CYBERSECURITY, MASTER OF SCIENCE (MS)

Required Core—this coursework provides core knowledge in the areas of cybersecurity research methods, advanced computer and information security, and advanced network security, engineering, and research methods.

CYBR 515	RESEARCH METHODS AND COLLOQUIUM	4
CYBR 525 & 525L	ADVANCED COMPUTER AND INFORMATION SECURITY and ADVANCED COMPUTER AND INFORMATION SECURITY LAB	4
CYBR 535 & 535L	ADVANCED NETWORK SECURITY and ADVANCED NETWORK SECURITY LAB	4
CYBR 599	DIRECTED STUDY	4
Choose One Concentration		**20**
General Cyber Concentration		
CYBR 505	PROJECT MANAGEMENT FOR CYBERSECURITY	
Choose four courses from the approved elective list at least three course must be at the 500-level. Note: this coursework provides the student an opportunity to take courses specialized to their particular area(s) of interest. Any 400-level or non-CYBR course must be approved by the CYBR graduate coordinator or the student's graduate committee chair. The course CYBR 539 may each apply more than once, provided distinct topics are studied.		
Secure AI Concentration		
All courses must be completed for the Secure AI designation. (If the CSCD courses or the CYBR 580 course have already been completed, choose 500-level CYBR elective courses.)		
CSCD 584 & 584L	MACHINE LEARNING and MACHINE LEARNING LAB	
CSCD 585 & 585L	DEEP LEARNING and DEEP LEARNING LAB	
CYBR 580 & 580L	AI FUNDAMENTALS and AI FUNDAMENTALS LAB	
CYBR 586 & 586L	AI METHODS AND VALIDATION and AI METHODS AND VALIDATION LAB	
CYBR 588 & 588L	SECURING AI and SECURING AI LAB	
Thesis or Project - A Minimum of 12 Credits are Required		
Note: The student is expected to expand their knowledge with a published thesis or to apply their knowledge to a significant project. Projects may be work-related. The thesis or project is defended in a final oral examination of the student's work.		
CYBR 600	THESIS	12
or CYBR 601	RESEARCH REPORT	
Total Credits		**48**

Students who earn an MS in Cybersecurity from EWU should be able to:

General MS Cybersecurity Concentration

- demonstrate cybersecurity principles in the securing of networks and software systems;
- possess an advanced understanding of core cybersecurity knowledge;
- use advanced cybersecurity skills in securing of networks and the development of software systems.

Secure AI Concentration

- demonstrate cybersecurity principles in the securing of networks and software systems;
- possess an advanced understanding of core cybersecurity knowledge;
- use advanced cybersecurity skills in securing of networks and the development of software systems;
- Understand the Legal and Ethical Implications: Navigate the legal and ethical considerations specific to AI security, including privacy, accountability, and the impact of AI on society;
- Understand AI and Machine Learning Fundamentals: Grasp the core principles of AI, including machine learning, neural networks, and data science, which underpin AI systems;
- Assess AI System Vulnerabilities: Identify and analyze potential vulnerabilities in AI models, including data poisoning, adversarial attacks, and model inversion;

- Secure AI Pipelines: Implement security measures throughout the AI development pipeline, from data collection and preprocessing to model training, deployment, and maintenance;
- Defend Against Adversarial Attacks: Develop strategies to protect AI models from adversarial attacks, which involve malicious inputs crafted to deceive the AI system;
- Ensure Data Integrity: Protect the integrity and confidentiality of the data used in AI systems, ensuring that the data is free from tampering and bias;
- Mitigate Bias and Fairness Issues: Identify and mitigate bias in AI systems to ensure fair and ethical outcomes, especially in high-stakes applications;
- Design Robust AI Systems: Create AI systems resilient to attacks, errors, and other disruptions, ensuring reliable and secure performance in various environments;
- Monitor AI System Performance: Monitor AI systems to detect and respond to security threats, performance degradation, and unexpected behaviors.