MASTER OF SCIENCE IN CYBERSECURITY

Course Listings

Management Core (Three Courses)

- MSM 505 Project Management
- MSM 508 Risk Management
- MSM 525 Spirit of Enterprise

Cybersecurity Concentration (Seven Courses)

- MIS 503 Cybersecurity Fundamentals
- MIS 504 Programming for Cybersecurity
- MIS 513 Advanced Cyber Defense
- MIS 514 Cloud Security
- MIS 526 Advanced Network Security Concepts
- MIS 555 Ethical Hacking
- MIS 674: Master's Capstone – Cybersecurity

Course Descriptions in the Cybersecurity Concentration

MIS 503: Cybersecurity Fundamentals

Cybersecurity Fundamentals provides a comprehensive introduction to the foundational principles and practices of cybersecurity, establishing a conceptual and technical framework for advanced study and professional application. The course begins by developing a shared understanding of cybersecurity terminology, concepts, and the evolving threat landscape. Students will explore critical domains including network and systems security, cryptography, data protection, and secure operating system design.

Building upon these core concepts, the course examines contemporary and emerging technologies such as the Internet of Things (IoT), mobile computing, robotics, and social media, emphasizing their unique security challenges and implications for organizational resilience. Students will analyze common cybersecurity attacks and defense mechanisms, evaluate risk management strategies, and assess the ethical, legal, and policy dimensions that shape modern cybersecurity practice.

MIS 504: Programming for Cybersecurity

This course provides an advanced exploration of programming concepts and techniques essential for cybersecurity professionals. Students will learn to design, implement, and analyze programs that enhance system security, automate security tasks, and identify vulnerabilities. The course covers secure coding practices, scripting for penetration testing and threat analysis, and the development of tools to detect and mitigate cyber-attacks. Emphasis is placed on applying programming skills to real-world cybersecurity challenges, with both hands-on exercises and critical evaluation of security implications.

MIS 513: Cyber Defense

This course provides an in-depth examination of the strategies, frameworks, and technologies used to protect organizational information assets from evolving cyber threats. Students will critically analyze adversarial tactics, techniques, and procedures (TTPs) used by malicious actors and evaluate advanced defensive methodologies for securing enterprise systems and networks. Emphasis is placed on the integration of cybersecurity controls with business objectives, risk management frameworks, and regulatory compliance requirements.

Key topics include advanced network and application defense, endpoint and mobile device security, identity and access management, incident response, and vulnerability assessment methodologies. Students will gain hands-on experience using contemporary security tools, including intrusion detection systems, firewalls, and threat intelligence platforms, while developing the analytical skills required to design, implement, and manage resilient cybersecurity architectures that align with organizational strategy.

MIS 514: Cloud Security

Cloud security covers an in-depth examination of cloud security architecture, governance, and risk management across public, private, and hybrid environments. Students will analyze frameworks for securing cloud infrastructures, evaluate compliance and regulatory considerations, and design resilient systems that align with enterprise cybersecurity strategies. Emphasis is placed on integrating advanced security controls, managing shared responsibility models, and addressing evolving threats within multi-cloud ecosystems.

The course prepares students for the Certificate of Cloud Security Knowledge (CCSK) and equips them with the practical and analytical skills necessary to lead secure cloud deployments in enterprise and government contexts.

MIS 525: Network Security Concepts

This course provides an in-depth exploration of modern network security principles, architectures, and governance frameworks. Students will critically examine the evolving landscape of network threats, vulnerabilities, and attack vectors, with a focus on advanced risk assessment methodologies and strategies. The course emphasizes the integration of technical, organizational, and regulatory considerations in designing and managing secure network infrastructures that align with enterprise objectives.

Key topics include advanced access control models, intrusion detection and prevention systems, secure network design, and application-layer security assessment. Students will also explore cryptographic foundations and emerging technologies such as blockchain within the context of data integrity and secure transactions. Special attention is given to the human dimension of cybersecurity—particularly social engineering, threat modeling, and compliance with legal and ethical standards. Through applied projects and case-based analysis, students will develop the analytical and strategic competencies required to assess, mitigate, and manage network security risks in complex organizational environments.

MIS 555: Ethical Hacking

This course explores the principles, methodologies, and tools of ethical hacking and network security. Students will examine system and network penetration testing, vulnerability exploitation, including social engineering and buffer overflows, as well as strategies for defending against cyber threats. The course emphasizes the role and definition of ethical hacking in protecting corporate and government data, providing both practical, hands-on experience and a critical understanding of cybersecurity challenges and solutions.

MIS 674: Master's Capstone - Cybersecurity

This capstone course serves as the culminating experience for the Master of Science in Cybersecurity, providing students the opportunity to synthesize and apply advanced knowledge through a comprehensive, simulation-based project. Students will engage in a realistic cybersecurity scenario that replicates the complexities of securing modern digital environments—such as defending against sophisticated attacks, managing incident response, or developing enterprise-level security strategies.

Students will analyze the simulated environment, assess vulnerabilities, design and test mitigation strategies, and implement defense mechanisms using an active environment. Emphasis is placed on strategic decision-making, technical proficiency, and the integration of governance, risk management, and compliance considerations.