CYBERSECURITY (CYBR)

CYBR 4930 - Special Topics
3 Credits (Repeatable for credit)

CYBR 5000 - Cybersecurity Principles
3 Credits
This course is an overview to the field of Cybersecurity. Students will be exposed to the key concepts of information and information security systems. Students will explore these concepts through a formal review of historical breaches across a variety of industries. Students will then explore best of practice security plans and process used in a holistic approach to cybersecurity for an organization.

CYBR 5010 - Networking Concepts
3 Credits
CYBR 5010 – Networking Concepts [Networking Concepts] This course will emphasize various networking technologies in use in modern networks. Students will design a basic network topology to meet the most common design requirements. Students will be introduced to network monitoring tools and networking mapping tools.

CYBR 5020 - Data Administration
3 Credits
This course combines the principles and practices of data security with scripting techniques for security tasks, offering a holistic approach to cybersecurity education. Students will gain in-depth skills in identifying and resolving security issues across diverse data system architectures and data management systems. Students will analyze and evaluate methods to protect the confidentiality, integrity, and availability of data throughout the data life cycle, covering topics such as data asset management, data audit principles, enforcement of access controls measures, data compliance, and policy development. Through a hands-on approach, students will learn to automate security tasks using various specific scripting tools and evaluate the suitability of different scripting languages and techniques in scenarios like network security, system administration, and vulnerability scanning.
Prerequisite(s): CYBR 5000 with a grade of C or higher

CYBR 5030 - Cyber Threats and Defense
3 Credits
This course is divided into two sections: computer network defense (CND) and computer network offense (CNA & CNE). Students will first review various security principles, controls and monitoring technologies (e.g., defense in depth, firewalls, IDS/IPS). Students will then review the various ways attackers defeat security controls and monitoring technologies. At the completion of the course, students will a more thorough understanding of how to defend networks.
Prerequisite(s): CYBR 5000 with a grade of C or higher

CYBR 5210 - Digital Investigations
3 Credits
This course will expose students to the forensic science principles and practices used in investigations. Students will be able to describe the steps in performing digital forensics from initial recognition of an incident through the steps of evidence gathering, preservation and analysis, and completion of legal proceedings.
Prerequisite(s): CYBR 5000 with a grade of C or higher

CYBR 5220 - Incident Response and Mitigation
3 Credits
This course will develop a student's ability to construct plans and processes for a holistic approach to cybersecurity for an organization. These plans will include the protection of intellectual property, the implementation of access controls and patch/change management.
Prerequisite(s): CYBR 5000 with a grade of C or higher

CYBR 5230 - Intrusion Detection and Analysis
3 Credits
This course will develop a student's competencies and skills related to detecting and analyzing vulnerabilities and threats and develop processes for taking steps to mitigate associated risks. Upon completing this course, students will demonstrate the ability to detect, identify, resolve and document intrusions.
Prerequisite(s): CYBR 5000 with a grade of C or higher

CYBR 5240 - Cloud Security
3 Credits
This course will develop a student's knowledge of the technologies and services that enable cloud computing. Students will analyze different types of cloud computing models and the security and legal issues associated with them.
Prerequisite(s): CYBR 5000 with a grade of C or higher

CYBR 5250 - Secure Software Development
3 Credits
This course will develop a student's competencies and skills related to the principles and practices of integrating security into the Software Development Lifecycle (SDLC) in order to design, create, and deploy secure software. Students will review industry standards for secure coding and testing techniques. Students will apply specific techniques such as entitlement models, data sensitivity analysis, regulatory and compliance review, and threat modeling to assess an application and then determine which manual and automated tools and techniques to integrate into each phase of the SDLC to remediate identified risks and vulnerabilities.
Prerequisite(s): CYBR 5020 with a grade of C or higher

CYBR 5850 - Advanced Cloud Computing Architectures and Applications
3 Credits
This course examines advanced cloud computing architectures and their applications in three critical domains: cloud-based analytics, cybersecurity, and cloud-native application development and deployment. Students will explore key architectural concepts in the areas of scalability, elasticity, fault tolerance, and their significance in various cloud service models such Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The course emphasizes designing and implementing solutions to address security challenges, developing and deploying applications using cloud-native methodologies, by utilizing technologies from industry-leading providers.
Prerequisite(s): CYBR 5240; IS 5800

CYBR 5910 - Internship Experience in Cybersecurity
1-3 Credits
This course provides students with an opportunity to complete an internship that requires them to apply the concepts and skills learned in their specific program of study. Prior to registration, students intending to complete this course are expected to have a formal letter from the organization providing details of the work expected from the student during the 8-weeks that constitute the length of the internship. The letter must be signed by an individual with appropriate authority from the organization sponsoring the internship. In addition, the internship is subject to approval by the program director who will assess the alignment between.
Restrictions:
Enrollment limited to students in the Schl for Professional Studies college.

Attributes: Special Approval Required

CYBR 5930 - Special Topics
3 Credits (Repeatable for credit)

CYBR 5960 - Masters Research Project
3 Credits
The Master's Research Project (MRP) emphasizes a synthesis and demonstration of the competencies gained during a student's time in the MS Cybersecurity program.
Prerequisite(s): ORLD 5050 with a grade of C or higher; CYBR 5000 with a grade of C or higher; CYBR 5010 with a grade of C or higher; CYBR 5020 with a grade of C or higher; CYBR 5030 with a grade of C or higher
Restrictions:
Enrollment limited to students in the Schl for Professional Studies college.

Attributes: Special Approval Required

CYBR 5980 - Graduate Independent Study in Cybersecurity
1 or 3 Credits (Repeatable for credit)