# INFORMATION SYSTEMS SECURITY (ISS)

**ISS 105 Intro to Cybersecurity (GI) (3 credits)**
This course introduces students to the evolving field of cybersecurity. Students learn about cyber-attacks and techniques for identifying, detecting, and defending against common cybersecurity threats. Students learn about software and hardware, network, Internet, and wireless security as well as a foundation for a more advanced study of cybersecurity.

**ISS 111 Cisco 1 (4 credits)**
This course, the first of three courses leading to the Cisco Certified Network Association (CCNA) certification, introduces the architectures, models, protocols, and networking elements that connect users, devices, applications and data through the internet and across modern computer networks - including IP addressing and Ethernet fundamentals. By the end of the course, students can build simple local area networks (LANs) that integrate IP addressing schemes, foundational network security, and perform basic configurations for routers and switches. Course includes 45 lecture hours and 30 lab hours per semester. Course fee: $40

Prerequisite(s): CIS 102

**ISS 112 Cisco 2 (4 credits)**
This course, the second of three courses leading to the Cisco Certified Network Association (CCNA) certification, focuses on switching technologies and router operations that support small-to-medium business networks and includes wireless local area networks (WLANs) and security concepts. Students learn key switching and routing concepts. They can perform basic network configuration and troubleshooting, identify and mitigate LAN security threats, and configure and secure a basic WLAN. Course includes 45 lecture hours and 30 lab hours per semester. Course fee.

Prerequisite(s): ISS 111

**ISS 210 Ethical Hacking & Systm Defens (3 credits)**
This course introduces the fundamentals of protecting information technology resources against network hacking. Students learn the tools and penetration testing methodologies used by ethical hackers, as well as the methods and tools to protect against attacks. Students identify potential network and system vulnerabilities. Computer crime-related laws and regulations are studied. This course provides additional preparation for the EC Council Certified Ethical Hacker exam.

Prerequisite(s): (CIS 210) and (ISS 105)

**ISS 212 Cisco Cybersecurity Operations (4 credits)**
This course aligns with the CCNA Cyber Ops certification. Students need to pass the 210-250 SECFND exam and the 210-255 SECOPS exam to achieve the CCNA Cyber Ops certification. CCNA Cybersecurity Operations covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level cybersecurity analyst working in a Security Operations Center (SOC). Course includes 45 lecture hours and 30 lab hours per semester.

Prerequisite(s): (CIS 210)

**ISS 213 Cisco 3 (4 credits)**
This course, the third of three courses leading to the Cisco Certified Network Association (CCNA) certification, describes the architectures and considerations related to designing, securing, operating, and troubleshooting enterprise networks. This course covers wide area network (WAN) technologies and quality of service (QoS) mechanisms used for secure remote access. ENSA also introduces software-defined networking, virtualization, and automation concepts that support the digitalization of networks. Students gain skills to configure and troubleshoot enterprise networks, and learn to identify and protect against cybersecurity threats. They are introduced to network management tools and learn key concepts of software-defined networking, including controller-based architectures and how application programming interfaces (APIs) enable network automation. Course includes 45 lecture hours and 30 lab hours per semester. Course fee.

Prerequisite(s): ISS 112

**ISS 214 Cisco 4 (4 credits)**
This course is the fourth of four courses leading to the Cisco Certified Network Associate (CCNA) designation. The course focuses on advanced Internet Protocol (IP) addressing techniques, such as, Network Address Translation (NAT), Port Address Translation (PAT), and Dynamic Host Configuration Protocol (DHCP), Wide Area Network (WAN) technology and terminology, Point-to-Point Protocol (PPP), Integrated Services Digital Network (ISDN), Dial-on-Demand routing (DDR), Frame Relay, network management, and introduction to optical networking. Course includes 45 lecture hours and 30 lab hours per semester. Course fee.

Prerequisite(s): ISS 213 (may be taken concurrently)

**ISS 220 Strategic Infrastructure Security (3 credits)**
This course focuses on security-related issues and the essential skills needed to implement security in a network in an enterprise environment, such as risk analysis, security policies, penetration testing techniques, Transfer Control Protocol (TCP), packet analysis, cryptography, operating system (OS) hardening, virus protection, and disaster recovery. CIS 210 should be taken prior to or at the same time as this course. Course fee.

Prerequisite(s): (CIS 210 (may be taken concurrently))

**ISS 221 Network Defense & Countermeasures (3 credits)**
This course focuses on the architecture for network defense including network attacks and defenses, firewall systems design and configuration, virtual private network (VPN) configuration, designing and configuring intrusion detection systems, intrusion signature, and network security policies and configurations. Course fee.

Prerequisite(s): (ISS 220)

**ISS 222 Computer Forensics (3 credits)**
This course introduces students to computer forensics, the emerging role of the computer forensics examiner, forensic evidence preservation, and legal and ethical foundations. This course provides a comparative study of information technology, evidence analysis, chain of custody, and data retrieval from computer hardware and software applications. Students have hands-on experiences using various computer forensic methods, evidence preservation techniques and documentation. Course fee.

Prerequisite(s): (CIS 210 and ISS 111 and ISS 112)