eDynamic Learning Course Title: Network Security Fundamentals 1a / 1b

State: TX
State Course Title: Principles of Cybersecurity
State Course Code: 1302810
State Standards: Principles of Cybersecurity

TEKS	Course Title. (a or b), if applicable, e.g. Game Design 1a	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;	Network Security Fundamentals 1b	Unit 5: Application Security	Activity
(B) identify and demonstrate positive personal qualities such as resilience, initiative, and a willingness to learn new knowledge and skills;	Network Security Fundamentals 1b	Unit 8: Careers and Education in Cybersecurity	Lessons 2-4
(C) employ effective reading and writing skills;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 2
(D) solve problems and think critically;	Network Security Fundamentals 1a	Unit 7: A Closer Look at Malware	Lessons 2-4
(E) demonstrate leadership skills and function effectively as a team member; and	Network Security Fundamentals 1b	Unit 5: Application Security	Activity 2
(F) demonstrate an understanding of ethical and legal responsibilities in relation to the field of information technology.	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Activity
(2) The student identifies various employment opportunities and skill competitions in the cybersecurity field.			
(A) identify job opportunities and accompanying job duties and tasks;	Network Security Fundamentals 1b	Unit 8: Careers and Education in Cybersecurity	Lessons 1, 2
(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;	Network Security Fundamentals 1b	Unit 8: Careers and Education in Cybersecurity	Lessons 1-5
(C) explain the functions of resumes and portfolios in the cybersecurity field;	Network Security Fundamentals 1b	Unit 8: Careers and Education in Cybersecurity	Lessons 3-5
(D) identify cybersecurity mental sports such as CyberPatriot, CyberLympics and Panoply; and	Network Security Fundamentals 1b	Unit 8: Careers and Education in Cybersecurity	Lessons 2-4
(E) identify and discuss cybersecurity certifications for cybersecurity related careers.	Network Security Fundamentals 1b	Unit 8: Careers and Education in Cybersecurity	Lessons 3, 4

(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;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(B) identify and define unethical practices such as hacking, phishing, social engineering, online piracy, spoofing, and data vandalism;	Network Security Fundamentals 1b	Unit 5: Application Security	Activity
(C) demonstrate ethical and legal behavior when confronted with usage dilemmas while using technology, technology systems, digital media, and information technology; and	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Activity
(D) apply citation rules for various sources and mediums.	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 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;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(B) evaluate arguments related to the impact of emerging technologies on privacy;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(C) discuss the role of privacy in the student's lives and the impact of technology on the student's privacy;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(D) identify the importance of online identity management and monitoring;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(E) identify the signs, emotional effects, and the legal consequences of cyberbullying; and	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(F) identify and discuss some effective ways to prevent, fight, and stop cyberbullying.	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(5) The student identifies the consequences of practicing ethical hacking versus malicious hacking.			
(A) identify motivations for hacking;	Network Security Fundamentals 1b	Unit 4: Managing Users and Permissions	Lesson 3
(B) identify and describe the impact of cyber-attacks on the global economy, society, and individuals;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(C) distinguish between a cyber defender and a cyber attacker;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3

(D) differentiate types of hackers based on behaviors such as black-hats, white-hats, and gray-hats hackers;	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 5
(E) determine possible outcomes and legal ramifications of ethical versus malicious hacking practices; and	Network Security Fundamentals 1a	Unit 7: A Closer Look at Malware	Lesson 1
(F) debate whether it is ever appropriate to engage in ethical or malicious hacking practice.	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(6) The student understands basic cybersecurity concepts and definitions.			
(A) define information security and cyber defense;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(B) identify basic risk management and risk assessment principles relating to cybersecurity threats and vulnerabilities;	Network Security Fundamentals 1a	Unit 1: Security (and What Threatens it)	Activity
(C) explain the fundamental concepts of Confidentiality, Integrity, and Availability also known as the CIA triad;	Network Security Fundamentals 1a	Unit 2: Fundamentals Concepts of Cybersecurity	Lesson 1
(D) identify and analyze current security concerns and recent cybersecurity breaches;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Activity
(E) define and discuss challenges faced by information security professionals;	Network Security Fundamentals 1a	Unit 2: Fundamentals Concepts of Cybersecurity	Lesson 2
(F) identify common risks, alerts, and warning signs of compromised computer and network systems;	Network Security Fundamentals 1a	Unit 1: Security (and What Threatens it)	Activity
(G) understand and explore the Internet of Things (IoT) and the vulnerability of network connected devices; and	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Activity
(H) create an academic vocabulary using appropriate cybersecurity terminology.	Network Security Fundamentals 1b	Unit 8: Careers and Education in Cybersecurity	Lessons 2-4
(7) The student understands and defines hacking.			
(A) establish the proper definition of a hacker;	Network Security Fundamentals 1a	Unit 7: A Closer Look at Malware	Lesson 1
(B) identify commonly used hacking tools; and	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 2
(C) define vulnerability, exploit, port scanning, network sniffing, packet sniffing, and payload as they relate to hacking.	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 2
(8) The student identifies and defines cyber terrorism and counterterrorism.			
(A) define and explain counterterrorism;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3

(B) compare and contrast physical terrorism and cyber terrorism;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(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;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(D) identify the role of cyber defenders in protecting nations and corporations from physical and cyber terrorism, including hacktivism and state-sponsored terrorism;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(E) identify the role of cyber defense in 21st century society and global economy; and	Network Security Fundamentals 1b	Unit 3: Operating System Administration	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.	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lessons 2-4
(9) The student understands and explains various types of malicious software.			
(A) define malicious software;	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 2
(B) identify characteristics and traits of malicious software, including transmission and function;	Network Security Fundamentals 1a	Unit 3: Building a Network	Lessons 2-4
(C) describe various types of malicious software, including Trojans, worms, and viruses;	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 2
(D) discuss how malicious software has shaped the global cybersecurity landscape and its future impact; and	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(E) identify and critique delivery techniques for various types of malware such as spoofing, email attachment, and end user error.	Network Security Fundamentals 1a	Unit 7: A Closer Look at Malware	Lessons 2-4
(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 antivirus software or anti-malware programs;	Network Security Fundamentals 1a	Unit 7: A Closer Look at Malware	Lessons 2-4
(B) evaluate and compare free and commercial versions of the same antivirus software; and	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 2
(C) evaluate anti-malware programs for efficacy.	Network Security Fundamentals 1a	Unit 7: A Closer Look at Malware	Lesson 2
(11) The student understands information security vulnerabilities, threats, and computer attacks.			
(A) identify and define cyber-attacks and computer vulnerabilities;	Network Security Fundamentals 1a	Unit 5: Building Our Defenses	Lesson 3

(B) explore computer security vulnerabilities and different approaches to cybersecurity;	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 2
(C) explain how computer vulnerabilities leave systems open to cyber-attacks;	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 2
(D) identify emerging threats to computer systems due to programmer error as well as malicious hackers such as back door attacks;	Network Security Fundamentals 1a	Unit 5: Building Our Defenses	Lesson 3
(E) identify and differentiate attacks using malware;	Network Security Fundamentals 1a	Unit 7: A Closer Look at Malware	Lesson 2
(F) identify and differentiate different types of social engineering attacks such as shoulder surfing and dumpster diving;	Network Security Fundamentals 1b	Unit 5: Application Security	Activity
(G) identify and classify various types of attacks on wireless systems; and	Network Security Fundamentals 1a	Unit 3: Building a Network	Lesson 5
(H) identify various types of application specific attacks.	Network Security Fundamentals 1a	Unit 3: Building a Network	Lesson 5
(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;	Network Security Fundamentals 1a	Unit 5: Building Our Defenses	Lesson 3
(B) identify and analyze different types of cyber-attack signatures;	Network Security Fundamentals 1a	Unit 5: Building Our Defenses	Lesson 3
(C) identify the capabilities of vulnerability assessment tools, including open source tools; and	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 2
(D) explain the concept of penetration testing, tools, and techniques.	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	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;	Network Security Fundamentals 1a	Unit 3: Building a Network	Lesson 5
(B) demonstrate basic use of system administration in control panel;	Network Security Fundamentals 1B	Unit 3: Operating Systems Administration	Lesson 2
(C) activate and explain the importance of automatic updates;	Network Security Fundamentals 1B	Unit 3: Operating Systems Administration	Lesson 2

(D) analyze and configure active and inactive services;	Network Security Fundamentals 1a	Unit 4: Protocols, Services, and Data Transfers	Lesson 2
(E) explain the importance of creating a restore point and backup files; and	Network Security Fundamentals 1b	Unit 2: Cryptology and Cryptography	Lessons 3, 4, 6
(F) research and understand best practices for securing computers, networks, and operating systems.	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Activity
(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;	Network Security Fundamentals 1a	Unit 3: Building a Network	Lesson 5
(B) analyze and establish incoming and outgoing rules for traffic passing through a computer network firewall;	Network Security Fundamentals 1a	Unit 3: Building a Network	Lesson 2, Activity
(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);	Network Security Fundamentals 1a	Unit 4: Protocols, Services, and Data Transfers	Lesson 3
(D) identify and block commonly exploited ports and protocols such as Port 21 (ftp) and Port 23 (telnet); and	Network Security Fundamentals 1a	Unit 4: Protocols, Services, and Data Transfers	Lesson 3
(E) identify common tools for monitoring ports and network traffic.	Network Security Fundamentals 1a	Unit 4: Protocols, Services, and Data Transfers	Lesson 3
(15) The student identifies best practices for creating secure local security policy.			
(A) establish secure password policy based on industry defined best practices;	Network Security Fundamentals 1b	Unit 4: Managing Users and Permissions	Lesson 2
(B) define what constitutes a complex and secure password;	Network Security Fundamentals 1b	Unit 4: Managing Users and Permissions	Lesson 2
(C) identify methods of attacking passwords, such as brute force and dictionary attacks;	Network Security Fundamentals 1b	Unit 4: Managing Users and Permissions	Lesson 3
(D) identify available user tools for the creation of complex secure passwords;	Network Security Fundamentals 1b	Unit 4: Managing Users and Permissions	Lesson 2
(E) implement a secure account lockout policy;	Network Security Fundamentals 1a	Unit 4: Protocols, Services, and Data Transfers	Lesson 5
(F) analyze and correctly configure the audit policy of a computer to create event logs;	Network Security Fundamentals 1b	Unit 1: Computer and Digital Forensics	Lessons 1-5

(G) analyze event logs for suspicious behavior; and	Network Security Fundamentals 1b	Unit 1: Computer and Digital Forensics	Lessons 1-5
(H) examine and correctly configure the security options of a computer to ensure only authorized users have access.	Network Security Fundamentals 1a	Unit 5: Building Our Defenses	Lesson 3
(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;	Network Security Fundamentals 1a	Unit 3: Building a Network	Lesson 5
(B) establish policy to determine which users should have administrative rights on a computer system with role-based access control;	Network Security Fundamentals 1b	Unit 4: Managing Users and Permissions	Lessons 4, 5
(C) explain the fundamental concepts and best practices related to authentication, authorization, and access control;	Network Security Fundamentals 1b	Unit 3: Operating System Administration	Lessons 2-4
(D) identify multiple methods for authentication such as passwords, biometric verification, and security tokens;	Network Security Fundamentals 1a	Unit 4: Protocols, Services, and Data Transfers	Lesson 5
(E) define and explain the purpose of an air-gapped computer;	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lessons 1-5
(F) define and explain how checksums may be used to validate the integrity of transferred data;	Network Security Fundamentals 1b	Unit 2: Cryptology and Cryptography	Lessons 3, 4, 6
(G) explain the importance of encrypting data to ensure integrity and to prevent unauthorized access; and	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 3
(H) identify applications commonly used to intercept data communication over wired and wireless networks.	Network Security Fundamentals 1a	Unit 3: Building a Network	Lesson 2
(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;	Network Security Fundamentals 1a	Unit 5: Building Our Defenses	Lesson 2
(B) determine and evaluate the potential negative consequences of connecting a portable device to an unsecured wireless network	Network Security Fundamentals 1a	Unit 3: Building a Network	Lessons 2-4
(C) explain portable device vulnerabilities and wireless security solutions;	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 2
(D) compare WEP and WPA2 encryption;	Network Security Fundamentals 1a	Unit 5: Building Our Defenses	Lesson 2

(E) justify the purpose of broadcasting or hiding your wireless SSID; and	Network Security Fundamentals 1a	Unit 3: Building a Network	Lessons 2-4
(F) research and discuss wireless attacks, including Bluetooth, MAC spoofing, war driving, eavesdropping, and man in the middle.	Network Security Fundamentals 1a	Unit 5: Building Our Defenses	Lesson 3
(18) The student analyzes common threats to computer applications.			
(A) define application security;	Network Security Fundamentals 1a	Unit 4: Protocols, Services, and Data Transfers	Lesson 5
(B) identify methods of application security such as application development security, application hardening, and patch management;	Network Security Fundamentals 1b	Unit 5: Application Security	Activity
(C) analyze web links in email, instant messaging, social media, and other online communication for spoofing or malicious links;	Network Security Fundamentals 1b	Unit 5: Application Security	Activity
(D) demonstrate knowledge of pop-up and pop-under management;	Network Security Fundamentals 1B	Unit 3: Operating Systems Administration	Lesson 2
(E) explain how users are the most common vehicle for compromising a system at the application level;	Network Security Fundamentals 1b	Unit 5: Application Security	Activity
(F) demonstrate how to properly configure applications for automatic updates;	Network Security Fundamentals 1b	Unit 5: Application Security	Activity
(G) research and explain ways to improve application security;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Activity
(H) identify web application vulnerability scanners and their function; and	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Lesson 2
(I) explain how coding errors can create vulnerabilities in the security of the application.	Network Security Fundamentals 1a	Unit 6: When the Intruders are at the Door	Activity
(19) The student explores possible exploits in mobile applications.			
(A) define rogue application and its use;	Network Security Fundamentals 1b	Unit 6: Mobile Threats and Security	Lessons 1-5
(B) explain how attackers are able to create rogue applications using reverse engineering;	Network Security Fundamentals 1a	Unit 5: Building Our Defenses	Lesson 3
(C) explain how changing the firmware to jail break a mobile devices can increase the potential for new exploits;	Network Security Fundamentals 1a	Unit 4: Protocols, Services, and Data Transfers	Lesson 5
(D) describe how users often give mobile applications unnecessary permissions which facilitates fraudulent activities; and	Network Security Fundamentals 1b	Unit 4: Managing Users and Permissions	Lessons 4, 5

(E) 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.	Network Security Fundamentals 1a	Unit 4: Protocols, Services, and Data Transfers	Lesson 5
(20) The student explores the field of computer forensics.			
(A) define computer forensics;	Network Security Fundamentals 1B	Unit 1: Computer and Digital Forensics	Lessons 1-6
(B) explain the importance of computer forensics to law enforcement and corporations and its implications for individuals;	Network Security Fundamentals 1b	Unit 7: Current Events in Cybersecurity	Lesson 3
(C) identify and explain the four steps of the forensics process, including collection, examination, analysis, and reporting;	Network Security Fundamentals 1B	Unit 1: Computer and Digital Forensics	Lessons 1-6
(D) identify under which circumstances a computer forensics investigation is necessary; and	Network Security Fundamentals 1B	Unit 1: Computer and Digital Forensics	Lessons 1-6
(E) identify what types of information can be recovered in computer forensics investigations.	Network Security Fundamentals 1B	Unit 1: Computer and Digital Forensics	Lessons 1-6