Regional Occupational Program

Cybersecurity 3: Security+ A-G 2026-2027

COURSE DESCRIPTION

This course prepares students to develop foundational and intermediate cybersecurity knowledge and skills aligned to current Security+ certification content. Students study security principles, threats, vulnerabilities, secure network and system practices, application and host security, identity and access management, cryptography, certificates, compliance, operational security, risk management, incident response, business continuity, and disaster recovery.

Through hands-on labs and project-based assignments, students analyze security scenarios, identify threats and vulnerabilities, apply security controls, document findings, evaluate risk, respond to simulated incidents, and develop recommendations to protect systems, data, users, and organizations. Students who achieve competency in this course will build skills aligned to CompTIA Security+ and will be prepared to continue in the cybersecurity and information technology course sequence.

Course Information:

Course Length:	1 Year
Prerequisite:	Cybersecurity 2: Network+
Course Level:	Capstone
UC:	Yes G - Elective
Articulated:	No
Industry Cert.:	CompTIA Security+
Industry Sector:	Information and Communication Technologies
Pathway:	Information and Support Services
CALPADS:	8112

O*Net SOC Codes:

15-1212	Information Security Analysts
15-1231	Computer Network Support Specialists
13-1199.07	Security Management Specialists

Legend:

CTE - PS	CTE Pathway Standards
CRP	Career Ready Practices
CTE - AS	CTE Anchor Standards
CCSS	Common Core State Standards
ISTE	International Society for Technology in Education

Includes updates from 25/26 ICT Advisory

Advisory Minutes

Cybersecurity 3: Security+

Course Orientation

a. Discuss objectives for this course, including competencies, teacher expectations, classroom policies, and procedures.
b. Identify and discuss the acquisition of transferable skills (communication, collaboration, creativity, and critical thinking) and their importance to being college and career ready and for future personal and professional success.
c. Review objectives, competencies, and course syllabus.
d. Discuss student and teacher expectations, including behavior, class rules, appropriate dress, pre-course knowledge, and grading policies, including enrollment and attendance requirements and procedures, and classroom/school safety and disaster procedures.
e. Discuss next steps in course sequence related to the career pathway, the need for reinforcement of basic skills, transferrable skills, and postsecondary and career options.
f. Discuss the Big Six: Career Ready Essentials and the Standards for Career Ready Practice as they relate to this course, all aspects of the industry sector, and being college and career ready.

Big Six: Career Ready Essentials

1. Effective Communication	CTE – PS	CRP	CTE - AS	CCSS	ISTE
a. Demonstrate effective verbal communication and conflict resolution skills. **b. Use the writing process to develop written communication with the appropriate tone, organization, and format for the identified audience.** c. Explain the effect of interpersonal skills on one's ability to communicate effectively and develop relationships. d. Describe the impact of ineffective communication on business relationships. e. Analyze the impact of vocabulary, body language, and tone on verbal communication. f. Demonstrate active listening skills. g. Accurately interpret industry-specific written communication. h. Model responsible and effective use of various communication technologies. i. Identify valid and reliable digital reference and resource materials. j. Gather information from multiple digital sources to compare and contrast, synthesize, and summarize. k. Identify and use appropriate communication and collaboration technologies. l. Utilize technology to problem solve, accomplish tasks, and to produce or publish products.		1 2 11	2 3 4 5 7 8 9 10 11	**LS** 9-10 11-12.6 **SLS** 11-12.2 9-10 11-12.1 11-12.1d **WS** 11-12.7 11-12.6	1b,c 2c 3b,c 5c 6b,c,d

2. Collaboration, Creativity, and Critical Thinking	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. Demonstrate critical thinking skills for a variety of purposes and in different settings. **b. Collaborate to reach consensus on an identical objective through the sharing of knowledge, tasks, and learning.** c. Discuss the importance of the critical thinking process to real-world applications.		2 4 5 7 9	2 3 4 5 7	**LS** 9-10 11- 12.6 **SLS**	1c 3c,d 4a-d 5c,d 6c

d. Evaluate the impact of creative thinking on problem solving and innovation in real-world applications. e. Compile work that demonstrates the process used to (elaborate, refine, analyze) evaluate original ideas and maximize creative efforts. f. Apply divergent and convergent thinking to the development of an original idea or solution. g. Examine real-world limits to adopting ideas. h. Demonstrate creative thinking (preparation, insight, evaluation, elaboration, and communication) to create a new idea or concept. i. Assume shared responsibility for collaborative work, and value the individual contributions made by each team member. j. Evaluate evidence, arguments, claims, and beliefs to identify connections. k. Identify bias, prejudice, propaganda, self-deception, distortion, and misinformation. l. Produce intellectual, informational, or material products that serve an authentic purpose. m. Work effectively and respectfully with those from diverse backgrounds or cultures. n. Demonstrate respect, trust, commitment, and the ability to compromise in collaborative projects.		10 11	8 9 11	9-10 11-12.1 11-12.1d 11-12.2 **WS** 11-12.7 11-12.6	7b,c,d
3. Leaders and Teams: Roles and Responsibilities	**CTE – PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Determine the individual and team members' roles and responsibilities. **b. Demonstrate leadership skills and qualities (i.e., reliability, negotiation skills, initiative, positive reinforcement, recognition of others' efforts, problem-solving skills, conflict resolution, and delegation).** c. Explain the importance of technical, social, and communication skills to team success. d. Compare and contrast leadership styles and their effectiveness in various situations. e. Organize and delegate responsibilities in a team setting to encourage ideas, perspectives, and contributions from all team members. f. Develop a strong sense of team identity by brainstorming solutions, volunteering, assisting others, practicing respect and courtesy, and taking initiative. g. Examine situations in which a follower becomes the leader. h. Describe twenty-first-century skills required across all occupations. i. Identify and discuss the characteristics of a successful team (i.e., leadership, cooperation, and effective decision-making). j. Leverage social and cultural differences to increase innovation and quality of work.		7 8 9	3 7 8 9 11	**SLS** 11-12.2 9-10 11-12.1 11-12.1d **WS** 11-12.6	7a,c
4. Legal, Ethical, and Environmental Considerations	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Demonstrate industry specific ethical and legal practices. **b. Identify eco-friendly industry specific practices and resources.** c. Identify local, state, and federal regulatory agencies, entities, laws, and regulations.		5 7 8	3 5 7	**WS** 11-12.6 11-12.7	2a,b 3a,b 5c

d. Identify discrimination based on race, nationality, religion, gender, age, disability, or sexual orientation. e. Summarize the ethical and legal implications of workplace discrimination and harassment. f. Explain the concept of corporate citizenship. g. Examine an employer's role in protecting the health and welfare of employees, the community, and the environment. h. Analyze current environmental laws and regulations and their impact on industry. i. Compare and contrast both society's and industry's impact on the environment.		12	8 9 11	**SLS** 9-10 11-12.1 11-12.1d 11-12.2	6c
5. Personal Growth and Career Planning	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Demonstrate continued personal development and growth. **b. Develop and manage a personal growth and career plan.** c. Explain the relationship between sound financial habits and financial security. d. Create and manage a personal financial plan. e. Demonstrate initiative in achieving personal and professional goals. f. Apply time management strategies to meet deadlines. g. Demonstrate a growth mindset through flexibility and a positive attitude. h. Select and demonstrate appropriate job-search and retention techniques. i. Demonstrate strategies to prepare for employment. j. Demonstrate interpersonal skills appropriate for the workplace. k. Elaborate on the importance of perseverance to personal and professional success. l. Discover personal career interests, aptitudes, and skills.		1 2 3 4 6	2 3 4 7 8 11	**LS** 9-10 11-12.6 **SLS** 9-10 11-12.1 11-12.1d 11-12.2 **WS** 11-12.6	1a 3a,c 4d 6a,d 7b
6. Workplace Safety and Personal Wellness	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Demonstrate proper industry specific safe work practices to prevent injury or illness. **b. Assess the potential impact of goal setting on personal and professional success.** c. Describe the role of security and emergency procedures in workplace safety. d. Describe the effect of preventative measures on emergencies in the workplace. e. Identify and describe the causes, prevention, and treatment of common accidents. f. Identify local, state, and federal agencies that regulate workplace safety. g. Explain the role of the California Occupational Safety and Health Administration (Cal-OSHA) and the Environmental Protection Agency (EPA). h. Discuss the basics of system operations. i. Demonstrate the proper use of personal protective equipment (PPE). j. Explain the purpose of and accurately interpret a Safety Data Sheet (SDS). k. Identify hazardous materials and chemicals. l. Demonstrate proper procedures to respond to work-related accidents and injuries. m. Describe how ergonomics, housekeeping, and maintenance are related to accidents and injuries.		2 5 6 8 12	2 5 6 7 8 10 11	**LS** 9-10 11-12.6 **WS** 11-12.7 11-12.6 **SLS** 9-10 11-12.1 11-12.1d	1a,d 2a,d 5b

n. Demonstrate cyber ethics, cyber safety, and cybersecurity. o. Assess the potential impact of preventative physical and mental health measures on workplace safety.					
Cybersecurity 3: Security+ Units of Instruction					
7. Security Fundamentals	**CTE-PS**	**CRP**	**CTE- AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to identify basic cybersecurity concepts and principles used to secure systems, networks, data, and users.** b. Identify the basic components of the information security cycle. c. Demonstrate the ability to identify and explain steganography concepts and detection methods using teacher-approved tools or examples. d. Demonstrate understanding of password attacks, credential exposure, and secure authentication practices using teacher-approved simulations or controlled lab activities. e. Identify the fundamental components of cryptography. f. Identify fundamental security policy concepts, including acceptable use, access control, password management, data protection, privacy, and incident reporting.	A5.1 A5.3	1 2 4 5	1 2 4 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
8. Identifying Security Threats and Vulnerabilities	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate an understanding of common threats, vulnerabilities, and attack vectors used to assess and protect systems, networks, applications, and data.** b. Identify social engineering attacks. c. Identify various malware threats. d. Identify application and software-based threats. e. Identify network-based threats. f. Identify wireless threats and vulnerabilities. g. Identify physical threats and vulnerabilities.	A5.2	1 2 4 5	1 2 4 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
9. Managing Data, Application, Device, and Host Security	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to apply security practices to protect end-user devices, software, applications, and data.** b. Demonstrate the ability to manage data security. c. Demonstrate the ability to manage application security. d. Demonstrate the ability to manage device and host security. e. Demonstrate the ability to manage mobile-device security using appropriate configuration, access, update, and data-protection practices.	A2.0 A2.2 A2.3 A2.4 A5.0 A5.3 A5.4	1 2 4 5	1 2 4 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
10. Implementing Network Security Practices	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**

a. **Demonstrate the ability to apply security practices to protect internal and external network components.** b. Demonstrate the ability to configure security parameters on network devices and technologies. c. Identify network design elements and components that support secure network architecture. d. Identify and apply secure network protocols and services where appropriate. e. Apply secure network administration principles, including least privilege, secure configuration, monitoring, documentation, and change control. f. Apply basic practices to secure wireless network traffic and access.	A3.0 A3.6 A5.0 A8.2	1 2 4 5	1 2 4 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
11. Implementing Identity, Access Control, Authentication, and Account Management	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to protect user identities and control access to organizational systems, applications, data, and network resources.** b. Implement or explain access-control methods and common authentication services using appropriate security practices. c. Implement or explain account-management security controls, including user provisioning, permissions, password practices, multi-factor authentication where appropriate, account review, and account removal.	A5.0 A5.3 A5.4	1 2 4 5	1 2 4 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
12. Managing Certificates and Public Key Infrastructure	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate how digital certificates and public key infrastructure support secure communications between users, devices, services, and clients on a network.** b. Explain or demonstrate the purpose and structure of a certificate authority (CA) hierarchy. c. Explain or demonstrate certificate enrollment for users, devices, services, or other network entities. d. Explain or demonstrate how certificates are used to secure network traffic and verify trust. e. Explain or demonstrate certificate renewal and lifecycle management. f. Explain or demonstrate secure backup, storage, and recovery practices for certificates and private keys. g. Explain or demonstrate certificate revocation and the role of revocation processes in maintaining trust.	A4.0 A4.1 A4.2 A4.3	1 2 4 5	1 2 4 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
13. Implementing Compliance, Operational Security, and Cyber Hygiene	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to explain security awareness, training, compliance, and operational security practices used to protect an organization and its resources.** b. Describe physical security issues and principles.	A5.1 A7.0 A7.1	1 2 4	1 2 4	**LS** 9-10 11-12.6	

c. Explain legal and compliance issues and principles related to cybersecurity, privacy, data protection, and organizational security. d. Describe concepts of cybersecurity related to legal and ethical decisions. e. Identify security awareness and training requirements. f. Describe the importance of cyber hygiene best practices. g. Explain security considerations for integrating systems, data, services, or access with third parties.	A7.2	5 9	9 10 11	**WS** 11-12.6 11-12.7 **SLS** 11-12.1b	
14. Risk Management	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to analyze risk, assess vulnerabilities, and recommend appropriate mitigation strategies.** b. Explain or demonstrate vulnerability assessment tools, techniques, and responsible use practices in a controlled or simulated environment. c. Identify mitigation, deterrent, and risk-reduction techniques used to reduce the likelihood or impact of security threats.	A1.2 A5.3	1 2 4 5	1 2 4 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
15. Responding to and Managing Security Incidents	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to identify, document, and manage key steps in responding to a security incident.** b. Demonstrate the ability to respond to a simulated security incident using appropriate containment, communication, escalation, and documentation practices. c. Demonstrate the ability to explain or apply recovery steps after a security incident, including restoration, verification, documentation, and recommendations to reduce future risk.	A6.0 A6.2 A6.3 A6.5	1 2 4 5	1 2 4 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
16. Business Continuity and Disaster Recovery	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to develop or evaluate basic business continuity and disaster recovery plans to reduce the impact of disruptions on an organization.** b. Describe business continuity concepts, including maintaining essential operations during and after a disruption. c. Plan for disaster recovery, including backup strategies, restoration priorities, recovery procedures, communication needs, and documentation. d. Explain or demonstrate disaster recovery procedures in a simulated or controlled environment.	A1.1 A4.1 A4.4	1 2 4 5	1 2 4 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	

A-G Approved Key Assignments

1.	**It's a Crime:** Student groups (3-4 students) work collaboratively to research and locate examples of cybercrimes or computer-related crimes learned about in this unit. Students should identify the type of crime, the intended goal of the attacker or actor, any legal outcomes from the crime, if any, and lessons learned, best practices, or tools that may help mitigate this type of activity in the future. Using a rubric and checklist, students prepare and present their findings to the class. *Unit(s) 7*
2.	**Read All About It!** Based on teacher-prepared prompts and a rubric, students research and write an essay (2-3 pages) on one of the following cybersecurity topics: recent trends, ethical issues, or approaches to computer and information security. *Unit(s) 7*
3.	**Build it:** Student groups (3-4 students) work collaboratively to create or configure a teacher-approved application, script, or lab activity capable of sending and receiving messages or files in a controlled network environment. Each group will prepare and demonstrate their work to the class and explain appropriate security considerations. *Unit(s) 8*
4.	**Cyber Attack**: Each student will research a significant cyberattack and, using a template and graphic organizer, create a flowchart that identifies the chronological steps of the attack, any countermeasures, and how the attacker or actor achieved the goal. *Unit(s) 8*
5.	**Hands On:** Students will demonstrate their mastery of the content by successfully completing teacher-approved network discovery and monitoring activities in a controlled lab environment. Students will use programming, scripting, network-discovery, or monitoring tools to identify and visually document active or inactive devices on a lab network. Students will also review TCP and UDP port information, connection status, logs, or other observable indicators to identify suspicious network activity and document findings such as IP address, MAC address when available, hostname, ports, protocols, and connection status. *Unit(s) 8*
6.	**PowerShell or Automation Script:** Students work in small groups (3-4 students) to create or modify a teacher-approved script or automation task to support system protection, backup, restore-point creation, or routine recovery preparation in a controlled lab environment. *Unit(s) 9*
7.	**Computer Restore:** Students use teacher-approved imaging, deployment, backup, or recovery tools to prepare a computer or lab system for restoration. Each student will restore a system or simulated system environment to an approved baseline state. Students capture the steps in their journal and write a short reflection on the process. *Unit(s) 9*
8.	**Encryption and Decryption Tool:** Students will use a teacher-approved programming, scripting, or cybersecurity lab tool to explore basic encryption and decryption concepts, including how keys or keyword-based mapping can be used to encode and decode messages in a controlled instructional activity. *Unit(s) 10*
9.	**System Imaging and Restore:** Students use teacher-approved imaging, deployment, backup, or recovery tools to prepare a computer or lab system for restoration. Each student will restore a system or simulated system environment to an approved baseline state. *Unit(s) 10, 12*
10.	**There Ought to Be a Law:** Student groups (3-4 students) will work collaboratively to research, design, and present their findings on important legislative or judicial outcomes that directly impact cybersecurity, privacy, data protection, digital evidence, or technology use. Each group will thoroughly research their topic, identify the pros and cons associated with the law or ruling, determine how it is being interpreted in the workplace today, and explain its impact on real or perceived benefits or limitations related to human rights and personal freedom. Each group will present their findings to the class and be assessed through the use of a presentation rubric. Each student will write a short 1-2-page reflection on what they learned through the research and collaborative process. *Unit(s) 10*
11.	**Stop Looking at Me!** Students will explore privacy issues related to modern technologies, such as cameras, virtual assistants, recording devices, social media, mobile devices, internet-connected tools, artificial intelligence, and cyberbullying. Small groups will identify examples of cybercrimes or technology-related harm, such as social-network misuse, sexting, identity theft, digital manipulation, misinformation, and privacy violations. Students will examine how technology affects evidence collection, digital evidence, credibility, and what may be considered reliable or truthful in criminal or civil cases. *Unit(s) 10*

12.	Risk Gallery Walk: Student pairs work collaboratively to research a teacher-assigned type of risk, such as security and privacy, information technology operations, business-system controls, information-system testing, reliability and performance management, technology asset management, project risk management, third-party risk, or change management. Students identify risk mitigation strategies that might be used to reduce the effect of threats and hazards and locate a real-world example. Students prepare a poster or digital display that outlines and describes their risk topic. The class participates in a gallery walk of the completed displays. *Unit(s) 11*
13.	Cybersecurity Risk Assessment: Students in small groups (3-4 students) complete a qualitative threat and risk assessment for a fictitious organization or company using teacher-provided organizational information. Student groups evaluate risks such as malware, unauthorized access, insider threats, weak incident-response procedures, third-party data exposure, competitor or external threats, and inadvertent release of information. Groups create a risk matrix or table identifying likelihood, impact, and recommended mitigation strategies, then prepare and present their findings. *Unit(s) 11*
14.	Automation Script: Students will create or modify a teacher-approved script or automation task to support system protection, restore-point creation, backup preparation, or routine recovery procedures in a controlled lab environment. *Unit(s) 9, 12, 13*
15.	Audit Log Analysis: In a controlled cybersecurity lab or simulation, students will analyze a teacher-approved mock security incident. Defensive teams will configure or explain common system defenses, while opposing teams will use approved simulated attack steps or scenario data provided by the teacher. Each team will produce or review audit logs and document observed events, potential vulnerabilities, defensive actions, and recommendations for improvement. *Unit(s) 12, 13*
16.	Write a Wrong: Students are given a cybersecurity incident scenario and are asked to prepare a written report for an organization's leadership that outlines the major incident-response points that need to be addressed and provides examples of each component. Students use clear, nontechnical language appropriate for a nontechnical audience and avoid unnecessary jargon. The report is limited to a maximum of two pages. Students utilize a writing rubric. *Unit(s) 12, 13*
17.	File System Analysis: Students demonstrate basic file-system analysis and recovery concepts using teacher-approved forensic, file-system, or recovery tools in a controlled lab environment. Students examine how file systems organize data and document the steps used to identify, analyze, or recover file-system information. *Unit(s) 14, 15, 16*
18.	Storage Capacity: Students work in teams to analyze storage capacity concepts using current storage terminology, such as partitions, volumes, sectors, file systems, storage media, and usable capacity. Students may compare legacy CHS concepts with current storage-addressing and capacity methods where appropriate. *Unit(s) 14, 15, 16*
19.	Secure Data Sanitization: Students use teacher-approved tools or simulations to explain or demonstrate secure data sanitization concepts for storage media in a controlled lab environment. Students document the purpose, method, verification steps, and safety or data-handling considerations related to securely erasing or sanitizing data. *Unit(s) 14, 15, 16*
20.	System Imaging and Deployment: Students use teacher-approved imaging, deployment, or configuration tools to prepare and deploy an operating-system image or baseline system configuration in a controlled lab environment. *Unit(s) 14, 15, 16*
21.	Network Backup and Deployment: Students use teacher-approved backup, imaging, or deployment tools to back up, restore, or deploy an operating system or system image over a network in a controlled lab environment. *Unit(s) 14, 15, 16*
22.	Technology and Information Systems Proposal: Students work in small teams (3-4 students) to determine needs, identify areas of risk, and develop or evaluate a basic business continuity and disaster recovery proposal based on a teacher-approved school, district, or organizational technology scenario. Students will prepare a proposal describing their recommendations, including backup retention, secure storage, privacy, data protection, recovery priorities, communication needs, and protection of confidential information. Teams present their proposals to the class and may receive feedback from technology staff or other appropriate reviewers when available. *Unit(s) 14, 15, 16*

Standards Alignment

The curricula have been aligned with the CTE Model Curriculum Standards released in 2013. Each industry sector was updated to meet the increased rigor and relevancy requirements of the Common Core State Standards. The curriculum also includes the new Standards for Career Ready Practices.

Standards for Career Ready Practice

1. *Apply appropriate technical skills and academic knowledge.*
2. *Communicate clearly, effectively, and with reason.*
3. *Develop an education and career plan aligned with personal goals.*
4. *Apply technology to enhance productivity.*
5. *Utilize critical thinking to make sense of problems and persevere in solving them.*
6. *Practice personal health and understand financial literacy.*
7. *Act as a responsible citizen in the workplace and the community.*
8. *Model integrity, ethical leadership, and effective management.*
9. *Work productively in teams while integrating cultural and global competence.*
10. *Demonstrate creativity and innovation.*
11. *Employ valid and reliable research strategies.*
12. *Understand the environmental, social, and economic impacts of decisions.*

CTE Anchor Standards—Common Core English Language Arts Alignment

Anchor Standard 1: Academics

Analyze and apply appropriate academic standards required for successful industry sector pathway completion leading to postsecondary education and employment. Refer to the industry sector alignment matrix for identification of standards. Note: alignment listed within each sector.

Anchor Standard 2: Communications

Language Standard: Acquire and accurately use general academic and domain-specific words and phrases sufficient for reading, writing, speaking, and listening at the (career and college) readiness level; demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression. LS 9-10, 11-12.6

Anchor Standard 3: Career Planning and Management

Speaking and Listening Standard: Integrate multiple sources of information presented in diverse formats and media (e.g., visually, quantitatively, orally) in order to make informed decisions and solve problems, evaluating the credibility and accuracy of each source and noting any discrepancies among the data. SLS 11-12.2

Anchor Standard 4: Technology

Writing Standard: Use technology, including the Internet, to produce, publish, and update individual or shared writing products in response to ongoing feedback, including new arguments and information.

Anchor Standard 5: Problem Solving and Critical Thinking

Writing Standard: Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem, narrow or broaden the inquiry when appropriate, and synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation. WS 11-12.7

Anchor Standard 6: Health and Safety

Reading Standards for Science and Technical Subjects: Determine the meaning of symbols, keywords, and other domain-specific words and phrases as they are used in a specific scientific or technical context. RSTS 9-10, 11-12.4

Anchor Standard 7: Responsibility and Flexibility

Speaking and Listening Standard: Initiate and participate effectively in a range of collaborative discussions (one-on-one, in groups, and teacher-led) with diverse partners, building on others' ideas and expressing their own clearly and persuasively. SLS 9-10, 11-12.1

Anchor Standard 8: Ethics and Legal Responsibilities

Speaking and Listening Standard: Respond thoughtfully to diverse perspectives; synthesize comments, claims, and evidence made on all sides of an issue; resolve contradictions when possible; and determine what additional information or research is required to deepen the investigation or complete the work. SLS 11-2.1d

Anchor Standard 9: Leadership and Teamwork

Speaking and Listening Standard: Work with peers to promote civil, democratic discussions and decision making; set clear goals and deadlines; and establish individual roles as needed. SLS 11-12.1b

Anchor Standard 10: Technical Knowledge and Skills

Writing Standard: Use technology, including the Internet, to produce, publish, and update individual or shared writing products in response to ongoing feedback, including new arguments or information. WS 11-12.6

Anchor Standard 11: Demonstration and Application

Demonstrate and apply the knowledge and skills contained in the industry-sector anchor standards, pathway standards, and performance indicators in the classroom, laboratory, and workplace settings, and the career technical student organization. Note: no alignment evident for this standard. WS 11-12.6

CTE Model Curriculum Standards—Industry Sectors and Pathways

Information and Communication Technologies

A. Information Support and Services Pathway

A1.1 Describe how technology is integrated into business processes.

A1.2 Identify common organizational, technical, and financial risks associated with the implementation and use of information and communication systems.

A2.0 Acquire, install, and implement software and systems.

A2.2 Investigate, evaluate, select, and use major types of software, services, and vendors.

A2.3 Install software and setup hardware.

A2.4 Define and use appropriate naming conventions and file management strategies.

A3.0 Access and transmit information in a networked environment.

A3.6 Describe and contrast the differences between various Internet protocols: hypertext transfer protocol (http), hypertext transfer protocol secure (https), file transfer protocol (ftp), simple mail transfer protocol (smtp).

A4.0 Administer and maintain software and systems.

A4.1 Use different systems and associated utilities to perform such functions as file management, backup and recovery, and execution of programs.

A4.2 Use a command line interface.

A4.3 Automate common tasks using macros or scripting.

A4.4 Evaluate the systems-development life cycle and develop appropriate plans to maintain a given system after assessing its impact on resources and total cost of ownership (TCO).

A5.0 Identify requirements for maintaining secure network systems.

A5.1 Follow laws, regulatory guidelines, policies, and procedures to ensure the security and integrity of information systems.

A5.2 Identify potential attack vectors and security threats.

A5.3 Take preventative measures to reduce security risks (e.g., strong passwords, avoid social engineering ploys, limit account permissions).

A5.4 Use security software and hardware to protect systems from attack and alert of potential threats, anti-malware software, and firewalls.

A6.0 Diagnose and solve software, hardware, networking, and security problems.

A6.1 Use available resources to identify and resolve problems using knowledge bases, forums, and manuals.

A6.2 Use a logical and structured approach to isolate and identify the source of problems and to resolve problems.

A6.3 Use specific problem-solving strategies appropriate to troubleshooting, eliminating possibilities, or guess and check.

A6.5 Evaluate solution methods recognizing the trade-offs of troubleshooting vs. reloading, reimaging, or restoring to factory defaults using a sandbox environment.

A7.0 Support and train users on various software, hardware, and network systems.

A7.1 Recognize the scope of duties ICT support staff have and tiered levels of support.

A7.2 Describe and apply the principles of a customer-oriented service approach to supporting users.

A8.2 Acquire, use, and manage necessary internal and external resources when supporting various organizational systems.

ISTE Standards for Students

1. Empowered Learner- Students leverage technology to take an active role in choosing, achieving, and demonstrating competency in their learning goals, informed by the learning sciences.

a) Students articulate and set personal learning goals, develop strategies leveraging technology to achieve them, and reflect on the learning process itself to improve learning outcomes.

b) Students build networks and customize their learning environments in ways that support the learning process.

c) Students use technology to seek feedback that informs and improves their practice and to demonstrate their learning in a variety of ways

d) Students understand the fundamental concepts of technology operations, demonstrate the ability to choose, use and troubleshoot current technologies and are able to transfer their knowledge to explore emerging technologies.

2. Digital Citizen- Students recognize the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world, and they act and model in ways that are safe, legal, and ethical.

a) Students cultivate and manage their digital identity and reputation and are aware of the permanence of their actions in the digital world.

b) Students engage in positive, safe, legal, and ethical behavior when using technology, including social interactions online or when using networked devices.

c) Students demonstrate an understanding of and respect for the rights and obligations of using and sharing intellectual property.

d) Students manage their personal data to maintain digital privacy and security and are aware of data-collection technology used to track their navigation online.

3.Knowledge Constructor- Students critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts, and make meaningful learning experiences for themselves and others.

a) Students plan and employ effective research strategies to locate information and other resources for their intellectual or creative pursuits.

b) Students evaluate the accuracy, perspective, credibility, and relevance of information, media, data, or other resources.

c) Students curate information from digital resources using a variety of tools and methods to create collections of artifacts that demonstrate meaningful connections or conclusions.

d) Students build knowledge by actively exploring real-world issues and problems, developing ideas and theories, and pursuing answers and solutions.

4. Innovative Designer- Students use a variety of technologies within a design process to identify and solve problems creating new, useful, or imaginative solutions.

a) Students know and use a deliberate design process for generating ideas, testing theories, creating innovative artifacts, or solving authentic problems.

b) Students select and use digital tools to plan and manage a design process that considers design constraints and calculated risks.

c) Students develop, test, and refine prototypes as part of a cyclical design process.

d) Students exhibit a tolerance for ambiguity, perseverance, and the capacity to work with open-ended problems.

5. Computational Thinker- Students develop and employ strategies for understanding and solving problems in ways that leverage the power of technological methods to develop and test solutions.

a) Students formulate problem definitions suited for technology-assisted methods such as data analysis, abstract models, and algorithmic thinking in exploring and finding solutions.

b) Students collect data or identify relevant data sets, use digital tools to analyze them, and represent data in various ways to facilitate problem-solving and decision-making.

c) Students break problems into component parts, extract key information, and develop descriptive models to understand complex systems or facilitate problem-solving.

d) Students understand how automation works and use algorithmic thinking to develop a sequence of steps to create and test automated solutions.

6. Creative Communicator- Students communicate clearly and express themselves creatively for a variety of purposes using platforms, tools, styles, formats, and digital media appropriate for their goals.

a) Students choose the appropriate platforms and tools for meeting the desired objectives of their creation or communication.

b) Students create original works or responsibly repurpose or remix digital resources into new creations.

c) Students communicate complex ideas clearly and effectively by creating or using a variety of digital objects such as visualizations, models, or simulations.

d) Students publish or present content that customizes the message and medium for their intended audiences.

7. Global Collaborator- Students use digital tools to broaden their perspectives and enrich their learning by collaborating with others and working effectively in teams locally and globally.

a) Students use digital tools to connect with learners from a variety of backgrounds and cultures, engaging with them in ways that broaden mutual understanding and learning.

b) Students use collaborative technologies to work with others, including peers, experts, or community members, to examine issues and problems from multiple viewpoints.

c) Students contribute constructively to project teams, assuming various roles and responsibilities to work effectively toward a common goal.

d) Students explore local and global issues and use collaborative technologies to work with others to investigate solutions.