Network Security Certificate of Accomplishment - Active

Department: Computer Networking & Information Technology

Approval: December 2012

This certificate includes instruction in the measures that must be taken to detect and prevent network security mistakes and vulnerabilities, and includes descriptions of common attacks and methods to configure the operating system, servers, routers, firewalls, and email. Students completing this certificate program will be qualified for employment in entry-level network security positions and be able to prepare for CompTIA Security+ exam.

Learning Outcomes
Upon completion of this program, students will be able to:

- Explain the basics of network security.
- Define confidentiality, integrity, availability, and non-repudiation (CIAN).
- Recognize viruses and worms, their differences and how to harden computer systems.
- Apply strategies for network defense using firewalls, routers, switches, antivirus, and anti-spyware tools.
- Protect the IT environment using hacking techniques.
- Discover hidden data in memory and hard drive using forensics rules, tools and techniques.

Students must complete each course with a grade of "C" or higher. A grade of Pass/No Pass cannot be applied towards CNIT degrees or certificates.

The minimum time for completion of this certificate is 2 semesters. Completion time will vary based on student preparation and number of classes completed per semester.

Courses Required for the Certificate of Accomplishment in Network Security

Course	Units
Required courses:	
CNIT 106 - Introduction to Networks	3.00
CNIT 120 - Network Security	3.00
CNIT 122 - Firewalls	3.00
CNIT 123 - Ethical Hacking & Network Defense	3.00
Total:	12.00
Choose one of the following courses:	
CNIT 124 - Advanced Ethical Hacking	3.00
CNIT 121 - Computer Forensics	3.00
CNIT 125 - Information Security Professional Practices	3.00
Total:	3.00
Total:	**15.00**

Generated on: 4/20/2017 7:21:45 PM