2026 Information Technology– Cybersecurity

Program CIP: 11.0101 — Computer and Information Sciences, General

Direct inquiries to:

Project Manager
Research and Curriculum Unit
Mississippi State University
P.O. Drawer DX
Mississippi State, MS 39762
662.325.2510
helpdesk@rcu.msstate.edu

Program Supervisor
Office of Career and Technical Education
and Workforce Development
Mississippi Department of Education
P.O. Box 771
Jackson, MS 39205
601.359.3974

Published by:

Office of Career and Technical Education
and Workforce Development
Mississippi Department of Education
Jackson, MS 39205

Research and Curriculum Unit
Mississippi State University
Mississippi State, MS 39762
helpdesk@rcu.msstate.edu

The Research and Curriculum Unit (RCU), located in Starkville, as part of Mississippi State University (MSU), was established to foster educational enhancements and innovations. In keeping with the land-grant mission of MSU, the RCU is dedicated to improving the quality of life for Mississippians. The RCU enhances the intellectual and professional development of Mississippi students and educators while applying knowledge and educational research to the lives of the people of the state. The RCU works within the contexts of curriculum development and revision, research, assessment, professional development, and industrial training.

Table of Contents

Acknowledgments

The Information Technology—Cybersecurity curriculum was presented to the Mississippi State Board of Education on January 15, 2026. The following people were serving on the state board at the time:

Dr. Lance Evans, State Superintendent of Education, Executive Secretary
Mr. Matt Miller, Southern Supreme Court District Representative, Chair
Mr. Matt Mayo, Central Supreme Court District Representative, Vice-Chair
Dr. Wendi Barrett, Teacher Representative
Mr. Glen East, Administrator Representative
Mr. Bill Jacobs, At-Large Representative
Dr. Ronnie McGehee, At-Large Representative
Mr. Mike Pruitt, At-Large Representative
Mrs. Billye Jean Stroud, Northern Supreme Court District Representative
Mrs. Mary Werner, At-Large Representative
Mr. Crosby Parker, Senior Student Representative
Ms. Michelle Xie, Junior Student Representative

The following Mississippi Department of Education (MDE) Office of Career and Technical Education (CTE) and Workforce Development (WD) and RCU managers and specialists assisted in the development of the Information Technology— Cybersecurity curriculum:

Brett Robinson, Associate State Superintendent, MDE Office of CTE and WD
Betsey Smith, Director, RCU
Myesha Wallace, Information Technology Program Supervisor, MDE Office of CTE and WD
Courtney McCubbins, CTE Curriculum and Assessment Manager, RCU
Courtney McAdams, Project Manager, RCU
Nathan King, Project Manager, RCU

Special thanks are extended to the educators who contributed to the development and revision of this framework and supporting materials:

Justin Dorris, Pontotoc Ridge Career and Technology Center, Pontotoc
Bryan Hudson, DeSoto County CTE West, Horn Lake

Appreciation is expressed to the following professionals who provided guidance and insight throughout the development process:

Tanner Bond, Instructor of Network Security, EMCC (Mayhew Campus)
Charlie Grace, Instructor of Computer Programming, EMCC (Mayhew Campus)
Shelly Hollis, Director, Center for Cyber Education at MSU
Horacio Leal, IST Instructor/Division Chair, EMCC (Mayhew Campus)
Kyle McDill, Project Manager, Center for Cyber Education at MSU
Jordan Miller, Instructor of Computer Networking, EMCC (Scooba Campus)
Martin Rivera, Manager, Mississippi Cyber Initiative Technology
Josh Stanford, Program Supervisor, Mississippi Department of Education

Standards

Standards and alignment crosswalks are referenced in the appendices. Depending on the curriculum, these crosswalks should identify alignment to the standards mentioned below, as well as possible related academic topics as required in the Subject Area Testing Program in Algebra I, Biology I, and English II, which could be integrated into the content of the units. Mississippi's CTE Information Technology—Cybersecurity curriculum is aligned to the following standards:

CompTIA CertMaster Learn Security+
CertMaster Learn standards validate essential skills required for core security functions and a career in IT security. They showcase professionals' capabilities in securing networks, applications, and devices, ensuring data integrity, confidentiality, and availability. These standards focus on practical, hands-on skills to tackle real-world challenges while also providing the knowledge necessary for advancing in the dynamic field of cybersecurity.
comptia.org

CompTIA TestOut CyberDefense Pro
CyberDefense Pro standards provide comprehensive training that equips students with advanced cybersecurity skills. It includes hands-on simulations and real-world scenarios designed to provide you with the knowledge to detect, analyze, and respond to threats in today's tech-driven world. These standards prepare students for the CompTIA Cybersecurity Analyst (CySA+) (V3) certification, ensuring success in a cybersecurity-related occupation.
comptia.org

College- and Career-Readiness Standards
College- and career-readiness standards emphasize critical thinking, teamwork, and problem-solving skills. Students will learn the skills and abilities demanded by today's workforce. The Mississippi College- and Career-Readiness Standards (MCCRS) provide a consistent, clear understanding of what students are expected to learn.
mdek12.org/academiceducation/mississipp-college-and-career-readiness-standards/

International Society for Technology in Education Standards (ISTE)

iste.org/standards

Career and Technical Student Organizations (CTSOs)
Mississippi's Career and Technical Education (CTE) curricula are aligned with the programs, activities, and competitive events offered through Career and Technical Student Organizations (CTSOs). These organizations provide students with opportunities to apply classroom knowledge in real-world contexts, develop leadership and employability skills, and connect with industry and community partners. Each pathway includes an appendix identifying the CTSOs most closely connected to the curriculum, ensuring that students' classroom learning is reinforced through co-curricular experiences that prepare them for success in both post-secondary education and the workforce.
mdek12.org/cte/so/

National Business Education Association (NBEA)—Information Technology Standards

The National Business Education Association (NBEA) is the nation's leading professional organization devoted exclusively to serving individuals and groups engaged in instruction, administration, research, and dissemination of information for and about business. It is a resource for any teacher focused on business education and 21st century skills. NBEA states, "IT is a common thread throughout every business." Additionally, it maximizes students' employability and their need to appreciate intellectual property, personal privacy, and security. NBEA encourages acting ethically, obeying the law, analyzing information, and developing service skills. Finally, the NBEA mentions that students have to be able to pragmatically solve IT problems and understand the value and impact of IT. NBEA Business Education Library (2023).
nbea.org

Preface

Secondary CTE programs in Mississippi face many challenges resulting from sweeping educational reforms at the national and state levels. Schools and teachers are increasingly being held accountable for providing applied learning activities to every student in the classroom. This accountability is measured through increased requirements for mastery and attainment of competency as documented through both formative and summative assessments. This document provides information, tools, and solutions that will aid students, teachers, and schools in creating and implementing applied, interactive, and innovative lessons. Through best practices, alignment with national standards and certifications, community partnerships, and a hands-on, student-centered concept, educators will be able to truly engage students in meaningful and collaborative learning opportunities.

The courses in this document reflect the statutory requirements as found in Section 37-3-49, *Mississippi Code of 1972*, as amended (Section 37-3-46). In addition, this curriculum reflects guidelines imposed by federal and state mandates (Laws, 1988, Ch. 487, §14; Laws, 1991, Ch. 423, §1; Laws, 1992, Ch. 519, §4 eff. from and after July 1, 1992; Strengthening Career and Technical Education for the 21st Century Act, 2019 [Perkins V]; and Every Student Succeeds Act, 2015).

Mississippi Teacher Professional Resources

The following are resources for Mississippi teachers:

Curriculum, Assessment, Professional Learning

- Program resources can be found at the RCU's website, rcu.msstate.edu.

Learning Management System: An Online Resource

- Learning management system information can be found at the RCU's website, under Professional Learning.

Should you need additional instructions, contact the RCU at 662.325.2510 or helpdesk@rcu.msstate.edu.

Executive Summary

Pathway Description
Information Technology is a pathway within the Digital Technology Career Cluster that provides the foundation, skills, and knowledge necessary for computer networking, applications, and support. Students will develop the skills necessary to prepare for certification exams and will learn how to develop, support, and integrate computing systems. They will acquire network-planning and management skills and the ability to provide technical support. The program provides hands-on experiences focused on skills related to computer system support, network setup, and system maintenance.

College, Career, and Certifications
For the most updated certification and assessment information regarding this pathway, review the blueprint located on the RCU's curriculum page.

Grade Level and Class Size Recommendations
It is recommended that students enter this program as sophomores, juniors, or seniors. Exceptions to this are a district-level decision based on class size, enrollment numbers, student maturity, and CTE delivery method. This is a hands-on, lab- or shop-based course. Therefore, a maximum of 15 students is recommended per class with only one class with the teacher at a time.

Student Prerequisites
For students to experience success in the program, the following student prerequisites are suggested:

1. C or higher in English (the previous year)
2. C or higher in high school-level math (last course taken, or the instructor can specify the level of math instruction needed)
3. Instructor approval

or

1. Instructor approval

Assessment
The latest assessment blueprint for the curriculum can be found at rcu.msstate.edu/curriculum.

Applied Academic Credit
The latest academic credit information can be found at mdek12.org/secondaryeducation/approved-courses.

Educator Licensure
The latest educator licensure information can be found at mdek12.org/licensure/.

Professional Learning
If you have specific questions about the content of any training sessions provided, please contact the RCU at 662.325.2510 or helpdesk@rcu.msstate.edu.

Course Outlines

Option 1—Two 1-Carnegie Unit Courses

This curriculum consists of two 1-credit courses that should be completed in the following sequence:

1. **Information Technology Cybersecurity I—Course Code: XXXXXX**
2. **Information Technology Cybersecurity II—Course Code: XXXXXX**

Course Description: Information Technology Cybersecurity I
In Cybersecurity I, students will explore career opportunities and essential computing skills while understanding the ethical and safety considerations involved. This course covers fundamental security concepts, zero-trust models, and techniques regarding security controls and encryption. The curriculum further introduces students to the different types of cybersecurity threats. It also covers security architecture and enterprise infrastructure.

Course Description: Information Technology Cybersecurity II
Cybersecurity II focuses on cybersecurity procedures, introduces program management basics, and equips students with career development skills. Students will apply techniques, use monitoring tools, and solve real-world security challenges related to system hardening and asset and vulnerability management. The curriculum provides a comprehensive understanding of security program administration, governance, compliance, and risk management. Students will have the opportunity to explore certifications and educational pathways to prepare them for successful entry into the workforce or continued education.

Information Technology Cybersecurity I —Course Code: XXXXXX

Unit	Title	Hours
1	Orientation to Cybersecurity	25
2	Basic Security Concepts	35
3	Cybersecurity Threats, Vulnerabilities, and Mitigations	40
4	Security Architecture	40
Total		**140**

Information Technology Cybersecurity II —Course Code: XXXXXX

Unit	Title	Hours
5	Cybersecurity Procedures	50
6	Security Program Management and Administration	45
7	Career Development	45
Total		**140**

Option 2—One 2-Carnegie Unit Courses

This curriculum consists of one 2-credit course that should be completed in the following sequence:

1. **Information Technology Cybersecurity —Course Code: XXXXXX**

Course Description: Information Technology Cybersecurity
In the Cybersecurity curriculum, students will begin by exploring career opportunities and essential computing skills while understanding the ethical and safety considerations involved. It covers fundamental security concepts and zero-trust models, allowing students to gain insight into security controls and encryption techniques. The curriculum further introduces students to the different types of cybersecurity threats. It also covers security architecture and enterprise infrastructure. This course encourages students to focus on cybersecurity procedures, program management, and career development. They will apply techniques for system hardening, asset and vulnerability management, and the use of monitoring tools. They will handle real-world security challenges. The curriculum also covers governance, compliance, and risk management to provide a comprehensive understanding of security program administration. Students will have the opportunity to work on career development skills by exploring certifications and educational pathways to prepare them for successful entry into the workforce or continued education.

Information Technology Cybersecurity —Course Code: XXXXXX

Unit	Unit Title	Hours
1	Orientation to Cybersecurity	25
2	Basic Security Concepts	35
3	Cybersecurity Threats, Vulnerabilities, and Mitigations	40
4	Security Architecture	40
5	Cybersecurity Procedures	50
6	Security Program Management and Administration	45
7	Career Development	45
Total		**280**

Career Pathway Outlook

Overview

The Information Technology— Cybersecurity program prepares students for information security analysis and cybersecurity consultant-related careers. Students will develop employability and critical thinking skills while investigating security measures. They will become proficient in maintaining firewalls and data encryption programs, as well as troubleshooting cybersecurity issues, including phishing attacks, malware infections, and compromised passwords. Occupations involving information security analysis and cybersecurity consultation typically monitor networks for security breaches and assess vulnerabilities in computer and network systems. Information security analysts monitor organizational networks, maintain software to protect sensitive information, and check for vulnerabilities in network systems. Information security analysts held about 180,700 jobs nationally in 2023. Prospective employers include information technology industries, insurance providers, and computer system design-related services. Most information security analysts work full-time, with the possibility of working more than 40 hours per week. Administrators may need to be on call outside of normal business hours in case of an emergency.

Most careers in cybersecurity require at least a bachelor's degree, although careers with the highest earning potential—senior or enterprise-level security analysts and postsecondary teachers, for example—may require advanced degrees (e.g., Master of Business Administration (MBA), Doctor of Philosophy (PhD) in computer science, etc.).

Needs of the Future Workforce

Relative to cybersecurity, two of the fastest-growing occupations nationally are information security analysts and data scientists. Their growth rates are 33% and 36%, respectively, according to the U.S. Bureau of Labor Statistics. They are the fourth and fifth-fastest-growing occupations nationally.

Table 1.1: Current and Projected Occupation Report

Description	Jobs, 2022	Projected Jobs, 2032	Change (Number)	Change (Percent)	Average Hourly Earnings, 2025
Computer and Information Research Scientists	320	400	80	25%	$36.01
Computer and Information Systems Managers	1,380	1,650	270	19.6%	$38.87
Computer Network Architects	300	310	10	3.3%	$29.70
Computer Network Support Specialists	1,020	1,140	120	11.8%	$17.37
Computer User Support Specialists	2,800	3,140	340	12.1%	$15.44
Database Administrators	250	280	30	12%	$27.11
Database Architects	90	110	20	22.2%	$28.54
Information Security Analysts	560	830	270	48.2%	$26.63
Network and Computer Systems Administrators	1,610	1,700	90	5.6%	$22.23
Software Developers	2,750	3,930	1,180	42.9%	$19.98

Software Quality Assurance Analysts and Testers	550	710	160	29.1%	$23.73
Web and Digital Interface Designers	230	290	60	26.1%	$19.35
Web Developers	200	270	70	35%	$19.70

Source: Mississippi Department of Employment Security; mdes.ms.gov (2025).

Perkins V Requirements and Academic Infusion

The Information Technology— Cybersecurity curriculum meets Perkins V requirements of introducing students to and preparing them for high-skill, high-wage occupations in information technology-related fields. It also offers students a program of study, including secondary, postsecondary, and institutions of higher learning courses, that will further prepare them for cybersecurity careers. Additionally, this curriculum is integrated with academic college- and career-readiness standards. Lastly, it focuses on ongoing and meaningful professional development for teachers as well as relationships with industry.

Transition to Postsecondary Education

The latest articulation information for secondary to postsecondary can be found at the Mississippi Community College Board website, mccb.edu.

Best Practices

Innovative Instructional Technologies

Classrooms should be equipped with tools that will teach today's digital learners through applicable and modern practices. The Information Technology— Cybersecurity educator's goal should be to include teaching strategies that incorporate current technology. To make use of the latest online communication tools—wikis, blogs, podcasts, and social media platforms, for example—the classroom teacher is encouraged to use a learning management system that introduces students to education in an online environment and places more of the responsibility of learning on the student.

Differentiated Instruction

Students learn in a variety of ways, and numerous factors—students' background, emotional health, and circumstances, for example—create unique learners. By providing various teaching and assessment strategies, students with various learning preferences can have more opportunities to succeed.

CTE Student Organizations

Teachers should investigate opportunities to sponsor a student organization. Mississippi offers CTSOs that will foster the types of learning expected from the Information Technology—Cybersecurity curriculum, such as SkillsUSA and TSA. Student organizations provide participants and members with growth opportunities and competitive events. They also open the doors to the world of information technology careers and scholarship opportunities.

Cooperative Learning

Cooperative learning can help students understand topics when independent learning cannot. Therefore, you will see several opportunities in the Information Technology—Cybersecurity curriculum for group work. To function in today's workforce, students need to be able to work collaboratively with others and solve problems without excessive conflict. This curriculum provides opportunities for students to work together and help each other complete complex tasks. There are many field experiences within the Information

Technology—Cybersecurity curriculum that will allow and encourage collaboration with professionals currently in the cybersecurity field.

Work-Based Learning

Work-based learning is an extension of understanding competencies taught in Information Technology—Cybersecurity classroom. This curriculum is designed in a way that necessitates active involvement by the students in the community around them and the global environment. These real-world connections and applications link all types of students to knowledge, skills, and professional dispositions. Work-based learning should encompass ongoing and increasingly more complex involvement with local companies and cybersecurity professionals. Thus, supervised collaboration and immersion into the information technology industry around the students are keys to students' success, knowledge, and skills development.

Professional Organizations

Center for Internet Security (CIS)
cisecurity.org

Chapters - Local Cybersecurity Chapters - (ISC^2)
isc2.org

Computing Technology Industry Association (CompTIA)
comptia.org

Cybersecurity and Infrastructure Security Agency (CISA)
cisa.gov

Information Systems Audit and Control Association (ISACA)
isaca.org

InfraGard (partnership with the FBI)
infragard.org

Institute - SysAdmin, Audit, Network, and Security (SANS)
sans.org

International Council of E-Commerce Consultants (EC-Council)
eccouncil.org

International Information System Security Certification Consortium (ISC^2)
isc2.org

National Initiative for Cybersecurity Education (NIST -NICE)
nist.gov

Open Worldwide Application Security Project (OWASP)
owasp.org

Special Interest Group on Security, Audit and Control (ACM SIGSAC)
sigsac.org

Using This Document

Competencies and Suggested Objectives
A competency represents a general concept or performance that students are expected to master as a requirement for satisfactorily completing a unit. Students will be expected to receive instruction on all competencies. The suggested objectives represent the enabling and supporting knowledge and performances that will indicate mastery of the competency at the course level.

Teacher Resources
All teachers should request to be added to the Canvas Resource Guide for their course. For questions or to be added to the guide, send a Help Desk ticket to the RCU by emailing helpdesk@rcu.msstate.edu.

Perkins V Quality Indicators and Enrichment Material
Some of the units may include an enrichment section at the end. This material will greatly enhance the learning experiences of students. If the Information Technology pathway utilizes a national certification, work-based learning, or another accountability measure that aligns with Perkins V as a quality indicator, this material may be assessed based on that quality indicator. It is the responsibility of the teacher to ensure all competencies for the selected quality indicator are covered throughout the year.

Unit 1: Orientation to Cybersecurity

Competencies and Suggested Objectives
1. Research educational, occupational, and leadership opportunities in cybersecurity. DOK3 a. Review student rules and regulations for the local school. b. Compare and contrast local program policies, procedures, and expectations to industry policies, procedures, and expectations. c. Identify and describe leadership opportunities available from CTE student organizations in the school and community.
2. Identify, discuss, and apply safety procedures in the computer classroom and lab. DOK2 a. Discuss the proper classroom and personal safety procedures, including fire extinguishers, electrical, ladders, clothing, jewelry, eye protection, etc. b. Care for and correctly use computer hardware. c. Identify potential hazards when working with technology equipment. d. Explore environmental impacts related to technology. e. Develop personal safety guidelines for using technology and the internet.
3. Publish and communicate research findings on emerging cybersecurity technologies, recent trends, and cybersecurity-related issues with peers, experts, and general audiences using technology. DOK3 a. Research safety issues related to technology and internet academic standards, where applicable. b. Define and apply digital citizenship, online safety, and appropriate use best practices and their importance regarding cybersecurity. c. Outline computer industry-related legal considerations, including software copyright issues and licensing, and internet ethics and policies. d. Review and adhere to the school's technology acceptable-use policy. e. Engage in positive, safe, legal, and ethical behavior when using technology, including social interactions online. f. Utilize online tools and electronic media to communicate effectively. g. Research, create, and present on emerging cybersecurity technologies, best practices, recent trends, and cybersecurity-related issues.
4. Define computing basics and manage file systems. DOK2 a. Demonstrate file management best practices, including creating, organizing, and managing files and folders. b. Utilize a file management system for efficient data organization and retrieval.
5. Explore cybersecurity careers and communicate effectively using technology. DOK3 a. Research and present on educational, occupational, and leadership opportunities in cybersecurity. b. Review student rules and regulations for the local school and compare them to industry standards.
6. Understand and explore the developments of artificial intelligence (AI). DOK4 a. Analyze the influence of AI on cybersecurity practices. b. Define and develop effective prompting or prompt engineering. c. Identify and evaluate best practices in using AI for cybersecurity. d. Discuss and analyze ethical dilemmas that arise when using AI for cybersecurity. e. Explore and assess how AI is currently being utilized in the cybersecurity field. f. Compare and contrast a variety of career opportunities within AI.

Note: Safety is to be taught as an ongoing part of the program. Students are required to complete a written safety test with 100% accuracy before entering the shop for lab simulations and projects. This test should be documented in each student's file.
Note: This unit will be ongoing throughout the year. Time allotted for this unit will be distributed over the entire year.

Unit 2: Basic Security Concepts

Competencies and Suggested Objectives
1. Analyze, test, and monitor types of security controls. DOK3 a. Define and describe the four categories of security controls. • Managerial • Operational • Physical • Technical b. Define and analyze the six types of security controls. • Compensating • Corrective • Detective • Deterrent • Directive • Preventive
2. Understand important security concepts that are critical for protecting information systems. DOK3 a. Examine the concepts of confidentiality, integrity, and availability (CIA). b. Define authentication, authorization, and accounting (AAA) and how it applies to cybersecurity. c. Define zero-trust and explain control plane components. • Adaptive identity • Threat scope reduction • Policy-driven access control • Policy administrator • Policy engine d. Explain how the data plane supports cybersecurity in a zero-trust structure. • Implicit trust zones • Subject/system interactions • Policy enforcement point e. Describe how physical security is effective. • Access badge • Access control vestibule • Bollards • Fencing • Infrared • Lighting • Microwave • Pressure • Security guard • Sensors • Ultrasonic • Video surveillance f. Develop a comprehensive deception technology plan based on cybersecurity needs. • Honeypot • Honeynet

- Honeyfile
- Honeytoken

3. Explain the significance of change management processes in cybersecurity. DOK2
   a. Analyze various business processes that influence security operations.
      - Impact analysis
      - Backout plan
   b. Understand critical technical aspects that must be considered during change management.
      - Allow lists/deny lists
      - Restricted activities
      - Legacy applications
      - Dependencies
   c. Develop thorough documentation concerning change management practices.
   d. Explore version control.

4. Explain and analyze data security encryption. DOK3
   a. Discuss the importance of encryption for protecting sensitive information during transmission and storage.
      - Algorithms
      - Asymmetric
      - Key exchange
      - Key length
      - Level
        - Full-disk
        - Partition
        - File
        - Volume
        - Database
        - Record
      - Symmetric
      - Transport/communication
   b. Recognize and apply cryptographic tools.
      - Hardware security module (HSM)
      - Key management system
      - Secure enclave
      - Trusted Platform Module (TPM)
   c. Define the concept and importance of hashing.

Unit 3: Cybersecurity Threats, Vulnerabilities, and Mitigations

Competencies and Suggested Objectives
1. Understand the different types of cybersecurity threat actors and the motivations behind their actions. DOK2 a. Compare and contrast types of cybersecurity threat actors and analyze their motives. • Cybercriminals • Hacktivists • Nation-state actors • Insider threats • Financial gain • Philosophical agendas • Ethics and data exfiltration
2. Compare and contrast the various cybersecurity threat vectors and attack surfaces. DOK2 a. Classify and investigate types of message-based threat vectors, types of schemes and practices used, and assess their impact. • Email • Short Message Service (SMS) • Instant messaging (IM) b. Explain the concept of cybersecurity supply chain attacks and detail their significance. • Managed service providers (MSPs) • Vendors • Suppliers c. Explain how human vectors relate to social engineering and describe its impact on cybersecurity. • Brand impersonation • Business email compromise (BEC) • Impersonation • Misinformation/disinformation • Phishing • Pretexting • Smishing • Typosquatting • Vishing • Watering hole attack
3. Identify, describe, and investigate different types of vulnerabilities in cybersecurity. DOK2 a. Classify and explain common application vulnerabilities, describe how they can be exploited, and identify their effect on system security. b. Recognize commonplace operating system (OS) platform vulnerabilities. c. Define virtualization and explain how to utilize virtual machines (VMs) within the context of cybersecurity. d. Classify common misconfigurations in IT systems and applications and describe how misconfigurations can lead to cybersecurity breaches. e. Classify security challenges and vulnerabilities associated with mobile devices. • Side loading • Jailbreaking

4. Categorize, investigate, and explain indicators of malicious activity in cybersecurity scenarios. DOK2
   a. Recognize and explore common types of malware attacks.
      - Adware/Bloatware, potentially unwanted programs (PUPs)
      - Keylogger
      - Logic bomb
      - Ransomware
      - Rootkit
      - Spyware
      - Trojan
      - Virus
      - Worm
   b. Recognize and explore types of physical security breaches.
      - Environmental threats (e.g., fire, flooding, overheating, power outages, etc.)
      - Radio frequency identification (RFID) cloning
      - Shoulder surfing
      - Social engineering
      - Tailgating

5. Compare and contrast mitigation techniques used in enterprise systems security. DOK2
   a. Explain access control, types of methods used, and its importance in enterprise security.
      - Access control list (ACL)
      - Permissions
   b. Clarify the importance of isolation in the context of cybersecurity and explore different isolation techniques.
   c. Define the principle of least privilege and explain how it reduces cybersecurity attack surfaces.
   d. Describe and explain system hardening techniques used within enterprise security.
      - Encryption
      - Installation of endpoint protection
      - Host-based firewall
      - Host-based intrusion prevention system (HIPS)
      - Disabling ports/protocols
      - Default password changes
      - Removal of unnecessary software

Mississippi Career Connections

Cybersecurity is a rapidly growing field across Mississippi as banks, hospitals, schools, manufacturers, and technology companies work to protect their networks and data. To connect this unit to real-world careers, students should assume the role of cybersecurity analysts and review a mock security incident for a Mississippi organization. Students identify the type of threat actor involved, determine the likely attack vector (email, SMS, social engineering, or supply chain), and recommend one mitigation strategy. This quick exercise helps students see how the concepts in this unit mirror the work done by IT professionals across the state.

Unit 4: Security Architecture

Competencies and Suggested Objectives
1. Explore and differentiate between security implications of varying architecture models. DOK3 a. Investigate the security features and weaknesses of cloud architecture. • Hybrid considerations • Responsibility matrix • Third-party vendors b. Describe the security implications of using Infrastructure as Code (IaC). c. Examine security measures in conventional network infrastructure. • Physical isolation • Logical segmentation • Software-defined networking (SDN) d. Consider the security issues associated with Internet of Things (IoT) devices. e. Explain the effect of scalability on security practices. f. Investigate the security concerns related to ease of deployment.
2. Compare and contrast security standards to secure enterprise infrastructure. DOK3 a. Discuss key infrastructure elements for safeguarding enterprise systems. • Attack surface • Connectivity • Device attribute • Device placement • Failure modes • Firewall types • Network appliances • Port security • Security zones b. Analyze secure communication and access methods in enterprise environments. • Remote access • Secure Access Service Edge (SASE) • Software-defined wide area network (SD-WAN) • Tunneling • Virtual private network (VPN)
3. Identify, discuss, and apply concepts and approaches to protect data. DOK3 a. Distinguish between types of data. • Financial information • Human- and not-human-readable • Intellectual property • Legal information • Regulated • Trade secret b. Understand and explore common data considerations. • Data states • Data sovereignty • Geolocation

c. Compare and contrast safe data methods such as access controls and encryption.
    - Encryption
    - Geographic restrictions
    - Hashing
    - Masking
    - Obfuscation
    - Permission restrictions
    - Segmentation
    - Tokenization

4. Communicate the significance of recovery and resilience in security architecture. DOK3
    a. Explore high availability and its importance in securing architecture.
    b. Analyze the importance of multi-cloud systems.
    c. Recognize the importance of testing within security architecture.
        - Tabletop exercises
        - Fail over
        - Simulation
        - Parallel processing
    d. Investigate exercises guaranteeing data backup recovery.
        - Encryption
        - Frequency
        - Journaling
        - Onsite/offsite
        - Recovery
        - Replication
        - Snapshots

Unit 5: Cybersecurity Procedures

Competencies and Suggested Objectives
1. Explore commonplace security techniques. DOK3 a. Communicate the techniques used when hardening targets. • Cloud infrastructure • Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) • Embedded systems • IoT devices • Mobile devices • Routers • Real-time operating system (RTOS) • Servers • Switches • Workstations b. Investigate mobile solutions involving device security. • Connection methods • Deployment models • Mobile device management c. Recognize and explore wireless security settings related to network environments. • AAA/Remote Authentication Dial-In User Service (RADIUS) • Authentication protocols • Cryptographic protocols • Wi-Fi Protected Access 3 (WPA3) d. Investigate application security measures. • Code signing • Input validation • Secure cookies • Static doe analysis
2. Investigate ways to properly secure hardware, software, and data asset management. DOK2 a. Explain the acquisition and procurement process as it relates to securing both hardware and software. b. Summarize the methods for monitoring and tracking assets. c. Critique the best practices for disposing of and decommissioning both data and hardware. • Certification • Data retention • Destruction • Sanitization
3. Define and describe vulnerability management activities. DOK2 a. Identify methods for discovering system and application vulnerabilities. • Application security • Penetration testing • Responsible disclosure program • System/process audit • Threat feed

- Vulnerability scan

b. Verify remediation effectiveness related to vulnerabilities.
   - Audit
   - Rescanning
   - Verification

4. Explain security alerting and monitoring concepts and tools. DOK2
   a. Recognize and explore security monitoring and notification tools.
      - Agents/agentless
      - Antivirus
      - Benchmarks
      - Data loss prevention (DLP)
      - NetFlow
      - Security Content Automation Protocol (SCAP)
      - Security information and event management (SIEM)
      - Simple Network Management Protocol (SNMP) traps
      - Vulnerability scanners

5. Investigate security enhancements related to enterprise capabilities. DOK2
   a. Investigate and apply firewall settings concepts to ensure a secure environment.
   b. Explore and examine Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS).
   c. Investigate web filtering solutions.
   d. Implement configurations for operating system security.
   e. Execute secure network communication protocols.
   f. Apply Domain Name System (DNS) filtering.
   g. Determine protective email security measures.
   h. Investigate network access control (NAC) in relation to security.
   i. Investigate user behavior analytics.

6. Formulate a plan to maintain access and identity management. DOK2
   a. Provision and deprovision of user accounts.
   b. Apply access control measures.
   c. Distinguish between account security and multifactor authentication methods.
   d. Consider concepts regarding password management.
   e. Employ privileged access management tools related to administrative account security.

7. Describe activities regarding incident response. DOK2
   a. Describe the process when recovering, detecting, or preparing stages.
   b. Investigate the importance of incident response training.
   c. Recognize and explore the idea of threat hunting.
   d. Investigate digital forensics standards related to incident response.

Unit 6: Security Program Management and Administration

Competencies and Suggested Objectives
1. Investigate the basics of successful security governance. DOK2 a. Identify and describe the tasks associated with security standards. b. Recognize the importance of maintaining security using common procedures. c. Investigate the roles and responsibilities concerning data security and systems.
2. Investigate the basics of successful security governance. DOK2 a. Identify and describe the tasks associated with security standards. b. Recognize the importance of maintaining security using common procedures. c. Investigate the roles and responsibilities concerning data security and systems.
3. Describe fundamentals of cybersecurity risk management. DOK2 a. Recognize the process of cybersecurity-related risk identification. b. Assess potential threats when conducting a risk assessment. c. Investigate the steps associated with risk analysis. d. Examine the significance of risk tolerance. e. Explore risk management strategies. f. Clarify the importance of risk reporting.
4. Investigate the essentials of security compliance. DOK2 a. Explain the elements and significance of compliance reporting. b. Recognize and explore the possible consequences of non-compliance. c. Examine compliance monitoring procedures, ensuring security policy compliance. d. Describe privacy standards in relation to program security.

Mississippi Career Connections
Security governance, risk management, and compliance are essential across various industries in Mississippi, including healthcare, banking, education, and manufacturing. To connect these concepts to real careers, give students a short scenario: • A regional Mississippi hospital discovers unusual login activity on its patient records system. As security governance analysts, students must identify which security standards apply, list the roles responsible for protecting the data, and complete a quick risk assessment outlining potential threats and risk tolerance. Students then recommend one mitigation step and explain a possible consequence if the hospital fails to meet compliance requirements.

Unit 7: Career Development

Competencies and Suggested Objectives
1. Develop and evaluate career readiness skills for success in cybersecurity professions. DOK4 a. Investigate career opportunities and emerging technologies in cybersecurity. b. Prepare a cover letter, a résumé, and a follow-up letter using word-processing software. c. Complete a job application. d. Demonstrate appropriate job interview skills in a real or mock interview.
2. Analyze appropriate communication skills and professional behavior when communicating with clients and coworkers. DOK4 a. Practice appropriate communication skills, including speaking clearly and concisely, using tact and discretion, avoiding jargon, asking pertinent questions, and exercising listening skills. b. Practice appropriate professional behavior, including maintaining a positive attitude and tone of voice, avoiding arguments or defensiveness, and respecting clients' privacy and property. c. Discuss the impact of social media profiles.
3. Research opportunities and apply concepts related to cybersecurity and participate in field experiences or simulations. DOK4 a. Investigate educational opportunities related to cybersecurity. b. Describe national standards and certification/licensing procedures related to cybersecurity. c. Describe the role of trade organizations, associations, and unions related to cybersecurity. d. Participate in a school-to-careers activity (e.g., shadowing, mentoring, simulations, career fair, etc.). e. Visit an industry/computer center. Observe, analyze, and discuss the following: • Hardware and software usage and needs • Educational training for personnel • Tasks performed by personnel • Outlook for those jobs
4. Research and critique the benefits of industry certifications for various information technology careers. DOK4 a. Compare and contrast entry-level and career-level certifications.

Mississippi Career Connections
Mississippi's cybersecurity needs vary widely across industries, from protecting patient data in healthcare systems to securing industrial machinery in manufacturing facilities and defending networks in state and local government. Students should select three Mississippi industries (e.g., healthcare systems in Jackson, banking in Tupelo, manufacturing in Columbus/Golden Triangle, education networks, energy/utilities, or new data centers). For each industry, students identify: • One cybersecurity role needed in that environment • One essential communication or professionalism skill required for that job • One certification or training path that aligns with that role • One emerging technology or threat relevant to that sector Students then combine their answers to create a three-person Mississippi Cyber team, each with different responsibilities and strengths, and write a short explanation of how their team helps defend the state's digital infrastructure.

Student Competency Profile

Student's Name: _____

This record is intended to serve as a method of noting student achievement of the competencies in each unit. It can be duplicated for each student, and it can serve as a cumulative record of competencies achieved in the course.

In the blank before each competency, place the date (MM/DD/YY) on which the student mastered the competency.

Unit 1: Orientation to Cybersecurity		
	1.	Research educational, occupational, and leadership opportunities in cybersecurity.
	2.	Identify, discuss, and apply safety procedures in the computer classroom and lab.
	3.	Publish and communicate research findings on emerging cybersecurity technologies, recent trends, and cybersecurity-related issues with peers, experts, and general audiences using technology
	4.	Define computing basics and manage file systems.
	5.	Explore cybersecurity careers and communicate effectively using technology
	6.	Understand and explore the developments of artificial intelligence (AI).
Unit 2: Basic Security Concepts		
	1.	Analyze, test, and monitor types of security controls.
	2.	Understand important security concepts that are critical for protecting information systems.
	3.	Explain the significance of change management processes in cybersecurity.
	4.	Explain and analyze data security encryption.
Unit 3: Cybersecurity Threats, Vulnerabilities, and Mitigations		
	1.	Understand the different types of cybersecurity threat actors and the motivations behind their actions.
	2.	Compare and contrast the various cybersecurity threat vectors and attack surfaces.
	3.	Identify, describe, and investigate different types of vulnerabilities in cybersecurity.
	4.	Categorize, investigate, and explain indicators of malicious activity in cybersecurity scenarios.
	5.	Compare and contrast mitigation techniques used in enterprise systems security.
Unit 4: Security Architecture		
	1.	Explore and differentiate between security implications of varying architecture models.
	2.	Compare and contrast security standards to secure enterprise infrastructure.
	3.	Identify, discuss, and apply concepts and approaches to protect data.
	4.	Communicate the significance of recovery and resilience in security architecture.

Unit 5: Cybersecurity Procedures		
	1.	Explore commonplace security techniques.
	2.	Investigate ways to properly secure hardware, software, and data asset management.
	3.	Define and describe vulnerability management activities.
	4.	Explain security alerting and monitoring concepts and tools.
	5.	Investigate security enhancements related to enterprise capabilities.
	6.	Formulate a plan to maintain access and identity management.
	7.	Describe activities regarding incident response.
Unit 6: Security Program Management and Administration		
	1.	Investigate the basics of successful security governance.
	2.	Describe fundamentals of cybersecurity risk management.
	3.	Investigate the essentials of security compliance.
Unit 7: Career Development		
	1.	Develop and evaluate career readiness skills for success in cybersecurity professions.
	2.	Analyze appropriate communication skills and professional behavior when communicating with clients and coworkers.
	3.	Research opportunities and apply concepts related to cybersecurity and participate in field experiences or simulations.
	4.	Research and critique the benefits of industry certifications for various information technology careers.

Appendix A: CCR-English II Standards

	Units						
Standards	**1**	**2**	**3**	**4**	**5**	**6**	**7**
RI.10.1	X	X	X			X	
RI.10.2	X		X			X	
RI.10.4	X	X	X	X			
W.10.2	X	X	X		X		X
W.10.4	X	X	X	X	X	X	X
W.10.6	X		X				X
W.10.7	X		X				
SL.10.1	X		X		X		X
SL.10.4	X		X	X	X		X
L.10.4	X	X	X	X	X	X	X
L.10.6	X	X	X	X	X	X	X

Reading Standards for Informational Text- College and Career Readiness Anchor Standards for Informational Text

Key Ideas and Details

1. Cite strong and thorough textual evidence to support analysis of what the text says explicitly as well as inferences drawn from the text.
2. Determine the central idea(s) of a text and analyze in detail the development over the course of the text, including how details of a text interact and build on one another to shape and refine the central idea(s); provide an accurate summary of the text based upon this analysis.

Craft and Structure

1. Determine the meaning of words and phrases as they are used in a text, including figurative, connotative, and technical meanings; analyze the cumulative impact of specific word choices on meaning and tone (e.g., how the language of a court opinion differs from that of a newspaper).

College and Career Readiness Anchor Standards for Writing

Text Types and Purposes

1. Write informative/explanatory texts to examine and convey complex ideas, concepts, and information clearly and accurately through the effective selection, organization, and analysis of content.
   a. Introduce a topic; organize complex ideas, concepts, and information to make important connections and distinctions; include formatting (e.g., headings), graphics (e.g., figures, tables), and multimedia when useful to aiding comprehension.
   b. Develop the topic with well-chosen, relevant, and sufficient facts, extended definitions, concrete details, quotations, or other information and examples appropriate to the audience's knowledge of the topic.
   c. Use appropriate and varied transitions to link the major sections of the text, create cohesion, and clarify the relationships among complex ideas and concepts.
   d. Use precise language and domain-specific vocabulary to manage the complexity of the topic.
   e. Establish and maintain a formal style and objective tone while attending to the norms and conventions of the discipline in which they are writing.
   f. Provide a concluding statement or section that follows from and supports the information or explanation presented (e.g., articulating implications or the significance of the topic).

Production and Distribution of Writing

1. Produce clear and coherent writing in which the development, organization, and style are appropriate to task, purpose, and audience. (Grade-specific expectations for writing types are defined in standards 1–3 above.)
2. Use technology, including the Internet, to produce, publish, and update individual or shared writing products, taking advantage of technology's capacity to link to other information and to display information flexibly and dynamically.

Research to Build and Present Knowledge

1. 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; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation.

College and Career Readiness Anchor Standards for Speaking and Listening

Comprehension and Collaboration

1. Initiate and participate effectively in a range of collaborative discussions (one- on-one, in groups, and teacher-led) with diverse partners on grades 9–10 topics, texts, and issues, building on others' ideas and expressing their own clearly and persuasively.
    a. Come to discussions prepared, having read and researched material under study; explicitly draw on that preparation by referring to evidence from texts and other research on the topic or issue to stimulate a thoughtful, well-reasoned exchange of ideas.
    b. Work with peers to set rules for collegial discussions and decision-making (e.g., informal consensus, taking votes on key issues, presentation of alternate views), clear goals and deadlines, and individual roles as needed.
    c. Propel conversations by posing and responding to questions that relate the current discussion to broader themes or larger ideas; actively incorporate others into the discussion; and clarify, verify, or challenge ideas and conclusions.
    d. Respond thoughtfully to diverse perspectives, summarize points of agreement and disagreement, and, when warranted, qualify or justify their own views and understanding and make new connections in light of the evidence and reasoning presented.

Presentation of Knowledge and Ideas

1. Present information, findings, and supporting evidence clearly, concisely, and logically such that listeners can follow the line of reasoning and the organization, development, substance, and style are appropriate to purpose, audience, and task.

College and Career Readiness Anchor Standards for Language

Vocabulary Acquisition and Use

1. Determine or clarify the meaning of unknown and multiple-meaning words and phrases based on grades 9–10 reading and content, choosing flexibly from a range of strategies.
    a. Use context (e.g., the overall meaning of a sentence, paragraph, or text; a word's position or function in a sentence) as a clue to the meaning of a word or phrase.
    b. Identify and correctly use patterns of word changes that indicate different meanings or parts of speech (e.g., analyze, analysis, analytical; advocate, advocacy).
    c. Consult general and specialized reference materials (e.g., dictionaries, glossaries, thesauruses), both print and digital, to find the pronunciation of a word or determine or clarify its precise meaning, its part of speech, or its etymology.
    d. Verify the preliminary determination of the meaning of a word or phrase (e.g., by checking the inferred meaning in context or in a dictionary).
2. Acquire and use accurately general academic and domain-specific words and phrases, sufficient for reading, writing, speaking, and listening at the college and career readiness level; demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression.

Appendix B: NBEA - Information Technology Standards

	Units						
Standards	**1**	**2**	**3**	**4**	**5**	**6**	**7**
IT2: Literacy	X	X	X	X	X	X	X
IT3: Citizenship	X						
IT4: Devices			X				
IT5: Operating Systems				X	X		
IT6: Input					X		
IT7: Applications			X		X		
IT10: Databases			X				
IT11: Project Mgmt						X	
IT12: Programming					X		
IT13: Networking				X			
IT14: Planning				X	X		
IT15: Security		X					
IT16: Support	X						X
IT17: Business						X	
IT18: Careers							X

National Business Education Association (NBEA): Information Technology Standards

2) INFORMATION LITERACY: Achievement Standard - Gather, evaluate, synthesize, use, cite, and disseminate information from technology sources.

Level 1 Performance Expectations

1. Use information technology resources to retrieve information
2. Evaluate the credibility, reliability, and bias of information sources
3. Interpret information for use in decision making
4. Cite information sources appropriately
5. Use search procedures appropriate to type of information, nature of source, and nature of query
6. Discuss and follow copyright rules, trademarks, intellectual property, creative commons, and regulations (e.g., images, music, video, software)
7. Explain plagiarism and its consequences

Level 2 Performance Expectations

8. Evaluate the accuracy, relevance, and comprehensiveness of retrieved information
9. Draw conclusions and make generalizations based on information gathered
10. Access, exchange, organize, and synthesize information
11. Analyze the effectiveness of information resources to support collaborative tasks, research, publications, communications, and increased productivity

Level 3–4 Performance Expectations

12. Synthesize information from data sources to formulate decisions across the curriculum
13. Analyze and use mathematical and/or statistical methods to manipulate data into useful information
14. Present analyzed information in a meaningful format

3) DIGITAL CITIZENSHIP: Achievement Standard - Demonstrate respectful, responsible, inclusive, and ethical behavior in a digital world.

Level 1-2 Performance Expectations

1. Identify and explore basic privacy issues associated with technology
2. Explore the risks and dangers of sharing personal information in a digital world (e.g., digital footprint, cyberbullying, cyberstalking, identity theft)
3. Explore the possibilities and perils of digital communications
4. Discuss and apply Internet safety practices
5. Identify how social media is used to learn across the curriculum
6. Explore how technology can be used to address bias and create more inclusive communities
7. Discuss basic issues related to responsible use of technology and describe personal or legal consequences of inappropriate use
8. Demonstrate respectful and responsible use and creation of media and technology
9. Demonstrate the appropriate and legal use of intellectual property
10. Demonstrate legal, inclusive, and ethical behaviors when using information technologies
11. Identify aspects of global connectivity and its implications
12. Demonstrate appropriate etiquette when using information technologies
13. Discuss the process of safely buying and selling online
14. Review acceptable use policies for legal and ethical use of information

Level 3–4 Performance Expectations

15. Recognize the importance of one's digital footprint and manage it professionally
16. Recognize responsible use of digital commerce
17. Recognize how information technology contributes to lifelong learning
18. Implement organizational policies and procedures dealing with legal, ethical, and inclusive issues
19. Compare and contrast various types of license agreements (e.g., open source, creative commons, multiple license agreements, single-user installation, site license)
20. Read, interpret, and adhere to software license agreements and legal mandates
21. Analyze legal and ethical dilemmas within the framework of current laws and legislation (e.g., virus development, hacking, threats, phishing)

4) DEVICES AND COMPONENTS: Achievement Standard - Describe current and emerging devices and components; configure, install, and upgrade equipment; diagnose problems; and repair hardware.

Level 1 Performance Expectations

1. Identify devices appropriate for specific tasks
2. Identify the components of devices
3. Connect needed external components
4. Evaluate the capabilities and limitations of devices for user needs
5. Explain the purpose, operation, and care of devices and components
6. Identify examples of emerging technologies
7. Identify storage options

Level 2 Performance Expectations

8. Describe interrelationships between device components and supportive applications
9. Troubleshoot and diagnose applications and devices using appropriate resources (e.g., help desks, online help, manuals, technical support specialists)
10. Evaluate devices and features to make sound consumer decisions
11. Compare and contrast various storage devices (e.g., local, removable, remote, cloud)
12. Remove, upgrade, store, and install computer hardware and supportive applications

Level 3-4 Performance Expectations

13. Troubleshoot and repair computer hardware and resolve related application problems
14. Obtain hardware certification(s) needed for a chosen career path
15. Evaluate and recommend devices to solve specific problems

16. Analyze cost-benefit and life cycle of devices
17. Evaluate device vendors, warranties, and purchasing options

5) OPERATING SYSTEMS: Achievement Standard - Identify, evaluate, select, install, use, upgrade, and customize operating systems. Diagnose and solve problems with various types of operating system utilities.

Level 1-2 Performance Expectations

1. Navigate the basic operating system
2. Manage local and cloud-based files and folders
3. Describe various operating systems, platforms, and utilities (e.g., Android, iPhone system, Chrome, opensource)
4. Describe features of operating systems that can be personalized
5. Differentiate between operating systems and applications

Level 3–4 Performance Expectations

6. Compare and contrast the functions, features, and limitations of different operating systems and utilities (e.g., open-source, mobile, and proprietary operating systems)
7. Select operating systems and utilities appropriate for specific hardware, software, and tasks
8. Install and customize operating systems and utilities
9. Diagnose and repair installation and operational problems of operating systems
10. Identify and use appropriate help resources (e.g., help desks, online help, and manuals) to install, configure, upgrade, diagnose, and repair operating systems and utilities
11. Maintain operating system security
12. Troubleshoot and repair network operating system connectivity
13. Describe the use and benefit of operating systems running in a virtual environment
14. Install operating systems running in a virtual environment
15. Obtain operating system certification(s) needed for a chosen career path

6) INPUT TECHNOLOGIES: Achievement Standard - Use various input technologies to enter and manipulate information appropriately.

Level 1 Performance Expectations

1. Develop and practice proper input techniques (e.g., keyboarding; voice recognition; facial recognition; handwriting recognition; virtual keypad; virtual reality; augmented reality; mixed reality; and the use of a multi-touch screen, mouse/pad, or stylus)
2. Identify appropriate input technology for various tasks
3. Describe ergonomic issues related to input technologies

Level 2–4 Performance Expectations

4. Select appropriate input technology to optimize performance
5. Apply a variety of input technologies to maximize productivity
6. Use a variety of input technologies to optimize academic and workplace performance
7. Create media using a variety of input technologies

7) APPLICATIONS: Achievement Standard - Identify, evaluate, select, install, use, upgrade, troubleshoot, and customize applications.

Level 1 Performance Expectations

1. Identify and use applications appropriate for specific tasks to improve academic achievement across the curriculum
2. Use collaborative application tools to support learning
3. Produce projects that include a variety of media (e.g., images, text, video, web-based tools, and audio)
4. Explore web-based communication applications (e.g., social media, image sharing, video chat, instant messaging)
5. Identify help features and reference materials to learn applications and solve problems

Level 2 Performance Expectations

6. Use help features and reference materials to learn applications
7. Evaluate and select the appropriate applications to productively complete tasks
8. Identify application installation options (local, web based, software as a service [SaaS])
9. Identify and use resources to solve problems using application software
10. Compare and contrast application features
11. Install, upgrade, and customize applications

Level 3-4 Performance Expectations

12. Evaluate providers, licensing, and purchasing options
13. Use the collaborative features of applications to accomplish organizational tasks
14. Apply advanced features of applications for productivity
15. Evaluate the effectiveness of applications to solve specific problems
16. Diagnose and solve problems resulting from an application's installation and use
17. Compare and contrast locally-installed, web-based, mobile app-based, and cloud-based, installations of software applications
18. Use applications to analyze data for making good business decisions
19. Obtain software industry certification(s) needed for a chosen career path
20. Demonstrate the transferability of skills between applications
21. Diagnose and solve application problems
22. Select and integrate productivity software products appropriate for various computer and cloud platforms
23. Identify, evaluate, and select software specific to an organizational function and/or industry
24. Analyze cost benefit and life cycle of applications
25. Create training materials for applications

10) DATABASE MANAGEMENT SYSTEMS: Achievement Standard - Use, plan, develop, and maintain database management systems.

Level 1 Performance Expectations

1. Retrieve and use information from a database
2. Define basic database terminology

Level 2 Performance Expectations

3. Identify the appropriate type of database for a particular situation
4. Identify the variety of data types that are stored in database management systems
5. Create, modify, and extract data from databases for decision making
6. Describe search strategies and use them to solve common information problems
7. Organize and present the results of data retrieval through reports

Level 3 Performance Expectations

8. Identify the concepts and terminology for enterprise-level databases
9. Plan, develop, and implement an enterprise-level database management system
10. Utilize the application development tools from various vendors to interact with a developed enterprise-level database management system
11. Analyze, assess, and troubleshoot enterprise-level database management systems
12. Deploy database development tools to create solutions for reaching organizational goals
13. Obtain database management industry certification(s)

Level 4 Performance Expectations

14. Develop retention schedules that adhere to organizational policies and governmental laws
15. Use data mining techniques to extract useful information
16. Explain the options for converting legacy records to electronic database management systems

11) PROJECT MANAGEMENT AND SYSTEMS ANALYSIS: Achievement Standard - Analyze and design projects and information systems using appropriate management and development tools.

Level 1–2 Performance Expectations

1. Define project management principles
2. Use project management to complete projects across the curriculum
3. Build timelines for projects
4. Apply project management concepts for collaborative works projects
5. Identify the different project management methodologies

Level 3-4 Performance Expectations

6. Identify and explain the steps in the systems development life cycle
7. Identify and describe various structured analysis and design tools
8. Use project management to manage information systems development projects
9. Analyze a current system using structured systems analysis tools
10. Define system requirements using structured systems analysis tools
11. Incorporate appropriate user interface design principles
12. Identify and apply appropriate application development tools
13. Develop a conversion plan
14. Develop design specifications for record types, output, and data stores
15. Create appropriate documentation for information systems
16. Develop a testing plan
17. Develop a training plan
18. Obtain project management industry certification

12) PROGRAMMING AND APPLICATION DEVELOPMENT: Achievement Standard - Design, develop, test, and implement programs and applications.

Level 1-2 Performance Expectations

1. Identify and define programming terminology
2. Demonstrate the ability to code using programming tools

Level 3–4 Performance Expectations

3. Identify and explain programming structures
4. Differentiate between source and object code
5. Choose the appropriate language or application development tool for specific tasks
6. Use scripting languages in application development
7. Apply design principles to programming tasks
8. Develop both procedural and object-oriented programs
9. Select and incorporate appropriate compiler
10. Code common tasks using application development tools
11. Code a program solution in more than one programming language
12. Test, debug, and document code
13. Maintain and modify existing code
14. Develop programs and applications for a variety of platforms
15. Explore the integration of artificial intelligence (AI) in application development
16. Design 3D, augmented reality, and gaming environments in relationship to the development of applications
17. Explore immersive and visualization techniques
18. Obtain programming industry certification(s)

13) DATA AND NETWORKING INFRASTRUCTURES: Achievement Standard - Develop the skills to design, deploy, and administer networks and telecommunications systems.

Level 1–2 Performance Expectations

1. Identify basic network connectivity concepts
2. Apply basic networking terminology to a network environment
3. Explore and explain the benefits of cloud computing
4. Identify and use basic networking resources
5. Recognize the impact of the convergence of communication technologies on networks
6. Configure basic networking devices and security

Level 3 Performance Expectations

7. Identify network connectivity hardware and related software
8. Identify network architecture and topologies
9. Identify and distinguish network protocols, standards, and theoretical models in actual implementations
10. Identify network hardware infrastructure components including networking media and connection hardware and software
11. Design and develop network infrastructure
12. Explore distributed cloud infrastructures
13. Install and configure network servers, routers, clients, and related hardware and software
14. Monitor and manage computer networks
15. Apply virtualization technologies to servers, networks, storage, and related infrastructure
16. Configure and manage network operating systems in multi-vendor environments
17. Implement hardware and software security solutions
18. Monitor and fortify network security
19. Develop enterprise networking solutions
20. Obtain cloud storage, data management, telecommunications or networking industry certification(s)

Level 4 Performance Expectations

21. Implement a distributed storage solution
22. Develop networking strategic plans
23. Develop policies, protocols, and procedures for maintaining enterprise networks

14) INFORMATION TECHNOLOGY PLANNING AND ACQUISITION: Achievement Standard - Plan the selection and acquisition of information technologies.

Level 1-2 Performance Expectations

1. Identify personal technology needs and budget
2. Identify and research reliable sources of information about information technologies
3. Select appropriate information technologies

Level 3-4 Performance Expectations

4. Identify and analyze user needs within an organization
5. Research and identify information technology solutions to meet organizational needs
6. Compare, contrast, and identify potential solutions to meet the needs for an organization
7. Analyze, compare, and contrast total costs of ownership for information technology solutions and the return on investment (ROI)
8. Explore sustainability strategies relative to information technology planning, acquisition, and disposal
9. Develop request for proposals for information systems
10. Evaluate bid specifications received from vendors
11. Identify the importance of inventory management and system life cycles on decision making
12. Develop and present a project plan for identifying, evaluating, selecting, purchasing, installing, and supporting an information system

15) SECURITY AND RISK MANAGEMENT: Achievement Standard - Design and implement security and risk management policies and procedures for information technology.

Level 1–2 Performance Expectations

1. Identify and discuss privacy issues and vulnerabilities relative to the individual and within an organization
2. Implement organizational policies and procedures for security, privacy, and risk management
3. Discuss the risks of data loss and methods of prevention
4. Apply ergonomic techniques to information technology tasks to avoid injury
5. Identify and demonstrate best practices at home and while working (e.g., computers, mobile phones, televisions, tablets)
6. Demonstrate cybersecurity best practices at home and while working with computers, mobile phones, televisions, tablets or other related devices.

Level 3 Performance Expectations

7. Analyze security, privacy, and risk management issues
8. Identify potential risks to enterprise systems from physical or cyber threats
9. Implement configuration management strategies
10. Implement procedures used to recover information from failures and security breaches
11. Implement controls to prevent loss of integrity of data and other information resources

Level 4 Performance Expectations

12. Identify risks to personnel, facilities, data, communications systems, and applications
13. Identify and select controls for personnel, facilities, data, communications systems, and applications appropriate to specific risks
14. Explore the integration of artificial intelligence (AI) in security systems
15. Develop mechanisms to protect an enterprise system from physical and cyber threats
16. Design and implement a security plan for information systems
17. Develop and implement data retention, records management, and destruction schedules
18. Develop and implement disaster prevention and recovery policies and procedures (e.g., Continuity of Operations Plan [COOP])

16) END-USER SUPPORT AND TRAINING: Achievement Standard - Develop the technical and interpersonal skills and knowledge to train and support a diverse user community.

Level 1-2 Performance Expectations

1. Work in a team to solve problems and share knowledge
2. Tutor and support others in information technology skills
3. Develop technical reading skills
4. Develop technical writing, digital communication, and presentation skills to work effectively with global cultures and diverse individuals
5. Develop critical thinking skills to locate resources to solve problems
6. Develop interpersonal skills
7. Use information technologies to facilitate learning
8. Explore online learning opportunities

Level 3 Performance Expectations

9. Demonstrate an inclusive, customer-oriented, service quality approach with users
10. Use a logical and structured approach to isolate, identify, and resolve problems
11. Identify, evaluate, and use resources for problem identification and resolution
12. Explore help-desk resources (e.g., software, videos, support specialists)
13. Develop help-desk procedures
14. Develop traditional and computer-mediated training materials for users
15. Obtain industry certification in one or more information technology areas
16. Explain the need for lifelong learning and professional growth
17. Design a job aid to teach a "how-to"

Level 4 Performance Expectations

18. Train end users to recognize and solve typical information technology problems
19. Identify, evaluate, and select training resources to meet user needs
20. Select appropriate training delivery methods
21. Create learning materials to facilitate user training
22. Plan and create resources to promote lifelong learning
23. Plan, design, deliver, and evaluate traditional and computer-mediated user training solutions

17) INFORMATION TECHNOLOGY AND BUSINESS FUNCTIONS: Achievement Standard - Describe the information technology components of business functions and explain their interrelationships.

Level 3-4 Performance Expectations

1. Identify and examine information systems and their impact on the enterprise (e.g., Enterprise Resource Planning [ERP] systems)
2. Identify and explain the major components of marketing and sales information technologies and their interrelationships
3. Identify and explain the major components of accounting and finance information technologies and their interrelationships
4. Identify and explain the major components of manufacturing and logistics information technologies and their interrelationships
5. Identify and explain the major components of research and development information technologies and their interrelationships
6. Identify and explain the major components of human resource management information technologies and their interrelationships

18) INFORMATION TECHNOLOGY CAREERS: Achievement Standard - Explore career opportunities in information technology.

Level 1-2 Performance Expectations

1. Identify information technologies commonly used in all careers
2. Discuss the impact of information technology on all careers
3. Identify common tasks performed in information technology careers
4. Identify and explore career opportunities in information technology (e.g., LinkedIn, Indeed, etc.)

Level 3-4 Performance Expectations

5. Describe best practices for posting a resume and professional information on job search websites
6. Examine education, experience, skills, and personal requirements for careers in information technology
7. Describe the impact of technological change on information technology positions and the resulting need for lifelong learning
8. Experience an information technology career (e.g., job shadowing, community service, apprenticeship, internship, entry-level job, virtual career exploration)
9. Identify the benefits of industry certifications and higher education for various information

Appendix C: TSA Competition Crosswalk

	Units						
TSA Competition	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Architectural Design				X			
CAD Architecture				X			
CAD Engineering				X			
Chapter Team							X
Coding					X		
Data Science & Analytics						X	
Digital Video Production	X						
Drone Challenge			X				
Engineering Design				X			
Future Technology Teacher							X
Music Production	X						
On Demand Video			X				
Prepared Presentation							X
Promotional Design	X						
Software Development					X		
Structural Design				X			
System Control Technology	X						
Technology Problem Solving			X				
Video Game Design			X				
Virtual Reality Simulation			X				
Webmaster				X			

National TSA Conferences High School Competitive Events

1. **Architectural Design:** In response to the annual design challenge, participants develop a set of architectural plans and related materials, and construct both a physical and computer-generated model to accurately depict their design. Semifinalists deliver a presentation and participate in an interview.
2. **Computer-Aided Design (CAD), Architecture:** Participants use complex computer graphic skills, tools, and processes to respond to a design challenge in which they develop representations of architectural subjects, such as foundation and/or floor plans, and/or elevation drawings, and/or details of architectural ornamentation or cabinetry. The solution to the design challenge and participant answers in an interview are evaluated.
3. **Computer-Aided Design (CAD), Engineering:** Participants use complex computer graphic skills, tools, and processes to respond to a design challenge in which they develop three-dimensional representations of engineering subjects, such as a machine part, tool, device, or manufactured product. The solution to the design challenge and participant answers in an interview are evaluated.
4. **Chapter Team:** Participants take a parliamentary procedure test to qualify for the semifinal round of competition. Semifinalists conduct an opening ceremony, items of business, parliamentary actions, and a closing ceremony.
5. **Coding:** Participants take a test, which concentrates on aspects of coding, to qualify for the semifinal round of competition. Semifinalists develop a software program – in a designated amount of time – that accurately addresses an onsite problem.
6. **Data Science and Analytics:** Participants identify a societal issue, collect or compile data from various sources about the issue, and then produce documentation and a digital scientific poster about their findings. Semifinalists create a synopsis and digital visual representation of a data set provided in an onsite challenge.
7. **Digital Video Production:** Participants develop and submit a digital video and a documentation portfolio (including such items as a storyboard, script, summary of references and sources, and equipment list) that reflects the annual theme. Semifinalists participate in an interview.

8. **Drone Challenge (UAV):** Participants design, build, assemble, document, and test fly an open-source Unmanned Aerial Vehicle (UAV) according to the stated annual theme/problem specifications. The required documentation portfolio must include elements such as a photographic log, wiring schematics, and a description of the programming software used. Semifinalists participate in an interview.
9. **Engineering Design:** Participants develop a solution to an annual theme that is based on a specific challenge noted by the National Academy of Engineering (NAE) in its compilation of the grand challenges for engineering in the 21st century. The solution will include a documentation portfolio, a display, and a model/prototype. Semifinalists deliver a presentation and participate in an interview.
10. **Future Technology Teacher:** Participants research a developing technology, prepare a video showing an application of the technology in the classroom, and create a lesson plan/activity that features the application and connects to the Standards for Technological and Engineering Literacy (STEL), as well as STEM initiatives and integration. Semifinalists demonstrate the lesson plan and answer questions about their presentation.
11. **Music Production:** Participants produce an original musical piece that reflects the annual theme on the TSA website under Themes & Problems. The quality of the musical piece and required documentation (including elements such as a plan of work, self-evaluation, and a list of hardware, software, and instruments used) determines advancement to the semifinal level of competition, during which semifinalist participants are interviewed.
12. **On Demand Video:** Once participants receive the challenge details (required criteria, such as props and a line of dialogue) at the national TSA conference, they have 36 hours to produce a 60-second film that showcases video skills, tools, and communication processes. The quality of the completed video production determines the finalists.
13. **Prepared Presentation:** Participants deliver a three-to-five-minute oral presentation related to the current national TSA conference theme. Both semifinalists and finalists are determined based on the quality of the presentation and the appropriate use and content of the accompanying required slide deck.
14. **Promotional Design:** Participants use computerized graphic communications layout and design skills to produce a promotional resource packet. The resource must address the annual theme/problem and include at least four printed publication items and required documentation. Semifinalists demonstrate publishing competency in an onsite technical design challenge.
15. **Software Development:** Participants use their knowledge of cutting-edge technologies, algorithm design, problem-solving principles, effective communication, and collaboration to design, implement, test, document, and present a software development project of educational or social value. Both semifinalists and finalists are determined based on the quality of the presentation and project.
16. **Structural Design and Engineering:** Participants apply the principles of structural engineering to design and construct a structure that complies with the annual challenge. An assessment of the required documentation and the destructive testing of the structure (to determine its design efficiency) determine both semifinalists and finalists.
17. **System Control Technology:** Participants develop a solution to a problem (typically one from an industrial setting) presented onsite at the conference. They analyze the problem, build a computer-controlled mechanical model, program the model, demonstrate the programming and mechanical features of the model-solution in an interview, and provide instructions for evaluators to operate the model.
18. **Technology Problem Solving:** Participants use problem-solving skills to design and construct a finite solution to a challenge provided onsite at the conference. Solutions are evaluated at the end of 90 minutes using measures appropriate to the challenge, such as elapsed time, horizontal or vertical distance, and/or strength.
19. **Video Game Design:** Participants design, build, and launch an E-rated online video game – with accompanying required documentation - that addresses the annual theme. Semifinalists participate in an interview to demonstrate the knowledge and expertise they gained during the development of the game.
20. **Virtual Reality Simulation (VR):** Participants use video and 3D computer graphics tools and design processes to create a two-to-three-minute VR visualization (accompanied by supporting documentation) that addresses the annual theme. Semifinalists deliver a presentation about their visualization and participate in an interview.
21. **Webmaster:** Participants design, build, and launch a website that addresses the annual challenge. Semifinalists participate in an interview to demonstrate the knowledge and expertise gained during the development of the website.

Appendix D: SkillsUSA Competition Crosswalk

	Units						
SkillsUSA Competitions	**1**	**2**	**3**	**4**	**5**	**6**	**7**
3D Visualization and Animation	X						
Advertising Design			X				X
Architectural Drafting				X		X	
Career Pathways – Business Management and Technology						X	X
Career Pathways Industrial and Engineering Technology				X	X		
Chapter Business Procedure						X	X
Commercial SUAS Drone			X	X			
Computer Programming			X		X		
Crime Scene Investigation			X		X		
Customer Service							X
Cyber Security		X	X		X		X
Employment Application Process							X
Engineering Technology Design	X			X			
Entrepreneurship							X
Extemporaneous Speaking	X						X
Information Technology Services				X	X	X	
Interactive Application and Video Game Development	X		X				
IoT Smart Home			X	X			
Internetworking				X	X		
Job Interview							X
Mobile Robotics Technology			X		X		
Prepared Speech	X						X
Principles of Engineering - Technology	X			X			
Quiz Bowl	X	X	X	X	X	X	X
Related Technical Math		X			X		
Robotics and Automation Technology	X		X		X		
Technical Computer Applications				X		X	
Technical Drafting				X		X	
Telecommunications Cabling				X	X		
Video Production	X						X
Web Design & Development			X		X		

National SkillsUSA Conferences High School Competitive Events

1. **3D Visualization and Animation:** The world of 3D is rapidly expanding, and career opportunities exist in a wide range of fields, including architecture, games, product and industrial design, civil engineering, and film and television animation. This competition allows students to step into a real-world 3D production environment where creative output must be accomplished within specific timeframes, resources, and design constraints. This is a two-person team event and includes a written exam. Competitors must produce high quality images and an animated short subject using computer-generated 3D images. Students are evaluated on their technical knowledge, production skills, and creative abilities, including visual development and storyboarding. Competitors can also interface with and get feedback from judges with successful careers in 3D visualization and animation.
2. **Advertising Design:** This competition tests technical skills and creative aptitude as though competitors worked for an advertising agency. In addition to a written test, competitors will recreate a provided advertisement on a computer. Competitors are judged on their accuracy, proficiency with industry software, and ability to meet a deadline. The competition also includes a creative portion. The creative portion involves the application of creative thinking and a design challenge. Layout, drawing, and illustration skills are used, as well as the ability to create vibrant, effective designs using a computer.

3. **Architectural Drafting:** Competitors will use their drafting skills to solve an architectural problem. The competition includes a written test, a hand sketch, and drawings that are either computer-generated or board drafted. The competition evaluates the competitors' problem-solving abilities, not simply CAD skills.
4. **Career Pathways – Business Management and Technology:** Student teams use their course of study as the basis of a project that will benefit their class, school, community or industry. The project must highlight an aspect of their Career Cluster training. Upon completion of the project, the students will develop a display and use it within the community to explain their training and project. This competition will judge mastery of their training, its application, the project's benefit to their community, and display and presentation techniques. Teams must be entered in the appropriate Career Pathways - Business Management and Technology based on the course enrollment of the students (not on the content of the project). The following career clusters are represented in this competition: Business Management and Administration; Finance; Information Technology; and Marketing.
5. **Career Pathways Industrial and Engineering Technology**: Student teams use their course of study as the basis of a project that will benefit their class, school, community or industry. The project must highlight an aspect of their Career Cluster training. Upon completion of the project, the students will develop a display and use it within the community to explain their training and project. This competition will judge mastery of their training, its application, the project's benefit to their community, and display and presentation techniques. Teams must be entered in the appropriate Career Pathways - Industrial and Engineering Technology based on the course enrollment of the students (not on the content of the project). The following career clusters are represented in this competition: Architecture and Construction; Manufacturing; Science, Technology, Engineering, and Mathematics; and Transportation Distribution and Logistics.
6. **Chapter Business Procedure:** Student teams demonstrate knowledge of parliamentary procedure in both a written exam and a team demonstration. The written exam covers questions related to materials found in Robert's Rules of Order—Newly Revised. During the presentation, the team will demonstrate the running of a typical business meeting using a standard order of business. During the presentation, the team must properly insert into the order of business the secretary's minutes, treasurer's report and business items identified by the technical committee. In addition to the debate and transaction of the business items, teams will also properly demonstrate different parliamentary procedure motions, including at least one of each of the following: main, privileged, subsidiary, incidental and motions that bring back issues to the floor. Minutes of the demonstration will be read by the secretary upon completion of the demonstration.
7. **Commercial sUAS Drone:** (Team of 2) This competition is designed to evaluate team members' skills and preparation for employment in multiple career fields related to the safe and efficient use of drone technology in the National Airspace System and to recognize outstanding performance by participants in real-world, scenario-based situations.
8. **Computer Programming:** Competitors demonstrate knowledge of computer programming, describe how programs and programming languages work, and describe the purposes and practices of structured programming. The competition may include a computer programming problem consisting of background information and program specifications. An appropriate (successfully executable) computer program from design notes and instructions will be developed.
9. **Crime Scene Investigation:** "Contestants will demonstrate basic skills associated with working a crime scene. Team members will take a test assessing overall crime scene knowledge. Team members will process a crime scene to include searching, identifying evidence, measuring, photographing, and preparing a sketch. Team members will also demonstrate basic crime scene skills such as lifting a fingerprint, swabbing serological evidence, packaging evidence, or similar skills. The team will interpret common crime scene evidence such as classifying a fingerprint pattern. Finally, the team will complete narratives, crime logs, and similar paperwork."
10. **Customer Service:** The competition evaluates students' proficiency in providing customer service. The competition involves live role-playing situations. Competitors demonstrate their ability to perform customer service in both written and oral forms including telephone and computer skills, communications, problem solving, conflict resolution, and business etiquette.
11. **Cyber Security:** The competition is open to active SkillsUSA members enrolled in programs with Cyber Security, Information Security, or Systems and Networking Security Architecture as occupational objectives. Students will be tested on the elements of the NIST Publication 800-181 Cybersecurity Workforce Framework categories including Securely Provision, Operate and Maintain, and Protect and Defend. This competition's skill performance stations are created to be part of a "scouting combine" where teams will demonstrate a wide range of skillsets needed in Cyber Security industry. This scouting combine will assess a team's knowledge and skills in a series of individual stations that will be totaled to determine the team's overall score.
12. **Employment Application Process:** This competition tests the competitor's readiness in applying for employment and their understanding of the process. The competition includes completing an application and interviewing with the judges. Their resume and portfolio are used during their interviews. The competition is available to students who are classified under the provisions of Public Law 105-17, Individuals with Disabilities Education Act, 1997.
13. **Engineering Technology – Design (includes Middle School):** (Team of 3) Students demonstrate their ability to design an innovative engineering project and present those ideas along with a display and live model. During the presentation,

students are judged on their performance as a professional team, presentation of their project to a panel of judges from the engineering field, their storyboard presentation model, and the overall effect of the presentation.

14. **Entrepreneurship:** A team event testing students' knowledge in starting their own businesses by developing business plans that identify needed products or services in a local market. Emphasis is placed on financial planning and practicality of the product/service. Teams give oral presentations based upon their written plans, and the team must successfully answer judges' questions in response to typical problems encountered by entrepreneurs during their first year of business.
15. **Extemporaneous Speaking (includes Middle School):** The competition requires competitors to give a three- to five-minute speech on an assigned topic with five minutes of advance preparation. Competitors enter the preparation area one at a time, where they are given a speech topic. They are judged on voice, mechanics, platform deportment, organization, and effectiveness.
16. **Information Technology Services:** Competitors demonstrate their skills with hands-on modules designed to test their knowledge as an IT service professional. The competition challenges competitors to correct end-user computing issues, configure and secure networks, manage virtual machines, navigate and modify operating system internals, deploy operating systems, leverage troubleshooting software and tools, identify virus and malware origins, work with mobile devices, and proficiently use command line interfaces. The operating systems used in the competition include Windows, Macintosh, and Linux. Additionally, competitors are evaluated on their interpersonal skills (such as communication, teamwork, and professionalism). Competitors will take a written exam which is aligned with CompTIA A+; the industry standard certification for Information Technology.
17. **Interactive Application and Video Game Development:** The competition is a two-person team event that tests technical knowledge and production skills, including critical thinking, creative problem solving, teamwork, interpersonal and visual communication, artistic design, and technical programming. Teams must produce an original prototype or sample of an interactive application or video game with at least one level and ten (10) minutes of interactive content. It must be created during the school year immediately preceding the competition deadline.
18. **Internetworking:** The competition tests the networking knowledge and hands-on ability of the competitors. The online written portion tests the student's complete knowledge of internetworking concepts. The hands-on component demonstrates the abilities of the competitor to make cables, troubleshoot network systems, configure routers, switches and servers, and to deliver customer service in a technical assistant center environment. The competitors will find errors in WAN and LAN networks; do a full network configuration using routers, switches, and servers; talk a technician through an error they are having on their network; and take an online certification-type test. The national competition is based on the most current CCNA certification. In today's job market system administration skills are needed, therefore server skills that will be scored include, but are not limited to DNS, Active Directory, and DHCP.
19. **Internet of Things (IOT) Smart Home:** The competition tests each competitor's preparation for employment and recognizes outstanding students for excellence and professionalism in the field of home technology integration. The competitors will complete both a written test and hands on demonstration of the installation of "smart home" residential products including bulbs; thermostats; locks; alarms; sensors; cameras; speakers; home theater systems; computer networking; and video security equipment. Construction of the various interconnecting cables such as cat 6/networking cables, coax cables and low and high voltage residential wiring will also be necessary. The competition will challenge competitors to configure and secure networks, update firmware/software and configure operating system settings. Troubleshooting skills will also be tested. Finally, the competition requires a demonstration of all hardware software set up, completed in an easy-to-understand manner fit for the typical customer.
20. **Job Interview:** Competitors are evaluated on their understanding of employment procedures faced in applying for positions in the occupational areas in which they are training. The competition is divided into phases, including the following: completion of employment application; introduction scenario with a receptionist; and an in-depth interview(s).
21. **Mobile Robotics Technology (includes Middle School):** (Team of 2) The competition includes activities that simulate situations encountered by robotic programmers and support professionals. Teams are given a task to solve using a mobile robotic system that is built ahead of time and brought to the competition. Teams will have two scored chances to solve the mobile robotic challenge and will be given a design and programming interview. Once a team has performed the required task or set of tasks, a design change may be introduced. Competitors are required to adhere to industry safety standards using the hardware and software they have selected.
22. **Prepared Speech (includes Middle School):** The competition requires students to deliver a five- to seven-minute prepared speech based on the annual SkillsUSA competition theme. Competitors are evaluated on their ability to present thoughts relating to the central theme clearly and effectively, and are rated on voice, mechanics and platform deportment.
23. **Principles of Engineering – Technology:** The competition evaluates competitors' understanding of basic technical concepts and principles of the applied sciences and their ability to demonstrate and explain the concept/principle in

action and application. Any technical concept may be demonstrated, provided it is related to the principles of technology or engineering curriculum and incorporates basic principles of the applied sciences.

24. **Quiz Bowl:** The Quiz Bowl competition tests a team of five to seven competitors on their ability to quickly respond to knowledge questions covering academics, current events
25. **Related Technical Math:** Through a written test, competitors demonstrate the skills required to solve mathematical problems correctly that are commonly found in the skilled trades and professional and technical occupations. Skills demonstrated include addition; subtraction; multiplication; division of whole numbers; fractions and decimals; applied word problems; percentages; ratio proportions; averages; area; volume; metric measures; and traditional (Imperial) measures and trigonometry.
26. **Robotics and Automation Technology:** In this competition, two-person teams will showcase their skills in designing and implementing an automated robotic work cell. Each team will be presented with a simulated task and accompanying wiring schematics. Using industry-standard best practices, participants must integrate a 6-axis industrial robot with a range of peripherals, including Programmable Logic Controllers (PLCs), motorized components, sensors, and machine vision systems. Teams are required to document their approach, configure and program the work cell, and present their solution to a panel of judges. Performance is evaluated based on technical accuracy, operational efficiency, speed, and collaboration.
27. **Technical Computer Applications:** Competitors will demonstrate installation, configuration and use of Windows, Mac OSX and Linux Professional Operating Systems and one or more integrated office suite packages including email, word processing, spreadsheet applications, database applications, web page development, money management applications, presentations applications, internet browser applications, etc. The use of open-source software such as OpenOffice is preferable. Microsoft Office and other integrated office suites can be used. The utilization of instant messaging, collaboration and social networking software will be required during the contest. Competitors are expected to perform in teams while demonstrating individual technical skills. The competition includes an oral presentation demonstrating the student's ability to communicate with others, a hands-on skills demonstration and a written examination.
28. **Technical Drafting:** The competition evaluates a competitor's preparation for employment and recognizes outstanding students for excellence and professionalism in the field of technical drafting. The competition will focus on the solution of industry-developed problems by applying appropriate technical drafting skills and tools including computer-aided drafting (CAD).
29. **Telecommunications Cabling:** This competition is intended for students interested in voice and data network cabling and installation. Industry indicates that 80% of the problems in networking, security systems installations and other installations are caused by cabling and connectivity issues, not the computers, servers, switches, etc. This competition tests students' knowledge of worldwide industry standards related to cabling and connectorization, which involves attaching physical connectors to the ends of cables, fibers, or other components, for data and voice connections, physical and logical networks and signal transmission. Competitors demonstrate skills in fiber and copper cable termination, pulling and mounting cabling, patch panel installation and termination, installing jacks, cable and fiber optic testing and troubleshooting, and providing customer service. The competition stresses safety in all activities.
30. **Video Production:** (Team of 2) Competitors are required to plan and shoot a video (generally 30 seconds or one minute in length) on location to convey the theme of the event. Editing is done in the competition area with special emphasis on professional production of the video by industry standards, quality of audio and video and adequate conveyance of the theme to the viewer of the final piece.
31. **Web Design and Development:** (Team of 2) Teams complete a series of challenges focusing on creating a website for a client and a specific target audience. Judging will focus on meeting the client's needs, usability and accessibility, and industry-standard best practices. Teams will also be evaluated on the process they use to meet the challenges and how well they work as a team. Teams will need Internet access as all competition materials (including the coding environment) will only be available online.

Appendix E: ISTE Student Standards

	Units						
Standards	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1.1	X		X	X			
1.2	X	X					
1.3	X	X	X				
1.4	X		X				
1.6	X	X		X	X	X	X
1.7	X			X	X	X	X

ISTE Standards: For Students: 2024 (v02)

SECTION 1: STUDENTS

1.1 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.

Students:

1. Connect their learning needs, strengths and interests to their goals and use technology to help achieve them and reflect on their progress.
2. Build networks and customize their learning environments in ways that support the learning process.
3. Use technology to seek feedback that informs and improves their practice and to demonstrate their learning in a variety of ways.
4. Understand fundamental concepts of how technology works, demonstrate the ability to choose and use current technologies effectively, and are adept at thoughtfully exploring emerging technologies.

1.2 Digital Citizen

Students recognize the responsibilities and opportunities for contributing to their digital communities.

Students:

1. Manage their digital identity and understand the lasting impact of their online behaviors on themselves and others and make safe, legal and ethical decisions in the digital world.
2. Demonstrate empathetic, inclusive interactions online and use technology to responsibly contribute to their communities.
3. Safeguard their well-being by being intentional about what they do online and how much time they spend online.
4. Take action to protect their digital privacy on devices and manage their personal data and security while online.

1.3 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. Students:

1. Use effective research strategies to find resources that support their learning needs, personal interests, and creative pursuits.
2. Evaluate the accuracy, validity, bias, origin, and relevance of digital content.
3. Curate information from digital resources using a variety of tools and methods to create collections of artifacts that demonstrate meaningful connections or conclusions.
4. Build knowledge by exploring real-world issues and gain experience in applying their learning in authentic settings.

1.4 Innovative Designer

Students use a variety of technologies within a design process to identify and solve problems by creating new, useful, or imaginative solutions. Students:

1. Know and use a deliberate design process for generating ideas, testing theories, creating innovative artifacts, or solving authentic problems.
2. Select and use digital tools to plan and manage a design process that considers design constraints and calculated risks.
3. Develop, test and refine prototypes as part of a cyclical design process.
4. Exhibit a tolerance for ambiguity, perseverance, and the capacity to work with open-ended problems.

1.5 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. Students:

1. Formulate problem definitions suited for technology assisted methods such as data analysis, abstract models, and algorithmic thinking in exploring and finding solutions.
2. 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.
3. Break problems into component parts, extract key information, and develop descriptive models to understand complex systems or facilitate problem-solving.
4. Understand how automation works and use algorithmic thinking to develop a sequence of steps to create and test automated solutions.

1.6 Creative Communicator

Students communicate clearly and express themselves creatively for a variety of purposes using the platforms, tools, styles, formats and digital media appropriate to their goals. Students:

1. Choose the appropriate platforms and digital tools for meeting the desired objectives of their creation or communication.
2. Create original works or responsibly repurpose or remix digital resources into new creations.
3. Use digital tools to visually communicate complex ideas to others.
4. Publish or present content that customizes the message and medium for their intended audiences.

1.7 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. Students:

1. Use digital tools to connect with peers from a variety of backgrounds recognizing diverse viewpoints and broadening mutual understanding.
2. Use collaborative technologies to work with others, including peers, experts, or community members, to examine issues and problems from multiple viewpoints.
3. Contribute constructively to project teams, assuming various roles and responsibilities to work effectively toward a common goal.
4. Explore local and global issues and use collaborative technologies to work with others to investigate solutions.

Appendix F: CompTIA Cyber Defense Pro

	Units						
Standards	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1.1	X						
2.1		X				X	
2.2		X				X	
2.3		X			X	X	
2.4			X		X		
2.5					X		
2.6			X		X		
3.1			X				
3.2			X				
3.3			X				
3.4			X		X		
4.1		X		X	X		
4.2				X	X		
4.3		X		X	X		
4.4		X		X	X		
4.5				X	X		
5.1			X		X		
5.2			X		X		
6.1			X		X		
6.2			X		X		
6.3			X		X		
6.4			X		X		
6.5			X		X		
6.6			X		X		
6.7			X		X		
6.8			X		X		
7.1			X		X		
7.2					X	X	
7.3					X	X	
7.4			X	X			
7.5			X	X			
7.6			X	X			
7.7			X	X			
8.1					X		
8.2					X		
8.3					X		
9.1					X		
9.2					X		
9.3					X		

CompTIA Cyber Defense Pro – Standards

1.0 Introduction

1. Introduction to TestOut CyberDefense Pro

2.0 Vulnerability Response, Handling, and Management

1. Regulations and Standards

2. Risk Management
3. Security Controls
4. Attack Surfaces
5. Patch Management
6. Security Testing

3.0 Threat Intelligence and Treat Hunting

1. Threat Actors
2. Threat Intelligence
3. Threat Hunting
4. Honeypots

4.0 System and Network Architecture

1. Operating System Concepts
2. Network Architecture
3. Identity and Access Management (IAM)
4. Protection
5. Logging

5.0 Vulnerability Assessment

1. Reconnaissance
2. Scanning
3. Enumeration
4. Vulnerability Assessments
5. Vulnerability Scoring Systems
6. Classifying Vulnerability Information

6.0 Network Security

1. Network Security
2. Security Monitoring
3. Wireless Security
4. Web Server Security
5. SQL Injection
6. Sniffing
7. Authentication Attacks
8. Cloud Security
9. Email Security
10. Denial-of-Service Attacks
11. Industrial Computer Systems

7.0 Host-Based Attacks

1. Device Security
2. Unauthorized Changes
3. Malware
4. Command and Control
5. Social Engineering
6. Scripting and Programming
7. Application Vulnerability

8.0 Security Management

1. Security Information and Event Management (SIEM)
2. Security Orchestration, Automation, and Response (SOAR)
3. Exploring Abnormal Activity

9.0 Post-Attack

1. Containment
2. Incident Response
3. Post-Incident Activities

Appendix G: CompTIA Security+ CertMaster Learn

	Units						
Standards	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1		X					
2			X				
3			X				
4		X					
5				X			
6				X			
7					X		
8					X		
9					X		
10					X		
11					X		
12					X		
13			X				
14						X	
15						X	
16						X	

CompTIA Security+ CertMaster Learn – Standards

1.0 Summarize Fundamental Security Concepts
1. Security Concepts
2. Security Controls

2.0 Compare Threat Types
1. Threat Actors
2. Attack Surfaces
3. Social Engineering

3.0 Explain Cryptographic Solutions
1. Cryptographic Algorithms
2. Public Key Infrastructure
3. Cryptographic Solutions

4.0 Implement Identity and Access Management
1. Authentication
2. Authorization
3. Identity Management

5.0 Secure Enterprise Network Architecture
1. Enterprise Network Architecture
2. Network Security Appliances
3. Secure Communications

6.0 Secure Cloud Network Architecture
1. Cloud Infrastructure
2. Embedded Systems and Zero Trust Architecture

7.0 Explain Resiliency and Site Security Concepts
1. Asset Management
2. Redundancy Strategies
3. Physical Security

8.0 Explain Vulnerability Management
1. Device and OS Vulnerabilities
2. Application and Cloud Vulnerabilities

3. Vulnerabilities Identification Methods
4. Vulnerabilities Analysis and Remediation

9.0 Evaluate Network Security Capabilities

1. Network Security Baselines
2. Network Security Capabilities Enhancement

10.0 Assess Endpoint Security Capabilities

1. Implement Endpoint Security
2. Mobile Device Hardening

11.0 Enhance Application Security Capabilities

1. Application Protocol Security Baselines
2. Cloud and Web Application Security Concepts

12.0 Explain Incident Response and Monitoring Concepts

1. Incident Response
2. Digital Forensics
3. Data Sources
4. Alerting and Monitoring Tools

13.0 Analyze Indicators of Malicious Activity

1. Malware Attack Indicators
2. Physical and Network Attacks Indicators
3. Application Attack Indicators

14.0 Summarize Security Governance Concepts

1. Policies, Standards, and Procedures
2. Change Management
3. Automation and Orchestration

15.0 Explain Risk Management Processes

1. Risk Management Processes and Concepts
2. Vendor Management Concepts
3. Audits and Assessments

16.0 Summarize Date Protection and Compliance Concepts

1. Data Classification and Compliance
2. Personnel Policies