CYB - CYBERSECURITY

CYB 2413 Advanced Networking (2-2-3)
This course equips the students with the essential skills and understanding of networking principles required to design, implement, and manage an enterprise network infrastructures. Through a balanced foundation of theoretical knowledge and practical experience, students will gain expertise in the fundamental concepts, protocols, and standards that underpin modern data communication.
Prerequisites: CIS 1313

CYB 2423 Cryptography and Data Protection (2-2-3)
The course provides an in-depth exploration of cryptography techniques and their applications in data protection. Students will learn about symmetric and asymmetric encryption algorithms, cryptographic protocols, key management, data classification, regulatory compliance, and privacy-enhancing technologies. Practical exercises and case studies will reinforce theoretical concepts, equipping students with the knowledge and skills to design and implement secure cryptographic solutions.
Prerequisites: CIS 1213

CYB 3513 Switching, Routing and Wireless Essentials (2-2-3)
This course equips students with the skills and knowledge necessary to effectively manage modern networks. Through a blend of theoretical concepts and practical hands-on experience, students will learn to configure and troubleshoot switching, routing, and wireless networking environments. Key topics include VLANs, inter-VLAN routing, network redundancy, IPv4 and IPv6 routing, and securing wireless LANs.
Prerequisites: CNS 2103 or CIN 2103 or CYB 2413

CYB 3523 Virtualization and Cloud Technologies (2-2-3)
This course equips students with the knowledge and skills required to understand virtualization concepts and apply different types of virtualization solutions in the context of cloud technologies. Students will gain insight into the fundamentals of cloud computing, covering essential topics such as cloud infrastructures, software-defined networks and storage, cloud storage, and programming models.
Prerequisites: CNS 2103 or CYB 2413

CYB 3533 Penetration Testing and Ethical Hacking (2-2-3)
This course introduces students to penetration testing and ethical hacking, focusing on skills to assess, enhance, and secure information systems. Through theoretical knowledge and practical exercises, students learn to think like hackers to defend against them. The course covers reconnaissance, scanning, enumeration, vulnerability assessment, exploitation techniques, and post-exploitation activities. With emphasis on ethical considerations and legal compliance, the course prepares students for roles in cybersecurity domain, equipping them to conduct effective and ethical penetration test.
Prerequisites: CIS 2903

CYB 3543 Digital Forensics and Investigation (2-2-3)
This course provides an in-depth exploration of computer forensics methodology, crucial for managing civil, criminal, and administrative investigations within the framework of Cyber Laws. It integrates essential elements of computer science and law, training students to proficiently collect and analyze data from various computer systems. Throughout the course, students will be introduced to advanced techniques for obtaining and scrutinizing digital evidence in legal contexts, emphasizing the acquisition, preservation, and evaluation of digital artifacts.
Prerequisites: CIS 2903

CYB 3613 Secure Software Architecture and Coding (2-2-3)
This course explores the principles and practices essential for engineering secure and dependable software systems. Students will explore the full system development lifecycle (SDLC) with an emphasis on integrating security at each phase. The curriculum covers secure design principles, threat modeling, secure coding practices, security testing, and maintenance. The course aims to equip students with the skills needed to build and maintain resilient systems that can withstand malicious attacks and protect sensitive data.
Prerequisites: CNS 3123 or CYB 3533

CYB 3623 Enterprise Networking, Security and Automation (2-2-3)
This course equips students with the skills and knowledge necessary to effectively manage modern networks. Through a blend of theoretical concepts and practical hands-on experience, students will learn to configure and troubleshoot switching, routing, and wireless networking environments. Key topics include VLANs, inter-VLAN routing, network redundancy, IPv4 and IPv6 routing, and securing wireless LANs.
Prerequisites: CNS 3003 or CIN 3003 or CYB 3513

CYB 3633 Security Operation and Threat Intelligence (2-2-3)
This course offers a comprehensive overview of cybersecurity operations and incident response. Students will develop skills in creating incident response and disaster recovery plans, mastering various monitoring and recovery tools. Emphasis is placed on integrating threat intelligence into incident response processes for proactive defense. The course also explores the application of AI tools to enhance cybersecurity defense, promoting a cohesive approach to managing and mitigating cyber threats. Through hands-on exercises and real-world case studies, students will gain practical skills.
Prerequisites: CNS 2103 or CYB 2413

CYB 3643 Cloud Architecting (2-2-3)
This course equips students with the technical and management skills needed to effectively design cloud-based solutions using appropriate architectural design principles and best practices. Students will learn to address customer requirements and deliver quality cloud-based solutions that achieve high availability, scalability, performance efficiency, and cost optimization.
Prerequisites: CCC 4013 or CIN 3503 or CCC 4003 or CIS 4403 or CYB 3523

CYB 4716 Apprenticeship I (1-20-6)
The Apprenticeship I course is a vital and engaging component of the HCT curriculum, integrating practical On-the-Job experience as a graduation requirement. Students are placed in carefully chosen Industrial Hosting Companies to gain real-world experience through a structured program. As a formal course, it requires each student to complete a minimum of 20 hours onsite per week throughout a regular semester.
Prerequisites: CIS 3303

CYB 4723 Cyberspace Law and Ethics (2-2-3)
This course is designed to provide an in-depth understanding of the intricate relationship between technology, law, and ethics, particularly in the context of cyberspace. Throughout the course, students will engage in a comprehensive analysis of how technological advancements impact legal frameworks, ethical considerations, and management decisions within organizations, both globally and specifically in the United Arab Emirates (UAE).
Prerequisites: CIS 1213
Corequisites: CYB 4716

CYB 4733 Capstone Project I (1-3-3)
Students form teams to explore new and innovative ideas and define their projects. They apply their knowledge of the development life cycle, project management, development tools, and skills gained throughout the program to propose, plan, analyze, and design an innovative Cybersecurity solution in response to an identified organizational or community need. Students complete project milestones and outcomes under the supervision of a faculty and an industry mentor. Students are evaluated on each project phase and their ability to communicate, work in a team, and apply project management tools.
Prerequisites: CIS 3603
Corequisites: CYB 4716

CYB 4816 Apprenticeship II (1-20-6)
The Apprenticeship II course is a crucial part of the HCT curriculum, offering practical On-the-Job experience as a graduation requisite. Students engage in a structured program at selected Industrial Hosting Companies, completing a minimum of 20 hours onsite weekly for a semester. With guidance from both host organization staff and HCT mentors, students apply cybersecurity practices and skills from their studies in a real-world environment.
Prerequisites: CYB 4716

CYB 4823 Cybersecurity Governance, Risk and Compliance (2-2-3)
This advanced course explores the complex dynamics between cybersecurity governance, risk management, and compliance (GRC) within modern enterprises. It covers key topics such as governance frameworks, risk assessment methodologies, and compliance management, enriched with case studies, simulations, and insights into emerging technologies. Designed for future cybersecurity leaders, the curriculum equips students to develop and implement comprehensive cybersecurity frameworks that enhance organizational security, ensure regulatory adherence, and promote operational integrity.
Prerequisites: CYB 3533
Corequisites: CYB 4816

CYB 4833 Capstone Project II (1-3-3)
The Capstone project is carried forward from the previous semester with student teams moving to the development, testing, and implementation of their project designs. Students continue to complete project milestones under the supervision of faculty and an industry mentor. They are evaluated on their ability to develop solutions based on their design, test the proposed solutions, and implement them. Students are expected to demonstrate skills in knowledge integration, computing, entrepreneurship, communication, self-management, and collaborative teamwork.
Prerequisites: CYB 4733
Corequisites: CYB 4816