BACHELOR OF APPLIED SCIENCE - COMPUTER INFORMATION SYSTEMS TECHNOLOGY, CYBERSECURITY SPECIALIZATION

Previous Degree Required: A.S./A.A.
Eligible for Financial Aid: Yes
Delivery Method(s): On-Campus, Hybrid
Location(s): Palm Bay
Additional Limited Access Application Process Required: No
Program Testing Requirements: Not Required
Academic Community: STEM
Program Code: CTBSCSCT
Classification of Instructional Programs (CIP) Code: 11.0401
Florida Department of Education CIP Code: 1101104011

The Cybersecurity Bachelor's Degree specialization at Eastern Florida State College prepares students for entry-level positions involving the fast-expanding field of computer security. Students will gain a fundamental understanding of cybersecurity and can specialize in one or more of the following areas.

- Database security
- Network security
- Application software security
- Forensics

Potential career positions include Software Developer, Database Administrator, Web Developer, Computer Forensics Technician and Network Security Analyst.

Refer to the Bachelor Degree Programs overview page to find information about admission, graduation, general education and other requirements. Students who need technical electives will work with a bachelor's advisor to determine the courses best suited to their plan of study.

Visit the program page for more details and how to apply.

Specialization Requirements

Code	Title	Credit Hours
Associate Degree		
Complete Associate Degree		60
General Education or Technical Concentration		
General Education (for A.S. degree students) or Technical Concentration (for A.A. degree students)		21
Computer Information Systems Technology - Major Courses		
GEB 3213	Foundations of Managerial Communications	3
ISM 3011	Introduction to Information Technology Management	3
ISM 4300	Information Systems Operations Management	3
MAN 4504	Operational Decision Making	3
Cybersecurity Specialization Major Courses		
CISC 3391	Computer Forensics	3
CISC 3392	Windows Forensics	3
CNT 3403	Network Defense Security	3
COP 3703	Database Design and Architecture	3
ISM 3321	Cybersecurity Fundamentals	3
ISM 3322	Advanced Cybersecurity Concepts	3
Cybersecurity Specialization Electives (Choose 9 Credits)		**9**
CEN 4341	Platform Technologies	
CEN 4949	Internship	
CNT 4704	Network Planning and Design	
COP 3330	Object Oriented Programming	
COP 3813	Internet Programming	
COP 4849	Web Applications Programming	
ISM 3113	Information Systems Analysis and Design	
ISM 3324	Applications in Information Security	
Total Credit Hours		**120**

- Satisfy the foreign language competency requirement
- Satisfy the civic literacy competency requirement

Important Note: Computer Information Systems Technology has two Common Program Prerequisites. hese courses must be completed with a grade of "C" or higher before being admitted to 3000 - 4000 level courses.

- COP 2334 Introduction to C++ Programming
- STA 2023 Statistics

Click on the course number to see course prerequisites. MAC 2311 will be accepted in place of STA 2023. Any Computer Programming course with a COP prefix will be accepted in place of COP 2334. No other course substitutions are permitted for either course.

Course Sequence

The following sequence is recommended. However, courses may not be offered in this order, so it is important that you work with an advisor to plan your schedule based on your specific needs.

Course	Title	Credit Hours
Term 1		
ISM 3011	Introduction to Information Technology Management	3
GEB 3213	Foundations of Managerial Communications	3
Technical Electives [1]		6
	Credit Hours	**12**
Term 2		
ISM 3113	Information Systems Analysis and Design	3
Technical Electives [1]		9
	Credit Hours	**12**
Term 3		
CISC 3391	Computer Forensics	3
ISM 4300	Information Systems Operations Management	3
	Credit Hours	**6**

Term 4		
CNT 3403	Network Defense Security	3
COP 3703	Database Design and Architecture	3
ISM 3321	Cybersecurity Fundamentals	3
MAN 4504	Operational Decision Making	3
	Credit Hours	**12**
Term 5		
CISC 3392	Windows Forensics	3
ISM 3322	Advanced Cybersecurity Concepts	3
Technical Electives [1]		6
	Credit Hours	**12**
Term 6		
Technical Electives [1]		6
	Credit Hours	**6**
	Total Credit Hours	**60**

[1] Students must select 9 credits from the following Cybersecurity Electives list: CEN 4341 Platform Technologies, CEN 4949 Internship, CNT 4704 Network Planning and Design, COP 3330 Object Oriented Programming, COP 3813 Internet Programming, COP 4849 Web Applications Programming, ISM 3113 Information Systems Analysis and Design, and ISM 3324 Applications in Information Security. Students are required to take 21 additional technical electives.

Learning Outcomes

1. Demonstrate the ability to use current techniques, skills, and tools necessary for the evaluation of information systems.
   - *Core Ability Supported: Think Critically and Solve Problems*
2. Systematically analyze data to improve organizational input and output processes, productivity and quality of work for users.
   - *Core Ability Supported: Process Information*
3. Demonstrate comprehensive understanding for information and network security; planning, risk management, security technologies, and personnel
   - *Core Ability Supported: Think Critically and Solve Problems*
4. Apply techniques for network design and network security defense.
   - *Core Ability Supported: Think Critically and Solve Problems*
5. Apply techniques for collecting and analyzing forensic data, computer systems and media using readily available open forensic investigative source tools available for popular commercial operating systems.
   - *Core Ability Supported: Think Critically and Solve Problems*
6. Apply techniques for storage and retrieval of data to support the organization's functional units and external customers.
   - *Core Ability Supported: Process Information*
7. Demonstrate the ability to design and write high quality computer programs that are well organized and documented.
   - *Core Ability Supported: Think Critically and Solve Problems*
8. Apply tools and techniques for mitigating security breaches in the Software Development Life Cycle (SDLC), considering security and privacy concerns in establishing system requirements, analysis and design artifacts, source code, quality assurance testing plans, installation and deployment strategies, and maintenance techniques.
   - *Core Ability Supported: Think Critically and Solve Problems*
9. Explain the fundamentals of cybersecurity and its impact on information systems, identify various types of cybersecurity threats, explain cybersecurity management methods and identify current security resources.
   - *Core Ability Supported: Think Critically and Solve Problems*
10. Assess network security controls and determine security concerns, authentication protocol services, network monitors, and secure data communication techniques.
    - *Core Ability Supported: Think Critically and Solve Problems*
11. Determine lab requirements for live acquisition analysis and list current tools, compare current tools for data collection and analysis, explain forensically sound data collection and storage techniques and create a live response testing environment.
    - *Core Ability Supported: Think Critically and Solve Problems*
12. Design implementation strategies for securing web information, apply techniques for securing information in web applications and web servers, examine vulnerabilities, threats and attacks and recommend strategies for securing web information.
    - *Core Ability Supported: Think Critically and Solve Problems*