eDynamic Learning Course Title: Operational Cybersecurity 1a / 1b

State: TX
State Course Title: Cybersecurity
State Course Code: 130.429
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;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 5: Security Awareness and Training	Lesson 5
(B) identify and demonstrate positive personal qualities such as authenticity, resilience, initiative, and a willingness to learn new knowledge and skills;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 5: Security Awareness and Training	Lesson 5
(C) solve problems and think critically;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 4: Response and Recovery Planning	Lessons 1, 2
(D) demonstrate leadership skills and function effectively as a team member;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 4: Response and Recovery Planning	Lesson 4
(E) demonstrate an understanding of ethical and legal responsibilities in relation to the field of cybersecurity.	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 3: Scenarios: testing and Troubleshooting	Lesson 3
(2) Employability skills. The student identifies various employment opportunities in the cybersecurity field.			
(A) develop a personal career plan along with the education, job skills, and experience necessary to achieve career goals;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 5: Security Awareness and Training	Lesson 5
(B) develop a resume or a portfolio appropriate to a chosen career plan;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 5: Security Awareness and Training	Lesson 5
(C) illustrate interview skills for successful job placement.	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 5: Security Awareness and Training	Lesson 5
(3) Ethics and laws. The student evaluates ethical and current 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) analyze and apply to a scenario local, state, national, and international cybersecurity laws such as David's Law, Computer Fraud and Abuse Act (CFAA), and Digital Millennium Copyright Act;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 6: Ethical Concerns in Cybersecurity	Lessons 2, 5
(B) evaluate noteworthy incidents historic cases or events regarding cybersecurity;	Operational Cybersecurity 1A: Introduction	Unit 2: Virtual Local Area Networks	Lesson 4

(C) evaluate explore compliance requirements such as Section 508 of the Rehabilitation Act of 1973, Family Educational Rights and Privacy Act of 1974 (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Gramm-Leach-Bliley Act (GLBA).	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 6: Ethical Concerns in Cybersecurity	Lessons 2, 5
(4) Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding significant issues relating to digital technology, safety, digital hygiene, and cyberbullying.			
(A) debate the relationship between privacy and security;	Operational Cybersecurity 1A: Introduction	Unit 3: Cryptology, Keys, and Certificates	Activity
(B) differentiate between identify ethical and or unethical behavior when presented with various scenarios related to cybersecurity cyber activities.	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 6: Ethical Concerns in Cybersecurity	Lesson 3
(5) Cybersecurity skills. The student simulates explains the importance and process of penetration testing.			
(A) illustrate define the phases of penetration testing, including plan, discover, attack, and report;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 3: Scenarios: testing and Troubleshooting	Lesson 3
(B) design develop a plan to gain authorization for penetration testing;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 3: Scenarios: testing and Troubleshooting	Lesson 4
(C) evaluate identify commonly used vulnerability scanning tools such as port scanning, packet sniffing, and password crackers;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 3: Scenarios: testing and Troubleshooting	Lessons 3, 4
(D) develop a list of exploits based on results of scanning tool reports; prioritize a list of mitigations based on results of scanning tool reports.	Operational Cybersecurity 1A: Introduction	Unit 6: Assessing and mitigating network Attacks	Lessons 1-3
(6) Cybersecurity skills. The student understands common cryptographic methods.			
(A) evaluate symmetric and asymmetric algorithms such as substitution cipher, Advanced Encryption Standard (AES), Diffie-Hellman, and Rivest-Shamir-Adleman (RSA);	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 2: Authentication at Work	Lesson 3
(B) interpret explain the purpose of hashing algorithms, including blockchain;			
(C) demonstrate explain the function of password salting;			
(D) explain and create a digital signature;	Operational Cybersecurity 1A: Introduction	Unit 1: Advanced Networking Concepts	Lesson 2
(E) illustrate explain steganography.			
(7) Cybersecurity skills. The student understands the concept of system cyber defense.			
(A) explain the purpose of establishing system baselines;	Operational Cybersecurity 1A: Introduction	Unit 4: Assessing Risk	Lessons 3, 4
(B) evaluate the role of physical security;	Operational Cybersecurity 1A: Introduction	Unit 8: Assessing and Mitigating Malware Attacks	Lesson 5

(C) evaluate the functions of network security devices such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and intrusion detection prevention systems (IDPS);	Operational Cybersecurity 1A: Introduction	Unit 6: Assessing and Mitigating Network Attacks	Lessons 1, 4
(D) analyze log files for anomalies;			
(E) develop a plan demonstrating the concept of defense in depth.	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 4: Response and Recovery Planning	Lesson 4
(8) Cybersecurity skills. The student demonstrates an understanding of secure network design.			
(A) explain the benefits of network segmentation, including sandboxes, air gaps, and virtual local area networks (VLAN);	Operational Cybersecurity 1A: Introduction	Unit 2: Virtual Local Area Networks	Lessons 1-4
(B) investigate the role of software-managed networks, including virtualization, containerization, and cloud computing;	Operational Cybersecurity 1A: Introduction	Unit 4: Assessing Risk	Lesson 4
(C) evaluate discuss the role of honeypots and honeynets in networks;	Operational Cybersecurity 1A: Introduction	Unit 4: Assessing Risk	Lessons 3, 4
(D) create an incoming and outgoing network policy for a firewall.	Operational Cybersecurity 1A: Introduction	Unit 8: Assessing and Mitigating Malware Attacks	Lessons 3, 4
(9) Cybersecurity skills. The student integrates principles of digital forensics.			
(A) identify cyberattacks by their signatures;			
(B) explain proper data acquisition;			
(C) examine evidence from devices for suspicious activities;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 4: Response and Recovery Planning	Lesson 2
(D) research and summarize current cybercrime cases involving digital forensics.	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 3: Scenarios: testing and Troubleshooting	Lesson 4
(10) Cybersecurity skills. The student explores expanding and emerging technology.			
(A) describe the integration of artificial intelligence and machine learning in cybersecurity;	Operational Cybersecurity 1A: Introduction	Unit 4: Assessing Risk	Lesson 4
(B) investigate impacts made by predictive analytics and big data on cybersecurity;	Operational Cybersecurity 1A: Introduction	Unit 5: Risk Mitigation and Management	Lesson 2
(C) research and investigate other emerging trends such as augmented reality and quantum computing.			
(11) Cybersecurity skills. The student uses various operating system environments.			
(A) select and execute appropriate issue commands via the command line interface (CLI) such as ls, cd, pwd, cp, mv, chmod, ps, sudo, and passwd;	Operational Cybersecurity 1A: Introduction	Unit 3: Cryptology, Keys, and Certificates	Lesson 2

(B) describe the file system structure for multiple operating systems;			
(C) manipulate and edit files within the CLI;			
(D) determine network status using the CLI with commands such as ping, ifconfig/ipconfig, traceroute/tracert, and netstat.			
(12) Cybersecurity skills. The student clearly and effectively communicates technical information.			
(A) collaborate with others to create a technical report;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 4: Response and Recovery Planning	Lesson 4
(B) create, review, and edit a report summarizing technical findings;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 3: Scenarios: testing and Troubleshooting	Lesson 3
(C) present technical information to a non-technical audience.			
(13) Risk assessment. The student understands risk and how risk assessment and risk management defend against attacks analyzes various types of threats, attacks, and vulnerabilities.			
(A) differentiate types of attacks, including operating systems, software, hardware, network, physical, social engineering, and cryptographic;	Operational Cybersecurity 1A: Introduction	Unit 6: Assessing and mitigating network Attacks	Lessons 1-3
(B) explain blended threats such as combinations of software, hardware, network, physical, social engineering, and cryptographic;			
(C) discuss risk response techniques, including accept, transfer, avoid, and mitigate;	Operational Cybersecurity 1A: Introduction	Unit 5: Risk Mitigation and Management	Lesson 2
(D) develop a plan of preventative measures based on threat modeling, discovered vulnerabilities, and the likelihood of a cyberattack to address cyberattacks;	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 3: Scenarios: testing and Troubleshooting	Lesson 3
(E) describe common web vulnerabilities such as cross-site scripting, buffer overflow, injection, spoofing, and denial of service;	Operational Cybersecurity 1A: Introduction	Unit 6: Assessing and mitigating network Attacks	Lessons 1-3
(F) describe common data destruction and media sanitation practices such as wiping, shredding, and degaussing;	Operational Cybersecurity 1A: Introduction	Unit 5: Risk Mitigation and Management	Lesson 2
(G) develop an incident response plan based on system prioritization for a given scenario or recent attack.	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 4: Response and Recovery Planning	Lesson 4
(14) Risk assessment. The student understands risk management processes and concepts.			
(A) describe various access control methods such as mandatory access control (MAC), role-based access control (RBAC), and discretionary access control (DAC);	Operational Cybersecurity 1A: Introduction	Unit 8: Assessing and Mitigating Malware Attacks	Lesson 5
(B) develop and defend a plan for multi-factor access control using components such as biometric verification systems, key cards, tokens, and passwords;	Operational Cybersecurity 1A: Introduction	Unit 3: Cryptology, Keys, and Certificates	Lessons 1, 2

(C) review and appraise a disaster recovery plan (DRP) that includes backups, redundancies, system dependencies, and alternate sites.	Operational Cybersecurity 1B: Security and Planning in the Workplace	Unit 4: Response and Recovery Planning	Lessons 1, 2
(15) Risk assessment. The student investigates the role and effectiveness of environmental controls.			
(A) explain commonly used physical security controls, including lock types, fences, barricades, security doors, and mantraps;	Operational Cybersecurity 1A: Introduction	Unit 8: Assessing and Mitigating Malware Attacks	Lesson 5
(B) describe the role of embedded systems such as fire suppression; heating, ventilation, and air conditioning (HVAC) systems; security alarms; video monitoring.			