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

State: TX
State Course Title: Foundations of Cybersecurity
State Course Code: 130.428
State Standards: Career and Technical Education (TEKS)
Date of Standards: 2022

TEKS	Course Title (a or b), if applicable, e.g. Game Design 1a	Unit Name(s)	Lesson(s) Numbers
(1) Employability skills. The student demonstrates necessary skills for career development and successful completion of course outcomes.			
(A) identify and demonstrate employable work behaviors such as regular attendance, punctuality, maintenance of a professional work environment, and effective written and verbal communication;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 8: Careers and Education in Cybersecurity	Discussion 1,2
(B) identify and demonstrate positive personal qualities such as authenticity, resilience, initiative, and a willingness to learn new knowledge and skills;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 7: Current Events in Cybersecurity	Activity 2
(C) solve problems and think critically;	Network Security Fundamentals 1a: Introduction	Unit 4: Protocols, Services, and Data Transfer	Activity 1
(D) demonstrate leadership skills and function effectively as a team member;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 1: Computer and Digital Forensics	Activity 1
(E) demonstrate an understanding of ethical and legal responsibilities and ramifications in relation to the field of cybersecurity.	Network Security Fundamentals 1b: Forensics and Permissions	Unit 7: Current Events in Cybersecurity	Activity 2
(2) Employability skills Professional Awareness. The student identifies various employment opportunities and requirements in the cybersecurity field.			
(A) identify job and internship opportunities as well as accompanying duties and tasks;	Network Security Fundamentals 1a: Introduction	Unit 2: Fundamental Concepts of Cybersecurity	Discussion 2
(B) research careers in cybersecurity and information assurance security and develop professional profiles that match along with the education and job skills required for obtaining a job in both the public and private sectors;	Network Security Fundamentals 1a: Introduction	Unit 2: Fundamental Concepts of Cybersecurity	Discussion 2
(C) identify and discuss certifications for cybersecurity-related careers;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 8: Careers and Education in Cybersecurity	Activity 2
(D) research and develop resumes, digital portfolios, or professional profiles in the cybersecurity field. explain the different types of services and roles found within a cybersecurity functional area, such as a security operations center (SOC).	Network Security Fundamentals 1b: Forensics and Permissions	Unit 8: Careers and Education in Cybersecurity	Activity 2
(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.			
(A) demonstrate and advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 1: Computer and Digital Forensics	Lesson 3

(B) investigate and analyze research local, state, national, and international cyber laws such as the PATRIOT Act of 2001, General Data Protection Regulation, and Digital Millennium Copyright Act, Computer Fraud and Abuse Act, and Health Insurance Portability, and Accountability Act;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 1: Computer and Digital Forensics	Lesson 3
(C) research investigate and analyze historic noteworthy cases incidents or events regarding cybersecurity;	Network Security Fundamentals 1a: Introduction	Unit 1: Security (and What Threatens It)	Activity 1
(D) demonstrate an understanding of ethical and legal behavior when presented with various scenarios related to cybersecurity cyber activities;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 7: Current Events in Cybersecurity	Activity 2
(E) define and identify tactics used in an incident techniques such as hacking, phishing, social engineering, denial of service, malware, online piracy, spoofing, and data vandalism;	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders Are at the Door	Lesson 1
(F) identify and use appropriate methods for citing sources.			
(4) Ethics and laws. The student identifies and defines cyberterrorism and counterterrorism.			
(A) define cyberterrorism, state-sponsored cyberterrorism, and hacktivism;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 7: Current Events in Cybersecurity	Activity 2
(B) compare and contrast physical terrorism and cyberterrorism, including domestic and foreign actors;			
(C) define and explain intelligence gathering and counterterrorism;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 7: Current Events in Cybersecurity	Activity 2
(D) explain identify the role of cyber defense defenders in protecting national interests and corporations;	Network Security Fundamentals 1a: Introduction	Unit 2: Fundamental Concepts of Cybersecurity	Lesson 1
(E) explain identify the role of cyber defense in society and the global economy;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 7: Current Events in Cybersecurity	Activity 2
(F) explain the importance of protecting public infrastructures such as electrical power grids, water systems, pipelines, transportation, and power generation facilities nuclear plants.			
(5) Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding significant issues related to digital technology, digital hygiene, and cyberbullying.			
(A) identify and understand the nature and value of privacy;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 7: Current Events in Cybersecurity	Activity
(B) analyze the positive and negative implications of a digital footprint and the maintenance and monitoring of an online presence;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 4: Managing Users and Permissions	Discussion 1,2
(C) discuss the role and impact of technology on privacy;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 7: Current Events in Cybersecurity	Activity
(D) identify the signs, emotional effects, and legal consequences of cyberbullying and cyberstalking;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 7: Current Events in Cybersecurity	Activity 1
(E) identify and discuss effective ways to prevent, deter, and report cyberbullying.	Network Security Fundamentals 1a: Introduction	Unit 5: Building Our Defenses	Activity 1
(6) Cybersecurity skills. The student understands basic cybersecurity concepts and definitions.			

(A) define cybersecurity and information security and cyber defense;	Network Security Fundamentals 1a: Introduction	Unit 1: Security (and What Threatens It)	Lesson 5
(B) identify basic risk management and risk assessment principles related to cybersecurity threats and vulnerabilities;	Network Security Fundamentals 1a: Introduction	Unit 1: Security (and What Threatens It)	Lesson 2
(C) explain the fundamental concepts of confidentiality, integrity, and availability (CIA triad), authentication, and authorization;	Network Security Fundamentals 1a: Introduction	Unit 2: Fundamental Concepts of Cybersecurity	Lessons 2-4
(D) describe the trade-offs inverse relationship between convenience privacy and security;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 7: Current Events in Cybersecurity	Activity
(E) identify and analyze cybersecurity breaches and incident responses such as conducting simulations;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 1: Computer and Digital Forensics	Lesson 3
(F) identify and analyze security challenges concerns in domains areas such as physical, network, cloud, and web;	Network Security Fundamentals 1a: Introduction	Unit 1: Security (and What Threatens It)	Lesson 1
(G) define and discuss challenges faced by cybersecurity professionals such as internal and external threats;	Network Security Fundamentals 1a: Introduction	Unit 1: Security (and What Threatens It)	Lesson 5
(H) identify common risks, warning signs, and alerts, and warning signs of compromised computer and network systems;			
(I) understand and explore the vulnerability of network-connected devices such as Internet of Things (IoT);	Network Security Fundamentals 1a: Introduction	Unit 3: Building a Network	Lesson 1
(J) use appropriate cybersecurity terminology;	Network Security Fundamentals 1a: Introduction	Unit 3: Building a Network	Lesson 2
(K) explain the concept of penetration testing, including tools, and techniques.	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders are at the Door	Lesson 2
(7) Cybersecurity skills. The student understands and explains various types of malicious software (malware).			
(A) define malware, including spyware, ransomware, viruses, and rootkits;	Network Security Fundamentals 1a: Introduction	Unit 7: A Closer Look at Malware	All Lessons Associated
(B) identify the transmission and function of malware such as trojan horses Trojans, worms, and viruses;	Network Security Fundamentals 1a: Introduction	Unit 7: A Closer Look at Malware	All Lessons Associated
(C) discuss the impact of malware has had on the cybersecurity landscape;	Network Security Fundamentals 1a: Introduction	Unit 7: A Closer Look at Malware	Lesson 2
(D) explain the role of reverse engineering for the detection of detecting malware and viruses;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 3: Operating Systems Administration	Lesson 3
(E) describe compare free and commercial antivirus and anti-malware software alternatives;	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders are at the Door	Lesson 2
(F) compare free and commercial anti-malware software alternatives.	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders are at the Door	Lesson 2
(8) Cybersecurity skills. The student understands and demonstrates knowledge of techniques and strategies to prevent a system from being compromised.			
(A) define system hardening;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 3: Operating Systems Administration	Lesson 1

(B) demonstrate basic use of system administration privileges;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 3: Operating Systems Administration	Lesson 2
(C) explain the importance of patching operating systems;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 5: Application Security	Lesson 5
(D) explain the importance of software updates;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 3: Operating Systems Administration	Lesson 2
(E) describe standard practices to configure system services;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 3: Operating Systems Administration	Lesson 1
(F) explain the importance of backup files;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 3: Operating System Administration	Lesson 5
(G) research and understand standard practices for securing computers, networks, and operating systems;	Network Security Fundamentals 1a: Introduction	Unit 2: Fundamental Concepts of Cybersecurity	Lesson 1
(H) identify vulnerabilities with the lack of cybersecurity awareness and training.	Network Security Fundamentals 1b: Forensics and Permissions	Unit 5: Application Security	Activity 2
(9) Cybersecurity skills. The student understands basic network operations.			
(A) identify basic network addressing and devices, including routers and switches and routers;	Network Security Fundamentals 1a: Introduction	Unit 3: Building a Network	Activity 1
(B) define network addressing;	Network Security Fundamentals 1a: Introduction	Unit 4: Protocols, Services, and Data Transfers	Lesson 2
(C) analyze incoming and outgoing rules for traffic passing through a firewall;	Network Security Fundamentals 1a: Introduction	Unit 3: Building a Network	Lesson 4
(D) identify well known ports by number and service provided, including port 22 (ssh), port 80 (http), and port 443 (https);	Network Security Fundamentals 1a: Introduction	Unit 4: Protocols, Services, and Data Transfers	Lessons 2, 3
(E) identify commonly exploited ports and services, including ports 20 and 21 (ftp) and port 23 (telnet);	Network Security Fundamentals 1a: Introduction	Unit 4: Protocols, Services, and Data Transfer	Lessons 3,4
(F) identify common tools for monitoring ports and network traffic.	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders are at the Door	Lesson 2
(10) Cybersecurity skills. The student identifies standard practices of system administration.			
(A) define what constitutes a secure password;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 4: Managing Users and Permissions	Lesson 2
(B) create a secure password policy, including length, complexity, account lockout, and rotation;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 4: Managing Users and Permissions	Lessons 1-4
(C) identify methods of password cracking such as brute force and dictionary attacks; and			
(D) examine and configure security options to allow and restrict access based on user roles.	Network Security Fundamentals 1b: Forensics and Permissions	Unit 4: Managing Users and Permissions	Lessons 4, 5
(11) Cybersecurity skills. The student demonstrates necessary steps to maintain user access on the computer system.			

(A) identify the different types of user accounts and groups on an operating system;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 4: Managing Users and Permissions	All Lessons Associated
(B) explain the fundamental concepts and standard practices related to access control, including authentication, authorization, and accounting (AAA);	Network Security Fundamentals 1b: Forensics and Permissions	Unit 4: Managing Users and Permissions	Lessons 4,5
(C) compare methods for single- and multi- dual-factor authentication such as passwords, biometrics, personal identification numbers (PINs), and secure security tokens;	Network Security Fundamentals 1a: Introduction	Unit 8: Security Design Principles	Lesson 4
(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.	Network Security Fundamentals 1b: Forensics and Permissions	Unit 2: Cryptology and Cryptography	Lesson 3
(12) Cybersecurity skills. The student explores the field of digital forensics.			
(A) explain the importance of digital forensics to organizations, private citizens, and the public sector law enforcement, government agencies, and corporations;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 1: Computer and Digital Forensics	Lessons 1-6
(B) identify the role of chain of custody in digital forensics;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 1: Computer and Digital Forensics	Lesson 3
(C) explain the four steps of the forensics process, including collection, examination, analysis, and reporting;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 1: Computer and Digital Forensics	Lessons 1-6
(D) identify when a digital forensics investigation is necessary;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 1: Computer and Digital Forensics	Lesson 1
(E) identify information that can be recovered from digital forensics investigations such as metadata and event logs;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 1: Computer and Digital Forensics	Lesson 1
(F) analyze the purpose of event logs and identify suspicious activity.	Network Security Fundamentals 1b: Forensics and Permissions	Unit 1: Computer and Digital Forensics	Lessons 1-6
(13) Cybersecurity skills. The student explores the operations of cryptography.			
(A) explain the purpose of cryptography and encrypting data;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 2: Cryptology and Cryptography	Lessons 2, 4, 6
(B) research historical uses of cryptography;	Network Security Fundamentals 1a: Introduction	Unit 1: Security (and What Threatens It)	Lesson 1
(C) review simple cryptography methods such as shift cipher and substitution cipher;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 2: Cryptology and Cryptography	Lesson 3
(D) define and explain public key encryption;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 2: Cryptology and Cryptography	Lessons 2, 4, 6
(E) compare and contrast symmetric and asymmetric encryption.	Network Security Fundamentals 1b: Forensics and Permissions	Unit 2: Cryptology and Cryptography	Lessons 2, 5
(14) Vulnerabilities, threats and attacks Risk assessment. The student understands information security vulnerabilities, threats, and computer attacks.			
(A) define and describe vulnerability, payload, exploit, port scanning, and packet sniffing as they relate to hacking;	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders are at the Door	Lesson 2

(B) define and describe cyberattacks, including man-in-the-middle, distributed denial of service, and spoofing, and back-door attacks;	Network Security Fundamentals 1a: Introduction	Unit 5: Building Our Defenses	Lesson 3
(C) explain how computer vulnerabilities leave systems open to cyberattacks;	Network Security Fundamentals 1a: Introduction	Unit 1: Security (and What Threatens It)	Lesson 5
(D) identify internal threats to systems such as logic bombs back-door attacks and insider threats;	Network Security Fundamentals 1a: Introduction	Unit 7: A Closer Look at Malware	All Lessons Associated
(E) differentiate types of social engineering techniques attacks such as phishing, web links in email, instant messaging, social media, and other online communication with malicious links; shoulder surfing;, hoaxes, and dumpster diving;	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders Are at the Door	Lesson 1
(F) explain how users are the most common vehicle for compromising a system at the application level;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 5: Application Security	Lessons 1,2
(G) identify various types of application-specific attacks such as cross-site scripting and injection attacks.	Network Security Fundamentals 1b: Forensics and Permissions	Unit 5: Application Security	Lessons 1,2
(15) Vulnerabilities, threats, and attacks Risk assessment. 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: Introduction	Unit 1: Security (and What Threatens It)	Lesson 5
(B) identify the capabilities of vulnerability assessment tools, including open source tools;	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders are at the Door	Lesson 2
(C) explain the concept of penetration testing, tools, and techniques.	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders are at the Door	Lesson 2
(16) Vulnerabilities, threats, and attacks Risk assessment. The student evaluates the vulnerabilities risks of wireless networks.			
(A) compare vulnerabilities risks associated with connecting devices to public and private wireless networks;	Network Security Fundamentals 1a: Introduction	Unit 5: Building Our Defenses	Lesson 1
(B) explain device vulnerabilities and security solutions on a wireless networks such as supply chain security and counterfeit products;	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders Are at the Door	Lesson 1
(C) compare and contrast wireless encryption protocols such as HTTP versus HTTPS;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 2: Cryptology and Cryptography	Lessons 3, 4, 6
(D) debate the broadcasting or hiding of a wireless service set identifier (SSID);	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders Are at the Door	Lesson 1
(E) research and discuss wireless threats such as MAC spoofing and packet sniffing war driving.	Network Security Fundamentals 1a: Introduction	Unit 5: Building Our Defenses	Lesson 3
(17) Vulnerabilities, threats, and attacks Risk assessment. The student analyzes threats to computer applications.			
(A) define application security;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 5: Application Security	Lessons 1,2
(B) identify methods of application security such as secure development policies and practices;	Network Security Fundamentals 1a: Introduction	Unit 2: Fundamental Concepts of Cybersecurity	Lesson 1

(C) discuss methods of online spoofing such as web links in email, instant messaging, social media, and other online communication with malicious links;	Network Security Fundamentals 1a: Introduction	Unit 7: A Closer Look at Malware	All Lessons Associated
(D) explain the purpose and function of vulnerability scanners;	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders are at the Door	Lesson 2
(E) explain how coding errors may create system vulnerabilities such as buffer overflows and lack of input validation;	Network Security Fundamentals 1a: Introduction	Unit 6: When the Intruders are at the Door	Lesson 3
(F) analyze the risks of distributing insecure programs.	Network Security Fundamentals 1b: Forensics and Permissions	Unit 3: Operating Systems Administration	Lesson 3
(18) Digital citizenship Risk assessment. The student understands the implications of sharing information and access with others.			
(A) define personally identifiable information (PII);	Network Security Fundamentals 1b: Forensics and Permissions	Unit 4: Managing Users and Permissions	Lessons 4, 5
(B) evaluate the risks and benefits of sharing personally identifiable information (PII);	Network Security Fundamentals 1b: Forensics and Permissions	Unit 4: Managing Users and Permissions	Lessons 1-4
(C) describe the impact of granting applications unnecessary permissions such as mobile devices accessing camera and contacts;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 4: Managing Users and Permissions	Lessons 1-4
(D) describe the risks of granting third parties access to personal and proprietary data on social media and systems;	Network Security Fundamentals 1b: Forensics and Permissions	Unit 2: Cryptology and Cryptography	Lesson 3
(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.	Network Security Fundamentals 1b: Forensics and Permissions	Unit 3: Operating Systems Administration	Lesson 1
(19) Risk assessment. The student understands risk, and how risk assessment and risk management defend against attacks.			
(A) define commonly used risk assessment terms, including risk, asset, and inventory;	Network Security Fundamentals 1a: Introduction	Unit 1: Security (and What Threatens It)	Lesson 1
(B) identify risk management strategies, including acceptance, avoidance, transference, and mitigation;	Network Security Fundamentals 1a: Introduction	Unit 1: Security (and What Threatens It)	Lesson 2
(C) compare and contrast risks based on an industry accepted rubric/metric such as Risk Assessment Matrix;	Network Security Fundamentals 1a: Introduction	Unit 1: Security (and What Threatens It)	Lesson 2