IT-5100:
IT SECURITY SPECIALIST

MS-6000: MICROSOFT OFFICE SERIES III

IT-5011: SECURITY +

Program Code/Title: IT-5100: IT Security Specialist

Program Hours:	192 Hrs
Duration (wks):	12 weeks (3 months)
Program Cost:	$2300

Core Courses:

- *MS-6000: Microsoft Office Series III*　　　　　　　　*96 Hours*
- *IT-5011: Security +*　　　　　　　　　　　　　　　*96 Hours*

Program Description:

The **IT Security Specialist** program is designed to help students prepare for the **Security+ (**SY0-401) exam administered by CompTIA. Students will learn to implement and monitor security on networks, applications, and operating systems, and how to respond to security breaches. This course is targeted toward an Information Technology (IT) professional who has networking and administrative skills in Windows-based TCP/IP networks and familiarity with other operating systems, such as OS X, Unix, or Linux, and who wants to further a career in IT by acquiring a foundational knowledge of security topics; prepare for the CompTIA Security+ Certification examination; or use Security+ as the foundation for advanced security certifications or career roles.

Students learn through hands-on labs, courseware review and demo activities, and recorded video lectures. Students receive on-going support and guidance from a team of instructors, advisors, and online mentors.

Upon successful completion of this program, students will be able to:

- identify the fundamental concepts of computer security.
- identify security threats and vulnerabilities.
- examine network security.
- manage application, data and host security.
- identify access control and account management security measures.
- manage certificates.
- identify compliance and operational security measures.
- manage risk.
- manage security incidents.
- develop business continuity and disaster recovery plans.

Core Exam (Security+) Topics covered include:

- Mitigating Threats
- Cryptography
- Peripheral Security
- Network Security
- Wireless Security
- Remote Access Security
- Vulnerability Testing and Monitoring

- Organizational Security
- Business Continuity
- Application and Messaging Security
- Authentication
- User- and Role-Based Security
- Public Key Infrastructure
- Ports and Protocol

Program Includes:

IT-5011 – Security+

IT-5011 Security+ is the primary course students will need in order to gain the skills and knowledge required to gain Security+ Certification. This course is targeted toward the information technology (IT) professional who has networking and administrative skills in Windows-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks and familiarity with other operating systems, such as Mac OS X, Unix, or Linux, and who wants to further a career in IT by acquiring a foundational knowledge of security topics. In this course, students will build on knowledge and experience with security fundamentals, networks, and organizational security as they acquire the specific skills required to implement basic security services on any type of computer network. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields. *Course Prepares Student for CompTIA Exam: SYO-401*

MS-6000 – Microsoft Office Series III

This set of courses will provide the range of skills needed to create professional-quality documents and effectively communicate and collaborate within an office environment. The content covered includes how to create, edit and enhance documents in Microsoft Word, how to organize, calculate and analyze information in Microsoft Excel, how to exchange information and manage your activities in Microsoft Outlook, and how to create effective and robust presentations in Microsoft PowerPoint. Additional skills will include how to create and format various types of diagrams with Microsoft Visio and how to collaborate effectively with the use of Office 365 Web Apps, OneDrive, and Skype for Business.

Core Certification:

CompTIA Security+   (CompTIA Exam: SYO—401)

About the Security+ Certification

Security+ Certification is the computer industry recognized credential that certifies the competency of a Network Security professional. The examination tests student's knowledge of security fundamentals, networks, and organizational security. It is sponsored by CompTIA - the Computing Technology Industry Association, and tests are administered by Prometric.

Skills Measured by the Security+ Exam

Key Objectives and skill sets measured by the **CompTIA Security+ Exam (SYO-401)** *include:*

- Explain general cryptography concepts
- Explain basic hashing concepts and map algorithms
- Explain and implement basic encryption applications and tools
- Explain core concepts of PKI
- Implement PKI and Certificate Services
- Identify security threats
- Assess security risks for system hardware and peripherals
- Implement OS hardening practice and procedures
- Identify, explain and implement ports and protocols
- Identify network elements and components
- Identify network security tools and apply them appropriately
- Identify best practices for Access Control and identify the best models
- Organize users and computers into appropriate security groups
- Apply file and print permissions
- Implement logical access control methods
- Summarize the different authentication models and deploy them appropriately

- Explain and apply physical security methods
- Establish application security
- Implement Security Applications
- Explain hardware virtualization
- Identify the vulnerabilities of wireless networking
- Use monitoring tools on systems and networks
- Compare and contrast various monitoring methodologies
- Evaluate proper logging procedures
- Conduct audits of system security settings
- Conduct assessments on risk mitigation
- Carry out vulnerability assessments
- Explain the use of penetration testing versus vulnerability scanning
- Explain redundancy planning and its components
- Implement disaster recovery procedures
- Execute appropriate incident response procedures
- Identify and explain applicable legislation and organizational policies
- Explain environmental controls
- Reduce the risk of social engineering

Description of Teaching Methodology

This program is delivered via **Remote Mentored Learning** (RML). Students can view the video content from anywhere with a high speed internet connection, and have access to an Online Mentor, who provides ongoing support throughout the program. This program is designed to be completed within a prescribed amount of time, with responsibilities for each course thoroughly outlined in order to pace the program effectively. In addition to viewing video content, students are engaged in skill-building labs and real-world exercises designed to translate what is learned into critical skill-building and preparation for entering a new career.

This multi-sensory learning method allows the student to control their learning schedule, the content covered, and the pace of the training while receiving one-on-one support from a qualified mentor.

Description of Instructional and Administrative Positions Related to this Program

This program is supported by a team of Student Services Representatives (*General and Technical Support*), and a primary Instructor (*Subject Matter Expert*).

- The **Primary Instructor** for this course must meet the following requirements:
    - Must have earned Security+ certification
    - Must have AT LEAST five (5) years of IT Experience
    - Must have Associates Degree or higher in related/relevant field of study

- Each **Student Services Representative** is required to hold a minimum of one (1) relevant and current certification related to disciplines taught by MedCerts. Each of these representatives provides general support services across a variety program topics/certifications (*Non-Instructional Support*). Each position also requires a minimum of an Associate's Degree in a related field, or three (3) years of related experience.

Equipment

MedCerts provides all required courseware, student guides, study guides and other program supplements and resources. In addition to the online video content, students will be provided access to all relevant labs and online/offline resources as necessary to complete the program.

Students must have (or have access to) a computer with high-speed internet (minimum 1.5Mbs), and a monitor with minimum screen resolution of 1024 X 768.

Careers

The IT Security Specialist program prepares students with the skills and certification necessary to accelerate their career in Information Technology. The following careers are examples of opportunities available to graduates of the program:

- *Security Architect*
- *Security Engineer*
- *Security Consultant/Specialist*
- *Information Assurance Technician*
- *Security Administrator*
- *Systems Administration*

- *IT System Administrator*
- *Application Systems Administrator*
- *IT Manager*
- *Technology Specialist*
- *Helpdesk Technician/Analyst*
- *Technical Support*