Columbia Southern University
21982 University Lane, Orange Beach, Alabama 36561
http://www.columbiasouthern.edu
Contact: Laurie Coleman| (800) 977-8449 x1840 | laurie.coleman@columbiasouthern.edu

Education & Training Plan
Computer Security Technician (CompTIA Security+ and Network+) Certification Program with Externship

Student Full Name: _____

Start Date: _____ End Date: _____

Program includes National Certification & an Externship Opportunity
Mentor Supported

Columbia Southern University Program with Externship

Course Code:	CSU-IT-CSTSN
Program Duration:	6 Months
Course Contact Hours:	375
Student Tuition:	$3,999.00

Computer Security Technician (CompTIA Security+ and Network+)

The Computer Security Technician CompTIA Security+ program is designed to prepare students to function as computer professionals in multiple technical, business, and healthcare settings. Sec+ technicians serve many technical support and IT operation roles with job titles such Systems Administrator, Security Administrator, Junior IT/Auditor, Penetration Tester, and Security Consultant as well as Network Field Technician, Help Desk Technician, and Network Support Specialist.

Computer Security Technician (CompTIA Security+ and Network+) Program

The Computer Security Technician CompTIA Security+ Program is to prepare students to support the IT infrastructure through installing and configuring systems to secure applications, networks, and devices as well as perform threat analysis and respond with appropriate mitigation techniques. It also prepares students to learn to manage, maintain, troubleshoot, install, operate, and configure basic network infrastructure as well as describe networking technologies, understand basic design principles, adhere to wiring standards, and use testing tools.

Education and National Certifications

- Students should have or be pursuing a high school diploma or GED.

- Students who complete this program can sit for the following exams:
  - **CompTIA Security+ Certification (Exam SY0-601)**
  - **CompTIA Network+ Certification (Exam N10-007)**

Program Objectives

- Fundamental networking concepts, such as protocol reference models, network devices and theory, network topologies, and network services
- WAN technologies including ISDN, Frame Relay, PPP, MPLS, Metro-Ethernet, and more
- How to work with different network cables and connectors
- Network design considerations
- Switch and wireless LAN configuration
- IPv4 and IPv6 addressing
- Routing fundamentals including RIP, OSPF, IS-IS, and BGP routing protocols; HSRP and VRRP; route aggregation; and routing metrics
- Unified communications, Voice over IP (VoIP), video, and Qos
- Virtualized devices, storage area network technologies (SAN), and cloud technologies
- Network security attacks, vulnerabilities, policies, defenses, and counter-measures
- Network monitoring tools and analysis, configuration management, and best practices
- Network troubleshooting
- Detect various types of compromise and have an understanding of penetration testing and vulnerability scanning concepts
- Install, configure, and deploy network components while assessing and troubleshooting issues to support organizational security
- Implement secure network architecture concepts and systems design
- Install and configure identity and access services, as well as management controls
- Implement and summarize risk management best practices and the business impact
- Install and configure wireless security settings and implement public key infrastructure
- Be familiar with every objective on the CompTIA Security+ Exam
- Employ tips to prepare for and pass the exam

National Certification

Students who complete the Columbia Southern University Computer Security Technician (CompTIA Security+ and Network+) program will be prepared to sit for the CompTIA Security+ Certification (Exam SY0-601) and CompTIA Network+ Certification (Exam N10-007) national certification exam(s). In order to work as a Computer Security Technician (CompTIA Security+ and Network+), many states nationwide are requiring that learners achieve national certification prior to working in that state. Students who complete this program are encouraged to complete the practical/clinical externship option with their program. This comprehensive program is designed to prepare students to sit for CompTIA Security+ Certification (Exam SY0-601) and CompTIA Network+ Certification (Exam N10-007) exam(s). Students who complete this program can and do sit for the CompTIA Security+ Certification (Exam SY0-601) and CompTIA Network+ Certification (Exam N10-007) national certification exam(s) 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. The institution 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 of Columbia Southern University 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.

Computer Security Technician (CompTIA Security+ and Network+) Program Detailed Student Objectives:

COMPTIA NETWORK+ MODULE

PROTOCOLS AND REFERENCE MODELS

- Explain OSI Model Layers
- Explain the TCP/IP Suite

EXPLAINING PROPERTIES OF NETWORK TRAFFIC

- Explain Media Types and Access Methods
- Deploy Ethernet Standards
- Configure and Monitor Network Interfaces

INSTALLING AND CONFIGUTING SWITCHED NETWORKS

- Install and Configure Hubs and Bridges
- Install and Configure Switches
- Compare and Contrast Network Topologies
- Compare and Contrast Network Types

CONFIGURING IP NETWORKS

- Configure IPv4 Addressing Components
- Test IP Interfaces with Command Line Tools
- Configure IPv4 Subnets
- Configure Private and Public IPv4 Addressing Schemes
- Configure IPv6 Addressing Components
- Configure DHCP Services

REINSTALLING AND CONFIGURING ROUTED NETWORKS

- Explain Characteristics of Routing
- Install and Configure Routers

CONFIGURING AND MONITORING PORTS AND PROTOCOLS

- Explain the Uses of Ports and Protocols
- Use Port Scanners and Protocol Analyzers
- Explain the Use of Name Resolution Services
- Configure DNS and IPAM Services

EXPLAINING NETWORK APPLICATION AND STORAGE SERVICES

- Explain the Uses of Network Applications
- Explain the Uses of Voice Services and Advanced Networking Devices
- Explain the Uses of Virtualization and Network Storage Services

- Summarize the Concepts of Cloud Services

MONITORING AND TROUBLESHOOTING NETWORKS

- Monitor Network Interfaces and Logs
- Explain Network Troubleshooting Methodology
- Troubleshoot Common Network Services Issues

EXPLAINING NETWORKING ATTACKS AND MITIGATIONS

- Summarize Common Networking Attacks
- Explain the Characteristics of VLANs
- Explain the Characteristics of NAT and Port Forwarding

INSTALLING AND CONFIGURING SECURITY DEVICES

- Install and Configure Firewalls and Proxies
- Explain the Uses of IDS/IPS and UTM

EXPLAINING AUTHENTICATION AND ACCESS CONTROLS

- Explain Authentication Controls and Attacks
- Explain the Uses of Authentication Protocols and Directory Services
- Explain the Uses of Port Security and NAC
- Implement Network Device Hardening
- Explain Patch Management and Vulnerability Scanning Processes

NETWORK CABLES AND CONNECTORS

- Deploy Structured Cabling Systems
- Deploy Twisted Pair Cabling Solutions
- Test and Troubleshoot Twisted Pair Cabling Solutions
- Deploy Fiber Optic Cabling Solutions

IMPLEMENTING AND TROUBLESHOOTING WIRELESS TECHNOLOGIES

- Install and Configure Wireless Technologies
- Troubleshoot Wireless Performance Issues
- Secure and Troubleshoot Wireless Connectivity

COMPARING AND CONTRASTING WAN TECHNOLOGIES

- Compare and Contrast WAN Core Service Types
- Compare and Contrast WAN Subscriber Service Types
- Compare and Contrast WAN Framing Service Types
- Compare and Contrast Wireless and IoT WAN Technologies

USING REMOTE ACCESS METHODS

- Use Remote Access VPNs

- Use Remote Access Management Methods

IDENTIFYING SITE POLICIES AND BEST PRACTICES

- Manage Networks with Documentation and Diagrams
- Summarize the Purposes of Physical Security Devices
- Compare and Contrast Business Continuity and Disaster Recovery Concepts
- Identify Policies and Best Practices

COMPTIA NETWORK+ EXAM PREPARATION

- Final Preparation
- How to Register for the Exam
- Study Strategies
- What to do on Exam Day
- Final Preparation Review

COMPTIA SECURITY+ MODULE

COMPARING SECURITY ROLESS AND SECURITY CONTROLS

- Compare and Contrast Information Security Roles
- Compare and Contrast Security Control and Framework Types

EXPLAINING THREAT ACTORS AND THREAT INTELLIGENCE

- Explain Threat Actor Types and Attack Vectors
- Explain Threat Intelligence Sources

PERFORMING SECURITY ASSESSMENTS

- Assess Organizational Security with Network Reconnaissance Tools
- Explain Security Concerns with General Vulnerability Types
- Summarize Vulnerability Scanning Techniques
- Explain Penetration Testing Concepts

IDENTIFYING SOCIAL ENGINEERING AND MALWARE

- Compare and Contrast Social Engineering Techniques
- Analyze Indicators of Malware-Based Attacks

SUMMARIZING BASIC CRYPTOGRAPHIC CONCEPTS

- Compare and Contrast Cryptographic Cipher
- Summarize Cryptographic Modes of Operation
- Summarize Cryptographic Use Cases and Weaknesses
- Summarize Other Cryptographic Technologies

IMPLEMENTING PUBLIC KEY INFRASTRUCTURE

- Implement Certificates and Certificate Authorities
- Implement PKI Management

IMPLEMENTING AUTHENTICATION CONTROLS

- Summarize Authentication Design Concepts
- Implement Knowledge-Based Authentication
- Implement Authentication Technologies
- Summarize Biometrics Authentication Concepts

IMPLEMENTING IDENTITY AND ACCOUNT MANAGEMENT CONTROLS

- Implement Identity and Account Types
- Implement Account Policies
- Implement Authorization Solutions
- Explain the Importance of Personnel Policies

IMPLEMENTING SECURE NETWORK DESIGNS

- Implement Secure Network Designs
- Implement Secure Switching and Routing
- Implement Secure Wireless Infrastructure
- Implement Load Balancers

IMPLEMENTING NETWORK SECURITY APPLIANCES

- Implement Firewalls and Proxy Servers
- Implement Network Security Monitoring
- Summarize the Use of SIEM

IMPLEMENTING SECURE NETWORK PROTOCOLS

- Implement Secure Network Operations Protocols
- Implement Secure Application Protocols
- Implement Secure Remote Access Protocols

IMPLEMENTING HOST SECURITY SOLUTIONS

- Implement Secure Firmware
- Implement Endpoint Security
- Explain Embedded System Security Implications

IMPLEMENTING SECURE MOBILE SOLUTIONS

- Implement Mobile Device Management
- Implement Secure Mobile Device Connections

SUMMARIZING SECURE APPLICATION CONCEPTS

- Analyze Indicators of Application Attacks
- Analyze Indicators of Web Application Attacks
- Summarize Secure Coding Practices
- Implement Secure Script Environments
- Summarize Deployment and Automation Concepts

IMPLEMENTING SECURE CLOUD SOLUTIONS

- Summarize Secure Cloud and Virtualization Services
- Apply Cloud Security Solutions
- Summarize Infrastructure as Code Concepts

EXPLAINING DATA PRIVACY AND PROTECTION CONCEPTS

- Explain Privacy and Data Sensitivity Concepts
- Explain Privacy and Data Protection Controls

PERFORMING INCIDENT RESPONSE

- Summarize Incident Response Procedures
- Utilize Appropriate Data Sources for Incident Response
- Apply Mitigation Controls

EXPLAINING DIGITAL FORENSICS

- Explain Key Aspects of Digital Forensics Documentation
- Explain Key Aspects of Digital Forensics Evidence Acquisition

SUMMARIZING RISK MANAGEMENT CONCEPTS

- Explain Risk Management Processes and Concepts
- Explain Business Impact Analysis Concepts

IMPLEMENTING CYBERSECURITY RESILIENCE

- Implement Redundancy Strategies
- Implement Backup Strategies
- Implement Cybersecurity Resiliency Strategies

EXPLAINING PHYSICAL SECURITY

- Explain the Importance of Physical Site Security Controls
- Explain the Importance of Physical Host Security Controls

ACING YOUR EXAM

- Understanding the Security+ Exam Structure
- Test Taking Strategies
- The Week Leading Up to You Exam
- What to Expect at the Testing Center

- Attaining and Maintaining Your Security+ Certification

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