Regional Occupational Program

Cybersecurity 3: Security+ A-G 2025-2026

COURSE DESCRIPTION

The Cybersecurity 3 course prepares students for post-secondary success in the cybersecurity field. In this course students engage with studies of the history and implications of network communications; the network protocols which make the internet possible; how networks provide access to services and communicate with one another, methods used to increase scalability, reliability, and security in the modern network, and the Internet of Things (IOT). Students targeting a cybersecurity career aligned with the Department of Defense (DoD) or Government related service can take this course to prepare for the CompTIA Security + certification, to meet DoD 8140 cyber security workforce requirements.

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 & Communication Technologies
Pathway:	Information 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 24/25 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	2 3 4 5	**LS** 9-10 11- 12.6	1c 3c,d 4a-d 5c,d

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.		9 10 11	7 8 9 11	**SLS** 9-10 11-12.1 11-12.1d 11-12.2 **WS** 11-12.7 11-12.6	6c 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 ideas and principles of securing computers.** b. Identify the basic components of the information security cycle. c. Demonstrate the ability to detect steganography. d. Demonstrate the ability to conduct password sniffing. e. Identify the fundamental components of cryptography. f. Identify fundamental security policy issues.	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 the ability to understand the types of possible threats and potential vulnerabilities to adequately protect systems.** b. Identify social engineering attacks. c. Identify various malware threats. d. Identify 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, and Host Security	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to properly secure end user devices, software, and data used on these devices.** 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 security.	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	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to secure both internal and external components of a network.** b. Demonstrate the ability to configure security parameters on network devices and technologies. c. Identify Network Design Elements and Components. d. Implement Network Protocols. e. Apply Secure Network Administration Principles.	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	

f. Secure Wireless Traffic.				11-12.7	
11. Implementing Access Control, Authentication and Account Management	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to protect the identity of users and adequately control access to organizational systems.** b. Implement access control and common authentication services. c. Implement account management security controls.	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	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate how to secure communications between services and clients on a network through digital certificate management.** b. Install a Certificate Authority (CA) hierarchy. c. Enroll certificates for entities. d. Secure network traffic using certificates e. Renew certificates f. Backup and restore certificates and private keys. g. Revoke certificates.	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 and Operational Security	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Demonstrate the ability to provide training and awareness to implement the level of security control and compliance required to protect the organization and its resources.** b. Describe physical security issues and principles. c. Understand legal compliance issues and principles 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. Integrate systems and data with third parties.	A5.1 A7.0 A7.1 A7.2	1 2 4 5 9	1 2 4 9 10 11	**LS** 9-10 11-12.6 **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 implement mitigation strategies**. b. Implement vulnerability assessment tools and techniques. c. Identify mitigation and deterrent techniques.	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. Troubleshooting and Managing Security Incidents	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. **Demonstrate the ability to troubleshoot and manage all aspects of a security incident.** b. Demonstrate the ability to respond to a security incident. c. Demonstrate the ability to recover from a security incident.	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 a Business Continuity Plan and a Disaster Recovery Plan to mitigate the overall impact on an organization.** b. Describe Business Continuity. c. Plan for disaster recovery. d. Execute disaster recovery plans and procedures.	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 computer crimes learned about in this unit. Students should identify the type of crime, the intended goal of the attacker, any legal outcomes from the crime, if any, and lessons learned, best practices, or tools that may mitigate this type of activity in the future. Using a rubric and checklist, students prepare and present their findings to the entire 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) from one of the following topics: Recent trends, ethical issues, and approaches in Computer Security. *Unit(s) 7*
3.	Build it: Student Groups (3-4 students) work collaboratively to create an application capable of sending/receiving messages and files. Each group will prepare and demonstrate their application to the entire class. *Unit(s) 8*
4.	Cyber Attack: Each student will research a significant cyber-attack that changed the global computing world and using a template and graphic organizer, create a flowchart that identifies the chronological steps of the attack, any counter measures, and how the attacker achieved his/her goal. *Unit(s) 8*
5.	Hands On: Students will demonstrate their mastery of the content by successfully doing the following: • Students will use VB.Net to create a network scanner that graphically displays computers that are on/off. • Students will scan TCP and UDP ports for real time system intrusion and identify the intruder's MAC address (netstatm arp, NBTstat). *Unit(s) 8*
6.	Powershell: Students work in small groups (3-4 students) to create a PowerShell script (ps1 file) to automatically create a system restore. *Unit(s) 9*
7.	Computer Restore: Students use SysPrep utility to prepare their computer for image deployment. Each student will then load his/her drive image to restore the computer to its original state. Students capture the steps in their journal and write a short reflection on the process. *Unit(s) 9*
8.	VB Net: Students will use VB.Net to create a decryption tool that allows key word mapping to resolve encrypted messages. *Unit(s) 10*
9.	SysPrep Utility: Students use SysPrep utility to prepare their computer for image deployment. Each student will then reload his/her drive image to restore the computer to its original 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 of important legislative or judicial outcomes that directly impact cybersecurity. Each group will thoroughly research their topic, identify the established pros and cons brought about by the law or ruling, determine how it is being interpreted in the workplace today, and its impact on real or perceived benefit or curtailment of human rights and personal freedom. Each group will present their findings to the entire 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 the collaborative process. *Unit(s) 10*
11.	Stop Looking at Me! Students will explore issues of privacy brought about by access to 21st century tools i.e.; cameras, virtual assistants such as Alexa, recording devices, and even the Internet itself as a weapon of cyberbullying. Small groups identify cybercrimes (those that occur through the use of some sort of technology, i.e., social networks, sexting, identity theft, social and political implications of photo and video manipulation, etc.) In this assignment students take a look at the change in evidentiary laws (In today's world is there such a thing as Prima Facia Evidence in a court of law?) and the impact technology has played on the gathering of evidence for a criminal or civil case and what is considered 'truth' by the judicial system. *Unit(s) 10*

12.	**Risk Gallery Walk:** Student pairs work collaboratively to identify a teacher-assigned type of risk (security and privacy, information technology operations, business systems control and effectiveness, information systems testing, reliability and performance management, information technology asset management, project risk management, and change management) to research and ascertain 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 that outlines and describes their 'risk' topic. The posters are affixed to the classroom walls, and the whole class participates in a gallery walk of the posters. *Unit(s) 11*
13.	**Hack-a-Thon:** Students in small groups (3-4 students) complete a qualitative threat assessment of the computer security of a fictitious organization or company (company or organizational information is provided by the teacher to each group). Student groups are to evaluate the following information and create a table identifying the 3-by-5 level analysis (probability) with the following data: Virus attacks, internet hacks, disgruntled employee hacks, weak incidence response mechanisms, theft of information by a trusted third-party contractor, competitor hacks, inadvertent release of noncritical information. Student group prepare and present their findings. *Unit(s) 11*
14.	**ps1 File:** Students will create a PowerShell script (ps1 file) to automatically create a system restore point. *Unit(s) 9, 12, 13*
15.	**Audit Log Analysis**: In advance of a mock cyber-attack, defending students (blue Team) will configure common system defenses to repel the attack while the attacking students (Red Team) will launch a multi-stage attack while maintaining their own defense during the counterattack. Each student team will produce their own audit log of the attack for analysis and documentation of potential vulnerabilities. *Unit(s) 12, 13*
16.	**Write a Wrong:** Students are given a scenario and are asked to prepare a written report for the organization's CEO that outlines the major points of an incident response that needs to be addressed and provide examples of each component. Use laymen's nontechnical language; avoid all jargon. The report is limited to a maximum of two pages. Students utilize a writing rubric. *Unit(s) 12, 13*
17.	**File Allocation Tables:** Students demonstrate the Rebuilding File Allocation Tables by using boot sector readers and utilities such as FTK or NTFS readers, etc. *Unit(s) 14, 15, 16*
18.	**Storage Capacity:** Students work in teams to determine the geometry of hard drive disks using CHS calculations (cylinders, heads, sectors) to determine storage capacity. *Unit(s) 14, 15, 16*
19.	**Wipe Clean:** Students use Debug to clean wipe a hard drive by resulting all binary bits to 1 on Interrupt 13. *Unit(s) 14, 15, 16*
20.	**SysPrep:** Students use Sysprep to deploy an image of Microsoft OS for departmental use. *Unit(s) 14, 15, 16*
21.	**Acronis:** Students use Acronis to deploy and backup Microsoft OS over a network. *Unit(s) 14, 15, 16*
22.	**Technology and Information Systems Proposal:** Students work in small teams (3-4 students) to determine the needs, identify weak areas and develop a business continuity and recovery plan based on their school district's technology and information systems. Students will prepare a proposal describing their recommendations, making sure to include long-term storage of backups and safe storage of critical and confidential student personal information. Teams present their proposals to the whole class and are provided feedback by the school district's Director of Technology and staff. *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) Stu 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.