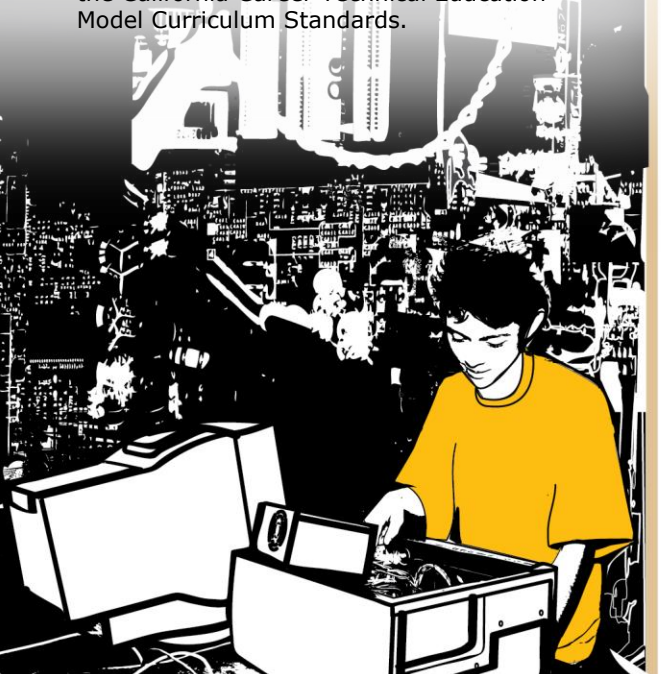
Course Outline

Information and Communication Technologies **REVISED June/2019**

Course Description:

This competency-based course provides a solid foundation in cybersecurity concepts, practices, functions, and applications. The course maps to the Computing Technology Industry Association's (CompTIA) Security+ examination. Technical instruction includes an introduction and covers basic networking security, threats and vulnerabilities, compliance and operation security principles, basic cryptograph, as well as application, data and host security, identity management. Emphasis is on preparing the student for the CompTIA Security+ SY0-501 Exam. The Security+ certification is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. The CompTIA Security+ course prepares candidates to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. The successful candidate will perform these tasks to support the principles of confidentiality, integrity, and availability. The competencies in this course are aligned with the California High School Academic Content Standards and the California Career Technical Education Model Curriculum Standards.



Job Title: Information Security Analyst

Career Pathway: Networking

Industry Sector: Information and Communication Technologies

O*NET-SOC CODE: 15-1122.00

CBEDS Title: Network Security

CBEDS No.: 4646

77-65-90

CompTIA Security +

Credits: 10 **Hours:** 120

Prerequisites:
Enrollment requires a 6.0 reading level as measured by the CASAS GOALS test, successful completion (or equivalent) of one of the Computer Operation courses (75-35-85, 75-45-50, 75-45-60, 75-45-70), and successful completion (or demonstrate competency) of Algebra I.

NOTE: For Perkins purposes this course has been designated as a **capstone** course.

This course **cannot** be repeated once a student receives a Certificate of Completion.

Los Angeles Unified School District
Division of Adult and Career Education
Instructional and Couseling Services Unit
Adult Curriculum Office
www.wearedace.org

COURSE OUTLINE COMPETENCY-BASED COMPONENTS

A course outline reflects the essential intent and content of the course described. Acceptable course outlines have six components. (Education Code Section 52506). Course outlines for all apportionment classes, including those in jails, state hospitals, and convalescent hospitals, contain the six required elements:

(EC 52504; 5CCR 10508 [b]; Adult Education Handbook for California [1977], Section 100)

COURSE OUTLINE COMPONENTS	**LOCATION**
GOALS AND PURPOSES	Cover
The educational goals or purposes of every course are clearly stated and the class periods are devoted to instruction. The course should be broad enough in scope and should have sufficient educational worth to justify the expenditure of public funds.	
The goals and purpose of a course are stated in the COURSE DESCRIPTION. Course descriptions state the major emphasis and content of a course, and are written to be understandable by a prospective student.	
PERFORMANCE OBJECTIVES OR COMPETENCIES	pp. 6-27
Objectives should be delineated and described in terms of measurable results for the student and include the possible ways in which the objectives contribute to the student's acquisition of skills and competencies.	
Performance Objectives are sequentially listed in the COMPETENCY-BASED COMPONENTS section of the course outline. Competency Areas are units of instruction based on related competencies. Competency Statements are competency area goals that together define the framework and purpose of a course. Competencies fall on a continuum between goals and performance objectives and denote the outcome of instruction.	
Competency-based instruction tells a student before instruction what skills or knowledge they will demonstrate after instruction. Competency-based education provides instruction which enables each student to attain individual goals as measured against pre-stated standards.	
Competency-based instruction provides immediate and continual repetition and in competency-based education the curriculum, instruction, and assessment share common characteristics based on clearly stated competencies. Curriculum, instruction and assessment in competency-based education are: explicit, known, agreed upon, integrated, performance oriented, and adaptive.	

COURSE OUTLINE COMPETENCY-BASED COMPONENTS (continued)

COURSE OUTLINE COMPONENTS	LOCATION
INSTRUCTIONAL STRATEGIES	p. 29
Instructional techniques or methods could include laboratory techniques, lecture method, small-group discussion, grouping plans, and other strategies used in the classroom. Instructional strategies for this course are listed in the TEACHING STRATEGIES AND EVALUATION section of the course outline. Instructional strategies and activities for a course should be selected so that the overall teaching approach takes into account the instructional standards of a particular program, i.e., English as a Second Language, Programs for Adults with Disabilities.	
UNITS OF STUDY, WITH APPROXIMATE HOURS ALLOTTED FOR EACH UNIT	Cover
The approximate time devoted to each instructional unit within the course, as well as the total hours for the course, is indicated. The time in class is consistent with the needs of the student, and the length of the class should be that it ensures the student will learn at an optimum level. Units of study, with approximate hours allotted for each unit are listed in the COMPETENCY AREA STATEMENT(S) of the course outline. The total hours of the course, including work-based learning hours (community classroom and cooperative vocational education) is listed on the cover of every CBE course outline. Each Competency Area listed within a CBE outline is assigned hours of instruction per unit.	pp. 6-29
EVALUATION PROCEDURES	p. 29
The evaluation describes measurable evaluation criteria clearly within the reach of the student. The evaluation indicates anticipated improvement in performances as well as anticipated skills and competencies to be achieved. Evaluation procedures are detailed in the TEACHING STRATEGIES AND EVALUATION section of the course outline. Instructors monitor students' progress on a continuing basis, assessing students on attainment of objectives identified in the course outline through a variety of formal and informal tests (applied performance procedures, observations, and simulations), paper and pencil exams, and standardized tests.	
REPETITION POLICY THAT PREVENTS PERPETUATION OF STUDENT ENROLLMENT	Cover
After a student has completed all the objectives of the course, he or she should not be allowed to reenroll in the course. There is, therefore, a need for a statement about the conditions for possible repetition of a course to prevent perpetuation of students in a particular program for an indefinite period of time.	

ACKNOWLEDGMENTS

Thanks to ROBERT YORGASON and ALEJANDRA SALCEDO for developing and editing this curriculum. Acknowledgment is also given to ERICA ROSARIO for designing the original artwork for the course covers.

ANA MARTINEZ
Specialist
Career Technical Education

ROSARIO GALVAN
Administrator
Division of Adult and Career Education

APPROVED:

JOSEPH STARK
Executive Director
Division of Adult and Career Education

CALIFORNIA CAREER TECHNICAL EDUCATION MODEL CURRICULUM STANDARDS
Information and Communications Technologies Industry Sector
Knowledge and Performance Anchor Standards

1.0 Academics
Analyze and apply appropriate academic standards required for successful industry sector pathway completion leading to postsecondary education and employment. Refer to the Information and Communication Technologies academic alignment matrix for identification of standards.

2.0 Communications
Acquire and accurately use Information and Communication Technologies sector terminology and protocols at the career and college readiness level for communicating effectively in oral, written, and multimedia formats.

3.0 Career Planning and Management
Integrate multiple sources of career information from diverse formats to make informed career decisions, solve problems, and manage personal career plans.

4.0 Technology
Use existing and emerging technology, to investigate, research, and produce products and services, including new information, as required in the Information and Communication Technologies sector workplace environment.

5.0 Problem Solving and Critical Thinking
Conduct short, as well as more sustained, research to create alternative solutions to answer a question or solve a problem unique to the Information and Communication Technologies sector using critical and creative thinking, logical reasoning, analysis, inquiry, and problem-solving techniques.

6.0 Health and Safety
Demonstrate health and safety procedures, regulations, and personal health practices and determine the meaning of symbols, key terms, and domain-specific words and phrases as related to the Information and Communication Technologies sector workplace environment.

7.0 Responsibility and Flexibility
Initiate, and participate in, a range of collaborations demonstrating behaviors that reflect personal and professional responsibility, flexibility, and respect in the Information and Communication Technologies sector workplace environment and community settings.

8.0 Ethics and Legal Responsibilities
Practice professional, ethical, and legal behavior, responding thoughtfully to diverse perspectives and resolving contradictions when possible, consistent with applicable laws, regulations, and organizational norms.

9.0 Leadership and Teamwork
Work with peers to promote divergent and creative perspectives, effective leadership, group dynamics, team and individual decision making, benefits of workforce diversity, and conflict resolution such as those practiced in the Future Business Leaders of America and SkillsUSA career technical student organization.

10.0 Technical Knowledge and Skills
Apply essential technical knowledge and skills common to all pathways in the Information and Communication Technologies sector, following procedures when carrying out experiments or performing technical tasks.

11.0 Demonstration and Application
Demonstrate and apply the knowledge and skills contained in the Information and Communication Technologies anchor standards, pathway standards, and performance indicators in classroom, laboratory, and workplace settings, and through career technical student organizations such as Future Business Leaders of America and SkillsUSA.

B. Networking Pathway
The Ornamental Horticulture pathway prepares students for careers in the nursery, landscaping, and floral industries. Topics include plant identification, plant physiology, soil science, plant reproduction, nursery production, and floriculture, as well as landscaping design, installation, and maintenance.

Sample occupations associated with this pathway:
- Computer Security Specialist
- Network Technician
- Network Engineer
- Network Administrator
- Telecommunication Specialist

B1.0 Identify, and describe the principles of networking and the technologies, models, and protocols used in a network.

B2.0 Identify, describe, and implement network media and physical topologies.

B3.0 Install, configure, and differentiate between common network devices.

B4.0 Demonstrate proper network administration and management skills.

B5.0 Demonstrate how to communicate and interpret information clearly in industry-standard visual and written formats.

B6.0 Use and assess network communication applications and infrastructure.

B7.0 Analyze a customer's organizational needs and requirements to identify networking needs.

B8.0 Identify security threats to a network and describe general methods to mitigate those threats.

COMPETENCY-BASED COMPONENTS for the CompTIA Security+ Course

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
A. ORIENTATION AND SAFETY Understand, apply, and evaluate classroom and workplace policies and procedures used in accordance with federal, state, and local safety and environmental regulations. (5 hours)	1. Identify the scope and purpose of the course. 2. Describe qualifications and prerequisites for employment in the Cybersecurity field. 3. Describe the CompTIA Security+ Exam. 4. Describe classroom policies and procedures. 5. Describe the different occupations in the Information and Communication Technologies (ITC) industry sector. 6. Describe the opportunities available for promoting gender equity and the representation of non-traditional populations in computer technology. 7. Pass the safety exam with 100% accuracy.	**Career Ready Practice:** 1, 2, 4, 7, 8, 12 **CTE Anchor:** Communications: 2.5, 2.6 Technology: 4.1, 4.2, 4.4, 4.5 Problem Solving and Critical Thinking: 5.3, 5.4, 5.5, 5.6, 5.11, 5.12 Ethics and Legal Responsibilities: 8.3, 8.6, 8.8 Technical Knowledge and Skills: 10.1, 10.5, 10.11 **CTE Pathway:** B1.1, B1.3, B1.5, B1.6, B2.1, B3.1, B3.3, B5.1, B8.4
B. THREATS, ATTACKS, AND VULERNABILITIES Understand and identify threats, compare and contrast cyber-attacks, explain and evaluate security vulnerabilities.	1. Analyze indicators of a compromised system and determine the type of malware. a) Viruses b) Crypto-malware c) Ransomware d) Worm e) Trojan f) Rootkit g) Keylogger h) Adware i) Spyware j) Bots k) RAT l) Logic bomb	**Career Ready Practice:** 1, 2, 8, 12 **CTE Anchor:** Communications: 2.5, 2.6 Technology: 4.1, 4.2, 4.4, 4.5 Problem Solving and Critical Thinking: 5.3, 5.4, 5.5, 5.6, 5.11, 5.12

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	m) Backdoor 2. Compare and contrast types of cyber-attacks a) Describe social engineering attacks i) Phishing ii) Spear phishing iii) Whaling iv) Vishing v) Tailgating vi) Impersonation vii) Dumpster diving viii) Shoulder surfing ix) Hoax x) Watering hole attack xi) Evaluate reasons for effectiveness (1) Authority (2) Intimidation (3) Consensus (4) Scarcity (5) Familiarity (6) Trust (7) Urgency b) Describe application and service attacks i) Denial of Service (DoS) ii) Distributed Denial of Service (DDoS) iii) Man-in-the-middle (MITM) iv) Buffer overflow v) Injection vi) Cross-site scripting vii) Cross-site request forgery Privilege escalation viii) Address Resolution Protocol (ARP) poisoning ix) Amplification x) Domain Name Service (DNS) poisoning xi) Domain hijacking xii) Man-in-the-browser (MITB) xiii) Zero day xiv) Replay xv) Pass the hash xvi) Hijacking and related attacks (1) Clickjacking (2) Session hijacking (3) Uniform Resource Locator (URL) hijacking (4) Typo squatting xvii) Driver manipulation (1) Shimming (2) Refactoring xviii) Media Access Control (MAC) address spoofing xix) Internet Protocol (IP) address spoofing c) Describe wireless network attacks i) Replay	Ethics and Legal Responsibilities: 8.3, 8.6, 8.8 Technical Knowledge and Skills: 10.1, 10.5, 10.11 **CTE Pathway:** B1.1, B1.2, B1.3, B1.5, B1.6, B2.1, B3.1, B3.3, B5.1, B8.1, B8.2, B8.4

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	ii) Initialization vector (IV) iii) Evil twin iv) Rogue Access Point (AP) v) Jamming vi) Wireless Protected Setup (WPS) vii) Bluejacking viii) Bluesnarfing ix) Radio Frequency Identification (RFID) x) Near Field Communication (NFC) xi) Disassociation d) Describe cryptographic attacks i) Birthday ii) Known plain text/cipher text iii) Rainbow tables iv) Dictionary v) Brute force (Online vs. offline) vi) Collision vii) Downgrade viii) Replay ix) Weak implementations 3. Explain threat actor types and their attributes. a) Define types of threat actors i) Script kiddies ii) Hacktivist iii) Organized crime iv) Nation states v) Advanced Persistent Threat (APT) Groups vi) Insiders vii) Competitors b) Describe attributes of threat actors i) Internal / External ii) Level of sophistications iii) Resources and funding iv) Intent and motivation c) Identify and demonstrate the use of open-source intelligence. 4. Explain penetration testing concepts. a) Active reconnaissance b) Passive reconnaissance c) Pivot d) Initial exploitation e) Persistence f) Escalation of privilege g) Black box h) White box i) Gray box j) Pen testing vs. vulnerability scanning 5. Explain vulnerability scanning concepts a) Passively test security controls b) Identify vulnerability	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(15 hours)	c) Identify lack of security controls d) Identify common misconfigurations e) Intrusive vs. non-intrusive f) Credentialed vs. non-credentialed g) False positive 6. Explain the impact associated with different vulnerability types. a) Race conditions b) Vulnerabilities due to: i) End-of-life systems ii) Embedded systems iii) Lack of vendor support c) Improper input handling d) Improper error handling e) Misconfiguration/weak configuration f) Default configuration g) Resource exhaustion h) Untrained users i) Improperly configured accounts j) Vulnerable business processes k) Weak cipher suites and implementations l) Memory/buffer vulnerability i) Memory leak ii) Integer overflow iii) Buffer overflow iv) Pointer dereference v) DLL injection m) System sprawl and undocumented assets n) Architecture/design weaknesses o) New threats/zero day p) Improper certificate and key management	
C. TECHNOLOGIES AND TOOLS Understand, evaluate, and apply hardware and software tools to implement and support organizational security goals..	1. Describe, install and configure hardware and software network components to support organizational security. a) Firewall i) Access Control List (ACL) ii) Application-based vs. network-based iii) Stateful vs. stateless iv) Implicit deny b) Virtual Private Network (VPN) concentrator i) Remote access ii) Site-to-site iii) Internet Protocol Security (IPSec) (1) Tunnel mode (2) Transport mode (3) Authentication Header (AH) (4) Encapsulating Security Payload (ESP) iv) Split tunnel vs. full tunnel	**Career Ready Practice:** 1, 2, 4, 5 **CTE Anchor:** Communications: 2.3, 2.5 Technology: 4.1, 4.2, 4.3, 4.6 Problem Solving and Critical Thinking 5.1, 5.3, 5.4, 5.6, 5.7 Technical Knowledge and Skills:

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	v) Transport Layer Security (TLS) vi) Always-on VPN c) Network Intrusion Detection Systems (NIDS) and Network Intrusion Prevention Systems (NIPS) i) Signature-based ii) Heuristic/behavioral iii) Anomaly iv) Inline vs. passive v) In-band vs. out-of-band Rules vi) Analytics (1) False positive (2) False negative d) Router i) Access Control Lists (ACLs) ii) Antispoofing e) Switch i) Port security ii) Layer 2 vs. Layer 3 iii) Loop prevention iv) Flood guard f) Proxy i) Forward and reverse proxy ii) Transparent iii) Application/multipurpose g) Load balancer i) Scheduling ii) Affinity iii) Round-robin iv) Active-passive v) Active-active vi) Virtual IPs h) Access point i) Service Set Identifiers (SSID) ii) Media Access Control (MAC) address filtering iii) Signal strength iv) Band selection/width v) Antenna types and placement vi) Fat vs. thin vii) Controller-based vs. standalone i) Security Information and Event Management (SIEM) i) Aggregation ii) Correlation iii) Automated alerting and triggers iv) Time synchronization v) Event deduplication vi) Logs / Write Once Read Many (WORM) j) Data Loss Prevention (DLP) i) USB blocking ii) Cloud-based	10.1, 10.3, 10.5, 10.8 Demonstration and Application: 11.1, 11.2 **CTE Pathway:** B1.1, B1.4, B1.5, B4.5, B6.1, B8.1, B8.2, B8.4, B8.5

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	iii) Email k) Network Access Control (NAC) i) Dissolvable vs. permanent ii) Host health checks iii) Agent vs. agentless l) Mail gateway i) Spam filter ii) Data Loss Preventions (DLP) iii) Encryption m) Bridge n) Secure Sockets Layer (SSL) and Transport Layer Security (TLS) accelerators o) Secure Sockets Layer (SSL) decryptors p) Media gateways q) Hardware security modules 2. Access the security posture of an organization using the appropriate software tools. a) Protocol analyzer b) Network scanners i) Rogue system detection ii) Network mapping c) Wireless scanners/cracker d) Password cracker e) Vulnerability scanner f) Configuration compliance scanner g) Exploitation frameworks h) Data sanitization tools i) Steganography tools j) Honeypot k) Backup utilities l) Banner grabbing m) Passive vs. active n) Command line tools i) ping ii) netstat iii) tracert iv) nslookup/dig v) arp vi) ipconfig/ip/ifconfig vii) tcpdump viii) nmap ix) netcat 3. Evaluate and troubleshoot common security issues. a) Unencrypted credentials/clear text b) Logs and events anomalies c) Permission issues d) Access violations e) Certificate issues f) Data exfiltration	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	g) Misconfigured devices i) Firewall ii) Content filter iii) Access points h) Weak security configurations i) Personnel issues i) Policy violation ii) Insider threat iii) Social engineering iv) Social media v) Personal email j) Unauthorized software k) Baseline deviation l) License compliance violation (availability/integrity) m) Asset management n) Authentication issues 4. Analyze and interpret output from security technologies. a) Host Intrusion Detection System (HIDS) b) Host Intrusion Prevention System (HIPS) c) Antivirus d) File integrity check e) Host-based firewall f) Application whitelisting g) Removable media control h) Advanced malware tools i) Patch management tools j) Unified Threat Management (UTM) k) Data Loss Prevention (DLP) l) Data execution prevention m) Web application firewall 5. Describe the secure deployment of mobile devices. a) Connection methods i) Cellular ii) IEEE 802.11 WiFi iii) Satellite Communication (SATCOM) iv) Bluetooth v) Near Field Communications (NFC) vi) Adaptive Network Technology (ANT) vii) Infrared viii) Universal Serial Bus (USB) b) Mobile device management concepts i) Application management ii) Content management iii) Remote wipe iv) Geofencing v) Geolocation vi) Screen locks vii) Push notification services viii) Passwords and pins	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	ix) Biometrics x) Context-aware authentication xi) Containerization xii) Storage segmentation xiii) Full device encryption c) Enforcement and monitoring for: i) Third-party application stores ii) Rooting and jailbreaking iii) Sideloading iv) Custom firmware v) Carrier unlocking vi) Firmware Over the Air (OTA) updates vii) Camera use viii) Short Message Service (SMS) ix) Multimedia Messaging Service (MMS) x) External media xi) USB On The Go (OTG) xii) Recording microphone xiii) Global Positioning System (GPS) tagging xiv) WiFi direct / ad hoc xv) Tethering xvi) Payment methods d) Deployment models i) Bring Your Own Device (BYOD) ii) Corporate Own Personally Enabled (COPE) iii) Choose Your Own Device (CYOD) iv) Corporate-owned v) Virtual Desktop Infrastructure (VDI) 6. Implement secure protocols in various scenarios. a) Protocols i) Domain Name System Security Extensions (DNSSEC) ii) Secure Shell Handler (SSH) iii) Secure/Multipurpose Internet Mail Extensions (S/MIME) iv) Secure Real-Time Transport Protocol (SRTP) v) Lightweight Directory Access Protocol over SSL (LDAPS) vi) File Transfer Protocol over SSL (FTPS) vii) Secure File Transfer Protocol (SFTP) viii) Simple Network Management Protocol Version 3 (SNMPv3) ix) Secure Sockets Layer (SSL), Transport Layer Security (TLS) x) HyperText Transfer Protocol Secure (HTTPS) xi) Secure Post Office Protocol (Secure POP) xii) Secure Internet Message Protocol (Secure IMAP) b) Describe use cases for; i) Voice and Video ii) Time synchronization iii) Email and web iv) File transfer v) Directory services	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(15 hours)	vi) Remote access vii) Domain name resolution viii) Router and switching ix) Network address allocation x) Subscription services	
D. ARCHITECTURE AND DESIGN Understand, analyze, and evaluate security frameworks used to implement and support secure network designs.	1. Explain use cases and purpose for frameworks, best practices and secure configuration guides. a) Industry-standard frameworks and reference architectures i) Regulatory ii) Non-regulatory iii) National vs. international iv) Industry-specific frameworks b) Benchmarks/secure configuration guides i) Platform/vendor specific guides (1) Web server (2) Operating system (3) Application server (4) Network infrastructure devices ii) General purpose guides c) Defense-in-depth/layered security i) Vendor diversity ii) Control diversity (1) Administrative (2) Technical iii) User training 2. Implement secure network architecture concepts a) Zones/topologies i) Demilitarized Zone (DMZ) ii) Extranet iii) Intranet iv) Wireless v) Guest vi) Honeynet vii) Network Address Translation (NAT) viii) Adhoc b) Segregation/segmentation/isolation i) Physical ii) Logical (VLAN) iii) Virtualization iv) Air gaps c) Tunneling / Virtual Private Networks (VPN) i) Site-to-site ii) Remote access d) Security device/technology placement i) Sensors ii) Collectors iii) Correlation engines	**Career Ready Practice:** 1, 2, 4, 5 **CTE Anchor:** Communications: 2.3, 2.5, 2.7 Technology: 4.3 Problem Solving and Critical Thinking: 5.1, 5.2, 5.6 Technical Knowledge and Skills: 10.1, 10.5, 10.8 Demonstration and Application: 11.2 **CTE Pathway:** B1.4, B3.1, B3.2, B3.7, B4.5, B4.9, B5.1, B5.2, B8.2, B8.3, B8.4

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	iv) Filters v) Proxies vi) Firewalls vii) Virtual Private Networks (VPN) concentrators viii) Secure Socket Layer (SS)L accelerators ix) Load balancers x) Distributed Denial of Service (DDoS) mitigator xi) Aggregation switches xii) Taps and port mirror e) Software Defined Networking (SDN) 3. Implement secure systems design for a given scenario. a) Hardware/firmware security i) Full Disk Encryption (FDE) / Self Encrypting Disk (SED) ii) Trusted Platform Module (TPM) iii) Hardware Security Module (HSM) iv) Unified Extensible Firmware Interface (UEFI) / Basic Input Output System (BIOS) v) Secure boot and attestation vi) Supply chain vii) Hardware root of trust viii) Electromagnetic interference (EMI) / electromagnetic pulses (EMP) b) Operating systems i) Types (1) Network (2) Server (3) Workstation (4) Appliance (5) Kiosk (6) Mobile OS ii) Patch management iii) Disabling unnecessary iv) ports and services v) Least functionality vi) Secure configurations vii) Trusted operating system viii) Application whitelisting/blacklisting ix) Disable default accounts/passwords c) Peripherals i) Wireless keyboards ii) Wireless mice iii) Displays iv) WiFi-enabled MicroSD cards v) Printers/Multifunction Devices (MFDs) vi) External storage devices vii) Digital cameras 4. Explain the importance of secure staging deployment concepts. a) Sandboxing b) Environment	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	i) Development ii) Test iii) Staging iv) Production c) Secure baseline d) Integrity measurement 5. Explain the security implications of embedded systems. a) Supervisory Control and Data Acquisition (SCADA)/ Industrial Control Systems (ICS) b) Smart devices/ Internet of Things (IoT) i) Wearable technology ii) Home automation c) Heating Ventilations and Air Conditioning (HVAC) d) Systems on a Chip (SoC) e) Real Time Operating Systems (RTOS) f) Printers / Multifunction Displays (MFDs) g) Camera systems h) Special purpose i) Medical devices ii) Vehicles iii) Aircraft / Unmanned Aerial Vehicle (UAV) 6. Summarize secure application development and deployment concepts a) Development life-cycle models: Waterfall vs. Agile b) Secure DevOps i) Security automation ii) Continuous integration iii) Baselining iv) Immutable systems v) Infrastructure as code c) Version control and change management d) Provisioning and deprovisioning e) Secure coding techniques i) Proper error handling ii) Proper input validation iii) Normalization iv) Stored procedures v) Code signing vi) Encryption vii) Obfuscation/camouflage viii) Code reuse/dead code ix) Server-side vs. client-side x) execution and validation xi) Memory management xii) Use of third-party libraries and SDKs xiii) Data exposure f) Code quality and testing i) Static code analyzers ii) Dynamic analysis (e.g., fuzzing)	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	iii) Stress testing iv) Sandboxing v) Model verification g) Compiled vs. runtime code 7. Summarize cloud and virtualization concepts. a) Hypervisor i) Type I ii) Type II iii) Application cells/containers b) Virtual Machine (VM) sprawl avoidance c) Virtual Machine (VM) escape protection d) Cloud storage e) Cloud deployment models i) Software as a service (SaaS) ii) Platform as a service (PaaS) iii) Infrastructure as a Service (IaaS) iv) Private v) Public vi) Hybrid vii) Community f) On-premise vs. hosted vs. cloud g) Virtual Desk Infrastructure (VDI) / Virtual Desk Environment (VDE) h) Cloud access security broker i) Security as a service 8. Explain how resiliency and automation strategies reduce risk. a) Automation/scripting i) Automated courses of action ii) Continuous monitoring iii) Configuration validation b) Templates c) Master image d) Non-persistence i) Snapshots ii) Revert to known state iii) Rollback to known configuration iv) Live boot media e) Elasticity f) Scalability g) Distributive allocation h) Redundancy i) Fault tolerance j) High availability k) Redundant array of inexpensive disks (RAID) 9. Explain the importance of physical security controls. a) Lighting b) Signs c) Fencing/gate/cage d) Security guards	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(15 hours)	e) Alarms f) Safe g) Secure cabinets/enclosures h) Protected distribution/Protected cabling i) Airgap j) Mantrap k) Faraday cage l) Lock types m) Biometrics n) Barricades/bollards o) Tokens/cards p) Environmental controls i) Heating, Ventilation, and Air Conditioning (HVAC) ii) Hot and cold aisles iii) Fire suppression q) Cable locks r) Screen filters s) Cameras t) Motion detection u) Logs v) Infrared detection w) Key management	
E. IDENTITY AND ACCESS MANAGEMENT Understand, evaluate, and apply identity and access management controls to secure organizations and computer networks.	1. Compare and contrast identity and access management concepts. a) Identification, authentication, authorization and accounting (AAA) b) Multifactor authentication i) Something you are ii) Something you have iii) Something you know iv) Somewhere you are v) Something you do c) Federation d) Single sign-on e) Transitive trust 2. Analyze a scenario, install and configure identity and access services. a) Lightweight Directory Access Protocol (LDAP) b) Kerberos c) Terminal Access Controller Access Control System (TACACS+) d) Challenge-Handshake Authentication Protocol (CHAP) e) Password Authentication Protocol (PAP) f) Microsoft Challenge Handshake Authentication Protocol (MSCHAP) g) Remote Authentication Dial in User Service (RADIUS) h) Security Assertions Markup Language (SAML) i) OpenID Connect j) Open Authorization (OAUTH) k) Shibboleth l) Secure token	**Career Ready Practice:** 1, 2, 4, 10 **CTE Anchor:** Communications: 2.4, 2.6 Technology: 4.1, 4.5 Problem Solving and Critical Thinking: 5.1, 5.3, 5.4, 5.11 Technical Knowledge and Skills: 10.1, 10.5, 10.8 Demonstration and Application: 11.1, 11.2 **CTE Pathway:** B1.1, B3.1, B3.2, B4.5, B4.9, B6.2, B8.2, B8.3, B8.4

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	m) NT Lan Manager (NTLM) 3. Analyze a scenario, implement identity and access management controls. a) Access control models i) Mandatory Access Control (MAC) ii) Discretionary Access Control (DAC) iii) Attribute-based access control (ABAC) iv) Role-based access control v) Rule-based access control b) Physical access control i) Proximity cards ii) Smart cards c) Biometric factors i) Fingerprint scanner ii) Retinal scanner iii) Iris scanner iv) Voice recognition v) Facial recognition vi) False acceptance rate vii) False rejection rate viii) Crossover error rate d) Tokens i) Hardware ii) Software iii) HAMC One-time password HOTP / Time-based one-time password (TOTP) e) Certificate-based authentication i) PIV/CAC/smart card ii) IEEE 802.1x f) File system security g) Database security 4. Analyze a scenario, differentiate common account management practices. a) Account types i) User account ii) Shared and generic iii) accounts/credentials iv) Guest accounts v) Service accounts vi) Privileged accounts b) General Concepts i) Least privilege ii) Onboarding/offboarding iii) Permission auditing and review iv) Usage auditing and review v) Time-of-day restrictions vi) Recertification vii) Standard naming convention viii) Account maintenance	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(10 hours)	ix) Group-based access control x) Location-based policies c) Account policy enforcement i) Credential management ii) Group policy iii) Password complexity iv) Expiration v) Recovery vi) Disablement vii) Lockout viii) Password history ix) Password reuse x) Password length	
F. RISK MANAGEMENT Understand and evaluate security procedures and controls to manage organizational risk.	1. Explain the importance of policies, plans and procedures related to organizational security a) Standard operating procedure b) Agreement types i) Business Partner Agreement (BPA) ii) Service Level Agreement (SLA) iii) Interconnection Security Agreement (ISA) iv) Memorandum of Understanding (MOU) / Memorandum of Agreement (MOA) c) Personnel management i) Mandatory vacations ii) Job rotation iii) Separation of duties iv) Clean desk v) Background checks vi) Exit interviews vii) Role-based awareness training (1) Data owner (2) Systems administrator (3) System owner (4) User (5) Privileged user (6) Executive user (7) Non-Disclosure Agreement (NDA) (8) Onboarding (9) Continuing education (10) Acceptable use policy/rules of behavior (11) Adverse actions d) General security policies i) Social media networks/applications ii) Personal email 2. Summarize business impact analysis concepts. a) Recovery Time Objective (RTO) / Recovery Point Objective (RPO)	**Career Ready Practice:** 1, 2, 4, 5, 8 **CTE Anchor:** Communications: 2.6 Technology: 4.2 Problem Solving and Critical Thinking: 5.4, 5.6 Ethics and Legal Responsibilities: 8.1, 8.5, 8.7, 8.8 Technical Knowledge and Skills: 10.1, 10.8 Demonstration and Application: 11.2 **CTE Pathway:** B4.2, B4.5, B8.2, B8.3, B8.4, B8.5

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	b) Mean time between failures (MTBF) c) Mean time to repair (MTTR) d) Mission-essential functions e) Identification of critical systems f) Single point of failure g) Impact i) Life ii) Property iii) Safety iv) Finance v) Reputation h) Privacy impact assessment i) Privacy threshold assessment 3. Explain risk management processes and concepts. a) Threat assessment i) Environmental ii) Manmade iii) Internal vs. external b) Risk assessment i) Single Loss Expectancy (SLE) ii) Annual Loss Expectancy (ALE) iii) Annualized Rate of Occurrence (ARO) iv) Asset value v) Risk register vi) Likelihood of occurrence vii) Supply chain assessment viii) Impact ix) Quantitative x) Qualitative xi) Testing (1) Penetration testing authorization (2) Vulnerability testing authorization xii) Risk response techniques (1) Accept (2) Transfer (3) Avoid (4) Mitigate c) Change management 4. Given a scenario, follow incident response procedures. a) Incident response plan i) Documented incident ii) types/category definitions iii) Roles and responsibilities iv) Reporting requirements/escalation v) Cyber-incident response teams vi) Exercise b) Incident response process i) Preparation ii) Identification	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	iii) Containment iv) Eradication v) Recovery vi) Lessons learned 5. Summarize basic concepts of forensics. a) Order of volatility b) Chain of custody c) Legal hold d) Data acquisition i) Capture system image ii) Network traffic and logs iii) Capture video iv) Record time offset v) Take hashes vi) Screenshots vii) Witness interviews e) Preservation f) Recovery g) Strategic intelligence / counterintelligence gathering i) Active logging h) Track man-hours 6. Explain disaster recovery and continuity of operations concepts. a) Recovery sites i) Hot site ii) Warm site iii) Cold site b) Order of restoration c) Backup concepts i) Differential ii) Incremental iii) Snapshots iv) Full d) Geographic considerations i) Off-site backups ii) Distance iii) Location selection iv) Legal implications v) Data sovereignty e) Continuity of operations planning i) Exercises/tabletop ii) After-action reports iii) Failover iv) Alternate processing sites v) Alternate business practice 7. Compare and contrast various types of controls. a) Deterrent b) Preventive c) Detective d) Corrective	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(15 hours)	e) Compensating f) Technical g) Administrative h) Physical 8. Analyze a scenario, carry out data security and privacy practices a) Data destruction and media sanitization i) Burning ii) Shredding iii) Pulping iv) Pulverizing v) Degaussing vi) Purging vii) Wiping b) Data sensitivity labeling and handling i) Confidential ii) Private iii) Public iv) Proprietary v) Personally Identifiable Information (PII) vi) Protected Health Information (PHI) c) Data roles i) Owner ii) Steward/custodian iii) Privacy officer d) Data retention e) Legal and compliance	
G. CRYPTOGRAPHY AND PUBLIC KEY INFRASTRUCTURE (PKI) Understand, analyze, and apply basic cryptographic concepts and algorithms to implement a public key infrastructure (PKI).	1. Compare and contrast basic concepts of cryptography. a) Symmetric algorithms b) Modes of operation c) Asymmetric algorithms d) Hashing e) Salt, IV, nonce f) Elliptic curve g) Weak/deprecated algorithms h) Key exchange i) Digital signatures j) Diffusion k) Confusion l) Collision m) Steganography n) Obfuscation o) Stream vs. block p) Key strength q) Session keys r) Ephemeral key s) Secret algorithm t) Data-in-transit	**Career Ready Practice:** 1, 4 **CTE Anchor:** Communications: 2.7 Technology: 4.5 Problem Solving and Critical Thinking: 5.3, 5.8 Ethics and Legal Responsibilities: 8.2 Technical Knowledge and Skills: 10.1, 10.5, 10.8 Demonstration and Application:

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	u) Data-at-rest v) Data-in-use w) Random/pseudo-random number generation x) Key stretching y) Implementation vs. algorithm selection i) Crypto service provider ii) Crypto modules z) Perfect forward secrecy aa) Security through obscurity bb) Common use cases i) Low power devices ii) Low latency iii) High resiliency iv) Supporting confidentiality v) Supporting integrity vi) Supporting obfuscation vii) Supporting authentication viii) Supporting non-repudiation ix) Resource vs. security constraints 2. Explain cryptography algorithms and their basic characteristics. a) Symmetric algorithms i) Advanced Encryption Standard, (AES) ii) Data Encryption Standard (DES) iii) Triple Data Encryption Standard (3DES) iv) Rivest Cipher 4 (RC4) v) Blowfish/Twofish b) Cipher modes i) Cipher Block Chaining CBC ii) Galois/Counter Mode (GCM) iii) Electronic Code Book (ECB) iv) Counter (CTR) v) Stream vs. block c) Asymmetric algorithms i) Rivest-Shamir-Adleman (RSA) ii) Digital Signature Algorithm (DSA) iii) Diffie-Hellman (1) Groups (2) Diffie-Hellman Ephemeral (DHE) (3) Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) (4) Elliptic curve (5) Pretty Good Privacy (PGP) / Gnu Privacy Guard (GPG) d) Hashing algorithms i) Message Digest algorithm 5 (MD5) ii) Secure Hash Algorithm (SHA) iii) Hash Message Authentication Code (HMAC) iv) RACE Integrity Primitives Evaluation Message Digest (RIPEMD) e) Key stretching algorithms i) BCRYPT	**CTE Pathway:** 8.1, 8.2, 8.4

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
	ii) PBKDF2 f) Obfuscation i) XOR ii) ROT13 iii) Substitution ciphers 3. Analyze a scenario, install and configure wireless security settings. a) Cryptographic protocols i) Wireless Protected Access (WPA) ii) Wireless Protected Access 2 (WPA2) iii) CCMP iv) Temporal Key Integrity Protocol (TKIP) b) Authentication protocols i) Extensible Authentication Protocol. (EAP) ii) Protected Extensible Authentication Protocol (PEAP) iii) EAP-FAST iv) EAP-TLS v) EAP-TTLS vi) IEEE 802.1x vii) RADIUS Federation c) Methods i) PSK vs. Enterprise vs. Open ii) WPS iii) Captive portals 4. Analyze a scenario, implement public key infrastructure a) Components i) Certificate Authority (CA) ii) Intermediate CA iii) Certificate Revocation List (CRL) iv) Online Certificate Status Protocol (OCSP) v) Certificate Signing Request (CSR) vi) Certificate vii) Public key viii) Private key ix) Object identifiers (OID) b) Concepts i) Online vs. offline CA ii) Stapling iii) Pinning iv) Trust model v) Key escrow vi) Certificate chaining c) Types of certificates i) Wildcard ii) SAN iii) Code signing iv) Self-signed v) Machine/computer vi) Email vii) User	

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(15 hours)	viii) Root ix) Domain validation x) Extended validation d) Certificate formats i) Distinguished Encoding Rules (DER) ii) Packed Encoding Rules (PEM) iii) Personal Exchange Format (PFX) iv) Canonical Encoding Rules (CER) v) Public Key Cryptography Standard number 12 (P12) vi) Public Key Cryptography Standard number (P7B)	
H. CERTIFICATION EXAM REVIEW SESSIONS WITH STUDY GUIDES AND SIMULATED ONLINE TESTING Understand, evaluate, and demonstrate the skills required to take written and simulated certification exams. (20 hours)	1. Review test from study guides with instructor. 2. Explain importance of time management skills and note taking for successfully passing certification tests. 3. Take a simulated certification exam on-line. 4. Evaluate test results and prepare for re-testing if necessary. 5. Prepare for a certification test with individualized lab reviews. 6. Identify the steps required to obtain the CompTIA Security+ certification a) Identify the required exam for the CompTIA Security+ certification. b) Explain the registration process for certification exams. c) Describe the exam-testing environment.	**Career Ready Practice:** 1, 2, 3 **CTE Anchor:** Communications: 2.2 Career Planning and Management: 3.4, 3.6 Technology: 4.4 Problem Solving and Critical Thinking: 5.3, 5.7 Technical Knowledge and Skills: 10.1 Demonstration and Application: 11.2 **CTE Pathway:** B1.1, B3.1, B8.1, B8.2, B8.3, B8.4, B8.5
I. EMPLOYABILITY SKILLS Understand, apply, and evaluate the employability skills required in the Cybersecurity field.	1. Identify other Cybersecurity certifications 2. Identify job titles and required industry certifications 3. Identify potential employers using traditional and Internet sources. 4. Describe the role of social media in job search. 5. Design sample resume and cover letters. 6. Explain the importance of filling out a job application legibly, with accurate and complete information. 7. Describe the common mistakes that are made on job applications.	**Career Ready Practice:** 2 **CTE Anchor:** Communications: 2.5 Career Planning Management:

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(10 hours)	8. Complete sample job application forms correctly. 9. State the importance of enthusiasm in the interview and on a job. 10. State the importance of appropriate appearance in the interview and on a job. 11. State the importance of the continuous upgrading of job skills. 12. Describe customer service as a method of building permanent relationships between the organization and the customer. 13. Describe and Demonstrate appropriate interviewing techniques. 14. Identify the informational materials and resources needed to be successful in an interview. 15. Design sample follow-up letters. 16. Describe and demonstrate appropriate follow-up procedures	3.1, 3.2, 3.3, 3.4, 3.6 Technology: 4.1, 4.2, 4.7 Problem Solving and Critical Thinking: 5.4 Responsibility and Flexibility: 7.2, 7.7 Ethics and Legal Responsibilities: 8.3, 8.4 Technical Knowledge and Skills: 10.1, 10.3 **CTE Pathway:** B4.2, B5.2

SUGGESTED INSTRUCTIONAL MATERIALS and OTHER RESOURCES

TEXTS AND SUPPLEMENTAL BOOKS

Author CompTIA , CompTIA Security+ Certification (SY0-501) Study Guide, CompTIA

David L. Prowse, CompTIA® Security+ SY0-501 Cert Guide Academic Edition, Pearson IT Certification 2017, ISBN 10: 0789759128

David L. Prowse, CompTIA Security+ SY0-501 Cert Guide (4th Edition), Pearson IT Certification, 2017, ISBN-10: 9780789758996

Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition, Cengage Learning, ISBN-10: 1-337-28878-0

ONLINE SOFTWARE

NDG Netlabs www.netdevgroup.com/online

SOFTWARE

Oracle VirtualBox (Free) www.virtualbox.org

Virtual Machines (Free)

- Security Onion securityonion.net
- Kali Linux www.kali.org
- Metasploitable metasploit.help.rapid7.com

Wireshark www.wireshark.org

RESOURCES

Employer Advisory Board Meetings
Employer Advisory Board Members

California Career Technical Education Model Curriculum Standards _ Information Technology
https://www.cde.ca.gov/ci/ct/sf/documents/infocomtech.pdf

Computing Technology Industry Association (CompTIA), 1815 S. Meyers Rd., Suite 300, Oakbrook Terrace, IL 60181-5228. Phone: (630) 678-8300. Fax: (630) 268-1384

TEACHING STRATEGIES and EVALUATION

METHODS AND PROCEDURES

A. Lecture and discussion

B. Multimedia presentations

C. Demonstrations and Hands-on Labs

D. Individualized instruction

E. Peer teaching

F. Role-playing

G. Guest speakers

H. Field trips and field study experiences

I. Projects

EVALUATION

SECTION A – Orientation and Safety – Pass the safety test with 100% accuracy.

SECTION B – Threats, Attacks, and Vulnerabilities - Pass all assignments and exams on threats, attacks, and vulnerabilities with a minimum score of 80% or higher

SECTION C –Technologies and Tools – Pass all assignments and exams on technologies and tools with a minimum score of 80% or higher.

SECTION D – Architecture and Design – Pass all assignments and exams on architecture and design with a minimum score of 80% or higher.

SECTION E – Identity and Access Management – Pass all assignments and exams on identity and access management with a minimum score of 80% or higher.

SECTION F – Risk Management – Pass all assignments and exams on risk management with a minimum score of 80% or higher.

SECTION G – Cryptography and Public Key Infrastructure (PKI) – Pass all assignments and exams on cryptography and public key infrastructure (PKI) with a minimum score of 80% or higher.

SECTION H – Certification Exam Review – Pass all assignments and review exams with a minimum score of 80% or higher.

SECTION I – Employability Skills – Pass all assignments and exams on employability skills with a minimum score of 80% or higher.

Statement for Civil Rights

All educational and vocational opportunities are offered without regard to race, color, national origin, gender, or physical disability.