THE ASSOCIATE OF APPLIED SCIENCE (A.A.S.)

The Associate of Applied Science Degree is designed for employment purposes, and it should not be assumed that the degree or the courses in the degree can be transferred to another institution. While a few institutions have recently begun to accept some courses in A.A.S. programs, the general rule is that courses in the A.A.S. degree are not accepted in transfer toward bachelor's degrees. Students to whom transfer is important should get assurance in writing in advance from the institution to which they wish to transfer.

ATTENTION STUDENTS: PLEASE SEE CURRENT CATALOG FOR ALL FEES AND CHARGES ASSOCIATED WITH THIS DEGREE.

DEGREE PLAN
ASSOCIATE OF APPLIED SCIENCE IN CYBERSECURITY
Degree Code: 0151 CIP Code: 11.1003

The program is designed for those students seeking career-oriented skills who can identify, assess, and manage cybersecurity threats. The two-year degree prepares students to defend computer operating systems, networks, and data from cyber attacks.

Student Learning Outcomes for Cybersecurity Program

The Associate of Applied Science in Cybersecurity prepares graduate for entry-level employment and advancement. Students simulate real-world cybersecurity threat scenarios and create opportunities for ethical hacking, security monitoring, analysis and resolution. Students configure and use threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization. The program emphasizes the practical application of the skills needed to maintain and ensure secure operational readiness of systems within an organization.

1. Be employable as an associate security analyst, incident responders, network security analyst, or cybersecurity risk analyst.
2. Implement data confidentiality, integrity, availability and security controls on networks, servers and applications.
3. Develop security principles and policies that comply with cybersecurity laws.
4. Explain the use of technologies, processes and procedures to defend all components of a network.
5. Develop career skills by combining classroom theory with hands-on practical applications.
6. Demonstrate critical thinking, complex problem solving, and collaboration.

Name: _____ Date: _____
Advisor: _____ Student ID# _____

COURSE CODE		COURSE NAME	CREDIT HOURS	HOURS COMPLETED
General Education Requirements (18 credit hours)				
BUS	2563	Business Communications	3	_____
CIS	2503	Microcomputer Business Applications	3	_____
ENG	1003	Composition I (must earn a "C" or better)	3	_____
ENG	1013	Composition II (must earn a "C" or better)	3	_____
MATH	1113	Applied Math or higher-level mathematics course	3	_____
POSC	2103	United States Government	3	_____
Business and Computer Core (15 credit hours)				
CIS	1023	Programming Fundamentals/Logic	3	_____
CIS	1203	Introduction to Computers	3	_____
CIS	1513	Object Oriented Programming	3	_____
CIS	2723	Cybersecurity Essentials	3	_____
CIS	1103	Networking Concepts	3	_____
Cybersecurity Content (27 credit hours)				
BUS	2843	Project Management	3	_____
CIS	1106	CISCO Network Academy I	6	_____
CIS	1206	CISCO Network Academy II	6	_____
CIS	2683	Computer Forensics	3	_____
CIS	2463	Linux	3	_____
CIS	2913	Ethical Hacking	3	_____
CRJ	2243	Cybersecurity Law and Ethics	3	_____

Program Total 60 Hours