Tom P. Haney Technical College
Computer Systems & Information Technology (CSIT)
Program Type: Career Preparatory - Information Technology
Program Number: Y100200
Program Length: 900 hours

Class of '25-'26
Instructors: Mr. Daniel Sanford
sanfod@bay.k12.fl.us
Mr. Andrew Farmer
farmea@bay.k12.fl.us
(850) 767-5500 ext. 212-3131
ext. 212-3123
Monday through Friday; 7am to 12pm

OCP D – Computer Security Technician (CTS0069 300 Hours)

CompTIA TestOut Security Pro V8.0 (SY0-701)

COURSE DESCRIPTION

CompTIA is here to help you get the tech career you deserve with industry-leading certifications, courses, and expert knowledge. Today's job market demands individuals have demonstrable skills, and the information and activities in this course can help you build your cybersecurity skill set so that you can confidently perform your duties in any entry-level computer security technician role.

With CompTIA Security+, you'll understand the core skills needed to succeed on the job – and employers will notice too. CompTIA Security+ represents the latest and greatest in cybersecurity, covering the most in-demand skills related to current threats, automation, zero trust, IoT, risk – and more. CompTIA Security+ is compliant with ISO 17024 standards and approved by the U.S. DoD to meet Directive 8140.03M requirements. Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.

GRADING SCALE	OCP A WEIGHTED GRADE CALCULATION
A = 90-100%	CertMaster Lab Assignments = 25%
B = 80-89%	CertMaster Formative Assessments (Exams) = 10%
C = 70-79%	Summative Assessment (Canvas Exams) = 50%
F = 0-69%	Employability Skills = 15%

NOTE: Your weighted grade in each OCP must be greater than or equal to 80% to pass this course.

COURSE ORGANIZATION

This instructor-led course utilizes online course materials via haney¡instructure¡com (Canvas) and CompTIA's.TestOut.Security.Pro.V❹16 course material meaning that most activities can be completed online. All email correspondence with students will take place via their student email account. Students need to check this email daily for information from the instructor and the college. Students will also need to log into Canvas daily to check for new announcements regarding any changes or information about instructional material, assignments. and activities and to upload their completed lab assignments. After every course chapter, students will complete the associated summative chapter exam. These assessments will have a time limit and allow for only one submission. Students will also complete hands-on labs to practice the skills learned in the lesson.

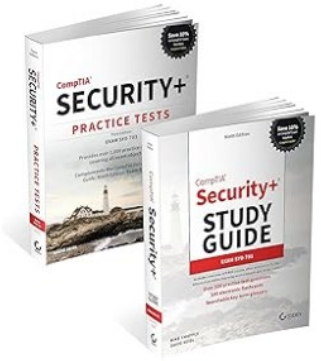
This course can prepare you for the CompTIA Security+ (SY0-701) certification examination and a job role in computer cybersecurity. It utilizes a learning progression model to help you learn and build skills related to the course objectives and job task requirements. This learning methodology uses a series of steps to contextualize what you're learning, elaborate on areas where additional instruction is needed, and provide relevance through practice and personalized feedback. You'll then apply what you learned and demonstrate the skills you've gained through a series of lab activities and quizzes.

On course completion, you will be able to:

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology.
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

REQUIRED TEXTS:

No textbook is required for this class. Below is a list of recommended reference books that can help you in class and/or study for your certification exam.



CompTIA Security+ Certification Kit: Exam SY0-701 7th Edition by Mike Chapple and David Seidl; ISBN-13 ： 978-1394211449

ATTENDANCE POLICY

Students are required to attend class Monday through Friday, 7 AM to 12 PM. Class will begin at 7 AM with morning announcements and chapter reviews. It is important to be on time each day. College policy requires that a student be present 90% of the enrollment period designated hours. For CSIT, an enrollment period is 450 hours (one semester), therefore a student is allowed to miss 45 hours per semester. If a student exceeds 45 hours absence in an enrollment period, the student will be withdrawn from the CSIT program. This policy is not negotiable. Withdrawal exceptions cannot and will not be made for any student exceeding their allowed 10% absences. Students will be responsible for any missed work or assignments. NOTE: Military veterans or dependents using VA assistance have a different attendance policy. Please refer to the Tom P. Haney Student Handbook for more information on Haney's attendance policy.

ACADEMIC INTEGRITY

Tom P. Haney Technical College is committed to providing an honest and fair learning environment and to preparing students for academic and career success. Students are expected to recognize and uphold standards of intellectual and academic integrity. Integrity means being honest, responsible, respectful, and ethical, and applies whether working independently or collaboratively, regardless of the level of supervision. Integrity and honesty are a part of professionalism and demonstrate employability skills. The College will not tolerate any dishonest practices, including plagiarism, in the academic environment.

ELECTRONIC DEVICE POLICY

- Cell phones are not allowed to be used in the classroom. Students will be able to store their cell phones in a cell phone locker in the back of the classroom. Students are allowed to use their cell phones outside of class when on breaks or at lunch. Please refer to Haney's Student Handbook for more information on our cell phone policy.
- Personal laptops and tablets are not allowed to be used in the classroom. If laptops are required in this course, the college will provide one per student. Students are not allowed to take their assigned laptops home for any reason and must be placed in the laptop cart at the end of the day.

FOOD AND DRINK POLICY

Food is not allowed in the classroom. Snacks and lunches are to be eaten in the Bldg 3 atrium or outside while on breaks. Water is allowed in class provided you use a container with a secured top such as water bottles, Tervis or Stanley tumblers. Fast food cups and aluminum cans are not considered secure containers. If you doubt your drink container is allowed, then ask your instructor.

STUDENTS WITH DISABILITIES STATEMENT

If you have a disability that may affect your academic performance and are seeking accommodations, it is your responsibility to inform the Student Services (Bldg 1). You may contact Ms. Sandy Johnson at (850) 767-5500 ext. 767-5527 if you have any questions concerning accommodations and services. You may visit the Disability Services webpage or the Disability Services section of the Student Handbook to learn more about accommodations and special services. It is important to request accommodations early enough to give the Counseling Services office adequate time to consider your request and recommend reasonable accommodations. Students are encouraged to initiate the request process as soon as possible at the beginning of a semester or class. Accommodations are not retroactive and only become active after all required documents are submitted. Instructors will provide necessary accommodations based solely on the recommendations of the Disability Services office.

COURSE CHAPTERS/MODULES

Listed below are the current set of chapters/modules and their associated competencies outlined for this course. Each module is an integrated unit of learning that consists of content, activities and assessments that target a specific set of competencies. The size of the module will depend on the depth of knowledge and skill needed to master the competency.

Module 1.0 – Security Concepts	• Examine the fundamental principles and goals of information security. • Identify and describe various types of security controls and their roles in risk management.

	• Explore common security threats and basic countermeasures to defend against them. • Practice applying knowledge in a realistic, interactive security simulator. • Develop your ability to analyze security scenarios and recommend appropriate controls.
Module 2.0 – Threats, Vulnerabilities, and Migrations	• Identify and explain common types of cyberattacks and the tactics attackers use. • Recognize various social engineering strategies and understand how to defend against them. • Describe different categories of malware and the damage they can cause. • Evaluate weaknesses and vulnerabilities within systems and organizations. • Apply basic mitigation techniques to reduce risk and enhance security posture.
Module 3.0 – Cryptographic Solutions	• Identify and explain common types of cyberattacks and the tactics attackers use. • Recognize various social engineering strategies and understand how to defend against them. • Describe different categories of malware and the damage they can cause. • Evaluate weaknesses and vulnerabilities within systems and organizations. • Apply basic mitigation techniques to reduce risk and enhance security posture.
Module 4.0 – Identity and Access Management	• Compare and contrast different access control models and explain their use cases. • Identify techniques and technologies for authentication, including methods for strengthening user credential security.

Module 5.0 – Network Architecture	• Explain authorization practices, including how permissions and policies govern access to resources. • Describe how directory services such as Active Directory and Linux-based systems manage users and groups. • Assess methods for enabling secure remote access and network authentication in distributed environments. • Explore core components and structure of enterprise-level networks. • Identify various security appliances and their roles in network defense. • Examine the implementation and benefits of screened subnets, firewalls, and VPNs. • Analyze access control mechanisms and network device vulnerabilities. • Assess threats associated with switch and router security, as well as network applications.
Module 6.0 – Resiliency and Site Security	• Recognize common physical threats and develop strategies to bolster site security. • Examine monitoring and reconnaissance techniques used to identify vulnerabilities. • Explore the use and configuration of intrusion detection systems to spot and respond to suspicious activities. • Gain hands-on experience with protocol analyzers for network traffic analysis. • Analyze different types of network and password attacks and learn how to effectively defend against them.

Module 7.0 – Vulnerability Management	• Explore the purpose and process of identifying and managing system vulnerabilities. • Perform vulnerability scans and interpret their results to inform security decisions. • Examine techniques for alerting and continuous monitoring of security threats. • Investigate methodologies and tools used in penetration testing. • Apply best practices to remediate identified vulnerabilities and strengthen organizational security.
Module 8.0 – Network and Endpoint Security	• Strengthen core systems by applying industry-standard operating system hardening techniques. • Secure file servers to protect sensitive information from unauthorized access or loss. • Evaluate and reinforce Linux host security measures specific to open-source environments. • Identify common wireless threats and deploy effective countermeasures to protect network communications. • Recognize best practices in application and web security, including secure development and defense against attacks.
Module 9.0 – Incident Response	• Examine the key phases and best practices of effective incident response and mitigation. • Explore techniques and tools for comprehensive log management and analysis. • Learn the fundamentals of digital forensics in the context of investigating security incidents.

	• Understand the importance of redundancy and how it supports business continuity. • Develop the skills to implement and manage reliable backup and restore strategies.
Module 10.0 – Protocol, App, and Cloud Security	• Explain the fundamentals of host virtualization and identify associated security considerations. • Describe virtual networking concepts and evaluate common threats and countermeasures. • Analyze the benefits and challenges associated with deploying cloud services in an organization. • Recognize key security approaches for managing mobile devices and enforcing BYOD policies. • Identify security risks unique to embedded and specialized systems, as well as best practices for email security.
Module 11.0 – Security Governance Concepts	• Identify the roles and importance of policies, standards, and procedures in organizational security. • Explain the processes and benefits of effective change management in security environments. • Describe the key concepts and advantages of leveraging automation and orchestration in security operations. • Evaluate how governance concepts support risk management and regulatory compliance. • Apply best practices for implementing and maintaining a resilient security framework within an organization.

Module 12.0 – Risk Management	• Understand the key steps and concepts involved in formal risk management processes. • Explore best practices for managing relationships with third-party vendors and minimizing associated risks. • Learn how to conduct and interpret audits and assessments within an organization. • Identify methods to integrate risk management with business objectives and compliance requirements. • Develop strategies to continuously monitor, review, and enhance risk management efforts.
Module 13.0 – Data Protection and Compliance	• Identify types of sensitive information and understand their classification. • Recognize the key requirements of major data protection and compliance regulations. • Explore best practices for handling, storing, and sharing sensitive data. • Evaluate how personnel policies can impact an organization's data protection efforts. • Apply compliance-focused decision-making in scenarios likely to arise in your workplace.

NOTE: This syllabus may change at the instructor's discretion. It is the responsibility of the student to record changes.