IT Security & Network Administrator Program

Admission Requirements: Students must be 18 years of age or older at the time of enrollment, must present a valid ID for verification, and must present evidence of completing high school or high school equivalency.

Program Description: The IT Network and Security Administrator Certification Program is an immersive and accelerated training program with a focus on creating the next generation of IT professionals. You will attend courses, do hands on labs, and apply your learning to successfully complete projects that address different topics such as networking and security fundamentals. Throughout the program you will interact with experts who will guide you through the program, answer questions, and help with labs and projects. The program will end with a capstone project where you will apply your learnings to real life information technology challenges. This is a 12-weeks program that includes 10 weeks of certification training and 2 weeks for exam preparation. Graduates of this program will learn critical skills for different network and security careers and will have access to career services as well.

Prerequisites: This program is aimed at those considering a career in IT and computer-related fields. There are no prerequisites for you to meet to successfully start this course.

Objectives:

This program covers following topics:

Networking Fundamentals

- Explain what bounded networking media is
- Identify major network communication methods along with basic network theory concepts.
- Explain what unbounded network media is
- Identify TCP/IP data delivery and addressing methods
- Analyze switching and routing technologies
- Identity the major kinds of network deployments
- Identify TCP/IP deployment components
- Deploy network security
- Analyze network security
- Identify virtualization and cloud computing components
- Identity WAN deployment components
- Identify remote network deployment components
- Troubleshoot network issues
- Manage networks

Security Fundamentals

- Proactively implement sound security protocols to mitigate security risks
- Quickly respond to security issues

- Retroactively identify where security breaches may have occurred
- Design a network, on-site or in the cloud, with security in mind
- System/Network Security
- Security Threats (Social Engineering, Malware)
- Identity and Assess Management

Program Outline:

CIP Number: 11.1003

Code	Course	Lecture	Lab	Total Hours
ITSNA	CompTIA Net+	12	24	36
ITSNA	CompTIA Sec+	30	24	54
Total Hours		42	48	90
Associated Industry Certifications*: CompTIA Network+, CompTIA Security+				

** 1 Examination voucher included. It is the student's responsibility to take all certification exams within twelve months of completion of their original program completion date at that time, all exam vouchers expire. All extensions must be approved by the school director.*

Program Fee*:	**$4,000**

**(Inclusive of registration, tuition fee, 1 exam cost, curriculum guides)*

Cost Per Single Subject*:	**N/A**

Class Schedule: This program is offered on-demand with optional weekly hours scheduled with course mentors. Students may access their program and complete coursework at any time within their enrollment term.

Instructional Methods: 1. Lecture 2. Laboratory

Class Dates: This program is offered on-demand with optional weekly hours scheduled with course mentors. Students may access their program and complete coursework at any time within their enrollment term.

See the school catalog for student technology requirements for online participation and school holidays and office hours.

Code: IT Security & Network Administrator Program

Subject Description:

1. **CompTIA Network+**

CompTIA Network+ validates the technical skills needed to securely establish, maintain and troubleshoot the essential networks that businesses rely on.

- Establish network connectivity by deploying wired and wireless devices.
- Understand and maintain network documentation.
- Understand the purpose of network services, basic datacenter, cloud, and virtual networking concepts.
- Monitor network activity, identifying performance and availability issues.
- Implement network hardening techniques.
- Manage, configure, and troubleshoot network infrastructure.

2. **CompTIA Security+**

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions
- Monitor and secure hybrid environments, including cloud, mobile, and IoT
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance
- Identify, analyze, and respond to security events and incidents

Subject Hours:
Lecture-42 / Lab-48 / Total - 90

Prerequisites:

This program is aimed at those considering a career in IT and computer-related fields. There are no prerequisites for you to meet to successfully start this course

Objectives:

This program covers following topics:

Networking Fundamentals

- Explain what bounded networking media is.
- Identify major network communication methods along with basic network theory concepts.
- Explain what unbounded network media is.
- Identify TCP/IP data delivery and addressing methods.

- Analyze switching and routing technologies
- Identity the major kinds of network deployments
- Identify TCP/IP deployment components
- Deploy network security
- Analyze network security
- Identify virtualization and cloud computing components
- Identity WAN deployment components
- Identify remote network deployment components
- Troubleshoot network issues
- Manage networks

Security Fundamentals

- Proactively implement sound security protocols to mitigate security risks
- Quickly respond to security issues
- Retroactively identify where security breaches may have occurred
- Design a network, on-site or in the cloud, with security in mind
- System/Network Security
- Security Threats (Social Engineering, Malware)
- Identity and Assess Management

Required textbook(s): Not applicable**.**

Instructional Methods: 1 Lectures
2. Lab simulations

Student/Instructional Ratios: **18:1**

Materials and Media Refences: Not Applicable

Content Outline:

Week 1	CompTIA Network+: Comparing OSI Model Network Functions CompTIA Network+: Deploying Ethernet Cabling CompTIA Network+: Deploying Ethernet Switching CompTIA Network+: Troubleshooting Ethernet Networks
Week 2	CompTIA Network+: Explaining IPv4 Addressing CompTIA Network+: Supporting IPv4 and IPv6 Networks CompTIA Network+: Configuring and Troubleshooting Routers CompTIA Network+: Explaining Network Topologies and Types
Week 3	CompTIA Network+: Explaining Transport Layer Protocols CompTIA Network+: Explaining Network Services CompTIA Network+: Explaining Network Applications CompTIA Network+: Ensuring Network Availability CompTIA Network+: Explaining Common Security Concepts
Week 4	CompTIA Network+: Supporting and Troubleshooting Secure Networks CompTIA Network+: Deploying and Troubleshooting Wireless Networks CompTIA Network+: Comparing WAN Links and Remote Access Methods
Week 5	CompTIA Network+: Explaining Organizational and Physical Security Concepts CompTIA Network+: Explaining Disaster Recovery and High Availability Concepts CompTIA Network+: Applying Network Hardening Techniques CompTIA Network+: Summarizing Cloud and Datacenter Architecture
Week 6	CompTIA Security+: Comparing Security Roles and Controls CompTIA Security+: Explaining Threat Actors and Threat Intelligence CompTIA Security+: Performing Security Assessments CompTIA Security+: Identifying Social Engineering and Malware CompTIA Security+: Summarizing Basic Cryptographic Concepts
Week 7	CompTIA Security+: Implementing Public Key Infrastructure CompTIA Security+: Implementing Authentication Controls CompTIA Security+: Implementing Identity and Account Management Controls CompTIA Security+: Implementing Secure Network Designs
Week 8	CompTIA Security+: Implementing Network Security Appliances CompTIA Security+: Implementing Secure Network Protocols CompTIA Security+: Implementing Host Security Solutions CompTIA Security+: Implementing Secure Mobile Solutions CompTIA Security+: Summarizing Secure Application Concepts
Week 9	CompTIA Security+: Implementing Secure Cloud Solutions CompTIA Security+: Explaining Data Privacy and Protection Concepts CompTIA Security+: Performing Incident Response CompTIA Security+: Explaining Digital Forensics
Week 10	CompTIA Security+: Summarizing Risk Management Concepts CompTIA Security+: Implementing Cybersecurity Resilience CompTIA Security+: Explaining Physical Security Exam preparation
Week 11	EXAM Preparation
Week 12	EXAM Preparation

Grading and Certificate of Completion: Grades are assessed based on the student's attendance, online lab completions, and offline projects.

90%+	A – Excellent
80-89.9%	B – Good
70-79.9%	C – Satisfactory
60-69.9%	D – Below Average
Below 60%	F – Very Poor/Fail
	I – Incomplete

- Attendance = 75% of grade
- Successful completion of labs = 15% of grade
- Projects/post-class assessment = 10% of grade

Upon program completion with a passing grade, students will receive a certificate of completion. Students are highly encouraged to take the industry-standard exam to receive a certification credential through the granting body or vendor.

See the school catalog for student technology requirements for online participation and school holidays and office hours.