

Career and Technical Education TEKS Review Final Recommendations

Texas Essential Knowledge and Skills (TEKS) for Career and Technical Education Final Recommendations
Science, Technology, Mathematics, and Engineering (STEM) Cluster

Program of Study:

Cybersecurity

The document reflects the final recommendations to the career and technical education Texas Essential Knowledge and Skills (TEKS) that have been recommended by the State Board of Education's TEKS review work groups for the following programs of study from the STEM Career Cluster:
Cybersecurity.

Proposed additions are shown in green font with underline (additions). Proposed deletions are shown in red font with strikethroughs (~~deletions~~). Text proposed to be moved from its current student expectation is shown in purple italicized font with strikethrough (~~*moved text*~~) and is shown in the proposed new location in purple italicized font with underlines (*new text location*). Numbering for the knowledge and skills statements in the document will be finalized when the proposal is prepared to file with the *Texas Register*.

Comments in the right-hand column provide explanations for the proposed changes. The following notations may be used as part of the explanations.

CCRS: refers to the College and Career Readiness Standards
MV: refers to multiple viewpoints expressed by work group members

Table of Contents

Cybersecurity	Pages
Foundations of Cybersecurity.....	1–10
Cybersecurity Capstone.....	11–16
Digital Forensics.....	17–21

§130.428. Foundations of Cybersecurity (One Credit), Adopted 2022

TEKS with edits		Work Group Comments/Rationale
(a)	General requirements. Students shall be awarded one credit for successful completion of this course. This course is recommended for students in Grades 9-12.	
(b)	Introduction.	
(1)	Career and technical education instruction provides content aligned with challenging academic standards and relevant technical knowledge and skills for students to further their education and succeed in current or emerging professions.	
(2)	The Science, Technology, Engineering, and Mathematics (STEM) Career Cluster focuses on planning, managing, and providing scientific research and professional and technical services, including laboratory and testing services, and research and development services.	
(3)	Cybersecurity is an evolving <u>a critical</u> discipline concerned with safeguarding computers, networks, programs, and data from unauthorized access. As a field, it has gained prominence with the emergence <u>expansion</u> of a globally-connected society. As computing has become more sophisticated, so too have the abilities <u>to access systems and of malicious agents looking to penetrate networks and seize private</u> sensitive information. By evaluating prior incidents, <u>Cybersecurity professionals have the ability to craft appropriate responses</u> prevent, detect and respond to minimize disruptions to corporations <u>governments, organizations,</u> and individuals.	Group removed words such as private because all data/information is not private. Cyber is no longer an emerging entity or like expanding. Updated vocabulary and clearly stated what Cybersecurity professionals do.
(4)	In the Foundations of Cybersecurity course, students will develop the knowledge and skills needed to explore fundamental concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will review and explore security policies designed to mitigate risks. The skills obtained in this course prepare students for additional study in cybersecurity. A variety of courses are available to students interested in this field. Foundations of Cybersecurity may serve as an introductory course in this field of study.	
(5)	Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.	
(6)	Statements that contain the word "including" reference content that must be mastered, while those containing the phrase "such as" are intended as possible illustrative examples.	
(c)	Knowledge and skills.	
(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;	
(C)	solve problems and think critically;	
(D)	demonstrate leadership skills and function effectively as a team member; and	
(E)	demonstrate an understanding of ethical and legal responsibilities <u>and ramifications</u> in relation to the field of cybersecurity.	Group agreed that to add rigor one needs to add responsibilities and ramifications.
(2)	Employability skills <u>Professional Awareness</u> . The student identifies various employment opportunities and requirements in the cybersecurity field. The student is expected to:	Group wanted to differentiate between employability Skills and professional awareness as it relates to cybersecurity security
(A)	identify job and internship opportunities as well as accompanying duties and tasks;	
(B)	research careers in cybersecurity and information assurance security and develop <u>professional profiles that match along with the</u> education and job skills required for obtaining a job in both the public and private sectors;	Group Combined elements from D into B to allow for a more succinct sentence structure about careers and professional profiles.
(C)	identify and discuss certifications for cybersecurity-related careers; and	
(D)	research and develop resumes, digital portfolios, or professional profiles in the cybersecurity field. <u>explain the different types of services and roles found within a cybersecurity functional area, such as a security operations center (SOC).</u>	Group wanted students to gain exposure to different roles and services within cybersecurity.
(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:	Only in SEs is it an issue.....understand maybe can stand in a Knowledge and Skill statement
(A)	demonstrate and advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;	
(B)	<u>investigate and analyze</u> research local, state, national, and international cyber laws such as the PATRIOT Act of 2001, General Data Protection Regulation, and Digital Millennium Copyright Act, <u>Computer Fraud and Abuse Act, and Health Insurance Portability, and Accountability Act;</u>	Group wanted to increase rigor with “investigate and analyze” instead of research. Group wanted to add additional laws to increase rigor. Thoughts: HIPPA vs FERPA COPPA possibility per industry feedback CIPA schools filter internet connections

(C)	research <u>investigate and analyze</u> historic-noteworthy cases-incidents or events regarding cybersecurity;	Group wanted to make sure that any area where “cyber” is written to write out the complete word: cybersecurity. Group wanted to increase understanding and rigor by adding in investigate and analyze and move beyond historic and use noteworthy and incidents instead of cases.
(D)	demonstrate an understanding of ethical and legal behavior when presented with various scenarios related to <u>cybersecurity</u> cyber activities;	Group wanted consistency with Cybersecurity
(E)	define and identify <u>tactics used in an incident</u> techniques such as hacking, phishing , social engineering, <u>malware, denial of service, online piracy</u> , spoofing, and data vandalism; and	Group wanted to increase rigor by the how with tactics and the what with techniques. Added in “as a service” per industry feedback to cover service of spammers, malware and hacking
(F)	identify and use appropriate methods for citing sources.	
(4)	Ethics and laws. The student <u>differentiates between</u> identifies the consequences of ethical versus malicious hacking. The student is expected to:	Group wanted to make sure students knew the difference between ethical and malicious.
(A)	identify motivations <u>and perspectives</u> for hacking;	Deleted F and added perspectives into A
(C)(B)	identify and describe the impact of cyberattacks on the global community, society, and individuals;	
(B)(E)	distinguish between <u>the types of threat actors such as hackers, criminals, state-sponsored actors, and foreign governments</u> a cyber attacker and a cyber defender ;	Group wanted to distinguish between the types of threat actors (industry use) such as hackers, criminals, nation state actors, and foreign governments Group suggests threat actor instead of cyber attacker.
(D)	differentiate <u>between industry terminology for</u> types of hackers such as black hats, white hats, and gray hats; <u>and</u>	Group was concerned with language used by industry may end up being revised and wanted to include such as
(E)	determine possible outcomes and legal ramifications of ethical versus malicious hacking practices. ; and	

(F)	debate the varying perspectives of ethical versus malicious hacking.	Delete and adding wording into (A)
(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 and counterterrorism;	Removed “and counterterrorism” because it is redundant from above.
(D)	explain identify the role of cyber defense defenders in protecting national interests and corporations;	Group increase rigor by explaining and wanted to match with cyber defense instead of defenders.
(E)	explain identify the role of cyber defense in society and the global economy; and	
(F)	explain the importance of protecting public infrastructures such as electrical power grids, water systems, pipelines, transportation, and power generation facilities nuclear plants.	Remove nuclear plants and use power generation facilities to cover more than one power source.
(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; and	
(E)	identify and discuss effective ways to prevent; deter; and report cyberbullying.	Group indicated that no effective way to prevent, only deter and report.
(8) (7)	Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:	Moving (18) to new (7) and renumber the KS statements.
(A)	define cybersecurity and information security and cyber defense;	Group: change cyber defense to cybersecurity.
(B)	identify basic risk management and risk assessment principles related to cybersecurity threats and vulnerabilities, including the Zero Trust model;	Per industry feedback adding in Zero Trust model
(C)	explain the fundamental concepts of confidentiality, integrity, and availability (CIA triad); authentication, and authorization;	CIA Triad good, authentication and authorization found elsewhere.

(D)	describe the <u>trade-offs</u> inverse relationship between <u>convenience</u> privacy and security;	Inverse as a typo from previous group work, group wanted to further define the detail in this sentence to include the trade off between convenience and security.
(E)	identify and analyze cybersecurity breaches and incident responses <u>such as conducting simulations</u> ;	Simulation skill that students need to know this foundation knowledge.
(F)	identify and analyze security <u>challenges</u> concerns in <u>domains</u> areas such as physical, network, cloud, and web;	Group: challenges instead of concerns instead of areas use domains to fit with industry language.
(G)	define and discuss challenges faced by cybersecurity professionals, <u>such as internal and external threats</u> ;	Group: identifying all vulnerabilities within a system as opposed to one for an adversary
(H)	Identify <u>indicators of compromise, such as</u> common risks, <u>warning signs, and</u> alerts, and warning signs of compromised computer and network systems;	Group: warned before alert and group wanted to be including by using systems only. Added in “indicators of compromise” based on industry feedback
(I)	understand and explore the vulnerabilities ty of network-connected devices, <u>such as Internet of Things (IoT)</u> ; and	IOT, Internet of Things....including IOT devices....
(J)	use appropriate cybersecurity terminology; and -	
(K)	<u>explain the concept of penetration testing, including tools, and techniques; and</u>	Moved from 16C
(L)	explore and identify common industry frameworks, such as MITRE ATT&CK, MITRE Engage, and Cyber Kill Chain, and the Diamond Model.	Per industry feedback added: common industry frameworks such as MITRE ATT&CK, MITRE Engage, and Cyber Kill Chain, and Diamond Model
(9)(8)	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;	
(B)	identify the transmission and function of malware such as <u>trojan horses</u> Trojans , worms, and viruses;	Correcting the trojan horses language.
(C)	discuss the impact of malware <u>and the model of “as a service”</u> ; has had on the cybersecurity landscape ;	Added “as a service” as an industry trend per industry feedback to include aspects of companies paying for a service of malware, spamming, etc.

(D)	explain the role of reverse engineering for <u>the detection of</u> detecting malware and viruses; <u>and</u>	
(E)	<u>describe</u> compare free and commercial antivirus <u>and anti-malware</u> software, <u>also known as Endpoint Detection and Response software.</u> alternatives; and	Combined E and F, added in new language to fit with industry standards and feedback
(F)	compare free and commercial anti-malware software alternatives.	
(10) (9)	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)	demonstrate basic use of system administration privileges;	
(C)	explain the importance of patching operating systems;	
(D)	explain the importance of software updates;	
(E)	describe standard practices to configure system services;	
(F)	explain the importance of backup files; and	
(G)	research and understand standard practices for securing computers, networks, and operating systems, <u>including the concept of least privilege; and.</u>	Per industry feedback added the concept of Least Privilege
<u>(H)</u>	<u>identify vulnerabilities with the lack of cybersecurity awareness and training, such as humans being a weakness in an organization</u>	Group wanted to add in the fact that the lack of training is a vulnerability, and it is a strategy and technique to avoid harm. So if someone was not trained well they open themselves up to threats. Added human error per industry feedback
(11) (10)	Cybersecurity skills. The student understands basic network operations. The student is expected to:	
(A)	identify basic network addressing and devices, including <u>routers and</u> switches and routers;	Group: separate out addressing and network devices.
<u>(B)</u>	<u>define network addressing;</u>	Create a new SE for network addressing.
(C) (B)	analyze incoming and outgoing rules for traffic passing through a firewall;	
(D) (C)	identify well known ports by number and service provided, including port 22 (ssh), port 80 (http), and port 443 (https);	
<u>(E)</u> (D)	identify commonly exploited ports and services, including ports 20 and 21 (ftp), and port 23 (telnet), <u>and port 3389 (rdp); and</u>	Added in port 3389 per industry feedback

(F)(E)	identify common tools for monitoring ports and network traffic.	
(12)(H)	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; and	
(D)	examine and configure security options to allow and restrict access based on user roles.	
(13)(I)	Cybersecurity skills. The student demonstrates necessary steps to maintain user access on the computer system. The student is expected to:	CUDD-create update delete disable
(A)	identify the different types of user accounts and groups on an operating system;	
(B)	explain the fundamental concepts and standard practices related to access control, including authentication, authorization, and <u>auditing</u> accounting ;	Updated language of auditing instead of accounting.
(C)	compare methods for single- and multi- dual factor authentication such as passwords, biometrics, personal identification numbers (PINs), and secure security tokens, <u>and other passwordless authentication methods</u> ;	Change: multi-factor instead of dual. Updated language from security tokens to secure tokens per industry feedback added passwordless auth methods
(D)	define and explain the purpose <u>and benefits</u> of an air-gapped computer; and	Students knowing the purpose and the benefits
(E)	explain how hashes and checksums may be used to validate the integrity of transferred data.	
(14)(I)	Cybersecurity skills. The student explores the field of digital forensics. The student is expected to:	
(A)	explain the importance of digital forensics to <u>organizations, private citizens, and the public sector</u> law enforcement, government agencies, and corporations ;	Added additional language to be more inclusive. Organizations includes corporations and is more encompassing
(B)	identify the role of chain of custody in digital forensics;	
(C)	explain the four steps of the forensics process, including collection, examination, analysis, and reporting;	Framework,
(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; and	

(F)	analyze the purpose of event logs and identify suspicious activity.	
(15) (14)	Cybersecurity skills. The student explores the operations of cryptography. The student is expected to:	
(A)	explain the purpose of cryptography and encrypting data;	
(B)	research historical uses of cryptography; and	
(C)	review simple cryptography methods such as shift cipher and substitution cipher; ;	
(D)	<u>define and explain public key encryption; and</u>	Adding an additional SE to include industry based knowledge of public encryption
(E)	<u>compare and contrast symmetric and asymmetric encryption.</u>	Adding an additional SE to include industry-based knowledge such as symmetric and asymmetric encryption
(16) (15)	<u>Vulnerabilities, threats and attacks</u> Risk assessment . The student understands information security vulnerabilities, threats, and computer attacks. The student is expected to:	Group states these are not risk assessment but rather vulnerabilities, threats, and attacks.
(C) (A)	define and describe vulnerability, payload, exploit, port scanning, and packet sniffing as they relate to hacking;	Extra verbiage removed Move to C
(E) (B)	define and describe cyberattacks, including man-in-the-middle, distributed denial of service, and spoofing, <u>and back-door attacks;</u>	
(A) (C)	explain how computer vulnerabilities leave systems open to cyberattacks;	This moves to A
(D) (E)	identify <u>internal</u> threats to systems such as <u>logic bombs</u> back-door attacks and insider threats;	Updated to explain internal threat and changed examples Move to D
(F)	differentiate types of social engineering <u>techniques</u> attacks such as phishing, <u>web links in email, instant messaging, social media, and other online communication with malicious links;</u> shoulder surfing; hoaxes; and dumpster diving; ;	Social engineering: attacks not digital, human element is the weakness. Moved from 18(C).
(B) (F)	explain how users are the most common vehicle for compromising a system at the application level; and	This becomes B
(G)	identify various types of application-specific attacks <u>such as cross-site scripting and injection attacks.</u>	Mark: such as examples SQL injections or cross-site scripting, Unpatched vulnerabilities
(16)	Vulnerabilities, threats, and attacks Risk assessment. The student understands, identifies, and explains the strategies and techniques of both ethical and malicious hackers. The student is expected to:	KS and SEs found in other places

(A)	identify internal and external threats to computer systems;	
(B)	identify the capabilities of vulnerability assessment tools, including open source tools; and	
(C)	explain the concept of penetration testing, tools, and techniques.	Moved to 7K to fit better with the KS 7
(17)	<u>Vulnerabilities, threats, and attacks</u> Risk-assessment . The student evaluates the <u>vulnerabilities risks</u> of wireless networks. The student is expected to:	Change risk to vulnerabilities so the KS category matches the content.
(A)	compare <u>vulnerabilities risks</u> associated with connecting devices to public and private wireless networks;	Including all types of networkers
(B)	explain device vulnerabilities and security solutions on a wireless networks <u>such as supply chain security and counterfeit products;</u>	Added further detail to build out the idea of device and the implications therein
(C)	compare <u>and contrast wireless encryption</u> protocols <u>such as HTTP versus HTTPS;</u>	Understanding secure vs non-secure
(D)	debate the broadcasting or hiding of a wireless-service set identifier (SSID); and	
(E)	research and discuss wireless threats such as MAC spoofing and <u>packet sniffing</u> war driving.	Added in additional detail with packet sniffing
(18)	<u>Vulnerabilities, threats, and attacks</u> Risk-assessment . The student analyzes threats to computer applications. The student is expected to:	
(A)	define application security;	
(B)	identify methods of application security such as secure development <u>policies and</u> practices;	Adding additional element to include policy with development
(C)	discuss methods of online spoofing such as web links in email, instant messaging, social media, and other online communication with malicious links;	Move to 15 E
(D)	explain the purpose and function of vulnerability scanners;	
(E)	explain how coding errors may create system vulnerabilities <u>such as buffer overflows and lack of input validation;</u> and	Group wanted to include examples
(F)	analyze the risks of distributing insecure programs.	Single risk
(18) (7)	<u>Digital citizenship</u> Risk-assessment . The student understands the implications of sharing information and access with others. The student is expected to:	Move up to KS 7 along with all the SEs below and move the KSs and SEs after 7 down to a new number. The work group felt that these student expectations were more appropriately placed in the digital citizenship strand.
(A)	<u>define personally identifiable information (PII)</u>	Group wanted to include PII and make sure this is associated with digital citizenship
(B)	<u>evaluate the risks and benefits of sharing personally identifiable information (PII)</u>	

(C) (A)	describe the impact of granting applications unnecessary permissions <u>such as mobile devices accessing camera and contacts</u> ;	specify mobile, such as granting mobile access to a user's contacts, camera access, microphone access.
(D) (B)	describe the risks of granting third parties access to personal and proprietary data on social media and systems; and	
(E) (C)	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.	
(19)	<u>Risk assessment. The student understands risk, and how risk assessment and risk management defend against attacks. The student is expected to:</u>	Adding in new KS and SEs From Tech Apps work: demonstrate adherence to Acceptable Use Policy (AUP) and practice and model safe, ethical, and positive online behaviors;
(A)	<u>define commonly used risk assessment terms, including risk, asset, and inventory;</u>	Group wanted students to understand terms used in risk
(B)	<u>identify risk management strategies, including acceptance, avoidance, transference, and mitigation;</u>	risk mgmt. strategies acceptance avoidance transference mitigation
(C)	<u>compare and contrast risks based on an industry accepted rubric/metric such as Risk Assessment Matrix;</u>	

DRAFT

§130.429. Cybersecurity Capstone (One Credit), Adopted 2022

TEKS with edits		Work Group Comments/Rationale
(a)	General requirements. Students shall be awarded one credit for successful completion of this course. This course is recommended for students in Grades 11 and 12. Recommended <u>P</u> prerequisite: Foundations of Cybersecurity.	Data analysis thoughts Group wanted to make a required prereq of Foundations
(b)	Introduction.	
(1)	Career and technical education instruction provides content aligned with challenging academic standards and relevant technical knowledge and skills for students to further their education and succeed in current or emerging foundations.	
(2)	The Science, Technology, Engineering, and Mathematics (STEM) Career Cluster focuses on planning, managing, and providing scientific research and professional and technical services, including laboratory and testing services, and research and development services.	
(3)	Cybersecurity is an evolving <u>a critical</u> discipline concerned with safeguarding computers, networks, programs, and data from unauthorized access. As a field, it has gained prominence with the emergence-expansion of a globally-connected society. As computing has become more sophisticated, so too have the abilities of malicious agents-adversaries looking to penetrate networks and <u>access</u> seize private-sensitive information. By evaluating prior incidents, <u>C</u> ybersecurity professionals have the ability to craft appropriate responses-prevent, detect and respond to minimize disruptions to corporations governments, <u>organizations</u> , and individuals.	Group removed words such as private because all data/information is not private. Cyber is no longer an emerging entity or expanding. Updated vocabulary and clearly stated what Cybersecurity professionals do.
(4)	In the Cybersecurity Capstone course, students will develop the knowledge and skills needed to explore advanced concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will develop security policies to mitigate risks. The skills obtained in this course prepare students for additional study toward industry certification. A variety of courses are available to students interested in the cybersecurity field. Cybersecurity Capstone may serve as a culminating course in this field of study.	
(5)	Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.	
(6)	Statements that contain the word "including" reference content that must be mastered, while those containing the phrase "such as" are intended as possible illustrative examples.	

(c)	Knowledge and skills.	
(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;	
(C)	solve problems and think critically;	
(D)	demonstrate leadership skills and function effectively as a team member; and	
(E)	demonstrate an understanding of ethical and legal responsibilities in relation to the field of cybersecurity.	
(2)	Employability skills. The student identifies various employment opportunities in the cybersecurity field. The student is expected to:	
(A)	develop a personal career plan along with the education, job skills, and experience necessary to achieve career goals;	
(B)	develop a resume or a portfolio appropriate to a chosen career plan; and	
(C)	illustrate interview skills for successful job placement.	
(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. The student is expected to:	
(A)	analyze and apply to a scenario local, state, national, and international <u>cybersecurity laws</u> such as David's Law and Digital Millennium Copyright Act;	
(B)	evaluate <u>noteworthy historic incidents</u> eases or events regarding <u>cybersecurity</u> ; and	Noteworthy encompasses more than just historic.
(C)	<u>evaluate explore</u> 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), <u>and Cybersecurity Maturity Model Certification (CMMC)</u> .	Change verb for more rigor CMMC-Cybersecurity Maturity Model Certification per industry feedback
(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. The student is expected to:	
(A)	debate the relationship between privacy and security; and	

(B)	<u>differentiate between</u> identify ethical <u>and</u> or unethical behavior when presented with various scenarios related to <u>cybersecurity</u> cyber activities.	More rigor in verb and including both ethical and unethical
(5)	Cybersecurity skills. The student <u>simulates</u> explains the importance and process of penetration testing. The student is expected to:	Added simulates to increase rigor for capstone course.
(A)	<u>illustrate</u> define the phases of penetration testing, including plan, discover, attack, and report;	Added illustrate to increase rigor for capstone course.
(B)	<u>design</u> develop a plan to gain authorization for penetration testing;	Added design to increase rigor for capstone course.
(C)	<u>evaluate</u> identify commonly used vulnerability scanning tools such as port scanning, packet sniffing, and password crackers;	Added evaluate to increase rigor for capstone course.
(D)	develop a list of exploits based on results of scanning tool reports; and	
(E)	prioritize a list of mitigations based on results of scanning tool reports.	
(6)	Cybersecurity skills. The student understands common cryptographic methods. The student is expected to:	
(A)	evaluate symmetric and asymmetric algorithms such as substitution cipher, Advanced Encryption Standard (AES), Diffie-Hellman, and Rivest-Shamir-Adleman (RSA);	
(B)	<u>interpret</u> explain the purpose of hashing algorithms, including blockchain;	Verb rigor
(C)	<u>demonstrate</u> explain the function of password salting;	Verb rigor
(D)	explain and create a digital signature; and	
(E)	<u>illustrate</u> explain steganography.	Verb rigor
(7)	Cybersecurity skills. The student understands the concept of <u>system</u> cyber defense. The student is expected to:	
(A)	explain the purpose of establishing system baselines;	
(B)	evaluate the role of physical security;	
(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), <u>and security information and event management (SIEM) systems;</u>	Add SIEM per industry feedback
(D)	analyze log files for anomalies; and	
(E)	develop a plan demonstrating the concept of defense in depth.	

(8)	Cybersecurity skills. The student demonstrates an understanding of secure network design. The student is expected to:	
(A)	explain the benefits of network segmentation, including sandboxes, air gaps, and virtual local area networks (VLAN);	
(B)	investigate the role of software-managed networks, including virtualization <u>and cloud architecture</u> ;	Added cloud architecture via industry feedback.
(C)	<u>evaluate</u> discuss the role of honeypots and honeynets in networks; and	Verb rigor
(D)	create an incoming and outgoing network policy for a firewall.	
(9)	Cybersecurity skills. The student integrates principles of digital forensics. The student is expected to:	
(A)	identify cyberattacks by their signatures, <u>indicators, or patterns</u> ;	Added indicators and patterns via industry feedback
(B)	explain proper data acquisition;	
(C)	examine evidence from devices for suspicious activities; and	
(D)	<u>critique</u> research current cybercrime cases involving digital forensics.	Verb rigor
(10)	Cybersecurity skills. The student explores <u>expanding and</u> emerging technology. The student is expected to:	
(A)	<u>describe the concept of Security as a Service and the role of managed security service providers (MSSP)</u> ;	added in new SE per industry feedback to include MSSP b/c it is a trend
(A) (B)	describe the integration of artificial intelligence and machine learning in cybersecurity;	
(B) (C)	investigate impacts made by predictive analytics on cybersecurity; and	
(C) (D)	research <u>and investigate</u> other emerging trends such as augmented reality and quantum computing.	Verb rigor
(11)	Cybersecurity skills. The student uses various operating system environments. The student is expected to:	
(A)	<u>select and execute appropriate</u> issue commands via the command line interface (CLI) such as ls, cd, pwd, cp, mv, chmod, ps, sudo, and passwd;	Verb change to fit what the students are actually doing
(B)	describe the file system structure for multiple operating systems;	
(C)	manipulate and edit files within the CLI; and	
(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. The student is expected to:	
(A)	collaborate with others to create a technical report;	
(B)	create, review, and edit a report summarizing technical findings; and	
(C)	present technical information to a non-technical audience.	
(13)	Risk assessment. The student <u>understands risk and how risk assessment and risk management defend against attacks</u> analyzes various types of threats, attacks, and vulnerabilities. The student is expected to:	
(A)	differentiate types of attacks, including operating systems, software, hardware, network, physical, social engineering, and cryptographic;	Quantify risk: business impact analysis, user risk matrix
(B)	explain blended threats such as combinations of software, hardware, network, physical, social engineering, and cryptographic;	Likelihood of an attack to systems Most important to least important Website vs database behind the website Inventory...know what you have and prioritize
<u>(C)</u>	<u>discuss types of risk, including business, operational, security, and financial</u>	
(C) (D)	discuss risk response techniques, including accept, transfer, avoid, and mitigate;	
(D) (E)	develop a plan of preventative measures <u>based on discovered vulnerabilities and the likelihood of a cyberattack</u> to address cyberattacks;	Students need to understand the importance of most important to least important priorities
<u>(F)</u>	<u>identify and discuss common vulnerability disclosure websites;</u>	Added in vulnerability disclosure websites per industry feedback
(E) (G)	describe common web vulnerabilities such as cross-site scripting, buffer overflow, injection, spoofing, and denial of service;	Move up to C
(F) (H)	describe common data destruction and media sanitation practices such as wiping, shredding, and degaussing; and	
(G) (I)	develop an incident response plan for a given scenario or recent attack.	

(14)	Risk assessment. The student understands risk management processes and concepts. The student is expected to:	
(A)	describe <u>Zero Trust, least privilege, and</u> various access control methods such as mandatory access control (MAC), role-based access control (RBAC), and discretionary access control (DAC);	Controls: risk mgmt. framework Controls: planning and policy not just a software/technology solution, students review controls as they relate to security policies and practices Added in Zero Trust and least privilege per group and industry feedback
(B)	develop and defend a plan for multi-factor access control using components such as biometric verification systems, key cards, tokens, and passwords; and	
(C)	review <u>and appraise</u> a disaster recovery plan (DRP) that includes backups, redundancies, system dependencies, and alternate sites.	Increase rigor with new verbs
(15)	Risk assessment. The student investigates the role and effectiveness of environmental controls. The student is expected to:	
(A)	explain commonly used physical security controls, including lock types, fences, barricades, security doors, and mantraps; and	
(B)	describe the role of embedded systems such as fire suppression; heating, ventilation, and air conditioning (HVAC) systems; security alarms; and video monitoring.	

DRAFT

§130.424. Digital Forensics (One Credit), Adopted 2022, ~~Beginning with School Year 2019-2020~~

TEKS with edits		Work Group Comments/Rationale
(a)	General requirements. Students shall be awarded one credit for successful completion of this course. <u>Prerequisite: Foundations of Cybersecurity</u> . This course is recommended for students in Grades 9-12.	Committee decided that a prerequisite is required as foundations of cybersecurity.
(b)	Introduction.	
(1)	Career and technical education instruction provides content aligned with challenging academic standards and relevant technical knowledge and skills for students to further their education and succeed in current or emerging professions.	
(2)	The Science, Technology, Engineering, and Mathematics (STEM) Career Cluster focuses on planning, managing, and providing scientific research and professional and technical services, including laboratory and testing services, and research and development services.	
(3)	Digital forensics is <u>a critical</u> an evolving discipline concerned with analyzing anomalous activity on computers, networks, programs, and data. As a discipline, it has grown with the <u>expansion</u> emergence of a globally-connected digital society. As computing has become more sophisticated, so too have the abilities of malicious agents to access systems and <u>sensitive private</u> information. By evaluating prior incidents, d Digital forensics professionals have the ability to investigate and craft appropriate responses to disruptions to corporations , <u>organizations</u> , and individuals. Whereas cybersecurity takes a proactive approach to information assurance to minimize harm, digital forensics takes a reactive approach to incident response.	Group edited the intro to reflect the other courses and the group defines organizations as including corporations.
(4)	Digital Forensics introduces students to the knowledge and skills of digital forensics. The course provides a survey of the field of digital forensics and incident response.	
(5)	Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.	
(6)	Statements that contain the word "including" reference content that must be mastered, while those containing the phrase "such as" are intended as possible illustrative examples.	
(c)	Knowledge and skills.	
(1)	Employability skills. The student identifies necessary skills for career development and employment opportunities. The student is expected to:	
(A)	investigate the need for digital forensics;	
(B)	research careers in digital forensics along with the education and job skills required for obtaining a job in both the public and private sector;	
(C)	identify job and internship opportunities as well as accompanying duties and tasks;	

(D)	identify and discuss certifications for digital forensics careers;	
(E)	explain ethical and legal responsibilities in relation to the field of digital forensics;	
(F)	identify and describe businesses and government agencies that use digital forensics;	
(G)	identify and describe the kinds of crimes investigated by digital forensics specialists; and	
(H)	solve problems and think critically.	
(2)	Employability skills. The student communicates and collaborates effectively. The student is expected to:	
(A)	apply effective teamwork strategies;	
(B)	collaborate with a community of peers and professionals;	
(C)	create, review, and edit a report summarizing technical findings; and	
(D)	present technical information to a non-technical audience.	
(3)	Ethics and laws. The student recognizes and analyzes ethical and current legal standards, rights, and restrictions related to digital forensics. The student is expected to:	
(A)	develop a plan to advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;	
(B)	research local, state, national, and international law such as the Electronic Communications Privacy Act of 1986, Title III (Pen Register Act); USA PATRIOT Act of 2001; and Digital Millennium Copyright Act;	
(C)	research historic cases or events regarding digital forensics or cyber;	
(D)	examine ethical and legal behavior when presented with confidential or sensitive information in various scenarios related to cyber activities;	
(E)	analyze case studies of computer incidents;	
(F)	use the findings of a computer incident investigation to reconstruct the incident;	
(G)	identify and discuss intellectual property laws, issues, and use;	
(H)	contrast legal and illegal aspects of information gathering;	
(I)	contrast ethical and unethical aspects of information gathering;	
(J)	analyze emerging legal and societal trends affecting digital forensics; and	
(K)	discuss how technological changes affect applicable laws.	

(4)	Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding digital technology, safety, digital hygiene, and cyberbullying. The student is expected to:	
(A)	identify and use digital information responsibly;	
(B)	use digital tools responsibly;	
(C)	identify and use valid and reliable sources of information; and	
(D)	gain informed consent prior to investigating incidents.	
(5)	Digital forensics skills. The student locates, processes, analyzes, and organizes data. The student is expected to:	
(A)	identify sources of data;	
(B)	analyze and report data collected;	
(C)	maintain data integrity, <u>such as enabling encryption</u> ;	Added additional language per industry feedback
(D)	examine metadata of a file; and	
(E)	examine how multiple data sources can be used for digital forensics, including investigating malicious software (malware) and email threats.	
(6)	Digital forensics skills. The student understands software concepts and operations as they apply to digital forensics. The student is expected to:	
(A)	compare software applications as they apply to digital forensics;	
(B)	describe the purpose of various application types such as email, web, file sharing, security applications, and data concealment tools;	
(C)	identify the different purposes of data formats such as pdf, wav, jpeg, and exe;	
(D)	describe how application logs and metadata are used for investigations, <u>such as Security Information and Event Management (SIEM) reports</u> ;	Uses of log mgmt. tools, added SIEM to match industry feedback.
(E)	describe digital forensics tools;	
(F)	select the proper software tool based on appropriateness, effectiveness, and efficiency for a given digital forensics scenario; and	
(G)	describe components of applications such as configurations settings, data, supporting files, and user interface.	
(H)	<u>Describe how the “as a service” model applies to incident response</u>	Adding “as a service” model to fit with industry feedback and current trends

(7)	Digital forensics skills. The student understands operating systems concepts and functions as they apply to digital forensics. The student is expected to:	
(A)	compare various operating systems;	
(B)	describe file attributes, including access and creation times;	
(C)	describe how operating system logs are used for investigations;	
(D)	compare and contrast the file systems of various operating systems;	
(E)	compare various primary and secondary storage devices; and	
(F)	differentiate between volatile and non-volatile memory.	
(8)	Digital forensics skills. The student understands networking concepts and operations as they apply to digital forensics. The student is expected to:	
(A)	examine networks, including Internet Protocol (IP) addressing and subnets;	
(B)	describe the Open Systems Interconnection (OSI) model;	
(C)	describe the Transmission Control Protocol/Internet Protocol (TCP/IP) model;	
(D)	use network forensic analysis tools to examine network traffic data from sources such as firewalls, routers, intrusion detection systems (IDS), and remote access logs; and	
(E)	identify malicious or suspicious network activities such as mandatory access control (MAC) spoofing and rogue wireless access points.	
(9)	Digital forensics skills. The student explains the principles of access controls. The student is expected to:	
(A)	define the principle of least privilege;	
(B)	describe the impact of granting access and permissions;	
(C)	identify different access components such as passwords, tokens, key cards, and biometric verification systems;	
(D)	explain the value of an access log to identify suspicious activity;	
(E)	describe the risks of granting third parties access to personal and proprietary data on social media and systems;	
(F)	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; and	
(G)	identify various access control methods such as mandatory access control (MAC) , attribute-based access control (ABAC) , role-based access control (RBAC), and discretionary access control (DAC).	Added in additional terminology based on industry input.

(10)	Incident response. The student follows a methodological approach to prepare for and respond to an incident. The student is expected to:	
(A)	define the components of the incident response cycle, including preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity;	
(B)	describe incident response preparation;	
(C)	discuss incident response detection and analysis;	
(D)	discuss containment and eradication of and recovery from an incident;	
(E)	describe post-incident activities such as reflecting on lessons learned, using collected incident data, and retaining evidence of an incident;	
(F)	develop an incident response plan; and	
(G)	describe ways a user may compromise the validity of existing evidence.	
(11)	Incident response. The student objectively analyzes collected data from an incident. The student is expected to:	
(A)	identify the role of chain of custody in digital forensics;	
(B)	describe safe data handling procedures;	
(C)	explain the fundamental concepts of confidentiality, integrity, availability, authentication, and authorization;	
(D)	identify and report information conflicts or suspicious activity;	
(E)	identify events of interest and suspicious activity by examining network traffic; and	
(F)	identify events of interest and suspicious activity by examining event logs.	
(12)	Incident response. The student analyzes the various ways systems can be compromised. The student is expected to:	
(A)	analyze the different signatures of cyberattacks; and	
(B)	identify points of weakness and attack vectors such as online spoofing, phishing, and social engineering; <u>and</u>	
(C)	<u>differentiate between simple versus multistage attacks</u>	Adding in additional SE to mirror industry feedback with simple and multistage attacks.