LAUSD UNIFIED **Division of Adult and Career Education**

Career Technical Education (CTE) Course Outline

Course Title:	CompTIA Security+
Course Number:	77-65-90
Date:	July 2025
Industry Sector:	Information and Communication Technologies
Pathway:	Networking
CBEDS Title:	Network Engineering
CBEDS Code:	4646
CalPADS	8122
Credits:	10

Hours:

Total
120

Course Description:

This competency-based course is designed to prepare students to pass the CompTIA Security+ certification examination. This is the third course in a sequence of three courses of the cybersecurity pathway. Technical instruction includes an introduction, safety, general security concepts, threats, vulnerabilities, and mitigations, security architecture, security operations, security program management and oversight, employability skills and resume preparation, and certification exam review. The competencies in this course are aligned with the California Common Core Standards and the California Career Technical Education Model Curriculum Standards.

Prerequisites:	Enrollment requires a 6.0 reading level as measured by the CASAS GOALS test, successful completion (or demonstrate competency) of Algebra 1, successful completion of Cybersecurity Essentials CCST (77-65-75), and/or CyberOps Associate (77-65-85).
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.
A-G Approval	N/A
Methods of Instruction:	Lecture and discussion, demonstration and participation, multimedia presentations, individualized instruction, peer teaching, role-playing, guest speakers, field trips and field study experiences, projects.
Student Evaluation:	Summative: End of section assessments
Industry Certification:	CompTIA Security+ certification.
Recommended Texts:	Security Pro: TestOut
Link to Resource Folder	https://bit.ly/CompTIAResources

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
A. INTRODUCTION Understand, apply, and evaluate classroom and workplace policies and procedures. (2 hours)	1. Describe the scope and purpose of the course. 2. Discuss and demonstrate Zoom, Schoology, and basic computer skills. 3. Identify classroom policies and procedures. 4. Discuss, identify, research, and draw conclusions about different career paths, occupations, employment outlook, and career advancements in the Information and Communications Technologies industry sector which impact cybersecurity. 5. Describe opportunities available for promoting gender equity and the representation of non-traditional populations in the Information and Communications Technologies industry sector. 6. Explain and recognize the importance of customer-oriented service, ethics, teamwork, respect of individual and cultural differences, and diversity in the workplace. 7. Describe the CompTia Security+ Exam.	**Career Ready Practice:** 1, 2, 3, 4, 8, 9, 10, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5, 2.8 Career Planning & Management: 3.1, 3.3, 3.4, 3.5 Technology: 4.2 Ethics & Legal Responsibilities: 8.4 Leadership & Teamwork: 9.3, 9.6 Demonstration & Application: 11.1 **CTE Pathway:** B2.2
B. SAFETY	1. Discuss classroom and workplace first aid, emergency procedures, and accidents or injury prevention.	**Career Ready Practice:** 1, 2, 10, 12

Understand safety procedures and techniques in the Information and Communication Technologies Industry Sector. (2 hours)	2. Discuss the California Occupational Safety and Health Administration (Cal/OSHA) workplace requirements for network technicians to maintain a safe and healthy working environment. 3. Discuss the use of the Safety Data Sheet (SDS) as it applies to the Information and Communication Technologies industry sector. 4. Practice personal safety when lifting, bending, or moving equipment and supplies. 5. Explain how each of the following insures a safe workplace: a. employees' rights as they apply to job safety b. employers' obligations as they apply to safety c. safety laws applying to electrical tools 6. Explain and sign the LAUSD Responsible Use Policy (RUP). 7. Pass the Safety Test with 100% accuracy.	**CTE Anchor:** Academics: 1.0 Communications : 2.1, 2.3, 2.5, 2.6 Health & Safety: 6.1, 6.2, 6.3, 6.4, 6.7 Demonstration & Application: 11.1 **CTE Pathway:** B2.2
C. GENERAL SECURITY CONCEPTS Explain how security controls, concepts, change management, and cryptography impact security.	1. Compare and contrast various types of security controls to include: a. preventive b. deterrent c. detective d. corrective e. compensating f. directive 2. Define the following fundamental security concepts: a. Confidentiality, Integrity, and Availability (CIA) b. non-repudiation c. Authentication, Authorization, and Accounting (AAA) d. gap analysis e. zero trust f. physical security g. deception and disruption technology 3. Explain the importance of change management processes and their impact to security: a. business processes impacting security operation b. technical implications c. documentation d. version control 4. Define cryptographic solutions to include: a. Public Key Infrastructure (PKI) b. encryption c. tools	**Career Ready Practice:** 1, 2, 4, 5 **CTE Anchor:** Academics: 1.0 Communications : 2.1, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.2, 5.3 Technical Knowledge & Skills: 10.1, 10.8 **CTE Pathway:** B1.1, B3.4, B4.2

(18 hours)	d. obfuscation e. hashing f. salting g. digital signatures h. key stretching i. blockchain j. open public ledger k. certificates 5. Pass a General Security Concepts assessment with an 80% score or higher.	
D. THREATS, VULNERABILITIES & MITIGATIONS Explain common threat actors, attacks, and mitigation techniques.	1. Compare and contrast common threat actors, attributes of actors, and motivations. 2. Define and explain common threat vectors and attack surfaces: a. message-based b. image-based c. file-based d. voice call e. removable device f. vulnerable software g. unsupported systems and applications h. unsecure networks i. open service ports j. default credentials k. supply chain l. human vectors/social engineering 3. Explain various types of vulnerabilities to include: a. application b. operating system (OS)-based c. web-based d. hardware e. virtualization f. cloud-specific g. supply chain h. cryptographic i. misconfiguration j. mobile device zero-day 4. Given a scenario, form teams to analyze the following indicators of malicious activity: a. malware attacks b. physical attacks c. network attacks d. application attacks e. cryptographic attacks f. password attacks	**Career Ready Practice:** 1, 2, 4, 5, 9, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2, 4.5 Problem Solving & Critical Thinking: 5.2, 5.3, 5.4 Leadership & Teamwork: 9.7 Technical Knowledge & Skills: 10.1 **CTE Pathway:** B1.1, B4.2, B4.5, B4.7, B8.2, B8.4

(18 hours)	g. indicators 5. Define and describe the purpose of the following mitigation techniques used to secure the enterprise: a. segmentation b. access control c. application allow list d. isolation e. patching f. encryption g. monitoring h. least privilege i. configuration enforcement j. decommissioning k. hardening techniques 6. Pass a Threats, Vulnerabilities, & Mitigations assessment with an 80% score or higher.	
E. SECURITY ARCHITECTURE Understand, analyze, and evaluate security frameworks used to implement and support secure network designs.	1. Compare and contrast security implications of architecture models including: a. architecture and infrastructure concepts b. considerations 2. Given a scenario, explain and form teams to apply security principles to secure enterprise infrastructure: a. infrastructure considerations b. secure communication/access c. selection of effective controls 3. Compare and contrast the following concepts and strategies to protect data: a. data types b. data classifications c. general data considerations d. methods to secure data 4. Describe the importance of resilience and recovery in security architecture: a. high availability b. site considerations c. platform diversity d. multi-cloud systems e. continuity of operations f. capacity planning g. testing h. backups i. power 5. Pass a Security Architecture assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 9, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2, 4.3, 4.5 Problem Solving & Critical Thinking: 5.1, 5.4 Leadership & Teamwork: 9.7 Technical Knowledge & Skills: 10.1, 10.8, 10.12 **CTE Pathway:**

(18 hours)		B1.4, B4.5, B4.8, B8.2, B8.4
F. SECURITY OPERATIONS Understand, analyze, and implement security measures, optimizing security operations, and ensuring effective incident response.	1. Define and demonstrate common security techniques listed below to computing resources: a. secure baselines b. hardening targets c. wireless devices d. mobile solutions e. wireless security settings f. application security g. sandboxing h. monitoring 2. Explain the following security implications of proper hardware, software, and data asset management: a. acquisition/procurement process b. assignment/accounting c. monitoring/asset tracking d. disposal/decommissioning 3. Describe the various activities associated with vulnerability management: a. identification methods b. analysis c. vulnerability response and remediation d. validation of remediation e. reporting 4. Demonstrate the following security alerting and monitoring concepts and tools: a. monitoring computing resources b. activities c. tools 5. Given a scenario, modify enterprise capabilities to enhance security via: a. firewall b. IDS/IPS c. web filter d. operating system security e. implementation of secure protocols f. DNS filtering g. email security h. file integrity monitoring i. DLP j. Network Access Control (NAC) k. Endpoint Detection And Response (EDR)/Extended Detection and Response (XDR) l. user behavior analytics	**Career Ready Practice:** 1, 2, 4, 5, 10, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.1, 5.4 Technical Knowledge & Skills: 10.1, 10.8, 10.12 Demonstration & Application: 11.1 **CTE Pathway:** B1.1, B4.1, B4.2, B4.5, B6.3, B8.1, B8.4, B8.5

(18 hours)	6. Describe Identity and Access Management (IAM): a. provisioning/deprovisioning user accounts b. permission assignments and implications c. identity proofing d. federation e. Single Sign-On (SSO) f. interoperability g. attestation h. access controls i. multi factor authentication j. password concepts k. privileged access management tools 7. Explain the importance of automation and orchestration related to secure operations: a. use cases of automation and scripting b. benefits c. other considerations 8. Discuss appropriate incident response activities listed below: a. process b. training c. testing d. root cause analysis e. threat hunting f. digital forensics 9. Given a scenario, use data sources to support an investigation: a. log data b. data sources 10. Pass a Security Operations assessment with an 80% score or higher.	
G. SECURITY PROGRAM MANAGEMENT & OVERSIGHT Understand, analyze, and evaluate effective security governance and risk management.	1. Define the following elements of effective security governance: a. guidelines b. policies c. standards d. procedures e. external considerations f. monitoring and revision g. types of governance structures h. roles and responsibilities for systems and data 2. Explain the following elements of the risk management process: a. risk identification	**Career Ready Practice:** 1, 2, 4, 5, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology:

(18 hours)	b. risk assessment c. risk analysis d. risk register e. risk tolerance f. risk appetite g. risk management strategies h. risk reporting i. business impact analysis 3. Discuss the following processes associated with third-party risk assessment and management: a. vendor assessment b. vendor selection c. agreement types d. vendor monitoring e. questionnaires f. rules of engagement 4. Discuss and summarize the following elements of effective security compliance: a. compliance reporting b. consequences of non-compliance c. compliance monitoring d. privacy 5. Define and explain types and purposes of audits and assessments to include: a. attestation b. internal c. external d. penetration testing 6. Given a scenario, implement the following security awareness practices: a. phishing b. anomalous behavior recognition c. user guidance and training d. reporting and monitoring e. development f. execution 7. Pass a Security Program Management & Oversight assessment with an 80% score or higher.	4.2, 4.5 Problem Solving & Critical Thinking: 5.1, 5.3 Technical Knowledge & Skills: 10.1, 10.8, 10.11, 10.14 **CTE Pathway:** B1.1, B4.2, B4.5, B4.9, B7.1, B8.1, B8.2
H. EMPLOYABILITY SKILLS AND RESUME PREPARATION Understand, apply, and evaluate the employability skills and	1. Understand and define employer requirements for soft skills to include: a. attitude toward work b. communication and collaboration c. critical thinking, problem solving, and decision-making	**Career Ready Practice:** 1, 2, 3, 4, 5, 7, 8, 9, 10, 11 **CTE Anchor:**

résumé preparation desired of networking technicians. (6 hours)	d. customer service e. diversity in the workplace f. flexibility and adaptability g. interpersonal skills h. leadership and responsibility i. punctuality and attendance j. quality of work k. respect, cultural and diversity differences l. teamwork m. time management n. trust and ethical behavior o. work ethic 2. Develop a career plan that reflects career interests, pathways, and post-secondary options. 3. Create/revise a résumé, cover letter, and/or portfolio. 4. Demonstrate, analyze, research, and review the role of online job searching platforms and career websites to make informed decisions. 5. Understand the importance of assessing social media account content for professionalism. 6. Demonstrate and complete and/or review an on-line job application. 7. Understand and demonstrate interview skills to get the job to include: a. do's and don'ts for job interviews b. how to dress for the job 8. Demonstrate and create sample follow-up letters. 9. Understand the importance of the continuous upgrading of job skills as it relates to: a. certification, licensure, and/or renewal b. professional organizations/events c. industry associations and/or organized labor	Academics: 1.0 Communications: 2.1, 2.3, 2.4. 2.5 Career Planning & Management: 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.8, 3.9 Technology: 4.1, 4.2, 4.3, 4.5 Problem Solving & Critical Thinking: 5.1, 5.4 Responsibility & Flexibility: 7.2, 7.3, 7.4, 7.7 Ethics & Legal Responsibilities: 8.3, 8.4, 8.5 Leadership & Teamwork: 9.1, 9.2, 9.3, 9.4, 9.6, 9.7 Technical Knowledge & Skills: 10.1, 10.3, 10.12 Demonstration & Application: 11.1, 11.2, 11.5 **CTE Pathway:** B4.7
I. CERTIFICATION EXAM REVIEW	1. Review test from study guides, and understand the exam objectives. 2. Explain the importance of test taking strategies to successfully pass exam, to include:	**Career Ready Practice:** 1, 2, 4, 5

Understand, evaluate, and demonstrate the skills required to take written and simulated certification exams. (20 hours)	a. reading instructions carefully b. time management c. note taking d. using the process of elimination e. using keywords from the question in your answer 3. Create a study plan. 4. Take a simulated online certification exam. 5. Assess test outcomes and identify areas requiring further testing, if necessary. 6. Explain the registration process to take the CompTia Security+ Certification Exam to include the exam-testing environment.	**CTE Anchor:** Academics: 1.0 Communications : 2.1, 2.2, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.1, 5.4 Technical Knowledge & Skills: 10.1, 10.2 **CTE Pathway:** B6.1

ACKNOWLEDGEMENTS

Thanks to the following individuals for their contributions in developing and editing this curriculum:

Ana Martinez, Trung Le, Silvia Quijada, and Robert Yorgason

Approved by: Renny L. Neyra, Executive Director