CYBERSECURITY ASSOCIATE OF SCIENCE

This degree provides graduates with foundational cybersecurity skills across a wide range of modern cybersecurity pillars including digital forensics, network security and defense, and penetration testing. In this program students receive extensive hands-on experience and develop the knowledge and abilities necessary to succeed in protection of an organization's data and operations. It is a rigorous program designed to help students master the fundamentals of cybersecurity by applying industry-accepted and emerging practices to solve real-world security problems. Upon completion of the program, students will be able to evaluate security trends, recognize best practices, and understand Information Technology security products and threats. This program also provides preparation for several nationally recognized, high demand certifications in the field of Cybersecurity.

Required Courses – Major:		**Units**
CSC 116	Information and Communication Technology Essentials	4
CSC 117	Computer Network Fundamentals	3
CSC 118	Introduction to Information Systems Security	3
CSC 152	Network OS and Administration	3
CSC 154	Network Security	3
CSC 156	Digital Forensics Fundamentals	3
CSC 158	Introduction to Cybersecurity: Ethical Hacking	3
CSC 159	Fundamentals of Penetration Testing	4
CSC 161	Cloud Infrastructure and Security	3
CSC 221	Programming and Algorithms I	3
Plus 3 additional units selected from the following:		**Units**
BUS 107	Customer Service	3
BUS 134	Human Relations in Business	3
BUS 170	Business Communication Skills for Managers	3

Total Major Units	**35**
Total Degree Units	**60**

Program Level Student Learning Outcomes:

1. Define best practices for computer forensics investigations.
2. Define the requirements for proper evidence collection, chain of custody and investigation reporting.
3. Apply strategies for network defense using firewalls, routers, switches, and anti-malware tools.
4. Design organizational plans for securing data while maintaining the confidentiality, integrity, and availability (CIA) of the information transmitted over communication networks.
5. Define best practices for penetration testing.
6. Implement penetration testing across a wide range of scenarios including internal/external/perimeter network penetration testing, web application penetration testing, and cloud penetration testing.

Career Opportunities in COMPUTER SCIENCE

This program prepares students for careers in the Cybersecurity field. Some common job titles and careers for this certificate include forensic analysts, cybercrime investigators, cyber defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, IT Security analyst, security operations center (SOC) analyst, vulnerability analyst, cybersecurity specialist, threat intelligence analyst, security engineer, cybersecurity analyst, ethical hackers, penetration testers, network server administrators, firewall administrators, security testers, system administrators and risk assessment professionals, information security analyst, and network security penetration testers.