**Continuing Education**
1717 S. Chestnut Ave.
Fresno, CA 93702-4709
(800) 372-5505
https://ce.fresno.edu

# TEC-52 – IT Cyber Security Professional with CompTIA Security+ Certificate Program with Externship

## Professional Education Course Syllabus

**Program includes National Certification & an Externship Opportunity**

**Course Contact Hours: 36**

**The IT Cyber Security Professional with CompTIA Security+**

Computer Technology Industry Association (CompTIA) Security+ training designates knowledgeable professionals in the field of IT security. As an international, vendor-neutral credential, CompTIA Security+ certification ensures successful students gain competency in network security, compliance and operational security, common/possible threats and vulnerabilities, application, data and host security, access control and identity management as well as cryptography. Earning CompTIA Security+ Certification signifies to employers that candidates will apply their knowledge of security concepts, tools and procedures to prevent security breaches, react accordingly to any security incidents and anticipate further security risks in order to effectively guard against them.

**The IT Cyber Security Professional with CompTIA Security+ Program**

The CompTIA Security+ course provides students with the basic knowledge and skills necessary to become an IT security professional. This course is designed to fully prepare students to sit for and pass the CompTIA Security+ certification exam. Students will gain the knowledge and skills necessary to identify risk and participate in risk mitigation activities as well as provide infrastructure, application, operational and information security. They will also acquire the knowledge necessary to apply security controls to maintain confidentiality, integrity and availability, as well as how to identify appropriate technologies and products. Finally, students will gain an awareness of applicable policies, laws and regulations with regard to IT security.

**Education and National Certifications**

- Students should have or be pursuing a high school diploma or GED.
- There are no state approval and/or state requirements associated with this program.
- There are several National Certification exams that are available to students who successfully complete this program:
  - **CompTIA Security+ (SY0-401) Certification Exam**
    - **NOTE: CompTIA® recommends candidates for the CompTIA A+ Exam have a minimum of two years of experience in IT administration with a focus on security**
  - **Microsoft Office Specialist (MOS) Certification Exam**.

**Program Objectives**

At the conclusion of this program, students will be able to:

- Describe common risks, vulnerabilities and controls
- Explain the triple constraint of information security

- Analyze and differentiate between types of malware and attacks
- Identify risks for common system hardware and peripherals
- Describe principles of software, data and host security
- Implement OS hardening procedures
- Identify common types of programming attacks
- Implement secure browsing practices
- Describe security vulnerabilities unique to virtualized environments
- Explain the purpose and vulnerabilities of common network devices
- Identify and secure common ports and protocols
- Describe security concerns unique to cloud computing environments
- Identify IDS and IPS solutions for host and network defense
- Describe differences in Access Control identification, authentication and authorization
- Identify various methods for access authentication
- Implement logical access control methods
- Distinguish between discretionary, mandatory, rule- and role-based access control
- Identify various types of risk management strategies
- Distinguish between management, technical and operational controls
- Calculate risk using subjective and objective measures
- Implement compliance audits for common security controls
- Explain the difference between penetration testing and vulnerability scanning
- Distinguish between symmetric and asymmetric forms of encryption
- Explain the use of public-key/private-key pairs to encrypt and decrypt a secure message
- Identify common security protocols (SSH, SSL, IPSec)
- Explain basic hashing concepts
- Distinguish between types of tickets, keys and certificate authorities in a PKI
- Distinguish between business continuity and disaster recovery objectives & timeframes
- Implement common backup rotation cycles
- Identify various types of redundant hardware and backup sites
- Recognize various types of environmental control solutions
- Identify RAID configurations for common availability and redundancy requirements
- Analyze and distinguish between forms of social engineering
- Describe the principles of operational security
- Identify common personnel security policies
- Describe data reminisce and secure disposal practices
- Explain common CIRT roles and responsibilities
- Use Microsoft Office

**National Certification**

Upon successful completion of this program, students would be eligible to sit for the CompTIA Security+ Certification Exam from CompTIA® and the Microsoft Office Specialist (MOS) exam. Although there are no state approval, state registration or other state requirements for this program, students who complete this program will be prepared and are eligible to sit for this national certification exam. Students who complete this program are encouraged to complete the externship option with their program. Students who complete this program can and do sit for the MOS national certification exams and are qualified, eligible and prepared to do so.

**Externship / Hands on Training / Practicum**

Although not a requirement, once students complete the program, they have the ability to participate in an externship and/or hands on practicum so as to practice the skills necessary to perform the job

requirements of a professional in this field. Students will be assisted with completing a resume and/or other requirements necessary to work in this field. All students who complete this program are eligible to participate in an externship and will be placed with a participating organization near their location.

**IT Cyber Security Professional with CompTIA S+ Program Detailed Student Objectives:**

**INTRODUCTION TO COMPUTER SECURITY**

- Explain the triple constraint of information security
- Describe common risks, vulnerabilities, and controls
- Differentiate between types of malware and attacks
- Identify risks for common system hardware and peripherals
- Explain common botnet uses for profit and attack

**SOFTWARE SECURITY**

- Implement OS hardening procedures
- Identify common types of programming attacks
- Describe principles of software, data, and host security
- Describe security vulnerabilities unique to virtualized environments
- Implement secure browsing practices

**NETWORK SECURITY**

- Explain the purpose and vulnerabilities of common network devices
- Describe security concerns unique to cloud computing environments
- Identify common ports and protocols
- Identify IDS and IPS solutions for host and network defense
- Describe vulnerabilities present in mobile and wireless data transport

**ACCESS CONTROL**

- Describe the differences between identification, authentication, and authorization in access control
- Identify various methods for access authentication
- Implement logical access control methods
- Distinguish between discretionary, mandatory, rule-based, and role-based access control implementations

**AUDITING, VULNERABILITY, AND RISK ASSESSMENT**

- Identify various types of risk management strategies
- Distinguish between management, technical, and operational controls
- Explain the difference between penetration testing and vulnerability scanning
- Calculate risk using subjective and objective measures
- Implement compliance audits for common security controls
- Explain the role of vulnerability management in discovering and mitigating security threats

**ENCRYPTION AND PKI**

- Distinguish between symmetric and asymmetric forms of encryption
- Explain the use of public and private key pairs to encrypt and decrypt a secure message
- Identify common security protocols
- Explain basic hashing concepts
- Distinguish between types of tickets, keys, and certificate authorities in a PKI

**DISASTER RECOVERY AND BUSINESS CONTINUITY**

- Distinguish between business continuity and disaster recovery objectives / timeframes
- Implement common backup rotation cycles

- Identify common security protocols
- Identify various types of redundant hardware and backup sites
- Recognize various types of environmental control solutions
- Identify RAID configurations for common availability and redundancy requirements

**ORGANIZATIONAL POLICIES AND PROCEDURES**

- Distinguish between forms of social engineering
- Describe the principles of operational security
- Identify common personnel security policies
- Describe data remanence and secure disposal practices
- Explain common CIRT roles and responsibilities

**MICROSOFT OFFICE Module**

- Use an integrated software package, specifically the applications included in the Microsoft Office suite
- Demonstrate marketable skills for enhanced employment opportunities
- Describe proper computer techniques for designing and producing various types of documents
- Demonstrate the common commands & techniques used in Windows desktop
- List the meaning of basic PC acronyms like MHz, MB, KB, HD and RAM
- Use WordPad and MSWord to create various types of documents
- Create headings and titles with Word Art
- Create and format spreadsheets, including the use of mathematical formulas
- Demonstrate a working knowledge of computer database functions, including putting, processing, querying and outputting data
- Define computer terminology in definition matching quizzes
- Use the Windows Paint program to alter graphics
- Use a presentation application to create a presentation with both text and graphics
- Copy data from one MS Office application to another application in the suite
- Use e-mail and the Internet to send Word and Excel file attachments
- Demonstrate how to use the Windows Taskbar and Windows Tooltips
- Explain how copyright laws pertain to data and graphics posted on the Internet
- Take the college computer competency test after course completion
- Follow oral and written directions and complete assignments when working under time limitations

## Fresno Pacific University Student Learning Outcomes (FPU-SLO)

| | |
|---|---|
| FPU-SLO 1 | **Student Learning Outcomes Oral Communication:** Students will *exhibit* clear, engaging, and confident oral communication – in both individual and group settings – and will critically *evaluate* content and delivery components. |
| FPU-SLO 2 | **Written Communication:** Students will *demonstrate* proficient written communication by *articulating* a clear focus, *synthesizing* arguments, and utilizing standard formats in order to *inform* and *persuade* others. |
| FPU-SLO 3 | **Content Knowledge:** Students will *demonstrate* comprehension of content-specific knowledge and the ability to apply it in theoretical, personal, professional, or societal contexts. |
| FPU-SLO 4 | **Reflection**: Students will *reflect* on their personal and professional growth and *provide evidence* of how such reflection is utilized to manage personal and vocational improvement. |

| | |
|---|---|
| FPU-SLO 5 | **Critical Thinking:** Students will *apply* critical thinking competencies by *generating* probing questions, *recognizing* underlying assumptions, *interpreting* and *evaluating* relevant information, and *applying* their understandings to new situations. |
| FPU-SLO 6 | **Moral Reasoning:** Students will *identify* and *apply* moral reasoning and ethical decision-making skills, and *articulate* the norms and principles underlying a Christian world-view. |
| FPU-SLO 7 | **Service**: Students will *demonstrate* service and reconciliation as a way of leadership. |
| FPU-SLO 8 | **Cultural and Global Perspective:** Students will *identify* personal, cultural, and global perspectives and will employ these perspectives to *evaluate* complex systems. |
| FPU-SLO 9 | **Quantitative Reasoning**: Students will accurately *compute* calculations and symbolic operations and *explain* their use in a field of study. |
| FPU-SLO 10 | **Information Literacy:** Students will *identify* information needed in order to fully understand a topic or task, *explain* how that information is organized, *identify* the best sources of information for a given enquiry, *locate* and critically *evaluate* sources, and accurately and effectively *share* that information. |

## Continuing Education Student Learning Outcomes (CE-SLO)

| | |
|---|---|
| CE-SLO 1 | Demonstrate proficient written communication by articulating a clear focus, synthesizing arguments, and utilizing standard formats in order to inform and persuade others, and present information applicable to targeted use. |
| CE-SLO 2 | Demonstrate comprehension of content-specific knowledge and the ability to apply it in theoretical, personal, professional, or societal contexts. |
| CE-SLO 3 | Reflect on their personal and professional growth and provide evidence of how such reflection is utilized to manage personal and professional improvement. |
| CE-SLO 4 | Apply critical thinking competencies by generating probing questions, recognizing underlying assumptions, interpreting and evaluating relevant information, and applying their understandings to the professional setting. |
| CE-SLO 5 | Reflect on values that inspire high standards of professional and ethical behavior as they pursue excellence in applying new learning to their chosen field. |
| CE-SLO 6 | Identify information needed in order to fully understand a topic or task, organize that information, identify the best sources of information for a given enquiry, locate and critically evaluate sources, and accurately and effectively share that information. |