WASHINGTON TECHNICAL INSTITUTE

CYB-201: Fundamentals of Network Defense

Description:
3 credits/126 hours
Prerequisite: None

This course will introduce the latest trends, developments, and technology within information security. It will provide students with a balanced focus that addresses all aspects of information security, beyond simply a technical perspective. Students will gain a solid foundation in information systems and cyber security.

Textbook: CompTIA Security+ Guide to Network Security Fundamentals, 7th ed. Ciampa– ISBN: 978-0-357-42437-7

Course objectives:
Throughout the course, you will meet the following goals:

- Gain a strong foundational understanding of the history of and need for information security
- Be able to explain and implement information technology concepts and processes
- Understand how to complete risk management assessments and build a strong information security plan
- Develop an understanding of the legal and ethical professional issues in information security
- Navigate information security concepts as they pertain to staff and personnel and overall security technology such as access controls, firewalls, and VPNs.

Contents:
Module 1: Introduction to Security
Module 2: Threat Management and Cybersecurity Resources
Module 3: Threats and Attacks on Endpoints
Module 4: Endpoint and Application Development Security
Module 5: Mobile, Embedded, and Specialized Device Security
Module 6: Basic Cryptography
Module 7: Public Key Infrastructure and Cryptographic Protocols
Module 8: Network Threats, Assessments, and Defenses
Module 9: Security Technology: Intrusion Detection and Prevention Systems and other Security Tools
Module 10: Cryptography
Module 11: Implementing Information Security
Module 12: Information Security Maintenance

Grading Scale	**Grade Weighting**	
A = 95-100%	**Chapter Quizzes……**	**50%**
B = 88-94.9%	**Activities ……..... **	**20%**

C = 80-87.9%
D = 70-79.9%
F = Below 70%

Final Exam ……..... 30%
100%