Cybersecurity B.S.

A Bachelor of Science degree program in Cybersecurity prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; Internet of Things (IoT); security system design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.

In accordance with the standards set forth by the Computing Accreditation Commission (CAC) of ABET, graduates from a Cybersecurity program will have the ability to:

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
3. Communicate effectively in a variety of professional contexts.
4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
5. Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
6. Apply security principles and practices to maintain operations in the presence of risks and threats.

Core Curriculum Courses		
See the Core Curriculum Requirements (https://coursecatalog.tamuc.edu/undergrad/core-curriculum-requirements/)		42
Required courses in the major		
COSC 1436	Introduction to Computer Science and Programming	4
COSC 1437	Programming Fundamentals II	4
COSC 2325	Introduction to Machine Language and Digital Logic	3
COSC 2336	Data Structures and Algorithms	3
CSCI 303	Technical Communication for Computing Professionals	3
CSCI 310	Cybersecurity	3
CSCI 340	Database	3
CSCI 345	Data Security and Privacy	3
CSCI 360	Cryptography	3
CSCI 399	Junior Cyber Design Project	3
CSCI 415	Ethics, Law & Cybersecurity	3
CSCI 430	Operating Systems	3
CSCI 434	Computer Networks	3
CSCI 451	Wireless and Mobile Security	3
CSCI 452	Malware Analysis and Reverse Engineering	3
CSCI 458	Network Security & Management	3
CSCI 459	AI Enhanced Security	3
CSCI 463	Systems Security & Trusted Computing	3
CSCI 465	Smart Things Security	3
CSCI 499	Senior Cyber Design Project	3
Required support courses		
MATH 2413	Calculus I *	
MATH 2414	Calculus II *	
MATH 2305	Discrete Mathematics *	
MATH 403	Mathematical Statistics II	3
ECO 2301	Prin Macro Economics *	
or ECO 2302	Principles of Micro Economics	
PHYS 2425	University Physics I *	
PHYS 2426	University Physics II *	
Advanced Cyber Elective		**9**
A minimum of three (3) courses, nine (9) credit hours must be selected from the following list.		
CSCI 323	Secure Programming	

CSCI 324	Software Engineering	
CSCI 352	Digital Forensics	
CSCI 353	Threat and Vulnerability Management	
CSCI 419	Secure Software Development	
CSCI 421	Intrusion Detection & Prevention	
CSCI 422	Cloud Computing & Security	
CSCI 489	Independent Study	
CSCI 497	Special Topics	
Total hours		**120**

* These courses should be used to satisfy the Core Curriculum Requirements in Social and Behavioral Science, Natural Sciences, Mathematics, and Language, Philosophy, & Culturerespectively; otherwise, the credit hours required to earn the B.S. in Cybersecurity will exceed 120.
A grade of “C” or higher must be earned in Required Courses, Required Support Courses, and Advanced Cybersecurity Electives in this major.

First Year

Fall	**Hours**
Delete This Text	
	0

Total Hours: 0