forensics investigations.	Cybersecurity 1B	Unit 7: Incident Response, Investigations, and Digital Forensics	Lesson 2