CYBERSECURITY - SECURITY ENGINEERING EMPHASIS REQUIREMENTS (MS)

The Master of Science (M.S.) in Cybersecurity program offers studies in core areas of cybersecurity that include offensive and defensive security operations, security awareness training, security tools design and implementation, cybersecurity management, security policy and law, and emerging areas in security and privacy. The proposed program offers both hands-on experiential learning and in-depth theoretical studies.

The M.S. in Cybersecurity is designed for both professionals and recent college graduates who aspire to advance their careers in cybersecurity. The degree program consists of 30 credits, including 15 credits of core courses and 15 credits of courses in an emphasis area: either cyber resilience or security engineering. The program will prepare students to obtain positions such as cybersecurity analyst, cybersecurity manager, cybersecurity engineer, or cybersecurity architect.

Degree Requirements

To earn this degree, students must satisfy all of the following requirements.

1. Complete the Common Body of Knowledge courses, or have prior coursework or experience in all topics that are included in the Common Body of Knowledge.
2. Complete all M.S. Cybersecurity core courses.
3. Complete one emphasis: either Cyber Resilience or Security Engineering.
4. Pass the M.S. Cybersecurity comprehensive exam for the selected emphasis. Students in the Security Engineering emphasis may choose to complete a capstone project (CYBER 789) or thesis (CYBER 799) in place of the comprehensive exam.
5. Have a graduate grade point average (GPA) of at least 3.0.

Code	Title	Units
Common Body of Knowledge		**0-9**
CYBER 701	SYSTEMS FUNDAMENTALS FOR CYBERSECURITY	
COMPSCI 170	INTRODUCTION TO PYTHON PROGRAMMING	
or COMPSCI 172	INTRODUCTION TO JAVA	
or COMPSCI 174	INTRODUCTION TO C++	
or ITSCM 180	INTRODUCTION TO PROGRAMMING FOR BUSINESS APPLICATIONS	
COMPSCI 220	INTERMEDIATE JAVA [1]	
or COMPSCI 222	INTERMEDIATE C++	
Core Courses		
CYBER 730	FUNDAMENTALS OF ETHICAL HACKING	3
CYBER 731	MANAGEMENT OF INFORMATION ASSURANCE AND SECURITY	3
CYBER 740	CYBERSECURITY AND PRIVACY LAW	3
CYBER 742	COMPUTER FORENSICS	3
CYBER 754	INTRUSION PREVENTION AND DETECTION	3
COMPSCI 750	SYSTEM AND SOFTWARE SECURITY	3
COMPSCI 755	CRYPTOGRAPHY AND SECURITY PROTOCOLS	3
Select 9 units from the following list:		**9**
CYBER 747	EMBEDDED SYSTEM SECURITY	
CYBER 752	MALWARE REVERSE ENGINEERING	
CYBER 758	CLOUD SECURITY	
CYBER 759	TOPICS IN CYBERSECURITY	
CYBER 789	CYBERSECURITY CAPSTONE PROJECT	
CYBER 799	THESIS RESEARCH	
COMPSCI 724	OPERATING SYSTEMS IN PRACTICE	
COMPSCI 766	ADVANCED DATABASES	
COMPSCI 767	BIG DATA AND DATA MINING	
Total Units		**30-39**

[1] or equivalent coursework or experience