CYBER (CYB)

CYB-251 NETWORKING I 4.00 Credits
This course lays a foundation for network fundamentals. In this course students will learn how to design and implement functional networks, configure, manage, and maintain essential network devices, and many more. Students gain hands-on experience to pass the CompTIA Network+ exam. The lab provides a hands-on learning experience in a safe, online environment. This course includes topics such as network policies; network components; Ethernet technology; routing IP packets; IPv4 and IPv6 addresses. Pre-requisite: CS-211.

CYB-252 NETWORKING II 4.00 Credits
This course introduces intermediate computer networking standards, best practices, theory, and practical application. In this course students will start to gain the skills required to pass the Cisco CCNA certification exam including TCP/IP network models, ethernet LANs, WANs and IP routing, command-line interfaces, switching management, and spanning tree protocol concepts. Pre-requisite: CYB-251.

CYB-253 NETWORKING III 4.00 Credits
This course comprehensively covers Ethernet LANs, command-line interface, LAN switching, networking protocols, subnets, and many more. The gives student's the knowledge and skills required to install, configure, and operate a small to medium-sized network. This course provides foundational knowledge in the essentials of networking, security, and automation. In this course students will gain the skills required to pass the Cisco CCNA certification exam. The lab is versatile and delivers hands-on experience, replacing expensive physical labs. Pre-requisite: CYB-252.

CYB-254 NETWORKING IV 4.00 Credits
In this course students are introduced to advanced computer networking concepts, theories, practices, and procedures. Students learn about the concepts of computer network defense and countermeasures. This course completely covers the techniques and methodologies related to network defense including knowledge and practical applications of firewalls and intrusion detection systems. The labs simulate real-world, hardware, software, and command-line interface environments. Pre-requisite: CYB-253.

CYB-271 CYBERSECURITY I 4.00 Credits
This cybersecurity course and lab cover the cybersecurity basics of infrastructure security, network security, security devices, local network security, and access control monitoring systems. In this course students learn the concepts and methodologies being used in the field of cybersecurity. The labs simulates real-world, hardware, software, and command line interface environments. Pre-requisite: CS-211.

CYB-272 CYBERSECURITY II 4.00 Credits
This course examines the tools and techniques used for traffic and intrusion analysis employed in today's cyber environment. This includes processes and procedures used by hackers, along with corresponding countermeasures that may be employed to protect against such attacks. Students will learn the skills necessary to take the CompTIA Security+ exam. Pre-requisite: CYB-271.

CYB-273 CYBERSECURITY III 4.00 Credits
In this course students gain hands-on expertise with Linux cybersecurity principles. The lab is cloud-based device-enabled. Students are provided the knowledge and skills in managing local storage, group, and user accounts; working on the command line, editing files, and developing a storage security policy. Pre-requisite: CYB-272.

CYB-274 CYBERSECURITY IV 4.00 Credits
In this course students will learn and be able to apply the appropriate incident response procedures, analyze potential indicators of compromise, and utilize basic digital forensics techniques. This course provides students with the ability required to capture, monitor, and respond to network traffic findings along with software and application security; automation, threat hunting, and IT regulatory compliance. This course will allow students to gain the skills required to pass the CompTIA Cybersecurity Analyst (CySA+) course and lab. Pre-requisite: CYB-273.

CYB-300 CYBER ETHICS 3.00 Credits
The goal of this course is to provide students with the conceptual tools to understand the technological, geopolitical, and legal environment affecting software, technology and information processing. Specific issues to be covered will include the internet and ethical values, regulation and governance of networked technologies, free speech and censorship in cyber space, intellectual property in cyberspace, privacy rights, and securing the digital infrastructure.

CYB-360 CYBERSECURITY MANAGEMENT 3.00 Credits
Covers the fundamental concepts required for cybersecurity management. Topics include: fundamental security management, organizational cybersecurity threat landscapes, qualitative and quantitative risk analysis, vulnerability assessment, return on security investment, legal and regulatory compliance, and security best practices. This course will focus heavily on case studies and court cases involving cybersecurity breaches. Pre-requisite: CYB-271.