CYBERSECURITY LEADERSHIP (CYB)

CYB 710. Foundations in Cybersecurity Leadership. (3 h)
This course provides a foundational understanding of the critical aspects of leading cybersecurity initiatives within an organization. The course includes frameworks and principles for developing and assessing a cybersecurity program. Students will explore cybersecurity terms and concepts, ethical considerations, leadership theories, risk management practices, strategic planning, and effective communication techniques necessary for driving cybersecurity initiatives. Through case studies and practical exercises, students will learn to navigate the complexities of cybersecurity leadership and build resilient cybersecurity programs. Students will be given an overview of the various roles and responsibilities that comprise a cybersecurity department in the industry.

CYB 712. Cybersecurity Law, Policy, and Privacy. (3 h)
An overview of cyber risks, along with the laws and regulations that apply to the rapidly changing threat landscape of cybersecurity. We will explore the impacts of cyberattacks, data privacy challenges, cyber-criminal motives, and common strategies used to combat cyber warfare. After studying the strategies and challenges of preserving the confidentiality, integrity, and availability of sensitive information such as personally identifiable information (PII), financial information, and protected health information (PHI), you will develop a cybersecurity risk mitigation strategy for workplace or personal data.

CYB 714. Advanced Information Security and Cyber Controls. (3 h)
This course covers fundamental security design principles and information assurance fundamentals. Students will explore a wide range of topics including cryptography, capability and access control mechanisms, authentication models, security models, operating systems security, malicious code, security policy formation and enforcement, vulnerability analysis, and the evaluation of secure systems. Emphasis will be placed on the implementation and management of cyber controls to mitigate risks and ensure robust security measures are in place.

CYB 720. Incident Management and Business Continuity. (3 h)
This course provides a comprehensive exploration of strategies and practices essential for responding to cybersecurity incidents and ensuring business continuity. Students will learn to plan, test, and execute incident management and disaster recovery strategies, including conducting Business Impact Analysis (BIA) to prioritize responses. The course emphasizes the importance of exercises to test preparedness plans and enhance cyber resilience. Topics include incident detection and response, crisis communication, ethics, coordination of recovery efforts, and the integration of cybersecurity measures into business continuity plans.

CYB 730. Emerging Cyber Technologies. (3 h)
This course is designed to keep students at the forefront of the rapidly evolving cybersecurity landscape by exposing them to the latest trends, tools, and innovations. This course covers cutting-edge technologies. Students will explore the potential impacts of these technologies on cybersecurity practices, assess their practical applications, and understand how to integrate them into existing security frameworks. Students will gain a comprehensive understanding of how to leverage emerging technologies in cybersecurity.

CYB 750. Cloud Security. (3 h)
This course explores advanced strategies and principles essential for securing cloud computing environments. Students will delve into the unique security challenges and considerations specific to cloud architectures, including multi-tenancy, cloud service models, data protection, and identity management. The course covers best practices for implementing and managing security controls in cloud environments, compliance requirements, and strategies for mitigating cloud-specific risks. Emphasis is placed on understanding cloud security frameworks, incident response in cloud environments, and the integration of cloud security into organizational cybersecurity strategies.

CYB 751. Proactive Cyber Defense. (3 h)
This course delves into advanced strategies and frameworks designed to anticipate, identify, and mitigate cyber threats. Key topics include security architectures such as Zero Trust, proactive threat hunting, continuous monitoring, and the integration of artificial intelligence (AI) and machine learning (ML) in cyber defense. Through a combination of theoretical knowledge and practical exercises, students will learn to design and implement robust defense mechanisms that enhance the resilience of digital infrastructures.

CYB 799. Capstone. (3 h)
This course requires students to synthesize and apply their acquired knowledge and skills through a comprehensive, project-based approach. Students will develop and present a capstone project that addresses real-world cybersecurity issues, integrating strategic, technical, and leadership aspects. Emphasis will be placed on aligning cybersecurity strategies with organizational goals and risk management frameworks, defining and ensuring adherence to cybersecurity policies and regulations, leveraging emerging technologies, planning and executing incident management and disaster recovery strategies, and addressing ethical challenges in cybersecurity. The course also focuses on enhancing executive communication and strategic communication across stakeholders.