Course Details – CompTIA Security+ Training

1.	Course Title	CompTIA Security+ Certification
2.	Type of Course	Technical
3.	Training Methodology	Classroom Visual/ Remote
4.	Skill Area	• Threats, Attacks & Vulnerabilities • Identity & Access Management • Technologies & Tools • Risk Management • Architecture & Design • Cryptography & PKI
5.	Duration (Days)	5 days / 40 hours
6.	Level of Certification	CompTIA Security+ Certification
7.	Certification Body (If Applicable)	CompTIA, the world's leading tech association, is a thought leader and an action leader. From our IT professional association to our leading certification programs, from our original research to our member communities and councils, our unparalleled programs set industry standards, foster skills development and generate knowledge and insight every day.
8.	Course Overview	CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them. Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.
9.	Prerequisites	• SPM / STPM • Diploma / Degree or Equivalent • CompTIA Network+ and two years of experience in IT administration with a security focus

10.	Course Objective	The CompTIA Security+ will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. The successful candidate will perform these tasks to support the principles of confidentiality, integrity, and availability.
11.	Learning Outcome	Security+ focuses on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection.
12.	Course content	Threats, Attacks, and Vulnerabilities • Indicators of Compromise • Critical Security Controls • Security Posture Assessment Tools • Incident Response Identity and Access Management • Cryptography • Public Key Infrastructure • Identification and Authentication • Identity and Access Services • Account Management Architecture and Design (1) • Secure Network Design • Firewalls and Load Balancers • IDS and SIEM • Secure Wireless Access • Physical Security Controls Architecture and Design (2) • Secure Protocols and Services • Secure Remote Access • Secure Systems Design • Secure Mobile Device Services • Secure Virtualization and Cloud Services Risk Management • Forensics • Disaster Recovery and Resiliency • Risk Management • Secure Application Development • Organizational Security

13.	Learning Activities	• Lecture • Practical Exercise • Case Studies • Learning Activities • Video Presentation
14.	Target Group	Systems Administrator Security Administrator Security Specialist Security Engineer Security Consultant Junior IT Auditor/ Penetration Tester Network Administrator Industry: IT Industry