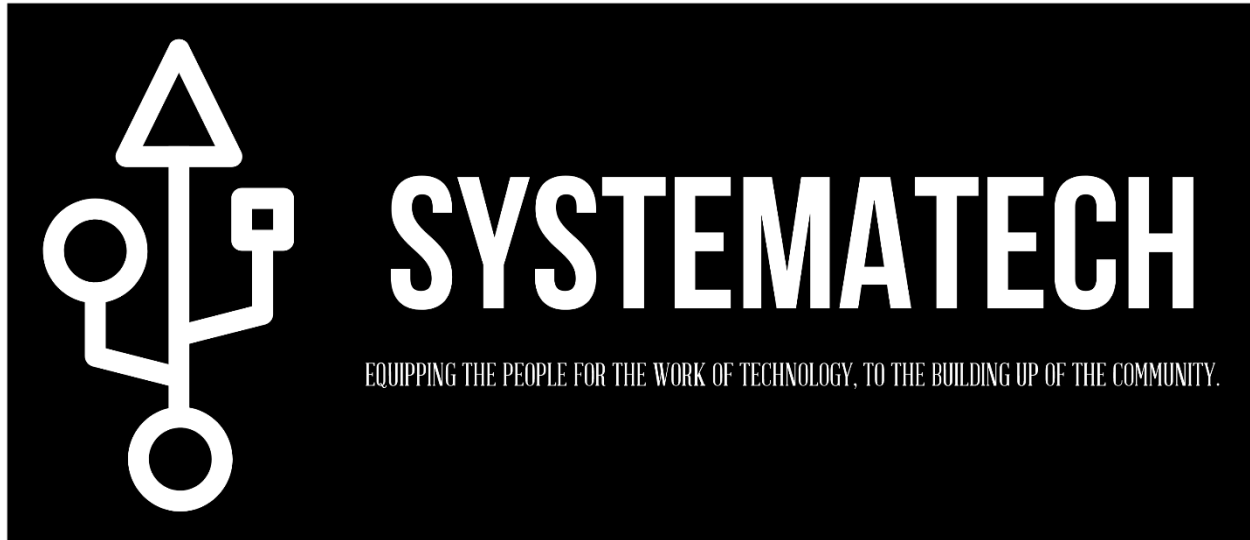


Exhibit IV. Catalog



Students are expected to be familiar with the information presented in this school catalog, with any supplements and addenda to the catalog, and with all school policies. By enrolling in SystemATech, students agree to accept and abide by the terms stated in this catalog and all school policies. If there is any conflict between any statement in this catalog and the enrollment agreement signed by the student, the enrollment agreement controls.

SYSTEMATECH

4123 Stone Pass Drive

Graniteville, South Carolina 29829

Telephone: (803)474-4407

Publication Date: May 5, 2020

Volume 1

Table of Contents

Mission Statement

Directory

Description of Facilities

Accrediting Agency

CHE Licensure Disclaimer

Job Placement Assistance

Transfer Credit

Program(s) Offered

Admission Policy

Important Calendar Dates (examples)

Holidays Observed

Attendance Policy & Class Participation

Tardiness

Makeup Work

Academic Performance & Completion Requirements

Maintenance of Student Records

Graduation Requirements

Progress Reports & Academic Probation and Suspension Policy

Grading Scale

Tuition

Cancellation & Refund Policy

Student Complaints

Directory

Name: President/CEO Ashley S. Felton

Name: Officer, Tammy Anthony

Name: Officer, Arnold Anthony

Name: Faculty, John Wray

Name: Faculty, Shereen Reeves

Name: Faculty, Steven Murray Jr

Name: Faculty, Malcolm Doe

Statement of Purpose

SystemATech exists to provide a quality skills education that will lead to new job opportunities, and a broadened personal horizon for each student. SystemATech seeks to unite many volunteers to help families through education, job-skills training, and career opportunity assistance; to witness men and women, young and old, reach their academic potential; and to help each program participant take the next steps in developing the skills necessary for meaningful employment and a rewarding life.

Description of Facilities

Our facility will be a classroom type location. The equipment our students will use are laptop computers. Our classroom size minimum is 5 students. Our maximum number of students is 20. Room and board options are currently unavailable through our organization.

Living Quarters

Systematech will not provide any living quarters or living assistance for current or future students.

South Carolina Commission on Higher Education

Licensed by the South Carolina Commission on Higher Education, 1122 Lady Street, Suite 300, Columbia, SC, 29201, telephone number 803-737-2260, and website address www.che.sc.gov. Licensure indicates only those minimum standards have been met; it is not an endorsement or guarantee of quality. Licensure is not equivalent to or synonymous with accreditation by an accrediting agency recognized by the US Department of Education.

Accrediting Agency

SystemATech is licensed by the South Carolina Commission on Higher Education to operate in the State of South Carolina. The Credit agencies is:

CompTIA located at 3500 Lacey Road, Suite 100- Downers Grove, IL 60515 (telephone 866-835-8021 / 630-678-8300). www.comptia.org.

ANSI located at 1899 L St NW 11 Floor, Washington, DC 20036 (telephone 202-293-8020) www.ansi.gov

Program(s) Offered



CompTIA A+ Certification - Exam 220-1001 - Core 1 Course Outline

Overview

The course shown here was designed for the new 220-1001 exam. CompTIA A+ certified professionals are proven problem solvers. They support today's core technologies from security to cloud to data management and more. CompTIA A+ is the industry standard for launching IT careers into today's digital world. It is the only industry recognized credential with performance-based items to prove pros can think on their feet to perform critical IT support tasks in the moment. It is trusted by employers around the world to identify the go-to person in end point management and technical support roles. CompTIA A+ is regularly re-invented by IT experts to ensure that it validates core skills and abilities demanded in the workplace.

The Official CompTIA® A+® Core 1 (Exam 220-1001) course provides the background knowledge and skills you will require to be a successful A+ technician. It will help you prepare to take the CompTIA A+ Core Series certification examination (exam number 220-1001), in order to become a CompTIA A+

Certified Professional.

Already have some IT experience?

Individuals with previous IT experience, should consider taking our Boot Camp A+ class that covers the content from both our A+ Hardware class and our A+ Operating System/Security class. That 10 days of material is delivered in a 5-day format and is supplemented with after-hours exam prep sessions that help fill in any gaps that you have. For more information on this classes schedule an appointment with us here:

[CompTIA A+ Certification – Boot Camp Training for 1001/1002](#)

***** NOTE: This class also available in eLearning Format *****

Too busy at work to miss 5 days out of the office to take this class? Consider the CompTIA On-Demand version of this course. Watch videos, take the same hands-on labs, access an online expert, and study at on your own time, at your own pace. For details on this alternative format, go to

CompTIA On-Demand A+ Certification Training CompTIA A+ Core 1 and Core 2 Includes live/online instruction from a certified CompTIA instructor, course materials, practice exams, 2 certification exams and complimentary lunch and refreshments.

Cost \$4995.00

8 weeks course

Hours: 198

***** Note Regarding Exam Preparation *****

Exam Prep Software

All of our CompTIA classes include access to web-based practice exams. CompTIA certification exams are very rigorous and challenging. By studying after the class and using these practice exams, you will greatly improve your chances of passing the actual certification exam the first time. Exam prep software is included with all CompTIA classes delivered by SYSTEMATECH Training Department.

Additional Notes Regarding CompTIA Certification Exams

As with most professional IT certifications, many addition hours of study are required before the class (meeting the prerequisites) and after the class (reviewing exam objectives and practice questions). Expect to spend a significant number of hours studying outside of the class before you take a CompTIA or any other IT professional exam. A criminal record may prevent the student from obtain employment in the field.

Course Objectives

In this course, you will install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers and digital devices. You will:

Install and configure PC system unit components and peripheral devices.

Install, configure, and troubleshoot display and multimedia devices.

Install, configure, and troubleshoot storage devices.

Install, configure, and troubleshoot internal system components.

SYSTEMATECH CO.

Explain network infrastructure concepts.
Configure and troubleshoot network connections.
Implement client virtualization and cloud computing.
Support and troubleshoot laptops.
Support and troubleshoot mobile devices.
Install, configure, and troubleshoot print devices.

Students

This course is designed for individuals who have basic computer user skills and who are interested in obtaining a job as an entry-level IT technician. This course is also designed for students who are seeking the CompTIA A+ certification and who want to prepare for the CompTIA A+ Core 1 220-1001 Certification Exam.

Prerequisites

To ensure your success in this course, you should have experience with basic computer user skills, be able to complete tasks in a Microsoft® Windows® environment, be able to search for, browse, and access information on the Internet, and have basic knowledge of computing concepts. You can obtain this level of skills and knowledge by taking the following official CompTIA courses:

The Official CompTIA® IT Fundamentals+ (Exam FC0-U61)

Note: The prerequisites for this course might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page: <https://certification.comptia.org/training/exam-objectives>

Course Outline

Lesson 1: Installing and Configuring PC Components

Topic A: Use Appropriate Safety Procedures

Topic B: PC Components

Topic C: Common Connection Interfaces

Topic D: Install Peripheral Devices

Topic E: Troubleshooting Methodology

Lesson 2: Installing, Configuring, and Troubleshooting Display and Multimedia Devices

Topic A: Install and Configure Display Devices

Topic B: Troubleshoot Display Devices

Topic C: Install and Configure Multimedia Devices

Lesson 3: Installing, Configuring, and Troubleshooting Storage Devices

Topic A: Install System Memory

Topic B: Install and Configure Mass Storage Devices

Topic C: Install and Configure Removable Storage

Topic D: Configure RAID

Topic E: Troubleshoot Storage Devices

Lesson 4: Installing, Configuring, and Troubleshooting Internal System Components

Topic A: Install and Upgrade CPUs

Topic B: Configure and Update BIOS/UEFI

Topic C: Install Power Supplies

Topic D: Troubleshoot Internal System Components

Topic E: Configure a Custom PC

Lesson 5: Network Infrastructure Concepts

Topic A: Wired Networks

Topic B: Network Hardware Devices

Topic C: Wireless Networks

Topic D: Internet Connection Types

Topic E: Network Configuration Concepts

Topic F: Network Services

Lesson 6: Configuring and Troubleshooting Networks

Topic A: Configure Network Connection Settings

Topic B: Install and Configure SOHO Networks

Topic C: Configure SOHO Network Security

Topic D: Configure Remote Access

Topic E: Troubleshoot Network Connections

Topic F: Install and Configure IoT Devices

Lesson 7: Implementing Client Virtualization and Cloud Computing

Topic A: Configure Client-Side Virtualization

Topic B: Cloud Computing Concepts

Lesson 8: Supporting and Troubleshooting Laptops

Topic A: Use Laptop Features

Topic B: Install and Configure Laptop Hardware

Topic C: Troubleshoot Common Laptop Issues

Lesson 9: Supporting and Troubleshooting Mobile Devices

Topic A: Mobile Device Types

Topic B: Connect and Configure Mobile Device Accessories

Topic C: Configure Mobile Device Network Connectivity

Topic D: Support Mobile Apps

Lesson 10: Installing, Configuring, and Troubleshooting Print Devices

Topic A: Maintain Laser Printers

Topic B: Maintain Inkjet Printers

Topic C: Maintain Impact, Thermal, and 3D Printers

Topic D: Install and Configure Printers

Topic E: Troubleshoot Print Device Issues
Topic F: Install and Configure Imaging Devices)
Copyright SystemATech Co. 2020



CompTIA A+ Core 2

CompTIA A+ Certification - Exam 220-1002 - Core 2 Course Outline

SYSTEMATECH CO.

Overview

The course shown here was designed for the new 220-1002 exam. CompTIA A+ certified professionals are proven problem solvers. They support today's core technologies from security to cloud to data management and more. CompTIA A+ is the industry standard for launching IT careers into today's digital world. It is the only industry recognized credential with performance-based items to prove pros can think on their feet to perform critical IT support tasks in the moment. It is trusted by employers around the world to identify the go-to person in end point management and technical support roles. CompTIA A+ is regularly re-invented by IT experts to ensure that it validates core skills and abilities demanded in the workplace.

The Official CompTIA® A+® Core 2 (Exam 220-1002) course provides the background knowledge and skills you will require to be a successful A+ technician. It will help you prepare to take the CompTIA A+ Core Series certification examination (exam number 220-1002), in order to become a CompTIA A+ Certified Professional.

Additional Notes Regarding CompTIA Certification Exams

As with most professional IT certifications, many additional hours of study are required before the class (meeting the prerequisites) and after the class (reviewing exam objectives and practice questions). Expect to spend a significant number of hours studying outside of the class before you take a CompTIA or any other IT professional exam. A criminal record may prevent the student from obtaining employment in the field.

Course Objectives

In this course, you will install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers, digital devices, and operating systems. You will:

- Support operating systems.
- Install, configure, and maintain operating systems.
- Maintain and troubleshoot Microsoft Windows.
- Configure and troubleshoot network connections.
- Manage users, workstations, and shared resources.
- Implement physical security.
- Secure workstations and data.
- Troubleshoot workstation security issues.
- Support and troubleshoot mobile devices.
- Implement operational procedures.

Target Student

This course is designed for individuals who have basic computer user skills and who are interested in obtaining a job as an entry-level IT technician. This course is also designed for students who are seeking the CompTIA A+ certification and who want to prepare for the CompTIA A+ Core 2 220-1002 Certification Exam.

Prerequisites

To ensure your success in this course, you should attend the CompTIA A+ Certification - Exam 220-1001 Core 1 class or have equivalent experience :

[CompTIA A+ Certification - Exam 220-1001 Core 1](#)

Note: The prerequisites for this course might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page:

[CompTIA A+ Certification Exam Objectives](#)

Course Outline

Lesson 1: Supporting Operating Systems

Topic A: Identify Common Operating Systems

Topic B: Use Windows Features and Tools

Topic C: Manage Files in Windows

Topic D: Manage Disks in Windows

Topic E: Manage Devices in Windows

Lesson 2: Installing, Configuring, and Maintaining Operating Systems

Topic A: Configure and Use Linux

Topic B: Configure and Use macOS

Topic C: Install and Upgrade Operating Systems

Topic D: Maintain OSs

Lesson 3: Maintaining and Troubleshooting Microsoft Windows

Topic A: Install and Manage Windows Applications

Topic B: Manage Windows Performance

Topic C: Troubleshoot Windows

Lesson 4: Configuring and Troubleshooting Networks

Topic A: Configure Network Connection Settings

Topic B: Install and Configure SOHO Networks

Topic C: Configure SOHO Network Security

Topic D: Configure Remote Access

Topic E: Troubleshoot Network Connections

Lesson 5: Managing Users, Workstations, and Shared Resources

Topic A: Manage Users

Topic B: Configure Shared Resources

Topic C: Configure Active Directory Accounts and Policies

Lesson 6: Security Concepts

Topic A: Logical Security Concepts

Topic B: Threats and Vulnerabilities

Topic C: Physical Security Measures

Lesson 7: Securing Workstations and Data

Topic A: Implement Security Best Practices

Topic B: Implement Data Protection Policies

Topic C: Protect Data During Incident Response

Lesson 8: Troubleshooting Workstation Security Issues

Topic A: Detect, Remove, and Prevent Malware

Topic B: Troubleshoot Common Workstation Security Issues

Lesson 9: Supporting and Troubleshooting Mobile Devices

Topic A: Secure Mobile Devices

Topic B: Troubleshoot Mobile Device Issues

Lesson 10: Implementing Operational Procedures

Topic A: Use Appropriate Safety Procedures

Topic B: Environmental Impacts and Controls

Topic C: Create and Maintain Documentation

Topic D: Use Basic Change Management Best Practices

Topic E: Implement Disaster Prevention and Recovery Methods

Topic F: Basic Scripting Concepts

Topic G: Professionalism and Communication

Appendix A: Mapping Course Content to CompTIA® A+® Core 2 (Exam 220-1002)



CompTIA Network+ Certification Training Course Outline

Overview

The CompTIA® Network+® (Exam N10-007) course builds on your existing user-level knowledge and experience with personal computer operating systems and networks to present the fundamental skills and concepts that you will need to use on the job in any type of networking career. If you are

SYSTEMATECH CO.

pursuing a CompTIA technical certification path, the CompTIA® A+® certification is an excellent first step to take before preparing for the CompTIA Network+ certification.

The CompTIA® Network+® (Exam N10-007) course can benefit you in two ways. It can assist you if you are preparing to take the CompTIA Network+ examination (Exam N10-007). Also, if your job duties include network troubleshooting, installation, or maintenance, or if you are preparing for any type of network-related career, it provides the background knowledge and skills you will require to be successful.

***** NOTE: This class also available in On-Demand, eLearning Format *****

Too busy at work to miss 5 days out of the office to take this class? Consider the CompTIA On-Demand version of this course. Watch videos, take the same hands-on labs, access an online expert 24/7, and study at on your own time, at your own pace.

Cost \$4995.00

8 weeks course

Hours: 198

For details on this alternative format, go to [CompTIA On-Demand Network+ Certification Training](#)

Network+ Exam Objectives

[Click here for Network+ Exam Objectives](#)

Exam Prep Software

All of our CompTIA classes include access to web-based practice exams. CompTIA certification exams are very rigorous and challenging. By studying after the class and using these practice exams, you will greatly improve your chances of passing the actual certification exam the first time. Exam prep software is included with all CompTIA classes delivered by SYSTEMATECH Training Centers.

Additional Notes Regarding CompTIA Certification Exams

As with most professional IT certifications, many additional hours of study are required before the class (meeting the prerequisites) and after the class (reviewing exam objectives and practice questions). Expect to spend a significant number of hours studying outside of the class before you take a CompTIA or any other IT professional exam. A criminal record may prevent the student from obtaining employment in the field.

Course Objectives

In this course, you will describe the major networking technologies and systems of modern networks, and be able to configure, manage, and troubleshoot modern networks.

You will:

- Identify basic network theory concepts and major network communications methods.
- Describe bounded network media.
- Identify unbounded network media.
- Identify the major types of network implementations.

SYSTEMATECH CO.

- Identify TCP/IP addressing and data delivery methods.
- Implement routing technologies.
- Identify the major services deployed on TCP/IP networks.
- Identify the infrastructure of a WAN implementation.
- Identify the components used in cloud computing and virtualization.
- Describe basic concepts related to network security.
- Prevent security breaches.
- Respond to security incidents.
- Identify the components of a remote network implementation.
- Identify the tools, methods, and techniques used in managing a network.
- Describe troubleshooting of issues on a network.

Target Audience

CompTIA Network+ is the first certification IT professionals specializing in network administration and support should earn. Network+ is aimed at IT professionals with job roles such as network administrator, network technician, network installer, help desk technician and IT cable installer.

Course Prerequisites

Students should meet the following criteria prior to taking the course:

Taken and passed both CompTIA A+ Certification exams or have 9-12 months knowledge and experience of IT administration

Be able to configure and support PC, laptop, mobile (smartphone / tablet), and print devices

Know basic network terminology and functions (such as Ethernet, TCP/IP, switches, routers)

Configure and manage users, groups, and shared resources in a simple SOHO network

Understand the use of basic access control measures, such as authentication, security policy, encryption, and firewalls

Course Outline

Module 1 / Local Area Networks

Topologies and the OSI Model • Key Features of Networks • Network Topologies • The OSI Model • Physical Layer • Data Link Layer • Network Layer • Transport Layer • Upper Layers • OSI Model Summary • Labs • VM Orientation

Ethernet • Transmission Media • Media Access Control • Broadcast Domains • Ethernet Frames • Ethernet Deployment Standards • MAC Addressing • Address Resolution Protocol (ARP) • Packet Sniffers • Labs • Configuring Ethernet Networking

Hubs, Bridges, and Switches • Hubs and Bridges • Switches • Switch Interface Configuration • Spanning Tree Protocol (STP) • Power over Ethernet (PoE)

Infrastructure and Design • Network Infrastructure Implementations • Planning an Enterprise Campus Network • Network Hierarchy and Distributed Switching • Software Defined Networking • Planning a SOHO Network • TCP/IP Protocol Suite

Policies and Best Practices • Procedures and Standards • Safety Procedures • Incident Response Policies • Security and Data Policies • Password Policy • Employee Policies

Module 2 / IP Addressing

Internet Protocol • IPv4 • IPv4 Address Structure • Subnet Masks • IP Routing Basics • ipconfig / ifconfig • ICMP and ping • Labs • Configuring IPv4 Networking

IPv4 Addressing • IPv4 Addressing Schemes • Classful Addressing • Public versus Private Addressing • Subnetting and Classless Addressing • Planning an IPv4 Addressing Scheme • Public

Internet Addressing • Variable Length Subnet Masks (VLSM) • Labs • Configuring IPv4 Subnets
IPv6 Addressing • IPv6 Address Format • IPv6 Addressing Schemes • IPv6 Address
Autoconfiguration • Migrating to IPv6 • Labs • Configuring IPv6 Networking
DHCP and APIPA • IPv4 Address Autoconfiguration • Configuring DHCP • DHCPv6 • Labs •
Configuring Address Autoconfiguration

Module 3 / Internetworking

Routing • Routing Basics • Routing Algorithms and Metrics • Dynamic Routing Protocols •
Administrative Distance and Route Redistribution • IPv4 and IPv6 Internet Routing • High Availability
Routing • Installing and Configuring Routers • Routing Troubleshooting Tools • Labs • Configuring
Routing
TCP and UDP • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • TCP and
UDP Ports • Port Scanners • Protocol Analyzers • Labs • TCP and Port Scanning
Name Resolution and IPAM • Host Names and FQDNs • Domain Name System • Configuring DNS
Servers • Resource Records • Name Resolution Tools • IP Address Management (IPAM) • Labs •
Configuring Name Resolution and IPAM
Monitoring and Scanning • Performance Monitoring • Network Monitoring Utilities • Logs and Event
Management • Simple Network Management Protocol • Analyzing Performance Metrics • Patch
Management • Vulnerability Scanning • Labs • Performance Testing and Monitoring
Network Troubleshooting • Troubleshooting Procedures • Identifying the Problem • Establishing a
Probable Cause • Establishing a Plan of Action • Troubleshooting Hardware Failure Issues •
Troubleshooting Addressing Issues • Troubleshooting DHCP Issues • Troubleshooting Name
Resolution • Troubleshooting Services

Module 4 / Applications and Security

Applications and Services • TCP/IP Services • HTTP and Web Servers • SSL / TLS and HTTPS •
Email (SMTP / POP / IMAP) • Voice Services (VoIP and VTC) • Real-time Services Protocols •
Quality of Service • Traffic Shaping • Bottlenecks and Load Balancing • Multilayer Switches • Labs •
Configuring Application Protocols
Virtualization, SAN, and Cloud Services • Virtualization Technologies • Network Storage Types •
Fibre Channel and InfiniBand • iSCSI • Cloud Computing • Configuring Cloud Connectivity
Network Security Design • Security Basics • Common Networking Attacks • Network Segmentation
and DMZ • Virtual LANs (VLAN) • VLAN Trunks • Network Address Translation (NAT) • Device and
Service Hardening • Honeypots and Penetration Tests
Network Security Appliances • Basic Firewalls • Stateful Firewalls • Deploying a Firewall •
Configuring a Firewall • Deploying a Proxy • Intrusion Detection Systems (IDS) • Denial of Service •
Labs • Configuring a NAT Firewall
Authentication and Endpoint Security • Authentication and Access Controls • Social Engineering •
Authentication Technologies • PKI and Digital Certificates • Local Authentication • RADIUS and
TACACS+ • Directory Services • Endpoint Security • Network Access Control • Labs • Secure
Appliance Administration

Module 5 / Operations and Infrastructure

Network Site Management • Network Cabling Solutions • Distribution Frames • Change and
Configuration Management • Network Documentation and Diagrams • Labeling • Physical Security
Devices • Business Continuity and Disaster Recovery • Network Link Management • Power
Management • Backup Management • Labs • Network Inventory Management
Installing Cabled Networks • Twisted Pair Cable (UTP / STP / ScTP) • Twisted Pair Connectors •
Wiring Tools and Techniques • Cable Testing Tools • Troubleshooting Wired Connectivity • Other

Copper Cable Types • Fiber Optic Cable and Connectors • Transceivers and Media Converters
Installing Wireless Networks • Wireless Standards (IEEE 802.11) • Wireless Network Topologies •
Wireless Site Design • Troubleshooting Wireless Connectivity • Wireless Security • Wi-Fi
Authentication • Extensible Authentication Protocol • Troubleshooting Wireless Security • Wireless
Controllers
Installing WAN Links • Wide Area Networks (WAN) • Telecommunications Networks • Modern
Telecommunications Networks • Local Loop Services • Installing WAN Links • Wireless WAN
Services • Internet of Things
Configuring Remote Access • Remote Access Services (RAS) • MPLS and PPP • SIP Trunks •
Virtual Private Networks (VPN) • SSL / TLS / DTLS VPNs • IPsec • Internet Key Exchange / ISAKMP
• Remote Access Servers • Remote Administration Tools • Managing Network Appliances • Remote
File Access • Labs • Configuring Secure Access Channels • Configuring a Virtual Private Network

Exam Code@ N10-007



CompTIA Security+ Certification Training Course Outline

Overview

CompTIA Security+ is aimed at IT professionals with job roles such as security architect, security engineer, security consultant/specialist, information assurance technician, security administrator, systems administrator and network administrator.

Course Prerequisites

Students should meet the following criteria prior to taking the course:

Recommended that students have taken CompTIA Network+ certification course and exam, together with 24 months experience in networking support/IT administration

Know the function and basic features of the components of a PC

Use Windows Server to create and manage files and use basic administrative features (Explorer, Control Panel, Management Consoles, Command Line Tools)

Operate the Linux OS using basic command-line tools

Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers)

Understand TCP/IP addressing, core protocols, and troubleshooting tools

Exam Prep Software

All of our CompTIA classes include access to web-based practice exams. CompTIA certification exams are very rigorous and challenging. By studying after the class and using these practice exams, you will greatly improve your chances of passing the actual certification exam the first time. Exam prep software is included with all CompTIA classes delivered by SystemATech Training Centers.

Additional Notes Regarding CompTIA Certification Exams

As with most professional IT certifications, many additional hours of study are required before the class (meeting the prerequisites) and after the class (reviewing exam objectives and practice questions). Expect to spend a significant number of hours studying outside of the class before you take a CompTIA or any other IT professional exam. A criminal record may prevent the student from obtain employment in the field.

Cost \$4995.00

8 weeks course

Hours: 198

Course Outline

Module 1 / Threats, Attacks, and Vulnerabilities

SYSTEMATECH CO.

Indicators of Compromise • Why is Security Important? • Security Policy • Threat Actor Types • The Kill Chain • Social Engineering • Phishing • Malware Types • Trojans and Spyware • Open Source Intelligence • Labs • VM Orientation • Malware Types

Critical Security Controls • Security Control Types • Defense in Depth • Frameworks and Compliance • Vulnerability Scanning and Pen Tests • Security Assessment Techniques • Pen Testing Concepts • Vulnerability Scanning Concepts • Exploit Frameworks • Lab • Using Vulnerability Assessment Tools

Security Posture Assessment Tools • Topology Discovery • Service Discovery • Packet Capture • Packet Capture Tools • Remote Access Trojans • Honeypots and Honeynets • Labs • Using Network Scanning Tools 1 • Using Network Scanning Tools 2 • Using Steganography Tools

Incident Response • Incident Response Procedures • Preparation Phase • Identification Phase • Containment Phase • Eradication and Recovery Phases

Module 2 / Identity and Access Management

Cryptography • Uses of Cryptography • Cryptographic Terminology and Ciphers • Cryptographic Products • Hashing Algorithms • Symmetric Algorithms • Asymmetric Algorithms • Diffie-Hellman and Elliptic Curve • Transport Encryption • Cryptographic Attacks • Lab • Implementing Public Key Infrastructure

Public Key Infrastructure • PKI Standards • Digital Certificates • Certificate Authorities • Types of Certificate • Implementing PKI • Storing and Distributing Keys • Key Status and Revocation • PKI Trust Models • PGP / GPG • Lab • Deploying Certificates and Implementing Key Recovery

Identification and Authentication • Access Control Systems • Identification • Authentication • LAN Manager / NTLM • Kerberos • PAP, CHAP, and MS-CHAP • Password Attacks • Token-based Authentication • Biometric Authentication • Common Access Card • Lab • Using Password Cracking Tools

Identity and Access Services • Authorization • Directory Services • RADIUS and TACACS+ • Federation and Trusts • Federated Identity Protocols

Account Management • Formal Access Control Models • Account Types • Windows Active Directory • Creating and Managing Accounts • Account Policy Enforcement • Credential Management Policies • Account Restrictions • Accounting and Auditing • Lab • Using Account Management Tools

Module 3 / Architecture and Design (1)

Secure Network Design • Network Zones and Segments • Subnetting • Switching Infrastructure • Switching Attacks and Hardening • Endpoint Security • Network Access Control • Routing Infrastructure • Network Address Translation • Software Defined Networking • Lab • Implementing a Secure Network Design

Firewalls and Load Balancers • Basic Firewalls • Stateful Firewalls • Implementing a Firewall or Gateway • Web Application Firewalls • Proxies and Gateways • Denial of Service Attacks • Load Balancers • Lab • Implementing a Firewall

IDS and SIEM • Intrusion Detection Systems • Configuring IDS • Log Review and SIEM • Data Loss Prevention • Malware and Intrusion Response • Lab • Using an Intrusion Detection System

Secure Wireless Access • Wireless LANs • WEP and WPA • Wi-Fi Authentication • Extensible Authentication Protocol • Additional Wi-Fi Security Settings • Wi-Fi Site Security • Personal Area Networks

Physical Security Controls • Site Layout and Access • Gateways and Locks • Alarm Systems • Surveillance • Hardware Security • Environmental Controls

Module 4 / Architecture and Design (2)

Secure Protocols and Services • DHCP Security • DNS Security • Network Management Protocols • HTTP and Web Servers • SSL / TLS and HTTPS • Web Security Gateways • Email Services • S/MIME • File Transfer • Voice and Video Services • VoIP • Labs • Implementing Secure Network Addressing Services • Configuring a Secure Email Service

Secure Remote Access • Remote Access Architecture • Virtual Private Networks • IPSec • Remote Access Servers • Remote Administration Tools • Hardening Remote Access Infrastructure • Lab • Implementing a Virtual Private Network

Secure Systems Design • Trusted Computing • Hardware / Firmware Security • Peripheral Device Security • Secure Configurations • OS Hardening • Patch Management • Embedded Systems • Security for Embedded Systems

Secure Mobile Device Services • Mobile Device Deployments • Mobile Connection Methods • Mobile Access Control Systems • Enforcement and Monitoring

Secure Virtualization and Cloud Services • Virtualization Technologies • Virtualization Security Best Practices • Cloud Computing • Cloud Security Best Practices

Module 5 / Risk Management

Forensics • Forensic Procedures • Collecting Evidence • Capturing System Images • Handling and Analyzing Evidence • Lab • Using Forensic Tools

Disaster Recovery and Resiliency • Continuity of Operations Plans • Disaster Recovery Planning • Resiliency Strategies • Recovery Sites • Backup Plans and Policies • Resiliency and Automation Strategies

Risk Management • Business Impact Analysis • Identification of Critical Systems • Risk Assessment • Risk Mitigation

Secure Application Development • Application Vulnerabilities • Application Exploits • Web Browser Exploits • Secure Application Design • Secure Coding Concepts • Auditing Applications • Secure DevOps • Lab • Identifying a Man-in-the-Browser Attack

Organizational Security • Corporate Security Policy • Personnel Management Policies • Interoperability Agreements • Data Roles • Data Sensitivity Labeling and Handling • Data Wiping and Disposal • Privacy and Employee Conduct Policies • Security Policy Training

Exam Code# **(SY0-601)**



CompTIA Cloud+ Certification Exam # CV0-003

Overview

While IT professionals today are expected to understand some basic cloud terminology and concepts, and most have likely worked with public cloud or Software-as-a-Service solutions, the ability to analyze, evaluate, design, and test cloud computing solutions is a difficult skillset to find, and it is currently in high demand. In this course, you will apply the skills required to evaluate and implement standard deployments. You will implement, maintain, and deliver cloud technologies including network, storage, and virtualization technologies to create cloud solutions. You will manage workload migrations, manage cloud vendors to control costs, use automation and orchestration to bring business value from cloud solutions, and ensure security of cloud implementations through the use of cybersecurity best practices. In addition, this course prepares you to pass the CompTIA® Cloud+® exam and earn the corresponding certification.

Course Objectives

In this course, you will deploy, test, secure, manage, optimize, and troubleshoot a cloud solution. You will:

Prepare to deploy cloud solutions.

Deploy a pilot project.

Test a pilot project deployment.

Design a secure network for cloud deployment.

Determine CPU and memory sizing for cloud deployments.

Determine storage requirements for cloud deployments.

Plan Identity and Access Management for cloud deployments.

Analyze workload characteristics to ensure successful migration to the cloud.

Secure systems to meet access requirements.

Maintain cloud systems.

Implement backup, restore, and business continuity measures.

Analyze cloud systems for required performance.

Analyze cloud systems for anomalies and growth forecasting.

Troubleshoot deployment, capacity, automation, and orchestration issues.

Troubleshoot connectivity issues.

Troubleshoot security issues.

Cost \$4995.00 8 weeks course Hours: 198

Target Student

This course is designed for IT professionals who wish to develop cloud computing skills to enable them to move IT workloads to the cloud and integrate products and services from different providers and industries. The focus is to ensure that cloud deployments are secure, that automation and orchestration are used effectively to bring business value from the cloud, and that costs are controlled through effective management of cloud vendors.

This course is also designed for students who are preparing to take the CompTIA Cloud+

certification exam CV0-002, or who plan to use Cloud+ as the foundation for more advanced cloud certifications or career roles. A criminal record may prevent the student from obtain employment in the field.

Prerequisites

To ensure your success in this course, you should have 24-36 months' experience with IT networking, network storage, and data center administration. You should also have familiarity with any major hypervisor technologies for server virtualization, basic knowledge of common cloud service models, and common cloud deployment models.

Course Content

Lesson 1: Preparing to Deploy Cloud Solutions

Topic A: Describe Interaction of Cloud Components and Services

Topic B: Describe Interaction of Non-cloud Components and Services

Topic C: Evaluate Existing Components and Services for Cloud Deployment

Topic D: Evaluate Automation and Orchestration Options

Topic E: Prepare for Cloud Deployment

Lesson 2: Deploying a Pilot Project

Topic A: Manage Change in a Pilot Project

Topic B: Execute Cloud Deployment Workflow

Topic C: Complete Post-Deployment Configuration

Lesson 3: Testing Pilot Project Deployments

Topic A: Identify Cloud Service Components for Testing

Topic B: Test for High Availability and Accessibility

Topic C: Perform Deployment Load Testing

Topic D: Analyze Test Results

Lesson 4: Designing a Secure and Compliant Cloud Infrastructure

Topic A: Design Cloud Infrastructure for Security

Topic B: Determine Organizational Compliance Needs

Lesson 5: Designing and Implementing a Secure Cloud Environment

Topic A: Design Virtual Network for Cloud Deployment

Topic B: Determine Network Access Requirements

Topic C: Secure Networks for Cloud Interaction

Topic D: Manage Cloud Component Security

Topic E: Implement Security Technologies

Lesson 6: Planning Identity and Access Management for Cloud Deployments

Topic A: Determine Identity Management and Authentication Technologies

Topic B: Plan Account Management Policies for the Network and Systems

Topic C: Control Access to Cloud Objects

Topic D: Provision Accounts

Lesson 7: Determining CPU and Memory Sizing for Cloud Deployments

Topic A: Determine CPU Size for Cloud Deployment

Topic B: Determine Memory Size for Cloud Deployment

Lesson 8: Determining Storage Requirements for Cloud Deployments

Topic A: Determine Storage Technology Requirements

Topic B: Select Storage Options for Deployment

Topic C: Determine Storage Access and Provisioning Requirements

Topic D: Determine Storage Security Options

Lesson 9: Analyzing Workload Characteristics to Ensure Successful Migration

Topic A: Determine the Type of Cloud Deployment to Perform

Topic B: Manage Virtual Machine and Container Migration

Topic C: Manage Network, Storage, and Data Migration

Lesson 10: Maintaining Cloud Systems

Topic A: Patch Cloud Systems

Topic B: Design and Implement Automation and Orchestration for Maintenance

Lesson 11: Implementing Backup, Restore, Disaster Recovery, and Business Continuity Measures

Topic A: Back Up and Restore Cloud Data

Topic B: Implement Disaster Recovery Plans

Topic C: Implement Business Continuity Plans

Lesson 12: Analyzing Cloud Systems for Performance

Topic A: Monitor Cloud Systems to Measure Performance

Topic B: Optimize Cloud Systems to Meet Performance Criteria

Lesson 13: Analyzing Cloud Systems for Anomalies and Growth Forecasting

Topic A: Monitor for Anomalies and Resource Needs

Topic B: Plan for Capacity

Topic C: Create Reports on Cloud System Metrics

Lesson 14: Troubleshooting Deployment, Capacity, Automation, and Orchestration Issues

Topic A: Troubleshoot Deployment Issues

Topic B: Troubleshoot Capacity Issues

Topic C: Troubleshoot Automation and Orchestration Issues

Lesson 15: Troubleshooting Connectivity Issues

Topic A: Identify Connectivity Issues

Topic B: Troubleshoot Connectivity Issues

Lesson 16: Troubleshooting Security Issues

Topic A: Troubleshoot Identity and Access Issues

Topic B: Troubleshoot Attacks Topic C: Troubleshoot Other Security Issues

CompTIA CYSA+ Exam Code (CS0-002)

Overview:

This course is intended for individuals wishing to obtain the qualification of a CompTIA CySA+ Cybersecurity Analyst Certification. CompTIA's CySA+ Certification is an intermediate-level certificate for IT professionals with previous experience working in IT security. The CompTIA CySA+ examination is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts. The exam certifies that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis. In turn, these skills will be used to interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization.

Certification track:

This courseware bears the seal of CompTIA Approved Quality Content. The seal signifies that this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple elearning tools to help increase coverage of the learning objectives. The contents of this training material were created for the CompTIA CYSA+ Cybersecurity Analyst Certification CS0-002 exam covering the 2020 Edition certification exam objectives.

Additional Notes Regarding CompTIA Certification Exams:

As with most professional IT certifications, many additional hours of study are required before the class and after the class. Expect to spend a significant number of hours studying outside of the class before you take a CompTIA or any other IT professional exam. A criminal record may prevent the student from obtain employment in the field.

Cost \$4995.00 8 weeks course Hours: 198

Target audience and course prerequisites:

CompTIA CYSA+ certification is aimed at IT professionals with (or seeking) job roles such as IT Security Analyst, Security Operations Center (SOC) Analyst, Vulnerability Analyst, Cybersecurity Specialist, Threat Intelligence Analyst, and Security Engineer.

Ideally, you should have successfully completed:

CompTIA Network+ Certification AND Security+ Certification courses or have equivalent knowledge before attending this training.

Specifically, it is recommended that you have the following skills and knowledge before starting this course:

- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools.
- Identify network attack strategies and defenses.
- Know the technologies and uses of cryptographic standards and products.
- Identify network- and host-based security technologies and practices.
- Describe the standards and products used to enforce security on web and communications technologies.

Course Outline:

Module 1 – Threat Management 1

- Cybersecurity Analysts
- Cybersecurity Roles and Responsibilities
- Frameworks and Security Controls
- Risk Evaluation
- Penetration Testing Processes
- Reconnaissance Techniques
- The Kill Chain
- Open Source Intelligence
- Social Engineering
- Topology Discovery
- Service Discovery
- OS Fingerprinting

Module 2 – Threat Management 2

- Security Appliances
- Configuring Firewalls
- Intrusion Detection and Prevention
- Configuring IDS
- Malware Threats
- Configuring Anti-virus Software
- Sysinternals
- Enhanced Mitigation Experience Toolkit
- Logging and Analysis
- Packet Capture
- Packet Capture Tools
- Monitoring Tools
- Log Review and SIEM
- SIEM Data Outputs
- SIEM Data Analysis
- Point-in-Time Data Analysis

Module 3 – Vulnerability Management

- Managing Vulnerabilities
 - Vulnerability Management Requirements
 - Asset Inventory
 - Data Classification
 - Vulnerability Management Processes
 - Vulnerability Scanners
 - Microsoft Baseline Security Analyzer
 - Vulnerability Feeds and SCAP
 - Configuring Vulnerability Scans
 - Vulnerability Scanning Criteria
 - Exploit Frameworks
- Remediating Vulnerabilities
 - Analyzing Vulnerability Scans
 - Remediation and Change Control
 - Remediating Host Vulnerabilities
 - Remediating Network Vulnerabilities
 - Remediating Virtual Infrastructure Vulnerabilities
- Secure Software Development
 - Software Development Lifecycle
 - Software Vulnerabilities
 - Software Security Testing
 - Interception Proxies
 - Web Application Firewalls
 - Source Authenticity
 - Reverse Engineering

Module 4 – Cyber Incident Response

- Incident Response
 - Incident Response Processes
 - Threat Classification
 - Incident Severity and Prioritization
 - Types of Data
- Forensics Tools
 - Digital Forensics Investigations
 - Documentation and Forms
 - Digital Forensics Crime Scene
 - Digital Forensics Kits
 - Image Acquisition
 - Password Cracking
 - Analysis Utilities

- Incident Analysis and Recovery
- Analysis and Recovery Frameworks
- Analyzing Network Symptoms
- Analyzing Host Symptoms
- Analyzing Data Exfiltration
- Analyzing Application Symptoms
- Using Sysinternals
- Containment Techniques
- Eradication Techniques
- Validation Techniques
- Corrective Actions

Module 5 – Security Architecture

- Secure Network Design
- Network Segmentation
- Blackholes, Sinkholes, and Honeypots
- System Hardening
- Group Policies and MAC
- Endpoint Security
- Managing Identities and Access
- Network Access Control
- Identity Management
- Identity Security Issues
- Identity Repositories
- Context-based Authentication
- Single Sign On and Federations
- Exploiting Identities
- Exploiting Web Browsers and Applications
- Security Frameworks and Policies
- Frameworks and Compliance
- Reviewing Security Architecture
- Procedures and Compensating Controls
- Verifications and Quality Control
- Security Policies and Procedures
- Personnel Policies and Training

Exam Code (CS0-003)

Admission Requirements

- Student must be at least 16 years of age to attend SystemATech Co.
- Student must NOT have a criminal background (contact school to discuss).
- Student must complete Enrollment Agreement.
- Must provide proof of citizenship.

The minimum number of students in a program/classroom is five. If the course needs to be rescheduled due to low enrollment, students will be notified by phone and email. Students will have the choice to attend the next scheduled class.

Application Procedure

Student must complete enrollment form and submit it to the institution. Students may submit their enrollment form on our website at www.systematech.us/courses. Students are required to pay an enrollment fee for each course they enroll in.

Transfer Credit

SystemATech Co. will not accept transfer credits or credit hours for courses taken at other institutions.

Standards of Progress

Grading Scale

SystemATech Co. uses a seven-point grading scale. Ten points will be deducted from overall grade for each absence. Assignments, quizzes and tests will be graded according to scale:

A 93 – 100

B 85 – 92

C 77 – 84

D 70 – 76

F 69 – 0

Minimum Score

Systematech minimum score requirements are 80%.

Progress Reports & Academic Probation and Suspension Policy

Students will receive feedback during the midpoint of the program through a brief one-on-one meeting with the instructor. During this meeting academic performance will be discussed. If a student's average is below 100% then an academic contract will be established with the student, specifying deadline dates for academic improvement to a minimum grade of 80%. If the student is unable to meet contractual agreement, then he or she will be dismissed from the program. If the student wishes to re-enroll, he or she must adhere to the Conduct & Re-Admission policy. The institution does not provide academic tutoring; however, students are encouraged to seek assistance from peers and/or meet with the instructor for counsel prior to the midpoint of program.

Conduct & Re-Admission Policy

Professional behavior is required while on campus. Failure to follow the classroom conduct guidelines could result in expulsion from the program.

The following guidelines must be followed:

- Be seated and prepared to begin class by the start time indicated.
- Disruptive and disrespectful behavior will not be permitted. Foul, vulgar, or offensive behavior is not permitted at any time.
- Drinks and snacks may be permitted during classroom time, per your instructor.
- Respect the rights, privacy, and property of others. Vandalism and theft are immediate cause for expulsion and legal action.
- Students will be respectful towards all staff and students.
- Cell phones must be on vibrate during class and out of sight. Cell phones are not to be used in the classroom for calls, texts, browsing, games, etc.
- Dress code in the classroom is appropriate casual and comfortable attire.
- Smoking on premises is prohibited.

Students may be terminated or suspended from SystemATech Co. due to misconduct and/or academic failure. A request for re-entry must be in writing and submitted to the director. Students may be subject to an interview with the director and re-enrollment into the program. The director will make the final decision.

Maintenance of Student Records

All records of students' academic progress will be kept on file electronically for six years. Transcripts will be maintained for 50 years.

Important Calendar Dates

Schedule	Quarter 1	Quarter 2	Quarter 3	Quarter 4
First Day of Class	01-01-2023	01-04-2023	04-07-2023	01-10-2023
Last Day to Drop	29-12-2022	29-03-2023	28-06-2023	28-9-2023
Progress Report/Feedback	Weekly	Weekly	Weekly	Weekly
Last Day of Class	8 Weeks from Start Date	8 Weeks from Start Date	8 Weeks from Start Date	8 Weeks from Start Date

Holidays Observed

- New Year's Day
- Martin Luther King Jr. Day
- President's Day
- Juneteenth
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- Day after Thanksgiving
- Christmas Eve
- Christmas Day

Vacations

- Spring Break
- Winter Break

Attendance Policy & Conduct

Students are required to be on time for every scheduled class date unless notified or approved by the Instructor or Program Director. Attendance will be taken at the beginning of each class meeting, capturing students' name, date and time of arrival and departure. Students are expected to attend all class meetings, as their attendance and participation is vital. Students are not allowed to miss any days as SystemATech Co. will not perform any makeup days for the course.

Makeup Work

In the event of an absence, no more than 8 hours, it is the students' responsibility to meet with the instructor and/or Program Director to arrange ways to make up the hours and assignments that were missed. SystemATech Co. offers many days throughout the program that simply cannot be missed, and this will need to be made up in the next available class. Make up work must be submitted to instructor within 72 hours.

Tardiness

Tardiness is not acceptable for the courses at SystemATech Co. One hundred percent participation is required.

Reentry

A request for re-entry must be in writing and submitted to the director. Students may be subject to an interview with the director and re-enrollment into the program. The director will make the final decision.

Tuition of Charges

Name of Program	Total Hours	Tuition	Program Length	Session Attended
CompTIA A+ Core 1 and Core 2	198	\$4995.00	8 weeks	
CompTIA Network+	198	\$4995.00	8 weeks	
CompTIA Security+	198	\$4995.00	8 weeks	
CompTIA Cloud+ Course	198	\$4995.00	8 weeks	
CompTIA CYSA	198	\$4995.00	8 weeks	

Cancellation & Refund Policy

Rejection: An application rejected by the institution is entitled to a refund of all monies paid.

Three- Day Cancellation: An applicant may cancel this agreement without penalty by notifying the institution within three business days after signing this agreement, excluding weekends and holidays. After the third day, but before classes begin, we may retain up to \$100 registration/administrative fee.

Other Cancellations: The minimum number of students in program/class is five. If the course is rescheduled due to low enrollment, students will be notified by phone and email. Students will have the choice to attend the next scheduled class. If the class start date is changed for a second time, the student will be eligible for a full refund of all monies paid.

Withdrawal: Student(s) who wish to withdraw from this institution after classes begin will be subject to the below refund policy. The institution may retain up to \$100 registration/administrative fee if student cancels class before the third day. After more than 3 days of attendance, the institution will charge for the

entire course. Refunds are issued within 40 days after the effective date of cancellation or last date attended.

Refund calculation example (for a 80-hour program):

Weeks Attended	Tuition Refund
1	97%
2	0%
3	0%
4	0%
5	0%
6	0%
7	0%
8	0%

Job Placement Assistance

SystemATech Co. LLC will assist students who have successfully passed their examination job placement at our discretion. Completion of any course or certificate program, including passing of

Employment

Enrollment or completion of program with Systematech Co. does not guarantee employment.

Student Complaints

If you encounter any problems concerning the education or administration of this program, please contact your instructor immediately and state your grievance in writing to allow us to help you.

The issue will not be addressed until a written grievance has been submitted to the following SystemATech Co.'s staff:

1st Level: Instructor Email: info@SystemATech.us telephone: (803-474-4407)

2nd Level: Administrator info@SystemATech.us telephone: (803-474-4407)

3rd Level: Director info@SystemATech.us telephone: (803-474-4407)

Once grievance has been received, we will consult with student to provide a resolution. All student grievances will be acknowledged within 3 business day. If students are not satisfied with SystemATech Co.'s assistance plan and have exhausted all staff levels of the grievance procedure, students may appeal in writing to the South Carolina Commission on Higher Education:

South Carolina Commission on Higher Education

1122 Lady Street, Suite 300

Columbia, South Carolina 29201

843-737-2260

www.che.sc.gov

The complaint form is available at the following link.

http://www.che.sc.gov/CHE_Docs/AcademicAffairs/License/Complaint_procedures_and_form.pdf

Transfer Credit

SystemATech Co. will not accept transfer or provide credits for courses taken at Systematech and other institutions.

Hold Harmless Agreement

SystemATech Co. and student acknowledge that there is some risk of accident or injury associated with use of equipment and other aspects of the course of study, including but not limited to direct care and contact of other students or clients at the training site. Student does hereby waive, release, and discharge SystemATech Co. of any and all liability and all claims for damages for death, personal injury, or property damage which I may have or which hereafter accrue to me as a result of participation in the program whether or not caused by negligence or fault of SystemATech Co.

This release is intended to discharge the school, and its officer's employees, representatives, volunteers, and agents from and against any and all liability arising out of or connected in any way with my participation in training, internship/externship, hands -on activities, practice, or activities.

Knowing risks exist, nevertheless, I hereby to assume those risks and to release and to hold harmless all persons or agencies mentioned above that might otherwise be liable to me or my heirs or assigns for damages. I further understand and agree that this waiver, release and assumption of risk is to be binding on my heirs and assigns.

In addition, I give permission to receive, if necessary, emergency medical services by authorized personnel, and that cost incurred as a result of such medical treatment will be my responsibility.

Student Name Print: _____

Date: _____

Student Name Signature: _____

Date: _____

School Administrator/Official Name Signature: _____

Date: _____

Computer Use Guideline

Misuse of Information systems is prohibited. Misuse includes the following:

- Attempting to modify or remove computer equipment, software, or peripherals without proper authorization.
- Accessing, without proper authorization, computers, software, information, or networks, regardless of whether the resource accessed is owned by the school.
- Taking actions, without authorization, which interfere with the access of others to information systems.
- Circumventing logon or other security measures.
- Using information systems for any illegal or unauthorized purpose.
- Violating any software license.
- Using electronic communications to violate the property rights of authors and copyright owners.
- Using electronic communications to disclose proprietary information without the explicit permission of the owner.
- Reading other users' information or files without permission.
- Using electronic communications to hoard, damage, or damage, or otherwise interfere with academic resources available electronically.
- Launching a computer worm, computer virus, or other rouge program.
- Downloading or posting illegal, proprietary, or damaging material.
- Violating any state or federal law or regulation in connection with use of any information system.
- Visiting and/ accessing prohibited sites such as Facebook, pornographic material, etc.
- I will not warrant executable files such as .exe, .vbs, .bat, and etc.

Violation of these guidelines will warrant immediate removal and termination from institution.

Exhibit V Sample Advertisement

SYSTEMATECH

READY TO TAKE YOUR EXAM? Learn how to pass on a First Exam!

Ride the Tech Wave

Equipping the people for the work of technology.

Call us on the web: www.systematech.us Contact Us: 803-474-4407

GET CERTIFIED
Training currently in session

CompTIA A+ CompTIA CySA+ CompTIA Security+

SYSTEMATECH CO.
WWW.SYSTEMATECH.US

**DREAM.
ACT.
ACHIEVE.**

NOW ACCEPTING APPLICANTS

We have a broad selection of courses that you can join. From information technology, information security, business analysis, cloud essentials, scrum, and 6 sigma courses. Visit our website for enrollment. Next cohort begins Thursday, March 24, 2022.

Contact us:
803-474-4407
info@systematech.us
www.systematech.us

SYSTEMATECH

Register for Career Training with SystemATech

Registration now Open for Our IT Support Specialist Training Class

CREATING THE NEXT IT & CYBER PROFESSIONALS

IT Support Specialist Training
Get Trained! Get Certified!

At the conclusion of this program students will have the skills to:

- Assemble components based on customer requirements
- Install, configure and maintain devices, PCs and software for end users
- Understand the basics of networking and security, including forensics
- Apply troubleshooting skills to diagnose, resolve and document common hardware and software issues
- Provide appropriate customer support
- Understand the basics of virtualization, desktop imaging and deployment

IT Support Specialist Training
Thursday, March 24, 2022 - Wednesday, May 18, 2022
Tues, Weds, Thurs
8:30 am - 4:30 pm
Online Training

This program will prepare students for the CompTIA A+ Core Series exams, Core 1 (220-1101) and Core 2 (220-1102).

CompTIA A+ is the industry standard for launching an IT career into today's digital world. CompTIA A+ is the preferred performance-based qualifying credential for a career in technical support and IT operational roles.

Participants must have a high school diploma or equivalent and basic computer knowledge.

For more information, go to www.systematech.us and complete the interest form under IT Support Specialist Training or email Tammy @ info@systematech.us.

SystemATech

Global Training Company
Contact: 1 (803) 474-4407
www.systematech.us

Systematech is a full-service training firm offering training, certifications, and job placement in IT and Infosec.

Exhibit VI

Enrollment Agreement

Systematech Co.

4123 Stone Pass Drive Graniteville, South Carolina 29829

803-474-4407

Student Information

Student Name: _____

Address: _____

City/State/Zip: _____

Home Number: _____

Mobile Number: _____

E-mail: _____

Emergency Contact: _____

Number: _____

PROGRAM INFORMATION

Name of Program: _____

Hours/Units: _____

Date of Admission: _____

Program Start Date: _____

Anticipated End Date: _____

<input type="checkbox"/> Full-Time	<input type="checkbox"/> Part-Time	<input type="checkbox"/> Day	<input type="checkbox"/> Evening
------------------------------------	------------------------------------	------------------------------	----------------------------------

Days/Evenings Class Meets: (*circle*) Mon. Tues. Wed. Thurs. Fri. Sat. Sun.

Time of Day/Evening Class Begins	
Time of Day/Evening Class Ends	
Number of Weeks	
Total Clock Hours	

SYSTEMATECH CO.

TUITION

REGISTRATION FEE: \$ _____

TUITION: \$ _____

BOOKS/SUPPLIES: \$ _____

MISC. EXPENSES: \$ *(itemize below)*

- Itemize item and cost _____
- Itemize item and cost _____
- Itemize item and cost _____
- Itemize item and cost _____
- Itemize item and cost _____

TOTAL COST: \$ _____

- Payment method can be cash, credit card, or money orders.
- Prices for books and supplies are subject to change.
- Tuition and associated fees must be paid in full by the middle of the session.

Note: Third-party loans must be repaid according to the terms of the note even if the borrower does not complete his or her education, cannot get a job after completion of the program, or is dissatisfied with the education.

Please read each statement carefully. Mark each to your understanding and sign at the bottom.

Please read each statement carefully. Mark each to your understanding and sign at the bottom.

- I have received a copy of the catalog and enrollment agreement.
- I understand the tuition charges, payment options, and refund policy.
- I understand tuition must be paid in full before graduation.
- I understand completion of the program does not guarantee employment.
- I acknowledge that this agreement becomes a legally binding contract once completed and signed by both parties.
- I understand SystemATech makes no claim or guarantee that credit earned will transfer to another institution.
- I understand a certificate of completion is awarded at graduation.
- I understand that Third-party loans must be repaid according to the terms of the note even if the borrower does not complete his or her education, cannot get a job after completion of the program, or is dissatisfied with the education.

Student Name Print: _____

Date: _____