# 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

| | |
|---|---|
| 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)

| | | |
|---|---|---|
| ~~(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 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 |

| | | |
|---|---|---|
| (D) | describe the trade-offs ~~inverse relationship~~ between convenience ~~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. such as conducting simulations; | |

(D)

| | | |
|---|---|---|
| (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) (Aexply.8 (c)-1.8 (t)-1 (ur)-481 re(h)-0.7 (15)-5.96 (p)-0.8 (g)-1.32 (k)166 (g)10.9 (e)- (t)-4-4.3 (k)108 (r)83.3.9 (.481 s)-2.  (t)-4.nd .8 (c)-1ub(u)10.9 (c

| | | |
|---|---|---|
| (C)~~(A)~~ | describe the impact of granting applications unnecessary permissions such as mobile devices accessing camera and contacts; | 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) | Risk assessment. The student understands risk, and how risk assessment and risk management defend against attacks. The student is expected to: | Adding in new KS and SEs<br>From Tech Apps work: demonstrate adherence to Acceptable Use Policy (AUP) and practice and model safe, ethical, and positive online behaviors; |
| (A) | define commonly used risk assessment terms, including risk, asset, and inventory; | Group wanted students to understand term used in risk |
| (B) | identify risk management strategies, including acceptance, avoidance, transference, and mitigation; | risk mgmt. strategies<br>acceptance avoidance transference<br>mitigation |

| | | |
|---|---|---|
| (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 cybersecurity laws such as David's Law and Digital Millennium Copyright Act; | |
| (B) | evaluate noteworthy ~~historic~~ incidents ~~cases~~ or events regarding cybersecurity; and | Noteworthy encompasses more then just historic. |
| (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), and Cybersecurity Maturity Model Certification (CMMC). | Change verb for more rigor |

| | | |
|---|---|---|
| (B) | differentiate between ~~identify~~ ethical and ~~or~~ unethical behavior when presented with various scenarios related to cybersecurity ~~cyber~~ activities. | More rigor in verb and including both ethica and unethical |

(5) Cyberifn.04 re f-4 (e)9.3 ( )-11 (r)-1.7 (r) [(ie f .69 0.3c ( ) ET 0 o19[(ie f .69[(()-4 (5))]TJ ETic)-10.7 (u)-9 (r)-12.9 (i (u)-9 (r)-1 0.48 0.48 re f.2 (a)-(r

| | | |
|---|---|---|
| (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 and cloud architecture; | Added cloud architecture via industry feedback. |
| (C) | evaluate ~~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, indicators, or patterns; | |

| | | |
|---|---|---|
| (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 understands risk and how risk assessment and risk management defend against attacks ~~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, us<br>risk matrix |
| (B) | explain blended threats such as combinations of software, hardware, network, physical, social engineering, and cryptographic;(24 343-7.7 f(2)- Tm i-1.6 4n(s)8sobusc]TJ ET | Likelihood |

| | | |
|---|---|---|
| (14) | Risk assessment. The student understands risk management processes and concepts. The student is expected to: | |
| (A) | describe Zero Trust, least privilege, and various access control methods such as mandatory access control (MAC), role-based access control (RBAC), and discretionary access control (DAC); | Controls:  risk mgmt. framework<br>Controls:  planning and policy not just a software/technology solution, students review controls as they relate to secu0 Tc 0 To sseacy |

| §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. Prerequisite: Foundations of Cybersecurity. This course is recommended for students in Grades 9-12. | Committee decided that a prerequisite is required as foundations of cybersecurity. |
| (b) | Introduction. | |

(1)

|  |  |  |
|---|---|---|
| (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 Transmi |  |

[redacted]

0)13.7 (22