austinfree.net

ACCESS IS POWER

ACCELERATE PROGRAM SUMMARY

According to the Texas Labor Market Information from the Strategic Workforce Assessment Program, Computer User Support Specialist & Network Computer System Administrator positions require no degree. Employment projected growth (2014-2024) is faster than average jobs at 9% to 13%, with an expected job openings of 150,500.

AUSTIN FREE- NET (AFN) will provide training for 180 participant to obtain COMPTIA IT Fundamental, A+, and /or Network +, or Security + Certifications to become Computer User Support Specialist or Network Computer System Administrators. At the end of these courses, the student will be prepared to take the national exams for certification.

All participants will take the IT Fundamentals and the A+ certification courses. These courses serve as the foundation for the other computer certification training. Students interested in pursuing the Network Computer System Administrative position will continue their learning to complete the Network + and Security + course work.   These certifications are the standard in establishing a successful career in the Information.

Courses

COMPTIA – IT Fundamentals & Prep Test, is a **33 hour** course focused on the basics understanding of computer components, operating systems, applications and networking principles.

CompTIA's A+ & Prep Test, is a two part course of **100 hours**. Fifty (50) hours for COMPTIA A+ part one- (901)+ test prep; and Fifty (50) hours for COMPTIA A+, part two –(902) + prep test. COMPTIA A+ courses are focused on computer repair.

CompTIA Network+ & Prep Test is a **60 hour** course which prepares students to operate as system and network administrators and understand topics which include but are not limited to: media and topologies, protocols, standards, network implementation, and network support.

CompTIA Security+ & Prep Test is a **62 hour** course which serves as a benchmark for best practices in IT security. This certification covers the essential principles for network security and risk management – making it an important stepping-stone of an IT security career.

COURSE OUTLINE

COMPTIA A+ course is a two-part course. **(100 hours)** (50 hours- Part 1- 901 & 50 hours- Part 2- 902)

 These courses cover computer hardware and computer software. Note computers require both hardware and software in order to function. In this course, students will install, upgrade repair configure, optimize troubleshoot, and perform preventative maintenance on basic personal computer hardware and operating systems. Students will work with Windows and different variants of Linux operating systems and install troubleshoot and update applications for each.

Students will:

- Identify the components of standard desktop personal computers.
- Identify fundamental components and functions of personal computer operating systems.
- Identify best practices followed by professional personal computer technicians.
- Install and configure computer components.
- Install and configure system components.
- Maintain and troubleshoot peripheral components.
- Troubleshoot System Components.
- Install and configure operating systems (windows, Linux)
- Maintain and troubleshoot installations of Microsoft Windows
- Identify Network Technologies
- Install and manage network connections.
- Support laptops and portable computing devices
- Support Printers
- Add users to Windows and Linux computers.
- Identify personal computer security concepts
- Support personal computer security

COMPTIA IT Fundamentals (33 hours)

The IT fundamentals certification developed and issued by the Computer Technology Industry Association (CompTIA). This certification displays basics understanding of computer components, operating systems, applications and networking principles. Students will be knowledgeable of:

- Core Components Hardware
- Peripherals and Components
- Operating Systems
- Software Applications
- Networking Technologies and Wireless Routers
- Network Sharing and Storage
- Mobile Devices
- Security Threats
- Security Best Practices
- Buying and Configuring a Workstation

- Computer Support and Backups
- Environmental and Safety Concepts
- Certification Testing Preparation

COMPTIA Network+ (Computer Networking) Certification   (60 hours)

The CompTIA Network+ course builds on your existing user-level knowledge and experience with personal computer operating systems and networks to present fundamental skills and concepts that you will use on the job in any type of networking career. If you are pursuing a CompTIA technical certification path, the

CompTIA A+ certification is an excellent first step to take before preparing for the CompTIA Network+ certification.

Upon completion of this course, students will be able to:
- Identify the basic components of network theory.
- Identify the major network communications methods.
- Identify network data delivery methods.
- List and describe network media and hardware components.
- Identify the major types of network implementations.
- Identify the components of a TCP/IP network implementation.
- Identify the major services deployed on TCP/IP networks.
- Identify the components of a LAN implementation.
- Identify the components of a WAN implementation.
- Identify major issues and technologies in network security.
- Identify the components of a remote network implementation.
- Identify major issues and technologies in disaster recovery.
- Identify major data storage technologies and implementations.
- Identify the primary network operating systems.
- Explore tools, methods, and techniques used in managing a network.
- Describe how to troubleshoot network issues.

CompTIA Security+ Certification (**62 Hours**) exam encompasses foundational information security principles for network security and enterprise risk management. This course will help you develop the knowledge and skills necessary to identify and mitigate risk, apply security controls to protect confidentiality, integrity, and availability, gain an understanding of typical security technologies, identify and troubleshoot security events and incidents, and understand the roles of policies, laws, and regulations. Topics include: cryptography, access control, and identity management. By the end of the course, students will have a firm grasp on application, information, infrastructure, and operational security principles.

The six core topics that will be covered in class include:

- Network Security
- Compliance and Operational Security
- Threats and Vulnerabilities
- Application, Data, and Host Security
- Access Control and Identity Management
- Cryptography