CYBERSECURITY OPTION, ASSOCIATE IN APPLIED SCIENCE

Program Description

The **Cybersecurity Option** within the Associate in Applied Science in Computer Science / Information Technology is designed for students seeking to develop practical skills in protecting computer systems, networks, and digital information. This career-focused option prepares students for entry-level roles supporting cybersecurity operations across business, government, and nonprofit organizations.

Students learn how to identify and respond to security threats, manage network security, and implement strategies to safeguard digital systems and data. Coursework emphasizes hands-on learning in areas such as cybersecurity fundamentals, network defense, system security, and risk management. Students develop technical troubleshooting skills while gaining an understanding of cybersecurity policies, ethical practices, and industry standards.

The program prepares graduates for workforce entry while also supporting continued professional development through industry certifications and advanced training.

Transfer Information

The Cybersecurity Option is part of the A.A.S. in Computer Science / Information Technology, which is designed primarily as a career-focused degree and is not structured under the New Jersey Statewide Transfer Agreement. Students interested in pursuing a bachelor's degree should consult with Advising & Transfer Services to explore articulation agreements or credit evaluation options at their intended transfer institution.

Students may also pursue industry-recognized certifications to strengthen their career opportunities in cybersecurity and information technology.

Career Information

The A.A.S. in Computer Science / Information Technology – Cybersecurity Option prepares graduates for entry-level roles in cybersecurity and information technology support.

Potential career paths include:

- Cybersecurity Support Specialist
- Network Security Technician
- Information Security Analyst (entry-level)
- Security Operations Center (SOC) Technician
- IT Security Support Specialist
- Systems or Network Support Technician

Students are encouraged to consult with faculty and Career Services to explore certification pathways, internships, and career opportunities in cybersecurity and information technology.

First Semester		Credit Hours
ENGL 151	English I	3
MATH 151	A Survey of Mathematics (or Higher)	3-4
CSIT 165	Programming I	4
CSIT 144 Introduction to Operating System Using Linux		3
Humanities or Social Science Gen. Ed. Requirement (https://catalog.ocean.edu/academic-information/general-education/#humanities)		3
	Credit Hours	**16-17**
Second Semester		
ENGL 152	English II	3
CSIT 145	Computing Fundamentals	3
CSIT 166	Programming II	4
CSIT 185	Networking I	3
CSIT 242	Penetration Testing Fundamentals	3
	Credit Hours	**16**
Third Semester		
CSIT 168	Introduction to Python Programming	2
CSIT 200	Information Security Fundamentals	3
CSIT 241	Cybersecurity Legal and Regulatory Overview	3
Any Gen. Ed. Requirement (https://catalog.ocean.edu/academic-information/general-education/#general education)		3
CSIT Elective (CSIT 115 or Higher)		3-4
	Credit Hours	**14-15**
Fourth Semester		
CSIT 240	Ethical Hacking: Hacker Techniques and Tools	3
CSIT 243	Cisco Networking Fundamentals	3
CSIT 244	Digital Forensics Fundamentals	3
Elective(s) to make 60 credits		3-5
	Credit Hours	**12-14**
	Total Credit Hours	**58-62**

The Cybersecurity option in the Computer Science/Informational Technology, Associate in Applied Science is designed to provide students the opportunity to apply their work experience to earning an associate degree in applied science. Students can earn credit for their work experience while they prepare for career advancement. Up to 17 credits may be awarded for work experience, including military experience, trade/proprietary school preparation, apprenticeship programs, certifications, and on-the-job-training.

Learning Outcomes

1. Explain the current topics and techniques of cybersecurity.
2. Apply the concepts, principles, and technologies of information security.
3. Demonstrate foundational computer science and cybersecurity knowledge.
4. Demonstrate an understanding of cryptography, authentication, and intrusion detection technologies.