CYBERSECURITY (CYBR)

CYBR 1201. Database Systems and Security (3)
The course covers a foundation in database management systems (DBMS) and the essential principles of securing and protecting sensitive data. Topics include data modeling, databases design and implementation, SQL (Structured Query Language), data security, security models, and basic database security mechanisms. Students will be equipped with the knowledge and skills to design, implement, and secure database systems.

CYBR 1401. Introduction to Webmaster (3)
This course will focus on the hands-on business of writing HTML code, knowledge of basic control structures, language syntax, and file structures. Students will learn to plan and design web sites for target audiences. Students will learn techniques for client interfacing, project development, and web page mock-up. A best practice didactic will focus on hypertext design and navigation, application interface, copyright and ownership issues, ethics, and privacy, licensing, and trademark issues.

CYBR 1601. Introduction to Linux (3)
This course is an overview of the Linux operating system reinforced with examples and exercises performed on a Linux system. Introductory elements of shell programming and system administration will be covered.

CYBR 2010. Intro to Computer Forensics (3)
This course introduces general concepts and techniques in computer and cyber forensics, including understanding of computer structures, operating systems, file systems, computer network communication, and user access control. General concepts incident-handling process and methods for extraction and preservation of legal evidence, uncovering illicit activities, and recovering are also introduced.
Prerequisites: CSCI 1701

CYBR 2214. Web Application Development (3)
This course exposes students to techniques used in database design and web application development for interactive content. Interactive web-based database application design and development are covered including control mechanisms, models, and views design and development. Server-side scripting and advanced web languages are introduced to facilitate students building dynamic web pages with graphics, sound, video, and animation while accessing customized databases via the Internet. Student teams build an integrated database application using high-level tools.
Prerequisites: CYBR 1201 and CYBR 1401

CYBR 2502. Fund. of Networking and Securi (3)
Introduction to terminology and applications of communications and networking as essential elements of information technology and information systems that includes OSI and TCP/IP models. Students gain familiarity with concepts of data communication infrastructure, industry trends, hardware, software, media, transmission equipment, wireless and satellite communication, and network security concepts. Includes an emphasis on LAN architecture, standards, protocols, and implementation.

CYBR 2530. Foundations of Ethical Hacking (3)
This course introduces the fundamental concepts of ethical hacking and how to perform penetration tests of computer networks. Students will use tools to discover weaknesses in computer networks and how to improve the defenses of those networks against malicious attacks. Topics include network and computer attacks, footprinting and social engineering, port scanning, reconnaissance, and various types of attacks and counter measures. Students will also learn the legal considerations for working as an ethical hacker.
Prerequisites: CSCI 1701

CYBR 3012. Information Risk Management (3)
This course will provide students with a good understanding of identifying, assessing, analyzing, measuring, and responding to information risk. Students will be able to make risk mitigation and acceptance decisions given its resource constraints. Students will be able to use risk management tools, regulations, and methodologies for metrics to monitor risk management activities.
Prerequisites: CSCI 1701

CYBR 3112. Secure Software Development (3)
This course will provide students with software development lifecycles while applying approaches to secure software systems design and development that tightly integrates security and systems design and software development together. It addresses the software development process from the perspective of a security practitioner to minimize software vulnerabilities and counter cyber threats.
Prerequisites: CSCI 1300

CYBR 3201. IoT, Cloud, & Mobile Security (3)
The course explores securing IoT devices, cloud infrastructures, and mobile applications. The students will gain a deep understanding of the unique threats associated with these technologies and develop practical skills to design, implement, and manage robust security measures.
Prerequisites: CYBR 2502

CYBR 3311. Cyb. Laws, Ethics, & Policies (3)
This course delves into the critical intersections of cybersecurity, legal frameworks, ethical considerations, and policy development. In an era where technology and information are integral to every aspect of our lives, understanding the legal and ethical dimensions of cybersecurity is paramount. Students will gain insights into the dynamic landscape of cybersecurity laws and policies, examining their evolution, status, and potential future developments.
Prerequisites: CSCI 1701

CYBR 3601. Sec Testing & Quality Assur (3)
This course covers security testing and quality assurance, emphasizing testing methodologies. Topics include code analysis, static and dynamic analysis techniques, sandboxing, test strategies, test planning, functionality testing, stability testing, and debugging techniques. Other topics include web application tests and identifying potential vulnerabilities, misconfigurations, and weaknesses in software, computers, or networks.
Prerequisites: CYBR 2530

CYBR 3630. Cryptography and Info Security (3)
This course introduces the tools and techniques used in modern cryptography. Topics include secret and public key ciphers, one-way hashing algorithms, authentication and identification, digital signatures, key establishment and management, steganography, secret sharing and data recovery, public key infrastructures, and efficient implementation. Privacy and security at the upper layers are also discussed.
Prerequisites: CYBR 2502

CYBR 4010. Digital Foren and Incident Res (3)
This course covers concepts and techniques in the field of computer and cyber forensics, which includes investigating, acquiring, preserving and analyzing digitally stored information. Students will practice performing digital forensics investigations using industry-standard forensic tools, techniques and procedures in the digital forensic process. Students will analyze various effective plans for crisis management and incident-handling process, including methods and standards for extraction and preservation of legal evidence, uncovering illicit activities, recovering information left on digital storages and extracting files from intentionally damaged media.
Prerequisites: CYBR 2010

CYBR 4208. Disaster Recovery Planning (3)
This course introduces the principles of disaster recovery planning and examines countermeasures that may be used to prevent system failure for an organization. It explores the plans and preparations needed to recover from disasters affecting enterprise information systems and critical infrastructures with the goal of maintaining business continuity. Emphasis is given to the technological aspect of the planning for recovery and business continuity planning. Topics include disaster recovery planning, risk control policies and countermeasures, disaster recovery tools and services, and virtualization principles.
Prerequisites: CYBR 2530

CYBR 4306. Computer & Network Security (3)
An intermediate course in concepts and applications of computer networks including network topologies, network devices, standards, and protocols. The course will emphasize WAN concepts with details of IP addressing, routing, subnet/supernet concepts, TCP/IP protocol suite, data security including security models, and access control.
Prerequisites: CYBR 2502

CYBR 4310. Data Security and Analytics (3)
This course will provide students with a good understanding of data security laws and standards, risk management of data security, data security models, data security and auditing, data encryption. We will also cover various artificial intelligence analysis and risk assessment techniques applied to data security. The AI-based solutions will be discussed to support data threats and risk assessments and detection.
Prerequisites: CYBR 1201

CYBR 4417. OS Security, Prog. and Admin. (3)
This course covers computer operating systems, such as UNIX and Linux, systems programming, systems administration, and operating systems hardening.
Prerequisites: CYBR 3630

CYBR 4502. Secure Networks and Comm Proto (3)
Topics include hardware and software diagnostic tools and utilities, LANs MANs, WANs, and the Internet, OSI protocol stack, flow control, switching, data compression, application program-network interface, and security issues. Also included are recent advances in TCP/IP protocols including IPv6.
Prerequisites: CYBR 2502

CYBR 4900. Cybersecurity Capstone (3)
The course is a culminating experience designed to integrate and apply the knowledge, skills, and methodologies acquired throughout the cybersecurity program. The students will gain practical experiences by engaging in comprehensive, real-world cybersecurity projects, tackling complex challenges and applying their proficiency in various cybersecurity domains.
Prerequisites: CYBR 4417 or CYBR 4010