Course: **Security+**

Contact Hours: **30**

Pre-requisite: **A+ & Network+ / Equivalent**

Abstract

This course covers knowledge of security concepts, tools and procedures to react to security incidents, anticipating security risks and guarding against them

Target Audience

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

Learning outcomes

On completion of this course, learners will be able to:

1. Identify fundamental concepts of computer security.
2. Identify security threats and vulnerabilities
3. Describe network security
4. Implement managing application, data, and host security
5. Describe access control, authentication, and account management
6. Describe compliance & operational security
7. Perform basic risk management
8. Manage security incidents
9. Describe business continuity and disaster recovery planning

Course Content

1. **Security Fundamentals**
    - The Information Security Cycle
    - Information Security Controls
    - Authentication Methods
    - Cryptography Fundamentals
    - Security Policy Fundamentals

2. **Identifying Security Threats and Vulnerabilities**
    - Social Engineering
    - Malware
    - Software-Based Threats
    - Network-Based Threats
    - Wireless Threats and Vulnerabilities
    - Physical Threats and Vulnerabilities

3. **Managing Data, Application, and Host Security**
    - Manage Data Security
    - Manage Application Security
    - Manage Device and Host Security
    - Manage Mobile Security

4. **Implementing Network Security**
    - Configure Security Parameters on Network Devices and Technologies
    - Network Design Elements and Components
    - Implement Networking Protocols and Services
    - Apply Secure Network Administration Principles
    - Secure Wireless Traffic

5. **Implementing Access Control, Authentication, and Account Management**
    - Access Control and Authentication Services
    - Implement Account Management Security Controls

6. **Managing Certificates**
    - Install a CA Hierarchy
    - Enroll Certificates
    - Secure Network Traffic by Using Certificates
    - Renew Certificates
    - Back Up and Restore Certificates and Private Keys
    - Revoke Certificates
7. **Implementing Compliance and Operational Security**
    - Physical Security
    - Legal Compliance
    - Security Awareness and Training
    - Integrate Systems and Data with Third Parties

8. **Risk Management**
    - Risk Analysis
    - Implement Vulnerability Assessment Tools and Techniques
    - Scan for Vulnerabilities
    - Mitigation and Deterrent Techniques

9. **Troubleshooting and Managing Security Incidents**
    - Respond to Security Incidents
    - Recover from a Security Incident

10. **Business Continuity and Disaster Recovery Planning**
    - Business Continuity
    - Plan for Disaster Recovery
    - Execute DRPs and Procedures

Assessment Criteria

In order to achieve Learning Outcome…	The Learner must…
1. Identify fundamental concepts of computer security	Describe what is security Identify Security concepts
2. Identify security threats and vulnerabilities	Differentiate Threats vs Vulnerability Identify major threats Identify major Vulnerability Explain the impact of vulnerabilities
3. Describe network security	Identify components of a secure networks Identify methodology of securing a network Identify and contrast security tools (hardware and software) and protocols
4. Implement managing application, data, and host security	Define cryptography Define IDS, IPS and DMZ Define methods to harden a Host Summarize Virtualization Explain resiliency and automation
5. Describe access control, authentication, and account management	Identify physical access control Identify network access control Identify Remote Access and authentication Explain concepts of account management
6. Describe compliance & operational security	Define physical security Identify major compliance laws
7. Perform basic risk management	Define risk Outline vulnerability testing Explain and Outline the use of policies, procedures and plans Outline Business Impact Analysis
8. Manage security incidents	Identify incident response methodology Summarize Forensic concepts
9. Describe business continuity and disaster recovery planning	Define cold, warm and hot sites Define backups, cloud and network Identify concepts for creating a disaster recovery plan

Essential Learning Resources:
Textbook
CompTIA Security + Study Guide (Exam SY0-501)

Websites
http://www.comptia.org