Columbia Southern University – Dept. of Continuing Education
21982 University Lane • Orange Beach, AL 36561
http://www.columbiasouthern.edu/
Contact: Laurie Coleman │800.977.8449 x1840│laurie.coleman@columbiasouthern.edu

Education & Training Plan
IT Cyber Security Professional with CompTIA Security+ Certificate Program with Externship
Columbia Southern University (CSU)

Student Full Name: _____

Start Date: _____ End Date: _____

Program includes National Certification & an Externship Opportunity
Mentor Supported

IT Cyber Security Professional with CompTIA Security+ Certificate Program with Externship

Course Code:	CSU-IT-CTS
Program Duration:	6 Months
Course Contact Hours:	375
Student Tuition:	$3,999

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 Professioanl 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 Columbia Southern University 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 at Columbia Southern University 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. Columbia Southern University works with each student to complete the exam application and register the student to take their national certification exam.

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. Columbia Southern University works with national organizations and has the ability to place students in externship opportunities nationwide.

Columbia Southern University contact: If students have any questions regarding this program including national certification and externships**, they should call Laurie Coleman at 800.977.8449 x1840 or via email at laurie.coleman@columbiasouthern.edu.**

Note: No refunds can be issued after the start date published in your Financial Award document.

About Columbia Southern University!

Welcome to Columbia Southern University!
OUR MISSION: Columbia Southern University provides diverse learning experiences and affordable, flexible distance education programs at the certificate, undergraduate, and graduate levels to a global student body, delivered by qualified, student-centered faculty committed to teaching and student learning. The University is dedicated to providing exceptional academic and student support services.

OUR VISION: The Vision of Columbia Southern University is to change and improve lives through higher education by enabling students to maximize their professional and personal potential.

The Continuing Education Department at Columbia Southern University is committed to a program of public service, outreach and continuing education by sharing resources with the workforce to enhance the intellectual capital of all those in need or desire lifelong learning and development. **http://www.columbiasouthern.edu/online-degree/continuing-education**

Columbia Southern University and Pearson Education
Columbia Southern University's eLearning programs were developed in partnership with Pearson Education to produce the highest quality, best-in-class content and delivery necessary to enhance the overall student learning experience, boost understanding and ensure retention. Pearson Education is the premier content and learning company in North America offering solutions to the higher education and career training divisions of colleges and universities across the country aimed at driving quality education programs to ensure student success. Please visit us at **www.pearson.com**.

About Pearson Education
Welcome to Pearson. We have a simple mission: to help people make more of their lives through learning. We are the world's leading learning company, with 40,000 employees in more than 80 countries helping people of all ages to make measurable progress in their lives. We provide a range of education products and services to institutions, governments and direct to individual learners, that help people everywhere aim higher and fulfil their true potential. Our commitment to them requires a holistic approach to education. It begins by using research to understand what sort of learning works best, it continues by bringing together people and organizations to develop ideas, and it comes back round by measuring the outcomes of our products.

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

Note: This program can be completed in 6 months. However, students will have online access to this program for a 24-month period.

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

Note: Although the Microsoft Office Module is not required to successfully complete this program, students interested in pursuing free Microsoft MOS certification may want to consider completing this Microsoft Office Module at no additional cost.

System Requirements:

Windows Users:

- Windows 8, 7, XP or Vista
- 56K modem or higher
- Soundcard & Speakers
- Firefox, Chrome or Microsoft Internet Explorer

Mac OS User:

- Mac OS X or higher (in classic mode)
- 56K modem or higher
- Soundcard & Speakers
- Apple Safari

iPad Users:

- Due to Flash limitations, eLearning programs are NOT compatible with iPads

Screen Resolution:

- We recommend setting your screen resolution to 1024 x 768 pixels.

Browser Requirements:

- System will support the two latest releases of each browser. When using older versions of a browser, users risk running into problems with the course software.
- Windows Users: Mozilla Firefox, Google Chrome, Microsoft Internet Explorer
- Mac OS Users: Safari, Google Chrome, Mozilla Firefox

Suggested Plug-ins:

- Flash Player
- Real Player
- Adobe Reader
- Java