ATTACHMENT
Text of Proposed New 19 TAC

Chapter 127. Texas Essential Knowledge and Skills for Career Development and Career and Technical Education

Subchapter O. Science, Technology, Engineering, and Mathematics

§127.788. Fundamentals of Computer Science (One Credit), Adopted 2022.

(a) Implementation. The provisions of this section shall be implemented by school districts beginning with the 2023-2024 school year.

(1) No later than August 1, 2023, the commissioner of education shall determine whether instructional materials funding has been made available to Texas public schools for materials that cover the essential knowledge and skills identified in this section.

(2) If the commissioner makes the determination that instructional materials funding has been made available this section shall be implemented beginning with the 2023-2024 school year and apply to the 2023-2024 and subsequent school years.

(3) If the commissioner does not make the determination that instructional materials funding has been made available under subsection (a) of this section, the commissioner shall determine no later than August 1 of each subsequent school year whether instructional materials funding has been made available. If the commissioner determines that instructional materials funding has been made available, the commissioner shall notify the State Board of Education and school districts that this section shall be implemented for the following school year.

(b) General requirements. This course is recommended for students in Grades 9-12.Students shall be awarded one credit for successful completion of this course.

(c) Introduction.

(1) Career and technical education instruction provides content aligned with challenging academic standards, industry-relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and 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 such as laboratory and testing services and research and development services.

(3) Fundamentals of Computer Science is intended as a first course for those students just beginning the study of computer science. Students will learn about the computing tools that are used every day. Students will foster their creativity and innovation through opportunities to design, implement, and present solutions to real-world problems. Students will collaborate and use computer science concepts to access, analyze, and evaluate information needed to solve problems. Students will learn computational thinking, problem-solving, and reasoning skills that are the foundation of computer science. By using computer science knowledge and skills that support the work of individuals and groups in solving problems, students will select the technology appropriate for the task, synthesize knowledge, create solutions, and evaluate the results. Students will learn digital citizenship by researching current laws, regulations, and best practices and by practicing integrity and respect. Students will gain an understanding of the principles of computer science through the study of technology operations and concepts.

(4) Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

(5) 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.

(d) Knowledge and skills.

(1) Employability. The student identifies various employment opportunities in the computer science field. The student is expected to:

(A) identify job opportunities and accompanying job duties and tasks;

(B) examine the role of certifications, resumes, and portfolios in the computer science profession;

(C) employ effective technical reading and writing skills;

(D) employ effective verbal and non-verbal communication skills;

(E) solve problems and think critically;

(F) demonstrate leadership skills and function effectively as a team member;

(G) demonstrate an understanding of legal and ethical responsibilities in relation to the field of computer science;

(H) demonstrate planning and time-management skills; and

(I) compare university computer science programs.

(2) Creativity and innovation. The student develops products and generates new knowledge, understanding, and skills. The student is expected to:

(A) investigate and explore various career opportunities within the computer science field and report findings through various media;

(B) create algorithms for the solution of various problems;

(C) discuss methods and create and publish web pages using a web-based language such as HTML, Java Script, or XML; and

(D) use generally accepted design standards for spacing, fonts, and color schemes to create functional user interfaces, including static and interactive screens.

(3) Communication and collaboration. The student communicates and collaborates with peers to contribute to his or her own learning and the learning of others. The student is expected to:

(A) seek and respond to advice or feedback from peers, educators, or professionals when evaluating problem solutions;

(B) debug and solve problems using reference materials and effective strategies; and

(C) publish information in a variety of ways such as print, monitor display, web pages, or video.

(4) Critical thinking, problem solving, and decision making. The student uses appropriate strategies to analyze problems and design algorithms. The student is expected to:

(A) demonstrate the ability to insert external standalone objects such as scripts or widgets into web pages;

(B) communicate an understanding of binary representation of data in computer systems, perform conversions between decimal and binary number systems, and count in binary number systems;

(C) identify a problem's description, purpose, and goals;

(D) demonstrate coding proficiency in a programming language by developing solutions that create stories, games, and animations;

(E) identify and use the appropriate data type to properly represent the data in a program problem solution;

(F) communicate an understanding of and use variables within a programmed story, game, or animation;

(G) use arithmetic operators to create mathematical expressions, including addition, subtraction, multiplication, real division, integer division, and modulus division;

(H) communicate an understanding of and use sequence within a programmed story, game, or animation;

(I) communicate an understanding of and use conditional statements within a programmed story, game, or animation;

(J) communicate an understanding of and use iteration within a programmed story, game, or animation;

(K) use random numbers within a programmed story, game, or animation; and

(L) test program solutions by investigating intended outcomes.

(5) Digital citizenship. The student explores and understands safety, legal, cultural, and societal issues relating to the use of technology and information. The student is expected to:

(A) discuss privacy and copyright laws and model ethical acquisition of digital information by citing sources using established methods;

(B) compare various non-copyright asset sharing options such as open source, freeware, and public domain;

(C) demonstrate proper digital etiquette and knowledge of acceptable use policies when using networks;

(D) explain the value of strong passwords and virus detection and prevention for privacy and security;

(E) discuss and give examples of the impact of computing and computing-related advancements on society; and

(F) analyze how electronic media can affect reliability of information.

(6) Technology operations and concepts. The student understands technology concepts, systems, and operations as they apply to computer science. The student is expected to:

(A) identify and explain the function of basic computer components, including a central processing unit (CPU), storage, and peripheral devices;

(B) use system tools, including appropriate file management;

(C) compare different operating systems;

(D) describe the differences between an application and an operating system; and

(E) use various input, processing, output, and primary/secondary storage devices.

§127.789. Computer Science I (One Credit), Adopted 2022.

(a) Implementation. The provisions of this section shall be implemented by school districts beginning with the 2024-2025 school year.

(1) No later than August 1, 2024, the commissioner of education shall determine whether instructional materials funding has been made available to Texas public schools for materials that cover the essential knowledge and skills identified in this section.

(2) If the commissioner makes the determination that instructional materials funding has been made available this section shall be implemented beginning with the 2024-2025 school year and apply to the 2024-2025 and subsequent school years.

(3) If the commissioner does not make the determination that instructional materials funding has been made available under subsection (a) of this section, the commissioner shall determine no later than August 1 of each subsequent school year whether instructional materials funding has been made

available. If the commissioner determines that instructional materials funding has been made available, the commissioner shall notify the State Board of Education and school districts that this section shall be implemented for the following school year.

(b) General requirements. This course is recommended for students in Grades 9-12. Prerequisite or corequisite: Algebra I. Students shall be awarded one credit for successful completion of this course.

(c) Introduction.

(1) Career and technical education instruction provides content aligned with challenging academic standards, industry-relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and 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 such as laboratory and testing services and research and development services.

(3) Computer Science I will foster students' creativity and innovation by presenting opportunities to design, implement, and present meaningful programs through a variety of media. Students will collaborate with one another, their instructor, and various electronic communities to solve the problems presented throughout the course. Through computational thinking and data analysis, students will identify task requirements, plan search strategies, and use computer science concepts to access, analyze, and evaluate information needed to solve problems. By using computer science knowledge and skills that support the work of individuals and groups in solving problems, students will select the technology appropriate for the task, synthesize knowledge, create solutions, and evaluate the results. Students will learn digital citizenship by researching current laws, regulations, and best practices and by practicing integrity and respect. Students will gain an understanding of the principles of computer science through the study of technology operations, systems, and concepts.

(4) Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

(5) 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.

(d) Knowledge and skills.

(1) Employability. The student identifies various employment opportunities in the computer science field. The student is expected to:

(A) identify job opportunities and accompanying job duties and tasks;

(B) examine the role of certifications, resumes, and portfolios in the computer science profession;

(C) employ effective technical reading and writing skills;

(D) employ effective verbal and non-verbal communication skills;

(E) solve problems and think critically;

(F) demonstrate leadership skills and function effectively as a team member;

(G) communicate an understanding of legal and ethical responsibilities in relation to the field of computer science;

(H) demonstrate planning and time-management skills; and

(I) compare university computer science programs.

(2) Communication and collaboration. The student communicates and collaborates with peers to contribute to his or her own learning and the learning of others. The student is expected to:

(A) participate in learning communities as a learner, initiator, contributor, and teacher/mentor; and

(B) seek and respond to advice from peers, educators, or professionals when evaluating quality and accuracy of the student's product.

(3) Programming style and presentation. The student utilizes proper programming style and develops appropriate visual presentation of data, input, and output. The student is expected to:

(A) create and properly label and display output;

(B) create interactive input interfaces, with relevant user prompts, to acquire data from a user such as console displays or Graphical User Interfaces (GUIs);

(C) write programs with proper programming style to enhance the readability and functionality of a code by using descriptive identifiers, internal comments, white space, spacing, indentation, and a standardized program style;

(D) format data displays using standard formatting styles; and

(E) display simple vector graphics using lines, circles, and rectangles.

(4) Critical thinking, problem solving, and decision making. The student uses appropriate strategies to analyze problems and design algorithms. The student is expected to:

(A) use program design problem-solving strategies such as flowchart or pseudocode to create program solutions;

(B) create a high-level program plan using a visual tool such as a flowchart or graphic organizer;

(C) identify the tasks and subtasks needed to solve a problem;

(D) identify the data types and objects needed to solve a problem;

(E) identify reusable components from existing code;

(F) design a solution to a problem;

(G) code a solution from a program design;

(H) identify error types, including syntax, lexical, run time, and logic;

(I) test program solutions with valid and invalid test data and analyze resulting behavior;

(J) debug and solve problems using error messages, reference materials, language documentation, and effective strategies;

(K) create and implement common algorithms such as finding greatest common divisor, finding the biggest number out of three, finding primes, making change, and finding the average;

(L) create program solutions that address basic error handling such as preventing division by zero and type mismatch;

(M) select the most appropriate construct for a defined problem;

(N) create program solutions by using the arithmetic operators to create mathematical expressions, including addition, subtraction, multiplication, real division, integer division, and modulus division;

(O) create program solutions to problems using available mathematics library functions or operators, including absolute value, round, power, square, and square root;

(P) develop program solutions that use assignment;

(Q) develop sequential algorithms to solve non-branching and non-iterative problems;

(R) develop algorithms to decision-making problems using branching control statements;

(S) develop iterative algorithms and code programs to solve practical problems;

(T) demonstrate the appropriate use of the relational operators;

(U) demonstrate the appropriate use of the logical operators; and

(V) generate and use random numbers.

(5) Digital citizenship. The student explores and understands safety, legal, cultural, and societal issues relating to the use of technology and information. The student is expected to:

(A) discuss and explain intellectual property, privacy, sharing of information, copyright laws, and software licensing agreements;

(B) practice ethical acquisition and use of digital information;

(C) demonstrate proper digital etiquette, responsible use of software, and knowledge of acceptable use policies;

(D) investigate privacy and security measures, including strong passwords, pass phrases, and other methods of authentication and virus detection and prevention; and

(E) investigate computing and computing-related advancements and the social and ethical ramifications of computer usage.

(6) Technology operations, systems, and concepts. The student understands technology concepts, systems, and operations as they apply to computer science. The student is expected to:

(A) identify and describe the function of major hardware components, including primary and secondary memory, a central processing unit (CPU), and peripherals;

(B) differentiate between current programming languages, discuss the general purpose for each language, and demonstrate knowledge of specific programming terminology and concepts and types of software development applications;

(C) differentiate between a high-level compiled language and an interpreted language;

(D) identify and use concepts of object-oriented design;

(E) differentiate between local and global scope access variable declarations;

(F) encapsulate data and associated subroutines into an abstract data type;

(G) create subroutines that do not return values with and without the use of arguments and parameters;

(H) create subroutines that return typed values with and without the use of arguments and parameters;

(I) create calls to processes passing arguments that match parameters by number, type, and position;

(J) compare data elements using logical and relational operators;

(K) identify and convert binary representation of numeric and nonnumeric data in computer systems using American Standard Code for Information Interchange (ASCII) or Unicode;

(L) identify finite limits of numeric data such as integer wrap around and floating point precision;

(M) perform numerical conversions between the decimal and binary number systems and count in the binary number system;

(N) choose, identify, and use the appropriate data types for integer, real, and Boolean data when writing program solutions;

(O) analyze the concept of a variable, including primitives and objects;

(P) represent and manipulate text data, including concatenation and other string functions;

(Q) identify and use the structured data type of one-dimensional arrays to traverse, search, and modify data;

(R) choose, identify, and use the appropriate data type or structure to properly represent the data in a program problem solution; and

(S) compare strongly typed and un-typed programming languages.

§127.790. Computer Science II (One Credit), Adopted 2022.

(a) Implementation. The provisions of this section shall be implemented by school districts beginning with the 2024-2025 school year.

(1) No later than August 1, 2024, the commissioner of education shall determine whether instructional materials funding has been made available to Texas public schools for materials that cover the essential knowledge and skills identified in this section.

(2) If the commissioner makes the determination that instructional materials funding has been made available this section shall be implemented beginning with the 2024-2025 school year and apply to the 2024-2025 and subsequent school years.

(3) If the commissioner does not make the determination that instructional materials funding has been made available under subsection (a) of this section, the commissioner shall determine no later than August 1 of each subsequent school year whether instructional materials funding has been made available. If the commissioner determines that instructional materials funding has been made available, the commissioner shall notify the State Board of Education and school districts that this section shall be implemented for the following school year.

(b) General requirements. This course is recommended for students in Grades 10-12. Prerequisites: Algebra I and Computer Science I or AP Computer Science Principles. Students shall be awarded one credit for successful completion of this course.

(c) Introduction.

(1) Career and technical education instruction provides content aligned with challenging academic standards, industry-relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and 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 such as laboratory and testing services and research and development services.

(3) Computer Science II will foster students' creativity and innovation by presenting opportunities to design, implement, and present meaningful programs through a variety of media. Students will collaborate with one another, their instructor, and various electronic communities to solve the problems presented throughout the course. Through computational thinking and data analysis, students will identify task requirements, plan search strategies, and use computer science concepts to access, analyze, and evaluate information needed to solve problems. By using computer science knowledge and skills that support the work of individuals and groups in solving problems, students will select the technology appropriate for the task, synthesize knowledge, create solutions, and evaluate the results. Students will gain an understanding of computer science through the study of technology operations, systems, and concepts.

(4) Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

(5) 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.

(d) Knowledge and skills.

(1) Employability. The student identifies various employment opportunities in the computer science field. The student is expected to:

(A) identify job opportunities and accompanying job duties and tasks;

(B) examine the role of certifications, resumes, and portfolios in the computer science profession;

(C) employ effective technical reading and writing skills;

(D) employ effective verbal and non-verbal communication skills;

(E) solve problems and think critically;

(F) demonstrate leadership skills and function effectively as a team member;

(G) identify legal and ethical responsibilities in relation to the field of computer science;

(H) demonstrate planning and time-management skills; and

(I) compare university computer science programs.

(2) Creativity and innovation. The student develops products and generates new understandings by extending existing knowledge. The student is expected to:

(A) use program design problem-solving strategies to create program solutions;

(B) read, analyze, and modify programs and their accompanying documentation such as an application programming interface (API), internal code comments, external documentation, or readme files;

(C) follow a systematic problem-solving process that identifies the purpose and goals, the data types and objects needed, and the subtasks to be performed;

(D) compare design methodologies and implementation techniques such as top-down, bottom-up, and black box;

(E) trace a program, including inheritance and black box programming;

(F) choose, identify, and use the appropriate abstract data type, advanced data structure, and supporting algorithms to properly represent the data in a program problem solution; and

(G) use object-oriented programming development methodology, including data abstraction, encapsulation with information hiding, inheritance, and procedural abstraction in program development.

(3) Communication and collaboration. The student communicates and collaborates with peers to contribute to his or her own learning and the learning of others. The student is expected to:

(A) use the principles of software development to work in software design teams;

(B) break a problem statement into specific solution requirements;

(C) create a program development plan;

(D) code part of a solution from a program development plan while a partner codes the remaining part;

(E) collaborate with a team to test a solution, including boundary and standard cases; and

(F) develop presentations to report the solution findings.

(4) Data literacy and management. The student locates, analyzes, processes, and organizes data. The student is expected to:

(A) use programming file structure and file access for required resources;

(B) acquire and process information from text files, including files of known and unknown sizes;

(C) manipulate data using string processing;

(D) manipulate data values by casting between data types;

(E) use the structured data type of one-dimensional arrays to traverse, search, modify, insert, and delete data;

(F) identify and use the structured data type of two-dimensional arrays to traverse, search, modify, insert, and delete data;

(G) identify and use a list object data structure to traverse, search, insert, and delete data; and

(H) differentiate between categories of programming languages, including machine, assembly, high-level compiled, high-level interpreted, and scripted.

(5) Critical thinking, problem solving, and decision making. The student uses appropriate strategies to analyze problems and design algorithms. The student is expected to:

(A) develop sequential algorithms using branching control statements, including nested structures, to create solutions to decision-making problems;

(B) develop choice algorithms using selection control statements based on ordinal values;

(C) demonstrate the appropriate use of short-circuit evaluation in certain situations;

(D) use Boolean algebra, including De Morgan's Law, to evaluate and simplify logical expressions;

(E) develop iterative algorithms using nested loops;

(F) identify, trace, and appropriately use recursion in programming solutions, including algebraic computations;

(G) trace, construct, evaluate, and compare search algorithms, including linear searching and binary searching;

(H) identify, describe, trace, evaluate, and compare standard sorting algorithms, including selection sort, bubble sort, insertion sort, and merge sort;

(I) measure time and space efficiency of various sorting algorithms, including analyzing algorithms using "big-O" notation for best, average, and worst-case data patterns;

(J) develop algorithms to solve various problems such as factoring, summing a series, finding the roots of a quadratic equation, and generating Fibonacci numbers;

(K) test program solutions by investigating boundary conditions; testing classes, methods, and libraries in isolation; and performing stepwise refinement;

(L) identify and debug compile, syntax, runtime, and logic errors;

(M) compare efficiency of search and sort algorithms by using informal runtime comparisons, exact calculation of statement execution counts, and theoretical efficiency values using "big-O" notation, including worst-case, best-case, and average-case time/space analysis;

(N) count, convert, and perform mathematical operations in the decimal, binary, octal, and hexadecimal number systems;

(O) identify maximum integer boundary, minimum integer boundary, imprecision of real number representations, and round-off errors;

(P) create program solutions to problems using a mathematics library;

(Q) use random number generator algorithms to create simulations;

(R) use composition and inheritance relationships to identify and create class definitions and relationships;

(S) explain and use object relationships between defined classes, abstract classes, and interfaces;

(T) create object-oriented class definitions and declarations using variables, constants, methods, parameters, and interface implementations;

(U) create adaptive behaviors using polymorphism;

(V) use reference variables for object and string data types;

(W) use value and reference parameters appropriately in method definitions and method calls;

(X) implement access scope modifiers;

(Y) use object comparison for content quality;

(Z) duplicate objects using the appropriate deep or shallow copy;

(AA) apply functional decomposition to a program solution;

(BB) create objects from class definitions through instantiation; and

(CC) examine and mutate the properties of an object using accessors and modifiers.

§127.791. Computer Science III (One Credit), Adopted 2022.

(a) Implementation. The provisions of this section shall be implemented by school districts beginning with the 2023-2024 school year.

(1) No later than August 1, 2023, the commissioner of education shall determine whether instructional materials funding has been made available to Texas public schools for materials that cover the essential knowledge and skills identified in this section.

(2) If the commissioner makes the determination that instructional materials funding has been made available this section shall be implemented beginning with the 2023-2024 school year and apply to the 2023-2024 and subsequent school years.

(3) If the commissioner does not make the determination that instructional materials funding has been made available under subsection (a) of this section, the commissioner shall determine no later than August 1 of each subsequent school year whether instructional materials funding has been made available. If the commissioner determines that instructional materials funding has been made available, the commissioner shall notify the State Board of Education and school districts that this section shall be implemented for the following school year.

(b) General requirements. This course is recommended for students in Grades 11 and 12. Prerequisite: Computer Science II, Advanced Placement (AP) Computer Science A, or International Baccalaureate (IB) Computer Science Standard Level or IB Computer Science Higher Level. Students shall be awarded one credit for successful completion of this course.

(c) Introduction.

(1) Career and technical education instruction provides content aligned with challenging academic standards, industry-relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and 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 such as laboratory and testing services and research and development services.

(3) Computer Science III will foster students' creativity and innovation by presenting opportunities to design, implement, and present meaningful programs through a variety of media. Students will collaborate with one another, their instructor, and various electronic communities to solve the

problems presented throughout the course. Through computational thinking and data analysis, students will identify task requirements, plan search strategies, and use computer science concepts to access, analyze, and evaluate information needed to solve problems. By using computer science knowledge and skills that support the work of individuals and groups in solving problems, students will select the technology appropriate for the task, synthesize knowledge, create solutions, and evaluate the results. Students will gain an understanding of advanced computer science data structures through the study of technology operations, systems, and concepts.

(4) Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

(5) 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.

(6) Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

(d) Knowledge and skills.

(1) Employability. The student identifies various employment opportunities in the computer science field. The student is expected to:

(A) identify job opportunities and accompanying job duties and tasks;

(B) examine the role of certifications, resumes, and portfolios in the computer science profession;

(C) employ effective technical reading and writing skills;

(D) employ effective verbal and non-verbal communication skills;

(E) solve problems and think critically;

(F) demonstrate leadership skills and function effectively as a team member;

(G) demonstrate an understanding of legal and ethical responsibilities in relation to the field of computer science;

(H) demonstrate planning and time-management skills; and

(I) compare university computer science programs.

(2) Creativity and innovation. The student develops products and generates new understandings by extending existing knowledge. The student is expected to:

(A) apply object-oriented programming, including data abstraction, encapsulation, inheritance, and polymorphism, to manage the complexity of a project;

(B) design and implement a class hierarchy;

(C) read and write class specifications using visual organizers, including Unified Modeling Language;

(D) identify, describe, evaluate, compare, and implement standard sorting algorithms that perform sorting operations on data structures, including quick sort and heap sort; and

(E) identify and use the appropriate abstract data type, advanced data structure, and supporting algorithms to properly represent the data in a program problem solution.

(3) Communication and collaboration. The student communicates and collaborates with peers to contribute to his or her own learning and the learning of others. The student is expected to:

(A) use networked tools for file management and collaboration; and

(B) work in software design teams.

(4) Data literacy and management. The student locates, analyzes, processes, and organizes data. The student is expected to:

(A) identify and use two-dimensional ragged arrays to traverse, search, modify, insert, and delete data;

(B) describe and demonstrate proper linked list management, including maintaining the head and safe addition and deletion of linked objects;

(C) create or trace program solutions using a linked-list data structure, including unordered single, ordered single, double, and circular linked;

(D) describe composite data structures, including a linked list of linked lists;

(E) create or trace program solutions using stacks, queues, trees, heaps, priority queues, graph theory, and enumerated data types;

(F) create or trace program solutions using sets, including hash and tree-based data structures;

(G) create or trace program solutions using map style data structures; and

(H) write and modify text file data.

(5) Critical thinking, problem solving, and decision making. The student uses appropriate strategies to analyze problems and design algorithms. The student is expected to:

(A) evaluate expressions using bitwise operators;

(B) evaluate expressions using the ternary operator;

(C) identify, trace, and appropriately use recursion in programming solutions, including processing binary trees;

(D) create or trace program solutions using hashing;

(E) explore common algorithms such as matrix addition and multiplication, fractals, Towers of Hanoi, and magic square; and

(F) create program solutions that exhibit robust behavior by recognizing and avoiding runtime errors and handling anticipated errors.

(6) Testing and documentation. The student demonstrates appropriate documentation and testing practices. The student is expected to:

(A) use appropriate formatting and write documentation to support code maintenance, including pre- and post-condition statements;

(B) write program assumptions in the form of assertions;

(C) write a Boolean expression to test a program assertion; and

(D) construct assertions to make explicit program invariants.

(7) Practical application of technology. The student utilizes technology concepts, systems, and operations as they apply to computer science. The student is expected to:

(A) analyze and create computer program workflow charts and basic system diagrams, documenting system functions, features, and operations;

(B) gather requirements, design, and implement a process by which programs can interact with each other such as using interfaces;

(C) create simple programs using a low-level language such as assembly;

(D) create discovery programs in a high-level language;

(E) create scripts for an operating system;

(F) explore industry best practices for secure programming; and

(G) explore emerging industry or technology trends.

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

(a) Implementation. The provisions of this section shall be implemented by school districts beginning with the 2023-2024 school year.

(1) No later than August 1, 2023, the commissioner of education shall determine whether instructional materials funding has been made available to Texas public schools for materials that cover the essential knowledge and skills identified in this section.

(2) If the commissioner makes the determination that instructional materials funding has been made available this section shall be implemented beginning with the 2023-2024 school year and apply to the 2023-2024 and subsequent school years.

(3) If the commissioner does not make the determination that instructional materials funding has been made available under this subsection, the commissioner shall determine no later than August 1 of each subsequent school year whether instructional materials funding has been made available. If the commissioner determines that instructional materials funding has been made available, the commissioner shall notify the State Board of Education and school districts that this section shall be implemented for the following school year.

(b) General requirements. This course is recommended for students in Grades 9-12.Students shall be awarded one credit for successful completion of this course.

(c) Introduction.

(1) Career and technical education instruction provides content aligned with challenging academic standards, industry and relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and 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 such as laboratory and testing services and research and development services.

(3) Cybersecurity is a critical discipline concerned with safeguarding computers, networks, programs, and data from unauthorized access. As a field, it has gained prominence with the expansion of a globally connected society. As computing has become more sophisticated, so too have the abilities of adversaries looking to penetrate networks and access systems and sensitive information. Cybersecurity professionals prevent, detect, and respond to minimize disruptions to governments, organizations, and individuals.

(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.

(d) 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 and ramifications in relation to the field of cybersecurity.

(2) Professional awareness. The student identifies various employment opportunities and requirements in the cybersecurity field. The student is expected to:

(A) identify job and internship opportunities and accompanying job duties and tasks;

(B) research careers in cybersecurity and information security and develop professional profiles that match education and job skills required for obtaining a job in both the public and private sectors;

(C) identify and discuss certifications for cybersecurity-related careers; and

(D) explain the different types of services and roles found within a cybersecurity functional area such as a security operations center (SOC).

(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:

(A) demonstrate and advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;

(B) investigate and analyze local, state, national, and international cybersecurity laws such as the USA PATRIOT Act of 2001, General Data Protection Regulation, Digital Millennium Copyright Act, Computer Fraud and Abuse Act, and Health Insurance Portability and Accountability Act of 1996 (HIPAA);

(C) investigate and analyze noteworthy incidents or events regarding cybersecurity;

(D) communicate an understanding of ethical and legal behavior when presented with various scenarios related to cybersecurity activities;

(E) define and identify tactics used in an incident such as social engineering, malware, denial of service, spoofing, and data vandalism; and

(F) identify and use appropriate methods for citing sources.

(4) Ethics and laws. The student differentiates between ethical and malicious hacking. The student is expected to:

(A) identify motivations and perspectives for hacking;

(B) distinguish between types of threat actors such as hacktivists, criminals, state-sponsored actors, and foreign governments;

(C) identify and describe the impact of cyberattacks on the global community, society, and individuals;

(D) differentiate between industry terminology for types of hackers such as black hats, white hats, and gray hats; and

(E) determine and describe possible outcomes and legal ramifications of ethical versus malicious hacking practices.

(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;

(D) explain the role of cyber defense in protecting national interests and corporations;

(E) explain 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 from cyberterrorism.

(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 deter and report cyberbullying.

(7) Digital citizenship. The student understands the implications of sharing information and access with others. The student is expected to:

(A) define personally identifiable information (PII);

(B) evaluate the risks and benefits of sharing PII;

(C) describe the impact of granting applications unnecessary permissions such as mobile devices accessing camera and contacts;

(D) describe the risks of granting third parties access to personal and proprietary data on social media and systems; and

(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.

(8) Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:

(A) define cybersecurity and information security;

(B) identify basic risk management and risk assessment principles related to cybersecurity threats and vulnerabilities, including the Zero Trust model;

(C) explain the fundamental concepts of confidentiality, integrity, and availability (CIA triad);

(D) describe the trade-offs between convenience and security;

(E) identify and analyze cybersecurity breaches and incident responses;

(F) identify and analyze security challenges in domains such as physical, network, cloud, and web;

(G) define and discuss challenges faced by cybersecurity professionals such as internal and external threats;

(H) identify indicators of compromise such as common risks, warning signs, and alerts of compromised systems;

(I) explore and discuss the vulnerabilities of network-connected devices such as Internet of Things (IoT);

(J) use appropriate cybersecurity terminology;

(K) explain the concept of penetration testing, including tools and techniques; and

(L) explore and identify common industry frameworks such as MITRE ATT&CK™, MITRE Engage™, and Cyber Kill Chain, and the Diamond Model.

(9) 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 trojan horses, worms, and viruses;

(C) discuss the impact of malware and the model of "as a service";

(D) explain the role of reverse engineering for the detection of malware and viruses; and

(E) describe free and commercial antivirus and anti-malware software also known as Endpoint Detection and Response software.

(10) 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) use basic 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;

(G) research and explain standard practices for securing computers, networks, and operating systems, including the concept of least privilege; and

(H) identify vulnerabilities caused by a lack of cybersecurity awareness and training such as weaknesses posed by individuals within an organization.

(11) Cybersecurity skills. The student understands basic network operations. The student is expected to:

(A) identify basic network devices, including routers and switches;

(B) define network addressing;

(C) analyze incoming and outgoing rules for traffic passing through a firewall;

(D) identify well known ports by number and service provided, including port 22 (Secure Shell Protocol/ssh), port 80 (Hypertext Transfer Protocol/http), and port 443 (Hypertext Transfer Protocol Secure/https);

(E) identify commonly exploited ports and services, including ports 20 and 21 (File Transfer Protocol/ftp), port 23 (telnet protocol), and port 3389 (Remote Desktop Protocol/rdp); and

(F) identify common tools for monitoring ports and network traffic.

(12) 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) Cybersecurity skills. The student demonstrates necessary steps to maintain user access on the system. The student is expected to:

(A) identify 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 auditing;

(C) compare methods for single- and multi-factor authentication such as passwords, biometrics, personal identification numbers (PINs), secure tokens, and other passwordless authentication methods;

(D) define and explain the purpose and benefits of an air-gapped computer; and

(E) explain how hashes and checksums may be used to validate the integrity of transferred data.

(14) Cybersecurity skills. The student explores the field of digital forensics. The student is expected to:

(A) explain the importance of digital forensics to organizations, private citizens, and the public sector;

(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;

(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) 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;

(C) review and explain simple cryptography methods such as shift cipher and substitution cipher;

(D) define and explain public key encryption; and

(E) compare and contrast symmetric and asymmetric encryption.

(16) Vulnerabilities, threats, and attacks. The student understands vulnerabilities, threats, and attacks. The student is expected to:

(A) explain how computer vulnerabilities leave systems open to cyberattacks;

(B) explain how users are the most common vehicle for compromising a system at the application level;

(C) define and describe vulnerability, payload, exploit, port scanning, and packet sniffing;

(D) identify internal threats to systems such as logic bombs and insider threats;

(E) define and describe cyberattacks, including man-in-the-middle, distributed denial of service, spoofing, and back-door attacks;

(F) differentiate types of social engineering techniques such as phishing; web links in email, instant messaging, social media, and other online communication with malicious links; shoulder surfing; and dumpster diving; and

(G) identify various types of application-specific attacks such as cross-site scripting and injection attacks.

(17) Vulnerabilities, threats, and attacks. The student evaluates the vulnerabilities of networks. The student is expected to:

(A) compare vulnerabilities associated with connecting devices to public and private networks;

(B) explain device vulnerabilities and security solutions on networks such as supply chain security and counterfeit products;

(C) compare and contrast protocols such as HTTP versus HTTPS;

(D) debate the broadcasting or hiding of a wireless service set identifier (SSID); and

(E) research and discuss threats such as mandatory access control (MAC) spoofing and packet sniffing.

(18) Vulnerabilities, threats, and attacks. 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 policies and practices;

(C) explain the purpose and function of vulnerability scanners;

(D) explain how coding errors may create system vulnerabilities such as buffer overflows and lack of input validation; and

(E) analyze the risks of distributing insecure programs.

(19) Risk assessment. The student understands risk and how risk assessment and risk management defend against attacks. The student is expected to:

(A) define commonly used risk assessment terms, including risk, asset, and inventory;

(B) identify risk management strategies, including acceptance, avoidance, transference, and mitigation; and

(C) compare and contrast risks based on an industry accepted rubric or metric such as Risk Assessment Matrix.

§127.793. Digital Forensics (One Credit), Adopted 2022.

(a) Implementation. The provisions of this section shall be implemented by school districts beginning with the 2023-2024 school year.

(1) No later than August 1, 2023, the commissioner of education shall determine whether instructional materials funding has been made available to Texas public schools for materials that cover the essential knowledge and skills identified in this section.

(2) If the commissioner makes the determination that instructional materials funding has been made available this section shall be implemented beginning with the 2023-2024 school year and apply to the 2023-2024 and subsequent school years.

(3) If the commissioner does not make the determination that instructional materials funding has been made available under this subsection, the commissioner shall determine no later than August 1 of each subsequent school year whether instructional materials funding has been made available. If the commissioner determines that instructional materials funding has been made available, the commissioner shall notify the State Board of Education and school districts that this section shall be implemented for the following school year.

(b) General requirements. This course is recommended for students in Grades 9-12. Prerequisite: Foundations of Cybersecurity. Students shall be awarded one credit for successful completion of this course.

(c) Introduction.

(1) Career and technical education instruction provides content aligned with challenging academic standards, , industry relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and 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, such as laboratory and testing services and research and development services.

(3) Digital forensics is a critical discipline concerned with analyzing anomalous activity on computers, networks, programs, and data. As a discipline, it has grown with the expansion of a globally connected digital society. As computing has become more sophisticated, so too have the abilities to access systems and sensitive information. Digital forensics professionals investigate and craft appropriate responses to disruptions to governments, organizations, and individuals. Whereas cybersecurity takes a proactive approach to information assurance to minimize harm, digital forensics takes a reactive approach to incident response.

(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.

(d) 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 and accompanying job 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 and discuss 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 and discuss historic cases or events regarding digital forensics or cybersecurity;

(D) analyze ethical and legal behavior when presented with confidential or sensitive information in various scenarios related to cybersecurity activities;

(E) analyze case studies of computer incidents;

(F) use the findings of a computer incident investigation to reconstruct a computer 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) discuss how to maintain data integrity such as by enabling encryption;

(D) examine and describe metadata of a file; and

(E) examine and describe 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 such as Security Information and Event Management (SIEM) reports;

(E) describe digital forensics tools;

(F) select the proper software tool based on appropriateness, effectiveness, and efficiency for a given digital forensics scenario;

(G) describe components of applications such as configurations settings, data, supporting files, and user interface; and

(H) describe how the "as a service" model applies to incident response.

(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).

(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;

(B) identify points of weakness and attack vectors such as online spoofing, phishing, and social engineering; and

(C) differentiate between simple versus multistage attacks.

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

(a) Implementation. The provisions of this section shall be implemented by school districts beginning with the 2023-2024 school year.

(1) No later than August 1, 2023, the commissioner of education shall determine whether instructional materials funding has been made available to Texas public schools for materials that cover the essential knowledge and skills identified in this section.

(2) If the commissioner makes the determination that instructional materials funding has been made available this section shall be implemented beginning with the 2023-2024 school year and apply to the 2023-2024 and subsequent school years.

(3) If the commissioner does not make the determination that instructional materials funding has been made available under this subsection, the commissioner shall determine no later than August 1 of each subsequent school year whether instructional materials funding has been made available. If the commissioner determines that instructional materials funding has been made available, the commissioner shall notify the State Board of Education and school districts that this section shall be implemented for the following school year.

(b) General requirements. This course is recommended for students in Grades 11 and 12. Prerequisite: Foundations of Cybersecurity. Students shall be awarded one credit for successful completion of this course.

(c) Introduction.

(1) Career and technical education instruction provides content aligned with challenging academic standards, industry relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and 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 such as laboratory and testing services, and research and development services.

(3) Cybersecurity is a critical discipline concerned with safeguarding computers, networks, programs, and data from unauthorized access. As a field, it has gained prominence with the expansion of a globally connected society. As computing has become more sophisticated, so too have the abilities of adversaries looking to penetrate networks and access sensitive information. Cybersecurity professionals prevent, detect, and respond to minimize disruptions to governments, organizations, and individuals.

(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.

(d) 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) communicate 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) demonstrate 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 incidents or events regarding cybersecurity; and

(C) evaluate 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), Gramm-Leach-Bliley Act (GLBA), and Cybersecurity Maturity Model Certification (CMMC).

(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) differentiate between ethical and unethical behavior when presented with various scenarios related to cybersecurity activities.

(5) Cybersecurity skills. The student simulates the process of penetration testing. The student is expected to:

(A) illustrate the phases of penetration testing, including plan, discover, attack, and report;

(B) design a plan to gain authorization for penetration testing;

(C) evaluate commonly used vulnerability scanning tools such as port scanning, packet sniffing, and password crackers;

(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) interpret the purpose of hashing algorithms, including blockchain;

(C) demonstrate password salting;

(D) explain and create a digital signature; and

(E) illustrate steganography.

(7) Cybersecurity skills. The student understands the concept of system 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), intrusion detection prevention systems (IDPS), and security information and event management (SIEM) systems;

(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 and discuss the role of software-managed networks, including virtualization and cloud architecture;

(C) evaluate the role of honeypots and honeynets in networks; and

(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;

(B) explain proper data acquisition;

(C) examine evidence from devices for suspicious activities; and

(D) critique current cybercrime cases involving digital forensics.

(10) Cybersecurity skills. The student explores expanding and emerging technology. The student is expected to:

(A) describe the concept of Security as a Service and the role of managed security service providers (MSSP);

(B) describe the integration of artificial intelligence and machine learning in cybersecurity;

(C) investigate impacts made by predictive analytics on cybersecurity; and

(D) research and investigate other emerging trends such as augmented reality and quantum computing.

(11) Cybersecurity skills. The student uses various operating system environments. The student is expected to:

(A) select and execute appropriate commands via the command line interface (CLI) such as ls, cd, pwd, cp, mv, chmod, ps, sudo, and passwd;

(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 understands risk and how risk assessment and risk management defend against attacks. The student is expected to:

(A) differentiate types of attacks, including operating systems, software, hardware, network, physical, social engineering, and cryptographic;

(B) explain blended threats such as combinations of software, hardware, network, physical, social engineering, and cryptographic;

(C) discuss types of risk, including business, operational, security, and financial;

(D) discuss risk response techniques, including accept, transfer, avoid, and mitigate;

(E) develop a plan of preventative measures based on discovered vulnerabilities and the likelihood of a cyberattack;

(F) identify and discuss common vulnerability disclosure websites;

(G) describe common web vulnerabilities such as cross-site scripting, buffer overflow, injection, spoofing, and denial of service;

(H) describe common data destruction and media sanitation practices such as wiping, shredding, and degaussing; and

(I) develop an incident response plan for a given scenario or attack.

(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);

(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 and appraise a disaster recovery plan (DRP) that includes backups, redundancies, system dependencies, and alternate sites.

(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.