MASTER OF CYBER SECURITY ENGINEERING

Rapid growth in the reliance of critical and personal information on cyber infrastructure has made us more vulnerable to cyber threats and cyberattacks. This master's program will educate students with techniques, tools, analysis, policies, and methodologies to solve complex cyber security problems of relevance to the engineering field.

There is a strong demand for security professionals in industries with the increase in cyber threats to their systems. This program will prepare students with extensive knowledge in cyber security, cyber-physical systems, cloud computing security, network engineering and cyber security for smart grid power systems, security vision systems, coding theory, and wireless secure communications.

Admission to the Master of Cyber Security Engineering program normally requires a bachelor of science degree in electrical or computer engineering from an institution accredited by the Accreditation Board of Engineering and Technology (ABET). Deficiency courses will be required for students who have not taken prerequisite or equivalent courses of the following: ECE 242 and MATH 374. A student may demonstrate proficiency by successfully completing the courses or by demonstrating satisfactory performance in one or more special examinations administered by the department.

Requirement	Credits
Minimum Credits Required	30
Maximum 400-Level Credit	12
Minimum 500-Level Credit	18
Maximum 700-Level Credit	4

Code	Title	Credit Hours
Core Courses		**(21-28)**
Select minimum 7 courses from the following:		21-28
ECE 518	Computer Cyber Security (required)	3
ECE 543	Computer Network Security (required)	3
ECE 420	Analytical Methods for Power System Economics and Cybersecurity	3
ECE 503	5G Wireless Network: Architecture, New Radio, and Security	3
ECE 504	Wireless Communication System Design	3
ECE 510	Internet of Things and Cyber Physical Systems	3
ECE 520	Information Theory and Applications	3
ECE 528	Application Software Design	3
ECE 541	Communications Networks Performance Analysis	3
ECE 545	Modern Internet Technologies	3
ECE 546	Wireless Network Security	3
ECE 573	Cloud Computing and Cloud Native Systems	3
Cyber Security Legal and Regulatory Course		**(2-3)**
Select 1 course from the following:		2-3
ECE 597	Special Problems (in Cybersecurity Law)	3
ITMS 538	Cyber Forensics	3
ITMS 578	Cyber Security Management	3
ITMS 584	Governance, Risk, and Compliance	3
LAW 215	E Commerce	2-3
LAW 252	Law of Privacy	3
LAW 285	Cyber Fraud-Priv Class Actions	2
LAW 295	Data Privacy and Security	2
LAW 478	Computer & Network Privacy	3
LAW 907	Law of Social Networks	2
LAW 926	Freedom of the Internet	2
Electrical and Computer Engineering Electives		**(7)**
Option to select two (2) courses from the following:		7
ECE 403	Digital and Data Communication Systems	3
ECE 408	Introduction to Computer Networks	3
ECE 437	Digital Signal Processing I	3

ECE 441	Smart and Connected Embedded System Design	4
ECE 446	Advanced Logic Design	4
ECE 501	Artificial Intelligence and Edge Computing	3
ECE 504	Wireless Communication System Design	3
ECE 508	Video Communications	3
ECE 511	Analysis of Random Signals	3
ECE 513	Communication Engineering Fundamentals	3
ECE 515	Modern Digital Communications	3
ECE 517	Modern Wireless Network Protocols and Standards	3
ECE 519	Coding for Reliable Communications	3
ECE 542	Design and Optimization of Computer Networks	3
ECE 544	Wireless and Mobile Networks	3
ECE 563	Artificial Intelligence in Smart Grid	3
ECE 565	Computer Vision and Image Processing	3
ECE 566	Machine and Deep Learning	3
ECE 569	Digital Signal Processing II	3
ECE 570	Fiber-Optic Communication Systems	3
ECE 573	Cloud Computing and Cloud Native Systems	3
ECE 585	Computer Organization and Design	3
ECE 586	Hardware Security and Advanced Computer Architectures	3
ECE 590	Object-Oriented Programming and Machine Learning	3
Total Credit Hours		**30-38**